EMPRESA **EXCELENTE**

Las mejores temáticas sobre Normas ISO, HSE y GRC

2024

NOVIEMBRE

ESGinnova Group

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

Índice

Índice

Índice

ESG Innova Group

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

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

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

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

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

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

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

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

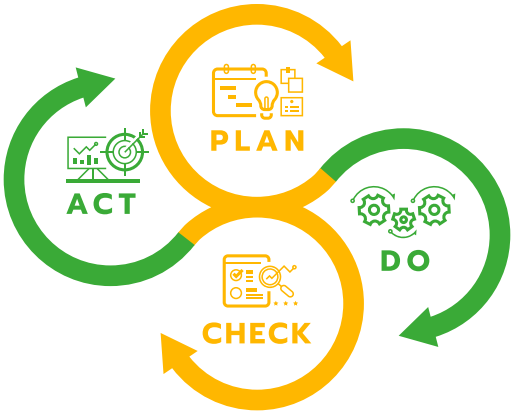
Plataforma ESG Innova

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

❖ Motor de mejora continua

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

ESGinnova Group



❖ Plan

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

❖ Do

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

❖ Check

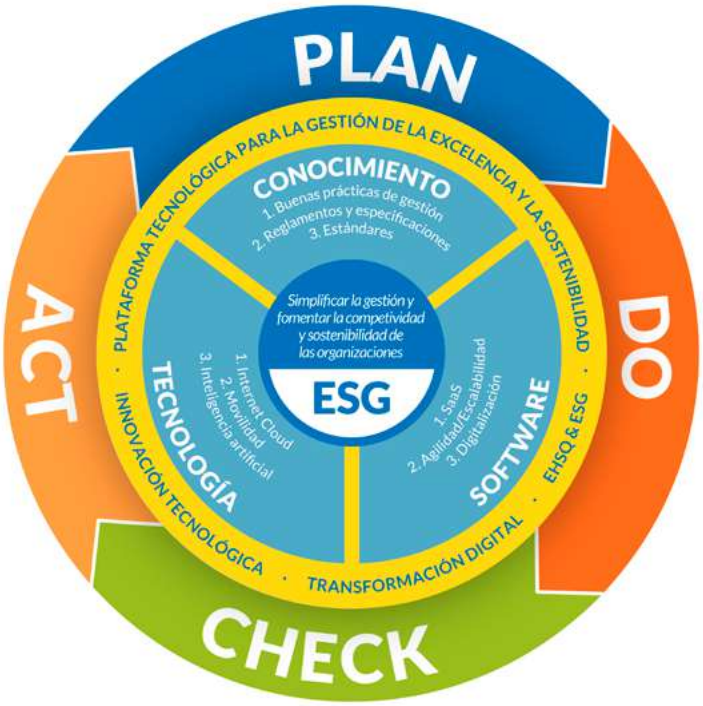
Simplificamos la monitorización y seguimiento, aportando información útil para la toma de decisiones.

❖ Act

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

Unidades de negocio

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



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

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

Unidades de negocio

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

ISOTools

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

HSETools

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

GRCTools

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

La Plataforma ESG aporta resultados en el corto plazo

Optimización del tiempo

50%
Menos de tiempo de resolución de una acción correctiva

20%
Menos de tiempo de preparación de las reuniones de gestión

75%
Menos de tiempo dedicado a recopilar y tratar indicadores

Optimización de los costes

90%
Menos de intercambios de documentación física entre sedes y dptos.

75%
Menos de costes indirectos derivados de la gestión documental

ROI
1-2 AÑOS
La inversión se rentabiliza entre el primer y el segundo año

Optimización del rendimiento

25%
Más de optimización en el sistema de gestión tras la etapa de consultoría

4
VECES
Más capacidad de resolución de problemas del sistema de gestión

100%
Más de trabajadores implicados en la gestión del sistema

ESGinnova Group

ISOTools

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

¿Cuál es la diferencia entre ISO 42001 e ISO 27001?

La **diferencia entre ISO 42001 e ISO 27001** se podría resumir en el objetivo de gestión: mientras la primera se enfoca en los **Sistemas de Inteligencia Artificial**, la segunda lo hace en la Seguridad de la Información.

Los dos estándares comparten una estructura de Alto Nivel y se enfocan en prevenir o eliminar riesgos en sus respectivas áreas. Aunque existen puntos de coyuntura y de colaboración relevantes, es la diferencia entre ISO 42001 e ISO 27001 la que permite entender cuál es la funcionalidad de cada una y por qué una no sustituye a la otra.

Diferencia entre ISO 42001 e ISO 27001 en alcance y objetivos

La principal diferencia entre ISO 42001 e ISO 27001 es **su objetivo de gestión**: mientras una se enfoca en la gestión de los Sistemas de Inteligencia Artificial (ISO 42001), la otra lo hace en la **Seguridad de la Información** (ISO 27001).

El objetivo específico de ISO 42001 es mitigar o eliminar los riesgos asociados al uso o desarrollo de Inteligencia Artificial relacionados con la ética, la transparencia, el respeto de los derechos humanos, la equidad, la inclusión, la gobernanza e incluso los derechos de propiedad intelectual.

ISO 27001 busca garantizar la seguridad, la confidencialidad y la transparencia en el tratamiento de la información de la organización o de aquella otra que la organización debe tratar por alguna razón, en cualquier formato: digital, papel u oral. De lo anterior se desprende que la norma tiene alcance sobre los equipos, las personas, las instalaciones físicas o sobre las redes de transmisión de datos, de voz o de información en general.

Además de compartir la estructura de Alto Nivel, **las dos entregan sendos anexos con controles para la prevención o eliminación de riesgos**. Por supuesto, cada una lo hace con el enfoque en las amenazas sobre la capacidad para alcanzar sus objetivos específicos.

Los dos, para hablar de similitudes y no solo de diferencia entre ISO 42001 e ISO 27001, son estándares que **contribuyen de forma significativa a la gobernanza de las organizaciones**, particularmente las que se compromete con criterios ESG.

¿La diferencia entre ISO 42001 e ISO 27001 impide su integración?

No. Al contrario, es el camino para tomar. Es importante entender que **las dos normas son complementarias** y que tienen puntos de confluencia inevitables, relacionados con la gestión de los datos y la privacidad de la información, que forman parte de las preocupaciones de ISO 42001.

ISO/DIS 37009: Conflicto de intereses en las organizaciones

ISO/DIS 37009

Para las organizaciones, llevar a cabo una adecuada gestión adecuada de los **conflictos de intereses** es un imperativo del entorno empresarial, lo que en ocasiones puede suponer un desafío. El manejo deficiente de este tipo de situación puede derivar en **problemas éticos, legales y de reputación**, afectando la integridad y la sostenibilidad de las operaciones. Aquí entra en juego la nueva norma en desarrollo, **ISO/DIS 37009**. Esta norma establece las directrices necesarias para abordar esta problemática crítica de las organizaciones.

¿Qué es ISO/DIS 37009?

ISO/DIS 37009, en su fase de Draft International Standard (DIS), proporciona un marco normativo integral para la **gestión de conflictos de intereses** en las empresas públicas y privadas.

Esta norma da respuesta a la necesidad de estándares internacionales que promueva la transparencia, la ética y la gobernanza responsable.

La ISO 37009 está diseñada como complemento para otras normas de gobierno corporativo como **ISO 37001 (Sistema de Gestión Antisoborno)** y **ISO 37301 (Sistema de Gestión de Cumplimiento)**. Su implementación ayuda a las empresas a prevenir, detectar y gestionar conflictos de intereses que puedan comprometer sus decisiones.

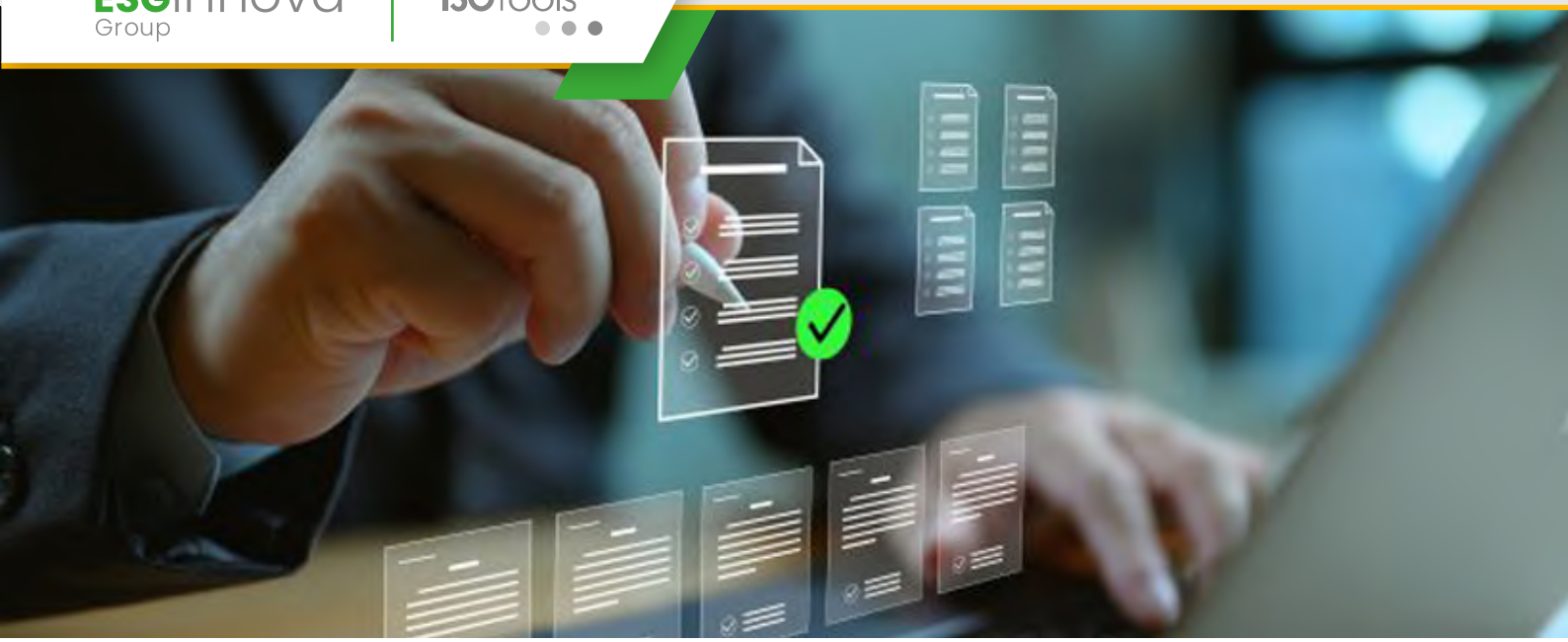
¿Por qué es importante gestionar los conflictos de intereses?

Un conflicto de intereses ocurre cuando una persona o grupo dentro de la organización tiene un interés personal que podría influir en la imparcialidad de sus decisiones. Si no se aborda de manera adecuada, este tipo situación puede mermar la confianza, afectar a la toma de decisiones y exponer a las empresas a **riesgos legales y de reputación**.

ISO/DIS 37009 propone herramientas y estrategias para:

- **Identificar y evaluar los riesgos de conflictos de intereses.** La identificación proactiva previene que los intereses personales interfieran con las funciones de la organización.
- **Establecer políticas claras.** La norma ISO/DIS 37009 guía a las empresas para desarrollar políticas que promuevan la transparencia y la integridad.
- **Implementar controles y medidas para mitigar.** Estas incluyen la declaración de intereses y la formación en materias éticas.

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO



No conformidades de calidad: qué proceso seguir para optimizar la gestión

No conformidades de calidad

Las **no conformidades de calidad** son elementos de importancia crítica en un sistema de gestión de la calidad. Aunque cualquier profesional en el área desearía no tener que tratar con ellas, lo cierto es que son inevitables, en mayor o menor cantidad.

Las consecuencias de **identificar no conformidades de calidad y reaccionar con prontitud**, siguiendo el procedimiento que indica la norma, son positivas para la gestión y para la **mejora continua** del sistema.

La reacción para atender no conformidades de calidad debe ser inmediata. La velocidad de la gestión en estos casos es la clave para **evitar un efecto dominó** que puede llegar hasta la parálisis de la operación, en casos de extrema gravedad.

Es preciso advertir que **no todas las no conformidades de calidad son iguales**. Existen varios tipos, dependiendo de su origen y de su gravedad. A continuación, exploramos esas variantes, el contexto exacto de lo que es una no conformidad y la forma procedente para tratarlas de acuerdo con lo prescrito por **ISO 9001:2015**.

Qué son no conformidades de calidad

Las no conformidades de calidad **son problemas, desviaciones, funcionamiento inadecuado** de un proceso o el incumplimiento total o parcial de un requisito del estándar ISO 9001.

Estas desviaciones o fallos **tienen diferentes orígenes**: error humano, falta de comprensión o de conocimiento, negligencia, confluencia de factores internos o externos, problemas técnicos, etc. Son factores que es necesario identificar para emprender el proceso de **acciones correctivas**.

Todas las no conformidades de calidad requieren acción correctiva. Algunas se generan debido a la ineficacia para identificar un riesgo. Todas, sin embargo, representan una oportunidad: la mejora continua.

Cuáles son los tipos de no conformidades de calidad

De acuerdo con su origen, las no conformidades de calidad **pueden ser internas o externas**. Las externas suelen relacionarse con **requisitos legales y reglamentarios en ISO 9001** de proveedores, de clientes o con incumplimiento de regulaciones. Las internas lo hacen con procedimientos o procesos en el interior de la organización.

Cuáles son los controles Operativos Eficientes según la Norma ISO14001

La **ISO14001** es una norma internacional que establece los requisitos para la **gestión ambiental** en las organizaciones. Los **controles operativos** son medidas clave en esta norma, ya que permiten a las empresas **gestionar** sus **impactos ambientales** de manera **eficiente**. Estos controles son procedimientos y prácticas diseñadas para **garantizar** que las **actividades, productos o servicios** se realicen en **línea** con los **objetivos** ambientales de la organización, **minimizando así el impacto negativo** sobre el medio ambiente.

ISO14001

Los **controles operativos** en la **ISO 14001** ayudan a las empresas a gestionar de forma **proactiva** los riesgos ambientales. En lugar de responder a los problemas después de que ocurren, estos controles permiten a las organizaciones **identificar y mitigar los riesgos desde el principio**.

Esto **reduce el impacto ambiental** y mejora la **eficiencia** y **sostenibilidad** de las operaciones.

La **ISO14001** requiere que las organizaciones **cumplan con todas las leyes y normativas** ambientales aplicables. Los controles operativos permiten **implementar** y verificar el **cumplimiento normativo**, ayudando a la organización a **evitar sanciones** legales y a **fortalecer su reputación** como entidad comprometida con el **medioambiente**.

Tipos de controles operativos eficientes

Controles preventivos

Los **controles preventivos** son aquellos que buscan **anticiparse** a los riesgos ambientales antes de que ocurran. Estos incluyen medidas como la planificación del **uso de recursos**, la **evaluación del ciclo de vida** de los productos y la implementación de prácticas de **mantenimiento preventivo** para reducir el consumo de energía y la emisión de contaminantes. Estos controles son esenciales para **minimizar el impacto ambiental** en cada etapa de las operaciones.

Controles correctivos

Cuando un problema ambiental ocurre, los **controles correctivos** permiten **tomar medidas rápidas y efectivas** para remediar la situación. Estos controles incluyen protocolos para manejar derrames, fugas o accidentes ambientales, así como **planes de respuesta en caso de emergencia**. La **ISO14001** exige que las empresas dispongan de **controles correctivos** bien definidos para **minimizar el impacto** de cualquier incidente.

¿Qué dice el proyecto ISO/DIS 37009?

El proyecto de **norma ISO/DIS 37009** aborda un desafío crucial en el ámbito organizacional: la **gestión de los conflictos de interés** dentro de los **sistemas para gestionar los riesgos y la seguridad**. Aunque los conflictos de interés son comunes en las organizaciones, gestionarlos adecuadamente es esencial para mantener la **ética** y la **integridad** en el trabajo. Esta futura norma proporciona una estructura completa para identificar, gestionar y resolver los conflictos de interés, promoviendo la transparencia y la confianza tanto en el **sector público** como **privado**.

ISO/DIS 37009

ISO/DIS 37009, que significa *Draft International Standard* o borrador de norma internacional, está diseñado para convertirse en una referencia global para la gestión de conflictos de interés en las organizaciones. Esta norma establece directrices claras para el manejo ético y proactivo de situaciones en las que los **intereses personales o de grupo** podrían afectar la toma de decisiones organizacionales.

El contenido del proyecto ISO/DIS 37009 abarca:

01. **Definiciones clave**: Especifica qué se entiende por conflictos de interés, desde los conflictos personales hasta los institucionales.

02. **Principios de gestión**: Promueve principios de transparencia, integridad y responsabilidad para prevenir y mitigar estos conflictos.

03. **Procedimientos recomendados**: Detalla pasos específicos para identificar y gestionar conflictos de interés, incluyendo la creación de políticas internas y la formación de los equipos.

ISO/DIS 37009: ¿Por qué es relevante para el sector empresarial?

Los conflictos de interés, aunque a menudo son percibidos como inevitables, representan un riesgo significativo para las empresas de todos los tamaños. Una **mala gestión** de estos conflictos puede **dañar la reputación corporativa**, disminuir la confianza de los inversores y provocar problemas legales y éticos. Por ello, adoptar la norma ISO/DIS 37009 permite que las empresas establezcan una estrategia para actuar con integridad y mantener relaciones transparentes y confiables.

ISO/DIS 37009 ayuda a las empresas a:

- **Aumentar la confianza** de sus clientes, empleados y otros stakeholders.
- **Minimizar riesgos de corrupción** y malas prácticas.

5 claves del nuevo marco sobre conflicto de interés: ISO 37009

ISO 37009

La transparencia y la ética son dos pilares muy importantes en lo que respecta al éxito y la sostenibilidad de las empresas. La **norma ISO 37009 busca reforzar estos principios**, a través de un marco sólido para la gestión de los conflictos de interés de forma eficaz. Esto ayudará a prevenir situaciones que comprometan la integridad corporativa.

Si tu organización aspira a **fortalecer el gobierno corporativo y construir un ambiente de trabajo ético**, es esencial entender los aspectos clave de esta norma. A continuación, te explicamos cinco puntos críticos del nuevo marco que no puedes pasar por alto.

1. Definir qué es un conflicto de interés

ISO 37009 define y actualiza el concepto de conflicto de interés para reflejar de la mejor forma posible los desafíos de las empresas actuales. La norma reconoce que los conflictos pueden surgir en las interacciones financieras, en decisiones estratégicas, relaciones personales y otros contextos menos evidentes. Esto permite a las empresas **ampliar su campo de actuación para detectar y prevenir de riesgos.**

2. Identificar y evaluar

El marco de ISO 37009 establece las guías para identificar posibles conflictos antes de que afecten las operaciones. Las empresas deben llevar a cabo análisis sistemáticos, considerando las situaciones obvias y los escenarios de conflicto potenciales. Además, se recomienda **hacer evaluaciones de forma periódicas para mantener el proceso actualizado.**

3. Establecer mecanismos de control y gestión con la ISO 37009

Una de las innovaciones de ISO 37009 es el énfasis en crear de mecanismos efectivos de **control interno**. La norma busca implementar políticas claras, crear comités de ética y usar de herramientas tecnológicas para el monitoreo continuo. De esta forma, se asegura una gestión robusta y alineada con las mejores prácticas internacionales.

4. Transparencia y comunicación

La transparencia es un valor ético y un mecanismo de protección para las empresas.

Beneficios de obtener la Certificación ISO/IEC 42001 para Sistemas de Gestión de Inteligencia Artificial

La **certificación ISO/IEC 42001** confirma el cierre de una etapa dentro de un proyecto en el que una organización decide crear un marco estandarizado para asegurar un uso responsable, transparente, ético e igualitario de los **Sistemas de Inteligencia Artificial**.

Con la certificación ISO/IEC 42001, un organismo avalado por ISO declara que la organización evaluada ha implementado un Sistema de Gestión de Inteligencia Artificial que está **conforme con los requisitos solicitados por la norma**.

Esto no significa, sin embargo, que el trabajo haya terminado. Es el comienzo de una etapa aún más interesante en la que se **busca la mejora continua** y, claro está, una revalidación de la certificación ISO/IEC 42001 en tres años.

Ante la previsible pregunta sobre si se justifica tanto esfuerzo, se anticipa una respuesta contundente: sí. Es así porque **los beneficios de la certificación ISO/IEC 42001 son muchos y muy atractivos para cualquier organización**. Los repasamos, tras una definición de la norma y su importancia.

Qué es ISO/IEC 42001 y por qué es importante

ISO/IEC 42001 es el estándar internacional provisto por ISO para gestionar los sistemas de Inteligencia Artificial. Puede ser utilizado por todas las organizaciones que desarrollen o hagan uso de ellos, sin importar su tamaño o su complejidad.

La norma crea una estructura de gestión basada en **tres ejes fundamentales: la ética, el cumplimiento legal y los derechos de las personas**. Estos ejes se alinean con la estrategia de negocios de la empresa, de tal forma que se utiliza la IA dentro de un marco de alta seguridad, contribuyendo al bienestar de las personas y de la comunidad.

Todos los sistemas de gestión son importantes. Pero este, y en particular obtener la certificación ISO/IEC 42001, cobra especial relevancia por una razón: **el uso de Inteligencia Artificial despierta serias preocupaciones** para millones de personas y cientos de organizaciones y estados.

Por eso, es importante contar con una herramienta que asegure el uso ético y responsable de tan interesante avance tecnológico.

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO

Cómo lograr la confianza digital a través de la norma ISO/IEC 27001

Confianza digital es un concepto que incorpora valores éticos y de transparencia para hacer que los usuarios de un sitio web, de una aplicación o cualquier tipo de plataforma se sientan seguros y protegidos a través de **Sistemas de Gestión de la Seguridad de la Información**.

Profundizando en esta definición, se puede decir que la confianza digital es algo más que **implementar medidas de seguridad o controles para garantizar la confidencialidad de la información sensible**. Por supuesto, esto es necesario, pero también se requiere que las personas lo sepan y lo crean.

Qué es la confianza digital

Blindar la información y los datos de los usuarios de un sitio o de una aplicación es la mitad del trabajo en el proceso de construir confianza digital.

La otra mitad es hacer que **las personas perciban con claridad el compromiso de la organización que administra o posee el sitio**.

Para cumplir con el segundo propósito, la organización puede expresar ese compromiso. Si esa publicación está acompañada de una **experiencia de uso que se muestra segura y transparente**, es posible que los usuarios crean que el sitio es confiable. Existirá entonces la confianza digital.

Sin embargo, puede ser necesario afianzar la confianza digital demostrando que la seguridad de la información es una prioridad y que se trabaja para **mejorar la eficacia de los controles y de la gestión**. Es ahí donde cobra relevancia ISO/IEC 27001.

Qué es ISO/IEC 27001

La **norma ISO 27001 es el estándar internacional para gestionar riesgos de seguridad de la información**, en todos sus formatos o medios y en todo tipo de organizaciones.

Entrega requisitos para planificar, implementar, auditar, certificar, mejorar y mantener un sistema de gestión que garantice la privacidad, confidencialidad e integridad de la información de la organización y de los datos de terceros.

ISO 27001 **solicita a la organización que identifique, evalúe y gestione de manera proactiva las amenazas** de seguridad de la información y que implemente los controles adecuados para protegerla.

Cuál es la relación entre ISO 9001 e ISO 19011

Las **normas ISO 9001** e **ISO 19011** están enfocadas en mejorar la calidad de sus procesos y productos. Si bien ambas normas tienen objetivos distintos, se complementan en la **gestión de calidad** y en la realización de **auditorías internas**. Tratar este tema en profundidad nos ocupará durante las siguientes líneas. Abordaremos cuál es la relación entre ISO 9001 e ISO 19011, cómo se apoyan mutuamente para fomentar una **mejora continua** y qué ventajas puede tener para el sector empresarial implementar un Sistema de Gestión de Calidad.

ISO 9001 e ISO 19011

ISO 9001 es la norma internacional que establece los requisitos para implementar un **Sistema de Gestión de la Calidad (SGC)**. Se aplica a organizaciones de cualquier sector o tamaño, y su propósito es optimizar la eficiencia de los procesos, mejorar la calidad de los productos y servicios y, en última instancia, aumentar la satisfacción del cliente.

Algunos de los elementos clave de ISO 9001 incluyen:

- **Enfoque en el cliente**: ISO 9001 busca asegurar que la organización comprenda las necesidades y expectativas de sus clientes y trabaje para satisfacerlas de manera consistente.

- **Liderazgo**: La alta dirección juega un papel esencial en la implementación del SGC, alineando los objetivos de calidad con la estrategia organizacional.

- **Enfoque basado en procesos**: ISO 9001 fomenta una visión sistémica en la que todos los procesos están interconectados, lo cual permite una gestión integral de la calidad.

- **Mejora continua**: La norma promueve la cultura de mejora, alentando a las empresas a buscar continuamente oportunidades de perfeccionamiento en sus operaciones.

¿Qué es ISO 19011 y cómo complementa a ISO 9001?

ISO 19011 es una **guía para la auditoría de sistemas de gestión**. A diferencia de ISO 9001, que establece requisitos específicos, ISO 19011 ofrece directrices sobre cómo llevar a cabo auditorías internas y externas de SGC. Además, también se ocupa de otros sistemas de gestión, como el ambiental (ISO 14001) o el de seguridad y salud ocupacional (ISO 45001). Los puntos destacados de ISO 19011 incluyen:

- **Principios de auditoría**: La norma detalla principios fundamentales como la integridad, la imparcialidad y la competencia, que son esenciales para asegurar auditorías efectivas y objetivas.

Ley de Inteligencia artificial de la UE: qué es y qué implicaciones tiene

La **Ley de Inteligencia artificial de la UE** es la primera en el mundo en responder a las expectativas y llamadas de atención de la sociedad, de los estados y de las organizaciones para que se regule el uso de un avance tecnológico que ha generado polémicas y discusiones.

Esas inquietudes son razonables por la forma acelerada en que la IA ha irrumpido en el trabajo, la vida familiar, la sociedad y el modo en que interactúan las personas. Se ha generado un ambiente de incertidumbre en el que **se discuten temas como privacidad de los datos, protección de los derechos de las personas o transgresión de la propiedad intelectual**, sin mencionar las consideraciones éticas.

Ante tal escenario, la Ley de Inteligencia artificial de la UE no solo resulta oportuna, sino que se recibe como un elemento que permitirá calmar las aguas y **facilitar la integración de la nueva tecnología** en un momento histórico en el que puede resolver

muchos problemas, antes que generar nuevos. Cualquier esfuerzo legislativo o normativo, así como la publicación de estándares de gestión como **ISO 42001**, contribuyen a ese propósito. Así, resulta procedente **conocer algunas particularidades sobre la Ley de Inteligencia artificial de la UE** y sus implicaciones.

Qué es la Ley de Inteligencia artificial de la UE

La Ley de Inteligencia artificial de la UE es pionera en su género en el mundo. La nueva legislación **busca crear un marco jurídico para tratar problemas como la ética en el uso de la tecnología**, el respeto de los derechos de las personas, la igualdad, la inclusión o la privacidad de los datos y de la **seguridad de la información**, entre otros.

La historia de la Ley de Inteligencia artificial de la UE se inicia en abril de 2021, momento en el que es propuesta por la Comisión Europea por primera vez. Pasarían, sin embargo, un poco más de dos años para que se aprobara, en mayo de 2024. **Su entrada en vigor en el territorio europeo tuvo lugar el 1 de agosto de 2024.**

Se prevé que **las normas regulatorias en cada estado entrarán en vigor en agosto de 2026**. Dada la urgencia que plantean ciertos temas, algunas disposiciones se adelantarán: las de sistemas de IA que suponen riesgo inaceptable lo harán a principios de 2025 y normas sobre desarrollos de IA de propósito general, en agosto de ese mismo año.

Sin embargo, y pese a existir un cronograma de entrada en vigor, la Comisión considera que los desarrolladores de sistemas de IA **pueden iniciar un plan de cumplimiento voluntario desde ahora**.

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO

Alcance de la norma ISO 19011

Norma ISO 19011

La norma ISO 19011 es una guía para hacer auditorías de sistemas de gestión, a través de un marco claro y conciso para planificar y ejecutar auditorías en empresas de cualquier sector o tamaño. En este artículo, vamos a explorar el alcance de la norma y cómo puede ayudar a mejorar la eficacia y la confiabilidad de los procesos de auditoría dentro de tu organización.

¿Qué es la norma ISO 19011?

La **ISO 19011** es una norma que establece los requisitos para hacer auditorías a sistemas de gestión, incluyendo las relacionadas con la **calidad**, el medio ambiente o la seguridad y salud ocupacional, entre otros.

Su principal objetivo es proporcionar las directrices para hacer una auditoría de sistemas de gestión y evaluar la competencia de los auditores.

Alcance de la norma

El alcance de la norma ISO 19011 abarca una gran variedad de aspectos en el proceso de auditoría, como:

- **Principios de Auditoría**: la norma establece los principios que guían el proceso de auditoría, garantizando que las auditorías sean objetivas, imparciales y basadas en evidencias.

- **Gestión del Programa de Auditoría**: ISO 19011 ofrece las directrices para planificar, establecer y gestionar un programa de auditoría, asegurando que las auditorías son sistemáticas, efectivas y eficientes.

- **Competencia de los Auditores**: la norma establece los requisitos y criterios para seleccionar y evaluar a los auditores competentes, garantizando que aquellos que hagan la auditoría tengan el conocimiento, las habilidades y la experiencia necesarias.

- **Proceso de Auditoría**: la norma ISO 19011 describe las fases del proceso de auditoría, desde la planificación inicial hasta la presentación de los resultados, para asegurar que el proceso se ejecute de forma coherente y profesional.

- **Auditoría de Sistemas de Gestión**: el alcance de ISO 19011 abarca las auditorías de diversos sistemas de gestión, incluidos los de calidad **(ISO 9001)**, medio ambiente (ISO 14001) y SST (ISO 45001), entre otros.

- **Evaluación de Riesgos y Oportunidades**: la norma sugiere cómo llevar a cabo la integración de la evaluación de riesgos y oportunidades en el proceso de auditoría para asegurar la mejora continua y la efectividad del sistema de gestión.

¿Cuáles son los criterios de auditoría según ISO 19011?

La **ISO 19011** es una norma internacional fundamental que establece **directrices para la auditoría de sistemas de gestión**. Esta norma proporciona un enfoque coherente para llevar a cabo **auditorías de calidad, medio ambiente, seguridad, entre otros** sistemas de gestión. En este artículo, exploraremos en detalle cuáles son **los criterios de auditoría según la ISO 19011**, así como su **importancia** y **aplicación** en diferentes organizaciones.

ISO 19011

La **ISO 19011**:2018 es una norma internacional que ofrece **pautas sobre la auditoría** de los sistemas de gestión, tanto internos como externos. Esta norma establece principios para la **planificación**, la **ejecución** y la **evaluación de auditorías**, además de orientar sobre cómo **gestionar a los auditores y equipos de auditoría**. Está dirigida a organizaciones de cualquier tamaño que busquen realizar auditorías internas o de terceros.

La ISO 19011 no solo se enfoca en la **auditoría de sistemas de gestión de calidad**, sino que también **cubre otros sistemas**, como el medio ambiente (ISO 14001) y la seguridad y salud en el trabajo (ISO 45001), entre otros.

Principales criterios de auditoría

La norma establece varios criterios fundamentales que los auditores deben seguir para **garantizar la efectividad de las auditorías**. A continuación, se describen los más relevantes:

1. Imparcialidad

La imparcialidad es uno de los principios más importantes de la ISO 19011. Un auditor debe **realizar su trabajo de manera objetiva**, sin sesgos que puedan influir en los resultados de la auditoría. Esto significa que el auditor debe ser **independiente del área o proceso que esté auditando**. De esta manera, se **asegura la credibilidad** del proceso de auditoría y la **confianza** en sus resultados.

Aplicación de la imparcialidad:

- Selección de auditores con la suficiente competencia.
- Evitar conflictos de interés que puedan comprometer la objetividad.
- Evaluación transparente de los sistemas de gestión auditados.

10 ventajas de certificarse en ISO 50001

La **sostenibilidad** y la **eficiencia energética** son conceptos que resuenan en nuestro día a día por lo relevante que es su gestión. La norma **ISO 50001** nos sirve de herramienta clave para las organizaciones que buscan optimizar su consumo de energía y reducir su impacto ambiental. Este estándar internacional para la gestión de la energía se encarga de aportar beneficios ambientales, a la vez que económicos y operativos, especialmente cuando se implementa con un software especializado.

ISO 50001

En este artículo, exploraremos las **10 ventajas principales de certificarse en ISO 50001** y cómo las empresas pueden maximizar su potencial al integrar un software de gestión energética.

1. Ahorro significativo en costos energéticos

La principal ventaja de implementar un Sistema de Gestión de la Energía (SGE) basado en ISO 50001 es la reducción de costos

energéticos. Este estándar ayuda a las organizaciones a identificar áreas de mejora en el uso de la energía, **optimizando recursos** y eliminando desperdicios. Un **software especializado** permite monitorear en tiempo real el consumo energético, detectando ineficiencias antes de que se conviertan en gastos innecesarios.

2. Mejora continua en el desempeño energético

La norma promueve un enfoque sistemático para alcanzar mejoras continuas en el rendimiento energético. Esto se traduce en operaciones más eficientes y sostenibles a largo plazo. Con las herramientas adecuadas, las organizaciones pueden **automatizar el seguimiento y análisis de datos**, asegurando que las **acciones correctivas** sean **oportunas** y **efectivas**.

3. Cumplimiento normativo y reducción de riesgos legales

En muchos países, las regulaciones sobre eficiencia energética y reducción de emisiones son cada vez más estrictas. **ISO 50001 asegura el cumplimiento normativo**, reduciendo riesgos legales y financieros. Las empresas pueden centralizar toda la documentación relacionada con el cumplimiento, asegurando auditorías más ágiles y sin contratiempos.

4. Disminución de la huella de carbono

Certificarse en ISO 50001 permite a las empresas reducir significativamente sus **emisiones de gases de efecto invernadero** (GEI), contribuyendo a la lucha contra el **cambio climático**. Un software especializado facilita la recopilación de datos y la generación de informes, lo que permite calcular con precisión la huella de carbono y comunicar estos logros a los **stakeholders**.

Principios y estructura de ISO 42001: la norma para sistemas de gestión de IA

La **estructura de ISO 42001** es la acostumbrada por ISO para sus estándares certificables, y con posibilidad de integración, publicados en la última década. Esta estructura, así como los principios que acompañan la norma, permiten crear un marco de operación de **Sistemas de Inteligencia Artificial** seguro, responsable, ético y legal.

La Inteligencia Artificial es **el desarrollo tecnológico más importante en la historia de la humanidad, pero también despierta recelos y temores**. La capacidad para aprender, razonar y comprender el lenguaje que utilizan las personas no es un tema que se pueda pasar por alto.

Por supuesto, las oportunidades son muchas, pero también lo son los riesgos.

ISO 42001, un estándar pionero

La estructura de ISO 42001 y sus principios **responden a los temores que despierta la Inteligencia Artificial, pero también a las expectativas que existen sobre un potencial aún no calculado**. Es lo que tuvieron en mente los expertos de ISO y de la Comisión Electrotécnica Internacional al diseñar la estructura de ISO 42001, el **primer estándar en Gestión de Sistemas de IA**.

ISO ya había incursionado en el área con normas como ISO 22989 (Terminología de IA), ISO 2023 (Marco de IA y ML) o ISO 23984 (riesgos relacionados con IA). Pero la estructura de ISO 42001, gracias a sus anexos, conforma la primera norma de Gestión para Sistemas de IA que **puede ser utilizada por todo tipo de organizaciones**, tanto si son desarrolladoras como usuarias de esta tecnología.

La estructura de ISO 42001, de Alto Nivel, **incorpora requisitos para que la organización redacte y publique políticas y elabore manuales de procedimientos**. También da pautas para diseñar procesos y adoptar las mejores prácticas de gobernanza para el desarrollo o uso de Sistemas de Inteligencia Artificial basados en el ciclo PDCA, que garantiza la mejora continua.

Cuáles son los principios y la estructura de ISO 42001

Generar Sistemas de Inteligencia Artificial confiables, seguros y transparentes es uno de los principios de la norma. La estructura de ISO 42001 se ha diseñado para producir un sistema de gestión que cumpla con este propósito.

¿Qué es la norma ISO 37008 para la gestión de investigaciones internas?

ISO 37008

La gestión de investigaciones internas en las empresas es clave para proteger la integridad empresarial, prevenir los riesgos y fortalecer la confianza en los sistemas de cumplimiento. En este contexto es donde surge la **norma ISO 37008**, una guía que estructura, ejecuta y supervisa las investigaciones internas de manera ética, eficiente y alineada con las buenas prácticas internacionales.

Un marco para la investigación interna

ISO 37008 establece un marco sistemático que permite a las organizaciones gestionar investigaciones internas con estándares uniformes. Desde la recepción de denuncias hasta la resolución final, esta **norma ISO** asegura que el proceso sea transparente, objetivo y proporcional, lo que garantiza resultados fiables y válidos.

Al **implementar ISO 37008**, las empresas obtienen herramientas para:

- **Identificar y abordar incidentes** de forma rápida y adecuada.
- Garantizar la **confidencialidad y protección** de las partes involucradas.
- Respetar los **principios legales y éticos** aplicables a cada jurisdicción.

Principios clave de la ISO 37008

La norma ISO 37008 se basa en una serie de principios que orientan la investigación hacia **la excelencia y el cumplimiento**:

- **Imparcialidad:** evitar el **conflicto de interés** y asegurar un enfoque objetivo.
- **Confidencialidad:** proteger la información y las identidades de los involucrados.
- **Eficiencia:** usar recursos de forma estratégica para reducir las interrupciones operativas.
- **Integridad:** garantizar que las decisiones se basen en hechos comprobados y análisis objetivos.

Beneficios de ISO/TS 37008

En el mundo empresarial actual, donde la **integridad** y la **transparencia** son esenciales para **construir confianza**, las organizaciones enfrentan el desafío de gestionar **relaciones con terceros de manera ética y eficiente**. La norma **ISO/TS 37008**, una extensión del marco de la **ISO 37001**, surge como una herramienta esencial para **establecer, implementar y mantener un sistema de gestión de la gobernanza de terceros** que fomente prácticas responsables y prevenga riesgos relacionados con el soborno y otras irregularidades.

Este artículo explora en detalle los beneficios de la **ISO/TS 37008**, su importancia para las organizaciones y cómo implementarla con éxito.

ISO/TS 37008

La **ISO/TS 37008** es una **especificación técnica** diseñada para ayudar a las organizaciones a establecer procedimientos eficaces para la **gobernanza de terceros**, garantizando que las **relaciones** comerciales con proveedores, socios y otras entidades externas se gestionen de manera **ética y conforme a las normativas vigentes**.

Esta norma complementa a la **ISO 37001** (Sistema de Gestión Antisoborno) al centrarse específicamente en los **riesgos asociados a terceros**, como el incumplimiento normativo, el fraude o la corrupción, que pueden poner en **peligro la reputación y sostenibilidad** de una organización.

Beneficios clave de implementar ISO/TS 37008

Adoptar la **ISO/TS 37008** ofrece múltiples **ventajas a las empresas**, tanto en términos de cumplimiento normativo como en la **mejora de las relaciones comerciales**.

Mitigación de riesgos asociados a terceros

La relación con terceros puede implicar **riesgos significativos**, como:

- **Fraude financiero.**
- **Incumplimiento normativo.**
- Daño a la **reputación** organizacional.

La implementación de **ISO/TS 37008** permite **identificar y gestionar estos riesgos** mediante la evaluación sistemática de terceros, asegurando que **cumplan con los estándares éticos y legales** establecidos.

Mejora de la transparencia

La norma fomenta una **mayor transparencia** en las interacciones con terceros, estableciendo **controles claros y procedimientos documentados**.

Nueva ISO 53002 sobre la directrices para contribuir a los ODS

La **ISO 53002:2024** es una herramienta clave para alinear las estrategias empresariales con los **Objetivos de Desarrollo Sostenible (ODS)**. Esta nueva norma fomenta la responsabilidad corporativa, estableciendo una guía para las organizaciones hacia un impacto positivo en el entorno social, ambiental y económico.

A continuación, exploraremos los fundamentos de esta norma, su relevancia para el sector empresarial y cómo la implementación a través de plataformas tecnológicas como **ISOTools** puede maximizar sus beneficios.

ISO 53002

La ISO 53002:2024 establece una serie de pautas para integrar los ODS en las operaciones organizacionales.

Por tanto, esta norma, desarrollada en colaboración con el PNUD (Programa de las Naciones Unidas para el Desarrollo), se centra en incorporar principios de sostenibilidad a través de:

- **Estrategias empresariales alineadas con los ODS**, como igualdad de género (ODS 5) o acción climática (ODS 13).
- **Gestión eficiente de recursos y reducción de impactos negativos** en la cadena de valor.
- **Transparencia y rendición de cuentas**, mediante informes verificables y de alta calidad.
- **Mejora continua**, utilizando el ciclo PDCA (Planificar-Hacer-Verificar-Actuar) para revisar y ajustar las estrategias de manera dinámica.

Impacto en el sector empresarial de la ISO 53002

La adopción de la **ISO 53002** proporciona una amplia gama de beneficios estratégicos y operativos para las empresas que desean avanzar hacia modelos de negocio más sostenibles y alineados con los Objetivos de Desarrollo Sostenible (ODS). En primer lugar, ofrece una **ventaja competitiva significativa**, ya que al incorporar los ODS en sus estrategias corporativas, las organizaciones obviamente mejoran su desempeño interno, buscando así fortalecer su posicionamiento frente a consumidores y grupos de interés más conscientes de la sostenibilidad. Este enfoque puede traducirse en una mayor **fidelidad del cliente** y **atracción de inversores** interesados en apoyar empresas responsables.

Gobernanza de la IA: concepto, tipos y marcos normativos

Gobernanza de la IA es un concepto cada día más común en el mundo corporativo. La razón se encuentra en lo novedosa que aún resulta esta tecnología, pero también en los riesgos, algunos de ellos ya identificados, que lleva aparejado el uso del avance tecnológico más popular del siglo XXI.

Es innegable el uso generalizado de Inteligencia Artificial en las organizaciones, también en la vida social y en el entretenimiento. Basta mencionar estos tres espacios para explicar las crecientes preocupaciones de especialistas, pero también de gobiernos y de la sociedad en general.

Esa preocupación es, precisamente, la que da origen al concepto de gobernanza de la IA. La expresión refleja ese **deseo de hacer uso de la Inteligencia Artificial, pero dentro de un marco** en el que la organización usuaria ejerza algún tipo de administración o autoridad.

A continuación, se analiza **qué significa con precisión gobernanza de la IA, cuántos niveles hay**, qué marcos normativos ayudan a ejercer autoridad sobre ella y qué buenas prácticas contribuirán a un uso responsable y seguro de la IA.

Qué es la Gobernanza de la IA

Gobernanza de la IA hace referencia a un conjunto de normas, políticas, prácticas y directrices, que establecen un marco de gestión para utilizar la tecnología y **aprovechar sus beneficios comerciales, preservando el respeto a la transparencia, a la igualdad** y a los derechos de las personas, entre ellos, los de autor.

La gobernanza de la IA **permite controlar riesgos** y definir un uso de la tecnología que responda a las **consideraciones éticas**, que respete la integridad y fomente confianza entre los usuarios, los consumidores, los empleados y cualquier otra parte interesada.

De esta manera, la gobernanza de la IA es, en una definición muy sucinta, **la autoridad que puede ejercer una organización para aprovechar, de forma controlada, los beneficios que puede entregar la tecnología.**

Cuántos niveles de gobernanza de la IA existen

La gobernanza de la IA en las empresas **se clasifica en tres niveles, de acuerdo con el rigor con el que se pone en práctica** y con la sofisticación que la acompaña. Ante un **panorama regulatorio de la inteligencia artificial** aún en desarrollo, las empresas toman decisiones que les permiten asumir un nivel de gobernanza que facilite controlar riesgos, pero sin limitar los beneficios.

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO

Guía para entender ISO/ UNDP PAS 53002:2024

ISO/UNDP PAS 53002:2024

La ISO/UNDP PAS 53002:2024 surge como una colaboración entre la Organización Internacional de Normalización (ISO) y el Programa de las Naciones Unidas para el Desarrollo (PNUD). Esta norma es una herramienta estratégica para que las organizaciones alineen sus operaciones con los **Objetivos de Desarrollo Sostenible (ODS)** de la ONU, promoviendo prácticas responsables en los ámbitos económico, social y ambiental.

Propósito y Enfoque

La norma busca facilitar la integración de los ODS en las estrategias empresariales, asegurando una contribución medible y efectiva al **desarrollo sostenible**. Esto incluye:

- **Planificación y Desarrollo de Iniciativas:** orienta a las empresas para el establecimiento de objetivos claros en relación con los ODS.

- **Implementación Sostenible**: proporciona directrices para incorporar la sostenibilidad en todas las operaciones diarias de la compañía.

- **Evaluación de Impacto**: establece métodos para monitorear y reportar el progreso hacia los objetivos globales de la organización.

Estructura de la Norma

La ISO/UNDP PAS 53002:2024 se organiza en módulos clave que cubren:

- **Marco Estratégico**: directrices para integrar la sostenibilidad en la visión y misión empresarial.

- **Implementación Operativa**: procedimientos para alinear prácticas de la organización con los Objetivos de Desarrollo Sostenible.

- **Indicadores de Desempeño**: empleo de métricas para la evaluación y **mejora continua.**

- **Transparencia y Reporte**: métodos para comunicar el impacto de las acciones sostenibles.

Beneficios Clave de la ISO/UNDP PAS 53002:2024

Implementar esta norma trae **múltiples ventajas**:

- **Refuerza el compromiso** de la empresa con la sostenibilidad.

3 Indicadores para la norma ISO 9001 que son esenciales en gestión de la calidad

Los **indicadores para la norma ISO 9001** son señales confiables que permiten suponer, antes de una auditoría interna que lo compruebe, que el **Sistema de Gestión de la Calidad** funciona, está conforme con los requisitos del estándar y alcanza los objetivos propuestos.

Los indicadores para la norma ISO 9001 **son herramientas que se emplean para monitorear el funcionamiento del Sistema de Gestión de la Calidad**. También son útiles para identificar problemas y oportunidades de mejora.

Existen muchos indicadores o métricas para evaluar un sistema de gestión. Incluso **si se limita la búsqueda a indicadores para la norma ISO 900, el número es abundante**. A continuación se profundiza en tres, en los que prestan un mejor servicio a profesionales que necesiten obtener información inmediata sobre la eficiencia del sistema que conducen.

Cuáles son los indicadores para la norma ISO 9001 más eficaces

En el **capítulo 9 de la ISO 9001** se **solicita que la organización implemente mecanismos o metodologías para evaluar el desempeño del sistema**. Inspecciones, auditorías y revisiones forman parte de las técnicas o métodos que puede utilizar la empresa para cumplir con el requisito. Pero también lo hacen los indicadores para la norma ISO 9001.

Por supuesto, **los indicadores no reemplazan las otras actividades de evaluación**. Pero sí son importantes, particularmente en momentos intermedios entre una y otra **auditoría interna del SGC** o ante una auditoría de recertificación.

La gran ventaja de los indicadores para la norma ISO 9001 es su **capacidad para proveer información inmediata**. Pero, como ya se advirtió, existe un número extenso de estas métricas. Tres de ellas, no obstante, destacan por centrarse en la eficacia del sistema

1. La satisfacción del cliente

El primero de los indicadores para la norma ISO 9001 es el más obvio. La satisfacción del cliente expresa en cuatro palabras el sentido y el objetivo de un sistema de gestión, ya que es la más relevante entre las **partes interesadas en ISO 9001**.

Es un indicador importante por otra razón: el mencionado capítulo 9, **incorpora una cláusula (9.1.2) que solicita medir y monitorear la satisfacción del cliente**.

¿Qué es la norma ISO 17025 y para qué sirve?

La **norma ISO 17025** es una de las más **importantes** en el ámbito de los **laboratorios de ensayo y calibración**. Proporciona un marco para garantizar que los laboratorios **operen** con **competencia técnica y generen resultados confiables**. En este artículo, exploraremos en detalle qué es la norma ISO 17025, sus principales beneficios y cómo las organizaciones pueden implementarla para garantizar la **calidad y la precisión** en sus operaciones.

ISO 17025

La **ISO 17025** es una norma internacional desarrollada por la Organización Internacional de Normalización (**ISO**) y el Comité Electrotécnico Internacional (**IEC**). Está diseñada para **garantizar que los laboratorios de ensayo y calibración** operen bajo un **sistema de gestión de calidad** que cumpla con **requisitos técnicos y organizativos** específicos.

Esta norma es aplicable a cualquier laboratorio, independientemente de su tamaño o sector, y se centra en dos aspectos principales:

- **Requisitos de gestión:** Alineados con los principios de la gestión de calidad, similares a los de la **ISO 9001**.

- **Requisitos técnicos:** Relacionados con la competencia del personal, los métodos de ensayo y calibración, los equipos y la validez de los resultados.

¿Para qué sirve la norma?

La **ISO 17025** sirve como **referencia para garantizar** que los laboratorios no solo **cumplen con los estándares de calidad**, sino que también generan **resultados técnicamente confiables**. Esta norma es especialmente importante para:

- Asegurar la **aceptación internacional** de los resultados de ensayo y calibración.

- Mejorar la **credibilidad** y la **confianza** de los clientes y las partes interesadas.

- Facilitar la **acreditación de laboratorios**, un requisito clave en sectores como la salud, la manufactura, la investigación y la ingeniería.

Beneficios de implementar la norma ISO 17025

Reconocimiento internacional

Los laboratorios acreditados según la **ISO 17025** son **reconocidos** globalmente por su capacidad para generar resultados confiables.

¿Qué es la ISO 27017 de controles de seguridad para servicios cloud?

El rápido avance de la tecnología ha convertido a la nube en el gran aliado de las empresas modernas. Pero, como todo gran poder, conlleva una gran responsabilidad: garantizar la seguridad de los datos que circulan y se almacenan en este entorno. En este sentido, la **ISO/IEC 27017** ofrece un conjunto de controles diseñados específicamente para blindar la información en los servicios cloud.

Más que un simple estándar, la ISO 27017 redefine las reglas del juego al proporcionar un marco de seguridad que beneficia tanto a los usuarios como a los proveedores de la nube. Durante las siguientes líneas, descubriremos cómo esta norma responde a los desafíos del entorno digital y cómo un **Software ISO 27001 – Seguridad de la Información** puede transformar la gestión de riesgos y la protección de datos en tu organización.

ISO 27017: Más allá de la seguridad tradicional

La ISO/IEC 27017 fue desarrollada como una extensión de la **ISO/IEC 27002** para proporcionar controles específicos que abordan los riesgos inherentes al uso de servicios en la nube. Si bien la **ISO/IEC 27001** establece un marco general para la gestión de la **seguridad de la información**, la **ISO 27017** adapta este enfoque para cubrir aspectos exclusivos del **entorno cloud**, como la virtualización, las responsabilidades compartidas y la privacidad de los datos.

Principales características de la ISO 27017:

Controles específicos para servicios cloud:
La norma introduce 7 controles adicionales diseñados para proteger la información en entornos de computación en la nube. Entre ellos, se encuentran:

- Gestión de responsabilidades compartidas entre proveedor y cliente.
- Configuración segura de entornos virtuales.
- Supervisión y registro de actividades en la nube.

Definición clara de roles y responsabilidades:
Uno de los principales retos del uso de servicios en la nube es la confusión sobre quién es responsable de qué. La ISO 27017 establece directrices claras para dividir las responsabilidades entre el **cliente** y el **proveedor**.

ESGinnova
Group

HSE Tools

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

Software de gestión HSE: 10 beneficios esenciales para las organizaciones modernas

Un **software de gestión HSE** es una inversión, no un coste. Ese es el principio básico que es preciso asimilar para obtener sus beneficios. La **gestión HSE** automatizada ayuda a controlar riesgos y a ganar en rapidez, en seguridad y en productividad.

Las ventajas de un software de gestión HSE, por otra parte, son palpables para muchas de las que se reconocen como partes interesadas. Por supuesto, **entre esas partes interesadas adquiere un papel predominante la Alta Dirección.** El argumento que convencerá a la junta directiva es, sin duda, el retorno de la inversión que proporcionan estas herramientas tecnológicas. El software de gestión HSE **entrega beneficios que pueden ser evaluados desde el punto de vista cualitativo y cuantitativo**. Damos un repaso a diez de los más destacados.

Beneficios que aporta un software de gestión HSE

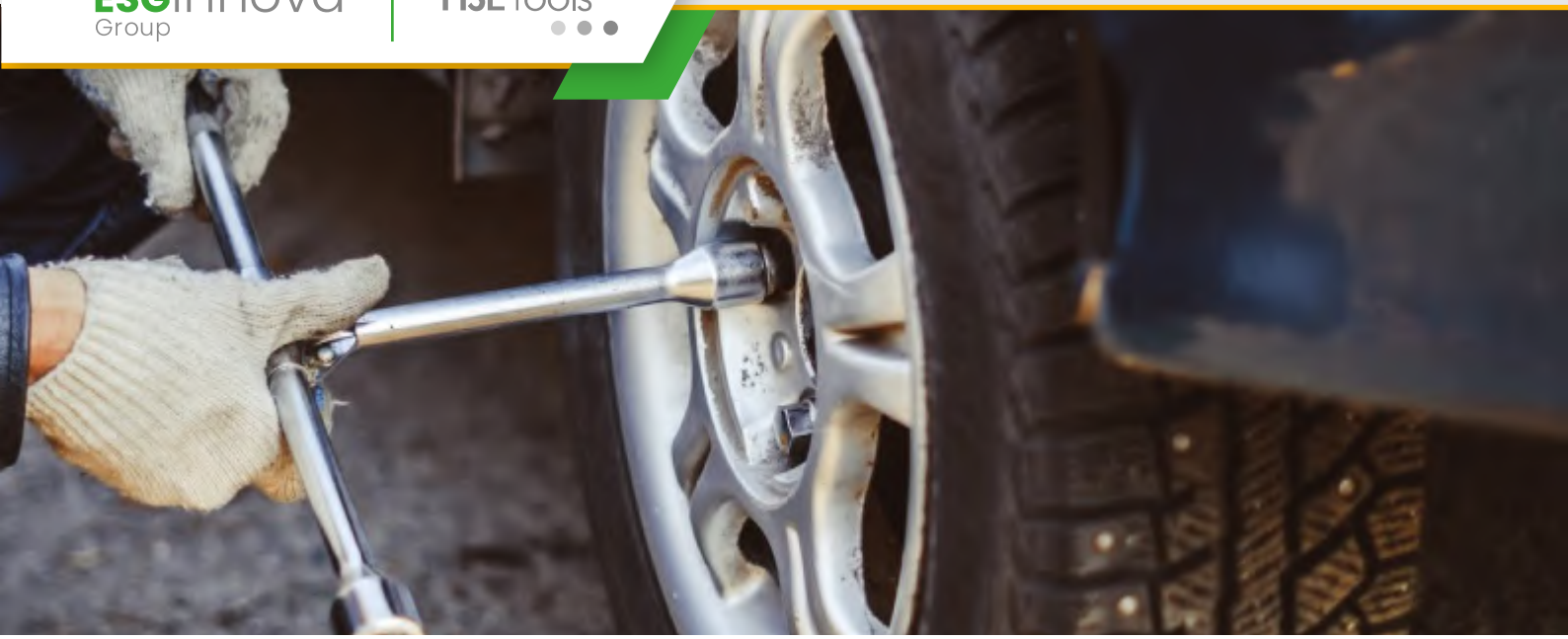
Un software de gestión HSE es una solución informática que **automatiza muchas de las tareas necesarias** para alcanzar objetivos en el área de gestión ambiental y de **seguridad y salud en el trabajo**. Pero el software puede hacer mucho más que eso: **crear flujos de trabajo, emitir alertas, avisar sobre incumplimientos**, generar canales de comunicación fluidos entre trabajadores y organización, admitir diversos formatos de información para facilitar los reportes, etc. Al realizar estas acciones el software de gestión HSE entrega interesantes beneficios:

1. Minimiza las pérdidas por eventos disruptivos

Los profesionales en gestión HSE trabajan para prevenir riesgos. Los eventos disruptivos, no obstante, son imprevisibles y sus efectos tienen un alto impacto lesivo sobre las organizaciones. El software de gestión HSE contribuye a minimizar ese impacto y reducir el coste del evento, ya que logra **generar escenarios posibles y con base en ellos proponer estrategias de acción inmediata** anteriores a la ocurrencia del suceso.

2. Evita sanciones y multas

El cumplimiento es uno de los aspectos que mayor preocupación genera en los profesionales que se ocupan de la gestión HSE. Es así porque el coste de multas, sanciones o incluso pérdidas de licencias o cierres temporales o definitivos de operaciones **pueden resultar demoledores para la organización**. Con un panorama siempre cambiante, es importante contar con una herramienta que permita vigilar, monitorear y garantizar el cumplimiento. Es una de las labores del software de gestión HSE.



Cómo garantizar la seguridad vial en la empresa

¿Cómo es de importante la **seguridad vial en el ámbito empresarial**? Las empresas deben plantearse esta como una parte importante de sus **Programas HSE**. La necesidad de movilidad y tránsito en las zonas urbanas está en constante crecimiento, si a esto le sumamos la necesidad que tienen algunas organizaciones de realizar su actividad mediante desplazamientos, es necesario tomar medidas proactivas para asegurar que los trabajadores estén protegidos.

Seguridad vial en la empresa

Los **accidentes de tránsito** son una de las principales causas de incidentes laborales en el mundo y pueden afectar significativamente la productividad de una empresa, los costos operativos y, sobre todo, la vida y bienestar de los empleados. La seguridad vial no solo es relevante para las organizaciones que dependen directamente de vehículos o traslados (como el sector logístico o de transporte), sino también para aquellas que tienen empleados desplazándose con frecuencia entre ubicaciones, como consultorías o ventas

externas. **Garantizar la seguridad vial** significa proteger a los empleados, reducir riesgos operativos y proyectar una imagen responsable ante la sociedad.

¿Cómo puede una empresa mejorar su seguridad vial?

La **implementación de una política de seguridad vial** efectiva en la empresa requiere un enfoque integral que combine prácticas de conducción segura, tecnología de monitoreo, capacitación y un sistema robusto para la gestión de riesgos.

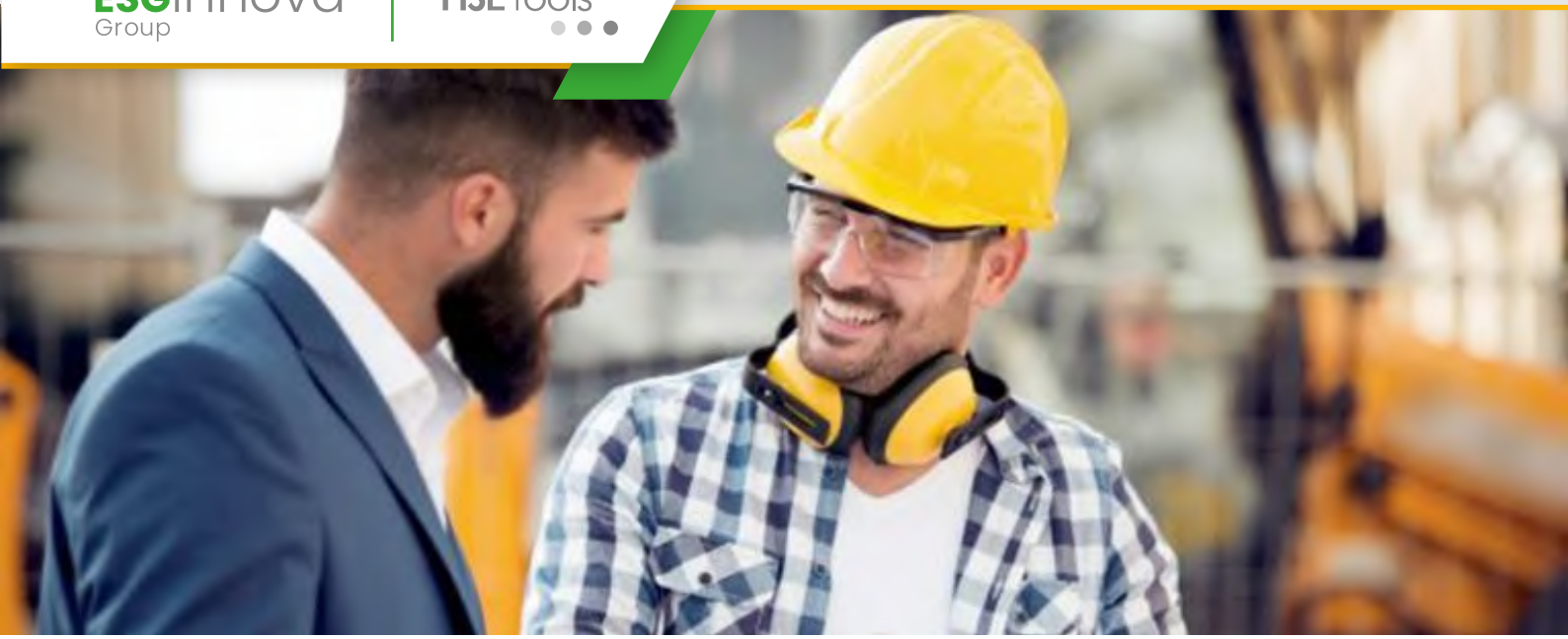
A continuación, se presentan los pilares fundamentales para una política de seguridad vial empresarial:

1. Establecimiento de una política de seguridad

Crear y comunicar una **política clara y detallada** sobre las expectativas y responsabilidades en cuanto a la seguridad vial es un primer paso crucial. Además, esta política debe incluir desde normativas específicas de conducta al volante hasta sanciones y consecuencias en caso de incumplimiento.

2. Capacitación y concienciación continua

La **formación en seguridad vial** no debe ser una actividad puntual. Invertir en campañas y programas educativos regulares ayuda a que los empleados estén informados sobre los riesgos, conozcan técnicas de conducción segura y asuman una mayor responsabilidad en sus desplazamientos diarios.



Buenas prácticas para gestionar contratistas en el lugar de trabajo

Adoptar **buenas prácticas para gestionar contratistas** ayuda a las empresas a gestionar riesgos, alcanzar objetivos, mantener una relación transparente y colaborativa con la fuerza laboral externa y garantiza, además, el cumplimiento normativo y regulatorio.

La eficacia aumenta y la organización adquiere reconocimiento como buen empleador. Por supuesto, gracias a la implementación de buenas prácticas para gestionar contratistas, la empresa puede seleccionar las mejores opciones en las mejores condiciones.

Buenas prácticas para gestionar contratistas que se pueden implementar en una organización

Las buenas prácticas para gestionar contratistas equivalen a **hacer bien las cosas, hacerlas cuando es oportuno y hacerlas pensando en los intereses de todos los involucrados.** Todo ello empezando, por supuesto, por esos terceros. Los beneficios serán

para todos: organización, contratistas, reguladores, los empleados de la empresa, etc. Las buenas prácticas para gestionar contratistas, para finalizar antes de entrar a describirlas, **son estrategias que tienen objetivos claros: seguridad, transparencia y cumplimiento**.

1. Debida diligencia

Aplicar debida diligencia a los contratistas **busca establecer el nivel de confiabilidad del proveedor del servicio**, la capacidad técnica y operativa para ejecutar el proyecto y la inexistencia de conflictos de intereses. También tiene por objetivo el cumplimiento de las normas de seguridad laboral e **identificar y gestionar riesgos** que puedan comprometer a terceros, a otros empleados de la empresa o a la misma organización. La debida diligencia **permite generar una base de datos de contratistas verificados** que elimina el laborioso trabajo de investigación en el futuro. Los contratistas seleccionados desde listas comprobadas respetan las reglas de seguridad, son confiables, saben hacer su trabajo y construyen una relación cada vez más sólida con la empresa.

Cómo aplicar la debida diligencia a los contratistas

La debida diligencia sobre contratistas es una tarea que requiere de un esfuerzo, pero los resultados lo justifican. Sin embargo, todo puede ser más sencillo si se cuenta con el apoyo de un **software HSE** que automatice las tareas repetitivas, que representan la mayor parte de la debida diligencia. Algunos **aspectos interesantes que se deben analizar** son los siguientes:

Información sobre la historia laboral del contratista, los resultados de los proyectos que ha desempeñado y la forma en que concluye sus contratos.

Plataforma HSE: 5 formas innovadoras en las que las empresas utilizan el software

Una **plataforma HSE** puede crear un entorno amigable para que un trabajador tome la iniciativa de informar de la presencia de condiciones cuya articulación genera un riesgo inminente para la seguridad de los trabajadores.

Al hacerlo, ese trabajador desencadena un proceso sistemático de **gestión de incidentes** que **culmina con una acción contundente que elimina la causa raíz del problema.** La existencia de una plataforma HSE, en este ejemplo, previene lesiones, heridas o alguna consecuencia aún más seria. Lesiones o enfermedades asociadas al trabajo que aparecen en circunstancias similares a la descrita son comunes en las organizaciones modernas. **La atención médica, sumada al coste del absentismo laboral, tienen un elevado coste para las empresas**.

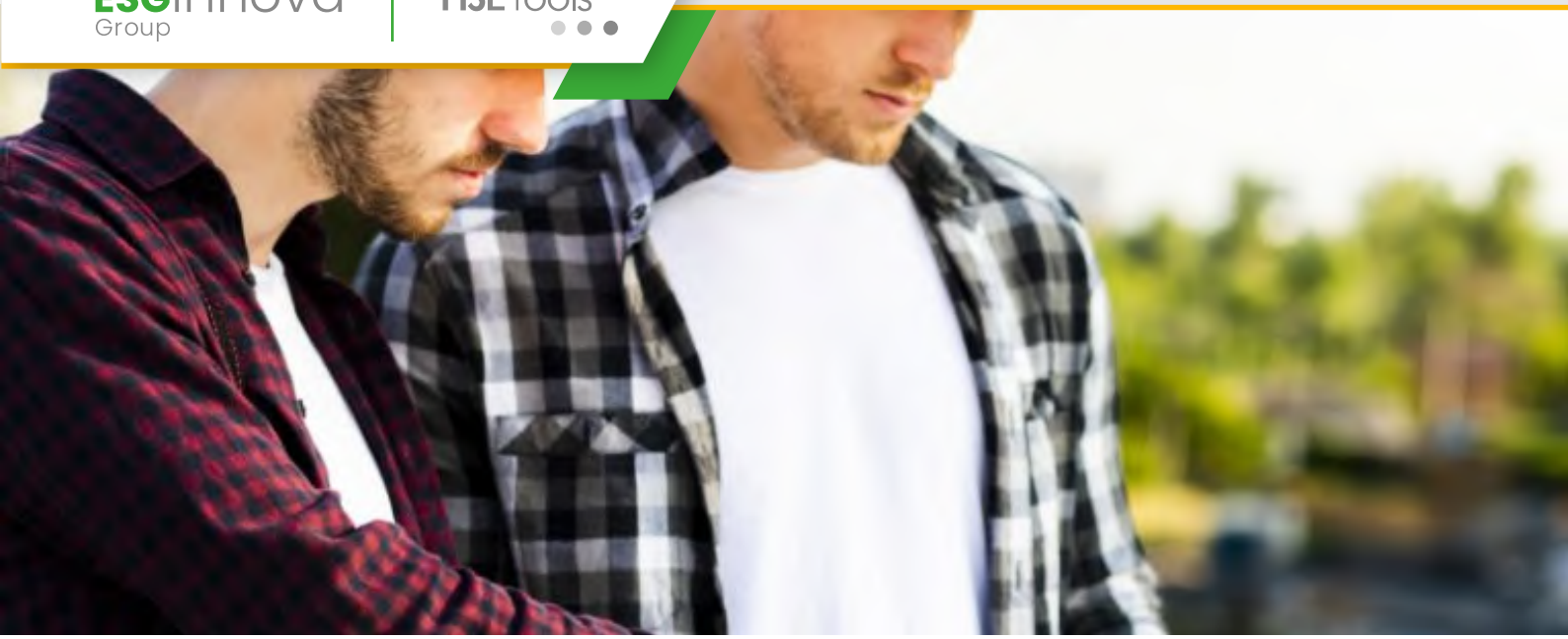
Uno de los motivos que con mayor recurrencia aparecen es la dificultad que encuentran los trabajadores para **interactuar con la organización, con los encargados de la seguridad en el trabajo** o con sus superiores. Es un problema que ayuda a resolver una plataforma HSE.

Cómo pueden las empresas aprovechar una plataforma HSE

La plataforma HSE puede hacer mucho más por una organización. Este tipo de software especializado se ha diseñado para identificar y **evaluar riesgos laborales**, pero también para **garantizar el cumplimiento regulatorio en el área de SST y el ambiental.** Cinco formas en las que las organizaciones pueden aprovechar el potencial de la plataforma HSE son las siguientes:

1. Reducir amenazas en los lugares de trabajo

Los accidentes laborales que tienen consecuencias severas o irreversibles, por fortuna, son pocos. El grueso de trabajadores que sufren accidentes o enfermedades asociadas al trabajo se ven afectados por **pequeños incidentes aparentemente inofensivos**: levantar algo muy pesado o hacerlo sin observar recomendaciones ergonómicas, resbalones, golpes fortuitos, etc. También hay pequeños accidentes en el hogar, espacio de trabajo habitual para muchas personas. Son tantas las fuentes y tan diversos los lugares en los que estas amenazas pueden aparecer, que controlarlas parece una tarea imposible. No lo es, sin embargo, para una plataforma HSE, que puede **estar presente en todos los espacios en los que haya un trabajador** con acceso a un dispositivo móvil.



¿Cuál es el rol del contratista en seguridad ocupacional?

En el ámbito de la **seguridad ocupacional**, el rol del **contratista** es clave para garantizar un entorno de trabajo seguro y libre de riesgos. En **sectores empresariales** de alta demanda, como la construcción, la minería, y la industria manufacturera, el trabajo con contratistas es una constante, y el compromiso de estos con la seguridad es determinante para el bienestar de todos los involucrados.

Pero, ¿en qué consiste exactamente su papel en seguridad ocupacional y cómo pueden las empresas optimizar esta gestión? En este artículo, abordaremos estas preguntas y exploraremos cómo la implementación de un **Software de Gestión de Contratistas** facilita esta labor, aportando seguridad, eficiencia y control.

Contratista

Los **contratistas**, al igual que los empleados directos de una empresa, deben cumplir con las **normativas** y **estándares de seguridad ocupacional** establecidos.

Sin embargo, su rol incluye responsabilidades específicas que se integran al sistema de seguridad de la empresa. Entre estas **responsabilidades** se destacan:

01. **Cumplimiento de normas y regulaciones**: Los contratistas deben familiarizarse y cumplir con las normativas de seguridad de la empresa contratante, así como con las regulaciones locales e internacionales, tales como las especificadas por la **ISO 45001**. Es vital que el contratista entienda los **requisitos específicos del sector** en el que trabaja y se adhiera a las prácticas de seguridad definidas.

02. **Evaluación y gestión de riesgos**: Antes de iniciar cualquier actividad, los contratistas deben participar en la evaluación de riesgos. Esto implica identificar peligros asociados a su labor, como el uso de maquinaria o la manipulación de materiales peligrosos, y proponer **medidas preventivas** para reducir riesgos.

03. **Capacitación en seguridad**: La capacitación incluye el uso adecuado del **equipo de protección personal** (EPP), **procedimientos de emergencia**, y habilidades para identificar y responder a riesgos en el lugar de trabajo. Una capacitación bien ejecutada empodera al equipo, fomentando una cultura de seguridad.

04. **Supervisión constante y monitoreo**: La supervisión es vital para mantener la seguridad ocupacional bajo control. Los contratistas deben realizar **inspecciones periódicas** de sus actividades y revisar continuamente las condiciones del lugar de trabajo, identificando riesgos potenciales y tomando **acciones correctivas** inmediatas si es necesario.

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO

Cómo aprovechar un software avanzado de gestión de contratistas para mejorar la producción

Contar con un **software avanzado de gestión de contratistas** es, para las organizaciones que dependen de esta fuerza laboral externa, una ventaja competitiva de alto valor, una herramienta indispensable en la eficiencia, el cumplimiento y la seguridad.

En el sector de la construcción, en muchas industrias transformadoras o manufactureras o, incluso, en industrias de extracción de minerales, mencionando algunas de las más representativas, **la tendencia es hacia la digitalización** que ofrece un software avanzado de gestión de contratistas. Las empresas aprovechan este tipo de soluciones digitales para **verificar el cumplimiento de sus contratistas**, crear canales para interactuar con ellos o controlar aspectos financieros y de cumplimiento regulatorio esenciales para una excelente relación.

Cómo aprovechar un software avanzado de gestión de contratistas para mejorar la producción

Gestionar contratistas en el lugar de trabajo es una tarea compleja. Factores como la seguridad ocupacional, la asignación de equipos de protección personal, la gestión remota cuando el contratista está en otro país, el control de la producción o los aspectos económicos del contrato requieren **un aliado tecnológico que incorpore funcionalidades que automaticen las tareas y optimicen la gestión**. Algunos de los aspectos en los que un software avanzado de gestión de contratistas es esencial para mejorar la producción son los que se explican a continuación:

1. Seleccionar los mejores contratistas

El **software para gestionar contratistas integra una base de datos** que registra nombres, direcciones, teléfonos, tarifas, especialidad, disponibilidad e incluso notas y calificaciones sobre el desempeño del contratista en su trabajo para la organización. Los contratistas nuevos también pueden ser seleccionados por un software avanzado de gestión de contratistas que aplique debida diligencia. **Puede investigar historial, establecer comparativas** y, finalmente, entregar las opciones que considera adecuadas.

2. Gestionar necesidades de formación y capacitación

De acuerdo con la información acumulada durante el proceso de selección, **el software identifica los programas de formación que debe recibir cada contratista.** Algunos programas serán obligatorios para todos los empleados, como los relacionados con las políticas de la organización, las normas internas o los reglamentos de seguridad y salud en el trabajo.

Elementos de protección personal más importantes en HSE

En el contexto de **Seguridad, Salud y Medio Ambiente (HSE)**, los **elementos de protección personal (EPP)** son fundamentales para garantizar la **seguridad** de los trabajadores en entornos de riesgo. Su uso correcto puede **prevenir accidentes y minimizar el impacto de posibles incidentes**. La **ISO 45001** establece pautas para implementar un sistema de gestión de seguridad que incluye la selección, uso y mantenimiento de estos equipos.

Elementos de protección personal

Los **elementos de protección personal (EPP)** son dispositivos, accesorios y prendas diseñados específicamente para **proteger a los empleados de riesgos** potenciales en su entorno laboral. Su propósito es **minimizar la exposición a peligros** que no se pueden eliminar completamente mediante otros medios de control, como los procedimientos de ingeniería o administrativos.

Los EPP actúan como una **barrera entre el trabajador y los riesgos presentes** en el lugar de trabajo.

El **uso de EPP** adecuado no solo **protege a los empleados**, sino que también contribuye al **cumplimiento normativo** de la **ISO 45001**. Esta norma internacional fomenta la creación de un **sistema de gestión de seguridad** que priorice el bienestar de los trabajadores, y los EPP son un componente clave de esta gestión, **reduciendo la posibilidad de lesiones y enfermedades laborales**.

Elementos de protección personal más importantes

Cascos de seguridad

Los **cascos de seguridad protegen la cabeza contra impactos, caídas de objetos y otros riesgos mecánicos**. Su uso es fundamental en sectores como la construcción, la minería y la manufactura, donde los trabajadores pueden estar **expuestos a golpes en la cabeza**. Los cascos también pueden **incluir características adicionales**, como protección facial y auditiva.

Protección ocular y facial

La **protección ocular** es esencial en trabajos donde existe **exposición a partículas, productos químicos o radiaciones**. Las **gafas de seguridad y las máscaras faciales** protegen contra salpicaduras, polvo y chispas, especialmente en actividades como la soldadura o el manejo de sustancias químicas. La **protección ocular** debe ser **cómoda** y **ajustarse bien al rostro** para garantizar una cobertura efectiva.

Beneficios de las soluciones digitales de seguridad y salud para maximizar la productividad

Las **soluciones digitales de seguridad y salud** en el trabajo ayudan a las organizaciones modernas a lograr objetivos, mejorar la productividad y garantizar el cumplimiento. Son tres ejes estructurales de la **gestión de SST** que necesitan atención y apoyo constantes.

Las soluciones digitales de seguridad y salud son un aliado de primer nivel en ese camino. Ofrecen, además, un gran valor agregado: **muchas tareas se automatizan**, liberando tiempo de los profesionales encargados en el área de SST. Tiempo que pueden dedicar a diseñar estrategias novedosas y anticiparse a las amenazas futuras.

Qué beneficios aportan las soluciones digitales de seguridad y salud en el trabajo

La gestión de seguridad y salud en el trabajo es una preocupación de orden prioritario para las organizaciones que operan en un vertiginoso mundo corporativo. Se trata de un entorno en el que **las regulaciones evolucionan todos los días y los riesgos se transforman**. A ello hay que sumar una tecnología que trae nuevas amenazas y las exigencias cada vez más complejas de las partes interesadas, entre ellas los trabajadores. En un entorno tan agitado, **pensar en mejorar la productividad resulta poco probable si no se cuenta con soluciones digitales** de seguridad y salud en el trabajo. Así, apoyarse en una **plataforma HSE** puede reportar beneficios más que interesantes:

1. Reducir los riesgos

Las soluciones digitales de seguridad y salud en el trabajo cuentan con funcionalidades, ya generadas por Inteligencia Artificial, **que monitorean y supervisan en tiempo real la actividad laboral** en busca de condiciones o circunstancias que tengan la capacidad para generar riesgos para los trabajadores. Los empleados, por otra parte, tienen a su disposición medios que permiten agilizar la **gestión de incidentes** en el mismo momento en que ocurren. Es posible informar utilizando vídeos, audios, textos, imágenes o cualquier formato y a través de todo tipo de dispositivos móviles. **Se consiguen así tiempos de respuesta más cortos.**

2. Disminuir costes

La automatización agiliza los procesos de SST, pero también aumenta la efectividad de las estrategias.

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO

3 claves para optimizar la seguridad en proyectos con contratistas

La colaboración con **contratistas** es una práctica común en proyectos empresariales de diversos sectores. Sin embargo, también supone **desafíos significativos** en términos de **seguridad laboral, cumplimiento normativo y gestión operativa**. Implementar medidas eficaces para optimizar la seguridad es vital para proteger a las personas, garantizar el éxito del proyecto y evitar sanciones legales.

Contratistas

Vamos a explorar juntos tres claves fundamentales para mejorar la seguridad en proyectos con contratistas, con un enfoque en cómo las empresas pueden potenciar estos esfuerzos mediante el uso de un **Software de Gestión de Contratistas** como el que ofrece **HSETools**.

1. Selección rigurosa de contratistas: Un punto de partida crítico

Seleccionar contratistas que cumplan con los **estándares de seguridad** de tu organización es el primer paso para minimizar riesgos. Para lograrlo, las empresas deben:

- **Auditar el historial de seguridad del contratista:** Revisar registros de incidentes, cumplimiento normativo y políticas internas.
- **Verificar certificaciones y capacitaciones:** Asegurar que sus trabajadores tengan formación en prevención de riesgos laborales.
- **Establecer criterios claros:** Incorporar cláusulas de seguridad en los contratos para definir responsabilidades y expectativas.

¿Cómo puede ayudarte HSETools?

Con nuestro Software de Gestión de Contratistas, puedes **centralizar toda la información** de evaluación, desde la documentación legal hasta los certificados de capacitación. Además, nuestra herramienta realiza **alertas automáticas** para documentos caducados, asegurando que los contratistas siempre estén actualizados.

2. Comunicación y capacitación continua: La base de una cultura segura

Un entorno laboral seguro depende de la comunicación efectiva y la formación adecuada. Esto aplica tanto a los trabajadores internos como a los contratistas.

Cómo gestionar el cumplimiento del contratista: pasos esenciales para una relación sin riesgos

Verificar el **cumplimiento del contratista** puede representar un verdadero desafío para una organización. Un reto que adquiere dimensiones colosales cuando la actividad se apoya en terceros en diferentes ubicaciones o es necesario optimizar la **seguridad en proyectos** allí donde esta fuerza laboral supera incluso a la plantilla propia.

Los contratistas necesitan cumplir con unas tareas en unos tiempos previstos y con unas normas de conducta mínimas. Además, **deben cumplir con las normas de Seguridad y Salud en el Trabajo**, una labor compleja que requiere de una vigilancia continua para cada contratista.

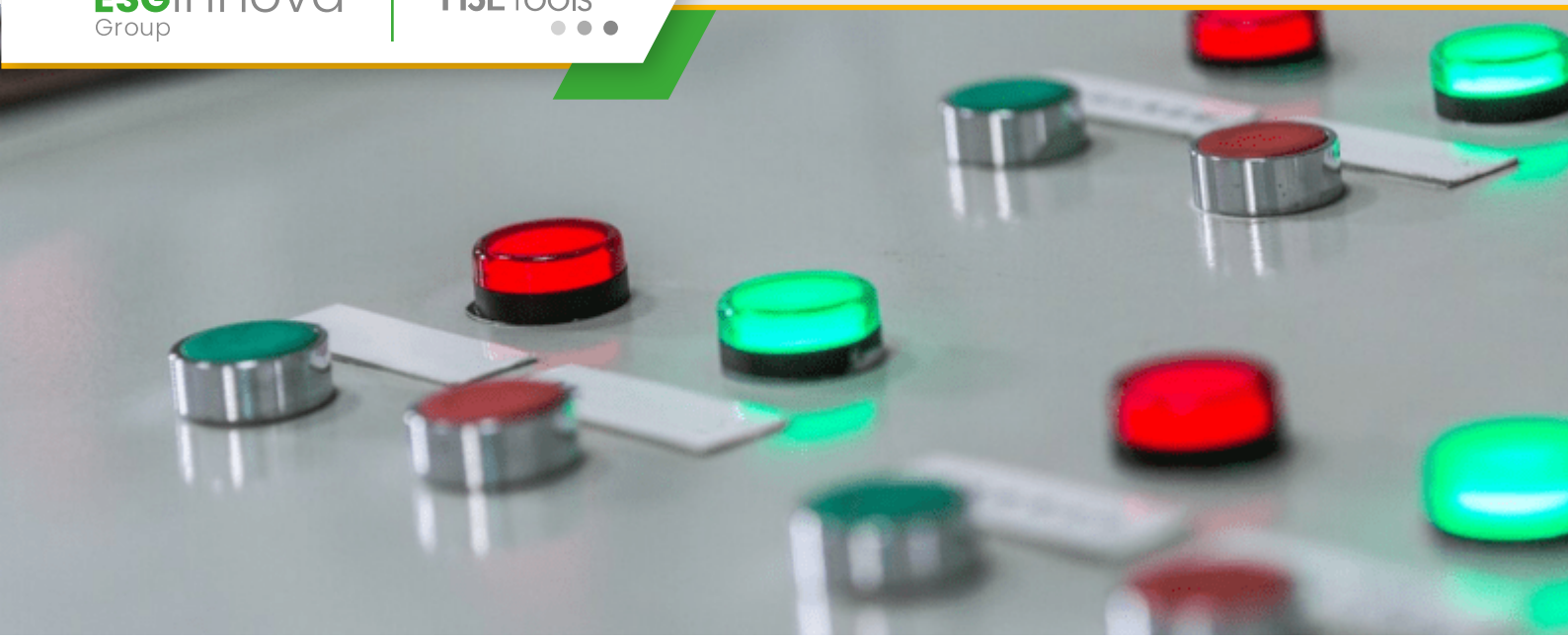
Qué es cumplimiento normativo de contratistas

La **gestión de contratistas** aborda temas como el cumplimiento del contratista de sus obligaciones contractuales, la capacidad para efectuar la tarea y la evaluación de la calidad del trabajo. También incluye el **cumplimiento de las obligaciones que la organización adquiere con el trabajador.** Dentro de esas obligaciones que la empresa adquiere con el contratista está la de **garantizar su seguridad y su integridad mientras realiza sus tareas**. Por supuesto, esta es una obligación compartida. Es, en otras palabras, un camino de doble vía. El cumplimiento normativo del contratista **integra controles, procedimientos, metodologías de verificación, inspecciones, evaluaciones**.

Por supuesto, incluye cualquier otra herramienta que se utilice para comprobar que el contratista o sus subcontratistas cumplen con las normas de seguridad, respetan los controles y adoptan como propios los **estándares de Seguridad y Salud en el Trabajo**. A pesar de todo ello, hay que tener en cuenta que el cumplimiento del contratista es apenas un segmento de la gestión de contratistas. Y dentro de ese segmento, **el cumplimiento normativo de SST es tal vez el más relevante**.

Cuáles son los desafíos que enfrenta el cumplimiento del contratista y cómo afrontarlos

La gestión del cumplimiento del contratista crece en complejidad con el número de terceros o con la dispersión de los lugares en los que prestan sus servicios. Para algunas empresas, verificar esta cuestión representa verdaderos desafíos.



Cómo lograr el éxito de tu proyecto con una matriz de riesgo

La **gestión de riesgos** es uno de los pilares fundamentales para **garantizar el éxito de cualquier proyecto**. Entre las herramientas más efectivas para **identificar, evaluar y priorizar riesgos** se encuentra la **matriz de riesgo**, un método visual que permite a las organizaciones tomar **decisiones informadas y minimizar impactos negativos**. Implementar una matriz de riesgo no solo **mejora la planificación**, sino que también **optimiza los recursos**, **evita contratiempos** y **fortalece la resiliencia** de los equipos ante situaciones inesperadas.

En este artículo, exploraremos qué es una matriz de riesgo, cómo elaborarla y cómo utilizarla para garantizar el éxito de tus proyectos.

Matriz de riesgo

La **matriz de riesgo** es una herramienta gráfica que clasifica los riesgos de un proyecto en función de su **probabilidad de**

ocurrencia y el **impacto** que tendrían si se materializan. Su principal objetivo es proporcionar una **visión clara y estructurada** de los riesgos para **priorizarlos y gestionarlos** de manera adecuada.

En una matriz de riesgo típica:

- El eje **vertical** representa el **impacto** del riesgo, desde leve hasta crítico.
- El eje **horizontal** representa la **probabilidad** de que el riesgo ocurra, desde improbable hasta muy probable.
- La intersección de estas dos variables asigna a cada riesgo una **prioridad** que puede ser **baja, media, alta o crítica**, dependiendo de su posición en la matriz.

Importancia en la gestión de proyectos

El uso de una matriz de riesgo aporta varios **beneficios** clave para el **éxito** de los proyectos:

- **Identificación temprana de riesgos:** Permite detectar problemas potenciales antes de que afecten al proyecto.
- **Priorización eficiente:** Ayuda a los equipos a concentrar sus esfuerzos en los riesgos más críticos.
- **Mejora en la toma de decisiones:** Proporciona datos claros para elegir las mejores estrategias de mitigación.
- **Optimización de recursos:** Reduce gastos innecesarios al abordar los riesgos de forma proactiva.

Equipos de protección en el lugar de trabajo: cómo garantizar que los empleados los usan

El uso de **equipos de protección en el lugar de trabajo** minimiza el riesgo de que los empleados sufran lesiones, heridas o consecuencias aún más graves en el caso de que se produzca un evento imprevisto, desde una simple caída a impactos, descargas eléctricas o fuego. Estos equipos son, por tanto, una medida de seguridad imprescindible en muchos puestos de trabajo y parte importante de la **gestión HSE**.

Los equipos de protección el lugar de trabajo, por otro lado, también **evitan que los empleados desarrollen enfermedades crónicas asociadas a su actividad laboral**. Es el caso de los dispositivos que protegen los oídos para empleados que trabajan sometidos a altos niveles de ruido o las gafas que protegen a trabajadores que utilizan equipos de soldadura. Pero las organizaciones no solo deben proporcionar a sus empleados los equipos de protección en el lugar de trabajo adecuados, también **deben asegurarse de que**

se utilizan siempre que la situación lo requiera. La primera razón para ello es, por supuesto, que garantizan la integridad de las personas. Pero también es un argumento válido el hecho de que el uso de equipos de protección en el lugar de trabajo **evita sanciones a la organización**, sin mencionar los costes de atención médica y asociados al **ausentismo laboral**.

Cómo hacer para que los empleados utilicen los equipos de protección en el lugar de trabajo

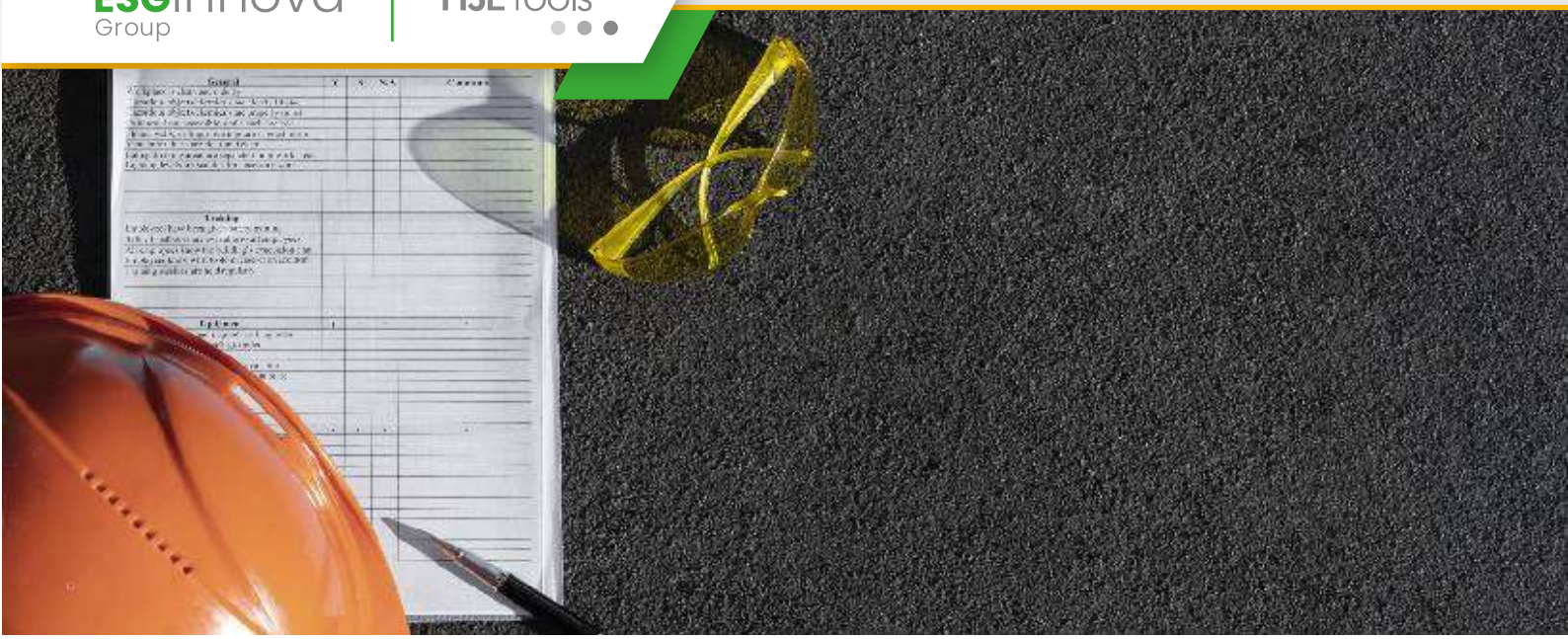
Pese a la importancia de los **elementos de protección personal**, hay empleados que se resisten a utilizarlos y las consecuencias pueden ser nefastas. Implementar estrategias para impulsar el uso de equipos de protección en el lugar de trabajo, por tanto, es fundamental. Se trata de una tarea que **se puede abordar desde diferentes puntos de vista y acciones** como las que se indican a continuación.

1. Enseñar a los empleados a utilizar los equipos

Aunque los EPP no requieren un complejo programa de formación para su uso, sí necesitan tiempo de capacitación para **entender la razón por la que se deben utilizar**, los momentos en los que se debe hacer y la forma correcta de usarlos. Por eso, la **política de equipos de protección individual** de la organización debe destinar unas horas a la formación, de hecho, puede ser suficiente para vencer la resistencia de un buen número de empleados.

2. Indicar las consecuencias de no utilizar EPP

Dentro de la misma capacitación se pueden utilizar un tiempo para explicar qué sucede cuando un trabajador omite la obligación de utilizar equipos de protección en el lugar de trabajo.



Principales normas de seguridad de la industria HSE

Las empresas deben estar comprometidas con la sostenibilidad del bienestar de su equipo humano. Para ello se crean políticas de seguridad y salud en el trabajo para sostener este pilar que es fundamental. En la **industria HSE** (Health, Safety, and Environment), cumplir con normas de seguridad es una obligación legal, que además se convierte en una oportunidad para transformar la cultura organizacional, minimizar riesgos y optimizar procesos.

Nos gustaría hacerte un recorrido por las principales normas de seguridad en la industria HSE y cómo su implementación, junto con un **Software de Requisitos Legales**, puede marcar la diferencia en la gestión empresarial.

Normas de seguridad

Las normas de seguridad en la industria HSE son **marcos regulatorios y estándares internacionales** diseñados para proteger a los trabajadores, las comunidades y el medio ambiente.

Estas regulaciones establecen requisitos específicos para prevenir accidentes, enfermedades laborales y daños ambientales, fomentando un desarrollo empresarial sostenible.

Principales normas de seguridad en la industria HSE

A continuación, te presentamos las normativas clave que rigen la industria HSE:

ISO 45001: Gestión de Seguridad y Salud en el Trabajo

- Proporciona un marco para identificar peligros, evaluar riesgos y establecer controles efectivos.
- Promueve un **entorno laboral seguro** y previene accidentes y enfermedades ocupacionales.

ISO 14001: Gestión Ambiental

- Ayuda a las empresas a gestionar su impacto ambiental.
- Impulsa prácticas sostenibles, como la reducción de residuos y emisiones.

NFPA (National Fire Protection Association)

- Establece estándares para la seguridad contra incendios.
- Incluye la **NFPA 70 (Código Eléctrico Nacional)** y la **NFPA 101 (Código de Seguridad Humana)**.

¿Por qué es tan importante un sistema HSEQ?

En el entorno empresarial actual, donde la sostenibilidad, la calidad y la seguridad son prioridades, contar con un **sistema de HSEQ** (Health, Safety, Environment, and Quality) es esencial. Este sistema integrado permite a las organizaciones gestionar de manera eficiente aspectos relacionados con la **salud**, la **seguridad**, el **medioambiente** y la **calidad**, garantizando el **cumplimiento normativo**, la **mejora continua** y la **competitividad** en el mercado.

En este artículo, exploraremos qué es un sistema HSEQ, sus beneficios y cómo puede transformar la forma en que las empresas gestionan sus operaciones.

HSEQ

El término **HSEQ** se refiere a un **enfoque integral** que combina cuatro áreas clave:

- **Salud (Health):** Protección de la salud física y mental de los empleados y stakeholders.

- **Seguridad (Safety):** Prevención de accidentes y gestión de riesgos en el lugar de trabajo.

- **Medioambiente (Environment):** Minimización del impacto ambiental de las actividades empresariales.

- **Calidad (Quality):** Aseguramiento de que los productos y servicios cumplen con estándares establecidos y las expectativas del cliente.

El sistema HSEQ se implementa a través de un marco integrado de **políticas, procedimientos y estándares** que se alinean con normativas internacionales, como las **ISO 45001** para seguridad y salud, la **ISO 14001** para gestión ambiental, y la **ISO 9001** para calidad.

Beneficios de implementar un sistema HSEQ

Adoptar un sistema HSEQ trae consigo múltiples **ventajas** para las organizaciones, tanto a nivel interno como externo.

Mejora la seguridad y el bienestar de los empleados

La **gestión de la seguridad y la salud** en el trabajo es uno de los pilares fundamentales del **HSEQ**. Un sistema bien implementado:

- Reduce la **tasa de accidentes** laborales.

- Promueve un **entorno** de trabajo más **seguro y saludable**.

- Incrementa la **satisfacción y motivación** de los empleados.

ESGinnova Group

GRCTools

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

COBIT 2019: Procesos clave y mejores prácticas de control

La **tecnología** se ha convertido en un activo estratégico, así pues, la alineación de los objetivos de TI con la estrategia corporativa es fundamental. **COBIT 2019** es una regulación referente que permite a las organizaciones gestionar y gobernar la **tecnología de la información (TI)** de manera óptima y alineada con sus objetivos estratégicos. Es necesario destacar los procesos clave y las mejores prácticas de control en COBIT 2019, y cómo una **Gestión de Riesgos IT – Seguridad de la Información**, como la de GRCTools, puede potenciar la implementación de estas prácticas para mejorar la resiliencia, el cumplimiento y la eficiencia en las organizaciones.

COBIT 2019

COBIT (Control Objectives for Information and Related Technologies) es un marco integral desarrollado por **ISACA** que proporciona un conjunto de herramientas y procesos para gestionar y controlar la información y la tecnología. COBIT 2019, la última versión de este marco, incorpora cambios significativos respecto a versiones anteriores, ofreciendo un **enfoque más flexible y adaptado a las**

necesidades actuales del negocio digital. Este marco se organiza en cinco dominios clave, cada uno con procesos específicos que cubren distintos aspectos de la gestión de TI.

Procesos clave en COBIT 2019

COBIT 2019 estructura sus procesos en cinco dominios que abarcan desde la planificación y alineación de TI hasta la entrega de servicios y el monitoreo. Veamos cada uno de ellos en detalle:

Evaluación, Dirección y Monitoreo (EDM)

Este dominio es esencial para asegurar que la TI esté alineada con los objetivos estratégicos de la organización. Incluye procesos para:

- **EDM01**: Asegurar el marco de gobernanza de TI alineado con la estrategia de negocio.
- **EDM02**: Asegurar la creación de valor y el cumplimiento de objetivos de rendimiento.
- **EDM03**: Asegurar el cumplimiento normativo y la gestión de riesgos.

El dominio EDM ayuda a los líderes de TI y de negocio a evaluar continuamente cómo la tecnología está contribuyendo a la estrategia general.

Principales beneficios del software GRC en la gestión de riesgos corporativos

En un entorno empresarial cada vez más complejo, donde los riesgos pueden surgir de múltiples áreas como las finanzas, la ciberseguridad, el cumplimiento normativo y la cadena de suministro, contar con una herramienta que facilite la **gestión integral de riesgos** es esencial. Aquí es donde entra en juego el **software GRC** (Governance, Risk, and Compliance), una solución que permite centralizar y optimizar la gestión de riesgos y el cumplimiento normativo en una sola plataforma.

En este artículo, exploraremos los beneficios clave de utilizar un software GRC en la gestión de **riesgos corporativos** y cómo puede ayudarte a proteger los activos de tu empresa, mejorar la toma de decisiones y asegurar el cumplimiento regulatorio.

¿Qué es un software GRC y cómo funciona?

Un software GRC es una plataforma diseñada para ayudar a las organizaciones a gestionar la gobernanza, los riesgos y el cumplimiento de manera centralizada y coordinada. Esta herramienta permite a las empresas identificar, evaluar y mitigar los riesgos en todas sus áreas operativas, desde los **riesgos financieros** hasta los riesgos de **seguridad de la información**.

Gracias a su capacidad para automatizar procesos y brindar una visión integral de los riesgos, el software GRC se ha convertido en una herramienta esencial para las empresas que buscan optimizar su gestión de riesgos corporativos.

Principales beneficios del software **GRC** en la gestión de riesgos corporativos

El uso de un software **GRC** ofrece múltiples ventajas que facilitan la gestión eficaz de los riesgos y mejoran el rendimiento general de la organización. A continuación, te mostramos los beneficios clave de implementar esta herramienta en tu empresa:

1. Centralización y visibilidad total de los riesgos

Uno de los mayores beneficios del software GRC es la capacidad de **centralizar toda la información relacionada con los riesgos corporativos en un solo sistema**. Esto permite a los directivos y equipos de gestión tener una visión completa y actualizada de los riesgos a los que está expuesta la empresa, lo que facilita una respuesta rápida y coordinada ante cualquier eventualidad.

Cumplimiento NERC-CIP: requisitos y mejores prácticas para la seguridad eléctrica

La seguridad en el sector eléctrico es un asunto crítico para proteger la infraestructura energética y garantizar la continuidad del suministro. En Norteamérica, el **cumplimiento NERC-CIP (North American Electric Reliability Corporation – Critical Infrastructure Protection)** establece los estándares que deben seguir las empresas de servicios eléctricos para proteger sus sistemas críticos frente a amenazas y vulnerabilidades. Cumplir con estos estándares no solo es una obligación regulatoria, sino también una práctica esencial para mitigar los riesgos de ciberseguridad y otros **riesgos corporativo**s asociados a la seguridad eléctrica.

En este artículo, exploraremos los requisitos clave del cumplimiento NERC-CIP y las mejores prácticas para implementarlo de manera efectiva en tu organización.

¿Qué es NERC-CIP?

El NERC-CIP es un conjunto de normas desarrolladas por la North American Electric Reliability Corporation (NERC) para **proteger las infraestructuras críticas de las redes eléctricas** en Estados Unidos, Canadá y partes de México. Estas normas están diseñadas para garantizar que los activos de alto valor y los sistemas de control de energía se mantengan seguros frente a amenazas físicas y cibernéticas, minimizando así el impacto de cualquier incidente que pudiera poner en riesgo el suministro eléctrico.

Los estándares NERC-CIP cubren una amplia gama de aspectos, desde la identificación de activos críticos hasta el control de accesos y la gestión de incidentes de seguridad.

Requisitos clave del cumplimiento NERC-CIP

El cumplimiento NERC-CIP incluye varios requisitos específicos que las empresas de servicios eléctricos deben seguir para proteger sus sistemas críticos. A continuación, te detallamos algunos de los más importantes:

CIP-002: Identificación y clasificación de activos críticos

Este estándar exige que las organizaciones identifiquen y clasifiquen los activos críticos de sus infraestructuras eléctricas.

El objetivo es asegurar que aquellos sistemas y activos cuya falla podría afectar la seguridad y fiabilidad de la red sean protegidos con controles específicos.

Integración de GRC en la estrategia de ciberseguridad corporativa

En un entorno empresarial cada vez más digitalizado, la **ciberseguridad corporativa** se ha convertido en una **prioridad** esencial para las organizaciones. La gestión de riesgos, la gobernanza y el cumplimiento (GRC, por sus siglas en inglés) juegan un papel crucial en la **protección de los activos y la información de la empresa**. Este artículo explora cómo la integración de GRC en la estrategia de **ciberseguridad corporativa** puede **mejorar la resiliencia organizativa**, **optimizar recursos** y asegurar el **cumplimiento normativo**.

Ciberseguridad corporativa

La **ciberseguridad corporativa** es esencial para **proteger los activos digitales** de la empresa y salvaguardar la confidencialidad, integridad y disponibilidad de la información. Los ciberataques son cada vez **más sofisticados**, y las consecuencias de una **violación de seguridad** pueden ser devastadoras.

Importancia de la ciberseguridad corporativa

Algunas de las principales **razones** para priorizar la ciberseguridad incluyen:

Protección de datos

Las organizaciones manejan una gran cantidad de **datos sensibles** que, si se ven comprometidos, pueden **causar daños** irreparables a la **reputación** y la **confianza** del cliente. Implementar una estrategia robusta de ciberseguridad corporativa ayuda a **proteger esta información**.

Cumplimiento regulatorio

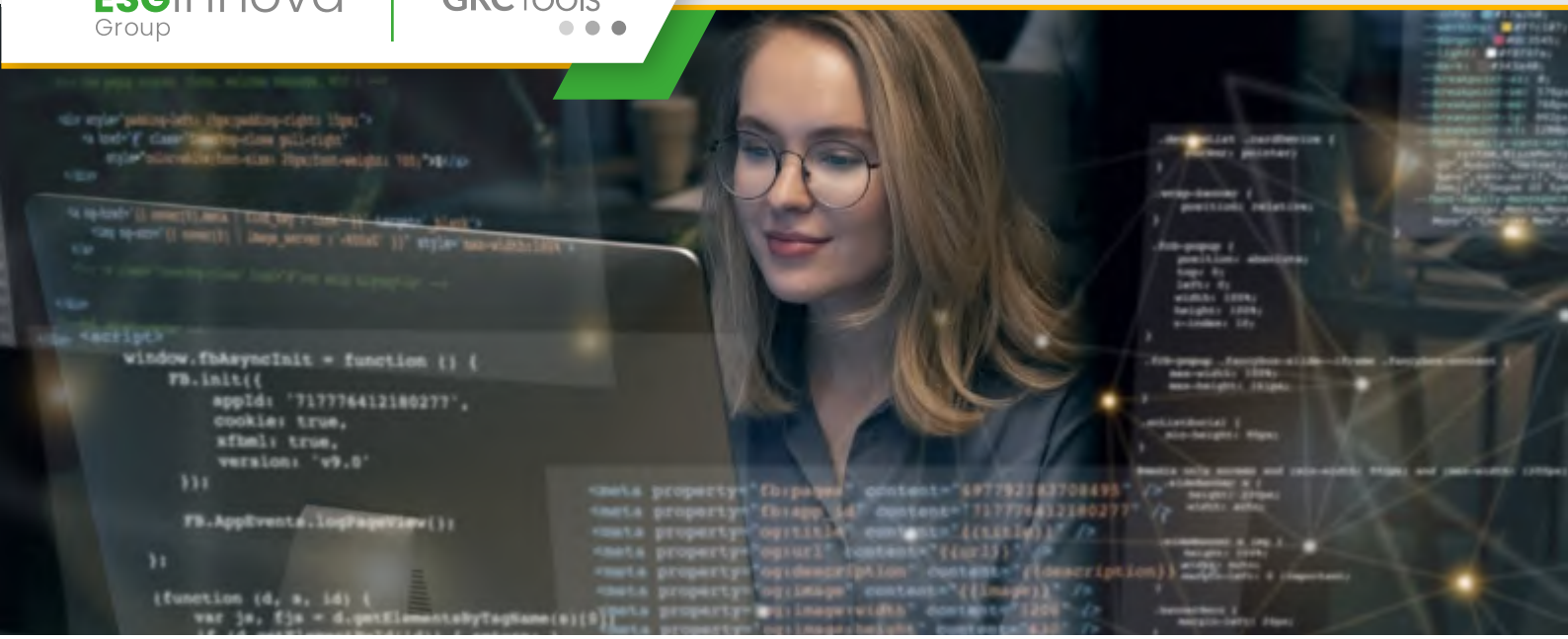
La falta de medidas adecuadas de ciberseguridad puede resultar en **multas y sanciones severas**.

Las empresas deben **cumplir** con una variedad de **regulaciones de protección de datos y privacidad**, lo que hace que la integración de GRC en la ciberseguridad sea aún más **crítica**.

Continuidad del negocio

Un incidente de seguridad puede interrumpir las operaciones comerciales y causar **pérdidas financieras significativas**.

Una estrategia efectiva de ciberseguridad corporativa asegura que la organización pueda **continuar operando** incluso ante un ataque cibernético.



Cumplimiento Normativo y Gestión de Riesgos: El Rol del Software GRC

El **Software GRC** (Gobierno, Riesgo y Cumplimiento) ha emergido como una solución tecnológica indispensable para apoyar a las empresas en su esfuerzo por gestionar de manera eficiente el **cumplimiento normativo** y la **gestión de riesgos**. A través de herramientas como las que ofrece la plataforma tecnológica **GRCTools**, las empresas pueden dar un salto hacia una gestión más ágil, integral y confiable de sus obligaciones normativas y los riesgos inherentes a su operación.

¿Qué es el Software GRC?

El Software GRC es una herramienta diseñada para gestionar las tres áreas clave en cualquier organización: el **gobierno corporativo**, la gestión de **riesgos** y el **cumplimiento normativo**. El objetivo de un sistema GRC es proporcionar un escenario único y centralizado para que las empresas puedan **identificar, evaluar, controlar y monitorear** tanto los riesgos como su alineación con las normativas locales e internacionales.

Esto es especialmente relevante en sectores donde la **regulación** es **estricta**, como el financiero, el de salud, el energético y el de manufactura, aunque cualquier empresa que busque fortalecer su **sostenibilidad** a largo plazo puede beneficiarse de un Software GRC.

Cumplimiento Normativo: Clave para la Sostenibilidad Corporativa

El cumplimiento normativo implica asegurar que todas las operaciones de una organización estén en línea con las **leyes, regulaciones y estándares de la industria**. Sin embargo, gestionar este cumplimiento es una **tarea compleja**, ya que implica mantenerse **actualizado** con normativas que cambian constantemente y que varían según la jurisdicción y el sector. En este sentido, un Software GRC como el de **GRCTools** permite a las empresas:

- **Automatizar el seguimiento de normativas:** La automatización reduce el margen de error humano y asegura que las políticas estén siempre actualizadas y que se cumplan sin necesidad de intervención manual constante.

- **Centralizar la documentación:** Una plataforma GRC almacena todos los documentos relacionados con las políticas de cumplimiento en un solo lugar, facilitando el acceso y mejorando la colaboración entre departamentos.

- **Generar reportes y auditorías fácilmente:** Los sistemas GRC permiten crear informes detallados que demuestran a los reguladores y auditores externos que la organización está en cumplimiento.

Cómo un Software GRC Fortalece la Toma de Decisiones Basadas en Riesgos

La **gestión de riesgos, la gobernanza y el cumplimiento** (GRC) son fundamentales en el entorno empresarial actual. En un contexto de constantes **cambios regulatorios** y de un **aumento en la complejidad de los riesgos**, las organizaciones necesitan tomar decisiones informadas para **minimizar el impacto negativo** en sus operaciones.

Es aquí donde entra en juego el **Software GRC**, una herramienta que no solo facilita el **cumplimiento y la gestión de riesgos**, sino que también **optimiza la toma de decisiones** a través de un enfoque integral de gobernanza, riesgo y cumplimiento.

Software GRC

Un **Software GRC** es una **plataforma digital** diseñada para **ayudar a las organizaciones a implementar y mantener procesos de gestión de riesgos, gobernanza y cumplimiento**. Estas herramientas permiten a las empresas automatizar, centralizar y coordinar los procesos de GRC en toda la organización, brindando una visión clara de los riesgos y facilitando el cumplimiento normativo.

Un Software GRC tiene una serie de características clave:

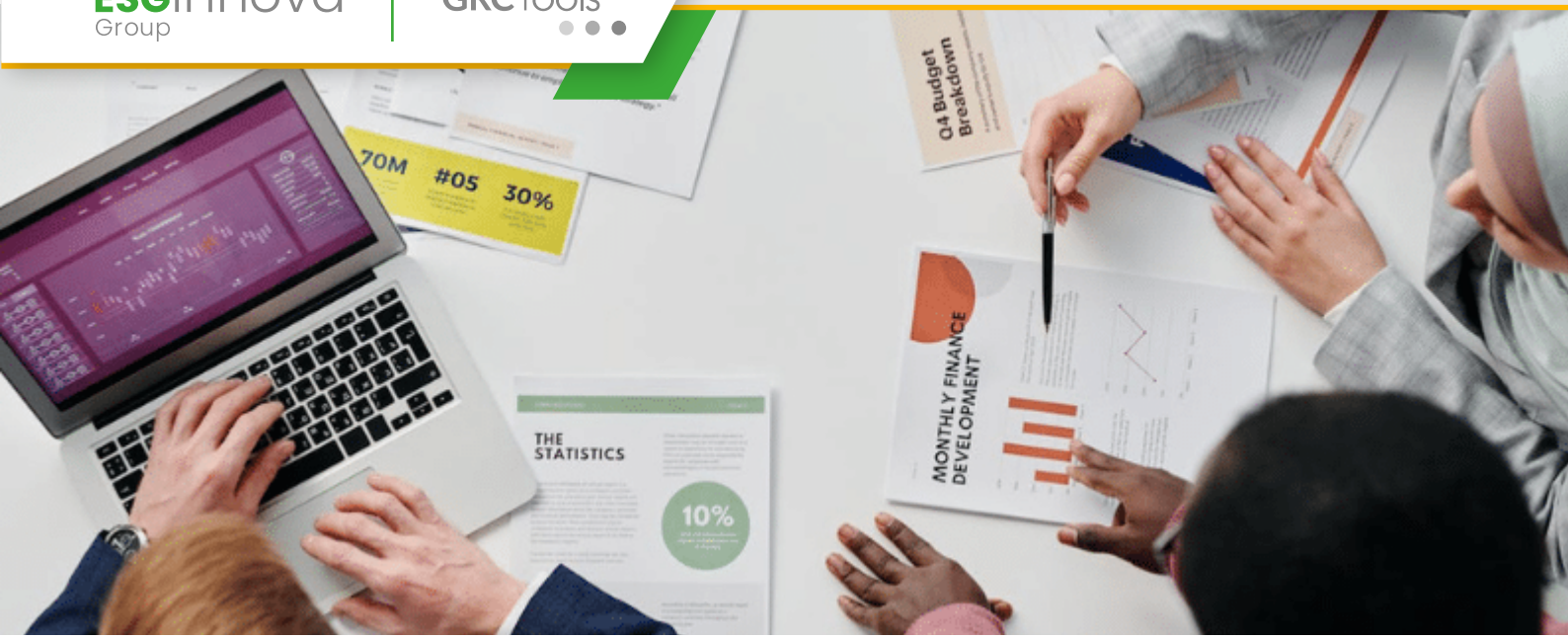
- **Automatización de procesos**: Un Software GRC permite automatizar tareas y flujos de trabajo, reduciendo el tiempo dedicado a procesos repetitivos y mejorando la eficiencia.

- **Centralización de datos**: Al unificar la información en un solo lugar, las organizaciones pueden acceder a una visión integral de sus riesgos y cumplir con los requisitos regulatorios de manera más ágil.

- **Reportes y análisis avanzados**: Estas herramientas ofrecen la capacidad de generar informes detallados que permiten a los líderes empresariales evaluar y monitorear riesgos en tiempo real.

La importancia de la toma de decisiones basada en riesgos

La toma de decisiones basada en riesgos implica **evaluar y priorizar los riesgos** para **tomar decisiones estratégicas** que **minimicen el impacto** negativo en la organización.



Gestión de riesgos estratégicos: clave para el éxito empresarial

En el entorno empresarial actual, las organizaciones se enfrentan a desafíos constantes y cambios rápidos que pueden afectar sus objetivos a largo plazo. La **gestión de riesgos estratégicos** se ha convertido en un componente esencial para aquellas empresas que buscan no solo sobrevivir, sino prosperar y mantenerse competitivas en el mercado. Estos riesgos incluyen factores externos, como cambios en el mercado o regulaciones, y factores internos, como la toma de decisiones de alto nivel y la adaptación a nuevas tecnologías.

En este artículo, exploraremos la importancia de la **gestión de riesgos estratégicos** y cómo una estrategia eficaz puede ayudar a las organizaciones a anticiparse y responder con agilidad a los desafíos empresariales.

¿Qué son los riesgos estratégicos?

Los **riesgos estratégicos** son aquellos que pueden impactar en la capacidad de una empresa para alcanzar sus objetivos y mantener su posición en el mercado. **Estos riesgos están directamente relacionados con las decisiones que definen la dirección de la empresa**, como la expansión a nuevos mercados, el desarrollo de productos innovadores o el establecimiento de alianzas estratégicas.

Algunos ejemplos de **riesgos estratégicos** incluyen:

Cambios en el entorno económico: Fluctuaciones en la economía global pueden afectar la demanda de productos o servicios, y generar incertidumbre en la planificación a largo plazo.

Innovación tecnológica: **No adaptarse rápidamente a los avances tecnológicos puede dejar a una empresa en desventaja competitiva**. Empresas que no innovan a tiempo pueden perder su relevancia en el mercado.

Competencia y cambios en el mercado: Nuevos competidores y cambios en las preferencias del consumidor pueden alterar el mercado, exigiendo que las empresas se adapten o redefinan sus estrategias.

Los riesgos estratégicos tienen el potencial de afectar no solo los resultados financieros de una empresa, sino también su reputación y sus relaciones con clientes e inversores.

Proceso clave para la evaluación de riesgos operacionales en negocios

La **evaluación de riesgos operacionales** es un proceso fundamental para identificar y gestionar amenazas que pueden afectar la eficiencia, productividad y seguridad de una empresa. Estos riesgos abarcan desde fallos en procesos internos y errores humanos hasta problemas de infraestructura y tecnología, los cuales pueden generar pérdidas financieras significativas y afectar la reputación de la organización. **Contar con una estrategia de evaluación de riesgos operacionales no solo permite minimizar el impacto de estos eventos, sino que también mejora la resiliencia organizacional y asegura la continuidad del negocio**.

En este artículo, exploraremos los pasos clave para una evaluación eficaz de riesgos operacionales, asegurando que tu empresa pueda identificar y mitigar las amenazas antes de que se conviertan en problemas graves.

¿Qué son los riesgos operacionales?

Los **riesgos operacionales** son aquellos que surgen de fallos o debilidades en los procesos internos de una organización, así como de factores externos que afectan su capacidad para operar de manera eficiente. **Estos riesgos pueden estar relacionados con la tecnología, las personas, los procesos o incluso con eventos externos imprevistos**, como desastres naturales.

Algunos ejemplos de riesgos operacionales incluyen:

- Fallos en los sistemas informáticos que afectan la productividad.
- Errores en la cadena de suministro que generan retrasos.
- Incidentes de seguridad o ciberataques que comprometen datos sensibles.
- Problemas de cumplimiento normativo que llevan a sanciones.

La evaluación de estos riesgos permite a las organizaciones identificar las áreas de mayor vulnerabilidad y diseñar estrategias de mitigación para reducir el impacto de posibles incidentes.

Pasos clave en el proceso de evaluación de riesgos operacionales

Para implementar una evaluación eficaz de riesgos operacionales, es necesario seguir un enfoque estructurado y basado en datos que permita identificar, evaluar y gestionar estos riesgos de manera sistemática.

Ley Marco de Ciberseguridad en Chile: Protegiendo la Infraestructura Crítica

La nueva **Ley Marco de Ciberseguridad en Chile** representa un avance significativo en la protección de la infraestructura crítica nacional, y en la regulación de estándares de seguridad, ofreciendo un enfoque integral para **reducir las amenazas digitales** en sectores esenciales como **energía**, **telecomunicaciones**, **transporte** y servicios **financieros**.

La normativa busca proteger sistemas y servicios fundamentales, si no también impulsar la colaboración público-privada, establecer directrices y ofrecer mecanismos de monitoreo y respuesta ante incidentes cibernéticos.

Esta ley es, sin duda, un paso adelante para posicionar a Chile como un país resiliente en ciberseguridad y un referente en la protección digital a nivel regional.

Ley Marco de Ciberseguridad en Chile

La Ley Marco de Ciberseguridad en Chile fue desarrollada en respuesta al creciente número de **ciberataques** y al riesgo que estos representan para la **seguridad nacional** y la **economía**. La ley establece un marco regulatorio y técnico que define las pautas para la protección de la infraestructura crítica y la gestión de ciberincidentes, promoviendo la adopción de **estándares internacionales** y **protocolos de seguridad**.

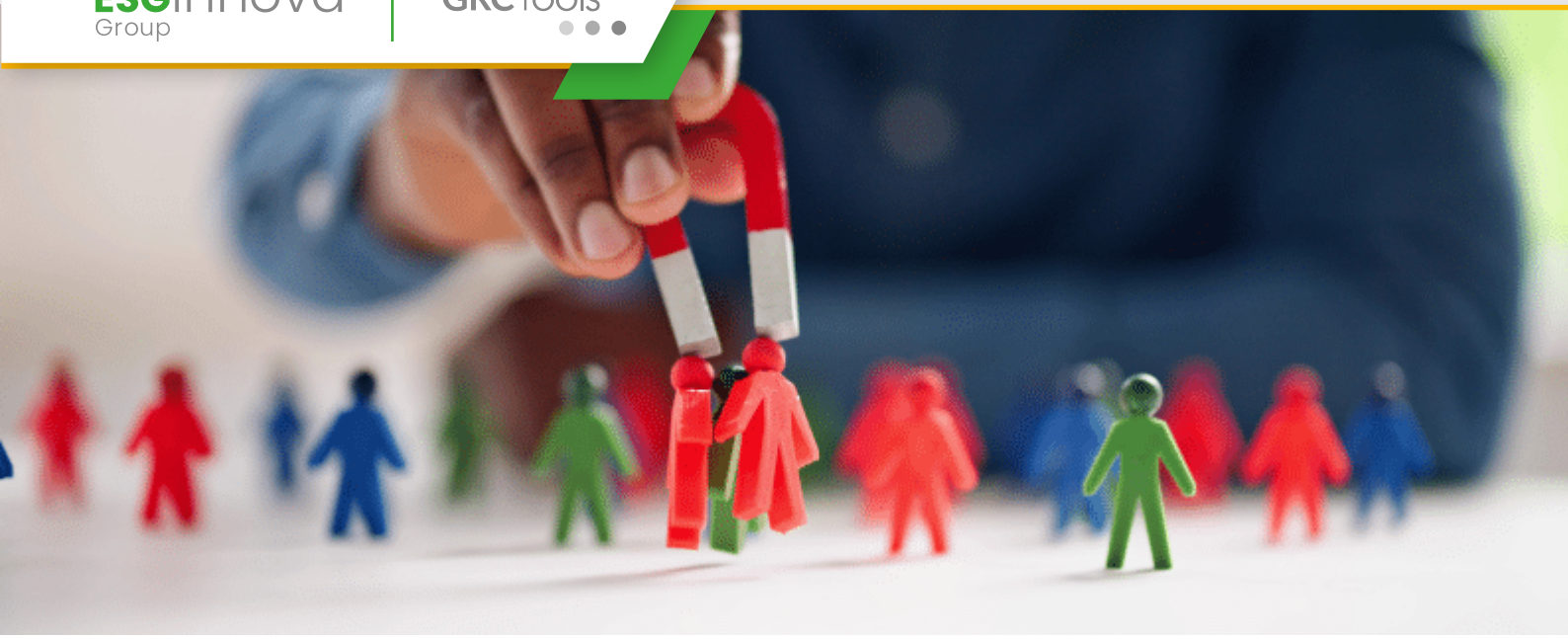
Principales objetivos de la Ley Marco de Ciberseguridad en Chile

Protección de infraestructura crítica: Define y categoriza las infraestructuras críticas, tales como energía, transporte y servicios financieros, imponiendo requisitos específicos de seguridad para su resguardo y resiliencia.

- **Colaboración público-privada:** Estimula la colaboración entre el gobierno y el sector privado para intercambiar información sobre amenazas y mejorar la respuesta ante incidentes.

- **Establecimiento de estándares:** La ley promueve la adopción de estándares internacionales, como la ISO/IEC 27001, y de marcos de ciberseguridad reconocidos a nivel mundial.

- **Capacitación y sensibilización:** Incorpora la capacitación y sensibilización en ciberseguridad para garantizar que todos los actores, públicos y privados, estén preparados para enfrentar amenazas digitales.



Claves para gestionar los riesgos de terceros en tu empresa

Gestionar los riesgos de terceros es fundamental para **garantizar que los socios, proveedores y contratistas** de una organización **operen en línea con sus objetivos y políticas**. A medida que las empresas dependen más de terceros, la **identificación** y **mitigación de riesgos** asociados se vuelve crítica para proteger la **integridad, reputación y continuidad del negocio**. En este artículo, veremos cómo gestionar eficazmente estos riesgos y las **mejores prácticas para minimizar su impacto**.

Gestionar los riesgos de terceros

Los **riesgos de terceros** abarcan todos los problemas potenciales que pueden surgir cuando una empresa se **asocia con organizaciones externas** para la provisión de servicios, productos o tecnología. Estos riesgos incluyen desde **problemas financieros y de cumplimiento normativo** hasta **vulnerabilidades de ciberseguridad y riesgos operacionales**.

La gestión de estos riesgos garantiza que todas las partes involucradas en el ecosistema empresarial sigan los **estándares de seguridad y calidad**.

Gestionar los riesgos de terceros de forma correcta permite a las empresas **reducir** la posibilidad de **problemas legales**, **incidentes de seguridad** y **fallos operativos**. Además, **mejora la transparencia y la confianza** entre las partes, proporcionando una mayor estabilidad en la relación comercial y asegurando que los proveedores y socios **cumplan con las normativas y los valores de la organización**.

Principales tipos de riesgos asociados

Riesgo de cumplimiento

El **riesgo de cumplimiento** surge cuando los proveedores o socios no cumplen con las leyes, reglamentos o estándares requeridos. Esto puede llevar a **sanciones legales y financieras** para la empresa contratante. Para gestionar este riesgo, es fundamental que los terceros **comprendan** y se **adhieran a las políticas internas y requisitos normativos** de la empresa.

Riesgo de ciberseguridad

El **riesgo de ciberseguridad** es una de las **mayores preocupaciones** para gestionar los riesgos de terceros, especialmente cuando se comparte **información confidencial**. Las empresas deben asegurarse de que los terceros cuenten con **protocolos de seguridad robustos** y que puedan proteger los datos **contra accesos no autorizados y ciberataques**.

Impacto del Software GRC en la Reducción de Riesgos Operativos

Las organizaciones enfrentan **desafíos constantes**, desde interrupciones en la cadena de suministro hasta incumplimientos regulatorios, que pueden poner en peligro su reputación, continuidad y resultados financieros. La importancia de un **Software GRC (Gobernanza, Riesgos y Cumplimiento)** en estas situaciones no es discutible. Contar con una solución diseñada para reducir **riesgos**, optimizar procesos y garantizar el cumplimiento normativo es necesario desde el punto de vista estratégico.

¿Quieres conocer más detalles sobre el impacto positivo que puede generar una plataforma tecnológica en la gestión de riesgos operativos? A continuación, te lo explicamos.

Software GRC

Los riesgos operativos incluyen cualquier amenaza que pueda **interrumpir las actividades** diarias de una organización.

Pueden abarcar:

- **Fallos en los procesos internos**.
- **Problemas tecnológicos**.
- **Factores externos como desastres naturales o cambios regulatorios**.

Una mala gestión de estos riesgos puede traducirse en pérdidas económicas, daños reputacionales y multas regulatorias. Por ello, la implementación de un **Software GRC** atenúa los riesgos y permite una gestión más eficiente y proactiva.

El papel del Software GRC en la reducción de riesgos operativos

El **Software GRC** es una herramienta esencial para las empresas modernas. Su implementación permite identificar, evaluar y mitigar riesgos de manera sistemática. Entre sus principales beneficios se encuentran:

1. Centralización de la información

El Software GRC consolida todos los datos relacionados con los riesgos en un **único sistema**. Esto permite una **visión integral** y **actualizada**, mejorando la toma de decisiones basadas en datos.

Comparativa: Software GRC vs. métodos tradicionales de gestión de riesgos

La **gestión integral de riesgos** es esencial para cualquier organización que desee protegerse contra amenazas internas y externas, cumplir con las normativas y optimizar sus operaciones. Tradicionalmente, muchas empresas han utilizado hojas de cálculo, documentos manuales y reuniones presenciales para gestionar sus riesgos. Sin embargo, con el avance de la tecnología, el software **GRC (Governance, Risk, and Compliance)** se ha posicionado como una solución más eficiente y efectiva.

En este artículo, analizamos las diferencias clave entre los métodos tradicionales de gestión de riesgos y las plataformas de software GRC, destacando sus ventajas, limitaciones y el impacto que pueden tener en la operación de una empresa.

Métodos tradicionales de gestión de riesgos

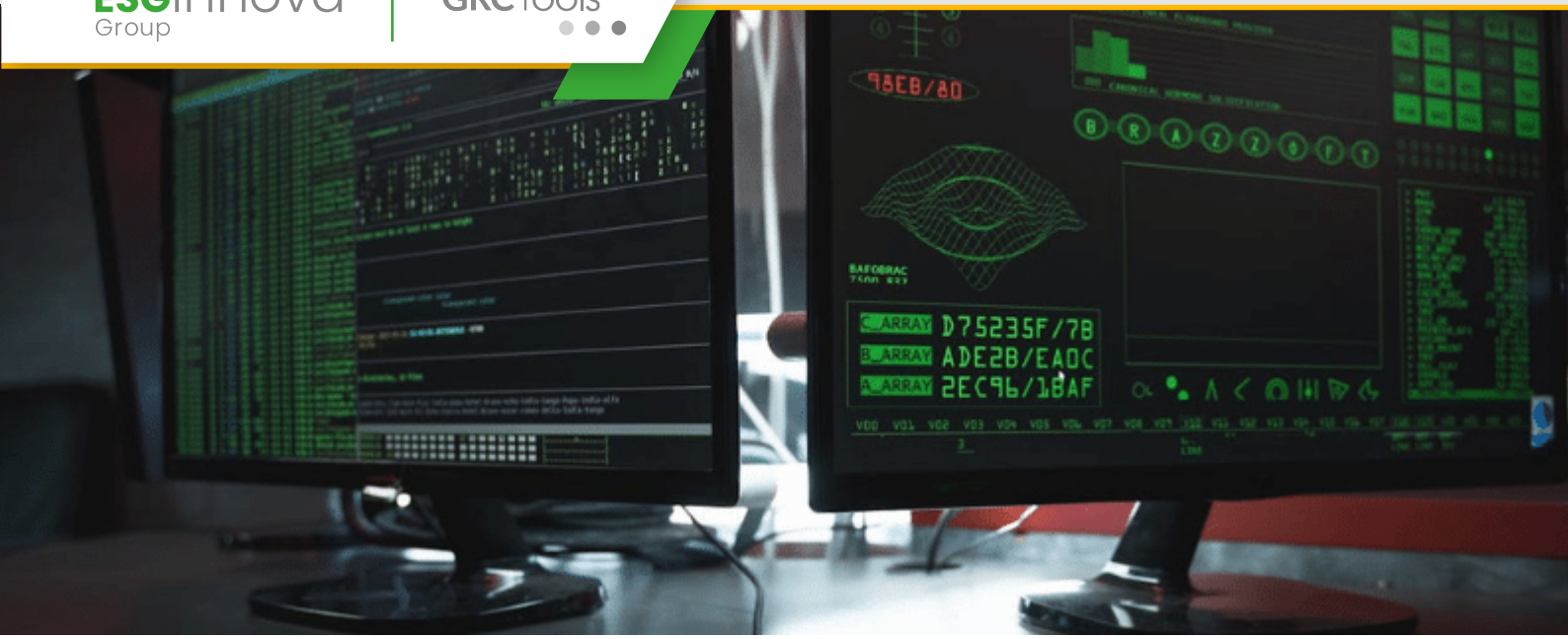
Los métodos tradicionales se basan en herramientas como hojas de cálculo, documentos compartidos y correos electrónicos para la identificación, evaluación y mitigación de riesgos. Si bien estas prácticas han sido utilizadas durante décadas, presentan desafíos importantes en un entorno empresarial cada vez más dinámico.

Ventajas de los métodos tradicionales:

- **Bajo costo inicial:** No requieren inversión en herramientas especializadas.
- **Flexibilidad inicial:** Las hojas de cálculo y documentos son personalizables según las necesidades de la empresa.
- **Familiaridad:** La mayoría de los empleados están acostumbrados a estas herramientas básicas.

Limitaciones de los métodos tradicionales:

- Alta propensión a errores humanos, ya que los datos son ingresados y gestionados manualmente.
- Falta de escalabilidad, lo que dificulta su uso en empresas grandes o con procesos complejos.
- Procesos lentos y manuales que consumen tiempo valioso del personal.
- Falta de integración, lo que genera una visión fragmentada de los riesgos en la organización.



Gestión de riesgos de ciberseguridad: clave para proteger tu empresa

En un mundo cada vez más conectado, las amenazas digitales no dejan de evolucionar, poniendo en riesgo la información, los sistemas y la reputación de las empresas. La **gestión de riesgos de ciberseguridad** se ha convertido en una prioridad estratégica para cualquier organización que quiera protegerse frente a ataques y minimizar el impacto de posibles incidentes.

En este artículo, exploraremos qué implica la gestión de riesgos de ciberseguridad, por qué es esencial para la continuidad del negocio y cómo implementar un enfoque eficaz para proteger tu empresa frente a estas amenazas.

¿Qué son los riesgos de ciberseguridad?

Los riesgos de ciberseguridad son aquellas amenazas que pueden comprometer la confidencialidad, integridad y disponibilidad de los datos y sistemas de una empresa.

Estas amenazas pueden originarse desde actores maliciosos externos, como hackers o grupos organizados, hasta errores humanos internos, como fallos en los procedimientos o falta de formación adecuada.

Ejemplos comunes de riesgos de ciberseguridad:

- Ataques de ransomware: Bloqueo de datos críticos de la empresa a cambio de un rescate.
- Phishing: Robo de credenciales a través de correos electrónicos o mensajes fraudulentos.
- Exfiltración de datos: Acceso no autorizado a información confidencial.
- Vulnerabilidades en software: Brechas de seguridad en sistemas o aplicaciones que pueden ser explotadas.
- DDoS (ataques de denegación de servicio): Saturación de servidores para interrumpir servicios críticos.

Estos riesgos pueden tener consecuencias devastadoras, desde pérdidas económicas hasta daños irreparables en la reputación de la organización.

La importancia de gestionar los riesgos de ciberseguridad

La gestión de riesgos de ciberseguridad no se limita a reaccionar ante incidentes; se trata de prevenir, mitigar y estar preparados para cualquier eventualidad. Un enfoque proactivo permite identificar amenazas antes de que se materialicen, minimizando los impactos en las operaciones de la empresa.

Marco de Riesgo NIST: Estrategias para una Protección Efectiva

El **Marco de Riesgo NIST** (National Institute of Standards and Technology Risk Management Framework) es un conjunto de lineamientos desarrollado por el Instituto Nacional de Estándares y Tecnología de los Estados Unidos, **diseñado para ayudar a las organizaciones a gestionar los riesgos** en la **seguridad de la información** de manera **estructurada** y **eficiente**. Este marco proporciona una **metodología flexible y adaptable** para **identificar, evaluar y gestionar los riesgos**, permitiendo a las organizaciones **proteger sus activos y datos críticos** ante amenazas cibernéticas en constante evolución.

A continuación, detallamos los **componentes y etapas** principales del Marco de Riesgo NIST, así como estrategias prácticas para su implementación y adaptación a las necesidades específicas de cada organización.

Marco de Riesgo NIST

El **Marco de Riesgo NIST** es una estructura que ayuda a las organizaciones a **abordar los riesgos de seguridad en la información** mediante un enfoque de **gestión de riesgos integral**. Este marco, originalmente diseñado para entidades del gobierno de los Estados Unidos, se ha convertido en un estándar para el sector privado gracias a su **enfoque exhaustivo y adaptable**.

El **objetivo** principal de este marco es ayudar a las organizaciones a:

- **Identificar y evaluar riesgos** relacionados con la seguridad de la información.
- Implementar **controles** efectivos que mitiguen estos riesgos.
- Asegurar el **cumplimiento regulatorio** en sectores críticos.
- Facilitar la **mejora continua** de la seguridad a través de revisiones periódicas.

La implementación del Marco de Riesgo NIST permite a las organizaciones **reducir** su exposición a **amenazas cibernéticas**, asegurar la **confidencialidad, integridad y disponibilidad** de los datos y **generar confianza** entre clientes y partes interesadas.

Componentes del Marco de Riesgo NIST

El **Marco de Riesgo NIST** se compone de seis fases clave, cada una de las cuales contribuye a una **gestión integral de los riesgos de seguridad**. A continuación, se detallan cada una de estas fases y su relevancia para la protección efectiva de los sistemas de información.

Software GRC y Ciberseguridad: Protegiendo tu Empresa Digitalmente

Con le evolución vertiginosa de la transformación digital, la **ciberseguridad** y la gestión de riesgos han pasado de ser un valor añadido a una necesidad crítica para las empresas. Con los datos convertidos en el activo más valioso, las organizaciones enfrentan amenazas cibernéticas más sofisticadas, regulaciones más estrictas y la presión de garantizar la continuidad del negocio. Para paliar esta situación se crea el **Software GRC**, aliado estratégico que revoluciona la protección empresarial.

Software GRC

Hoy en día, las empresas operan en un entorno digital donde el panorama de amenazas evoluciona constantemente. Ataques de ransomware, robo de datos y vulnerabilidades en la cadena de suministro digital son solo algunos ejemplos.

Además, normativas como el **Reglamento General de Protección de Datos (GDPR)**, **ISO/IEC 27001**, o la **Ley Sarbanes-Oxley (SOX)** obligan a las empresas a adoptar estándares de seguridad rigurosos. El desafío no es solo mitigar riesgos, sino también garantizar el cumplimiento normativo de manera eficiente y sostenible.

El rol transformador del Software GRC en ciberseguridad

El **Software de Gobierno, Riesgo y Cumplimiento**, centraliza la gestión de riesgos, y también fortalece la postura de ciberseguridad empresarial al integrar controles específicos en cada área organizacional. Su implementación garantiza una estrategia proactiva frente a amenazas y una alineación con los objetivos de negocio.

¿Cómo contribuye a la ciberseguridad el Software GRC?

- **Automatización del cumplimiento normativo:** Elimina tareas manuales y asegura que las políticas estén actualizadas frente a las últimas regulaciones.
- **Gestión integral de riesgos:** Detecta, evalúa y prioriza riesgos cibernéticos para proteger los activos más críticos de la organización.
- **Auditorías en tiempo real:** Proporciona herramientas para monitorizar continuamente el cumplimiento de los estándares de seguridad.
- **Planes de respuesta a incidentes:** Mejora la capacidad de recuperación con protocolos estandarizados y actualizados frente a ciberataques.

Principales riesgos laborales y cómo prevenirlos en tu empresa

La **identificación y gestión** de los **riesgos laborales** es una práctica fundamental para cualquier organización que desee **proteger a sus empleados** y **promover un ambiente de trabajo seguro**. Los riesgos laborales abarcan todas aquellas **condiciones o situaciones que pueden provocar accidentes, enfermedades o cualquier tipo de perjuicio físico o psicológico** en el entorno laboral. En este artículo, analizaremos los principales **tipos de riesgos laborales** y proporcionaremos **estrategias prácticas** para prevenirlos, con el fin de **minimizar el impacto** en los empleados y en la **productividad** de la empresa.

Riesgos laborales

Los **riesgos laborales** son **situaciones o factores** presentes en el ambiente de trabajo **que pueden afectar negativamente la salud, seguridad o bienestar de los empleados.**

Estos riesgos pueden estar relacionados con el espacio físico, los equipos de trabajo, la organización de las tareas o incluso con factores psicosociales, como el estrés.

Una gestión efectiva de los riesgos laborales implica:

- **Identificación y evaluación de riesgos** en cada área de trabajo.
- Implementación de **medidas preventivas** para reducir la exposición a riesgos.
- **Formación y concienciación** de los empleados sobre prácticas seguras.

Una organización que se esfuerza en la prevención de riesgos no solo **cuida de su equipo**, sino que también **reduce costos asociados** a accidentes y **fortalece su reputación** como un lugar seguro para trabajar.

Principales tipos de riesgos laborales

Los riesgos laborales se dividen en varias categorías según sus **características** y **efectos** en los trabajadores. A continuación, exploramos los tipos más comunes de riesgos en el entorno laboral.

1. Riesgos físicos

Los **riesgos físicos** son aquellos derivados de **factores ambientales** que pueden causar **lesiones en los trabajadores**. Estos riesgos son comunes en sectores como la construcción, la manufactura y en espacios de trabajo con condiciones específicas.

Cómo el software GRC reduce la evaluación de riesgos en tiempo real

La **gestión integral de riesgos** es un pilar fundamental para cualquier empresa que desee proteger sus activos, cumplir con normativas y optimizar sus operaciones. Sin embargo, los métodos tradicionales para evaluar riesgos suelen ser lentos, manuales y propensos a errores, lo que dificulta la respuesta ágil ante amenazas emergentes. Aquí es donde el **software GRC** (Governance, Risk, and Compliance) se convierte en una herramienta clave, al simplificar la evaluación de riesgos en tiempo real y proporcionar una visión integral y automatizada de la situación de la empresa.

En este artículo, exploramos cómo el **software GRC** revoluciona la forma en que las organizaciones evalúan riesgos, las ventajas que ofrece y por qué es esencial en el entorno empresarial actual.

Desafíos de la evaluación de riesgos con métodos tradicionales

La evaluación de riesgos es un proceso crítico, pero cuando se realiza mediante métodos manuales como hojas de cálculo o documentos independientes, puede volverse un desafío operativo. Algunos de los principales problemas que enfrentan las empresas incluyen:

- Procesos lentos y manuales que dificultan la identificación rápida de amenazas.
- Falta de visibilidad integral sobre los riesgos en diferentes áreas de la empresa.
- Datos desactualizados, lo que genera evaluaciones imprecisas y decisiones erróneas.
- Alta propensión a errores humanos, especialmente en la recopilación y análisis de datos.

En un entorno donde los riesgos evolucionan rápidamente, estos métodos no son suficientes para garantizar la protección y continuidad del negocio.

¿Cómo simplifica el software GRC la evaluación de riesgos en tiempo real?

El software GRC está diseñado para optimizar y centralizar la gestión de riesgos, eliminando las limitaciones de los métodos tradicionales.

Con esta herramienta, las empresas pueden realizar evaluaciones en tiempo real y tomar decisiones rápidas e informadas basadas en datos precisos y actualizados.

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO

Prevención de riesgos laborales: seguridad vial en el trabajo

La seguridad vial en el entorno laboral es un aspecto crucial dentro de la **gestión de riesgos laborales**, especialmente para las empresas cuyos empleados deben desplazarse regularmente por motivos laborales. Los accidentes de tráfico, tanto en desplazamientos in itinere como en misión, representan una de las principales causas de siniestralidad laboral.

Garantizar la seguridad vial no solo protege a los trabajadores, sino que también reduce costos, mejora la productividad y refuerza la reputación de la empresa.

¿Qué son los riesgos laborales relacionados con la seguridad vial?

Los riesgos laborales asociados a la seguridad vial incluyen cualquier situación que pueda derivar en accidentes durante los desplazamientos laborales.

Estos riesgos pueden estar relacionados con factores como:

- La planificación inadecuada de rutas y horarios.
- El mantenimiento deficiente de los vehículos.
- La falta de capacitación en conducción segura.
- Factores externos como el clima, el estado de las vías o el tráfico.

Además de los impactos físicos y emocionales para los empleados, estos riesgos generan costos económicos significativos para las empresas, incluyendo gastos médicos, reparaciones y pérdida de productividad.

¿Cómo ayuda GRCTools en la gestión de riesgos viales?

GRCTools proporciona soluciones avanzadas para gestionar los riesgos laborales, incluidas herramientas específicas para garantizar la seguridad vial. Su plataforma permite a las empresas abordar este desafío mediante un enfoque integral, eficiente y adaptado a las necesidades de cada organización.

Identificación y evaluación de riesgos

La plataforma de GRCTools permite identificar y evaluar los riesgos relacionados con la seguridad vial. Esto incluye analizar rutas habituales, identificar puntos críticos en los desplazamientos y evaluar la capacitación de los empleados en conducción segura. Con esta información, las empresas pueden diseñar estrategias proactivas para mitigar los riesgos más significativos.

Certificación TISAX: ¿Qué es y cómo afecta a proveedores y empresas automotrices?

En la industria automotriz, donde la innovación y la tecnología avanzan a pasos agigantados, la protección de la información se ha convertido en una prioridad estratégica. Para abordar esta necesidad, nace la certificación **TISAX** (Trusted Information Security Assessment Exchange), un estándar diseñado específicamente para garantizar la **seguridad de la información** en la cadena de suministro automotriz.

Pero seguro que te quedan muchas dudas al respecto, por ello vamos a abordar qué es TISAX, cómo afecta a las empresas del sector y como herramientas especializadas como el **Software de Ciberseguridad** pueden facilitar la adopción de este estándar.

Certificación TISAX

La certificación TISAX fue desarrollada por la Asociación Alemana de la Industria Automotriz (**VDA**) para satisfacer los crecientes

requerimientos de confidencialidad, integridad y disponibilidad de la información en el sector automotriz.

Se basa en los principios de la norma **ISO/IEC 27001**, pero está adaptada a las necesidades específicas de esta industria, incluyendo aspectos únicos como:

- La **protección de prototipos** y diseños confidenciales.
- La seguridad en el **intercambio de información sensible** entre fabricantes y proveedores.
- La garantía de un nivel de protección uniforme en toda la cadena de suministro.

¿Cómo funciona TISAX?

TISAX no solo evalúa la seguridad de la información, sino que también permite compartir los resultados con otros socios comerciales a través de su plataforma de intercambio, conocida como **TISAX Exchange**. Este proceso incluye:

01. **Autoevaluación inicial:** Las empresas identifican sus necesidades de seguridad según los datos que manejan.
02. **Auditoría externa:** Organismos acreditados evalúan la implementación de las medidas de seguridad necesarias.
03. **Intercambio de resultados:** Los resultados de la auditoría se suben a TISAX Exchange, donde las empresas autorizadas pueden consultarlos, ahorrando tiempo y costos.

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO

¿Qué es el compliance? Cómo prevenir riesgos normativos en tu negocio

En un entorno de negocios cada vez más **regulado y globalizado**, las empresas enfrentan la creciente necesidad de asegurar que sus operaciones se **ajusten a las normativas locales e internacionales**. Esto ha llevado a que el concepto de **compliance** cobre una importancia crítica, ya que representa un conjunto de prácticas que permiten a las organizaciones **cumplir con las leyes y regulaciones** aplicables a sus actividades. El cumplimiento normativo o compliance ayuda a **mitigar** los **riesgos normativos**, **protegiendo** a las empresas de **sanciones legales**, **pérdidas financieras** y **daños** a su **reputación**.

En este artículo, exploraremos el concepto de compliance, el **impacto de los riesgos** normativos en las organizaciones y las **estrategias clave** para prevenirlos de forma efectiva.

Riesgos normativos

Los **riesgos normativos** son los riesgos que enfrenta una organización debido a **incumplimientos de leyes, normas y regulaciones**. Estos riesgos pueden derivar en sanciones legales, multas, demandas o incluso en la suspensión de actividades comerciales.

- El **incumplimiento** de las normativas aplicables puede tener **efectos significativos** en una organización, tales como:

- **Sanciones financieras**: Las multas impuestas por las autoridades regulatorias pueden ser cuantiosas y afectar la viabilidad económica de la empresa.

- **Daños a la reputación**: El incumplimiento puede deteriorar la imagen de la empresa ante clientes, inversores y socios comerciales.

- **Pérdida de licencias o permisos**: En algunos sectores, el incumplimiento puede llevar a la suspensión de permisos esenciales para operar.

- **Problemas legales**: Los riesgos normativos pueden desencadenar demandas legales y procesos judiciales que generen pérdidas de tiempo y recursos.

- La gestión de los riesgos normativos permite **minimizar estas consecuencias** y asegurar que la empresa **opere de manera ética y responsable**.

¿Qué características debe tener un buen Software GRC?

Imagina una **orquesta sinfónica**: cada instrumento debe estar en perfecta sintonía para crear una melodía armoniosa. Ahora, piensa en una organización enfrentando desafíos complejos: el **gobierno corporativo**, la **gestión de riesgos** y el **cumplimiento normativo** son como los diferentes instrumentos que necesitan trabajar juntos para lograr el éxito.

En este contexto, un **software GRC** actúa como el **director de orquesta**, asegurando que cada elemento esté alineado y funcionando de manera óptima. Sin embargo, no todos los directores (o software) son iguales. Para que una organización alcance la **excelencia operativa**, es fundamental elegir una solución que reúna las **características necesarias** para orquestar todos estos procesos de manera eficaz.

Software GRC

En este artículo, exploraremos las claves que definen un **buen software GRC** y cómo **GRCTools** puede convertirse en ese

director que lleva a las empresas a gestionar sus operaciones con **precisión**, **innovación** y **eficiencia**.

1. Centralización e integración de procesos

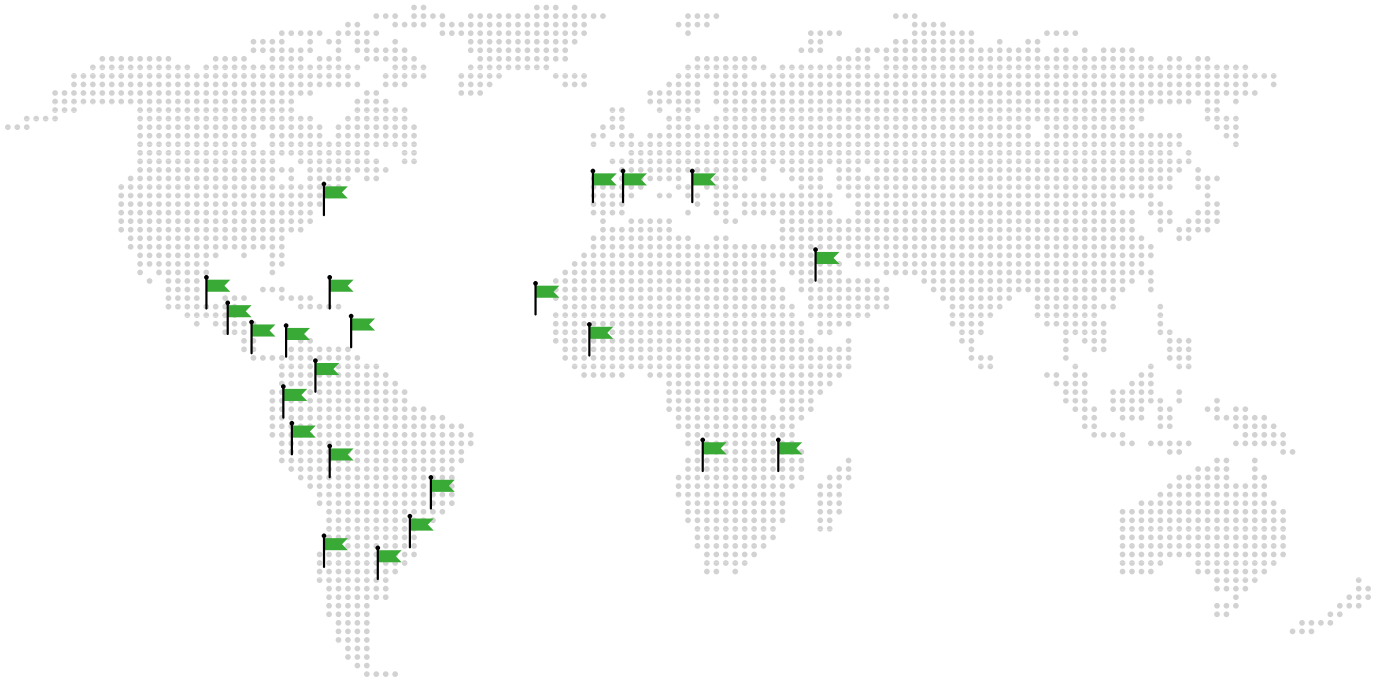
Un buen software GRC debe integrar todas las áreas relacionadas con gobierno, riesgos y cumplimiento en una **única plataforma**. Esto no solo simplifica la gestión, sino que también reduce los silos organizacionales, mejorando la comunicación y la colaboración entre departamentos.

Con **GRCTools**, las empresas pueden centralizar la administración de políticas, controles, riesgos y auditorías, asegurando una visión holística y en tiempo real de su desempeño.

2. Automatización y eficiencia operativa

La automatización de procesos es clave para reducir errores humanos y mejorar la eficiencia. Un software GRC efectivo debe permitir la automatización de tareas como:

- **Identificación y evaluación de riesgos.**
- **Generación de reportes de cumplimiento.**
- **Seguimiento de acciones correctivas.**



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, 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

México DF, México

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