EMPRESA **EXCELENTE**

Las mejores temáticas sobre Normas ISO, HSE y GRC

2024

OCTUBRE

ESGinnova Group

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

Índice

Índice

ESG Innova Group

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

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

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

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

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

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

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

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

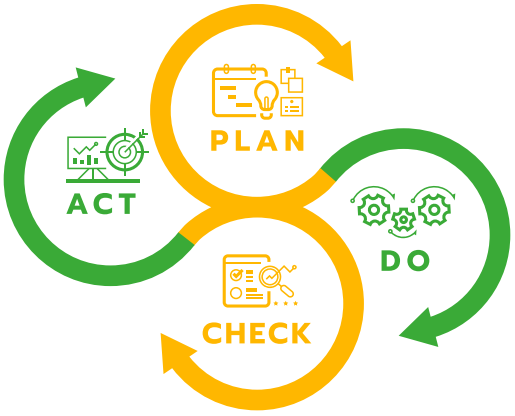
Plataforma ESG Innova

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

❖ Motor de mejora continua

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

ESGinnova Group



❖ Plan

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

❖ Do

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

❖ Check

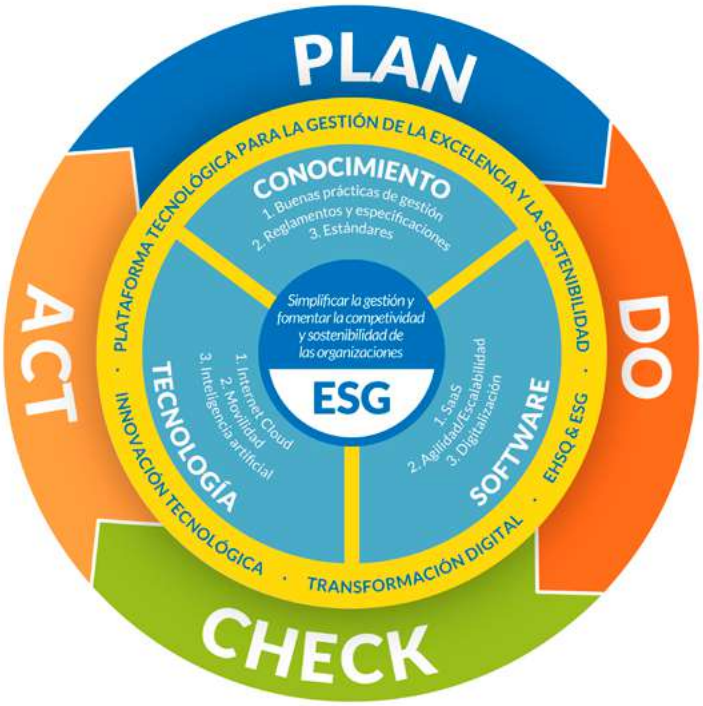
Simplificamos la monitorización y seguimiento, aportando información útil para la toma de decisiones.

❖ Act

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

Unidades de negocio

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



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

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

Unidades de negocio

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

ISOTools

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

HSETools

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

GRCTools

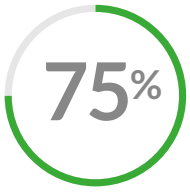
Transformación Digital para la gestión de Gobierno, Riesgo y Cumplimiento.

La Plataforma ESG aporta resultados en el corto plazo

Optimización del tiempo

Menos de tiempo de resolución de una acción correctiva

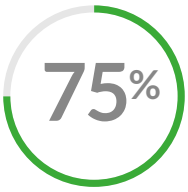
Menos de tiempo de preparación de las reuniones de gestión



Menos de tiempo dedicado a recopilar y tratar indicadores

Optimización de los costes

Menos de intercambios de documentación física entre sedes y dptos.



Menos de costes indirectos derivados de la gestión documental

La inversión se rentabiliza entre el primer y el segundo año

Optimización del rendimiento

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

Más capacidad de resolución de problemas del sistema de gestión

Más de trabajadores implicados en la gestión del sistema

ESGinnova Group

ISOTools

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

ISO 45001 Requisitos para Implementar un Sistema de Gestión de SST

ISO 45001 requisitos

La ISO 45001 establece el marco para implementar un sistema de gestión de seguridad y salud en el trabajo (SG-SST). El principal objetivo de este estándar es la mejora de la seguridad laboral en las empresas, al reducir riesgos y crear así unas condiciones de trabajo seguras y saludables para todos. En este post, vamos a analizar los **requisitos de ISO 45001** y cómo implementarlos de manera eficaz en tu empresa.

La norma ISO 45001 tiene una estructura de diez secciones. A continuación, se describen las más relevantes para la implementación de un **sistema de gestión de Seguridad y Salud en el Trabajo:**

1. Contexto de la organización

Toda organización debe y tiene que **entender su contexto tanto interno como externo**. Esto incluye la identificación de stakeholders o partes interesadas, sus expectativas, y los riesgos y oportunidades que pueden afectar a un sistema de gestión de Seguridad y Salud en el Trabajo.

2. Liderazgo y participación de los trabajadores

El **compromiso de la alta dirección** es muy importante. La norma ISO 45001 exige que los líderes empresariales que demuestren su compromiso con la gestión de la Seguridad y Salud en el Trabajo. Para ello deben proporcionar los recursos que sean necesarios y fomentar la participación activa de todos los trabajadores en el sistema de gestión SST.

3. Planificación

La planificación lleva aparejada la **identificación de riesgos y oportunidades en relación con la seguridad y salud de los empleados**. En esta línea se deben realizar evaluaciones de riesgos, determinar los objetivos de la Seguridad y Salud en el Trabajo y cómo se van a alcanzar.

4. Apoyo

La norma ISO 45001 pone énfasis en el papel que juega el **apoyo empresarial,** que va desde la disponibilidad de recursos, la formación y sensibilización en materia de seguridad y salud en el trabajo.

Cómo decidir si certificar ISO 42001 es la opción adecuada para tu organización

Los beneficios implícitos y evidentes suelen ser el argumento más efectivo para tomar la decisión de **certificar ISO 42001** en una organización. La certificación del estándar sobre **Gestión de Sistemas de Inteligencia Artificial** no es requisito legal o regulatorio, por lo menos, no lo es de forma explícita y directa.

Esa es, entre otras razones, la que lleva la Alta Dirección de muchas organizaciones a solicitar **argumentos convincentes para tomar la decisión de certificar ISO 42001**. Esos argumentos existen y son contundentes, los desglosamos a continuación.

Por qué decidir certificar ISO 42001

Certificar ISO 42001 es la mejor opción para una organización que utiliza o desarrolla aplicaciones, productos o funcionalidades de Inteligencia Artificial. Una primera gran razón es que el **sistema de gestión basado en la norma** entrega una estructura habilitada

para **respaldar los objetivos estratégicos y operativos, de forma segura, de una organización** que utiliza o desarrolla productos de IA. Pero este es un argumento muy general, hay otros más específicos:

1. Garantiza el uso seguro, legal, ético y responsable de IA

No existe una regulación, una directiva o una ley que obligue a implementar **sistemas de gestión para el uso IA**, ni a certificar ISO 42001. Pero es importante entender que **los aspectos legales, éticos y de responsabilidad social sí son obligaciones de cumplimiento** para todas las organizaciones.

Implementar el sistema de gestión garantiza el cumplimiento de los aspectos legales, regulatorios y éticos, pero **certificar ISO 42001 hace que la organización cuente con una prueba indiscutible** de que eso es así.

2. Mejora el cumplimiento regulatorio en otras áreas

Muchas organizaciones, en especial las que operan en Europa, están sujetas a **obligaciones regulatorias estrictas**. Si La industria o el mercado son altamente regulados, las exigencias aumentan.

ISO 42001 ayuda a mejorar las opciones de cumplimiento de una organización, alineando estos esfuerzos con la estrategia comercial y con los **estándares de cumplimiento internacionales**. Por supuesto, la certificación ISO 42001 es la forma de comprobarlo en cualquier lugar del mundo.

¿Cuál es el rol de las partes interesadas ISO 45001?

Partes interesadas ISO 45001

La **ISO 45001** es la norma internacional que establece los requisitos para implementar un sistema de gestión de **Seguridad y Salud en el Trabajo (SST)**. Su objetivo principal es prevenir accidentes laborales y mejorar la seguridad en el lugar de trabajo. Sin embargo, ¿sabías que uno de los factores clave para que un sistema de gestión sea efectivo es la **involucración de las partes interesadas**?

¿Qué son las partes interesadas en ISO 45001?

Las **partes interesadas** son todas aquellas personas u organizaciones que pueden influir o verse afectadas por las decisiones y actividades relacionadas con la gestión de la seguridad y salud en el trabajo de una organización. En la ISO 45001, las partes interesadas incluyen:

- **Empleados y representantes**: Su seguridad es la prioridad del sistema de gestión.

- **Proveedores y contratistas**: Su cumplimiento con los estándares de SST impacta directamente en la seguridad de las operaciones.

- **Entidades reguladoras**: Aseguran que la empresa cumpla con las normativas de seguridad y salud.

- **Clientes y comunidad local**: Sus expectativas pueden incluir la gestión segura y responsable de los riesgos operativos.

La importancia de las partes interesadas en ISO 45001

Involucrar a las partes interesadas no es solo un requisito formal de la norma. Su participación activa es crucial para lograr un **sistema de gestión de SST eficaz y sostenible**. Algunas razones clave por las que las partes interesadas son fundamentales en la implementación de la ISO 45001 incluyen:

01. **Detección temprana de riesgos**: Los empleados, por ejemplo, están directamente expuestos a las condiciones de trabajo diarias. Su conocimiento y experiencia permiten identificar **riesgos y peligros** que podrían pasar desapercibidos para la alta dirección. La consulta y participación de los trabajadores es esencial para detectar riesgos antes de que se conviertan en problemas graves.

02. **Mejora continua del sistema de gestión**: La ISO 45001 enfatiza la **mejora continua** del sistema de gestión de SST. Las partes interesadas proporcionan una fuente constante de retroalimentación que impulsa esta mejora. ¿Quién mejor que los empleados o contratistas para sugerir formas de hacer el entorno laboral más seguro?

7 dimensiones del Modelo Integrado de Planeación y Gestión

El Modelo Integrado de Planeación y Gestión (MIPG) es una solución que abarca siete dimensiones: **planeación estratégica**, gestión de recursos, monitoreo y evaluación, gestión del riesgo, mejora continua, participación y colaboración, y comunicación efectiva. Estas siete dimensiones alinean la estrategia con la ejecución y fomentan una cultura de adaptación y aprendizaje continuo, esencial para el éxito y la sostenibilidad de la organización.

Modelo Integrado de Planeación y Gestión

En el entorno empresarial actual, la capacidad para adaptarse a los cambios y gestionar eficazmente los recursos es muy importante para el **éxito empresarial**. El Modelo Integrado de Planeación y Gestión es una herramienta para lograr una gestión eficiente y alineada con los objetivos estratégicos. A continuación, se explican las siete dimensiones del MIPG y su importancia en la gestión de la organización.

1. Planeación Estratégica

La planeación estratégica establece el rumbo que debe seguir la empresa. A través de un análisis exhaustivo del entorno interno y externo, se definen metas y objetivos para guiar las acciones en el futuro. Esta dimensión garantiza que todos los esfuerzos estén **alineados con la visión a largo plazo de la empresa.**

2. Gestión de Recursos

La gestión eficiente de los **recursos humanos** y materiales es crucial para maximizar la productividad. Esta dimensión del MIPG se centra en asignar recursos, capacitar al personal y optimizar los procesos, asegurando que la empresa opere de forma sostenible y efectiva.

3. Monitoreo y Evaluación con el Modelo Integrado de Planeación y Gestión

Para garantizar el éxito de la planificación, es necesario establecer mecanismos para monitorear y evaluar. Esta dimensión del MIPG realiza un **seguimiento continuo de los avances y resultados**, facilitando la identificación de desviaciones y la implementación de medidas correctivas si es necesario.

4. Gestión del Riesgo

Identificar y **gestionar el riesgo** son componentes esenciales del Modelo Integrado de Planeación y Gestión. Las empresas tienen que ser capaces de **anticipar y mitigar posibles riesgos que puedan afectarles**. Esto implica hacer análisis de riesgos y desarrollar estrategias ante posibles situaciones adversas.

10 Pasos Cruciales para la Implementación Exitosa de ISO 14001

La **ISO 14001** es la norma internacional más reconocida para la implementación de un **Sistema de Gestión Ambiental (SGA)**. Adoptar esta norma permite a las empresas mejorar su desempeño ambiental, cumplir con las regulaciones y demostrar un compromiso con la sostenibilidad. A continuación, se describen los **10 pasos cruciales** para una **implementación exitosa** de **ISO 14001**.

10 Pasos para la Implementación Exitosa de ISO 14001

1. Compromiso de la alta dirección

El **compromiso de la alta dirección** es esencial para el éxito en la implementación de ISO 14001. Los líderes deben asignar los **recursos necesarios** y definir claramente los **objetivos ambientales** de la empresa. Además, es crucial que la alta dirección se involucre activamente para garantizar que el sistema de gestión ambiental se alinee con la estrategia corporativa.

2. Realizar un análisis inicial

Antes de comenzar, es importante realizar un **análisis inicial** para evaluar la situación actual de la empresa en términos de **cumplimiento ambiental**. Este análisis identifica las **áreas críticas** que requieren mejora, los impactos ambientales más significativos y las **oportunidades de mejora**.

3. Establecer una política ambiental para la Implementación Exitosa de ISO 14001

La empresa debe establecer una **política ambiental** que refleje sus compromisos de protección del medio ambiente, cumplimiento de la legislación aplicable y mejora continua. Esta política debe ser clara, estar comunicada a todos los niveles de la organización y ser revisada periódicamente.

4. Identificación de aspectos ambientales

Un paso clave es la **identificación de aspectos ambientales**, es decir, las actividades, productos y servicios que pueden tener un **impacto** en el medio ambiente. Se deben evaluar estos aspectos para priorizar las acciones correctivas o preventivas.

5. Definir objetivos y metas

Los **objetivos ambientales** deben estar alineados con la política ambiental de la organización. Estos objetivos deben ser **específicos, medibles, alcanzables, realistas y limitados en el tiempo** (SMART), lo que permitirá un seguimiento efectivo y garantizará la mejora continua del desempeño ambiental.

Cómo implementar la norma ISO 27001: consejos de expertos

La Seguridad de la Información es una gran preocupación a nivel global. Por ello, **implementar la norma ISO 27001** es un propósito que se han planteado muchas organizaciones. Algunas lo han conseguido ya, otras avanzan en el proyecto o están a la espera de la **certificación del estándar de seguridad de a información**.

Implementar la norma ISO 27001 **es un proyecto que requiere trabajo, planificación y una buena dosis de sentido común.** Para las organizaciones que han encontrado alguna dificultad en el proceso, una guía corta, pero precisa, ayudará a avanzar en todo lo relacionado con la planificación del proyecto.

Cómo implementar la norma ISO 27001

El primer paso para implementar la norma ISO 27001 **es realizar el análisis de brechas o análisis GAP**.

Esta evaluación permite establecer en qué estado se encuentra la Gestión de Seguridad de la Información, en qué puntos se alcanza conformidad con los requisitos de la norma y qué falta para llegar al **cumplimiento de los requisitos de ISO 27001**.

El análisis GAP es un buen punto de partida para organizaciones que ya han adoptado algún estándar de Seguridad de la Información, que tienen un departamento dedicado al área o que han implementado medidas para proteger su información.

Aquellas que no cumplan estos requisitos pueden **ahorrar recursos iniciando directamente el proceso** para implementar la norma ISO 27001, que pasa por las siguientes fases:

1. Presentar el proyecto a la Alta Dirección

Antes de invertir tiempo, recursos y esfuerzos, conviene saber si la Alta Dirección apoyará o no el proyecto. Obtener el aval exige la presentación de **beneficios**, **valor y retorno de la inversión y tiempo necesario** para la implementación la norma ISO 27001. Esta es la información que necesita la Alta Dirección para decidir.

2. Planificar la implementación con base en el ciclo PDCA

La planificación es un factor determinante para el éxito del proyecto. Las expectativas aumentan si se utiliza, desde el inicio, el ciclo PDCA. Es natural: **los estándares ISO se basan en esta metodología**, que es la que proporciona la capacidad para mejorar de forma continua, uno de los componentes clave del estándar **ISO 27001**.

ISO 45003: ¿Qué es, qué tiene que ver con la salud mental y por qué es tan importante su publicación?

El **bienestar de los empleados** se ha convertido en un tema central para las organizaciones, y cada vez toma más relevancia gracias al movimiento social que se genera en torno a esta temática. Una corriente que se está abriendo paso dentro de esta problemática es la **salud mental**. Más allá de la seguridad física, los empleadores también están comenzando a reconocer la psicología como un pilar clave para el **éxito** y la **productividad**.

En este contexto, la **ISO 45003** ha sido una de las publicaciones más relevantes de los últimos años. Pero, ¿qué es exactamente ISO 45003? ¿Por qué tiene tanta relevancia en el ámbito de la salud mental y la seguridad laboral? Vamos a explorarlo.

ISO 45003

La **ISO 45003:2021** es la primera norma internacional que proporciona directrices específicas para la gestión de **riesgos psicosociales** en el lugar de trabajo. Es una extensión de la **ISO 45001**, que se centra en la gestión de la seguridad y salud en el trabajo (SST). Mientras que la ISO 45001 abarca los aspectos físicos, la ISO 45003 pone el foco en los **riesgos psicosociales**, aquellos factores que afectan el bienestar mental, emocional y social de los empleados.

Estos riesgos pueden incluir:

- **Estrés laboral**.
- **Ambientes de trabajo tóxicos**.
- **Acoso o intimidación**.
- **Exceso de carga de trabajo o expectativas poco claras**.

La norma ISO 45003 proporciona una guía clara para identificar estos factores, evaluarlos y, lo más importante, **gestionar los riesgos** para proteger a los empleados.

¿Qué tiene que ver ISO 45003 con la salud mental?

El bienestar mental en el trabajo ha pasado de ser un tema de conversación a una **prioridad estratégica**. Los empleados expuestos a riesgos psicosociales sin una gestión adecuada son más propensos a sufrir problemas de **estrés crónico**, **ansiedad**, **depresión**, e incluso **burnout**. Esto afecta directamente a su productividad, y también su calidad de vida.

¿Qué es la norma ISO 45003?

La **ISO 45003** es la primera norma internacional que ofrece directrices para gestionar los **riesgos psicosociales** en el trabajo, complementando a la **ISO 45001** en la gestión de la **salud y seguridad laboral**. Esta norma proporciona un marco para **identificar, evaluar y prevenir riesgos** que afecten la salud mental y el bienestar emocional de los empleados. Su implementación es clave para crear un **ambiente de trabajo saludable**, donde el **estrés**, la **fatiga** y otros factores psicológicos sean gestionados de manera adecuada.

ISO 45003

La **ISO 45003** tiene como **objetivo principal proteger** la **salud mental** de los empleados, promoviendo el **bienestar emocional** y reduciendo el impacto de los factores estresantes en el lugar de trabajo. A diferencia de otras normas centradas en **riesgos físicos**, esta norma pone énfasis en la **prevención de riesgos psicosociales**, como el estrés laboral, la carga de trabajo excesiva y la falta de apoyo.

La **ISO 45003** también busca mejorar el **ambiente laboral**, fomentando un entorno positivo donde los empleados puedan desarrollarse profesionalmente sin que su bienestar se vea **comprometido**.

La norma promueve una **cultura organizacional** basada en el respeto, la seguridad emocional y la inclusión, lo que contribuye a una mayor **productividad** y **retención del talento**.

Beneficios de la implementación de la norma

Implementar la norma ISO 45003 sobre riesgos psicosociales, brinda múltiples **beneficios** como:

- **Reducción del estrés laboral**

Uno de los beneficios clave de la **ISO 45003** es la **reducción del estrés laboral**. Al identificar los factores que generan estrés en los empleados, las empresas pueden implementar medidas preventivas para **minimizar su impacto**, lo que a su vez mejora la **calidad de vida laboral** y reduce el **absentismo**.

- **Mejora del rendimiento y productividad**

Al gestionar de manera adecuada los riesgos psicosociales, las organizaciones experimentan un **aumento en la productividad**. Los empleados que trabajan en un ambiente que cuida de su bienestar emocional tienden a estar más **motivados**, ser más **creativos** y ofrecer un **mejor rendimiento**.

Esto no solo mejora la **eficiencia operativa**, sino que también reduce los costos asociados con la **rotación de personal**.

IEC62443: Fortaleciendo la Ciberseguridad en la Industria

La interconexión actual hace que la automatización y la tecnología operativa (OT) sean fundamentales para el funcionamiento de industrias críticas. Estas garantizan la **ciberseguridad**, una prioridad absoluta en este contexto.

IEC62443

La **norma IEC62443** es un marco diseñado específicamente para proteger los **sistemas de control industrial (ICS)**, ayudando a mitigar los riesgos cibernéticos en sectores como la energía, manufactura, petróleo y gas, entre otros.

Quédate con nosotros para explorar cómo **IEC 62443** fortalece la ciberseguridad industrial, qué pasos implica su implementación, y por qué es vital para proteger las infraestructuras críticas.

1. ¿Qué es la norma IEC62443?

La **IEC 62443** es un conjunto de estándares desarrollados por la Comisión Electrotécnica Internacional (IEC) que define los requisitos y mejores prácticas para garantizar la seguridad de los **sistemas de automatización y control industrial** (ICS). Este estándar abarca tanto aspectos técnicos como organizacionales, permitiendo a las empresas adoptar un enfoque integral frente a las **amenazas cibernéticas**.

¿Por qué es importante? Los ICS controlan procesos industriales clave y, si son vulnerados, podrían causar interrupciones operativas, pérdidas económicas significativas e, incluso, poner en riesgo la seguridad pública. Implementar la IEC 62443 ayuda a las empresas a minimizar esos riesgos.

2. Principios clave de la IEC 62443

2.1 Segmentación de redes: Zonas y Conduits

Uno de los pilares de la IEC 62443 es la **segmentación de las redes industriales**. Esto se logra dividiendo los sistemas en **zonas** según su criticidad y riesgos asociados, y conectándolas mediante **canales seguros** (conduits). Este enfoque asegura que un ataque en una zona no afecte a todo el sistema, limitando su impacto.

2.2 Enfoque basado en niveles de seguridad

La norma define varios **niveles de seguridad (Security Levels)** que se aplican según el riesgo y la exposición de cada sistema.

Anexo A en ISO 14001: qué es y cómo se utiliza

El **Anexo A en ISO 14001** es una novedad incorporada en la edición 2015 del estándar internacional para **Sistemas de Gestión Ambiental**. Este apéndice de la norma ha pasado, de cierta forma, inadvertido para muchas personas.

Algunas no saben cuál es su función exacta. Otras, por el contrario, la entienden muy bien, pero la consideran innecesaria. Lo cierto es que el Anexo A en ISO 14001 se diseñó e incluyó como parte integral del texto de la norma, pensando en que se convierta en **una herramienta eficaz para facilitar su comprensión** y evitar así la libre interpretación de los requisitos del estándar.

Por supuesto, un profesional en gestión ambiental puede trabajar en la implementación de un sistema basado en la norma prescindiendo del uso del Anexo A en ISO 14001. Seguro lo hará bien, pero si existe una ayuda que **permite avanzar con mayor seguridad**, ¿por qué no utilizarla?

Qué función cumple el Anexo A en ISO 14001

El Anexo A en ISO 14001 **es un documento que guarda una correspondencia exacta con la estructura de requisitos de la norma de gestión ambiental**. De esta manera, ofrece orientaciones y directrices útiles para la implementación, evitando así la posibilidad de que se asuman o interpreten de forma libre sus directrices. El objetivo es evitar errores u omisiones.

Un interesante ejemplo

El **capítulo 4 de la norma, en su cláusula 4.1**, **solicita a la organización identificar y comprender el contexto** (interno y externo) de la organización. Hasta ahí, no parece haber mayor problema, en especial tomando en cuenta que el contexto dentro de las normas ISO es algo de fácil comprensión y de uso común.

En el Anexo A en ISO 14001 **se encuentra la correspondiente cláusula A.4.1, titulada "comprensión del contexto de la organización".** En este texto se aclara que la intención de los redactores de la norma fue "permitir una comprensión conceptual de Alto Nivel sobre las cuestiones internas y externas que tienen la capacidad para afectar de forma negativa o positiva la forma en que la organización gestiona sus **aspectos e impactos ambientales**".

Es importante destacar en esta aclaración del Anexo A en ISO 14001 la expresión "Alto Nivel", **que denota un tratamiento diferente al que se asumiría si se prescinde de ella.** Esto es ya un aporte que marca una interesante diferencia.

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO

Riesgos desde el enfoque de la norma ISO 31000

La **norma ISO 31000** es el estándar internacional para la **gestión de riesgos** y proporciona un **enfoque estructurado y flexible** para identificar, evaluar y gestionar los riesgos que enfrentan las organizaciones. Este enfoque se aplica a todo tipo de organizaciones, independientemente de su tamaño, industria o ubicación, y tiene como objetivo mejorar la **toma de decisiones**, la **eficiencia operativa** y el **cumplimiento normativo**.

ISO 31000

La **ISO 31000** proporciona principios y **directrices** para la **gestión del riesgo**. Su objetivo es ayudar a las organizaciones a desarrollar un **enfoque proactivo** y **sistemático** para gestionar los riesgos que puedan amenazar sus **objetivos empresariales**. Esta norma no es prescriptiva, lo que significa que no impone soluciones específicas, sino que ofrece un marco que las organizaciones pueden **adaptar a sus necesidades particulares**.

La **ISO 31000** se basa en varios principios clave, entre ellos:

- **Integración**: La gestión de riesgos debe ser parte integral de todos los procesos organizacionales.
- **Personalización**: El enfoque debe adaptarse al entorno interno y externo de cada organización.
- **Mejora continua**: La gestión de riesgos debe ser un proceso dinámico y de mejora constante.

Estos principios aseguran que las organizaciones gestionen los riesgos de manera **eficaz y eficiente**, mejorando su **resiliencia** ante eventos inesperados.

Enfoque de la norma para la gestión de riesgos

Identificación de riesgos

El primer paso en la **gestión de riesgos** bajo la norma ISO 31000 es la **identificación de riesgos**. Esto implica detectar las **amenazas potenciales** que podrían impactar negativamente los **objetivos** de la organización. Este proceso incluye tanto **riesgos internos** (como fallos operativos) como **externos** (como fluctuaciones del mercado o desastres naturales).

La identificación temprana de los riesgos permite a las organizaciones **prepararse y mitigar** sus **efectos antes** de que se conviertan en un **problema**.

¿Qué es MIPG y para qué sirve?

El **Modelo Integrado de Planeación y Gestión (MIPG)** es una herramienta fundamental en el ámbito de la gestión pública en Colombia. Su implementación permite que las entidades públicas trabajen de manera articulada, eficiente y transparente, orientándose hacia el cumplimiento de los objetivos de desarrollo nacional y la satisfacción de las necesidades ciudadanas. Sin embargo, su impacto también se extiende al sector privado, donde una buena implementación de los principios de MIPG permite a las empresas alinear sus procesos de gestión y optimización de recursos.

MIPG

El MIPG es el modelo de gestión del **Gobierno de Colombia** que busca unificar y simplificar la forma en que las entidades públicas del país planean, gestionan y evalúan sus acciones. Surge para superar las limitaciones de modelos anteriores, estructurándose en un sistema integral que asegura el cumplimiento de los fines esenciales del Estado de manera eficiente y sostenible.

Este modelo articula **siete dimensiones clave**, cada una de ellas diseñada para cubrir aspectos fundamentales en la administración pública:

01. **Talento humano**: Enfocado en fortalecer la capacitación y el compromiso de los empleados públicos.

02. **Dirección y estrategia**: Orienta a las entidades para que sus objetivos estratégicos estén alineados con los planes nacionales de desarrollo.

03. **Gestión con valores para resultados**: Promueve una cultura de trabajo basada en la ética y la orientación hacia resultados.

04. **Evaluación de resultados**: Garantiza que las acciones sean monitoreadas y evaluadas de forma periódica.

05. **Información y comunicación**: Fomenta la transparencia y asegura que la información esté disponible para la ciudadanía.

06. **Gestión del conocimiento e innovación**: Facilita la innovación y la mejora continua de procesos.

07. **Control interno**: Verifica el cumplimiento de las normas y procedimientos establecidos.

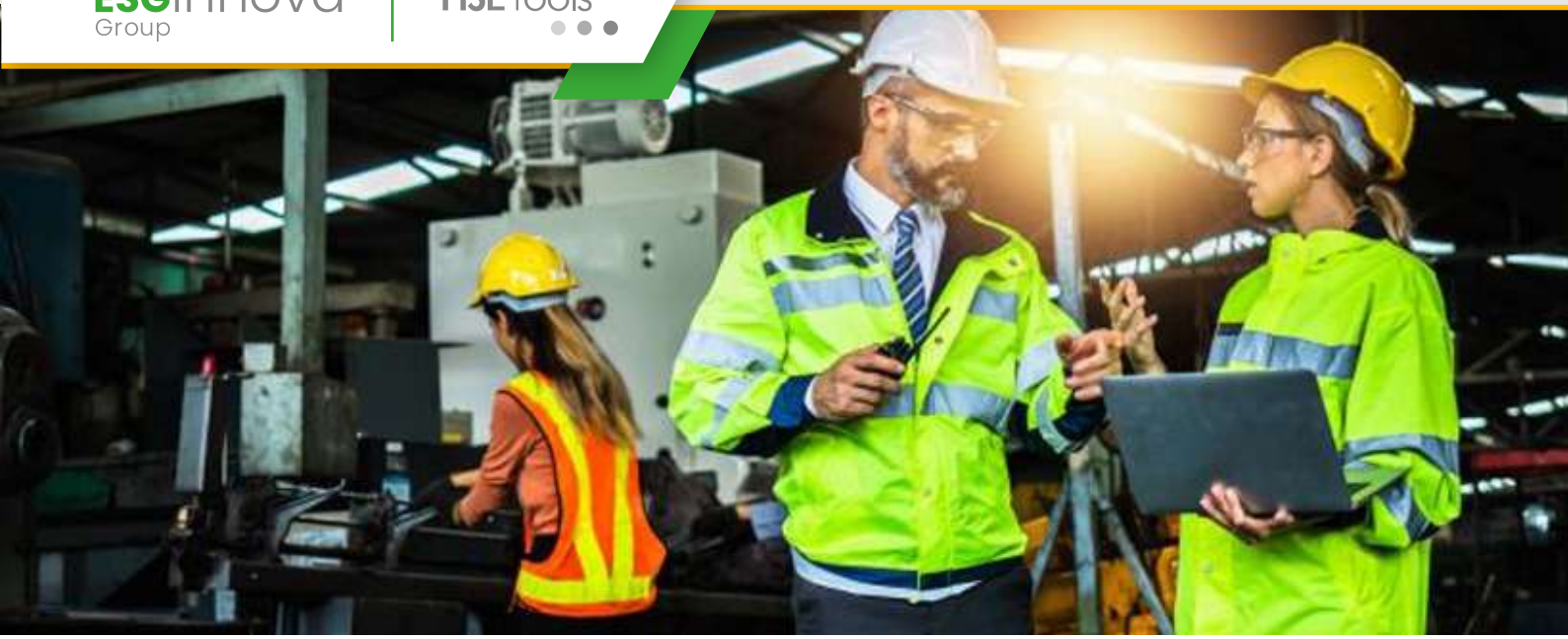
¿Para qué sirve el MIPG?

El MIPG sirve para **optimizar la gestión de recursos y procesos** en las entidades públicas, promover la transparencia y fortalecer la rendición de cuentas.

ESGinnova
Group

HSE Tools

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



5 Razones por las que la investigación de incidentes es crucial para la seguridad en el trabajo

La **investigación de incidentes** es el proceso que analiza la información contenida en el **reporte de incidentes**, las evidencias y pruebas recopiladas en el lugar del hecho, así como los datos aportados por testigos para procesar, analizar y obtener una conclusión. La investigación de incidentes muestra una visión de esa eventualidad y permite comprender lo sucedido, establecer una línea de tiempo e **identificar los factores o elementos que intervinieron**. El objetivo será siempre hallar la causa raíz del problema para implementar las medidas oportunas.

Para que exista una investigación de incidentes **es preciso que, de manera previa, se presente un informe**. La falta de soporte tecnológico para la **gestión de incidentes** suele ser la causa recurrente para que los empleados no comuniquen la eventualidad, impidiendo así el inicio de las pesquisas. Reporte e investigación son,

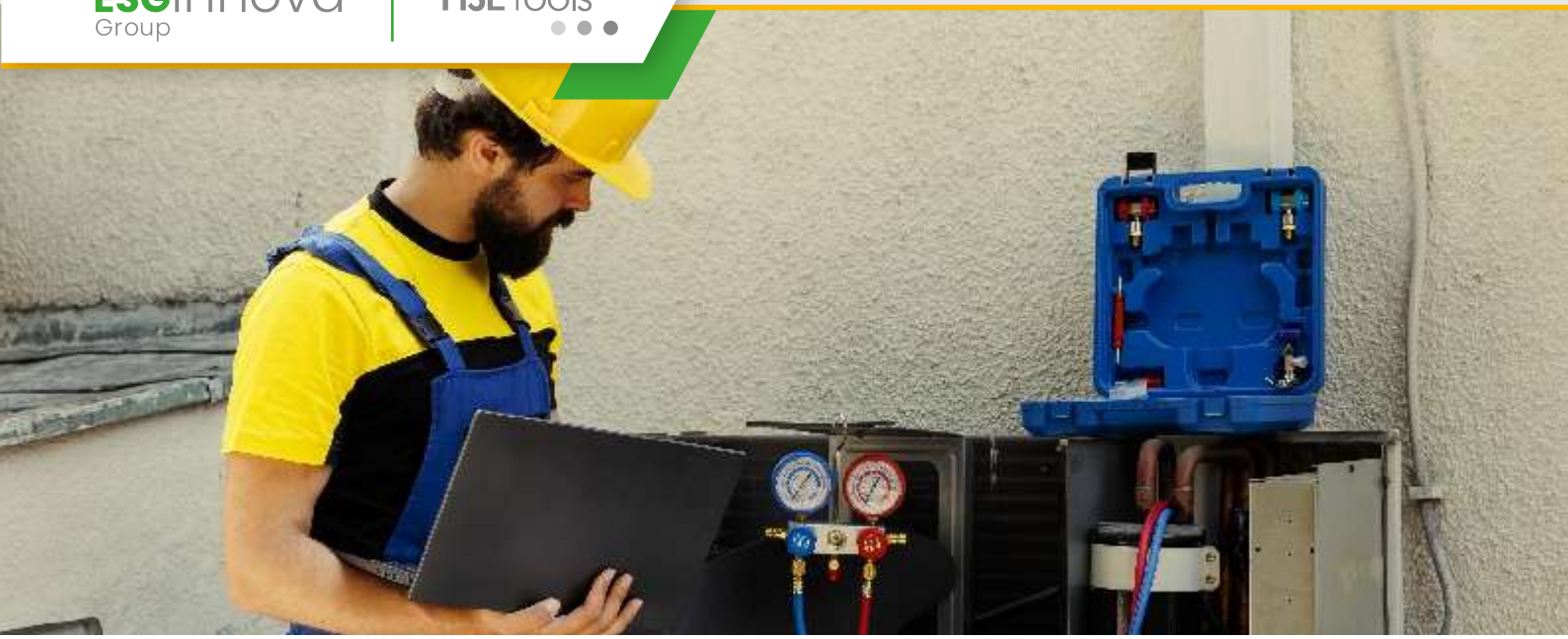
de esta forma, elementos esenciales en la **prevención de riesgos laborales**. Analizamos a continuación la relevancia del segundo aspecto, la investigación de incidentes, dentro de la gestión de seguridad en el trabajo.

Por qué es importante la investigación de incidentes para la seguridad en el trabajo

Existe una delgada línea que separa el incidente del **casi accidente**. Por supuesto, el accidente va mucho más allá por sus consecuencias. La línea de separación la define la probabilidad o no de que existan lesionados. Para algunos profesionales en Seguridad Laboral, todos **los incidentes pueden ser accidente en un futuro**. Esta es una posición que define una línea de acción proactiva. De hecho, la investigación de incidentes es rica en resultados y pródiga en conclusiones. Analizar eventos que no tuvieron consecuencias graves permite **anticipar y eliminar las causas de posibles accidentes en el futuro**. Algunas razones por las que la investigación de incidentes es importante son las siguientes:

1. Identifica riesgos no visibilizados

Un incidente sucede porque hay riesgos o elementos concatenados susceptibles de generar una amenaza y que han pasado desapercibidos por los especialistas en el área. **Esos riesgos no visibilizados, y por ello no tratados, son más lesivos que otros por su poder para mimetizarse y ocultarse**. La investigación de incidentes logra individualizarlos, definirlos, estudiarlos y entender la **causa raíz** para proceder a eliminarla.



Importancia del Mantenimiento Preventivo en HSE

Mantenimiento Preventivo en HSE

Una estrategia clave para evitar accidentes, reducir costos y cumplir con las normativas es el **mantenimiento preventivo** mediante **inspecciones y checklist** en el área de **HSE (Health, Safety, and Environment)**.

En la actualidad, la **seguridad** y el **bienestar de los trabajadores**, así como la **protección del medio ambiente**, son elementos críticos para el éxito de cualquier organización.

Pero, ¿qué lo hace tan esencial? A continuación, exploramos las razones por las cuales el **mantenimiento preventivo** es vital en la gestión de HSE.

1. Seguridad primero: Menos riesgo de accidentes laborales con el Mantenimiento Preventivo en HSE

El mantenimiento preventivo permite **identificar y corregir fallos potenciales** antes de que se conviertan en amenazas graves. Equipos defectuosos o instalaciones mal mantenidas pueden generar accidentes laborales que ponen en riesgo la vida de los empleados. Al mantener los equipos en condiciones óptimas, **se minimiza la posibilidad de incidentes**, creando un entorno de trabajo seguro.

Un programa de mantenimiento adecuado garantiza que **los equipos críticos** sean revisados y reparados de forma periódica, evitando fallos inesperados que podrían causar lesiones o incluso la pérdida de vidas.

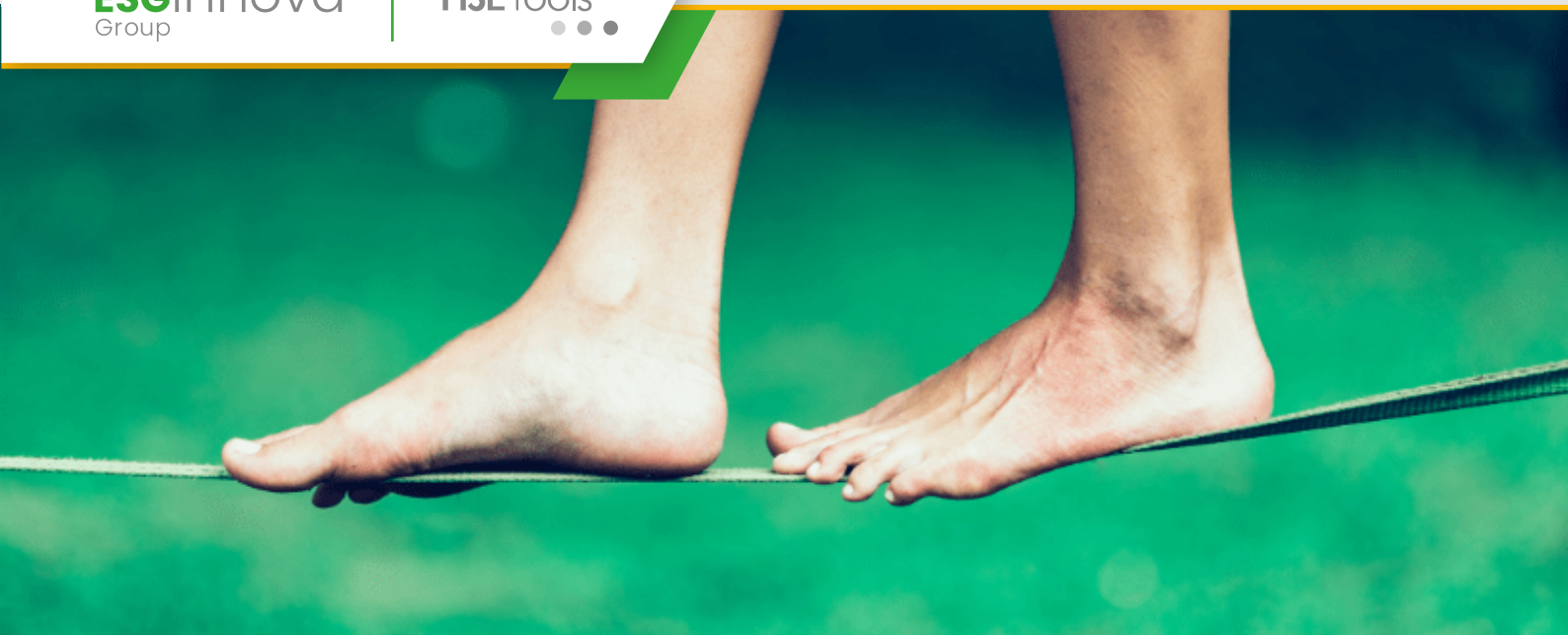
2. Cumplimiento normativo y evitación de sanciones

Muchas normativas de seguridad industrial y ambiental exigen que las empresas implementen un **mantenimiento preventivo** regular. El no cumplimiento de estas normativas puede derivar en **costosas sanciones** y, en casos extremos, en la suspensión de las operaciones.

Un plan de mantenimiento bien estructurado te ayudará a **evitar multas** y te permitirá demostrar tu **compromiso con la seguridad** y el cumplimiento de las normativas, lo que mejorará la reputación de tu empresa ante clientes, empleados y organismos reguladores.

3. Aumento de la productividad: Menos paradas inesperadas

¿Sabías que los fallos imprevistos de los equipos pueden costar una gran cuantía económica en reparaciones y pérdida de productividad? Aquí es donde el **mantenimiento preventivo** brilla.



¿Qué es la gestión de la prevención de riesgos?

Gestión de la prevención de riesgos

La **gestión de la prevención de riesgos** es el proceso sistemático de **identificar**, **evaluar y controlar** los riesgos en el entorno laboral para garantizar la seguridad y salud de los empleados. Este enfoque permite **minimizar los accidentes y enfermedades** ocupacionales, **mejorando** la **seguridad** y el **bienestar** de los trabajadores, al tiempo que se asegura el **cumplimiento de las normativas** vigentes.

Importancia de hacer una buena Gestión de la prevención de riesgos

Reducción de accidentes y costos

Implementar un sistema de **gestión de la prevención de riesgos** efectivo ayuda a reducir el número de **accidentes laborales** y enfermedades ocupacionales. Al identificar los riesgos y tomar medidas preventivas, las empresas pueden **reducir** considerablemente

los **costos** asociados con indemnizaciones, **tiempo** perdido y **problemas legales**. Un ambiente de trabajo seguro también mejora la **productividad** y la **satisfacción** de los empleados.

Cumplimiento normativo

La gestión de la prevención de riesgos es clave para **cumplir con las leyes y normativas** de seguridad laboral impuestas por organismos gubernamentales y sectoriales. Cumplir con estos requisitos no solo **evita sanciones**, sino que también **refuerza** la **reputación** de la empresa, demostrando un **compromiso** genuino con la seguridad y la salud de los trabajadores.

Cultura preventiva

Fomentar una **cultura preventiva** dentro de la organización es fundamental. Al involucrar a todos los niveles de la empresa en la **identificación y gestión de riesgos**, se promueve una **mayor responsabilidad y conciencia** en torno a la seguridad. La participación activa de los empleados en el proceso de **prevención** permite una **detección temprana** de posibles problemas y facilita la implementación de **medidas correctivas**.

Elementos clave

Identificación de riesgos

El primer paso en la gestión de la prevención de riesgos es la **identificación de peligros** en el entorno laboral. Estos pueden **incluir riesgos físicos, químicos, biológicos o ergonómicos**.

Qué buscar en un Sistema Digital de Gestión de Contratistas

Un **Sistema Digital de Gestión de Contratistas** es una herramienta indispensable para ayudar a las organizaciones a afrontar los desafíos que plantea la **contratación de trabajadores externos**. En muchos casos, esos terceros **son esenciales para la operación de la empresa** por sus conocimientos, por la transferencia de tecnología que ofrecen o por las oportunidades estratégicas que representan.

En un mundo sin fronteras comerciales y dominado por la **tecnología**, **las organizaciones necesitan encontrar oportunidades que les permitan ser competitivas**. Es una, entre muchas razones, por las que las empresas, cada vez más, encuentran ventajas estratégicas en la incorporación de contratistas para sus operaciones.

Qué es la gestión de contratistas

La particularidad de los contratistas es que **no son empleados directos de la organización**. Pueden ser empresas que suministran, como un servicio, la fuerza laboral que otra empresa solicita o pueden ser trabajadores independientes.

La gestión de contratistas reúne los procedimientos, actividades y tareas necesarias para **aprovechar el aporte de esa fuerza laboral.** Genera un valor agregado para la organización y evita o previene los posibles riesgos en diferentes áreas, como **seguridad laboral**, cumplimiento o seguridad de la información. Es una cuestión de tal valor, que hace necesaria la incorporación de un Sistema Digital de Gestión de Contratistas.

Por qué es importante implementar un Sistema Digital de Gestión de Contratistas

Un error en las organizaciones es considerar a los contratistas como empleados de la organización y utilizar las mismas **herramientas digitales para la gestión de las relaciones laborales y comerciales** con ellos. En el otro extremo están aquellas que no conceden a sus contratistas ninguno de los beneficios de los empleados directos.

La organización es **responsable de tratar todos los riesgos de seguridad y salud en el trabajo** que amenacen a sus trabajadores directos, pero también a sus **contratistas**. La relación con estos tiene puntos de coyuntura con la relación con trabajadores directos, pero también aristas que se contraponen. Es lo que hace imprescindible contar con un Sistema Digital de Gestión de Contratistas.

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO

Cómo evaluar la conformidad en HSE con Contratistas Externos para proteger el ambiente laboral

Cuando trabajamos con **contratistas externos**, es crucial asegurar que estos cumplan con los mismos estándares HSE que la organización. Es la base esencial que crea la protección de los empleados para minimizar los riesgos dentro del entorno laboral, evitar sanciones y fomentar un ambiente de trabajo seguro y sostenible.

Contratistas Externos

A continuación, te ofrecemos una guía completa sobre **cómo evaluar la conformidad en HSE con contratistas externos** y garantizar un ambiente profesional protegido.

1. Establece criterios claros de selección basados en HSE

El primer paso para asegurar la conformidad en HSE es seleccionar a los contratistas adecuados. Incluye **criterios HSE** en el proceso de selección, como:

- Certificaciones en **ISO 45001** (gestión de salud y seguridad en el trabajo) e **ISO 14001** (gestión ambiental).
- Revisión del historial de seguridad del contratista, incluyendo **indicadores clave de desempeño** (KPI) como tasas de accidentes.
- Verificación de sus políticas y procedimientos HSE.

Consejo: Elegir contratistas con un enfoque proactivo en HSE mejorará la seguridad en el sitio de trabajo, a la vez que también reduce incidentes que podrían afectar la productividad.

2. Capacita y concientiza a los Contratistas Externos

Una vez seleccionados, los contratistas deben estar al tanto de las **políticas y procedimientos HSE** de tu empresa. Una buena práctica es implementar:

- **Inducciones HSE obligatorias** antes de que los contratistas comiencen sus actividades.
- Capacitaciones continuas sobre riesgos laborales y prácticas ambientales sostenibles.

¿Qué es ser una empresa saludable?

Una **empresa saludable** es aquella que promueve y mantiene el **bienestar físico, mental y social** de sus empleados. No se trata solo de evitar enfermedades o accidentes laborales, sino de crear un entorno de trabajo en el que los trabajadores se sientan motivados, seguros y apoyados. Esto implica implementar políticas que aborden tanto la **salud ocupacional** como la **calidad de vida laboral**, mejorando el clima organizacional y, a su vez, la **productividad**.

Empresa saludable

Una empresa saludable, tiene tres **características** principales:

Promoción de la salud física y mental

Las **empresas saludables** fomentan la adopción de hábitos saludables entre sus empleados. Esto incluye programas de **prevención de enfermedades**, iniciativas para fomentar la **actividad física**, y políticas que ayuden a gestionar el **estrés laboral** y mantener el **bienestar mental**.

Además, se promueve un equilibrio entre la vida personal y laboral para garantizar que los empleados estén **motivados y productivos**.

Entorno laboral seguro

El establecimiento de un entorno de trabajo **seguro y saludable** es fundamental para una empresa saludable. La gestión adecuada de los riesgos laborales, la **prevención de accidentes y la protección** de la salud de los empleados son pilares esenciales. Implementar políticas de **Seguridad y Salud en el Trabajo (SST)**, como la **ISO 45001**, asegura que los trabajadores estén **protegidos** frente a los riesgos ocupacionales.

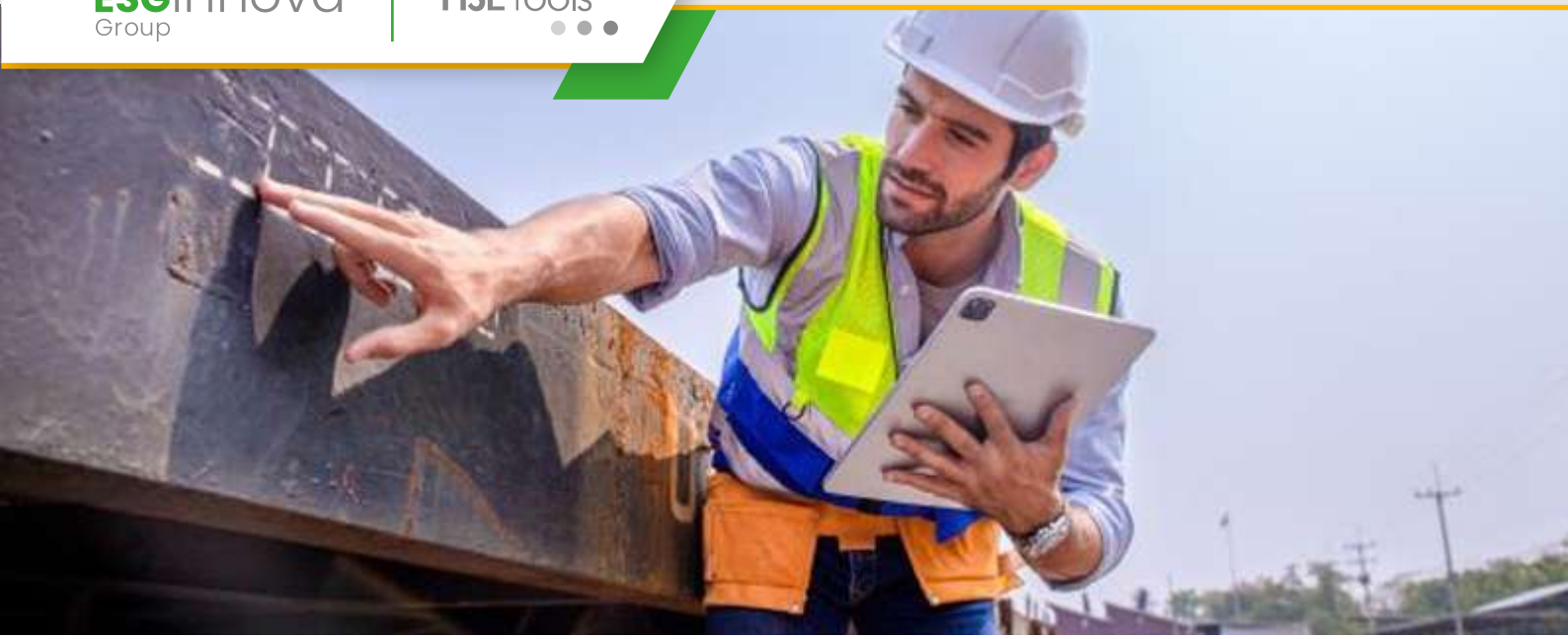
Clima organizacional positivo

Un clima organizacional positivo es otra característica de una **empresa saludable**. Fomentar una **cultura de apoyo**, donde los empleados se sientan valorados y escuchados, mejora la **moral** y contribuye al **bienestar emocional**. La **comunicación abierta** y la creación de canales de retroalimentación permiten a los empleados **expresar sus preocupaciones** y contribuyen a **resolver problemas** de manera colaborativa.

Beneficios de conseguirla

Contar con una empresa saludable tiene numerosos **beneficios**, entre los que destacan:

Aumento de la productividad: El bienestar de los empleados tiene un impacto directo en su **rendimiento laboral**. Una empresa que cuida la salud física y mental de sus trabajadores **reduce** los días de **ausentismo** y **mejora la motivación**.



Software de gestión de incidentes de seguridad en el trabajo: 6 características imprescindibles

El **software de gestión de incidentes de seguridad** es una **herramienta tecnológica** diseñada para digitalizar, monitorear y documentar los procesos de reporte, investigación, análisis, evaluación, conclusión y registro de los eventos que ocurren en el lugar de trabajo o asociados a la actividad laboral y que tienen la capacidad potencial para herir o lesionar a las personas.

Los incidentes de seguridad en el trabajo, aunque no son deseables, tienen un alto valor en la gestión de seguridad en el trabajo porque **aportan información muy valiosa que evita futuros accidentes**. Sin embargo, la ausencia de un software adecuado suele generar abstención de informar en organizaciones que no han iniciado procesos de transformación digital. **Implementar un software de gestión de incidentes y accidentes** aporta muchos beneficios.

A continuación profundizamos en las **características esenciales que debe buscar la organización** a la hora de seleccionar un software para automatizar la seguridad en el trabajo.

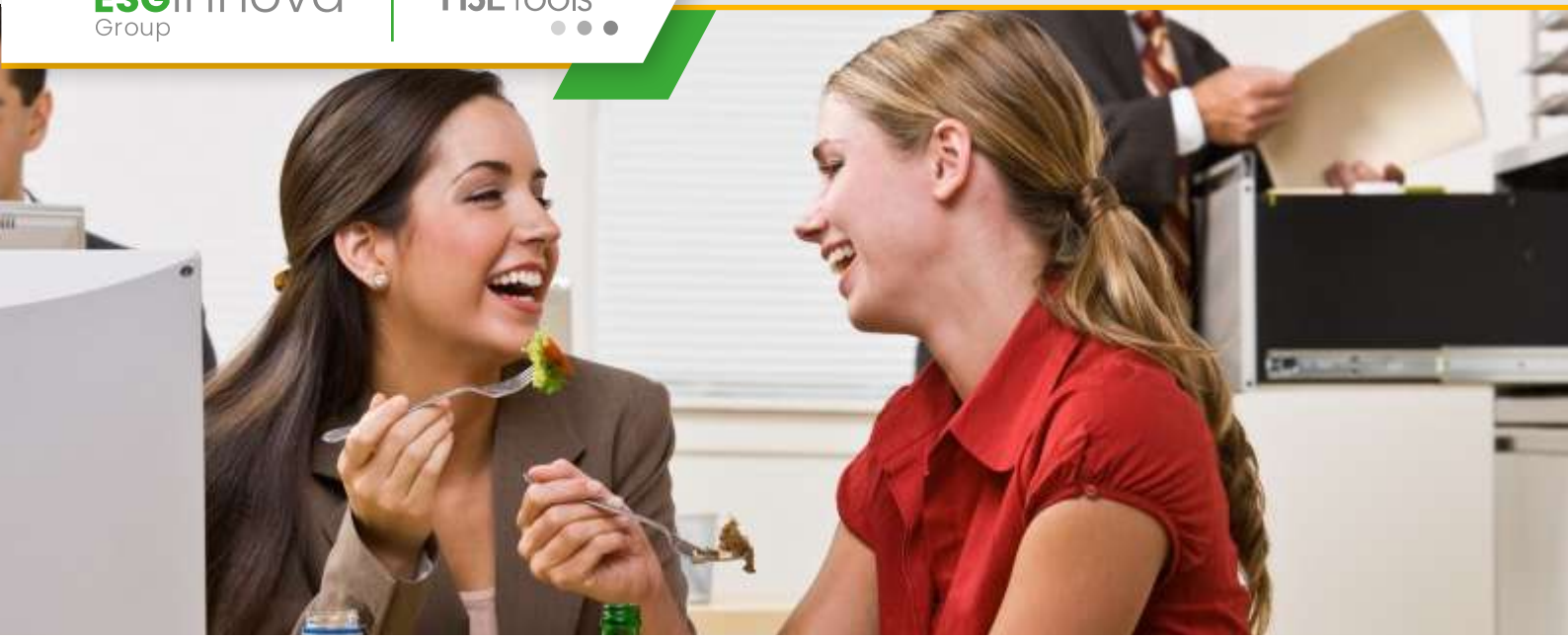
Qué es un software de gestión de incidentes de seguridad en el trabajo

La gestión de incidentes originados o relacionados con la actividad laboral **es un proceso complejo que se desarrolla en varias etapas:** reporte, investigación, **documentación y registro**, diseño de acciones correctivas, verificación de la eficacia, nuevas acciones correctivas e informes finales. En la ejecución de cada etapa se realizan **tareas y actividades que comprometen a diferentes personas y diferentes áreas**. Se asignan responsabilidades y labores y, así, la gestión se torna compleja. Dependiendo del tamaño de la organización y de la gravedad del problema, puede llegar a ser inmanejable. El software de gestión de incidentes de seguridad en el trabajo evita que esto suceda. **Las tareas que son susceptibles de ser automatizadas lo son** y las que deben ser atendidas por personas se asignan de acuerdo con flujos de trabajo gestionados en la plataforma.

Cómo funciona un software de gestión de incidentes de seguridad

Las personas a quienes asigna una actividad son notificadas, junto con las que pueden tener algún interés en esa actividad. **El sistema emite alertas por retrasos o por incumplimientos** y presenta una visión en tiempo real sobre el avance de la gestión para cada incidente o para todos en conjunto. La tarea del software de gestión de incidentes de seguridad en el trabajo se inicia desde el mismo momento en que sucede el evento.

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO



¿Cuáles son los 4 elementos del modelo de organización saludable según la OMS?

Si ponemos el **bienestar de los empleados** en el centro organizativo de las empresas, estas, además de asegurar un **entorno laboral saludable**, estarán trabajando a favor de la productividad. Estos factores son cruciales para mantenerse competitivo en entornos masificados.

Organización saludable

La Organización Mundial de la Salud (OMS) ha propuesto un modelo integral que ayuda a las organizaciones a crear ambientes de trabajo **saludables** y sostenibles. Este modelo se basa en cuatro elementos clave que abordan tanto la salud física como la mental de los empleados. A continuación, te explicamos estos cuatro componentes esenciales para construir una **organización saludable**.

1. Ambiente físico de trabajo saludable

El primer pilar se centra en el **entorno físico** donde los empleados realizan sus tareas. Un ambiente físico adecuado previene lesiones y enfermedades, y garantiza que los empleados puedan trabajar de manera segura. Para lograrlo, las empresas deben:

- Diseñar espacios de trabajo **ergonómicos**.
- Proporcionar condiciones de trabajo seguras, con **protocolos de seguridad** claros.
- Controlar la exposición a **sustancias peligrosas** y asegurar una buena ventilación e iluminación.

Al cuidar el ambiente físico, la salud de los empleados se ve reforzada y su predisposición al trabajo es más positiva, lo que repercute en la mejora de su **rendimiento** y su satisfacción general.

2. Ambiente psicosocial de trabajo saludable

El segundo elemento es el ambiente psicosocial, que abarca aspectos como el **bienestar emocional** y la **salud mental** de los empleados. Este aspecto cobra cada vez más relevancia, dado el creciente impacto del **estrés laboral** en la salud. Las empresas deben:

Fomentar una **cultura organizacional positiva**, donde se valoren las relaciones de apoyo y respeto.

¿Por qué una organización debe ser una empresa saludable?

El concepto de **empresa saludable** va más allá de la prevención de accidentes laborales y enfermedades profesionales. Implica crear un entorno de trabajo que fomente el **bienestar físico, mental y social** de los empleados. Ser una organización saludable no solo **mejora la calidad de vida** de los trabajadores, sino que también impacta positivamente en la **productividad**, la **retención de talento** y la **reputación corporativa**. En este artículo, exploraremos las razones por las cuales las empresas deben adoptar este enfoque para mejorar su rendimiento general.

Empresa saludable

Una **empresa saludable** es aquella que se preocupa por el **bienestar integral** de sus empleados, implementando estrategias que promuevan tanto la **salud física** como el **bienestar emocional**. No se limita solo a **cumplir con las normativas** de **seguridad y salud en el trabajo**, sino que fomenta la creación de un **ambiente**

de trabajo positivo que permita a los empleados desarrollarse en su **máximo potencial**. Una organización saludable abarca diversas dimensiones:

- **Salud física**: Implementar programas de actividad física, promover hábitos saludables y ofrecer acceso a servicios de salud.
- **Salud mental**: Crear un entorno que reduzca el estrés y fomente el equilibrio entre la vida laboral y personal.
- **Salud social**: Promover la **cohesión del equipo**, fomentar la diversidad y proporcionar un ambiente de apoyo.

Beneficios de ser una empresa saludable

Aumento de la productividad

El **bienestar de los empleados** tiene un impacto directo en la **productividad**. Los trabajadores que se sienten **valorados** y que cuentan con un ambiente de trabajo saludable tienden a ser más **comprometidos**, lo que resulta en **mayor eficiencia** y **mejores resultados**. Las empresas que invierten en la salud de sus empleados ven **reducciones** en el **absentismo** y **mejoras en el desempeño**.

Reducción de costos

Al mejorar las condiciones laborales, las empresas saludables pueden **reducir** los **costos asociados a enfermedades y accidentes**. La **prevención de riesgos** y la promoción de hábitos saludables disminuyen las tasas de **enfermedades ocupacionales** y reducen el uso de los servicios de salud, lo que implica un **ahorro** significativo para la organización.

Beneficios que aporta una cultura de seguridad y salud en el trabajo sólida

La ausencia de **cultura de seguridad** es una causa recurrente por la que programas de **seguridad y salud en el trabajo** no ofrecen los resultados esperados, pese a la implementación de sistemas de gestión avanzados o la asignación de recursos suficientes.

Los entornos laborales modernos son complejos. Son tantas y tan diversas las fuentes de riesgos físicos, sociales y psicosociales, que la gestión SST es más que una necesidad: **es un activo de alto valor para la organización y para sus trabajadores.** Un activo, sin embargo, que requiere de la cultura de seguridad como elemento indispensable para funcionar y cumplir con sus objetivos en la organización. Uno de los retos que deben enfrentar los encargados de velar por la seguridad de los trabajadores a la hora de crear y difundir cultura de seguridad **es la falta de comprensión exacta sobre lo que este concepto significa**. Si no se entiende lo que es, resulta complicado que se acepten sus beneficios.

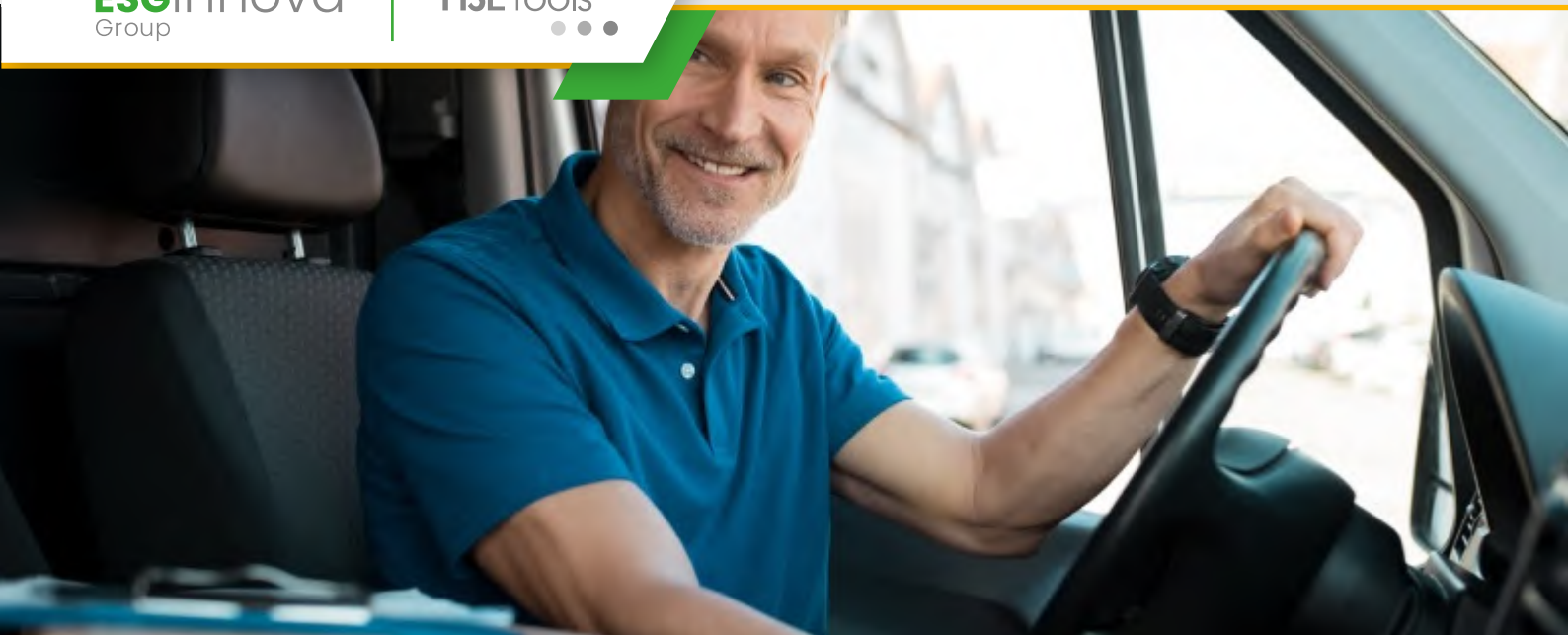
Qué es cultura de seguridad y salud en el trabajo

A la luz de la semántica, la cultura es el conjunto de conocimientos, saberes y costumbres que caracterizan a un grupo humano, un país o un conjunto de personas que comparte intereses comunes. Bajo esta definición, **el problema de falta de cultura de seguridad se solucionaría capacitando a las personas**. De hecho, se trata de una de las estrategias más efectivas para generarla. Pero el problema, en el caso de la seguridad y salud en el trabajo, es un tanto más complejo. En este caso, la cultura reúne otros elementos, además del conocimiento. La cultura, en el área de seguridad laboral, **requiere liderazgo, compromiso y convencimiento de lo que se está haciendo y las razones por las que se hace**. Aparece entonces un término nuevo: concientización. Así, la cultura de seguridad y salud en el trabajo es el conjunto de conocimientos sobre este tema que se aceptan, promueven de forma activa y se aprovechan por la fuerza laboral de una empresa. **Educación y concientización** son claves, **existe cultura de seguridad cuando se sabe qué hacer, se hace, se está convencido de la razón por la que se hace y se difunde ese convencimiento de forma proactiva.**

Beneficios de la cultura de seguridad y salud en el trabajo

Difundir conocimientos sobre prevención de riesgos y sobre el funcionamiento de un **sistema de gestión de seguridad y salud en el trabajo** es importante y es uno de los componentes de esa cultura. Sin embargo, si los empleados no establecen relación directa entre ese conocimiento y sus beneficios, no estarán convencidos del proyecto y no asumirán el liderazgo que requiere. Por eso es tan importante **conocer, entender y aceptar los beneficios de la cultura de seguridad**.

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO



¿Qué es la seguridad vial en una empresa?

La **seguridad vial en el entorno laboral** es un aspecto crucial para garantizar la integridad de los colaboradores, a la vez que reduces costos y mejoras la eficiencia operativa. Para una empresa que gestiona trabajadores en constante desplazamiento o que depende de la logística vehicular, la seguridad vial es un factor estratégico en su gestión de seguridad y salud en el trabajo.

Por lo tanto, vemos imprescindible profundizar en **qué es la seguridad vial en una empresa**, por qué es fundamental su implementación, y cómo la tecnología, a través de plataformas como **HSETools**, puede transformar la gestión de seguridad vial en el ámbito empresarial.

Seguridad vial en una empresa

La **seguridad vial en una empresa** abarca todas **aquellas políticas, procedimientos y acciones** encaminadas a **reducir los riesgos asociados a los desplazamientos laborales**.

Esto aplica tanto a aquellos trabajadores que usan vehículos corporativos como a los que se desplazan en sus propios vehículos durante horas de trabajo. La gestión de la seguridad vial implica la implementación de medidas para proteger a los empleados, reducir el índice de accidentes y, al mismo tiempo, mejorar la cultura de seguridad dentro de la organización.

Este enfoque es especialmente relevante en **industrias como el transporte, la logística y la construcción**, y en aquellas donde los empleados deban hacer desplazamientos frecuentes.

Importancia de la Seguridad Vial en el ámbito empresarial

En el contexto empresarial, la **seguridad vial** representa un compromiso con la integridad física de los colaboradores, y además tiene un impacto directo en:

01. **Reducción de costos**: Los accidentes laborales que involucran vehículos conllevan gastos por daños materiales, pérdidas operativas y, en casos severos, indemnizaciones y costos legales. Invertir en seguridad vial puede reducir estos gastos de manera considerable.

02. **Productividad y moral de los empleados**: Un entorno de trabajo seguro mejora la moral de los empleados, lo cual se traduce en mayor productividad. Cuando los trabajadores perciben que la empresa prioriza su seguridad, su compromiso y sentido de pertenencia aumentan.

03. **Imagen corporativa**: Una empresa comprometida con la seguridad vial proyecta una imagen responsable y ética hacia sus clientes, socios y la sociedad en general.

10 cosas que pueden hacer las empresas y sus trabajadores por la seguridad vial

La **seguridad vial** en el entorno laboral es esencial, especialmente para empresas que dependen del **transporte y movilidad de sus empleados**. Los accidentes de tránsito afectan tanto a la **salud de los trabajadores** como a la **rentabilidad de las empresas**. La implementación de medidas de seguridad vial no solo **reduce accidentes**, sino que también mejora el **compromiso** y **bienestar** de los empleados. Aquí te ofrecemos 10 acciones clave que pueden tomar tanto las organizaciones como sus trabajadores para **promover la seguridad vial**.

Acciones de las empresas para mejorar la seguridad vial

1. Implementar políticas de seguridad vial

Una política de **seguridad vial** clara y bien estructurada es fundamental. Este documento debe definir las **normas y conductas** esperadas, los procedimientos para **casos de emergencia y las medidas**

preventivas. Esta política también debe contemplar la **capacitación en seguridad vial**, tanto para empleados que conducen como parte de su trabajo como para quienes se desplazan a diario en vehículos.

2. Capacitación constante para los conductores

La capacitación es clave para **mejorar la seguridad vial**. Las empresas deben ofrecer cursos regulares sobre **conducción segura**, técnicas de **prevención de accidentes** y manejo en **condiciones adversas**. Esto ayuda a **reducir los riesgos** y a **mejorar la confianza** de los empleados al volante.

3. Monitoreo de la salud de los conductores

La salud de los conductores afecta directamente su capacidad para conducir de manera segura. Implementar un **programa** de **vigilancia de la salud** es crucial para asegurar que los empleados se encuentren en **óptimas condiciones físicas y mentales**. Esto incluye controles periódicos de visión, presión arterial, niveles de estrés y otros aspectos de la salud que puedan **impactar su seguridad** en el volante.

4. Mantenimiento preventivo de los vehículos

El **mantenimiento preventivo** es esencial para **reducir el riesgo de fallos mecánicos** que puedan derivar en accidentes. Las empresas deben **programar revisiones técnicas** de todos los vehículos y asegurar que se encuentren en **buen estado** antes de su uso. Esto también incluye la revisión de neumáticos, frenos, luces y otros elementos críticos para la seguridad vial.

ESGinnova Group

GRCTools

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

¿Qué son los riesgos corporativos y cómo gestionarlos eficientemente?

Riesgos corporativos

El **riesgo** es la posibilidad de que ocurra un evento o condición que pueda tener consecuencias negativas, afectando el logro de objetivos o la estabilidad de una organización, proyecto o inversión. Se mide generalmente en términos de **probabilidad** e **impacto**, y puede derivarse de diversas fuentes, incluyendo factores **financieros**, **operativos**, **estratégicos**, **legales**, y de **reputación**. La gestión del riesgo implica identificar, evaluar y mitigar estos eventos adversos para proteger los activos y garantizar la **continuidad del negocio**.

En concreto, los **riesgos corporativos** se definen como eventos o condiciones que pueden impactar negativamente en la capacidad de una empresa para alcanzar sus objetivos. Estos riesgos pueden surgir de diversas áreas y su identificación es clave para el éxito organizacional. Los principales tipos de riesgos incluyen:

- **Riesgos corporativos financieros**: Pueden incluir fluctuaciones en los mercados, cambios en las tasas de interés y problemas de liquidez.

- **Riesgos operativos**: Derivan de fallos en procesos internos, tecnología o errores humanos.

- **Riesgos de cumplimiento**: Surgen del incumplimiento de leyes y regulaciones que rigen el sector.

- **Riesgos estratégicos**: Resultan de decisiones erróneas que afectan la dirección y competitividad de la empresa.

- **Riesgos de reputación**: Asociados a crisis de imagen, malas prácticas o escándalos.

- **Riesgos cibernéticos**: Amenazas que ponen en riesgo la seguridad de la información y sistemas digitales.

La importancia de gestionar los riesgos

La gestión de riesgos corporativos no es solo una medida de protección; es una estrategia integral que puede transformar la manera en que una organización opera. **Identificar y gestionar eficientemente los riesgos** puede conducir a:

- **Protección de activos**: Evitar pérdidas financieras y daños a la reputación.

- **Mejora en la toma de decisiones**: Facilitar decisiones más informadas y estratégicas.

¿Qué es la NERC-CIP? Guía completa sobre la protección crítica de infraestructura

La normativa NERC-CIP (North American Electric Reliability Corporation – Critical Infrastructure Protection) es un conjunto de estándares de seguridad diseñados para proteger las infraestructuras críticas del sector eléctrico en Norteamérica. Estos estándares son esenciales para garantizar la fiabilidad de los sistemas de energía y la seguridad de la infraestructura que los soporta. En este post, te ofrecemos una guía completa sobre qué es la NERC-CIP y su papel en la **gestión integral de riesgos** dentro de la industria eléctrica.

¿Qué es la NERC-CIP?

La normativa NERC-CIP es una serie de estándares obligatorios desarrollados por la NERC, una organización sin ánimo de lucro que regula la fiabilidad de las redes eléctricas en Estados Unidos, Canadá y parte de México.

El objetivo principal de estos estándares es asegurar la protección de los sistemas de control y la infraestructura crítica asociados con la generación, transmisión y distribución de electricidad.

NERC-CIP se centra principalmente en proteger los activos cibernéticos relacionados con estas infraestructuras, así como en establecer protocolos de seguridad física y procedimientos para la respuesta ante incidentes. En otras palabras, su implementación es crucial para mitigar los riesgos de ciberseguridad, además de otros riesgos operacionales y estratégicos, dentro del sector energético.

Principales estándares de NERC-CIP

NERC-CIP está compuesto por un conjunto de estándares específicos que abarcan diferentes aspectos de la **protección de infraestructuras críticas**. A continuación, se destacan algunos de los más relevantes:

- **CIP-002: Identificación de Activos Críticos**

Este estándar se centra en la identificación y clasificación de los activos críticos que requieren protección. Un paso fundamental en la gestión integral de riesgos, ya que ayuda a determinar qué partes de la infraestructura eléctrica son más vulnerables a amenazas cibernéticas o físicas.

- **CIP-004: Control de Acceso y Capacitación**

CIP-004 establece procedimientos para controlar el acceso a los sistemas críticos y asegurar que los empleados tengan la formación necesaria para gestionar correctamente los riesgos de seguridad de la información.

Cómo implementar un sistema de riesgos operacionales en tu empresa

La **gestión integral de riesgos** es un aspecto fundamental en cualquier empresa, ya que permite anticiparse a eventos que puedan afectar la continuidad operativa, la seguridad y la rentabilidad del negocio. Uno de los aspectos más críticos dentro de esta gestión es el manejo de los **riesgos operacionales**, aquellos que surgen por fallos en los procesos internos, personas, sistemas o eventos externos. En este artículo, exploraremos cómo implementar un sistema efectivo para gestionar estos riesgos en tu empresa, protegiendo así tus operaciones y asegurando un crecimiento sostenible.

¿Qué son los riesgos operacionales y por qué son tan importantes?

Los **riesgos operacionales** se refieren a las posibles pérdidas o problemas que pueden derivarse de fallos en los procesos de negocio, errores humanos, deficiencias tecnológicas o eventos externos como desastres naturales.

Estos riesgos pueden tener un impacto directo en la **productividad**, **reputación** y **salud financiera** de una empresa.

Por ejemplo, un error en la gestión de datos puede llevar a una pérdida significativa de información, mientras que un fallo en un proceso clave podría generar retrasos en la cadena de suministro. La identificación y gestión de estos riesgos es esencial para minimizar sus consecuencias y garantizar una respuesta rápida ante cualquier imprevisto.

Pasos para implementar un sistema de riesgos operacionales

Un sistema eficiente de **gestión de riesgos operacionales** requiere una serie de pasos bien estructurados, que deben integrarse en la cultura organizacional y en los procesos diarios de la empresa. A continuación, te detallamos cómo implementarlo:

Identificación de riesgos operacionales

El primer paso para implementar un sistema de gestión es identificar todos los posibles **riesgos operacionales** que pueden afectar a tu empresa. Esto incluye analizar cada área de negocio, desde los procesos financieros hasta la gestión de recursos humanos, pasando por la cadena de suministro, la producción y la tecnología.

La identificación de riesgos debe ser exhaustiva e incluir no solo los riesgos internos, como los fallos de procesos, sino también los **riesgos de terceras partes** que surgen al depender de proveedores externos o aliados estratégicos.

Guía Completa de Ciberseguridad NIST: Protegiendo tus Datos en la Era Digital

Ciberseguridad NIST

La **Ciberseguridad NIST** (National Institute of Standards and Technology) ha ganado un papel fundamental en la **protección de datos empresariales**, ya que establece un marco **confiable y reconocido** para gestionar y mitigar los **riesgos cibernéticos**. En la era digital, las **amenazas de ciberseguridad** evolucionan constantemente, y adoptar estándares como el NIST permite a las organizaciones **proteger sus activos más valiosos** de manera eficaz.

El **marco de ciberseguridad NIST** es un conjunto de directrices y **buenas prácticas** desarrolladas por el National Institute of Standards and Technology para ayudar a las organizaciones a **gestionar** los **riesgos de ciberseguridad**.

Este marco no es una norma obligatoria, pero se ha convertido en un **estándar** ampliamente **adoptado por empresas** de diferentes sectores, tanto en el ámbito privado como en el público.

El **objetivo** principal del marco es proporcionar una estructura flexible para **identificar**, **proteger**, **detectar**, **responder** y **recuperarse** de los incidentes de **ciberseguridad**. Estas cinco funciones clave permiten que las organizaciones desarrollen un enfoque integral para **manejar las amenazas y proteger sus datos**.

Componentes principales del marco NIST

El marco NIST se organiza en cinco **funciones principales**:

01. **Identificar**: Consiste en desarrollar un entendimiento del entorno empresarial para **gestionar los riesgos de ciberseguridad**. Incluye la identificación de activos, sistemas, datos y amenazas potenciales.

02. **Proteger**: Se enfoca en implementar medidas de seguridad que **reduzcan** las posibilidades de **sufrir un ataque cibernético**. Esto incluye el control de acceso, la protección de datos y la capacitación del personal.

03. **Detectar**: Hace referencia a la capacidad de **monitorear las amenazas y detectar** posibles **incidentes** en tiempo real. Esta función es clave para minimizar el impacto de un ataque.

04. **Responder**: En caso de que ocurra un incidente, es fundamental tener un **plan de respuesta eficiente** que permita contener y mitigar el daño lo antes posible.

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO

¿Qué es el riesgo de terceros y cómo gestionarlo eficientemente?

El **riesgo de terceros** es un tema cada vez más relevante en la gestión empresarial moderna. A medida que las organizaciones dependen más de **proveedores**, **contratistas** y **socios externos**, los riesgos asociados con estos terceros pueden comprometer la **seguridad**, el **cumplimiento normativo** y la **continuidad del negocio**. Es muy importante explorar qué es el riesgo de terceros, los tipos más comunes y cómo gestionarlo eficientemente para evitar impactos negativos en tu organización.

Riesgo de terceros

El riesgo de terceros se refiere a los posibles problemas o fallos que pueden surgir de las **relaciones comerciales con entidades externas**. Esto incluye riesgos operativos, financieros, legales y reputacionales. Por ejemplo, los terceros pueden abarcar desde proveedores de materias primas hasta consultores especializados o contratistas encargados de servicios críticos para el negocio.

¿Por qué es importante gestionar el riesgo de terceros?

Las organizaciones de todos los tamaños dependen de terceros para optimizar sus operaciones. Sin embargo, si estos terceros no cumplen con sus obligaciones o sufren fallos críticos, los efectos pueden repercutir directamente en tu empresa. Desde problemas con la **calidad de los productos** hasta **filtraciones de datos sensibles**, las consecuencias pueden ser devastadoras.

Tipos comunes de riesgo de terceros

Riesgo operativo

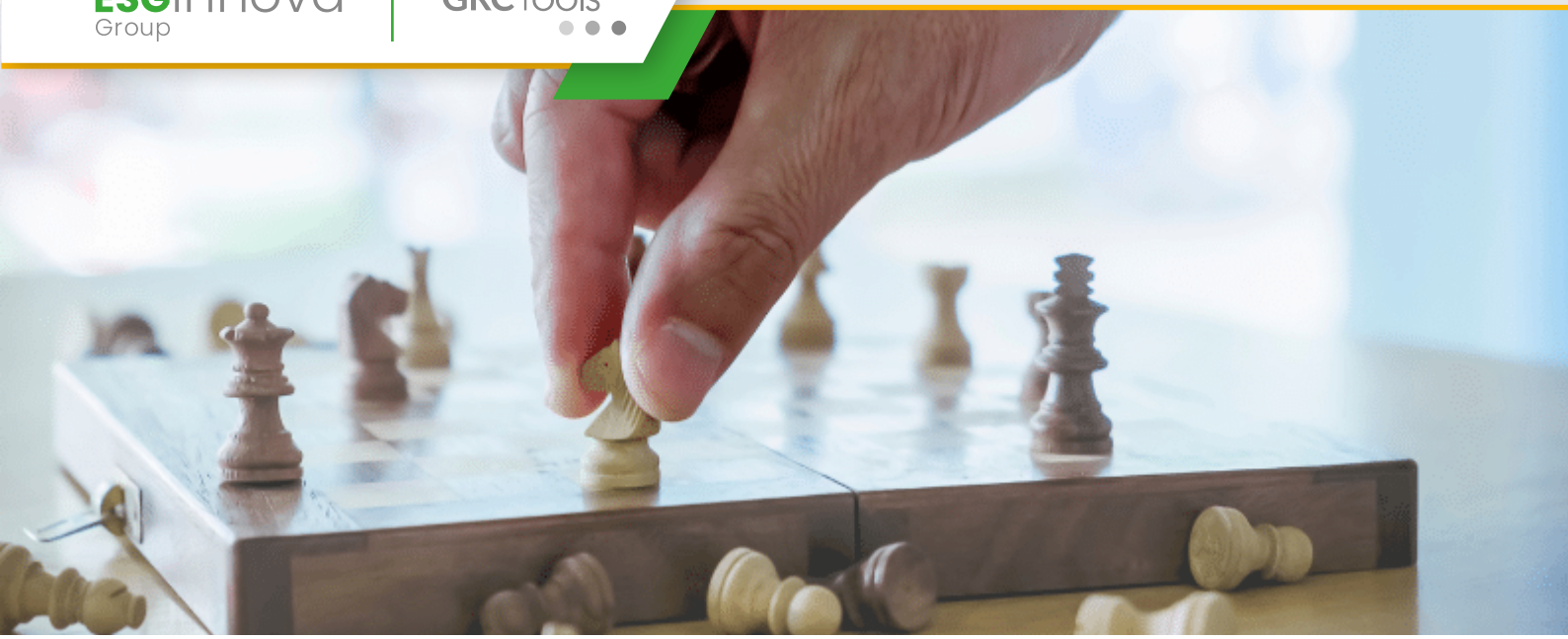
Este tipo de riesgo ocurre cuando **un proveedor o contratista no cumple con los niveles de servicio acordados**, lo que puede afectar la **cadena de suministro** o el funcionamiento diario de tu empresa. Por ejemplo, la interrupción en la entrega de insumos clave puede paralizar la producción.

Riesgo de cumplimiento normativo

Si uno de tus proveedores no cumple con las normativas locales o internacionales, tu empresa podría enfrentarse a sanciones legales. Esto es especialmente crítico en sectores altamente regulados como la **salud**, la **banca** o la **tecnología**.

Riesgo financiero

Si un tercero atraviesa dificultades financieras o incluso quiebra, tu empresa podría verse afectada. Este tipo de riesgo es más común en relaciones a largo plazo con proveedores clave.



Guía completa sobre la evaluación y tratamiento de Riesgos Corporativos – ERM

La **evaluación y tratamiento de riesgos corporativos** es un proceso esencial para garantizar la **resiliencia** de una empresa frente a desafíos internos y externos. Los Riesgos Corporativos – ERM (**Enterprise Risk Management**) proporcionan un marco estructurado para **identificar, analizar, gestionar y mitigar riesgos** de manera eficiente. En este artículo, te mostramos cómo las organizaciones pueden integrar la gestión de riesgos en sus operaciones y te invitamos a participar en el **webinar exclusivo** sobre la **evaluación y tratamiento de riesgos corporativos**.

Riesgos corporativos – ERM

El **Enterprise Risk Management (ERM)** es un enfoque integral para la **gestión de los riesgos corporativos** que permite a las organizaciones **identificar y gestionar** tanto los **riesgos estratégicos** como los operativos. ERM abarca todos los aspectos de la gestión de riesgos, desde los financieros hasta los de cumplimiento,

asegurando que las empresas no solo **protejan sus activos**, sino que también **optimicen su rendimiento** al **gestionar** de forma efectiva las **amenazas y oportunidades**.

La implementación de un marco ERM robusto permite a las organizaciones:

- **Identificar riesgos** de manera proactiva.
- Mitigar los riesgos que puedan afectar los **objetivos estratégicos**.
- Garantizar la **continuidad del negocio** mediante la gestión de incidentes inesperados.
- Mejorar la **toma de decisiones** basada en el análisis de riesgos.

Evaluación de riesgos corporativos – ERM

Identificación de riesgos

El primer paso en la **evaluación de riesgos corporativos** es la identificación de los peligros potenciales que podrían afectar a la empresa. Esto incluye tanto riesgos internos, como fallos en los procesos, como riesgos externos, como **fluctuaciones en el mercado** o **cambios regulatorios**.

Un enfoque estructurado, basado en el **análisis de datos** y el conocimiento profundo del negocio, es clave para **identificar las amenazas** con precisión.

Riesgos de ciberseguridad en empresas: soluciones con GRCTools

Desde ataques de ransomware hasta violaciones de datos, las amenazas cibernéticas son múltiples y cada vez más sofisticadas. La **gestión integral de riesgos** se ha convertido en un imperativo para proteger la información sensible y garantizar la continuidad del negocio. En este artículo, exploraremos cómo **GRCTools** puede ofrecer soluciones efectivas para gestionar los **riesgos de ciberseguridad** en tu empresa.

Los riesgos de ciberseguridad más comunes en las empresas

Antes de profundizar en las soluciones, es importante identificar los **riesgos de ciberseguridad** más comunes a los que se enfrentan las empresas hoy en día. A continuación, te detallamos algunos de los principales:

1. Ataques de ransomware

Uno de los mayores peligros que enfrentan las empresas es el ransomware, un tipo de malware que bloquea el acceso a los sistemas o datos de la empresa hasta que se paga un rescate. Las consecuencias de un ataque de ransomware pueden ser catastróficas, afectando la operativa diaria y generando **riesgos financieros** significativos.

2. Fugas de datos

Las violaciones de seguridad que resultan en la fuga de datos pueden causar graves daños a la reputación de una empresa. Los datos comprometidos, como la información de clientes o detalles financieros, pueden ser utilizados por delincuentes para fraudes o ventas en el mercado negro. Esto, además de afectar la confianza, puede generar **riesgos de compliance** si no se cumplen las normativas de protección de datos.

3. Phishing y ataques de ingeniería social

El phishing es una técnica de ciberataque donde los hackers se hacen pasar por entidades confiables para engañar a empleados o usuarios y obtener acceso a información confidencial.

Estos ataques no solo afectan la **seguridad de la información**, sino que también suponen un **riesgo operacional** para las empresas, que pueden perder acceso a sistemas críticos.

TISAX: Seguridad de la información automotriz y su relevancia en la industria

La **industria automotriz** maneja una gran cantidad de datos sensibles diariamente, por ello la **seguridad de la información** es una base fundamental para todas las industrias, y en concreto para esta. En esta situación, el estándar **TISAX** (Trusted Information Security Assessment Exchange) ha surgido como una solución que garantiza el cumplimiento de estrictos requisitos de seguridad de la información, asegurando la **confidencialidad, integridad y disponibilidad** de los datos en toda la cadena de suministro.

TISAX: ¿Qué es y por qué es esencial en la industria automotriz?

TISAX es un **mecanismo de evaluación** desarrollado por la Asociación Alemana de la Industria Automotriz (**VDA**) y gestionado por **ENX**, una organización encargada de supervisar las auditorías y asegurar que los resultados sean consistentes y fiables.

Este estándar se enfoca en asegurar que las empresas automotrices, y especialmente sus proveedores, cumplan con los requisitos más exigentes de **seguridad de la información**, lo que resulta vital en un entorno cada vez más digitalizado.

La información es poder y en ocasiones se utiliza para fines inmorales, por ello, la **protección de datos sensibles** como **planos de diseño**, **especificaciones técnicas** y **estrategias de desarrollo** es indispensable. Si esta información cae en las manos equivocadas, las consecuencias pueden ser devastadoras, desde la pérdida de propiedad intelectual hasta ataques cibernéticos que afecten la **reputación** y el **rendimiento financiero** de las compañías.

¿Por qué la certificación TISAX es un diferencial competitivo?

- **Confianza en la seguridad de la cadena de suministro**: TISAX permite a los fabricantes de automóviles asegurar que sus proveedores manejan los datos de manera adecuada. **Contar con la certificación TISAX** demuestra un compromiso con los más altos estándares de seguridad, lo que puede convertirse en un diferenciador clave al competir por contratos dentro de la industria.

- **Cumplimiento normativo**: Las regulaciones sobre la **protección de datos** y la **ciberseguridad** están en aumento a nivel global. TISAX ayuda a las empresas a alinearse con las normativas más estrictas y facilita el cumplimiento continuo, evitando así **multas** y **sanciones** regulatorias.

- **Facilita el intercambio seguro de datos**.

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO

Cómo gestionar los riesgos de compliance en tu empresa de manera eficiente

En un entorno empresarial cada vez más regulado, la gestión de los **riesgos de compliance** se ha convertido en un aspecto fundamental para **garantizar el cumplimiento normativo y evitar sanciones**. Los riesgos de compliance son aquellos asociados con el **incumplimiento de leyes**, **regulaciones** o **estándares** que rigen las actividades de una empresa. Estos pueden tener consecuencias legales, financieras y reputacionales, lo que hace esencial una **gestión eficaz**.

Riesgos de compliance

Los **riesgos de compliance** son aquellos relacionados con la posibilidad de que una **empresa no cumpla con las leyes, normativas o regulaciones** que le son aplicables. Esto incluye tanto normas nacionales como internacionales, así como estándares específicos del sector.

El incumplimiento puede dar lugar **a multas, sanciones, pérdida de licencias o daño reputacional**, lo que afectará negativamente a la operación de la empresa.

Algunos ejemplos de **riesgos de compliance** incluyen:

- **Incumplimiento de leyes laborales**, como el pago de salarios o las condiciones de seguridad.
- **Incumplimiento de normativas medioambientales**, como las leyes de gestión de residuos.
- **Violación de políticas de privacidad de datos**, como las regulaciones de protección de datos personales (GDPR).
- **Corrupción o soborno**, cuando no se implementan controles adecuados para prevenir prácticas ilícitas dentro de la organización.

Importancia de gestionar los riesgos de compliance

Protección legal y financiera

Una gestión efectiva de los riesgos de compliance ayuda a las empresas a **protegerse de sanciones legales** y multas significativas.

El incumplimiento normativo puede acarrear **consecuencias financieras** importantes, que no solo afectan los resultados de la empresa, sino que también pueden llevar a su **desprestigio** y pérdida de confianza entre clientes e inversores.

Cómo implementar un plan de prevención de riesgos laborales efectivo

La **prevención de riesgos laborales** es fundamental para asegurar la salud y seguridad de los trabajadores en cualquier organización. Implementar un **plan de prevención efectivo** reduce accidentes, aumenta la productividad y mejora el clima laboral.

Prevención de riesgos laborales

A continuación, te explicaremos **paso a paso** cómo desarrollar un plan exitoso que cumpla con la normativa y proteja a tus empleados.

1. Evaluación de riesgos laborales

El primer paso para un plan efectivo es realizar una **evaluación exhaustiva de los riesgos** presentes en el entorno de trabajo. Esto implica:

- **Identificación de peligros**: Detecta todos los factores de riesgo en los diferentes puestos de trabajo, desde peligros físicos, ergonómicos, hasta riesgos psicosociales.

- **Análisis de probabilidad y gravedad**: Clasifica cada riesgo según su probabilidad de ocurrencia y la gravedad del daño que puede causar. Este análisis te ayudará a priorizar qué riesgos deben abordarse con mayor urgencia.

Una herramienta útil para esta fase es la **matriz de riesgos**, que permite visualizar de manera clara qué peligros son más críticos y requieren medidas inmediatas.

2. Establecimiento de objetivos claros para el plan de prevención de riesgos laborales

Una vez que has evaluado los riesgos, es importante establecer **objetivos de prevención medibles**. Asegúrate de que estos objetivos sean:

- **Específicos**: Define claramente qué deseas lograr (por ejemplo, «reducir los accidentes de trabajo en un 15% en los próximos 6 meses»).

- **Medibles**: Utiliza indicadores de desempeño que te permitan evaluar el progreso.

- **Alcanzables**: Asegúrate de que los objetivos son realistas en función de los recursos y tiempo disponible.

- **Relevantes**: Que estén alineados con la normativa de seguridad y salud en el trabajo (por ejemplo, la Ley de Prevención de Riesgos Laborales o la norma ISO 45001).

¿Qué son los riesgos ambientales y cómo gestionarlos eficientemente?

Los **riesgos ambientales** son aquellos que surgen de la interacción entre una organización y su entorno natural, y pueden tener un impacto significativo en la sostenibilidad, reputación y operación de las empresas. Estos riesgos pueden derivar de fenómenos naturales, como inundaciones o terremotos, o de las actividades propias de la empresa, como la emisión de contaminantes o la generación de residuos. Gestionar estos riesgos de manera eficiente es clave para cumplir con normativas medioambientales y minimizar el impacto negativo sobre el medio ambiente y la comunidad.

En este post, explicaremos qué son los **riesgos ambientales** y cómo implementar una estrategia eficaz de **gestión integral de riesgos** para minimizarlos y proteger tu negocio.

¿Qué son los riesgos ambientales?

Los **riesgos ambientales** son amenazas que pueden afectar negativamente tanto al entorno natural como a las operaciones y la rentabilidad de una empresa. Estas amenazas pueden ser causadas por factores externos, como fenómenos climáticos extremos, o por la propia actividad de la empresa, especialmente en sectores que interactúan directamente con el medio ambiente, como la industria, la energía o la construcción.

Algunos ejemplos de **riesgos ambientales** incluyen:

- **Contaminación del aire, agua o suelo**: La liberación de sustancias contaminantes durante las operaciones industriales puede afectar los ecosistemas circundantes y la salud de las personas.

- **Fenómenos naturales**: Inundaciones, terremotos, incendios forestales y otros desastres naturales pueden interrumpir las operaciones y poner en peligro la infraestructura de la empresa.

- **Cambios en la normativa ambiental**: Las empresas deben cumplir con una serie de regulaciones ambientales que cambian con el tiempo. No cumplir con estas normativas puede generar sanciones económicas y dañar la reputación de la organización.

- Estos riesgos no solo tienen consecuencias operacionales y financieras, sino que también pueden tener un fuerte impacto en la imagen corporativa y en las relaciones con la comunidad y los reguladores.

ISO 31000: la norma clave para la gestión integral de riesgos

La **gestión integral de riesgos** es un aspecto esencial para la supervivencia y éxito de cualquier organización en el entorno actual, caracterizado por la incertidumbre y la constante evolución de los riesgos. En este contexto, la **ISO 31000** se ha convertido en una norma clave que proporciona directrices internacionales para la gestión eficaz de los riesgos en todo tipo de organizaciones.

En este artículo, exploraremos qué es la **ISO 31000**, por qué es tan importante para la **gestión de riesgos** y cómo puede ayudarte a proteger tu negocio frente a una amplia gama de amenazas, desde los **riesgos operacionales** hasta los **riesgos de ciberseguridad**.

¿Qué es la ISO 31000?

La **ISO 31000** es una norma internacional emitida por la Organización Internacional de Normalización (ISO), que proporciona principios y directrices para la **gestión integral de riesgos**.

Su objetivo es ayudar a las organizaciones a identificar, evaluar y mitigar los riesgos de manera eficaz, facilitando la toma de decisiones informadas en todos los niveles de la organización.

A diferencia de otras normas, la **ISO 31000** es aplicable a cualquier tipo de organización, sin importar su tamaño o sector, y puede integrarse en la gestión de riesgos corporativos, estratégicos, financieros, operacionales, y muchos más. Esto la convierte en una herramienta versátil para abordar los **riesgos de compliance**, los **riesgos ambientales** o los **riesgos de seguridad de la información**, entre otros.

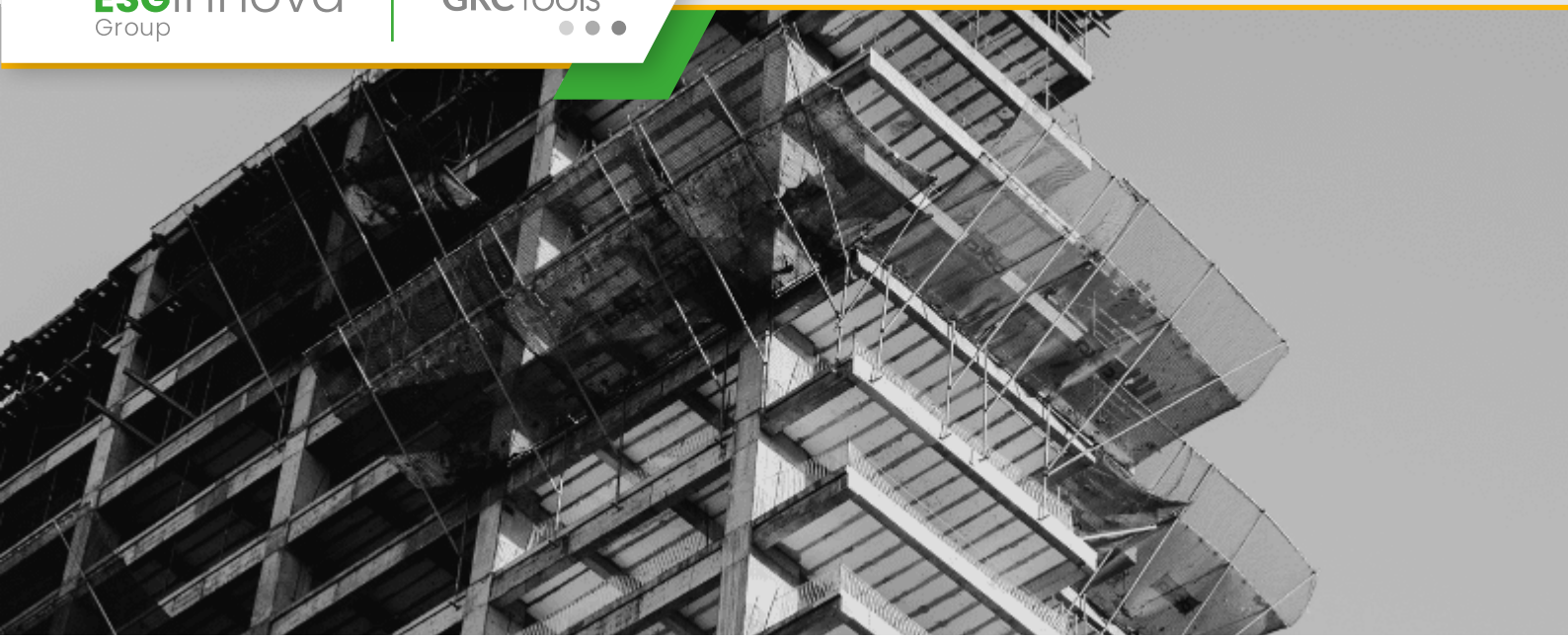
Principios clave de la ISO 31000

La **ISO 31000** se basa en una serie de principios fundamentales que orientan la forma en que las organizaciones deben abordar la **gestión de riesgos**. Estos principios no solo proporcionan una estructura coherente, sino que también garantizan que los riesgos se gestionen de manera eficaz y alineada con los objetivos estratégicos de la empresa.

A continuación, destacamos los principios clave:

1. Gestión basada en el valor

La gestión de riesgos debe contribuir a la creación de valor para la organización. Esto significa que cualquier medida de mitigación o control debe estar alineada con los objetivos estratégicos, optimizando los resultados y minimizando las posibles pérdidas derivadas de los **riesgos corporativos**.



Directiva NIS 2: Impulsando la Ciberseguridad en la Unión Europea

La **Directiva NIS 2** (Network and Information Security) es una actualización de la **Directiva NIS** original, adoptada por la **Unión Europea** para fortalecer la **ciberseguridad** en los Estados miembros. Con el creciente número de ciberataques, la NIS 2 busca mejorar las capacidades de **protección, respuesta y recuperación de las infraestructuras críticas** de Europa, estableciendo nuevos estándares y requisitos para los sectores clave. En este artículo, abordaremos los puntos clave de la directiva y cómo su implementación impactará a las empresas.

Directiva NIS 2

La **Directiva NIS original**, aprobada en 2016, fue la primera legislación a nivel europeo enfocada en **mejorar la ciberseguridad de infraestructuras críticas** como energía, transporte, salud y finanzas.

Sin embargo, con la evolución de las amenazas cibernéticas, la Comisión Europea consideró necesaria una actualización. La **Directiva NIS 2**, aprobada en 2022, tiene como objetivo **abordar las deficiencias de la directiva** anterior, ampliando su alcance y estableciendo normas más estrictas para la **gestión de riesgos** y la **cooperación internacional**.

Uno de los principales cambios introducidos por la **Directiva NIS 2** es la ampliación del alcance, incluyendo más sectores y entidades esenciales, como el suministro de agua, las infraestructuras digitales y las **tecnologías de la información**. Esta ampliación obliga a más empresas a **cumplir** con los nuevos estándares de **ciberseguridad**, incluyendo el fortalecimiento de sus capacidades para la **detección** y **respuesta a incidentes cibernéticos**.

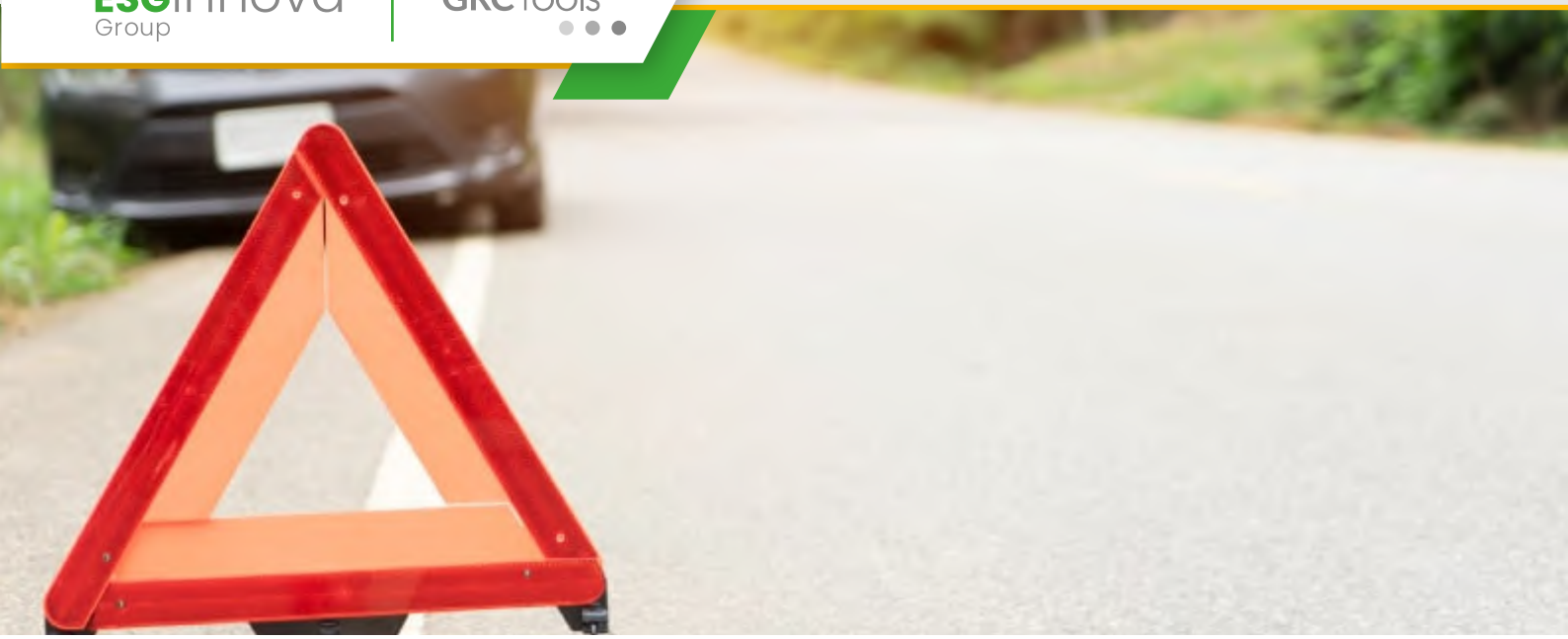
Requisitos clave de la Directiva NIS 2

Gestión de riesgos de ciberseguridad

La **gestión de riesgos** es un elemento central de la Directiva NIS 2. Las empresas afectadas deben implementar un marco sólido que les permita **identificar, evaluar y mitigar** los **riesgos cibernéticos** de manera efectiva. Esto incluye el desarrollo de **políticas de ciberseguridad**, la implementación de **controles de seguridad** y la **evaluación** constante de las **amenazas**.

Obligaciones de notificación

La Directiva NIS 2 introduce nuevos plazos y estándares más rigurosos en cuanto a las **obligaciones de notificación** de incidentes de seguridad.



Ley de Seguridad Vial vigente: Claves para su implementación

La **seguridad vial** es una prioridad para cualquier sociedad moderna. La implementación de una **Ley de Seguridad Vial** es clave para reducir accidentes, proteger a los usuarios de las vías y promover un tránsito más fluido y ordenado. Sin embargo, para que estas leyes sean efectivas, su implementación debe estar bien estructurada y apoyada por todos los actores del sistema vial.

Ley de seguridad vial

A continuación, te mostramos las **claves para la implementación** exitosa de una Ley de Seguridad Vial vigente, garantizando que no solo sea efectiva, sino también sostenible en el tiempo.

1. Legislación actualizada y adaptada a la realidad vial

Uno de los aspectos más importantes es que la **normativa de seguridad vial** debe estar **actualizada** y adaptada a las condiciones actuales del tránsito. Es crucial que las leyes reflejen los avances tecnológicos y los nuevos modos de transporte que han surgido, como los **vehículos eléctricos** o **sistemas autónomos**.

Además, es necesario que incluya regulaciones específicas sobre:

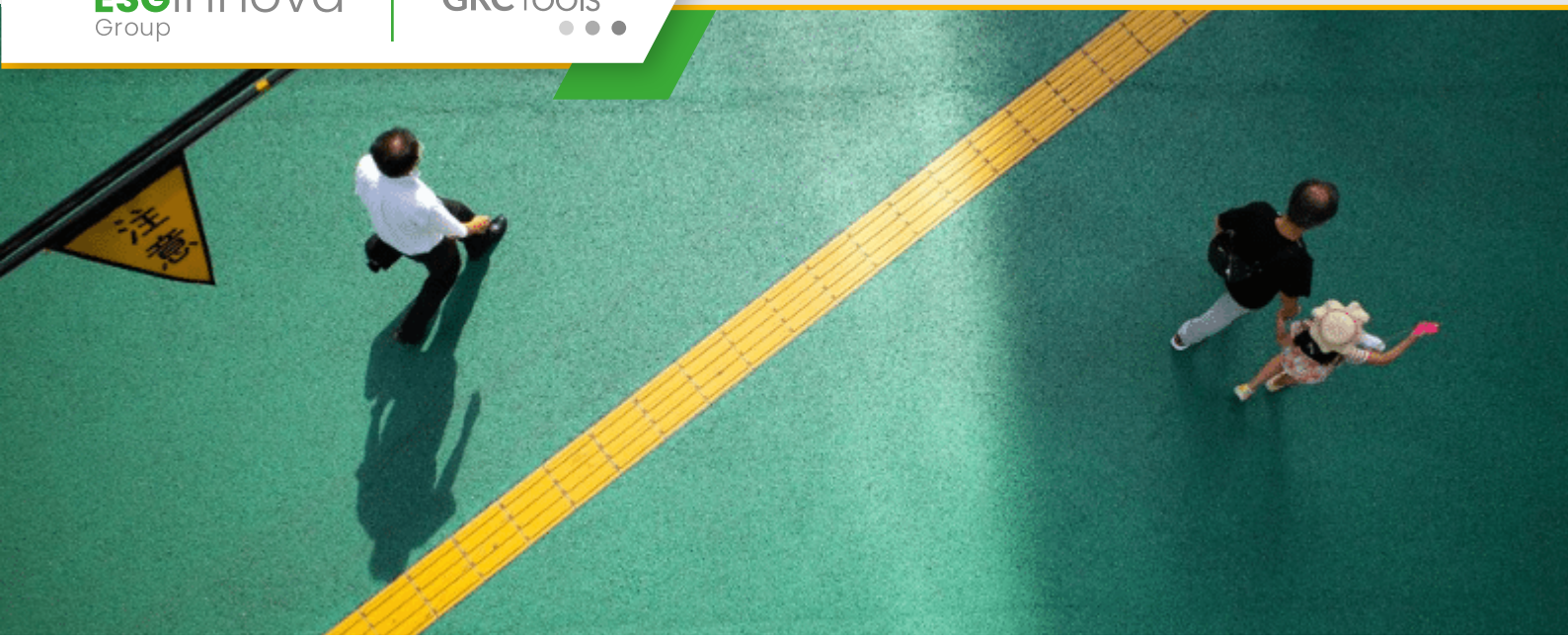
- **Límites de velocidad**.
- **Uso obligatorio de cinturón de seguridad**.
- **Normas para vehículos de carga**.
- **Regulación de conductores de transporte público y privado**.

Esto asegura que todos los actores del tráfico estén correctamente regulados, promoviendo un ambiente más seguro.

2. Concientización y educación continua

La **educación vial** es un pilar fundamental para la correcta implementación de cualquier ley.

No basta con imponer sanciones, es esencial que los conductores y peatones estén **informados** y **conscientes** de la importancia de respetar las normas de tránsito.



Tipos de gestión de riesgos y cómo aplicarlos en tu empresa

La **gestión de riesgos** es fundamental para garantizar la **sostenibilidad** y el **éxito** de cualquier organización. Con un enfoque sistemático, se pueden **identificar, evaluar y mitigar los riesgos** que pueden amenazar los **objetivos empresariales**. Los diferentes tipos de gestión de riesgos **varían según el enfoque y la naturaleza** de los riesgos, y cada empresa debe **adaptar su estrategia** a sus necesidades específicas. En este artículo exploraremos los **principales tipos de gestión de riesgos** y cómo **aplicarlos eficazmente** en tu empresa.

Tipos de gestión de riesgos

Gestión de riesgos operacionales

La **gestión de riesgos operacionales** abarca aquellos riesgos **asociados con los procesos internos de la empresa**. Estos riesgos pueden surgir de fallos en los sistemas, errores humanos, o interrupciones en la cadena de suministro.

Un **enfoque proactivo** para gestionar los riesgos operacionales incluye la **automatización de procesos**, la **implementación de controles internos** y la **mejora de la capacitación** del personal.

Gestión de riesgos financieros

Los **riesgos financieros** afectan directamente la **liquidez**, la **rentabilidad** y la **estabilidad financiera** de la organización. Esto incluye riesgos de tipo de cambio, fluctuaciones en los mercados financieros, incumplimiento de obligaciones y cambios en las tasas de interés. Las empresas deben implementar **políticas de cobertura**, **análisis financiero** riguroso y **monitoreo constante** del entorno económico para **mitigar estos riesgos**.

Gestión de riesgos estratégicos

Los **riesgos estratégicos** surgen de **decisiones de largo plazo** que pueden **afectar** el **crecimiento** y la **dirección** de la empresa. Estos riesgos incluyen la entrada a nuevos mercados, fusiones y adquisiciones, y cambios en las estrategias de productos. La gestión de riesgos estratégicos requiere una **evaluación profunda de las oportunidades y amenazas**, así como **planes de contingencia** para adaptarse a cambios inesperados en el entorno.

Gestión de riesgos de cumplimiento

Los **riesgos de cumplimiento** se refieren a la posibilidad de que una empresa **infrinja normativas legales** o **regulaciones específicas** de la industria. El incumplimiento normativo puede derivar en sanciones, multas o pérdida de reputación.

¿Qué son los riesgos financieros y cómo gestionarlos eficazmente?

Los **riesgos financieros** son aquellos que afectan la estabilidad económica y el rendimiento de una empresa. Estos riesgos pueden surgir de fluctuaciones en los mercados, problemas de liquidez, cambios en las tasas de interés, incumplimientos crediticios o factores macroeconómicos que pueden poner en peligro la capacidad de una organización para generar ingresos. Gestionar eficazmente estos riesgos es clave para asegurar la supervivencia y el crecimiento de una empresa en un entorno financiero cada vez más volátil.

En este post, analizaremos en detalle qué son los **riesgos financieros**, por qué es fundamental gestionarlos y qué estrategias puedes implementar para mitigar su impacto.

¿Qué son los riesgos financieros?

Los **riesgos financieros** se refieren a la posibilidad de pérdidas económicas debido a factores internos o externos que afectan

a la salud financiera de una organización. Estos riesgos pueden manifestarse de diversas formas y afectar diferentes áreas del negocio, desde la rentabilidad hasta la capacidad de financiación.

Algunos de los principales **riesgos financieros** son:

- **Riesgo de mercado**: La exposición a fluctuaciones en los precios de los activos, tipos de cambio o tasas de interés que pueden afectar el valor de las inversiones de la empresa.

- **Riesgo de crédito**: La posibilidad de que un cliente o socio comercial no cumpla con sus obligaciones de pago, lo que puede generar pérdidas significativas.

- **Riesgo de liquidez**: La incapacidad de la empresa para cumplir con sus obligaciones financieras a corto plazo debido a la falta de recursos líquidos.

- **Riesgo operacional**: Aunque se asocia con los procesos internos de la empresa, un fallo operativo puede generar un impacto financiero directo, por ejemplo, a través de multas o pérdidas de negocio.

Estos riesgos no solo afectan el desempeño financiero de la empresa, sino que también pueden impactar su reputación, acceso a crédito y estabilidad a largo plazo.

¿Cómo gestionar eficazmente los riesgos financieros?

Para gestionar los **riesgos financieros** de manera eficaz, es fundamental implementar una estrategia de **gestión integral de riesgos.**

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO

Cómo ISO 14971 ayuda en la gestión de riesgos en dispositivos médicos

La seguridad y eficacia de los dispositivos médicos es una prioridad tanto para los fabricantes como para los reguladores, y es en este contexto donde la norma **ISO 14971** juega un papel crucial. Esta norma internacional proporciona un marco para la **gestión integral de riesgos** en todas las etapas del ciclo de vida de los dispositivos médicos, desde el diseño hasta la comercialización. Cumplir con la **ISO 14971** no solo es un requisito regulatorio en muchos países, sino que también es una práctica esencial para asegurar la calidad y la seguridad del producto.

En este artículo, exploraremos cómo la **ISO 14971** ayuda en la **gestión de riesgos** asociados a los dispositivos médicos, qué beneficios ofrece y cómo implementar un sistema eficaz para minimizar los riesgos.

¿Qué es la ISO 14971?

La **ISO 14971** es una norma internacional desarrollada específicamente para la gestión de riesgos en el diseño, desarrollo y fabricación de dispositivos médicos. Establece un proceso sistemático para identificar, evaluar y controlar los riesgos asociados al uso de estos dispositivos, con el objetivo de garantizar la seguridad del paciente, así como el cumplimiento de las regulaciones aplicables en el sector médico.

La norma también exige una evaluación continua de los riesgos durante todo el ciclo de vida del dispositivo, lo que asegura que cualquier cambio o mejora en el producto sea evaluado desde la perspectiva de la seguridad.

Principios clave de la gestión de riesgos según ISO 14971

La **ISO 14971** se basa en una serie de principios clave que deben seguirse para gestionar eficazmente los riesgos relacionados con los dispositivos médicos. Estos principios garantizan que el enfoque de **gestión de riesgos** esté alineado con las mejores prácticas de la industria y las regulaciones internacionales.

Algunos de los principios clave incluyen:

- **Identificación de riesgos**: La identificación exhaustiva de todos los posibles riesgos relacionados con el uso del dispositivo médico, desde su diseño inicial hasta su utilización en entornos clínicos.

- **Evaluación del riesgo**: Cada riesgo identificado debe ser evaluado en términos de su **probabilidad de ocurrencia** y su **impacto potencial** en la seguridad del paciente.

¿Qué significa DORA? Explorando la resiliencia operativa en el contexto financiero

La resiliencia operativa es primordial para el sector de las finanzas global, especialmente en un entorno donde los riesgos financieros digitales, como ciberataques y amenazas tecnológicas, son cada vez más frecuentes y cuenta con más sofisticación. La Unión Europea ha implementado el **Reglamento de Resiliencia Operativa Digital** (conocido como **DORA**, por sus siglas en inglés: Digital Operational Resilience Act), que establece un reglamento integral para garantizar la capacidad de las instituciones financieras de prever, resistir, recuperarse y adaptarse a incidentes operativos y tecnológicos.

DORA

DORA es una respuesta directa a la creciente dependencia de la tecnología en el sector financiero y a la necesidad de fortalecer la **resiliencia digital** para mitigar cualquier interrupción que pudiera afectar la estabilidad financiera. Con el objetivo de proteger a los consumidores y garantizar la continuidad de los servicios financieros críticos, DORA introduce una serie de **requisitos obligatorios para todas las entidades reguladas**, desde bancos y aseguradoras hasta proveedores de infraestructura tecnológica.

Principales componentes de DORA

Para cumplir con sus objetivos, DORA se centra en cinco áreas clave que las instituciones financieras deben gestionar de manera rigurosa:

- **Gestión de riesgos tecnológicos y digitales**: Las entidades deben implementar un sistema óptimo de gestión de riesgos que cubra desde la ciberseguridad hasta la continuidad de negocio. Esto incluye la identificación de los activos digitales críticos, la evaluación constante de amenazas y la aplicación de controles y medidas de mitigación.

- **Pruebas de resiliencia operativa**: Uno de los requisitos más destacados de DORA es la realización de pruebas periódicas de resiliencia operativa, que permiten a las organizaciones evaluar la efectividad de sus sistemas en entornos simulados de alta presión. Estas pruebas incluyen desde ejercicios de ciberseguridad hasta simulaciones de escenarios de interrupción tecnológica.

Claves para un sistema de gestión integral de riesgos exitoso

En un entorno empresarial cada vez más complejo, la **gestión de riesgos** se ha convertido en un aspecto crucial para **asegurar la continuidad y el crecimiento** de las organizaciones. Un **sistema de gestión integral de riesgos** (SGIR) permite a las empresas identificar, evaluar y mitigar riesgos potenciales, garantizando así una **toma de decisiones informada** y fundamentada. En este artículo, exploraremos las claves para implementar un SGIR exitoso.

Sistema de gestión integral de riesgos

La **gestión de riesgos** es un proceso sistemático que permite a las organizaciones **anticiparse a** posibles **eventos adversos**. La importancia de contar con un SGIR radica en varios factores:

- Implementar un SGIR efectivo ayuda a **minimizar** las **pérdidas financieras** y **operativas**. Al identificar y evaluar los riesgos, las empresas pueden desarrollar **estrategias para mitigar su impacto** y, en última instancia, proteger sus activos.

- Un SGIR proporciona información valiosa que permite a los líderes empresariales **tomar decisiones más informadas**. Con una comprensión clara de los riesgos, se pueden **priorizar iniciativas** y **asignar recursos** de manera más efectiva.

- Las organizaciones operan bajo un **marco normativo cada vez más riguroso**. Un SGIR bien implementado asegura el cumplimiento de leyes y regulaciones, **reduciendo** así la exposición a **sanciones y repercusiones legales**.

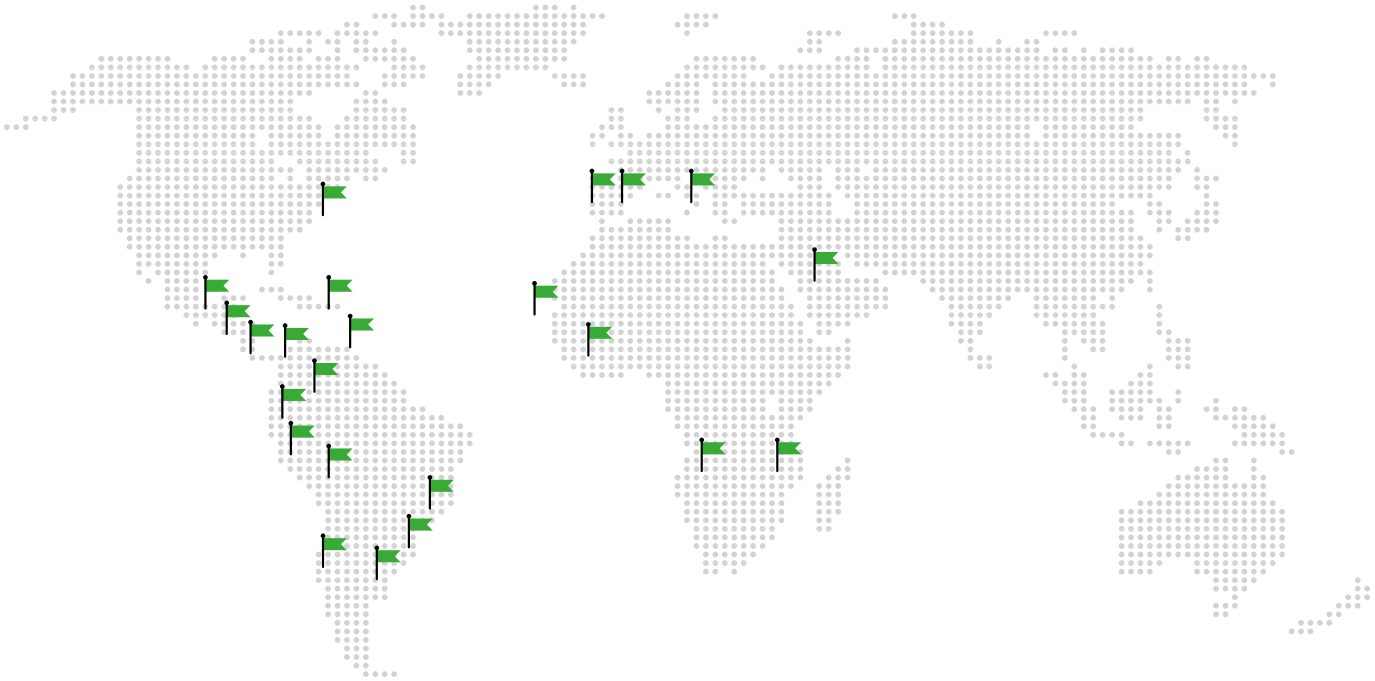
Claves para un Sistema de Gestión Integral de Riesgos exitoso

Compromiso de la alta dirección

- El **compromiso de la alta dirección** es fundamental para el éxito de cualquier SGIR. Sin el apoyo y liderazgo de los directivos, las iniciativas de **gestión de riesgos pueden carecer de recursos y relevancia**. Para fomentar este compromiso:

- **Definir una cultura de riesgos**: La alta dirección debe promover una cultura organizacional que valore la gestión de riesgos como un componente clave en la estrategia empresarial.

- **Asignar recursos adecuados**: Es esencial destinar los recursos necesarios, tanto humanos como financieros, para la implementación efectiva del SGIR.



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