EMPRESA **EXCELENTE**

Las mejores temáticas sobre Normas ISO, HSE y GRC

2024

DICIEMBRE

ESGinnova Group

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

Índice

Índice

Índice

ESG Innova Group

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

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

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

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

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

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

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

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

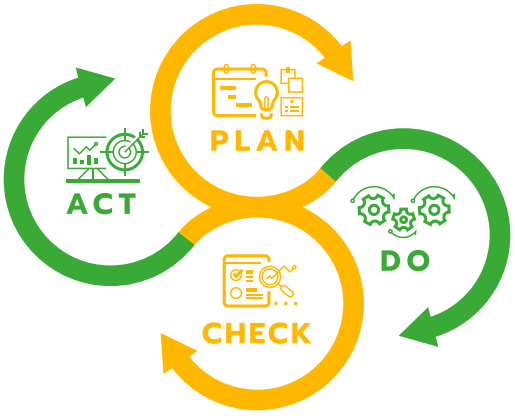
Plataforma ESG Innova

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

❖ Motor de mejora continua

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

ESGinnova Group



❖ Plan

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

❖ Do

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

❖ Check

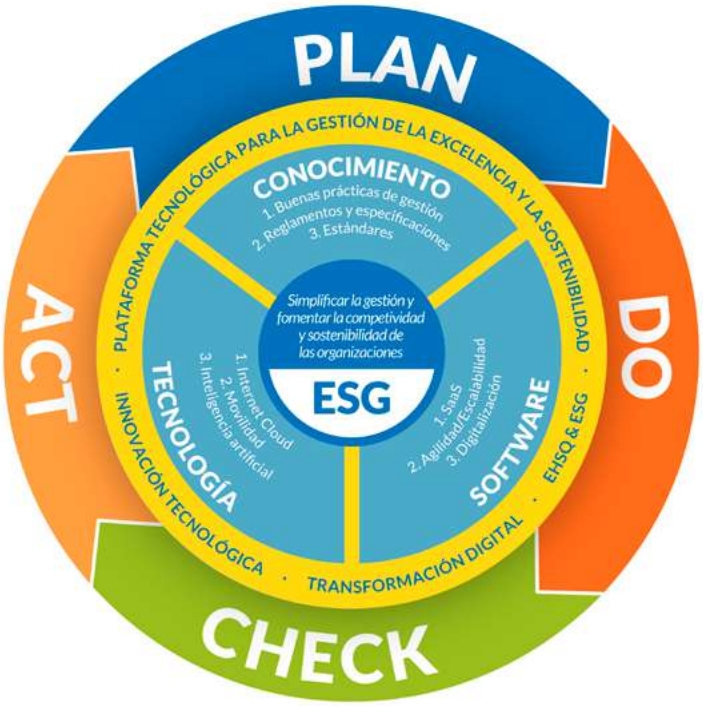
Simplificamos la monitorización y seguimiento, aportando información útil para la toma de decisiones.

❖ Act

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

Unidades de negocio

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



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

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

Unidades de negocio

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

ISOTools

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

HSETools

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

GRCTools

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

La Plataforma ESG aporta resultados en el corto plazo

Optimización del tiempo

50%
Menos de tiempo de resolución de una acción correctiva

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

75%
Menos de tiempo dedicado a recopilar y tratar indicadores

Optimización de los costes

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

75%
Menos de costes indirectos derivados de la gestión documental

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

Optimización del rendimiento

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

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

100%
Más de trabajadores implicados en la gestión del sistema

ESGinnova Group

ISOTools

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

Importancia del cumplimiento de ISO/IEC 27017

La **seguridad de la información** en la nube es esencial, esto es un imperativo para cualquier empresa. Es por ello que el cumplimiento con la norma ISO/IEC 27017 es en una prioridad para las empresas que manejan datos sensibles en entornos virtuales. Esta normativa complementa la **ISO/IEC 27001**, ya que proporciona controles específicos para reforzar la seguridad en los servicios de computación en la nube, tanto para proveedores como para clientes.

¿Qué es la ISO/IEC 27017?

La norma ISO 27017 establece las mejores prácticas diseñadas para reducir los riesgos en entornos de nube.

Incluye controles adicionales a los definidos en la **ISO 27002**, adaptados a los desafíos específicos de la computación en la nube, como:

- Protección de **datos sensibles** en tránsito y almacenamiento.

- Gestión de responsabilidades entre proveedores y clientes de **servicios en la nube**.

- **Auditorías y control de acceso** en infraestructuras virtuales.

¿Por qué es crucial su cumplimiento?

Cumplir con esta norma es clave para las empresas que quieran garantizar la confianza de sus clientes y socios comerciales. Entre los beneficios de su cumplimiento se encuentran:

- **Reducción de riesgos cibernéticos**: con la implementación de controles específicos, las empresas previenen brechas de seguridad que pueden comprometer datos críticos.

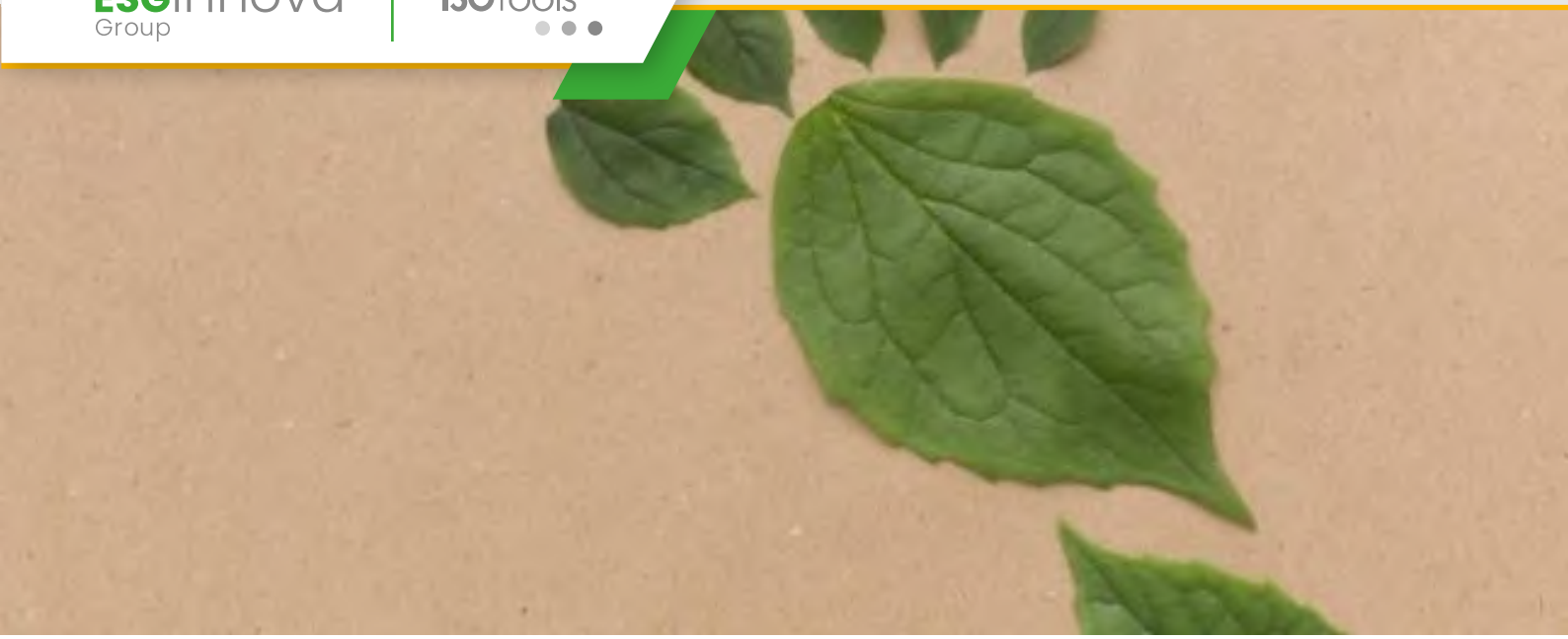
- **Cumplimiento legal y normativo**: ciertas legislaciones y marcos globales exigen estándares elevados de seguridad, donde la norma ISO/IEC 27017 actúa como garantía de conformidad.

- **Ventaja competitiva**: certificar el cumplimiento de ISO 27017 demuestra un compromiso con la excelencia en la **gestión de la seguridad de la información**, lo que fortalece la reputación empresarial.

- **Claridad en el rol y las responsabilidades**: ayuda a establecer acuerdos claros entre las partes involucradas en el uso de servicios en la nube, reduciendo los posibles conflictos y malentendidos.

El Rol de ISOTools en la Implementación

Para las empresas, independientemente de su tamaño o sector, adoptar y mantener la conformidad con ISO/IEC 27017 es un proceso desafiante.



Descubre la ISO 14067 vinculada a la sostenibilidad

La **sostenibilidad** es un tema que ha ganado una enorme relevancia en los últimos años, especialmente en el ámbito empresarial. Las empresas se encuentran ante la creciente demanda de integrar prácticas responsables que contribuyan a la protección del **medio ambiente**, y que también mejoren su **competitividad** y **reputación**. Un escenario fundamental para medir y reducir el impacto ambiental de los productos es la **ISO 14067**, una norma internacional que proporciona las directrices necesarias para calcular y comunicar **la huella de carbono** de un producto, ayudando a las organizaciones a implementar prácticas sostenibles.

Para ello, exploraremos en profundidad qué es la ISO 14067, su vinculación con la sostenibilidad, y cómo las empresas pueden beneficiarse de su implementación, especialmente cuando se apoya con soluciones tecnológicas como las que ofrece **ISOTools**, una plataforma tecnológica líder en gestión de normas ISO.

¿Qué es la ISO 14067?

La **ISO 14067** es una **norma internacional que establece los requisitos para el cálculo y la comunicación de la huella de carbono de los productos**. Se enfoca en medir las emisiones de gases de efecto invernadero (**GEI**) asociadas a las fases de ciclo de vida de un producto, desde su producción hasta su disposición final. La norma está diseñada para ayudar a las organizaciones a evaluar su impacto climático y a tomar decisiones informadas sobre cómo reducirlo.

La huella de carbono en el contexto de la sostenibilidad

La huella de carbono es un indicador clave del impacto ambiental de un producto. La **ISO 14067** permite a las empresas cuantificar la cantidad de **CO_2** y otros gases de efecto invernadero que se emiten en el ciclo de vida de sus productos, lo que les proporciona una base para implementar **estrategias de reducción de emisiones**. Esta norma es esencial para las empresas que buscan ser más sostenibles, ya que la medición precisa de la huella de carbono es el primer paso hacia la **mejora continua**.

La sostenibilidad, hoy en día, no solo está ligada a la protección del medio ambiente, sino también a la competitividad y la reputación de las organizaciones. Los consumidores, reguladores y otras partes interesadas están exigiendo cada vez más **productos con menores impactos ambientales**. Al adoptar la **ISO 14067**, las empresas pueden demostrar su compromiso con la sostenibilidad, aumentar su credibilidad y, a la vez, cumplir con las normativas y regulaciones medioambientales internacionales.

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO

¿Qué es la Norma ISO 14030?

ISO 14030

Equilibrar la rentabilidad empresarial y la sostenibilidad por parte de las organizaciones no es tarea fácil. Por el contrario, supone todo un desafío. Con ello, la **Norma ISO 14030** emerge como una herramienta que impulsa inversiones verdes y proyectos sostenibles. Pero, ¿qué es exactamente esta norma y por qué está ganando relevancia en la actualidad?

Una guía para las finanzas sostenibles

La ISO 14030 es una norma internacional desarrollada por la Organización Internacional de Normalización (ISO) que establece criterios para evaluar y etiquetar proyectos de inversión como sostenibles desde el punto de vista ambiental.

Se centra, sobre todo en los **bonos verdes**, ofreciendo un marco estándar para garantizar que los fondos que se recaudan se empleen en iniciativas alineadas con objetivos medioambientales específicos, como la reducción del **cambio climático** o la conservación de los recursos naturales.

Principales objetivos de la norma

El objetivo de la norma ISO 14030 es **fomentar la transparencia y la confianza** en los mercados financieros sostenibles. Entre sus objetivos se pueden señalar:

- **Definir proyectos sostenibles**: identificar qué acciones se consideran "verdes" y cómo deben evaluarse.
- **Hacer un estándar para los procesos**: establecer estándares claros para la emisión, seguimiento y verificación de bonos verdes.
- **Reducir el riesgo de caer en greenwashing**: proteger a los inversores y al mercado de falsas afirmaciones sobre sostenibilidad.

Estructura de la ISO 14030

La norma está dividida en varias partes, que abordan diferentes **aspectos de las finanzas sostenibles**, tales como:

- **Criterios de sostenibilidad**: parámetros técnicos y científicos para evaluar el impacto ambiental.
- **Gestión de datos y reportes**: directrices sobre cómo comunicar el uso de los fondos y los resultados obtenidos.
- **Auditoría y certificación**: requisitos para garantizar la objetividad y credibilidad de las evaluaciones.

Sistema de Gestión de Inteligencia Artificial (SGIA): 10 cuestiones clave

La publicación de ISO 42001, estándar para un **Sistema de Gestión de Inteligencia Artificial** (SGIA), marca un nuevo rumbo para las organizaciones cada vez más numerosas que desarrollan o hacen uso de esta revolucionaria tecnología.

ISO 42001:2023 es el primer estándar que **entrega requisitos y directrices para planificar, implementar, auditar, mejorar de forma continua y mantener un Sistema de Gestión de Inteligencia Artificial**. Es válido para organizaciones de todos los tamaños, todas las complejidades y todas las industrias posibles, siempre que desarrollen productos con base en la IA o hagan uso de esa tecnología.

Es una primera cuestión interesante en este estándar. La mayoría de las normas ISO están diseñadas para todo tipo de empresas. En la definición de **alcance de ISO 42001** así se advierte, pero **en la práctica se limita a las organizaciones que tienen una**

interacción directa con IA. De otra forma no se explica la necesidad de construir un Sistema de Gestión de Inteligencia Artificial.

Aspectos clave en ISO 42001, estándar para un Sistema de Gestión de Inteligencia Artificial

La Inteligencia Artificial es el desarrollo más importante realizado hasta ahora, pero también es controvertido. Una de las razones para crear un estándar para Sistema de Gestión de Inteligencia Artificial es, precisamente, **generar un marco de trabajo en el que se puedan gestionar con eficacia los riesgos**, entre ellos, por supuesto, los que tantas dudas despiertan.

ISO 42001:2023, estándar para este tipo de sistemas de gestión, por su reciente publicación también está acompañado de ciertas dudas. Son las que buscamos aclarar al responder **diez preguntas clave sobre la nueva norma para un Sistema de Gestión de Inteligencia Artificial.**

1. Para quién se ha creado ISO 42001:2023

ISO 42001 se ha diseñado para ser utilizado por **cualquier tipo de empresa, en cualquier lugar del mundo, siempre que cree, genere o produzca Inteligencia Artificial** o haga uso de ella para producir algún bien o servicio.

2. Qué elementos conforman la norma ISO 42001:2023

ISO 42001 es un estándar construido sobre la estructura de Alto Nivel utilizada por las normas ISO más populares, como ISO 9001, ISO 45001 e **ISO 27001**.

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO

ISO 37101: Sistemas de Gestión para el Desarrollo Sostenible en Comunidades

La norma ISO 37101 establece un marco estratégico para que las comunidades, ya sean ciudades, regiones o localidades, desarrollen **prácticas sostenibles** que impulsen su resiliencia, sostenibilidad y bienestar. Con un enfoque integrador, esta norma fomenta la **alineación de los objetivos de desarrollo sostenible** (ODS) de las Naciones Unidas con las necesidades y prioridades locales.

En este artículo, exploraremos qué es la **ISO 37101**, sus beneficios, los pasos clave para implementarla y cómo contribuye al desarrollo sostenible.

ISO 37101

La **ISO 37101** es una norma internacional que proporciona directrices para la **implementación** de un **sistema de gestión sostenible en comunidades**.

Su objetivo principal es **mejorar la sostenibilidad** de las comunidades **y aumentar** su **capacidad** para **afrontar desafíos globales** como el cambio climático, la urbanización y la pérdida de biodiversidad.

Objetivos principales de la ISO 37101:

- **Promover la sostenibilidad:** Fomentar un equilibrio entre las necesidades económicas, sociales y ambientales.
- **Incrementar la resiliencia:** Ayudar a las comunidades a adaptarse y recuperarse frente a crisis y adversidades.
- **Fortalecer la identidad local:** Respetar y potenciar la cultura y el patrimonio de la comunidad.
- **Mejorar la calidad de vida:** Establecer condiciones para un bienestar integral de los ciudadanos.

Beneficios de implementar la ISO 37101

Adoptar la **ISO 37101** no solo **genera ventajas** en términos de **sostenibilidad**, sino que también aporta **beneficios** concretos a las comunidades y sus habitantes.

Mejora de la planificación estratégica

La norma fomenta un enfoque estructurado para planificar el **desarrollo sostenible**, asegurando que las **decisiones estén alineadas** con las prioridades comunitarias y los ODS.

Guía completa de la norma ISO 21001:2018

La calidad educativa es un aspecto fundamental en el desarrollo de individuos y organizaciones. La norma ISO 21001:2018 surge como una herramienta clave para mejorar los sistemas de gestión de las organizaciones educativas, permitiendo alinear los procesos con las necesidades de los estudiantes y otras partes interesadas. En este artículo, exploraremos en profundidad los principios, beneficios y etapas de implementación de la **ISO 21001**, así como su aplicación en el sector empresarial y cómo el **Software ISOTools** puede facilitar este proceso.

¿Qué es la norma ISO 21001:2018?

La **ISO 21001:2018** es una norma internacional diseñada para establecer un **Sistema de Gestión de Organizaciones Educativas (EOMS)**. Esta norma está basada en la estructura de la **ISO 9001** y se centra en mejorar la calidad de los procesos educativos, satisfaciendo las expectativas y necesidades de los estudiantes y otras partes interesadas.

Su objetivo principal es promover la **educación inclusiva, equitativa y de calidad**, con un enfoque en el aprendizaje continuo y la mejora constante.

Principios fundamentales de la ISO 21001:2018

La norma ISO 21001 se estructura en torno a una serie de principios que guían su implementación:

- **Enfoque en los estudiantes y otras partes interesadas**: Garantizar que las necesidades de los estudiantes y demás actores educativos sean la prioridad.
- **Responsabilidad social**: Fomentar la educación inclusiva y equitativa.
- **Accesibilidad e igualdad**: Eliminar barreras y garantizar igualdad de oportunidades.
- **Aprendizaje continuo**: Promover el desarrollo sostenible a través del aprendizaje permanente.
- **Innovación y mejora continua**: Optimizar los procesos educativos con el objetivo de alcanzar la excelencia.
- **Gestión basada en evidencia**: Tomar decisiones informadas y fundamentadas en datos.

Ley de Ciberresiliencia de la UE: nuevo hito en la Ciberseguridad Europea

La Ley de Ciberresiliencia (CRA, por sus iniciales en inglés) es la obligación regulatoria y legal más reciente en el campo de la **seguridad de la información**, la ciberseguridad y la protección de los usuarios de productos digitales en la Unión Europea.

La Ley de Ciberresiliencia marca un hito en el camino hacia la **seguridad de los usuarios de dispositivos o productos que se conectan de forma directa o indirecta a una red** o que lo hacen a través de otro dispositivo. Las obligaciones que impone la nueva ley se aplican a fabricantes y minoristas.

Cuáles son las novedades de la Ley de Ciberresiliencia

La nueva Ley de Ciberresiliencia **introduce normas estandarizadas** para regularizar la llegada al mercado de todo tipo de productos o dispositivos que estén dotados con software o cualquier otro tipo de componentes digitales.

La ley también **crea un marco para reglamentar la producción de dispositivos o productos** que cumplan con las condiciones determinadas, en cada una de las etapas de la cadena de valor y en cada momento desde el diseño hasta la distribución, pasando por la planificación y la producción.

Los fabricantes tendrán la obligación de cumplir con lo ordenado por la Ley de Ciberresiliencia antes de 2027. Los productos que lo hagan **exhibirán la marca CE como demostración del cumplimiento**. Los consumidores tendrán así un nuevo elemento útil para la toma de decisiones informadas en un escenario en el que la concienciación sobre seguridad de la información es cada vez mayor.

Cuál es el origen de la Ley de Ciberresiliencia de la UE

La Ley de Ciberresiliencia tiene su origen en la Estrategia de Ciberseguridad de la UE de 2020. La estrategia, creada por la Agencia de la UE para la Ciberseguridad, busca **estandarizar la ciberseguridad en la Unión Europea**, inicialmente en servicios esenciales como medios de transporte, servicios sanitarios, redes de transmisión de energía y telecomunicaciones.

Después, la estrategia aborda los **dispositivos y objetos interconectados de uso común en hogares y oficinas**. Y es en este punto en donde aparece la Ley de Ciberresiliencia de la UE, que se publica el 20 de noviembre de 2024. El 10 de diciembre de 2024 se inicia un programa de entrada en vigor escalonado que culminará en 2027 y que contempla la obligación de presentar informes para los fabricantes.

¿Qué es la norma ISO 19011 y para qué sirve?

ISO 19011

La norma ISO 19011 es una guía internacional que proporciona directrices para la auditoría de sistemas de gestión. Su principal objetivo es establecer un marco común para facilitar la realización de auditorías internas y externas de forma eficiente, sistemática y efectiva. Publicada por la Organización Internacional de Normalización (ISO), esta norma es clave para garantizar que los sistemas de gestión cumplan con los requisitos establecidos, identifiquen áreas de mejora y promuevan la excelencia empresarial.

¿Cuáles son los objetivos de la norma ISO 19011?

ISO 19011 tiene como principal objetivo ayudar a las empresas a planificar y hacer auditorías que generen valor.

Entre sus objetivos más destacados se pueden destacar los siguientes:

- **Proveer directrices claras**: la norma ISO 19011 establece los principios y los pasos necesarios para hacer auditorías coherentes y efectivas.

- **Fomento de la mejora continua**: al realizar auditorías adecuadas, se pueden identificar oportunidades para optimizar procesos y sistemas empresariales.

- **Promoción de la confianza**: este estándar ayuda a garantizar que los sistemas de gestión generen confianza y cumplan con los requisitos normativos y de la organización.

¿En qué ámbitos se aplica ISO 19011?

Aunque ISO 19011 se centra fundamentalmente en las **auditorías de sistemas de gestión**, su aplicación abarca diversos ámbitos, como son:

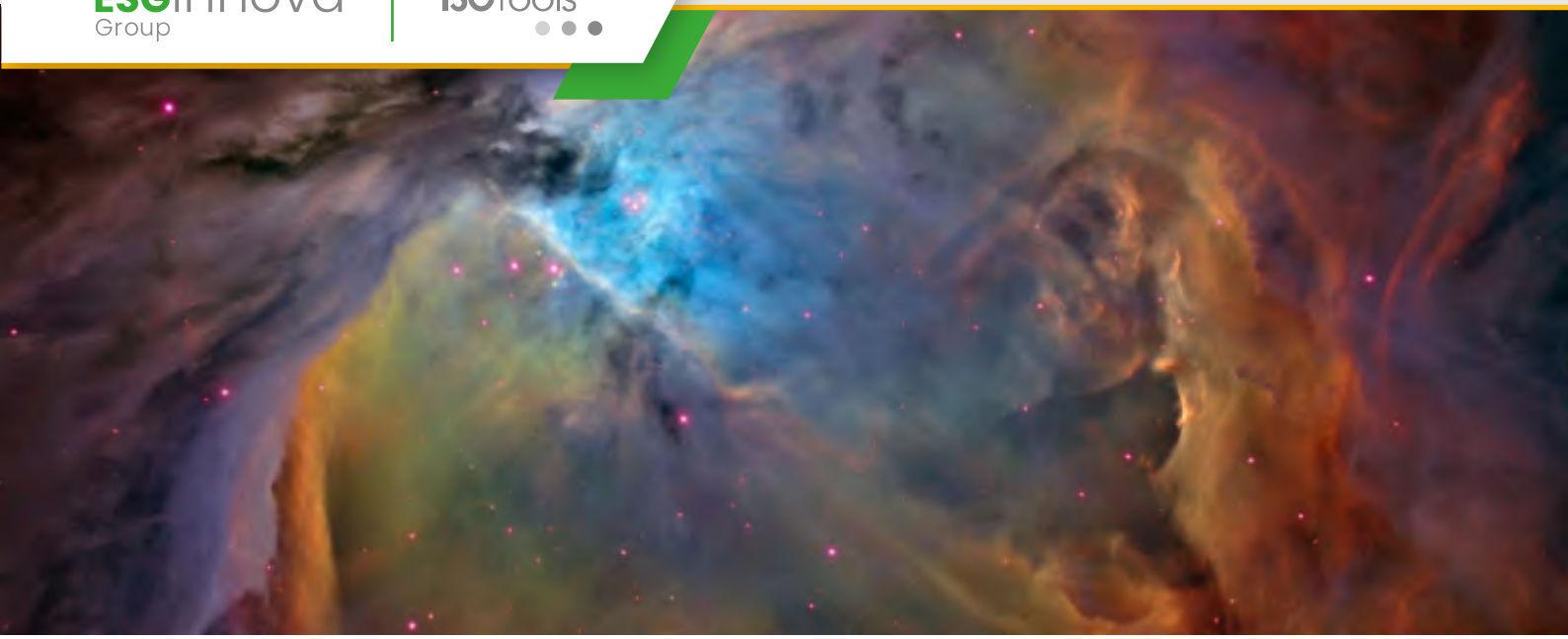
- Sistemas de gestión de calidad (**ISO 9001**).

- Sistemas de gestión ambiental (**ISO 14001**).

- Sistemas de gestión de la seguridad y salud en el trabajo (**ISO 45001**).

- Sistemas de gestión de la seguridad de la información (**ISO 27001**).

Es importante tener en cuenta que esta norma es útil tanto para empresas que llevan a cabo **auditorías internas** como para aquellas otras que contratan servicios externos de auditoría.



¿Qué es la norma ISO 14064 sobre gases de efecto invernadero?

La ISO 14064 es una norma internacional que proporciona un marco para **medir, cuantificar y reportar las emisiones y reducciones de gases de efecto invernadero** (GEI). Este estándar es fundamental para organizaciones que buscan gestionar su **impacto ambiental** y contribuir a la mitigación del **cambio climático**.

A continuación, exploraremos en detalle qué es la **ISO 14064**, sus beneficios, las claves para su implementación y su importancia en el contexto empresarial actual.

ISO 14064

La **ISO 14064** es parte de la familia de normas ISO relacionadas con la **gestión ambiental**. Esta norma se centra específicamente en los gases de efecto invernadero y está estructurada en tres partes principales:

ISO 14064-1

Define los principios y requisitos para la **cuantificación y reporte de las emisiones de GEI**. Este apartado es aplicable a organizaciones que **desean medir y gestionar** su huella de carbono.

ISO 14064-2

Proporciona directrices para la **cuantificación, monitoreo y reporte** de actividades de reducción de emisiones y **mejora** de los sumideros de carbono.

ISO 14064-3

Establece los **requisitos para la validación y verificación** de las declaraciones relacionadas con los GEI.

Beneficios de implementar la ISO 14064

Adoptar la norma ofrece una serie de **beneficios estratégicos**, tanto para las organizaciones como para el medio ambiente:

- **Gestión precisa de las emisiones:** La norma permite identificar y cuantificar las fuentes de emisión de GEI, lo que facilita el diseño de estrategias para reducirlas.
- **Cumplimiento normativo:** Ayuda a las empresas a alinearse con las regulaciones nacionales e internacionales sobre cambio climático, **evitando sanciones y mejorando su reputación**.
- **Acceso a mercados de carbono:** Las organizaciones que **implementan la ISO 14064** participan en mercados.

Norma ISO 27011:2024 Seguridad de la Información para empresas de telecomunicaciones

La era digital ha transformado por completo la manera en que vivimos, trabajamos y nos comunicamos. En este escenario, las empresas de telecomunicaciones desempeñan un rol clave, siendo el puente que conecta a personas y organizaciones a nivel global. Sin embargo, esta misma posición estratégica las convierte en objetivos recurrentes de **ciberamenazas avanzadas**, poniendo en riesgo sus operaciones y la confianza de millones de usuarios que dependen de sus servicios.

Ante este desafío, la norma **ISO 27011:2024** se presenta como una solución fundamental. Diseñada específicamente para el sector de telecomunicaciones, esta norma proporciona un marco robusto para fortalecer la **seguridad de la información**, proteger infraestructuras críticas y garantizar la continuidad del negocio en un entorno cada vez más complejo.

¿Qué es la norma ISO 27011:2024?

La norma **ISO/IEC 27011:2024** es una norma internacional desarrollada como una extensión de la **ISO/IEC 27001**, enfocada en los **operadores de telecomunicaciones** y en todas las organizaciones que brindan servicios de comunicación. Esta norma proporciona directrices específicas para la aplicación de un **Sistema de Gestión de Seguridad de la Información (SGSI)** en un sector clave para la infraestructura global.

El objetivo principal de la ISO 27011 es **proteger la confidencialidad, integridad y disponibilidad de la información** dentro de las redes y servicios de telecomunicaciones. Las empresas en este sector se enfrentan a riesgos únicos, como el incremento de los **ciberataques**, la interceptación de datos y la vulnerabilidad de la infraestructura crítica, lo que hace indispensable contar con un marco normativo adaptado.

Importancia de la ISO 27011 en el Sector Telecomunicaciones

Las telecomunicaciones son la columna vertebral de la sociedad digital actual. Empresas y usuarios dependen de servicios seguros y fiables, lo que convierte a las organizaciones del sector en objetivos prioritarios de las ciberamenazas. Además, la evolución de tecnologías como **5G**, el **Internet de las Cosas (IoT)** y la computación en la **nube** han multiplicado los riesgos y las vulnerabilidades.

Entre los problemas que enfrentan las empresas están:

- **Ciberataques a infraestructuras críticas** que pueden paralizar servicios esenciales.

Integración de la ISO 45001 con Otros Sistemas de Gestión: Calidad, Medio Ambiente y Seguridad Informática

Integración de la ISO 45001 con Otros Sistemas de Gestión

En entornos de alta competencia las empresas siempre buscan optimizar sus procesos con la implementación de sistemas de gestión basados en normas internacionales. Entre estos, la integración de la norma ISO 45001, orientada a la seguridad y salud en el trabajo, con otros sistemas como la norma ISO 9001 (Calidad), la ISO 14001 (Medio Ambiente) e ISO 27001 (Seguridad de la Información), se presenta como una estrategia clave para lograr eficiencia, coherencia y mejores resultados.

Beneficios de la Integración de Sistemas de Gestión

La integración de estos sistemas ofrece **numerosos beneficios**, entre los que sobresalen los siguientes:

- **Mayor eficiencia operativa:** evita que los esfuerzos se dupliquen y establece una serie de procesos unificados lo que permite ahorrar tiempo y recursos.
- **Visión holística de la empresa:** facilita la gestión de forma simultánea de aspectos clave como la **calidad**, la sostenibilidad, la seguridad laboral y la protección de datos.
- **Cumplimiento normativo simplificado:** al alinear los requisitos de diferentes normas, las auditorías y los controles se vuelven más eficientes.
- **Mejora continua coordinada:** promueve un enfoque integrado para identificar riesgos, oportunidades y áreas de mejora en todos los sistemas integrados.

Puntos Clave para una Integración Exitosa

Estructura basada en el Anexo SL

Las normas ISO actuales, como pueden ser la ISO 45001, ISO 9001, ISO 14001 e ISO 27001, comparten una estructura común conocida como **Anexo SL**. Esto facilita su integración al usar términos, definiciones y requisitos compatibles, como el contexto de la organización, la gestión del riesgo y la mejora continua.

Pasos Fundamentales para la Implementación de la Norma ISO 45001 en tu Empresa

La Norma ISO 45001 es un estándar internacional que establece **requisitos para la implementación de un Sistema de Gestión de Seguridad y Salud en el Trabajo** (SST). Su objetivo principal es **mejorar la seguridad laboral**, **reducir los riesgos** y crear un **entorno** de trabajo **más saludable y seguro** para todos los empleados.

En este artículo, exploraremos los **pasos fundamentales** para implementar la **ISO 45001** en tu empresa, destacando sus **beneficios y los retos asociados**. Además, hablaremos sobre cómo el **Software ISO 45001 de ISOTools** puede facilitar este proceso.

Implementación de la Norma ISO 45001

La **ISO 45001** es una norma que proporciona un marco para que las organizaciones **identifiquen, controlen y reduzcan los riesgos laborales**.

Está diseñada para ser compatible con otras normas de gestión, como la **ISO 9001** y la **ISO 14001**, facilitando la integración de sistemas.

Beneficios de la implementación:

Implementar la norma **ISO 45001** ofrece múltiples **beneficios**:

- **Reducción de riesgos laborales**, disminuyendo accidentes y enfermedades en el lugar de trabajo.
- **Cumplimiento normativo**, asegurando que la organización cumpla con las leyes y regulaciones locales e internacionales.
- **Mejora continua**, fomentando la optimización constante de los procesos relacionados con la seguridad y salud ocupacional.
- **Mayor compromiso del personal**, creando una cultura de seguridad proactiva dentro de la empresa.

Pasos para la implementación de la Norma ISO 45001

La implementación de la **ISO 45001** requiere **planificación y compromiso** por parte de toda la organización. Aquí te presentamos los pasos clave.

1. Compromiso de la alta dirección

El primer paso para implementar la **ISO 45001** es garantizar el **compromiso de la alta dirección**. Este liderazgo es crucial para establecer una **cultura de seguridad sólida** y proporcionar los recursos necesarios para el proyecto.

Mejora Continua en la ISO 9001: Implementación de Acciones Correctivas y Preventivas

La Mejora Continua es el corazón de la norma **ISO 9001** y una pieza clave en cualquier **Sistema de Gestión de la Calidad (SGC)**. Las organizaciones deben centrarse en optimizar sus procesos, eliminar no conformidades y prevenir problemas antes de que sucedan. Para lograrlo, la implementación de **acciones correctivas y preventivas** se convierte en un paso imprescindible.

Es importante profundizar en qué son las acciones correctivas y preventivas dentro de la ISO 9001, cómo implementarlas y, especialmente, cómo el uso de un **Software ISO 9001**, como el de **ISOTools**, puede potenciar la mejora continua y llevar a las empresas hacia un éxito sostenible.

¿Qué es la Mejora Continua en la ISO 9001?

La mejora continua es un **proceso iterativo** que permite optimizar de manera constante los procesos, productos y servicios de una organización. Basada en el ciclo **PHVA** *(Planificar – Hacer – Verificar – Actuar),* esta filosofía impulsa a las organizaciones a adaptarse y evolucionar para alcanzar sus objetivos de calidad.

La ISO 9001:2015 exige que las organizaciones no solo solucionen los problemas cuando ocurren, sino que también tomen medidas preventivas para **anticiparse** a posibles desviaciones o no conformidades.

Acciones Correctivas y Preventivas: Claves para la Mejora Continua

❖ Acciones Correctivas

Las acciones correctivas son las medidas que se toman para **eliminar la causa de una no conformidad detectada**, evitando que el problema se repita. Este proceso, además de centrarse en solucionar la situación actual, permite identificar la **causa raíz** y erradicarla.

Ejemplo: Si un cliente recibe un producto defectuoso, la organización debe analizar qué falló en la producción, corregir el proceso y asegurar controles para evitar errores similares.

❖ Acciones Preventivas

Por otro lado, las acciones preventivas son aquellas que se implementan **antes de que ocurra una no conformidad**, identificando riesgos potenciales y minimizando su impacto.

ESGinnova
Group

HSE Tools

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

Software para gestión HSE: guía del comprador

Pocas organizaciones modernas pueden prescindir del uso de un **software para gestión HSE**. En la práctica, es difícil alcanzar una competitividad mínima sin utilizar una herramienta tecnológica que ayude a **asegurar el cumplimiento normativo y regulatorio**, a centralizar la información y la documentación y, lo más importante, a mejorar la seguridad y salud en el trabajo y la relación con el medio ambiente.

La Gestión de Seguridad y Salud en el Trabajo y del Medio Ambiente (HSE, por sus iniciales en inglés) **es un área esencial y crítica para cualquier organización moderna**. Su importancia es estratégica. Si no recibe atención, soporte y recursos, la gestión en estas áreas puede convertirse en un problema que amenace la continuidad del negocio. De ahí la relevancia de trabajar con un software para gestión HSE.

Qué es un software para gestión HSE

El software para gestión HSE es una solución tecnológica **diseñada para automatizar muchas de las tareas requeridas en esta área**, crear flujos de trabajo automáticos para desarrollar otras y hacer seguimiento y monitoreo de la actividad general para producir informes inmediatos y relevantes para la toma de decisiones. Para cumplir con su objetivo, el software para gestión HSE **recopila información y datos, los procesa y analiza**. Con la ayuda de la Inteligencia Artificial y Big Data presenta informes como mapas de calor, en los que se resaltan los problemas o los puntos críticos de la gestión. Con base en esos informes, una **plataforma HSE es capaz de presentar escenarios hipotéticos, crear flujos de trabajo** y notificar a las personas que necesitan realizar tareas o asumir funciones. Además, puede presentar alertas sobre el atraso o incumplimiento de trabajos asignados, y, finalmente, entregar informes en tiempo real sobre el estado de la gestión y sobre los indicadores o métricas de rendimiento general y de las personas que tienen responsabilidades.

Beneficios del software para gestión HSE

Los **beneficios de un software HSE** son enormes. Es la herramienta más eficaz para **llevar a la práctica los propósitos que se expresan en la política de HSE de la organización**.

1. Elimina el consumo de papel

Eliminar el consumo de papel tiene impacto sobre las finanzas de la organización, pero también sobre sus **indicadores ambientales**. Esto, además, **mejora la productividad de la gestión** y contribuye a eliminar el error humano.

Responsabilidad HSE de la empresa contratista

Imagina un **gran proyecto industrial** en marcha: maquinaria operando a pleno rendimiento, decenas de **contratistas** trabajando en distintas áreas y un sinfín de normativas HSE que cumplir. En este escenario, la pregunta no es si sucederá algo inesperado, sino si estamos preparados para enfrentarlo.

La **gestión de Salud, Seguridad y Medio Ambiente** (HSE) es una obligación para las empresas contratistas; es la base que garantiza la continuidad del negocio, la confianza de los clientes y la sostenibilidad del entorno en el que operan. Vamos a analizar cómo las empresas contratistas pueden asumir su rol en HSE con eficacia y cómo herramientas como el **Software de Gestión de Contratistas de HSETools** están revolucionando esta labor, convirtiendo los desafíos en oportunidades de mejora continua.

¿Qué implica la responsabilidad HSE de una empresa contratista?

Una empresa contratista tiene el deber de garantizar que sus operaciones y las de sus subcontratistas se realicen bajo estándares que protejan la salud de los empleados, promuevan un entorno laboral seguro y respeten el medio ambiente. Esto incluye:

01. **Cumplimiento normativo:** Cumplir con las regulaciones locales e internacionales en salud, seguridad y medio ambiente.

02. **Gestión de riesgos:** Identificar, evaluar y mitigar riesgos asociados con las actividades contratadas.

03. **Formación y sensibilización:** Capacitar a sus empleados y subcontratistas para trabajar de manera segura y responsable.

04. **Prevención de accidentes:** Implementar medidas proactivas para evitar incidentes laborales y ambientales.

05. **Supervisión constante:** Monitorear las actividades para asegurar el cumplimiento de los estándares HSE.

El incumplimiento de estas responsabilidades obviamente puede derivar en **sanciones legales**, pero también en daños irreparables a la **reputación corporativa** y en la pérdida de **oportunidades** de negocio.

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO

Control de documentación de contratistas: cómo realizar seguimiento del cumplimiento

El **control de documentación de contratistas** es uno de los elementos clave en la gestión de la fuerza laboral externa. La relevancia de la documentación en la **gestión de contratistas** se explica por el número de documentos, su importancia y sus implicaciones regulatorias y normativas.

El control de documentación de contratistas se ocupa de **recopilar, revisar, verificar el estado, aprobar y almacenar documentos de índole muy diversa.** Entre ellos se encuentran licencias, pólizas de seguros, certificaciones de capacitaciones necesarias para desarrollar algunas labores, exámenes médicos, referencias de experiencia, etc. **La diversidad de las fuentes de las que provienen estos documentos es un desafío** al que se enfrenta el control de documentación de contratistas. También lo es la verificación continua de la actualidad del documento. Algunos, como los cursos para trabajar en alturas o las pólizas de seguros, pueden requerir varias actualizaciones durante el desarrollo del contrato.

Cómo verificar el cumplimiento en el control de documentación de contratistas

Conviene **disponer de una lista de verificación para el control de documentación de contratistas**. Esta incluiría, a grandes rasgos, las siguientes cuestiones: **permisos de trabajo**, satisfacción de los requisitos exigidos por la empresa, autenticidad de los documentos, fechas de vencimiento y cumplimiento de los requisitos legales, normativos y contractuales. Una vez pasada la etapa de verificación es necesario asegurar el orden, el **almacenamiento seguro y lógico** y la validez de las fechas durante la ejecución del contrato para los documentos que así lo requieran. Por supuesto, el control de documentación de contratistas **necesita asegurar la accesibilidad de los documentos en todo momento**, de forma segura y para las personas autorizadas. Por eso es importante contar con una guía para hacerlo. Estas cuatro recomendaciones ayudarán a realizar el seguimiento del **cumplimiento del contratista** y mantener un control de documentación de contratistas seguro y eficaz:

1. Mantener los documentos en una ubicación centralizada

Buscar un documento en un archivo en papel es una tarea poco productiva. Hacerlo en todas las oficinas de la empresa multiplica el esfuerzo hasta llevarlo a un nivel difícil de tolerar. Si el número de contratistas y de documentos exigidos a cada uno de ellos es elevado, la tarea se torna imposible de realizar. La mejor recomendación es **concentrar el almacenamiento de documentos en una única ubicación centralizada**. Es posible hacer mucho más, si se utiliza un **software avanzado de gestión de contratistas** con funcionalidad de control de documentos. Una plataforma tecnológica de estas características **podrá digitalizar los documentos, verificar su estado, su cumplimiento y su validez.**

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO

Qué tiene que ver h.s.e.q con la salud ocupacional

Imagina una organización donde cada colaborador se sienta seguro, cuidado y valorado. Ahora, añade a esta visión un **enfoque estratégico** que no solo protege a las personas, sino que también impulsa el rendimiento empresarial, el cumplimiento normativo y la sostenibilidad. Ese es el corazón de **HSEQ**.

Hablar de h.s.e.q es mucho más que mencionar siglas; es abordar un sistema integrado que conecta la **salud**, la **seguridad**, el **medioambiente** y la **calidad** en un ecosistema que beneficia tanto a las personas como a las empresas. Dentro de este enfoque, la **salud ocupacional** es uno de los pilares fundamentales, garantizando que los trabajadores puedan desempeñar sus labores en condiciones óptimas.

Pero, ¿cómo se traducen estos conceptos en resultados tangibles? ¿Y qué papel puede jugar la tecnología para simplificar su implementación? Quédate con nosotros para explorar estas cuestiones y descubrir cómo soluciones como **HSETools** pueden marcar una diferencia significativa para las organizaciones.

El papel de la salud ocupacional dentro de h.s.e.q

La **salud ocupacional** se centra en **proteger y mejorar el bienestar físico y mental de los trabajadores** dentro del entorno laboral. Este componente se vincula directamente con la "H" de HSEQ (**Health**), abordando aspectos clave como:

01. **Prevención de enfermedades laborales:** Desde trastornos musculoesqueléticos hasta enfermedades causadas por exposición a agentes químicos o biológicos.

02. **Promoción de la salud mental:** Abordar el estrés laboral, el agotamiento profesional (burnout) y otros factores psicosociales.

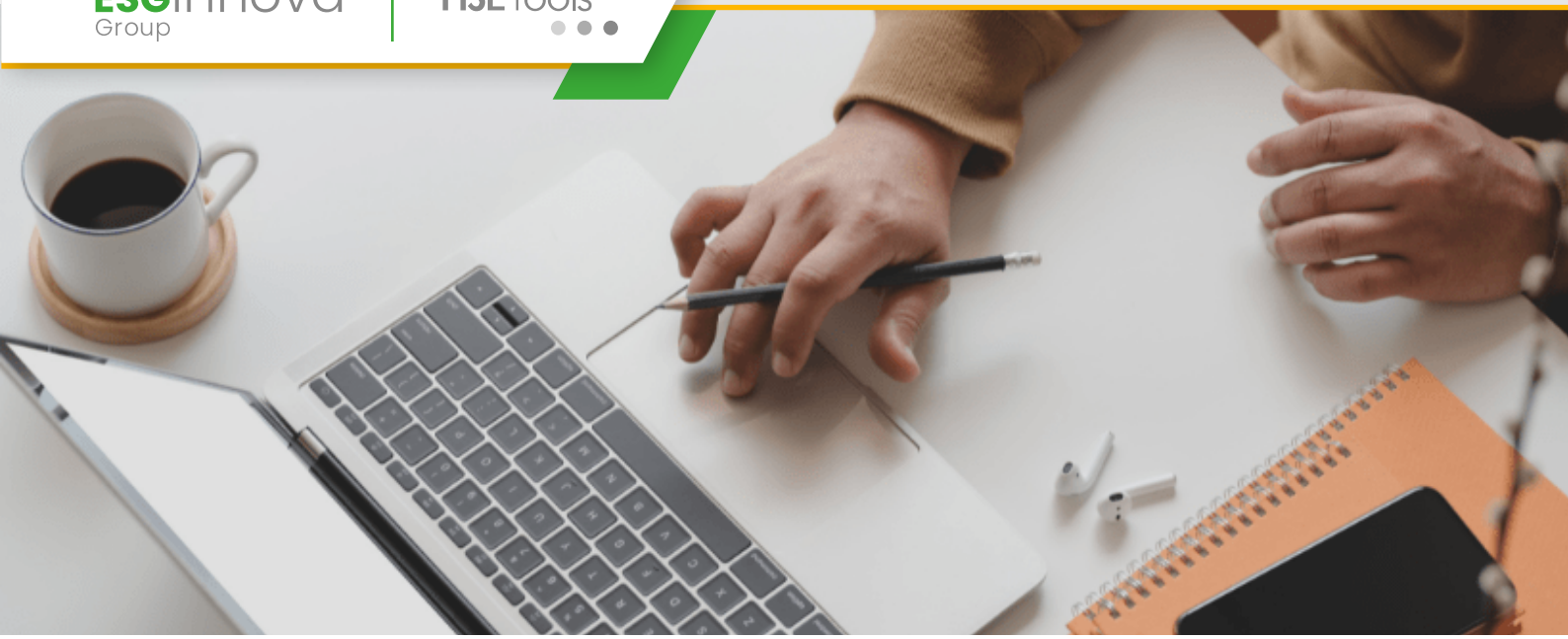
03. **Fomento de un entorno laboral seguro:** Asegurar que las instalaciones y prácticas laborales sean seguras para todos los trabajadores.

La salud ocupacional, al formar parte de h.s.e.q busca la protección de los empleados, y como consecuencia también mejora el rendimiento y la productividad organizacional al **reducir ausencias por enfermedad o accidentes**.

El impacto del h.s.e.q en el sector empresarial

Para las empresas, implementar un sistema HSEQ sólido es una cuestión de **responsabilidad corporativa**, además de una ventaja competitiva.

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO



¿Cuál es el procedimiento de trabajo en SST?

En el ámbito de la **Seguridad y Salud en el Trabajo (SST)**, los procedimientos de trabajo son fundamentales para garantizar un **entorno laboral seguro y eficiente**. Estos procedimientos no solo reducen la probabilidad de accidentes, sino que también aseguran el cumplimiento de normativas locales e internacionales.

En este artículo, exploraremos qué es un **procedimiento de trabajo**, su importancia en el marco de SST, y los pasos necesarios para implementarlo eficazmente en cualquier organización.

Procedimiento de trabajo

Un **procedimiento de trabajo** es un conjunto de **instrucciones específicas** que describe cómo **llevar a cabo una tarea o actividad de manera segura, eficiente y conforme a las normativas aplicables**. Este documento sirve como guía para los empleados, asegurando que se minimicen los riesgos asociados a cada actividad laboral.

Características principales de un **procedimiento de trabajo:**

- **Estandarización**: Garantiza que todas las actividades se realicen de manera uniforme.
- **Prevención de riesgos**: Incluye controles específicos para mitigar peligros identificados en el entorno laboral.
- **Cumplimiento normativo**: Se alinea con leyes y estándares de SST.
- **Documentación clara**: Utiliza un lenguaje comprensible para todos los empleados involucrados.

Importancia del procedimiento de trabajo en SST

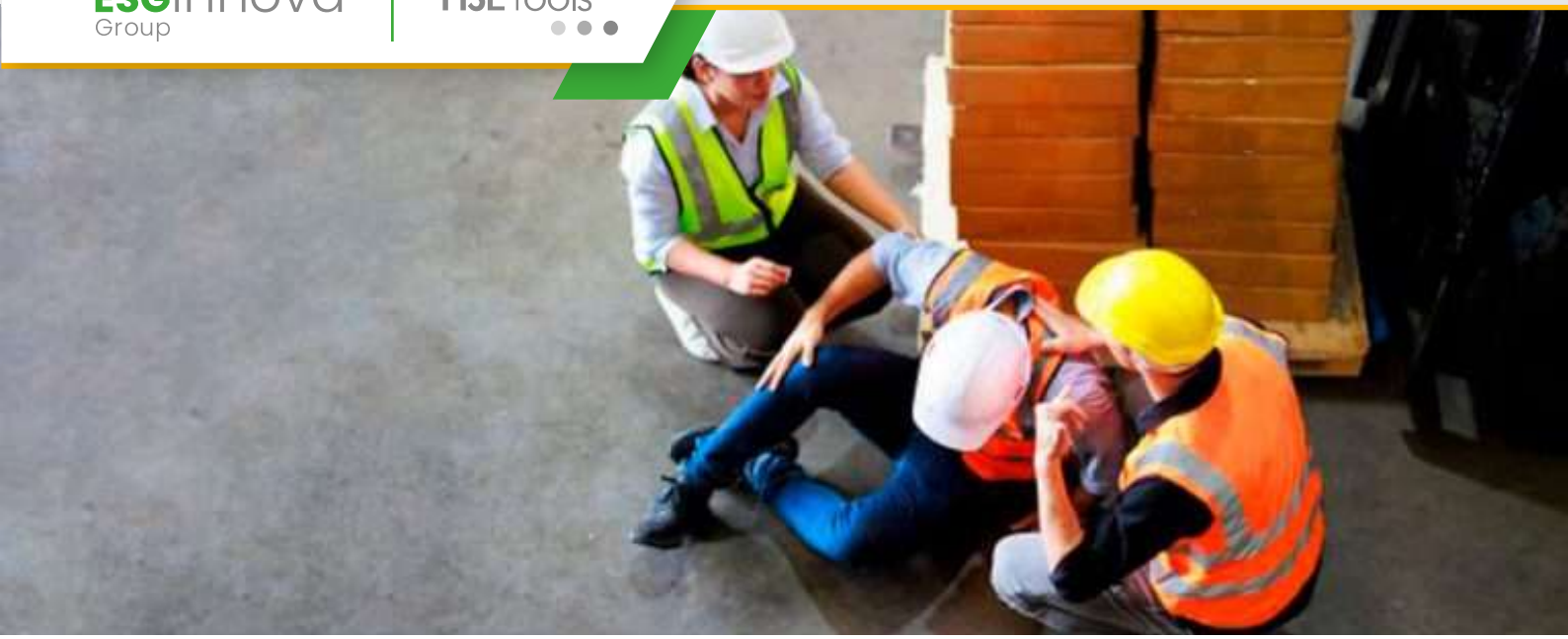
El diseño e implementación de **procedimientos de trabajo bien estructurados** son esenciales para cualquier sistema de SST. Veamos algunas razones clave para su **relevancia**:

Reducción de accidentes y enfermedades laborales

Los procedimientos detallan las mejores prácticas para **evitar riesgos específicos**, reduciendo significativamente la probabilidad de lesiones.

Cumplimiento de normativas legales

La legislación en SST exige que las empresas establezcan **medidas de control documentadas**. Los procedimientos de trabajo ayudan a cumplir con estas exigencias, **evitando multas o sanciones**.



Investigación de accidentes de trabajo: guía paso a paso para hacerlo de forma eficaz

En la mayoría de las circunstancias, los accidentes laborales están precedidos de avisos que se han pasado por alto, no se han notificado o a los que no se ha dado la importancia que tenían. La investigación de accidentes de trabajo es fundamental no para encontrar culpables, sino para hallar la causa real y trabajar en su solución, contribuEs un hecho que, al revisar registros históricos de investigaciones proactivas y eficaces, es fácil percibir que la causa raíz de un accidente es en muchos casos **un proceso con fallos en su diseño o una deficiencia de capacitación, de competencias o de comunicación**, antes que el error de la persona que estaba más cerca. Para obtener las conclusiones más productivas y ajustadas a la realidad, es preciso realizar una investigación de accidentes de trabajo sistemática, que aporte luz sobre las verdaderas causas y permita **conservar un registro de información útil para trabajar en la prevención** en el futuro.

Por qué es importante realizar una investigación de accidentes de trabajo eficaz

Los accidentes de trabajo son eventos complejos, que **resultan de la conjunción o el encadenamiento de otros eventos** y circunstancias que no se atendieron de forma debida cuando tomaron la forma de un incidente. Esta es una primera conclusión. Iniciar la **investigación de incidentes**, encontrar su causa raíz y eliminarla es la ruta acertada para prevenir accidentes. Pero, cuando estos ocurren, realizar una investigación de accidentes de trabajo eficaz ofrece información valiosa:

- **Se entiende qué sucedió** y dónde aparecen los problemas y eventos que dieron paso al accidente.
- **Establece la causa raíz que originó el accidente**, lo que permitirá tratarla y eliminarla evitando la no repetición.
- **Identifica brechas de seguridad** o brechas de cumplimiento del programa de seguridad o del sistema de gestión. Estas brechas de seguridad tienen la posibilidad de crear otros problemas mayores después del accidente si no se investigan y tratan.
- **Genera confianza en los trabajadores** en un momento de confusión e incertidumbre, consecuencias naturales de un accidente.
- **Promueve la mejora continua**, ya que señala problemas, deficiencias, procesos ineficaces u otras desviaciones que, al ser eliminadas, mejoran la gestión y sus resultados.

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO

Como construir un Arbol de Causas

La identificación de las causas de un incidente o problema es fundamental para evitar que vuelva a ocurrir. En el ámbito de la Seguridad, Salud y Medioambiente (HSE), esta tarea adquiere una importancia crítica para prevenir accidentes laborales, proteger a los empleados y asegurar el cumplimiento normativo. Una de las metodologías más efectivas para realizar este análisis es la creación de un **Árbol de Causas**. En este artículo, te enseñaremos paso a paso cómo construirlo y cómo puede ayudarte a identificar las causas raíz de cualquier problema dentro de tu organización.

¿Qué es un Arbol de Causas?

Un **Árbol de Causas** es una herramienta visual y metodológica que se utiliza para identificar las **causas inmediatas** y las **causas raíz** de un incidente o problema. Su objetivo principal es determinar **qué ha pasado, por qué ha pasado y cómo evitar que vuelva a suceder**.

Esta técnica se basa en descomponer un incidente en partes más pequeñas para poder encontrar sus orígenes, usando una estructura jerárquica similar a un árbol, donde el **problema principal** se coloca en la parte superior y las **causas** van descendiendo en ramas.

Pasos para construir un Arbol de Causas

1. Definir el problema o incidente

El primer paso es identificar y definir claramente el problema que se ha producido. Es fundamental especificar **qué ha ocurrido, quién estuvo involucrado, cuándo y dónde sucedió**, y cómo se ha detectado el problema.

Por ejemplo: "Un trabajador se resbaló y cayó desde una escalera mientras realizaba tareas de mantenimiento".

2. Reunir información detallada

Recolecta toda la información relacionada con el incidente:

- **Testimonios** de los empleados involucrados y testigos.
- Fotografías, vídeos o **evidencias físicas**.
- **Historial de mantenimiento** o registros de seguridad.
- Factores ambientales, como condiciones del clima o iluminación.

3. Identificar las causas inmediatas

Las **causas inmediatas** son las más cercanas al incidente.

El poder de las auditorías de salud y seguridad para mejorar el desempeño de los contratistas

Las auditorías de salud y seguridad, al igual que otras revisiones o inspecciones, sirven para mejorar el sistema, la gestión o el programa, según sea el caso. Lo interesante es que también son muy útiles para mejorar el desempeño de la **gestión de contratistas**, asegurando que cumplen con las prácticas y normas de seguridad. Para comprenderlo y aprovecharlo, es preciso revisar con precisión la definición de auditorías de salud y seguridad, **cuáles son sus componentes y sus beneficios** y, finalmente, cómo impactan en el desempeño de los contratistas.

Qué son las auditorías de salud y seguridad

Las auditorías de salud y seguridad en el trabajo son **evaluaciones técnicas, sistemáticas e integrales**, que buscan comprobar el cumplimiento con una regulación, una ley o la conformidad con los

requisitos de un estándar de gestión, que en estos casos suele ser **ISO 45001**. Las auditorías de salud y seguridad en el trabajo también buscan evidencia del cumplimiento de las normas de seguridad por parte de los contratistas. Así, **identifican riesgos, brechas de seguridad y de cumplimiento**, entre otros objetivos específicos:

1. Identificar brechas de cumplimiento

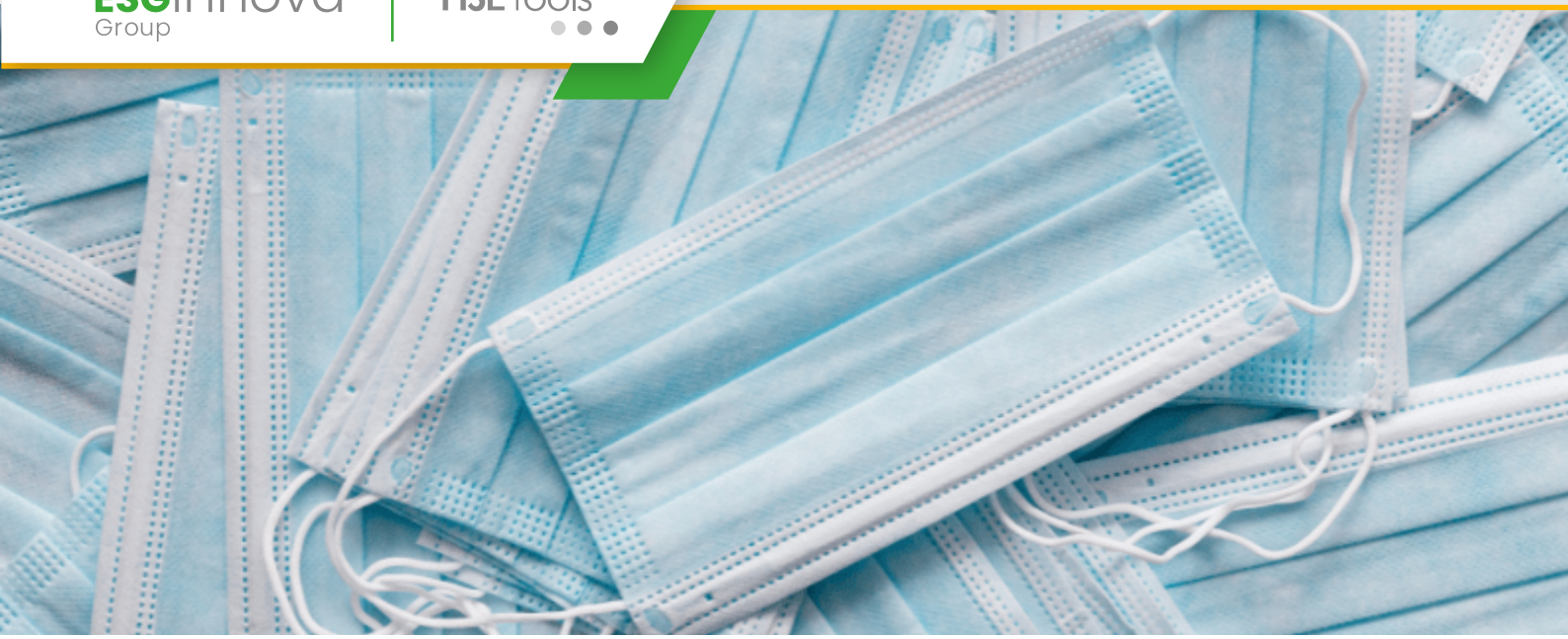
En este caso, las auditorías de salud y seguridad buscan fallos de cumplimiento específicos: **normas que no se están cumpliendo, requisitos regulatorios que se ignoran**, uso indebido o inexistente de los **equipos de protección personal** o contravención de las políticas de seguridad de la organización.

2. Verificar la eficacia de la gestión de riesgos

La auditoría comprueba la eficacia de la **gestión de riesgos del contratista** y la forma en que este adopta los controles y las medidas implementadas para prevenirlos. **Las auditorías pueden encontrar riesgos no identificados por la gestión.**

3. Crear y promover cultura de seguridad en el trabajo

Las auditorías de salud y seguridad en el trabajo hacen que los trabajadores, también los contratistas, **perciban que la organización se preocupa por sus condiciones de trabajo** y por cualquier elemento que implique un riesgo. También mantiene vigente el tema de la seguridad. Las dos condiciones son generadoras de cultura de seguridad. Finalmente, **las auditorías pueden ser internas, realizadas con profesionales formados dentro de la organización** o por consultor contratado por la empresa, o externas, cuando la iniciativa y la necesidad es de un tercero, como un organismo regulador, un cliente o un asegurador.



Elementos de protección más importantes en la industria minera

La industria minera es uno de los sectores más desafiantes y peligrosos del mundo laboral. Las condiciones extremas, el manejo de maquinaria pesada y la exposición a sustancias tóxicas convierten la **seguridad en una prioridad absoluta**. Para **mitigar los riesgos y proteger la integridad** de los trabajadores, el uso adecuado de los **elementos de protección** es esencial.

En este artículo, exploraremos los principales **elementos de protección** necesarios en la minería, su importancia y las mejores prácticas para **garantizar su efectividad**.

Elementos de protección

Los **elementos de protección** son equipos y dispositivos diseñados **para minimizar los riesgos a los que están expuestos los trabajadores durante sus actividades**.

En la minería, estos riesgos pueden incluir caídas, inhalación de polvo o gases tóxicos, lesiones por maquinaria o explosiones.

Tipos de elementos de protección:

- **Elementos de protección personal (EPP):** Uso individual por cada trabajador, como cascos o guantes.
- **Elementos de protección colectiva (EPC):** Diseñados para proteger a grupos, como sistemas de ventilación o barandillas.
- Ambos son indispensables para una gestión efectiva de la **seguridad y salud en el trabajo**.

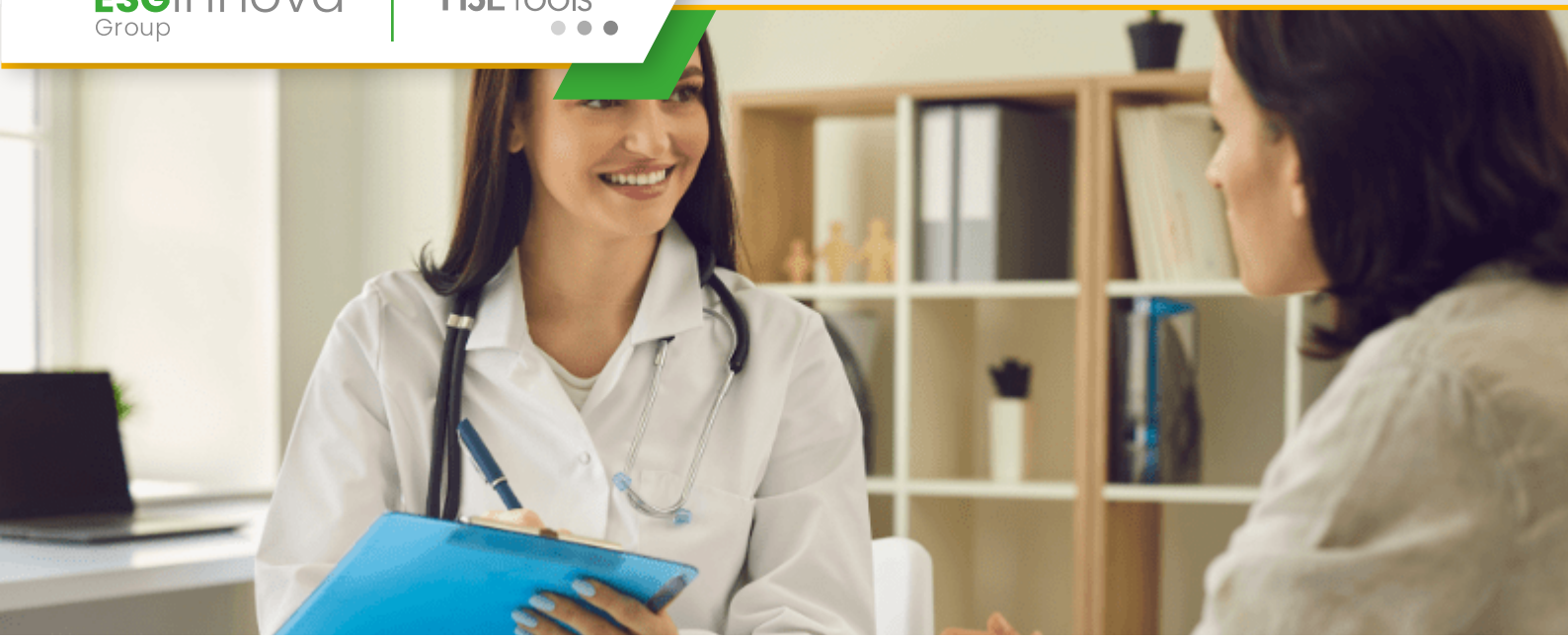
Principales elementos de protección en la industria minera

Cascos de seguridad

El casco es uno de los **elementos de protección más básicos y esenciales** en la minería. Está diseñado para **proteger la cabeza** contra:

- Caída de objetos.
- Golpes contra superficies duras.
- Proyecciones de material.

Los cascos deben cumplir con normativas internacionales como las de la **ANSI** o la **EN 397**, que garantizan su **resistencia y durabilidad**.



¿Cuáles son los beneficios de la promoción de la salud ocupacional?

La salud ocupacional es una **disciplina** clave dentro de la **gestión empresarial moderna**. Su **objetivo** principal es **promover y proteger la salud física, mental y social** de los trabajadores, optimizando su bienestar y **aumentando su productividad**. En este artículo, analizaremos en detalle qué es la **salud ocupacional**, los beneficios que aporta a las organizaciones y cómo se puede implementar de manera efectiva.

Salud ocupacional

La **salud ocupacional** se define como el **conjunto de actividades, procedimientos y políticas** dirigidas a **identificar, prevenir y controlar los riesgos** laborales que pueden afectar la salud de los empleados. Este concepto va más allá de la prevención de accidentes laborales, centrándose también en la **promoción del bienestar integral** de los trabajadores.

Principales objetivos de la salud ocupacional:

- **Prevenir enfermedades laborales:** Reducir la incidencia de enfermedades relacionadas con el trabajo.
- **Promover el bienestar físico y mental:** Crear un entorno laboral que potencie el desarrollo personal y profesional.
- **Mejorar las condiciones laborales:** Garantizar que los espacios de trabajo cumplan con estándares de seguridad y ergonomía.

Beneficios de la promoción de la salud ocupacional

La inversión en **salud ocupacional** genera múltiples **beneficios** tanto para los **trabajadores** como para las **empresas**. Veamos los más relevantes.

Reducción de accidentes y enfermedades laborales

Implementar estrategias de **salud ocupacional** permite **identificar y mitigar riesgos** laborales, **reduciendo** significativamente los **incidentes** en el lugar de trabajo. Esto no solo **protege a los empleados**, sino que también **disminuye los costos asociados** con indemnizaciones, interrupciones operativas y reemplazos temporales.

Incremento en la productividad

Un trabajador saludable es un **trabajador productivo**. Cuando los empleados gozan de buena salud, tanto física como mental, su rendimiento aumenta. Además, la **reducción de ausencias** por enfermedad se traduce en una **mayor continuidad** de los procesos productivos.

ESGinnova Group

GRCTools

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

Cómo Obtener la Certificación COBIT 5: Guía Completa para Profesionales

¿Qué es COBIT 5 y por qué es relevante?

La certificación COBIT 5 (Control Objectives for Information and Related Technologies) es un marco reconocido a nivel internacional que establece las mejores prácticas para la gobernanza y gestión de TI. **Permite a las empresas maximizar el valor de sus inversiones tecnológicas, optimizar el uso de los recursos y minimizar los riesgos asociados.**

COBIT 5 es especialmente útil para abordar desafíos relacionados con:

- **Riesgos estratégicos**, asegurando que las decisiones tecnológicas estén alineadas con los objetivos del negocio.
- **Riesgos de ciberseguridad**, mediante la implementación de controles efectivos para proteger los sistemas y la información.

- **Riesgos de compliance**, asegurando el cumplimiento de normativas locales e internacionales.

Obtener la certificación COBIT 5 es un paso crucial para los profesionales que desean fortalecer sus habilidades en la gestión de TI y riesgos, y convertirse en referentes en su campo.

Beneficios de la certificación COBIT 5

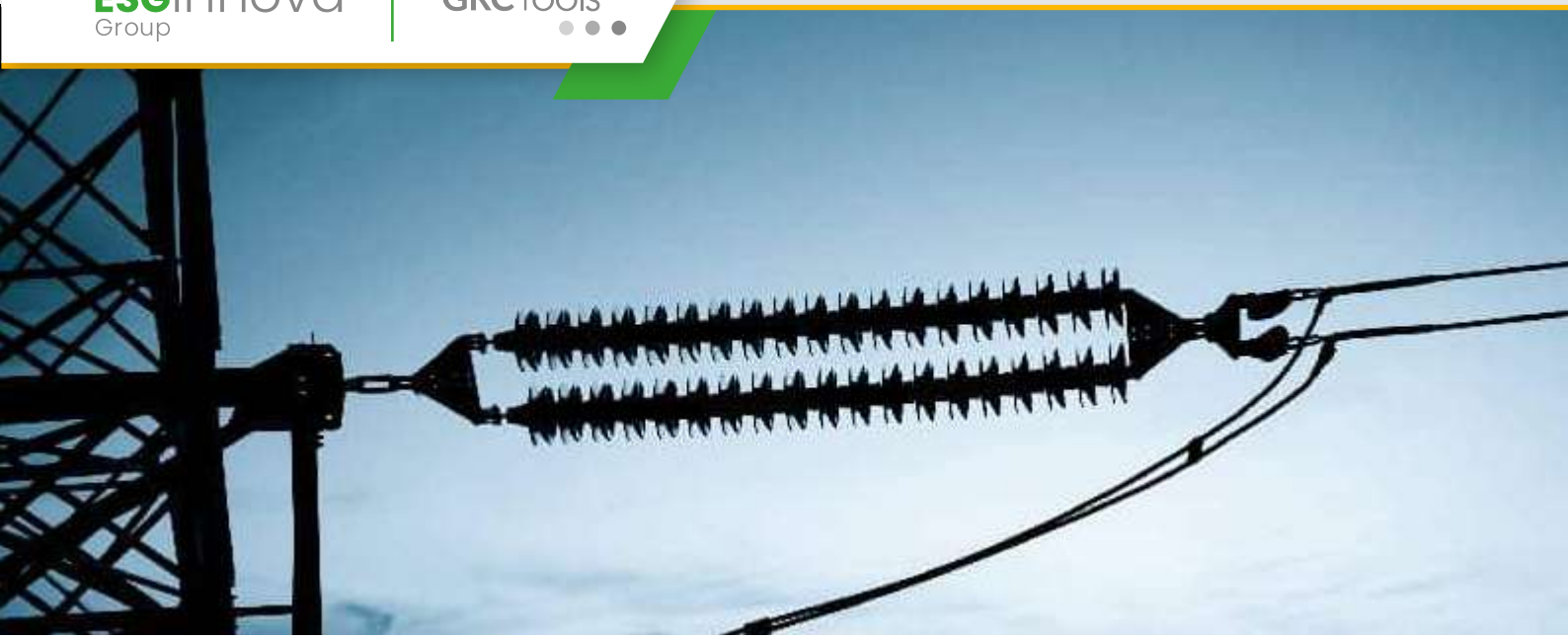
- **Mejora en la gestión de riesgos corporativos**
  COBIT 5 ofrece herramientas para identificar, evaluar y mitigar los riesgos en toda la organización, incluidos los **riesgos operacionales**, **riesgos laborales** y **riesgos de seguridad de la información**. Esto asegura que los procesos tecnológicos estén alineados con las necesidades del negocio.

- **Fortalecimiento del cumplimiento normativo**
  El marco COBIT 5 ayuda a las organizaciones a cumplir con regulaciones clave, reduciendo los **riesgos de compliance** y evitando sanciones legales.

- **Optimización del uso de recursos tecnológicos**
  COBIT 5 permite maximizar la eficiencia en el uso de la tecnología, reduciendo los costos asociados y mejorando la productividad.

- **Reconocimiento profesional**
  Los profesionales certificados en COBIT 5 son altamente valorados en el mercado laboral, especialmente en roles relacionados con la **gestión de riesgos corporativos** y la gobernanza de TI.

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO



Certificación NERC-CIP: Cómo garantizar la confiabilidad del suministro eléctrico

En un mundo cada vez más digitalizado y dependiente de la electricidad, la confiabilidad del suministro eléctrico es crítica para el bienestar económico, social y tecnológico. La **certificación NERC-CIP** (North American Electric Reliability Corporation – Critical Infrastructure Protection) es el estándar principal para garantizar la seguridad de las infraestructuras críticas en el sector eléctrico en Norteamérica.

Diseñada para proteger la red eléctrica contra amenazas cibernéticas y físicas, la certificación NERC-CIP no solo asegura el cumplimiento normativo, sino que también mitiga los **riesgos corporativos** y asegura la continuidad del servicio eléctrico.

¿Qué es la certificación NERC-CIP y por qué es importante?

La **certificación NERC-CIP** es un conjunto de estándares desarrollados para proteger la infraestructura crítica del sector eléctrico frente a amenazas que puedan comprometer la estabilidad del suministro. Estos estándares son obligatorios para todas las entidades reguladas por NERC, como operadores de redes, generadores de energía y transmisores.

Los objetivos principales de NERC-CIP incluyen:

- **Protección de activos críticos**: Identificar y proteger los activos esenciales para el suministro eléctrico.
- **Mitigación de riesgos de ciberseguridad**: Implementar controles para prevenir y responder a ataques cibernéticos.
- **Cumplimiento normativo**: Garantizar que las operaciones eléctricas cumplan con las leyes y regulaciones aplicables.

La importancia de cumplir con NERC-CIP radica en la creciente sofisticación de los ataques cibernéticos y en el impacto potencial de una falla en la red eléctrica, que podría generar **riesgos estratégicos**, **riesgos financieros** y un daño irreparable a la reputación de la organización.

Componentes clave de NERC-CIP

El estándar de la certificación NERC-CIP está compuesto por una serie de requisitos divididos en trece categorías principales, cada una diseñada para abordar aspectos críticos de la seguridad eléctrica.

Importancia de la Ciberseguridad en Chile: Leyes y Regulaciones

La **ciberseguridad en Chile** se ha convertido en un tema de **alta relevancia** en los últimos años debido al **aumento de los ataques cibernéticos** y la necesidad de proteger los datos sensibles de empresas y ciudadanos. La transformación digital, acelerada por la pandemia, ha expuesto a organizaciones y gobiernos a mayores riesgos, haciendo imprescindible **adoptar medidas robustas** para **garantizar la seguridad digital**.

En este artículo, exploraremos por qué la ciberseguridad es crucial en Chile, las **normativas y regulaciones vigentes**, y cómo las empresas pueden **fortalecer su postura** frente a estas amenazas.

Ciberseguridad en Chile

La **ciberseguridad** es el conjunto de **prácticas, tecnologías y procesos diseñados para proteger sistemas, redes, dispositivos y datos frente a ataques digitales**.

Estas amenazas pueden incluir malware, phishing, ransomware y accesos no autorizados, entre otros.

Importancia de la ciberseguridad en el contexto actual:

- **Protección de datos sensibles:** Las organizaciones manejan grandes volúmenes de información personal, financiera y estratégica que necesitan salvaguardar.
- **Prevención de interrupciones operativas:** Los ciberataques pueden paralizar operaciones, impactando la productividad y reputación.
- **Cumplimiento normativo:** Chile cuenta con regulaciones que exigen a las empresas adoptar medidas de seguridad específicas.

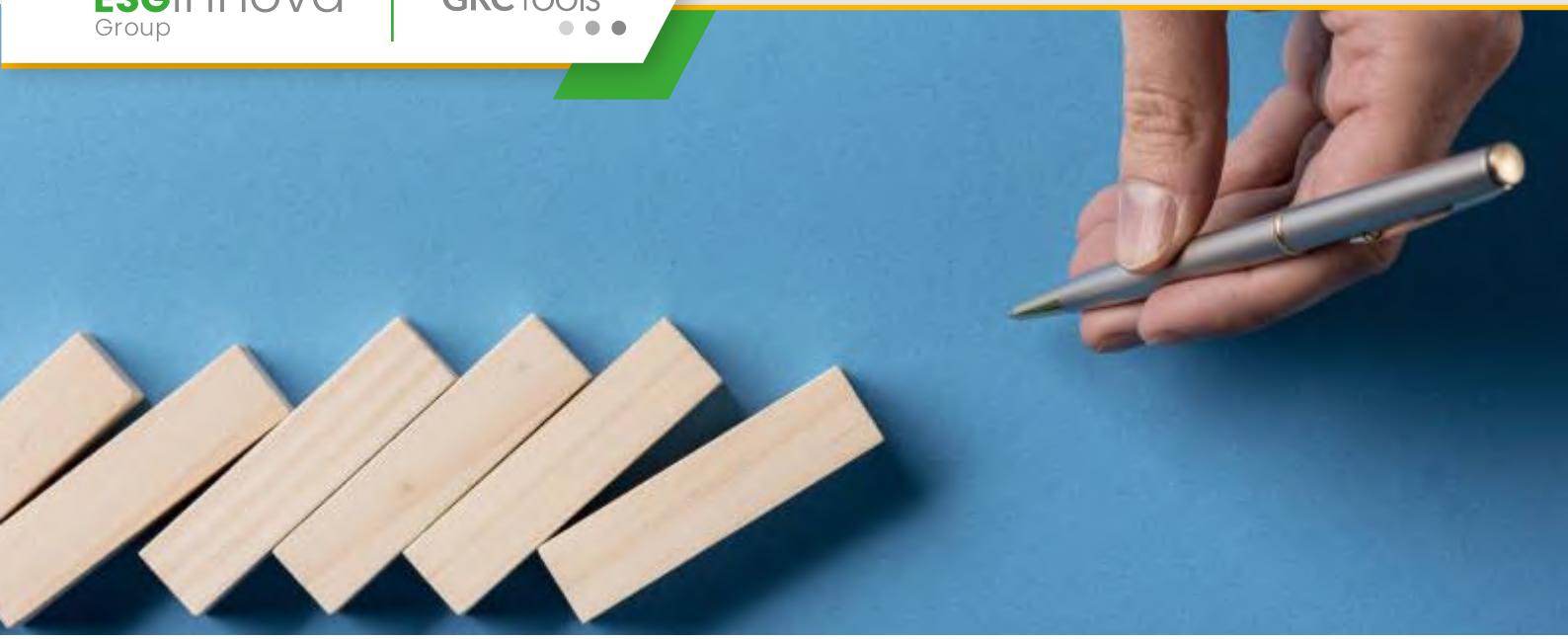
La situación actual de la ciberseguridad en Chile

Aumento de los ciberataques

En los últimos años, Chile ha registrado un **incremento** significativo en **incidentes de seguridad digital**. Según estudios recientes, sectores como la banca, telecomunicaciones y gobierno son los más vulnerables. Los cibercriminales buscan **explotar debilidades** en **sistemas de protección** para **robar información, extorsionar o desestabilizar** operaciones.

Transformación digital y sus riesgos

La digitalización de procesos ha sido clave para **mejorar la competitividad** empresarial, pero también ha **generado nuevas vulnerabilidades**.



Tipos de riesgos corporativos: ejemplos clave y estrategias de mitigación

Riesgos Corporativos

La capacidad de una empresa para prosperar no depende únicamente de sus éxitos, sino también de cómo maneja las incertidumbres y desafíos que enfrenta en su camino. Los **riesgos corporativos** son inevitables, pero cuando se gestionan de manera estratégica, pueden convertirse en una ventaja competitiva.

Estar al tanto de los principales tipos de riesgos que afectan a las organizaciones es esencial. Vamos a hablar de ejemplos concretos y estrategias para mitigarlos eficazmente. Además, te mostraremos cómo un **Software de Riesgos Corporativos ERM** puede ayudarte a transformar la gestión de riesgos en una herramienta clave para la toma de decisiones y el **crecimiento sostenible**.

¿Qué son los Riesgos Corporativos?

Los riesgos corporativos son **eventos** o **circunstancias** que pueden **impactar negativamente en los objetivos estratégicos, operativos o financieros** de una organización. Desde fluctuaciones del mercado hasta **ciberataques**, cada riesgo tiene el potencial de amenazar la estabilidad de una empresa si no se gestiona de manera efectiva.

Sin embargo, los riesgos no son solo amenazas; también pueden convertirse en **oportunidades** si se identifican y gestionan con un enfoque estratégico.

Tipos de riesgos corporativos y ejemplos clave

1. Riesgos financieros

Amenazas relacionadas con pérdidas económicas debido a fluctuaciones en el mercado, incumplimientos de pago o problemas de liquidez.

- **Ejemplo**: Fluctuaciones en los tipos de cambio o incumplimientos de pago por parte de clientes.
- **Impacto**: Pérdidas económicas directas o disminución de la liquidez.
- **Estrategia de mitigación**: Implementar análisis financieros periódicos y diversificar las fuentes de ingresos y financiamiento.

2. Riesgos operativos

Peligros asociados con fallos internos en procesos, personas o sistemas que pueden interrumpir las actividades diarias.

¿Qué son los riesgos estratégicos en una empresa?

En un entorno empresarial en constante cambio, **identificar y gestionar** los **riesgos estratégicos** es esencial para **garantizar la sostenibilidad y el éxito** de una organización. Estos riesgos, asociados a la planificación y ejecución de la estrategia corporativa, pueden **impactar** significativamente en los **objetivos a largo plazo** y en la **competitividad** de la empresa.

En este artículo, exploraremos qué son los riesgos estratégicos, sus principales tipos, cómo **identificarlos y gestionarlos eficazmente**, y por qué son críticos en el contexto actual.

Riesgos estratégicos

Los **riesgos estratégicos** son aquellos que surgen de **decisiones relacionadas** con la **dirección estratégica** de una organización. Estos riesgos pueden derivarse de cambios en el mercado, avances tecnológicos, decisiones de inversión o incluso de factores externos como regulaciones gubernamentales y eventos globales inesperados.

Características principales de los **riesgos estratégicos:**

- **Impacto significativo:** Pueden afectar los objetivos clave de la empresa y comprometer su sostenibilidad.
- **Horizonte a largo plazo:** Generalmente están asociados a decisiones o situaciones con efectos prolongados.
- **Difícil previsión:** Suelen ser más complejos de identificar y gestionar en comparación con otros tipos de riesgos.

Principales tipos de riesgos estratégicos

Riesgos del mercado

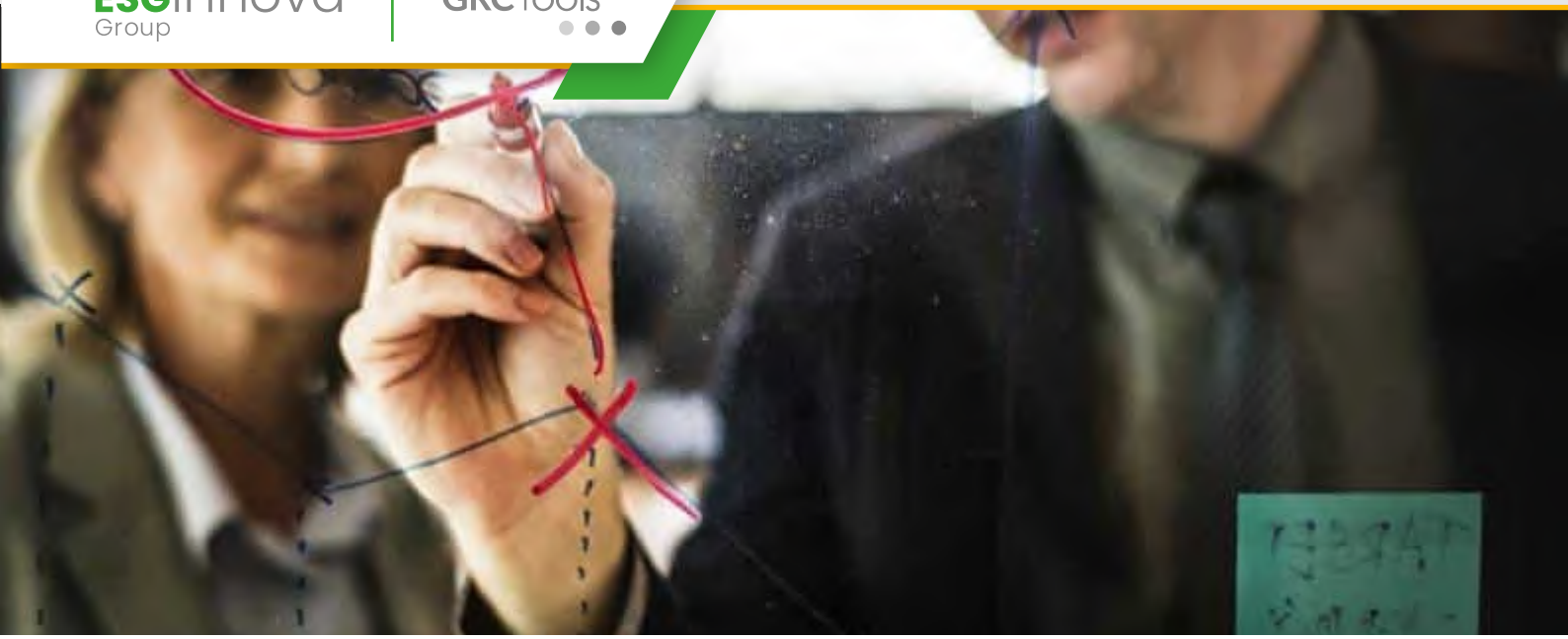
Estos riesgos se relacionan con **cambios en la dinámica del mercado**, como variaciones en la demanda de los clientes, entrada de nuevos competidores o fluctuaciones económicas.

Ejemplos comunes:

- Aparición de nuevos modelos de negocio disruptivos.
- Cambios en las preferencias del consumidor.

Riesgos regulatorios

Surgen de **cambios en las leyes y normativas** que afectan la operación o los productos de una empresa.



Beneficios de gestionar riesgos estratégicos con software GRC Tools

En un entorno empresarial donde la incertidumbre y la competencia son constantes, la gestión de **riesgos estratégicos** se convierte en una prioridad para garantizar el éxito y la sostenibilidad de las organizaciones. Estos riesgos, que afectan la capacidad de una empresa para alcanzar sus objetivos a largo plazo, pueden derivar de cambios en el mercado, decisiones de alto nivel, innovación tecnológica o incluso factores externos como regulaciones y el entorno macroeconómico.

Para abordar estos desafíos, el uso de herramientas especializadas como **GRCTools** se ha consolidado como una solución eficiente y estratégica. **Estas plataformas permiten a las organizaciones centralizar, automatizar y optimizar la gestión de riesgos, asegurando decisiones más informadas y una mayor resiliencia ante las adversidades.**

¿Qué son los riesgos estratégicos?

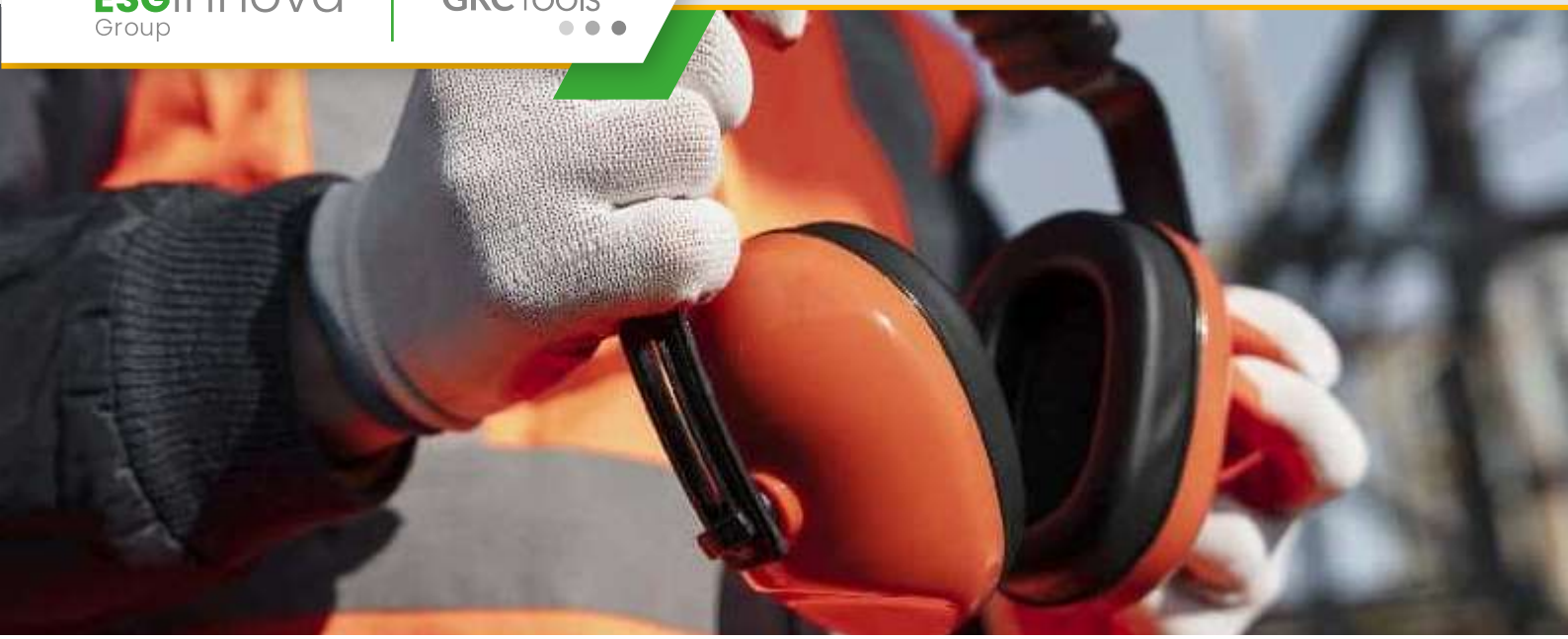
Los **riesgos estratégicos** son aquellos que afectan directamente la capacidad de una empresa para cumplir con su misión y alcanzar sus objetivos de negocio. **Estos riesgos están vinculados a decisiones fundamentales que tienen un impacto significativo en la dirección de la empresa.**

Ejemplos comunes de riesgos estratégicos incluyen:

- Cambios en las preferencias del cliente o del mercado.
- Entrada de nuevos competidores.
- Innovaciones tecnológicas disruptivas.
- Cambios en la regulación que impacten el modelo de negocio.
- Problemas derivados de la falta de alineación entre los objetivos de negocio y los recursos disponibles.

Beneficios de gestionar los riesgos estratégicos con GRCTools

El uso de **software GRC** ofrece un enfoque integral para gestionar estos riesgos de manera más eficiente.



Gestión de riesgos operacionales: Métodos y herramientas eficientes

La **gestión de riesgos operacionales** es fundamental para garantizar la continuidad y eficiencia de las operaciones en cualquier organización. Estos riesgos, relacionados con procesos internos, personas, tecnología o eventos externos, pueden afectar significativamente los resultados financieros, la reputación y la productividad de una empresa.

En este artículo, exploraremos los métodos más eficaces para gestionar los riesgos operacionales y las herramientas que pueden ayudarte a implementar una estrategia robusta, como las soluciones de **GRCTools**.

¿Qué son los riesgos operacionales?

Los **riesgos operacionales** son aquellas amenazas que surgen de fallos en los procesos internos, errores humanos, problemas tecnológicos o eventos externos como desastres naturales.

Estos riesgos están presentes en todas las organizaciones y pueden generar pérdidas económicas, interrupciones en las operaciones y daños a la reputación corporativa.

Ejemplos comunes incluyen:

- Fallos en sistemas tecnológicos.
- Errores humanos en la ejecución de procesos.
- Incidentes de seguridad en la información.
- Problemas en la cadena de suministro.
- Pérdida de activos físicos debido a desastres naturales o accidentes.

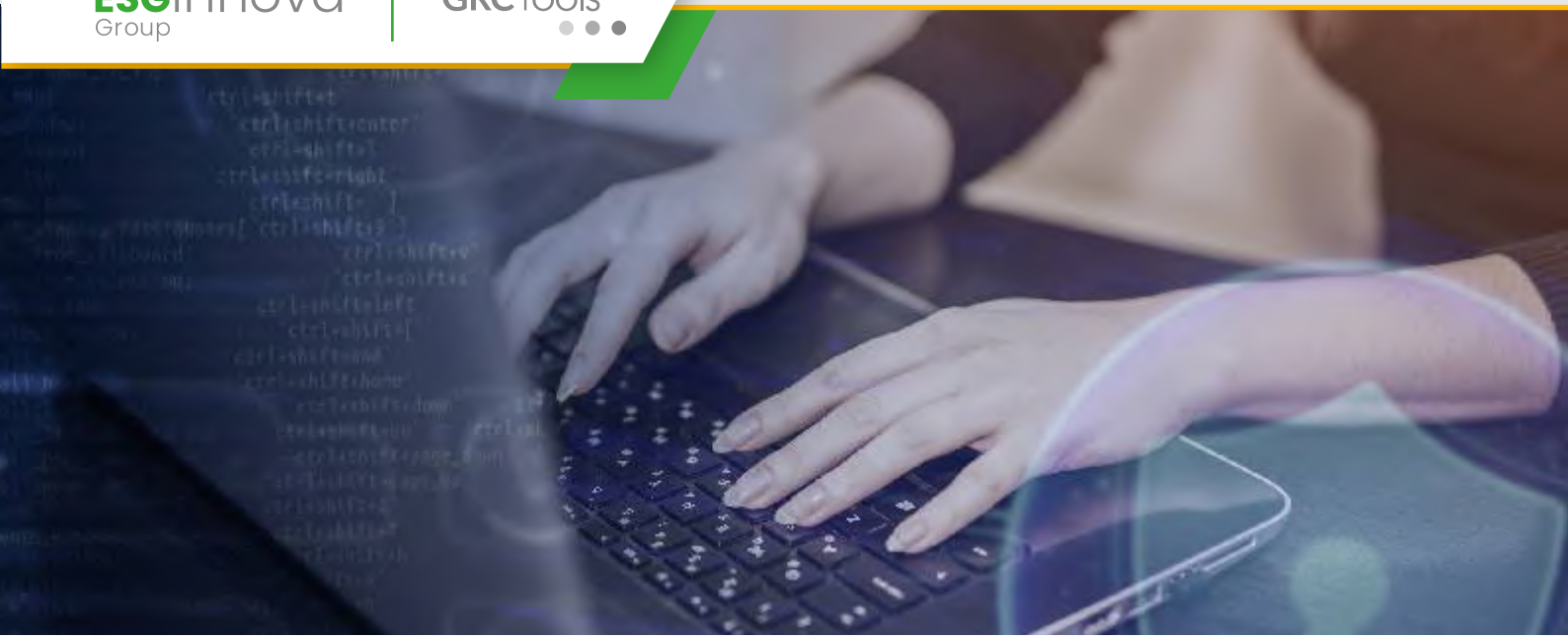
Una gestión eficaz de estos riesgos no solo minimiza su impacto, sino que también fortalece la resiliencia organizacional.

Métodos para la gestión de riesgos operacionales

La gestión de riesgos operacionales requiere un enfoque estructurado que permita identificar, evaluar, mitigar y monitorear las amenazas. A continuación, se describen los métodos más utilizados:

Identificación de riesgos

El primer paso es **identificar todos los posibles riesgos operacionales** que puedan afectar a la empresa. Este proceso incluye analizar los procesos internos, la infraestructura tecnológica, las capacidades del personal y las posibles amenazas externas.



Certificación NIST: Cómo Cumplir con los Estándares de Seguridad Cibernética

La **certificación NIST** es más que un estándar; es una herramienta clave para proteger la información crítica de tu organización. Imagina que un correo aparentemente inofensivo llega a tu bandeja de entrada. En cuestión de segundos, un clic abre la puerta a un **ciberataque** que compromete datos confidenciales de tu empresa. Este tipo de incidentes no es un caso aislado, sino una amenaza diaria para miles de organizaciones.

En este artículo, analizaremos los problemas más frecuentes que enfrentan las empresas en materia de seguridad cibernética y cómo el **Software de Ciberseguridad de GRCTools** puede convertir estos desafíos en oportunidades para fortalecer tu organización. Además, te explicaremos cómo esta herramienta puede ser tu mejor aliado para lograr la certificación NIST y garantizar un nivel superior de protección.

Certificación NIST

La **ciberseguridad** sostiene la confianza, la continuidad y la competitividad en un mercado hiperconectado. Cumplir con los estándares del **Instituto Nacional de Estándares y Tecnología (NIST)** te asegura proteger tus activos, y también de prepararte para los desafíos del futuro.

Proteger la **información crítica** y mantener la integridad de los sistemas se ha convertido en una lucha constante frente a desafíos cada vez más complejos. Algunos de los problemas más recurrentes incluyen:

1. Complejidad en la gestión de riesgos

La diversidad de amenazas, desde ataques de **malware** hasta errores humanos, exige un enfoque integral para identificar, evaluar y mitigar riesgos. Sin embargo, muchas organizaciones carecen de una estrategia clara o recursos adecuados para gestionar este proceso.

2. Desactualización de infraestructura tecnológica

Sistemas obsoletos o no actualizados son un blanco fácil para los ciberdelincuentes. Pese a ello, un gran número de empresas no priorizan la modernización tecnológica debido a **limitaciones presupuestarias** o falta de conocimiento técnico.

3. Falta de concienciación y capacitación interna

La seguridad cibernética no solo depende de tecnologías avanzadas, sino también del factor humano. Empleados que desconocen las políticas de seguridad o caen en **técnicas de phishing** representan una vulnerabilidad crítica.

Riesgos de terceros: Consejos para minimizar daños a terceros

En un mundo empresarial cada vez más interconectado, las organizaciones dependen de terceros como **proveedores, contratistas y socios estratégicos** para llevar a cabo sus operaciones. Aunque estas relaciones son fundamentales para **la eficiencia y el crecimiento**, también pueden **introducir riesgos de terceros** que, si no se gestionan adecuadamente, podrían **comprometer la seguridad**, **reputación** y **sostenibilidad** de una empresa.

En este artículo, exploraremos qué son los riesgos de terceros, sus **implicaciones** y las **mejores prácticas** para minimizarlos.

Riesgos de terceros

Los **riesgos de terceros** son **amenazas asociadas con las actividades, comportamientos o incumplimientos** de las entidades externas que tienen una relación contractual o estratégica con una organización.

Estos riesgos pueden tener un **impacto directo o indirecto** en los objetivos empresariales y pueden afectar diversas áreas como la **seguridad de los datos**, la **calidad del servicio** o el **cumplimiento normativo**.

Ejemplos comunes de riesgos de terceros:

- **Incumplimientos normativos:** Un proveedor que no cumple con las regulaciones puede exponer a tu empresa a sanciones legales.
- **Fugas de información confidencial:** Cuando un tercero tiene acceso a datos sensibles y no los protege adecuadamente.
- **Riesgos financieros:** Quiebra o inestabilidad económica de un proveedor clave.
- **Daños reputacionales:** Asociarse con una empresa involucrada en prácticas poco éticas.

Importancia de gestionar los riesgos de terceros

El impacto de los riesgos de terceros puede ser **significativo y afectar la operación y reputación de tu empresa**. Una adecuada gestión de estos riesgos ayuda a:

- **Proteger la reputación de la empresa.**
- **Evitar sanciones legales o regulatorias.**
- **Mantener la continuidad operativa.**

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO

Cómo gestionar los riesgos a terceros en obras y proyectos

En la gestión de obras y proyectos, los terceros, como subcontratistas, proveedores o consultores, desempeñan un papel crucial en el éxito o fracaso de una iniciativa. Sin embargo, trabajar con terceros también conlleva riesgos significativos, desde incumplimientos contractuales hasta accidentes laborales o problemas de calidad. Gestionar los riesgos a terceros de manera efectiva es esencial para proteger tanto los intereses de la organización como la seguridad de todos los involucrados.

A continuación, vamos a explorar las claves para **gestionar los riesgos a terceros** en obras y proyectos. Además, veremos cómo GRCTools, una plataforma Software GRC especializada en la Transformación Digital de Gobierno, Riesgo y Cumplimiento, puede ser un aliado estratégico para optimizar este proceso.

Gestionar los riesgos a terceros

Los riesgos a terceros se refieren a las posibles amenazas que pueden surgir de las actividades, decisiones o incumplimientos de terceros implicados en un proyecto. Estos riesgos pueden incluir:

- **Riesgos financieros**: Retrasos en la entrega de materiales o servicios que impactan en el presupuesto.
- **Riesgos legales**: Incumplimiento de normativas legales, como las relacionadas con seguridad y medio ambiente.
- **Riesgos operativos**: Problemas de calidad o falta de cumplimiento de los plazos establecidos.
- **Riesgos reputacionales**: Asociarse con terceros que no cumplan con principios éticos o normativas puede dañar la imagen de la organización.

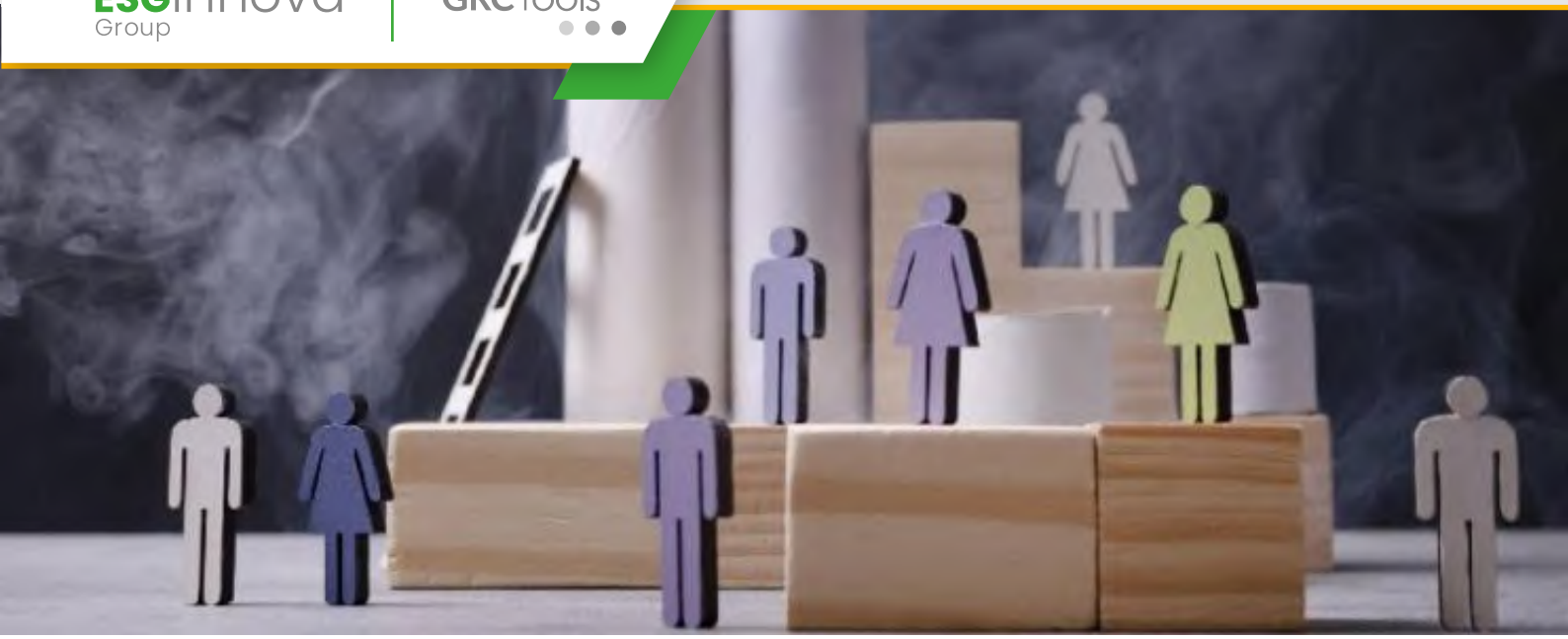
Identificar, evaluar y mitigar estos riesgos es fundamental para evitar interrupciones en los proyectos y garantizar su éxito.

Pasos clave para gestionar los riesgos a terceros

1. Identificación y evaluación de riesgos

El primer paso es comprender los riesgos específicos asociados a cada tercero. Esto incluye:

- Realizar una debida diligencia para evaluar la solvencia financiera, capacidad técnica y antecedentes legales del tercero.



Seguridad en la información: Herramientas GRC para empresas modernas

En la era digital, la seguridad en la información se ha convertido en una prioridad estratégica para las empresas. Los riesgos asociados al manejo y protección de datos, como los ataques cibernéticos, las brechas de seguridad y el acceso no autorizado, pueden tener consecuencias devastadoras, desde pérdidas económicas hasta daños irreparables a la reputación.

Para abordar estos desafíos, las empresas modernas están adoptando **herramientas GRC (Governance, Risk, and Compliance)**, que les permiten gestionar la seguridad de la información de manera centralizada y eficiente. Estas plataformas no solo garantizan la protección de datos, sino que también ayudan a cumplir con las regulaciones más estrictas y a mitigar riesgos en tiempo real.

¿Por qué es esencial la seguridad en la información para las empresas modernas?

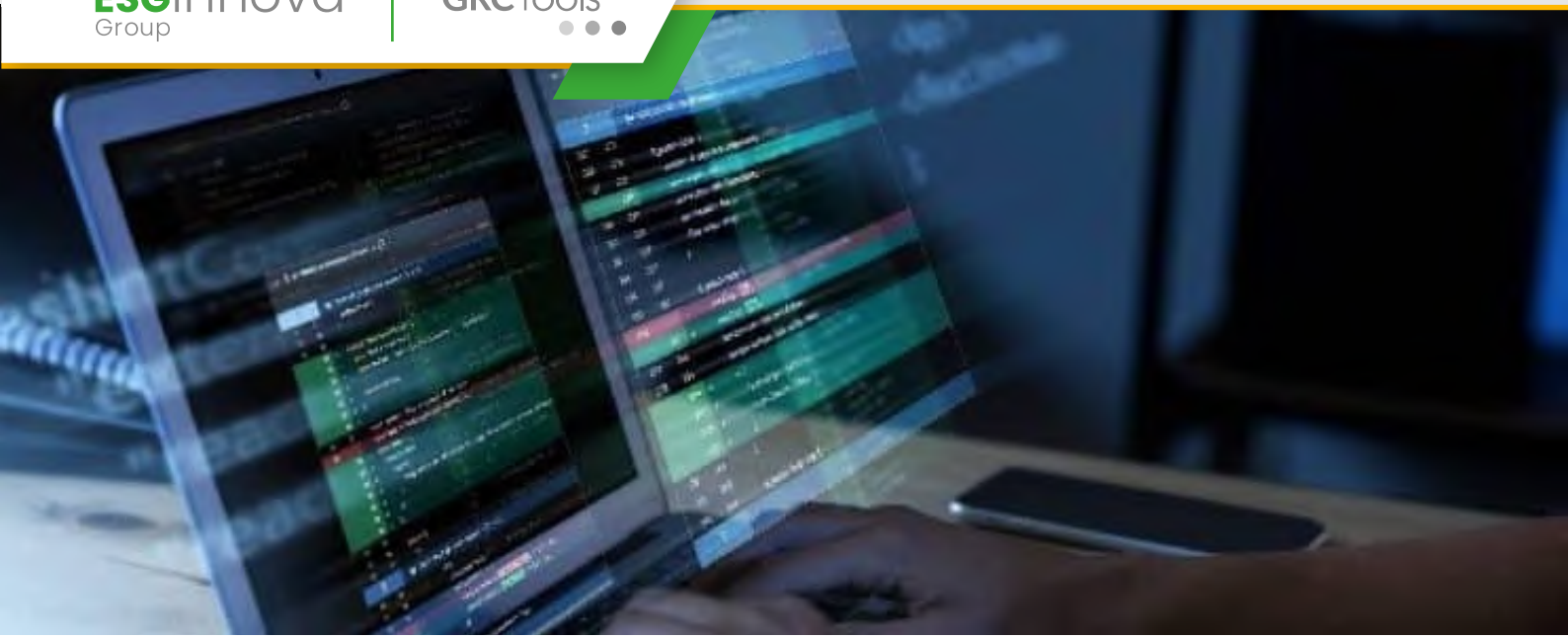
La información es uno de los activos más valiosos para cualquier organización. **La pérdida o exposición de datos sensibles puede afectar la continuidad del negocio, generar sanciones legales y dañar la confianza de los clientes.** Los riesgos más comunes incluyen:

- **Ataques cibernéticos:** Amenazas como ransomware, phishing y malware que buscan comprometer los sistemas de la empresa.
- **Errores humanos:** Fallos en la configuración de sistemas, acceso indebido o eliminación accidental de datos.
- **Cumplimiento normativo:** Incumplir con regulaciones como el GDPR o la Ley de Protección de Datos puede llevar a sanciones significativas.

La seguridad de la información no solo protege los activos de una empresa, sino que también es un diferenciador competitivo en un mercado donde los clientes valoran la privacidad y la integridad.

Herramientas GRC: el aliado ideal para la seguridad de la información

Las **herramientas GRC** se han posicionado como la solución más efectiva para gestionar la seguridad de la información en empresas modernas. Estas plataformas integran la gobernanza, la gestión de riesgos y el cumplimiento normativo en un solo sistema, lo que permite a las organizaciones abordar las amenazas de manera proactiva.



Gestión de riesgos de ciberseguridad con software GRC: Ventajas clave

En un mundo cada vez más digitalizado, los riesgos de ciberseguridad se han convertido en una de las mayores amenazas para las empresas. Desde ataques de ransomware hasta brechas de datos, los ciberataques pueden tener consecuencias devastadoras en términos económicos, legales y reputacionales. **La gestión de riesgos de ciberseguridad es ahora una prioridad estratégica, y el uso de software especializado como GRCTools se ha posicionado como una solución clave para abordar estos desafíos de manera eficaz.**

En este artículo, exploraremos las ventajas de utilizar un software GRC, como GRCTools, para gestionar los riesgos de ciberseguridad en empresas modernas.

¿Por qué es esencial la gestión de riesgos de ciberseguridad?

La gestión de **riesgos de ciberseguridad** afecta a empresas de todos los tamaños y sectores, exponiendo datos sensibles, interrumpiendo operaciones y generando pérdidas económicas. Entre las amenazas más comunes se incluyen:

- **Ataques de ransomware:** Secuestro de datos críticos a cambio de un rescate.
- **ransomware:** Suplantación de identidad para robar credenciales y datos sensibles.
- **Vulnerabilidades en software:** Brechas de seguridad en aplicaciones o sistemas operativos.
- **Accesos no autorizados:** Fallos en la gestión de usuarios y contraseñas.

Sin una gestión adecuada, estas amenazas pueden poner en peligro la continuidad del negocio y la confianza de los clientes.

¿Qué ofrece GRCTools para la gestión de riesgos de ciberseguridad?

GRCTools es una plataforma avanzada diseñada para simplificar y optimizar la gestión de riesgos, incluyendo los asociados a la ciberseguridad. Con un enfoque centralizado e integrado, el software permite a las empresas identificar, evaluar, mitigar y monitorear riesgos de manera eficiente.

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO

Cumplimiento con la Directiva NIS 2: Guía para Entidades Esenciales e Importantes

La Directiva NIS 2 (Network and Information Security Directive 2) representa un hito en la **ciberseguridad europea**. Adoptada por el Parlamento Europeo en 2022, esta normativa **actualiza el marco previo de la Directiva NIS**, con el objetivo de mejorar la resiliencia de las entidades esenciales e importantes frente a las **amenazas digitales**.

En este artículo exploraremos qué implica la Directiva NIS 2, cuáles son sus **principales requisitos** y cómo las organizaciones pueden **garantizar su cumplimiento** para **evitar sanciones** y fortalecer su seguridad.

Directiva NIS 2

La **Directiva NIS 2** establece un marco normativo para **mejorar la seguridad de las redes y sistemas de información** en los países de la Unión Europea.

Esta norma refuerza los requisitos para entidades que desempeñan un **papel clave en sectores críticos**, incluyendo:

- Energía.
- Transporte.
- Salud.
- Infraestructura digital.

Principales diferencias de la Directiva NIS 2 con la original

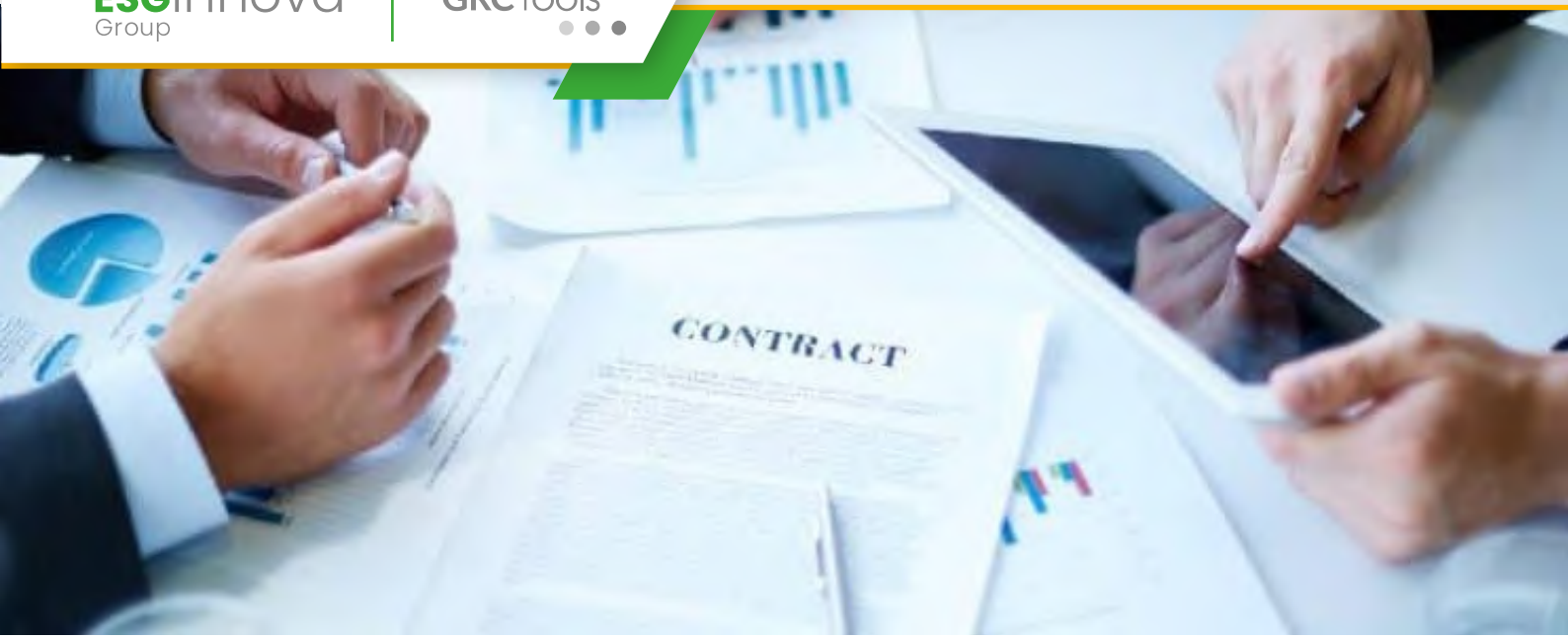
Ampliación del alcance: NIS 2 introduce más sectores y entidades bajo su jurisdicción.

Mayor responsabilidad: Las empresas deben demostrar un cumplimiento activo, no solo reactivo.

Régimen de sanciones más severo: Sanciones significativas por incumplimientos.

Objetivo principal de la Directiva NIS 2

Garantizar que tanto las **entidades esenciales** como las **entidades importantes** implementen medidas robustas para **gestionar y mitigar riesgos** en la ciberseguridad.



Beneficios de implementar software GRC en la gestión de riesgos compliance

¿Cuáles son los problemas más comunes que enfrentan las empresas en el actual entorno empresarial y cómo puede un software GRC, como el que ofrece **GRCTools**, ayudar a resolverlos? Vamos a explorarlo.

La regulación y las exigencias del mercado son cada vez más estrictas, por ello, las empresas enfrentan un reto significativo: mantener un equilibrio entre el cumplimiento normativo y la eficiencia operativa. La **gestión de riesgos de compliance** se ha convertido en una prioridad estratégica para evitar sanciones, salvaguardar la reputación corporativa y garantizar el éxito a largo plazo.

Software GRC: Gestión de riesgos y compliance

La gestión de riesgos de compliance presenta una serie de **desafíos comunes** para las organizaciones, independientemente de su sector. Entre los problemas más frecuentes se encuentran:

1. Fragmentación de la información

Muchas empresas gestionan los riesgos y el cumplimiento normativo a través de sistemas manuales, hojas de cálculo o **herramientas desconectadas entre sí**. Esto genera una fragmentación de la información, **dificultando la trazabilidad y el análisis integral** de los riesgos.

2. Dificultades para mantenerse al día con las normativas

Las regulaciones cambian constantemente, y mantenerse actualizado con las normativas aplicables es un desafío continuo. Las organizaciones suelen carecer de un sistema que automatice el seguimiento de cambios regulatorios y evalúe su **impacto en tiempo real**.

3. Falta de visibilidad y transparencia

La ausencia de un enfoque centralizado y estandarizado para gestionar riesgos y cumplimiento dificulta obtener una visión clara del estado actual de los riesgos en toda la organización. Esto no solo **complica la toma de decisiones**, sino que también puede poner en peligro la reputación empresarial.

4. Procesos manuales propensos a errores

La dependencia de procesos manuales incrementa la **posibilidad de errores humanos**, lo que puede resultar en evaluaciones de riesgos imprecisas, reportes incorrectos o incluso incumplimientos regulatorios.

Prevención de riesgos ambientales en el entorno laboral actual

La prevención de riesgos ambientales se ha convertido en una prioridad en el entorno laboral moderno. Las empresas no solo enfrentan **desafíos** relacionados con la **sostenibilidad**, sino que también tienen la responsabilidad de **garantizar la seguridad de los trabajadores y minimizar el impacto ambiental** de sus operaciones. Este enfoque integral no solo **protege al medio ambiente**, sino que también **mejora la reputación corporativa** y asegura el **cumplimiento de normativas** estrictas.

En este artículo exploraremos qué son los riesgos ambientales, su importancia en el entorno laboral, y cómo prevenirlos de manera efectiva.

Riesgos ambientales

Los **riesgos ambientales** son aquellos factores que, debido a las actividades de una organización, pueden **generar impactos**

negativos en el medio ambiente o **afectar la salud y seguridad** de los trabajadores. Estos riesgos están presentes en diversos sectores, desde la industria manufacturera hasta el sector de servicios.

Ejemplos comunes de riesgos ambientales:

- **Contaminación del aire:** Emisiones de gases nocivos.
- **Gestión inadecuada de residuos:** Desechos peligrosos sin tratamiento adecuado.
- **Vertidos químicos:** Derrames que contaminan suelos y aguas subterráneas.
- **Ruido excesivo:** Que afecta tanto a empleados como a comunidades cercanas.

En el entorno laboral, estos riesgos pueden derivar de procesos operativos, uso de maquinaria, transporte de materiales peligrosos o falta de control en las emisiones. La **prevención eficaz** requiere **identificar estos peligros y tomar medidas** concretas para mitigarlos.

Importancia de la prevención de riesgos ambientales

La **prevención de riesgos ambientales** no solo protege al medio ambiente, sino que también genera **múltiples beneficios** para las empresas y la sociedad.

5 factores de riesgo en Seguridad Vial que debes conocer

La seguridad vial es un componente esencial en la prevención de riesgos laborales, especialmente en empresas cuyos empleados realizan desplazamientos frecuentes. **Identificar los factores de riesgo en seguridad vial permite a las organizaciones tomar medidas proactivas para proteger a sus trabajadores, reducir accidentes y mejorar la eficiencia operativa.**

5 Factores de Riesgo en Seguridad Vial

En este artículo, exploramos cinco factores clave que pueden comprometer la seguridad vial y cómo gestionarlos para minimizar su impacto.

1. Fatiga al volante

La fatiga es uno de los principales factores de riesgo en la seguridad vial.

Conducir durante largas horas sin descansos adecuados reduce los niveles de concentración y aumenta el tiempo de reacción ante imprevistos.

Para mitigar este riesgo, es esencial establecer políticas que limiten las horas de conducción y fomenten pausas regulares durante trayectos largos. Además, promover el descanso adecuado antes de iniciar un viaje es una práctica crucial.

2. Condiciones climáticas adversas

La lluvia, la nieve, el hielo y la niebla son factores que afectan significativamente la seguridad en la carretera. **Estas condiciones disminuyen la visibilidad, reducen la adherencia de los neumáticos y dificultan el control del vehículo.**

Una gestión adecuada de los factores de riesgo en seguridad vial incluye la capacitación en conducción bajo condiciones climáticas adversas, así como el uso de tecnologías como sistemas de asistencia al conductor y vehículos equipados para enfrentar estas situaciones.

3. Distracciones al conducir

Las distracciones, como el uso de dispositivos móviles, comer o manipular equipos en el vehículo, son causas frecuentes de accidentes. **Incluso una distracción de unos segundos puede tener consecuencias graves en la carretera.**

Para minimizar este riesgo, es fundamental concienciar a los empleados sobre la importancia de mantener la atención en la conducción y prohibir el uso de teléfonos móviles mientras están al volante.

Guía completa: Cómo gestionar los riesgos financieros en proyectos

La gestión de riesgos financieros es una parte esencial del éxito de cualquier proyecto. Estos riesgos, que pueden derivarse de factores internos y externos, afectan la estabilidad económica del proyecto, su viabilidad y la capacidad de cumplir con los objetivos establecidos. **Identificar, evaluar y mitigar los riesgos financieros no solo asegura el control de los costos, sino que también refuerza la confianza de los stakeholders y minimiza sorpresas desagradables.**

En esta guía completa, exploraremos las etapas clave para gestionar eficazmente los riesgos financieros en proyectos, así como las herramientas y prácticas recomendadas para lograrlo.

¿Qué son los riesgos financieros en proyectos?

Los **riesgos financieros** en proyectos se refieren a cualquier factor que pueda impactar negativamente el flujo de caja, los presupuestos

o la rentabilidad esperada. Estos riesgos pueden surgir debido a cambios en el mercado, fluctuaciones de precios, incumplimientos contractuales, errores en la planificación financiera o decisiones incorrectas de inversión.

Algunos ejemplos comunes incluyen:

- Incremento inesperado en los costos de los materiales.
- Retrasos en los pagos de clientes o socios.
- Fluctuaciones en los tipos de cambio o tasas de interés.
- Cambios en las regulaciones fiscales o legales.
- Problemas de flujo de efectivo debido a retrasos en la ejecución del proyecto.

La gestión de riesgos corporativos es fundamental para garantizar que el proyecto se mantenga dentro del presupuesto y alcance sus objetivos financieros.

Pasos clave para gestionar los riesgos financieros en proyectos

Una gestión eficaz de riesgos financieros requiere un enfoque estructurado que abarque desde la identificación hasta el monitoreo continuo de los riesgos.

DORA: La nueva regulación de Ciberseguridad para el Sector Financiero

DORA, que significa **Digital Operational Resilience Act**, es una regulación de la Unión Europea destinada a reforzar la resiliencia operativa digital en el sector financiero. Fue adoptada en diciembre de 2022 y entrará en vigor plenamente en 2025. Su objetivo principal es garantizar que las entidades financieras en Europa puedan resistir, responder y recuperarse eficazmente de cualquier incidente cibernético o fallo tecnológico que pueda afectar sus operaciones críticas.

Imagina un banco cuya actividad diaria depende completamente de sistemas digitales para procesar millones de transacciones, resguardar datos confidenciales y atender a sus clientes en tiempo real. Ahora imagina que, de un momento a otro, esos sistemas se detienen debido a un **ciberataque**, exponiendo datos sensibles y generando pérdidas millonarias. Este no es un escenario hipotético: es una realidad que muchas instituciones financieras enfrentan hoy en día.

Ante esta creciente amenaza, la Unión Europea ha implementado la regulación DORA (**Digital Operational Resilience Act**), un marco que busca blindar al sector financiero frente a los riesgos cibernéticos. Pero ¿qué significa esto para las instituciones y cómo pueden adaptarse a los nuevos estándares?

En este artículo, analizaremos los principales problemas de **ciber-seguridad** que enfrenta el sector financiero y cómo el **Software de Ciberseguridad de GRCTools** puede ser la clave para cumplir con **DORA** y fortalecer la resiliencia digital.

Problemas de Ciberseguridad en el sector financiero

El sector financiero es uno de los más atractivos para los ciberdelincuentes debido a la cantidad de **datos sensibles** y recursos económicos que gestiona. Algunos de los problemas más comunes incluyen:

1. Creciente sofisticación de los ataques cibernéticos

Los ataques **de ransomware, phishing y violaciones de datos** han evolucionado, empleando técnicas avanzadas que dificultan su detección. El sector financiero es especialmente vulnerable debido a su dependencia de **tecnologías digitales** para la gestión de transacciones y datos sensibles.

2. Dependencia de terceros proveedores

Muchas instituciones financieras recurren a servicios de proveedores externos, como **plataformas en la nube** y **software de gestión**. Si estos proveedores no cumplen con altos estándares de seguridad, pueden convertirse en una puerta de entrada para los atacantes.

¿Por qué la Gestión Integral de Riesgos es Clave en el Entorno Empresarial Actual?

En un entorno empresarial marcado por la **incertidumbre** y la constante evolución de los mercados, la gestión integral de riesgos ha emergido como un pilar esencial para asegurar la **sostenibilidad y el éxito de las organizaciones.** Este enfoque permite a las empresas identificar, evaluar y mitigar los riesgos que pueden afectar sus operaciones, reputación y objetivos estratégicos.

En este artículo, exploraremos en profundidad qué implica la gestión integral de **riesgos**, por qué es clave para el entorno empresarial actual y cómo implementarla de manera efectiva.

Gestión Integral de Riesgos

La **gestión integral de riesgos** es un enfoque sistemático y estructurado que permite a las organizaciones **identificar, analizar y gestionar los riesgos en todas sus áreas operativas.** A diferencia de la gestión tradicional, que suele centrarse en riesgos específicos o

departamentos aislados, esta metodología abarca una visión global, asegurando que todas las interacciones entre procesos y áreas estén alineadas con los **objetivos estratégicos de la empresa.**

Componentes clave de la gestión integral de riesgos:

- **Identificación de riesgos:** Reconocer amenazas potenciales en todos los ámbitos, desde financieros y operativos hasta tecnológicos y ambientales.
- **Evaluación de riesgos:** Determinar la probabilidad de ocurrencia y el impacto de cada riesgo.
- **Implementación de controles:** Desarrollar medidas para prevenir, mitigar o responder eficazmente a los riesgos.
- **Monitoreo continuo:** Supervisar la evolución de los riesgos y ajustar las estrategias de gestión conforme a los cambios en el entorno.

Importancia de la Gestión Integral de Riesgos

En el entorno empresarial actual, caracterizado por la globalización, la **transformación digital** y un **creciente escrutinio** regulatorio, las empresas enfrentan **riesgos más complejos y diversos** que nunca.

La **gestión integral de riesgos** se convierte en una **ventaja competitiva** al proporcionar **claridad y control** sobre estos desafíos.

Cómo un Software GRC ayuda a cumplir con normativas de seguridad y riesgos

Las empresas en la actualidad necesitan favorecer la protección y el **cumplimiento** de normativas que les aseguren su **continuidad**. Las normativas en constante cambio y las amenazas a la seguridad presentan desafíos significativos en el manejo adecuado de los **riesgos**. En este contexto, las soluciones tecnológicas, como el **Software GRC** (Gobernanza, Riesgo y Cumplimiento) de GRCTools, se presentan como una alternativa indispensable para optimizar el control y garantizar una gestión eficiente de estos aspectos cruciales.

Software GRC: Los problemas que enfrenta el Sector Empresarial

Las empresas de todos los sectores enfrentan diariamente problemas relacionados con la **gestión de riesgos** y el **cumplimiento de normativas**. Estos son algunos de los más comunes:

1. Entornos regulatorios complejos y cambiantes

Las leyes y normativas en materia de seguridad, protección de datos y gestión de riesgos están en constante evolución. Desde regulaciones internacionales como el **RGPD (Reglamento General de Protección de Datos)** hasta estándares específicos como la **ISO 27001** o la **ISO 31000**, las empresas deben adaptarse rápidamente para evitar sanciones y daños reputacionales.

2. Falta de visibilidad sobre los riesgos

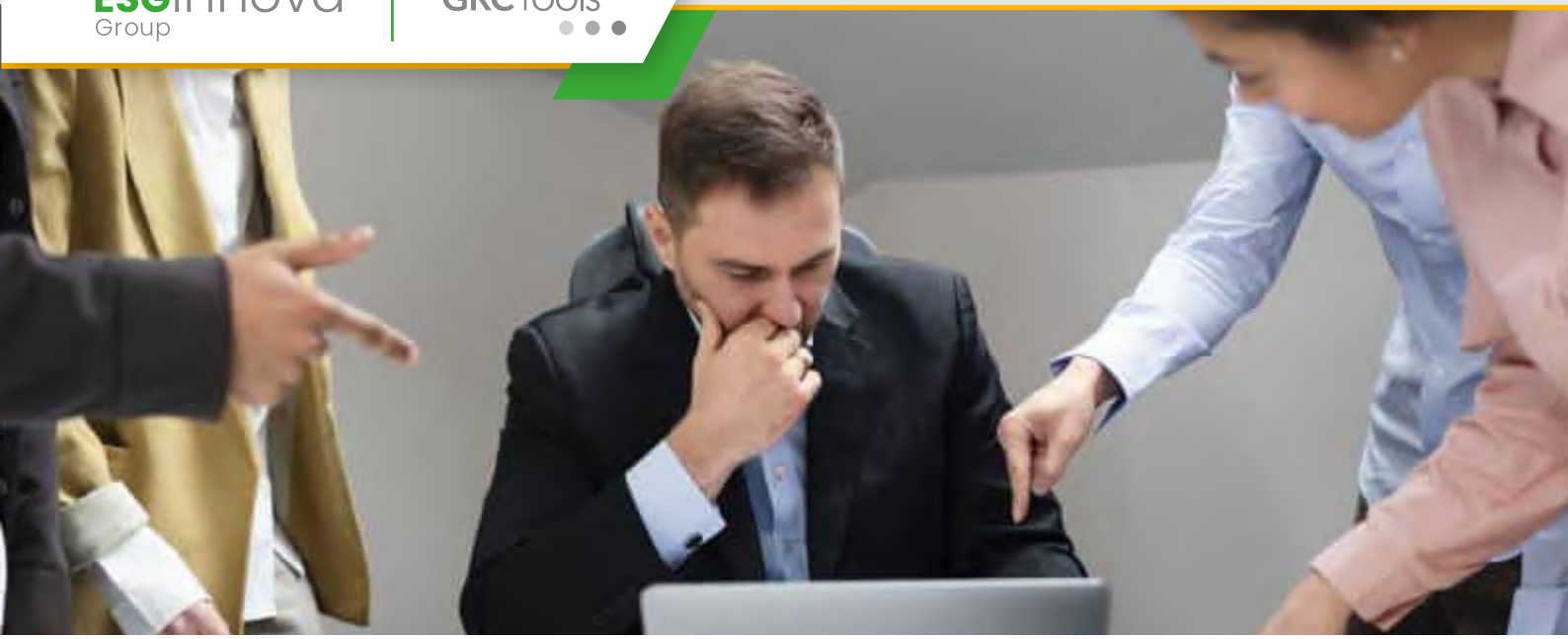
Muchas organizaciones carecen de herramientas centralizadas para identificar, analizar y priorizar riesgos. Esta falta de visibilidad genera una **gestión reactiva**, que aumenta la vulnerabilidad frente a amenazas internas y externas.

3. Procesos manuales y fragmentados

El uso de hojas de cálculo, correos electrónicos y sistemas independientes para gestionar riesgos y cumplimiento **genera ineficiencias y errores**. Estos procesos manuales no solo ralentizan las auditorías, sino que también dificultan el seguimiento de los controles.

4. Costos elevados por incumplimiento

El incumplimiento normativo puede resultar en **multas significativas, litigios legales y pérdida de confianza por parte de clientes e inversores**. Además, la falta de prevención adecuada puede generar costos elevados asociados a incidentes de seguridad o interrupciones operativas.



Gestión integral de riesgos corporativos: herramientas y beneficios

En un entorno empresarial cada vez más complejo y dinámico, la gestión integral de riesgos corporativos es esencial para garantizar la sostenibilidad y el crecimiento de las organizaciones. Los riesgos corporativos, que abarcan desde amenazas operacionales y financieras hasta ciberseguridad y cumplimiento normativo, tienen el potencial de impactar gravemente en los resultados y la reputación de una empresa si no se gestionan de manera efectiva.

En este artículo, exploramos qué implica la gestión integral de **riesgos corporativos,** las herramientas clave para abordarla y los beneficios que aporta a las empresas modernas.

¿Qué es la gestión integral de riesgos corporativos?

La gestión integral de riesgos corporativos (ERM, por sus siglas en inglés) es un enfoque sistemático y estructurado que permite identificar, evaluar, mitigar y monitorear los riesgos que afectan a una

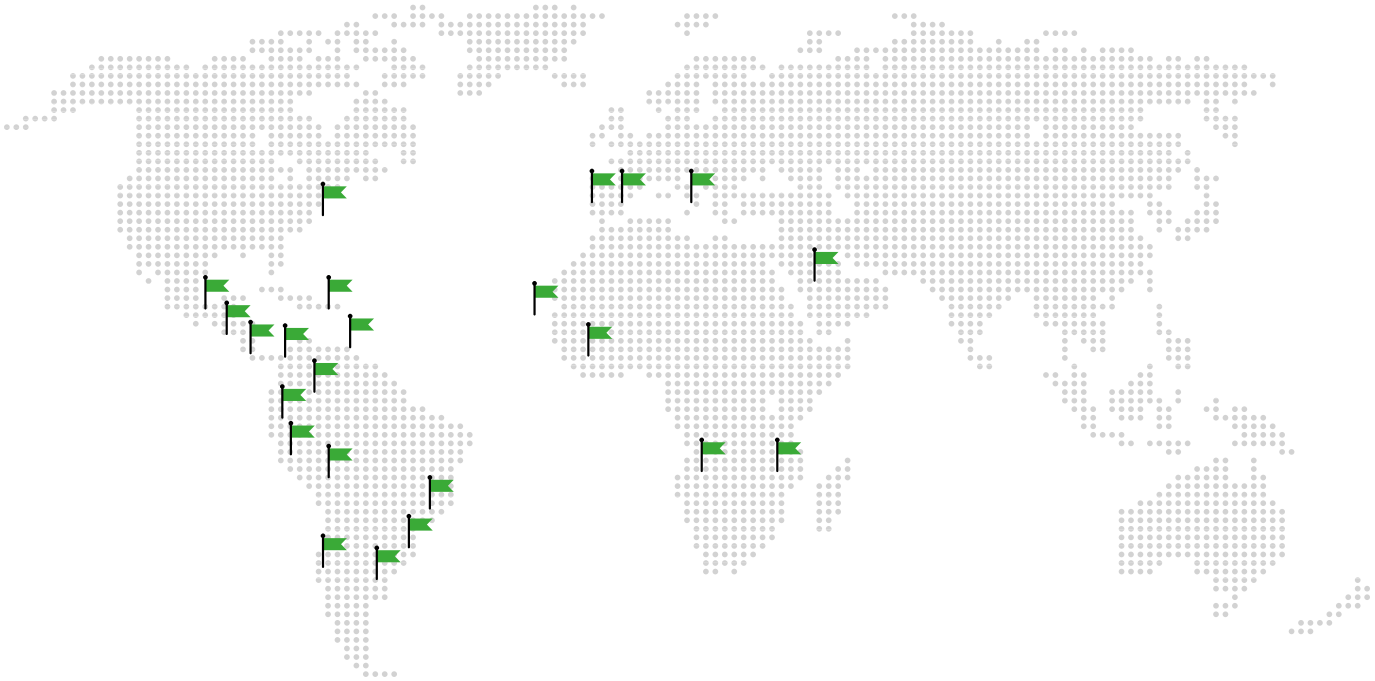
organización. **Este enfoque considera todos los tipos de riesgos, desde los estratégicos y financieros hasta los operacionales y ambientales, asegurando que la empresa esté preparada para enfrentar desafíos en todos los niveles.**

Principales categorías de riesgos corporativos

Los riesgos corporativos pueden clasificarse en varias categorías, entre las cuales destacan:

- **Riesgos estratégicos:** Relacionados con decisiones clave que afectan la dirección de la empresa.
- **Riesgos operacionales:** Asociados a procesos internos, fallos tecnológicos o errores humanos.
- **Riesgos de ciberseguridad:** Amenazas digitales como ataques de ransomware o filtraciones de datos.
- **Riesgos financieros:** Cambios en los mercados, fluctuaciones de divisas o problemas de liquidez.
- **Riesgos de compliance:** Incumplimiento de normativas y regulaciones.
- **Riesgos ambientales:** Impactos negativos relacionados con el entorno natural o regulaciones ambientales.

La gestión integral aborda estos riesgos de manera holística, alineándolos con los objetivos estratégicos de la organización y asegurando una respuesta coordinada y efectiva.



El camino hacia la Excelencia

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

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

+2.500 organizaciones

+25 años

+30 países

+240.000 usuarios

ESGinnova
Group

Córdoba, España

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

Écija, España

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

Santiago de Chile, Chile

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

Lima, Perú

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

Bogotá, Colombia

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

México DF, México

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