EMPRESA **EXCELENTE**

Las mejores temáticas sobre Normas ISO, HSE y GRC

ABRIL 2025

ESGinnova Group

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

Índice

Índice

ESG Innova Group

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

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

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

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

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

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

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

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

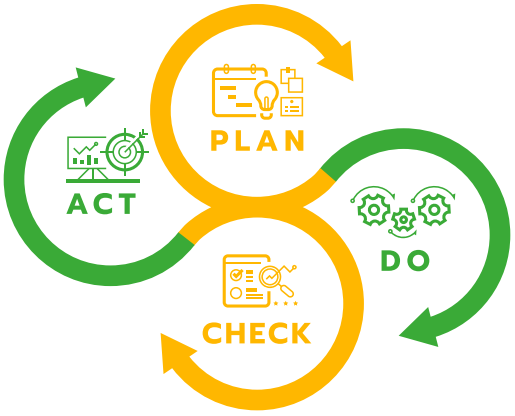
Plataforma ESG Innova

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

❖ Motor de mejora continua

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

ESGinnova Group



❖ Plan

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

❖ Do

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

❖ Check

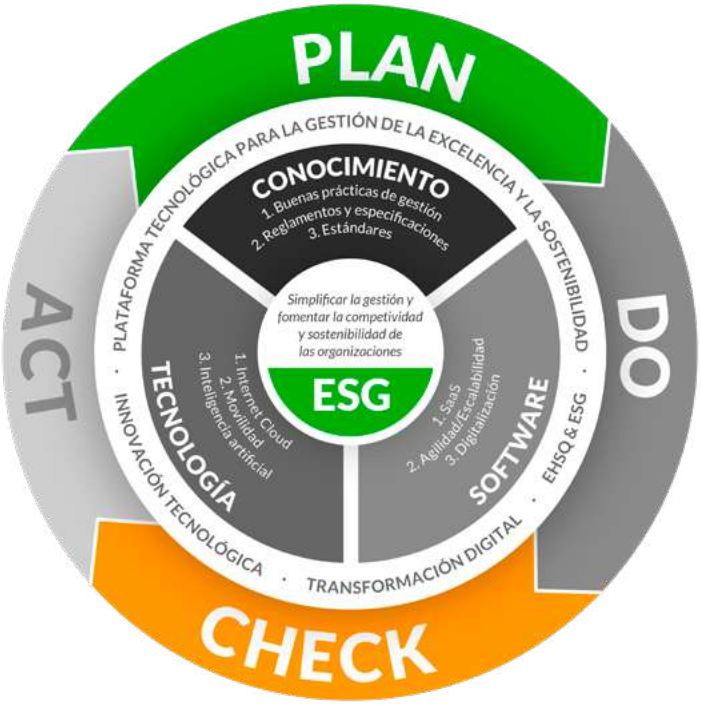
Simplificamos la monitorización y seguimiento, aportando información útil para la toma de decisiones.

❖ Act

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

Unidades de negocio

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



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

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

Unidades de negocio

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

ISOTools

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

HSETools

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

GRCTools

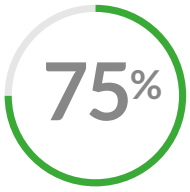
Transformación Digital para la gestión de Gobierno, Riesgo y Cumplimiento.

La Plataforma ESG aporta resultados en el corto plazo

Optimización del tiempo

Menos de tiempo de resolución de una acción correctiva

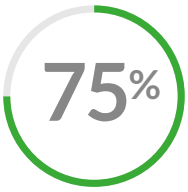
Menos de tiempo de preparación de las reuniones de gestión



Menos de tiempo dedicado a recopilar y tratar indicadores

Optimización de los costes

Menos de intercambios de documentación física entre sedes y dptos.



Menos de costes indirectos derivados de la gestión documental

La inversión se rentabiliza entre el primer y el segundo año

Optimización del rendimiento

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

Más capacidad de resolución de problemas del sistema de gestión

Más de trabajadores implicados en la gestión del sistema

ESGinnova Group

ISOTools

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

Incidentes de ciberseguridad: plan de respuesta para mitigar riesgos

En el escenario digital en el que están inmersas organizaciones de todos los tamaños y sectores, la **gestión de la seguridad de la información** es clave. Los **incidentes de ciberseguridad** son una de las grandes preocupaciones, pero hay acciones y estrategias válidas para prevenirlos y evitar sus nefastas consecuencias.

Es preciso, para ello, contar con un plan de respuesta para minimizar el impacto negativo. **Las empresas necesitan trabajar para tener escudos de defensa** apropiados para proteger sus datos y su información de cualquier tipo de incidentes de ciberseguridad, como se verá a continuación.

Qué es un plan de respuesta a incidentes de ciberseguridad

El plan de respuesta a incidentes de ciberseguridad entrega una guía sistemática para **detener el avance del ataque, proteger**

la información y los datos esenciales, alertar sobre el evento e iniciar procesos de investigación, análisis, evaluación y corrección para evitar que se repita.

El plan de respuesta para mitigar los riesgos de los incidentes de ciberseguridad, recoge paso a paso la forma de proceder de cada empleado con funciones críticas afectadas. Además, **asigna responsabilidades, crea un flujo de alerta** para informar sobre lo que está ocurriendo y sobre los recursos que se necesitarán para atender la emergencia y prevé sistemas alternos que se pondrán en marcha para mantener la operabilidad de la empresa en condiciones mínimas.

Por qué es preciso contar con un plan de respuesta a incidentes de ciberseguridad

Las **vulnerabilidades de la seguridad de la información** están en la base de muchos incidentes de ciberseguridad, y estos pueden generan pánico. Si no se responde de forma adecuada, el daño se extenderá por todos los dispositivos de la organización. Al contrario, si existe **una guía precisa, clara y probada para hacer lo que es correcto y minimizar el impacto negativo, los daños serán irrelevantes.**

Un plan de respuesta diseñado con base en elementos técnicos y enfocado en la estructura tecnológica y de recursos humanos de la organización podrá mitigar el impacto inmediato, pero también **tratará los riesgos legales y regulatorios asociados a la ocurrencia de un ciberataque**. La respuesta a un incidente de ciberseguridad necesita ajustarse a los requisitos legales y regulatorios que enmarcan la gestión de seguridad de información y datos en momentos de normalidad.

Sistemas de IA de alto riesgo según la Ley de Inteligencia Artificial de la UE

La Inteligencia Artificial ha irrumpido en todos los ámbitos y sectores comerciales, industriales y sociales. Las oportunidades son muchas y muy atractivas, pero también es preciso considerar riesgos. Para ello surgen estándares como **ISO 42001** o normas como la Ley de Inteligencia Artificial de la Unión Europea, que reconoce que existen **sistemas de IA de alto riesgo** y que estos están sujetos a requisitos acordes con el desafío que representa su gestión segura.

Si bien todas las aplicaciones y desarrollos de esta tecnología plantean riesgos, es evidente que existen sistemas de IA de alto riesgo que despiertan preocupaciones adicionales **por sus funcionalidades, por el sector en el que operan o por el acceso ilimitado que los caracterizan**, entre otras razones.

Qué son sistemas de IA de alto riesgo

La **Ley de Inteligencia Artificial de la UE** define los sistemas de IA

de alto riesgo como aquellos que **tienen una capacidad superior para ocasionar daños a las personas**, afectar a su integridad o su seguridad, vulnerar sus derechos fundamentales, invadir su privacidad o inducirlas a tomar decisiones de las que no son conscientes. Los sistemas de IA de alto riesgo se categorizan de acuerdo con el nivel de daño que pueden causar como consecuencia de su **uso indebido o de fallos en su funcionamiento**, usualmente asociados a sesgos en el aprendizaje del sistema.

Aunque los sistemas de IA de alto riesgo, de acuerdo con la Ley de IA de la UE, se clasifican en dos grandes grupos, lo cierto es que **estos sistemas pueden trabajar en áreas críticas como el sector sanitario, educación, RR. HH., seguridad o gestión de infraestructuras**. Algunos ejemplos de los riesgos asociados al uso de IA en estos sectores son los siguientes:

Sector	Riesgos
Sanitario	Diagnósticos errados o sesgos a la hora de asignar tratamientos o medicamentos.
Educación	Sistemas entrenados con sesgos limitarían las opciones futuras de algunos estudiantes.
RR. HH.	Los sistemas podrían conducir la contratación en favor de personas utilizando criterios religiosos, políticos, sociales, étnicos o de género.
Seguridad	Invasión de la privacidad o restricciones de acceso a ciertos lugares con base en sesgos de los algoritmos.
Infraestructuras	Fallos que pueden interrumpir el suministro de servicios públicos esenciales para algunas personas.

Factores de riesgo ambiental: evaluación y estrategias de respuesta

Identificar los **factores de riesgo ambiental** es un proceso esencial para las empresas comprometidas con la **gestión ambiental**. Permite anticiparse a posibles daños, realizar evaluaciones técnicas efectivas y diseñar estrategias de respuesta que eviten consecuencias negativas para el entorno, la comunidad y para la propia organización.

En un escenario de presión social y regulatoria cada vez mayor, la identificación de los factores de riesgo ambiental ayuda a las organizaciones a **enfocar los esfuerzos de gestión en las áreas y los procesos que generan verdaderas amenazas.** Operar con responsabilidad permite contribuir a la preservación del planeta y ganar legitimidad ante los grupos de interés.

Qué es una evaluación de factores de riesgo ambiental

La evaluación de factores de riesgo ambiental busca **identificar, evaluar, calificar y priorizar los elementos o determinantes de**

riesgos asociados con la operación de una organización. El objetivo principal es entender cuáles son las condiciones o los elementos que tienen la capacidad para generar riesgos.

La información recibida es esencial en la **gestión de riesgos ambientales**, sirve para **abordar de forma efectiva las amenazas**, eliminando o reduciendo su capacidad de daño negativo. Pero, además, la evaluación de factores de riesgo ambiental también resulta de gran utilidad para el área de cumplimiento. La detección oportuna de factores de riesgo asegura el cumplimiento de normas, leyes o directivas en el área ambiental.

Por qué es importante la evaluación de factores de riesgo ambiental

La evaluación de factores de riesgo ambiental muestra a los equipos de gestión los elementos o las condiciones que tienen mayor capacidad para generar afectaciones negativas al medio ambiente, pero la tarea ofrece otros **beneficios destacados**:

1. Mejora el cumplimiento de la organización

Conocer los factores de riesgo ambiental es el primer paso para diseñar estrategias efectivas para proteger los recursos naturales y garantizar la calidad del aire, entre otras tareas que son solicitudes normativas o regulatorias de alcance local, regional, nacional o internacional. **Las empresas evitan multas, sanciones y deterioro de su reputación**.

2. Protege de forma efectiva el ambiente y el entorno

Muchas de las acciones que emprenden los equipos de gestión ambiental no tienen un impacto directo sobre el medio ambiente.

Sanciones de la Ley de IA de la UE: el alto coste del incumplimiento

La Ley de IA de la Unión Europea es pionera en el mundo en su clase y se convierte en punto de referencia obligado para los estados que intentan regular el uso de la **Inteligencia Artificial**. Las **sanciones de la Ley de IA de la UE** por el incumplimiento de sus disposiciones siguen un sistema escalonado, en el que las infracciones más graves conllevan sanciones más severas.

Una de las características más interesantes de esta ley es la distinción que hace de los obligados a su cumplimiento de acuerdo con su nivel de riesgo. Las sanciones de la Ley de IA de la UE son proporcionales al nivel de riesgo en el que se clasifica a los obligados. En general, esta ley **impone las sanciones más altas en su segmento**, incluso superiores a las determinadas por el RGPD o el **Reglamento de Resiliencia Operativa Digital (DORA)**.

Qué enfoque se utiliza para establecer las sanciones de la Ley de IA de la UE

Para entender el enfoque escalonado de sanciones de la Ley de IA de la UE es preciso conocer quiénes son los obligados a cumplir con los requisitos. **La ley se dirige a tres grupos de organizaciones**: operadores de sistemas de Inteligencia Artificial, proveedores de modelos de IA de propósito general e instituciones y organismos de la Unión Europea.

Para cada uno de estos actores obligados existe un escalafón de sanciones. Existen tres niveles de gravedad, de acuerdo con el nivel de riesgo del infractor, para el primer grupo, que es el de operadores de sistemas de IA. La escala de sanciones de la Ley de IA de la UE prevé sanciones específicas para los proveedores de modelos de propósito general y dos niveles de sanciones para las instituciones y organismos de la Unión Europea.

Sanciones de la Ley de IA de la UE para los operadores de sistemas de IA

Las sanciones de la Ley de IA de la UE para los operadores de sistemas de IA se clasifican en tres diferentes niveles, de acuerdo con el tipo de incumplimiento así:

1. Primer nivel: incumplimiento de prohibiciones

En este primer nivel de gravedad, las multas se imponen por incumplir la prohibición de utilizar o poner a disposición de usuarios sistemas prohibidos de forma expresa por la **Ley de Inteligencia Artificial de la UE**.

¿Cuáles son los principios de implementación ESG de IWA 48:2024?

La IWA 48:2024 no es una norma certificable, pero sí una referencia clave que orienta a las empresas hacia una gestión responsable y sostenible, alineada con las expectativas de inversores, consumidores, organismos reguladores y la sociedad en su conjunto. Su valor reside en traducir conceptos ESG en **principios operativos** que permiten transformar la cultura organizacional, los procesos de decisión y la gestión de riesgos y oportunidades.

¿Qué es la IWA 48:2024 y por qué es relevante?

La **IWA (International Workshop Agreement) 48:2024** es una publicación reciente de ISO que proporciona principios y orientaciones para la implementación de prácticas ESG dentro de las organizaciones. A diferencia de otras normas ISO, una IWA se construye a través de talleres colaborativos entre expertos de diversos sectores, lo que permite una respuesta ágil a necesidades emergentes, como lo es el enfoque ESG.

Esta guía se enfoca en ofrecer una estructura que permita:

- **Comprender e integrar los riesgos y oportunidades ESG**.
- **Tomar decisiones basadas en evidencias y expectativas de las partes interesadas**.
- Asegurar la **coherencia** entre la estrategia, los valores y la operación diaria de la organización.

Su implementación es especialmente relevante en el actual escenario regulatorio, donde normativas como la **CSRD (Corporate Sustainability Reporting Directive)** en Europa, las normas **GRI**, **SASB**, o los estándares de **IFRS/ISSB**, requieren mayor trazabilidad, transparencia y rendición de cuentas sobre el desempeño no financiero de las organizaciones.

Los 12 principios de implementación ESG según la IWA 48:2024

La IWA 48:2024 establece **12 principios fundamentales** para guiar la implementación efectiva de un enfoque ESG. Estos principios están diseñados para ser integrados en los **Sistemas de Gestión existentes** o en nuevos modelos de gobernanza sostenible.

1. Debida diligencia en IWA 48:2024

Las organizaciones deben aplicar procesos estructurados para **identificar, prevenir, mitigar y remediar impactos negativos** reales o potenciales relacionados con factores ESG, tanto propios como en su cadena de valor.

Qué debe contener la politica ambiental norma ISO 14001

La politica ambiental es el **corazón del Sistema de Gestión Ambiental (SGA)** según la norma ISO 14001. No se trata simplemente de un documento decorativo o un compromiso genérico. Es una declaración estratégica que define la postura de una organización frente a la protección del medio ambiente, el cumplimiento legal y la mejora continua. En un contexto global cada vez más consciente de la sostenibilidad, contar con una política ambiental sólida, actualizada y coherente con los principios de la **ISO 14001:2015**, es clave para cualquier organización que aspire a operar de manera responsable y resiliente.

Con la última versión de la norma ISO 14001, se han introducido mejoras significativas que amplían la perspectiva del desempeño ambiental. Hoy se exige una comprensión más profunda del **contexto organizacional**, una participación más activa del **liderazgo** y una **visión estratégica a largo plazo**, que permita integrar el **SGA** con otros sistemas de gestión y objetivos corporativos. Esta evolución responde a una necesidad urgente: que las empresas no solo reduzcan sus impactos, sino que se conviertan en **agentes de cambio hacia un desarrollo sostenible real**.

Los elementos esenciales de una politica ambiental norma ISO 14001

Según la norma ISO 14001:2015, la política ambiental debe construirse a partir de tres grandes compromisos, fundamentales para la gestión ambiental moderna:

1. Compromiso con la protección del medio ambiente

Este compromiso debe ir más allá de la simple prevención de la contaminación. Las organizaciones deben considerar acciones específicas como la **gestión eficiente de recursos naturales**, la **mitigación del cambio climático**, la **conservación de la biodiversidad** y el impulso de prácticas sostenibles en toda su cadena de valor. La política debe reflejar estas intenciones de forma clara y específica.

2. Compromiso con el cumplimiento de requisitos legales y otros compromisos aplicables

La organización debe declarar expresamente su voluntad de cumplir con toda la **normativa ambiental vigente a nivel local, nacional e internacional**, así como con otros requisitos voluntarios que haya adoptado (certificaciones, acuerdos sectoriales, compromisos públicos, etc.). Este cumplimiento debe estar integrado en la cultura organizacional.

3. Compromiso con la mejora continua

La política debe fomentar una actitud proactiva hacia la mejora continua del SGA, enfocándose en el **desempeño ambiental**.

Software para gestionar ISO 27001: funcionalidades clave que debe tener

Afrontar la carga documental y operativa que implica la implementación del estándar es la razón por la que muchas organizaciones optan por apoyarse en un **software para gestionar ISO 27001**. Es la herramienta más eficiente para cumplir con los requisitos que exige un sistema de gestión de Seguridad de la Información en lo que respecta a documentos, asociados con la complejidad de los riesgos que se espera tratar.

Es el primer desafío que necesitan afrontar los equipos de implementación de la norma. El número de documentos, el control de versiones, el flujo del proceso de aprobación y la estimación del periodo de vigencia son, entre otros, retos que se espera resolver con ayuda de un software para gestionar ISO 27001.

Problemas de gestión de documentos que resuelve un software para gestionar ISO 27001

El software para gestionar ISO 27001 busca resolver los **desafíos que plantea la implementación y mantenimiento de un SGSI** basado en la norma internacional. Entre ellos, los que requieren atención inmediata en la etapa de implementación son los que conciernen a la **gestión de documentos**. Los cinco más relevantes son los siguientes:

1. Accesibilidad de los documentos

La facilidad de acceso a los documentos es clave para la operatividad de un sistema de gestión documental. Sin embargo, en sistemas no automatizados puede convertirse en un reto. No solo la accesibilidad, sino poder disponer de información actualizada y perfectamente organizada, cuestiones que resuelve un software para gestionar ISO 27001.

2. Falta de un procedimiento claro de creación, modificación y aprobación

Los documentos que no siguen una ruta jerárquica de aprobación y que no están sujetos a ningún control **representan un riesgo de no conformidad** y de difusión de información errónea, sin mencionar la posibilidad de duplicidad o de incumplimientos.

3. Acceso ilimitado a los documentos

Un **sistema de gestión de Seguridad de la Información** requiere documentos públicos, documentos de acceso limitado y documentos reservados solo para la Alta Dirección.

Cómo evaluar y abordar los riesgos de la Inteligencia Artificial con la norma ISO/IEC 42001:2023

La implementación de la norma **ISO 42001** crece a ritmo acelerado alrededor del mundo, demostrando que es la herramienta más eficaz para evaluar y gestionar los **riesgos de la Inteligencia Artificial**.

La gestión de los riesgos de la Inteligencia Artificial bajo los requisitos del estándar ISO 42001 guarda algunas similitudes con la gestión de seguridad de **ISO 27001**. No obstante, la norma de IA **entrega un enfoque holístico e integral, aportando controles específicos** para los riesgos que implica la nueva tecnología.

Los requisitos para la gestión de riesgos de la Inteligencia Artificial **aparecen en las cláusulas 6.1.2 a 6.1.4**. Es en estos apartados del estándar donde se incluyen los requisitos críticos sobre los que el auditor enfocará su atención para avalar el sistema de gestión y recomendar la certificación.

Requisitos de ISO 42001 para la gestión de riesgos de la Inteligencia Artificial

ISO 42001 es un estándar diseñado para ayudar no solo a las organizaciones que desarrollan o utilizan **sistemas de IA de alto riesgo**, si no a todas aquellas que los usan, a **tratar las amenazas asociadas a esta tecnología de manera proactiva**, eficaz y responsable.

Para hacerlo, la gestión de riesgos de la Inteligencia Artificial **solicita a las organizaciones, realizar tres actividades clave**, que son las requeridas en las mencionadas cláusulas 6.1.2. a 6.1.4. Estas son las siguientes:

1. Evaluación de riesgos de la Inteligencia Artificial

La evaluación de riesgos de la Inteligencia Artificial **busca identificar las amenazas, estableciendo la gravedad del posible impacto** y la probabilidad de ocurrencia. El propósito es obtener una lista priorizada de los riesgos a los que están expuestas las organizaciones, las personas, los consumidores, los empleados y otras partes interesadas.

En este listado **aparecerán riesgos relacionados con seguridad de la información, sesgos en toma de decisiones**, entrenamiento no intencionado y violaciones de derechos de autor de las personas, entre otros.

Proceso de gestión de calidad: 6 señales de que está fallando

Para saber si un **proceso de gestión de calidad** es eficiente, funciona bien y cumple con el propósito para el que fue diseñado o con los requisitos de estándares como **ISO 9001**, las empresas disponen de herramientas como las revisiones, las auditorías o las inspecciones.

El problema está en que cuando entran en acción los inspectores o los auditores, algunos **fallos en el proceso de gestión de calidad pueden haber provocado ya consecuencias negativas**: retirada de productos, reclamaciones multitudinarias de consumidores o multas y sanciones millonarias impuestas por reguladores.

Es preciso contar con algún tipo de **instrumento que permita medir el pulso al proceso de gestión de calidad**, con mayor frecuencia y menos formalismos, antes de que el valor de las multas o la afectación a la reputación sean irreversibles.

Señales de que un proceso de gestión de calidad está fallando

El proceso de gestión de calidad no es estático. Pensar que funciona porque el auditor que lo evaluó hace dos años así lo consignó, es un error. Lo es más cuando la empresa ha emprendido nuevos negocios desde la **auditoría de calidad**, ha agregado líneas de productos o ha sustituido muchos procesos por causa de la automatización.

Por eso es esencial contar con un detector de fallos que permita **identificar debilidades, no conformidades o desviaciones** en el proceso de gestión de calidad. Si ese teórico detector existiese, probablemente se enfocaría en encontrar errores que son comunes, como los siguientes:

1. Brechas de cumplimiento para aprobar una auditoría

Un proceso de gestión de calidad eficaz tendría que estar preparado para una auditoría sorpresa o una revisión inmediata en todo momento. En algunos casos, **la dificultad para afrontar una auditoría puede estar relacionada con problemas para reunir la documentación** y los registros que solicitará el auditor como evidencia. Esto, además de indicar lo ya señalado, significa que el proceso está clamando por automatización y digitalización.

2. Procesos, procedimientos y documentos en papel

Los sistemas en papel resultan poco eficientes. Resultan engorrosos, proclives al error, ralentizadores y fuentes de otros muchos problemas, sobre todo en organizaciones de gran tamaño o en plena expansión.

ESGinnova
Group

HSE Tools

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

Regulaciones ambientales: cómo hacer seguimiento de normativas y riesgos con un software HSE

Cumplir las **regulaciones ambientales** es tan importante como gestionar los riesgos que tienen capacidad para deteriorar los recursos naturales, afectar el clima o destruir la biodiversidad. Para ello, es preciso conocer obligaciones, leyes y requisitos, pero también realizar una adecuada **gestión de documentos** y una permanente vigilancia de la evolución de las normas. Una herramienta eficaz para ello es una aplicación HSE.

El cumplimiento de las regulaciones ambientales tiene un impacto positivo e inmediato en la seguridad de los trabajadores, en su salud y, por supuesto, en los esfuerzos para proteger el entorno. **El software HSE ayuda a las organizaciones a conservar o mejorar el cumplimiento de las regulaciones ambientales**.

Cómo un software HSE monitorea y hace seguimiento al cumplimiento de las regulaciones ambientales

Si se expresara la colaboración que presta el software HSE en el cumplimiento de las regulaciones ambientales, se podría afirmar que lo hace mediante **un seguimiento constante a las normas, leyes y otras obligaciones en el área**. Algunas de las formas en que lo realiza son las siguientes:

1. Rastrea el movimiento regulatorio

El marco regulatorio ambiental es muy dinámico e imprevisible. Dos razones lo explican: las nuevas regulaciones que provienen de la multitud de foros internacionales que se realizan cada año y el acontecer climático y atmosférico, que presiona la implementación de nuevas exigencias. Por citar solo un año como ejemplo, 2024 presenció la realización de tres COPs, cada una de ellas con nuevas solicitudes. Pero también **es preciso vigilar el acontecer legislativo nacional y supranacional**, que en el caso de Europa es generoso. La tarea es abrumadora, pero un **software HSE tiene capacidad para rastrear de forma automática fuentes de regulaciones ambientales**. De esta forma, alerta sobre la aparición de alguna norma, la modificación de otra o la extinción de un buen número de ellas. Esto se extiende a los requisitos para obtener licencias o permisos para operar en determinadas áreas, todo ello en tiempo real.

2. Monitorea el comportamiento de indicadores y métricas

En el área ambiental los indicadores y las métricas lo son todo. Los **KPIs de HSE** determinan si se están haciendo bien o no las cosas, pero también **son la evidencia que solicitan muchas regulaciones ambientales**.

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO

Riesgos de seguridad de los contratistas: peligros comunes en las operaciones de los contratistas

Los **riesgos de seguridad de los contratistas** se han convertido en un apartado de importancia estratégica en la gestión de seguridad y salud en una empresa. En el complejo panorama corporativo moderno, los contratistas son la fuerza laboral que hace posible culminar muchos proyectos gracias a la movilidad que los caracteriza y al valioso aporte de conocimiento y experiencia en áreas en las que la organización no puede contar con empleados fijos.

Identificar y tratar los riesgos de seguridad de los contratistas **es tan importante como velar por el bienestar de los empleados**. Es necesario considerar que, en muchas ocasiones, los contratistas trabajan en condiciones extremas, en ubicaciones remotas y bajo presiones inusuales.

Qué es la gestión de riesgos de seguridad de los contratistas

La gestión de riesgos de seguridad de los contratistas es el proceso sistemático utilizado para **identificar, evaluar, priorizar y tratar las amenazas de todo tipo** a las que puede estar expuesta la fuerza laboral externa de la organización en su relación con esta. La gestión de riesgos de seguridad de los contratistas **tiene alcance durante todo el ciclo de vida de un contrato**, desde la selección y contratación hasta el cierre final, que llega con la liquidación total del contrato. El alcance es también sobre todas las ubicaciones en las que el contratista desarrolle sus tareas, sean estas instalaciones de la organización o no. La gestión de seguridad de los contratistas **es una labor proactiva.** Tiene un claro enfoque en la **prevención de riesgos laborales**, pero también incorpora acciones reactivas en caso de que un riesgo no se pueda contener. El primer objetivo es eliminar los riesgos. De no ser posible se implementarán acciones para mitigarlo o trasladarlo. Es importante entender que, en algunos casos, los contratistas comparten espacios con empleados de la organización y, por tanto, riesgos. Esto implica que **cuidar la seguridad de los contratistas puede ser, a la vez, cuidar la de los propios trabajadores de la empresa**.

Cuáles son los riesgos de seguridad de los contratistas más comunes

El primer paso para gestionar los riesgos de seguridad de los contratistas es saber cuáles son para poder hacer una primera aproximación que **servirá para determinar la acción de tratamiento más efectiva**.

Cómo realizar evaluaciones ergonómicas para prevenir lesiones y problemas de salud ocupacional

La **vigilancia de la salud** incluye infinidad de aspectos. Todos son importantes, pero en algunos casos, como puede ocurrir con las **evaluaciones ergonómicas**, pasan inadvertidos o a un segundo plano. Eso ocurre cuando la gestión SST se enfoca en riesgos que tienen un impacto más inmediato entre los empleados.

Los accidentes tienen consecuencias inmediatas y evidentes. Por ello, las estrategias que rebajan el número de lesionados adquieren gran visibilidad ante las partes interesadas. Las evaluaciones ergonómicas, por su parte, **tratan de prevenir problemas que se manifestarán en el futuro**. Es posible, incluso, que el empleado ya no esté en la empresa cuando sufra las consecuencias de no haber integrado la **ergonomía en el trabajo**.

Por qué realizar evaluaciones ergonómicas

Las evaluaciones ergonómicas son actividades necesarias que, como cualquier tarea relevante, **consumen recursos humanos, tecnológicos y financieros**, además de tiempo. Es probable que existan empresas en las que la decisión de hacerlo requiera aval de la Alta Dirección, sobre todo por el impacto económico que tienen las medidas destinadas a prevenir este tipo de riesgos. Sin embargo, los beneficios son muchos:

1. Beneficios económicos

El primer y el mejor argumento para vender cualquier proyecto a la Alta Dirección de cualquier empresa siempre será el que muestra beneficios económicos. Las evaluaciones ergonómicas, y sus efectos, **permitirán disminuir el absentismo laboral y disminuir los costes de atención médica.** Todo ello, sin mencionar los errores que puede cometer un empleado que no está entrenado para ocupar el puesto que deja el trabajador ausente. También **se evitan los costes de las reclamaciones judiciales** de empleados que hayan desarrollado problemas músculo-esqueléticos por falta de atención al problema en su empresa.

2. Aumento de la productividad

Un empleado que realiza tareas en **condiciones de incomodidad disminuye de forma paulatina su productividad**. Las organizaciones necesitan garantizar la seguridad y la salud, pero también la comodidad si esperan un aumento sostenido de los niveles de productividad.

Transformación digital para evitar costes excesivos en las auditorías internas

Las **auditorías internas** desempeñan un papel crucial en la solidez y mejora continua de los **sistemas de gestión**, especialmente en áreas clave como **Salud, Seguridad y Medio Ambiente (HSE)**. No obstante, a medida que las regulaciones se intensifican y las expectativas sociales en materia de sostenibilidad aumentan, muchas organizaciones se ven desbordadas por el alto coste oculto que conllevan los procesos de **inspecciones y checklist**, tanto en términos económicos como operativos. En este contexto, muchas organizaciones buscan alternativas que les permitan **evitar costes excesivos en las auditorías internas** sin comprometer la calidad del proceso ni su impacto estratégico.

El coste oculto de las auditorías internas tradicionales

Expertos como **Richard F. Chambers**, expresidente del *Institute of Internal Auditors (IIA),* y **Norman Marks**, referente mundial en auditoría interna y gestión de riesgos, han aportado perspectivas

críticas sobre el verdadero coste de las auditorías internas. En su libro *The Speed of Risk: Lessons Learned on the Audit Trail,* Chambers plantea la urgencia de «auditar a la velocidad del riesgo» y al ritmo que impone el negocio moderno. Su enfoque promueve auditorías más ágiles, enfocadas en los riesgos clave y adaptadas tecnológicamente.

Por su parte, Marks, autor de obras como *Auditing that Matters* y *Auditing at the Speed of Risk*, advierte que muchas auditorías fallan al enfocarse en aspectos que no aportan valor al negocio. Desde su experiencia como Chief Risk Officer y consultor internacional, enfatiza que «una auditoría no debe durar más de lo que vale su contribución al negocio».

Encuestas recientes revelan que una auditoría interna promedio puede consumir entre **300 y 1.500 horas de trabajo**, y en algunos casos superarlas. Este esfuerzo no solo implica el coste directo de los equipos de auditoría, sino también la interrupción de las operaciones y el tiempo del personal operativo, lo que se traduce en una pérdida de eficiencia global.

La transformación digital como respuesta inteligente y estratégica para evitar costes excesivos en las auditorías internas

Ante un contexto de creciente **complejidad regulatoria**, presión por la **eficiencia** y demandas sociales en materia de **sostenibilidad**, la transformación digital se posiciona como una respuesta estratégica para las organizaciones que buscan optimizar sus **auditorías internas** sin comprometer la calidad ni el cumplimiento. Especialmente en el ámbito de **Salud, Seguridad y Medio Ambiente (HSE)**.

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO

Mitigación de riesgos del contratista: estrategias y buenas prácticas para la mejora continua

La **mitigación de riesgos del contratista** es uno de los objetivos de aquellas organizaciones que trabajan con terceros. La **gestión de contratistas** tiene en cuenta, entre otros aspectos, que la fuerza laboral externa está expuesta a riesgos específicos relacionados con el tipo de trabajo que realiza, los lugares en los que desarrolla sus actividades y su condición itinerante, entre otras razones

La mitigación de riesgos del contratista parte de la premisa de que **no todas las amenazas se pueden eliminar, pero sí es posible mitigar el impacto negativo** o la probabilidad de que ocurran con una adecuada gestión.

Qué es la gestión de riegos de contratistas

Muchas industrias aprovechan las **ventajas estratégicas que representan los contratistas** para el desarrollo de sus proyectos. Sin embargo, las mismas características que hacen que resulten tan atractivos para las empresas, son las que originan los riesgos a los que están expuestos. La gestión de riesgos de contratistas es el apartado de la **gestión HSE** de las organizaciones que se ocupa de **identificar, evaluar, priorizar y diseñar las estrategias para eliminar o mitigar** los riesgos que afectan a la fuerza laboral externa. La mitigación de riesgos del contratista busca, además, **asegurar recursos y "propietarios del riesgo".** El propietario es la persona que asumirá la responsabilidad de implementar las estrategias, monitorearlas y rendir informes sobre la efectividad o inocuidad de las acciones. Gestionar los riesgos de terceros es importante porque muchas de esas amenazas pesan también sobre empleados de la empresa. No solo eso, la mitigación de riesgos del contratista **tiene un impacto positivo directo sobre la percepción que esos trabajadores tienen de la organización**.

Riesgos a los que están expuestos los contratistas

La mitigación de riesgos del contratista se enfoca en cuatro grandes grupos de amenazas. En estos cuatro grupos están ubicadas las eventualidades que impactan a los contratistas y su seguridad, pero también los riesgos a los que se puede exponer la organización:

- **Riesgos financieros**: el trabajo del contratista puede no representar el valor invertido por la organización, además, el incumplimiento o retraso del contratista genera sanciones financieras para la organización.

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO

Gestión de reclamaciones en HSE: claves para una respuesta eficaz y segura La **gestión de reclamaciones** es uno de los aspectos más relevantes dentro de los **planes de acción HSE**. Es el proceso que utiliza la organización para atender y solucionar problemas que se relacionan con la seguridad y la salud de los trabajadores o que afectan al medio ambiente. Pero, pese a su importancia, a veces queda en un segundo plano.

La gestión de reclamaciones en el área HSE se diferencia de la **gestión de incidentes** en que se trata de solucionar una eventualidad que ha tenido consecuencias negativas para uno o varios trabajadores o para al entorno en el que opera la organización y que, por ende, **ha generado demandas y exigencias**. Así, lo primero que debe quedar claro es que la gestión de reclamaciones **no se limita a registrar, documentar e investigar el problema**. Requiere una acción inmediata para detener el impacto negativo y tratar de restaurar la integridad de las personas o recursos naturales afectados.

Cuáles son las mejores prácticas atender la gestión de reclamaciones en HSE

La falta de **notificación de incidentes laborales** puede tener efectos devastadores, y lo mismo ocurre si no se atienden de forma adecuada las reclamaciones en HSE. Además de los daños que hayan podido causar, habrá que afrontar **multas, sanciones o litigios**

judiciales. Tal es la importancia de adoptar las mejores prácticas para la gestión de reclamaciones.

1. Priorizar la atención inmediata de lesiones o heridas

Algunas lesiones se pueden tratar de forma inmediata dentro de la misma organización con **equipos de primeros auxilios entrenados y dotados de medios adecuados**. La conformación de estos equipos y el diseño de procedimientos actuación se deben diseñar con antelación, probar y documentar. Para casos en los que sea necesaria asistencia externa, la gestión de reclamaciones **necesita un plan de respuesta inmediato y eficaz.** Además de la disponibilidad de los servicios sanitarios, debe incluir la logística del traslado seguro y la capacitación a los empleados, afectados o no, sobre la forma en que deben proceder.

2. Documentar y registrar los hechos

Es fundamental que existan procedimientos de obligatorio cumplimiento para registrar de forma clara y fehaciente todo aquello que permita **obtener evidencia no contaminada de los hechos**. Es de gran importancia en la **investigación de incidentes y accidentes** y, por tanto, en la gestión de reclamaciones. **Todos los eventos que resulten en lesiones o heridas deben ser reportados**, registrados, documentados e investigados. Estos procesos son competencia de la gestión de reclamaciones porque todos pueden generar en un momento dado una solicitud o una demanda por parte de los afectados. Para que esto se cumpla, **es preciso que los procedimientos sigan las directrices** de una política sobre reporte e investigación de todos los eventos descritos y que esta política se respete en el proceso de gestión de reclamaciones.

Cómo alinear la cultura de seguridad con contratistas y proveedores en 5 pasos

Es probable que la **cultura de seguridad con contratistas** o con proveedores de una organización difiera en profundidad, en intensidad y en calidad de la que registran los empleados de la empresa. Pese a ello, es un elemento fundamental dentro de la **gestión de contratistas**.

La cultura de seguridad se mide por **el conocimiento, la comprensión, la aceptación y el cumplimiento de las normas** y protocolos de seguridad. Si los empleados de la organización tienen hábitos diarios saludables, se preocupan por conocer las actualizaciones sobre seguridad y salud en el trabajo y proponen acciones de mejora, entre otras cuestiones, es posible afirmar que hay cultura de seguridad sólida, sostenible y efectiva. **Construir cultura de seguridad es uno de los desafíos más interesantes** para los equipos de **seguridad y salud en el trabajo**.

Alienar la cultura de seguridad con contratistas con la que se ha cimentado con los empleados es otro reto que requiere acudir a estrategias especialmente diseñadas para ello.

Cómo alinear la cultura de seguridad con contratistas y la de los empleados de la empresa

Alinear la cultura de seguridad con contratistas y con proveedores es una manera de proteger la cultura de SST de la empresa. Es, además, **una forma de afianzar la relación entre empleadores y trabajadores externos** que mejora la percepción que tiene esta fuerza laboral con respecto a la organización como empleadora. Cinco estrategias útiles para alinear la cultura de seguridad con contratistas y proveedores son las siguientes:

1. Implementar debida diligencia en la selección

Desde la etapa de preselección, **la organización necesita conocer los antecedentes del contratista** en diferentes ámbitos: calidad de su servicio, experiencia en el área, formación y capacitación y, por supuesto, seguridad y salud en el trabajo. Dentro de la cultura de seguridad con contratistas y proveedores, **la debida diligencia pretende establecer si el contratista tiene los conocimientos necesarios**.

Su historial de seguridad, que es lo que se pretende conformar con el proceso de debida diligencia, entrega información valiosa: número de incidentes o accidentes en los que fue uno de los actores, reclamaciones por no respetar las normas de seguridad o, por el contrario, participación en equipos de **SST** en otras organizaciones.

ESGinnova Group

GRCTools

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

Tendencias y perspectivas clave en el mercado GRC

El mercado GRC ya no es visto como una función de cumplimiento reactiva, sino como un **habilitador de valor**. Integrar **gobierno corporativo**, **gestión de riesgos** y **cumplimiento normativo** dentro de una misma visión estratégica permite a las organizaciones anticipar amenazas, optimizar procesos y generar confianza en sus stakeholders. Esta visión **holística** del mercado GRC impulsa la **resiliencia empresarial** en un entorno marcado por cambios rápidos y disruptivos.

Las organizaciones líderes están reconociendo que una buena gestión del mercado GRC, además de **prevenir sanciones** y evitar **riesgos reputacionales**, también **crea ventajas competitivas sostenibles**. Empresas con un enfoque maduro en GRC logran anticiparse a escenarios de crisis, optimizan sus inversiones, y consolidan una **cultura organizacional basada en la transparencia** y la mejora continua.

Tendencias clave que están redefiniendo el mercado GRC

1. Digitalización e inteligencia artificial

Las herramientas basadas en **inteligencia artificial (IA)** y **automatización** están revolucionando el modo en que se identifican, evalúan y mitigan los riesgos. Los **modelos predictivos** y el **machine learning** permiten anticipar comportamientos anómalos y responder proactivamente, mejorando la eficiencia operativa y la **toma de decisiones basada en datos**.

A través de **algoritmos avanzados**, las plataformas GRC con IA pueden analizar grandes volúmenes de datos, identificar patrones y sugerir **acciones preventivas** antes de que los riesgos se materialicen. Esto representa una **evolución frente al enfoque reactivo tradicional**.

2. Plataformas GRC integradas

La **fragmentación** de procesos y sistemas ha dado paso a **plataformas GRC centralizadas** que unifican la gestión de riesgos, cumplimiento, auditoría y seguridad. Estas soluciones proporcionan una **visión 360° del entorno de riesgo** y fortalecen la **coherencia en la toma de decisiones** a nivel organizacional.

Las plataformas integradas permiten **romper los silos entre departamentos**, alineando **objetivos estratégicos** con el cumplimiento normativo y la gestión de riesgos operativos. Además, facilitan una **mejor trazabilidad**, **auditorías más eficaces** y **flujos de trabajo más fluidos**.

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO

Cómo los ODS pueden transformar el impacto de tu empresa

Vivimos en una era marcada por **grandes desafíos globales**: el cambio climático avanza aceleradamente, los niveles de desigualdad siguen creciendo, los recursos naturales se agotan a un ritmo insostenible y millones de personas aún carecen de acceso a servicios básicos como salud, educación o agua potable. A esto se suma una creciente presión social sobre las empresas, que ya no pueden operar como si estuvieran ajenas al contexto. En este escenario, la **sostenibilidad** se convierte en una respuesta urgente, y los **Objetivos de Desarrollo Sostenible** (ODS) ofrecen un marco concreto para que las organizaciones actúen con responsabilidad y generen un impacto positivo real.

Estos problemas no son ajenos al mundo corporativo: **afectan cadenas de suministro, mercados, marcos regulatorios y relaciones con los grupos de interés**. Ignorarlos no es una opción. Por el contrario, reconocerlos e integrarlos en la toma de decisiones es una señal de madurez empresarial y una condición para la sostenibilidad a largo plazo.

¿Qué son los ODS y por qué deberían importarle a tu empresa?

Adoptados por la Asamblea General de la ONU en 2015 como parte de la **Agenda 2030**, los ODS comprenden 17 metas globales que abarcan temas críticos como la pobreza, el cambio climático, la igualdad de género, la producción responsable, entre otros. Si bien fueron diseñados inicialmente para gobiernos, hoy se reconoce que el sector privado juega un rol clave en su cumplimiento.

Incorporar los ODS a la estrategia empresarial no solo fortalece la **reputación corporativa**, sino que también impulsa **la innovación, la eficiencia y la competitividad**. Según estudios de PWC y el World Business Council for Sustainable Development (WBCSD), las empresas que alinean sus objetivos con los ODS logran:

- Identificar oportunidades de negocio sostenibles.
- Reducir riesgos ambientales, sociales y reputacionales.
- Mejorar relaciones con inversores, reguladores y consumidores.
- Atraer y retener talento comprometido.

La buena noticia es que existe una guía compartida para abordar estos desafíos de forma estratégica: los **Objetivos de Desarrollo Sostenible (ODS)**. Lejos de ser una declaración de buenas intenciones, los ODS ofrecen un **lenguaje común y una hoja de ruta concreta** para que las empresas puedan generar valor económico mientras contribuyen activamente a un mundo más justo, seguro y habitable.

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO

7 consejos sobre riesgos de terceros

En la era de la Transformación Digital, donde las cadenas de suministro y las colaboraciones empresariales son cada vez más complejas, la gestión de **riesgos de terceros** se ha convertido en un pilar fundamental dentro de los marcos de **Gobierno, Riesgo y Cumplimiento (GRC)**. Las organizaciones ya no operan de manera aislada; su éxito depende en gran medida de proveedores, socios y contratistas externos. Sin embargo, esta interdependencia introduce vulnerabilidades significativas que, si no se gestionan adecuadamente, pueden derivar en **brechas de seguridad, sanciones regulatorias o daños reputacionales irreparables**.

Para las empresas comprometidas con la **excelencia en GRC**, es crucial adoptar estrategias proactivas que mitiguen estos riesgos de terceros sin sacrificar la agilidad operativa. A continuación, presentamos **siete consejos clave** para fortalecer la gestión de terceros, junto con insights sobre cómo una **plataforma tecnológica especializada como GRCTools** puede optimizar este proceso.

1. Realizar una evaluación inicial de riesgos de terceros rigurosa (Due Diligence)

Antes de integrar a un tercero en la cadena de valor, es imprescindible llevar a cabo una **evaluación exhaustiva** que analice su solvencia financiera, historial de cumplimiento normativo y protocolos de seguridad. Un error común es limitar esta evaluación a la fase inicial, cuando en realidad debe ser un proceso continuo.

Cómo GRCTools puede ayudar: La plataforma automatiza la recopilación y análisis de datos críticos, desde certificaciones de seguridad hasta informes financieros, permitiendo una **calificación objetiva de riesgos de terceros** basada en inteligencia de negocio.

2. Establecer contratos con mecanismos de protección claros

Un contrato bien estructurado es la primera línea de defensa contra riesgos de terceros legales y operativos. Debe incluir cláusulas específicas sobre **confidencialidad, responsabilidades en caso de incumplimiento y requisitos de cumplimiento normativo**, adaptables a regulaciones como el **GDPR, SOX o la LGPD**.

Cómo GRCTools puede ayudar: Ofrece plantillas inteligentes que se ajustan automáticamente a las normativas aplicables, reduciendo el margen de error humano y asegurando que todos los acuerdos cumplan con los estándares corporativos.

3. Implementar un monitoreo continuo y proactivo de los riesgos de terceros

El riesgo asociado a un tercero no es estático; puede evolucionar debido a cambios financieros, operativos o regulatorios.

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO

¿Qué es la Ley Karin de Chile?

Chile ha dado un paso decisivo hacia la modernización de su **normativa laboral** con la promulgación de la **Ley Karin**. Esta legislación representa un avance clave en la protección de los derechos de las y los trabajadores, al poner en el centro del debate empresarial un tema históricamente invisibilizado: **el acoso, la violencia y el maltrato en el entorno laboral**. En un escenario donde la transformación digital redefine la gestión de riesgos y cumplimiento, esta ley se presenta como una oportunidad —y un imperativo— para repensar la cultura organizacional desde un enfoque preventivo, ético y tecnológico.

Más que una obligación legal, esta nueva normativa representa un avance en las **prácticas preventivas** para garantizar un entorno laboral saludable, justo y seguro.

¿Qué es la Ley Karin?

La **Ley N.º 21.643**, conocida como Ley Karin, fue promulgada el 15 de enero de 2024 y entró en vigencia el 1 de agosto del mismo año. Su origen está profundamente ligado a un hecho trágico: el fallecimiento de **Karin Salgado**, técnica en enfermería víctima de acoso laboral

en el Hospital Herminda Martín de Chillán. Su caso conmovió a la opinión pública y reveló las carencias estructurales en la prevención y abordaje de este tipo de situaciones en el ámbito laboral.

En respuesta, el Estado chileno articuló una legislación que establece **un marco integral para prevenir, investigar y sancionar** el acoso sexual, el acoso laboral y otros tipos de violencia en el trabajo. La Ley Karin se aplica tanto en el sector público como en el privado, y exige a los empleadores tomar medidas concretas y sostenidas para proteger a sus trabajadores.

¿Qué regula esta ley?

1. Prevención obligatoria

Todas las organizaciones deben contar con protocolos específicos para **prevenir conductas de acoso y violencia laboral**. Esto implica:

- Difundir políticas claras de prevención.
- Capacitar a los trabajadores y líderes.
- Promover ambientes laborales inclusivos y seguros.

2. Investigación con debidos resguardos

La ley establece que, ante cualquier denuncia, se debe iniciar un procedimiento que garantice:

- **Confidencialidad** y protección a las partes involucradas.

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO

¿Qué pautas establece la Ley 21643?

Con la llegada de la **Ley 21643**, también llamada **"Ley Karin"**, se abre un nuevo capítulo para las organizaciones chilenas, donde el acento está puesto en prevenir el acoso, proteger la integridad de las personas y consolidar una cultura laboral basada en el respeto. Esta nueva normativa, que entró en vigor el 1 de agosto de 2024, responde a un reclamo social sostenido por **ambientes laborales más seguros y libres de violencia**, alineándose con los estándares internacionales del **Convenio 190 de la OIT**.

En este artículo, exploraremos en profundidad las **pautas clave de la Ley 21643**, su impacto en el **Gobierno, Riesgo y Cumplimiento (GRC)** empresarial, y cómo las organizaciones pueden apalancar tecnologías como el **software de Riesgos Laborales de GRCTools** para garantizar un cumplimiento efectivo, sistemático y sostenible.

Ley 21643: Una nueva mirada a la prevención del acoso y la violencia laboral

La Ley 21643 redefine profundamente el concepto de ambientes laborales seguros. Entre sus principales disposiciones se destacan:

Reconocimiento del acoso y la violencia laboral

Se elimina el requisito de que las conductas sean reiteradas para que constituyan acoso: una sola acción puede ser suficiente.

Se incorpora la violencia ejercida por terceros (clientes, proveedores, etc.), ampliando el espectro de protección.

Obligatoriedad de protocolos internos

- Todas las organizaciones deben implementar protocolos con enfoque preventivo, incluyendo:

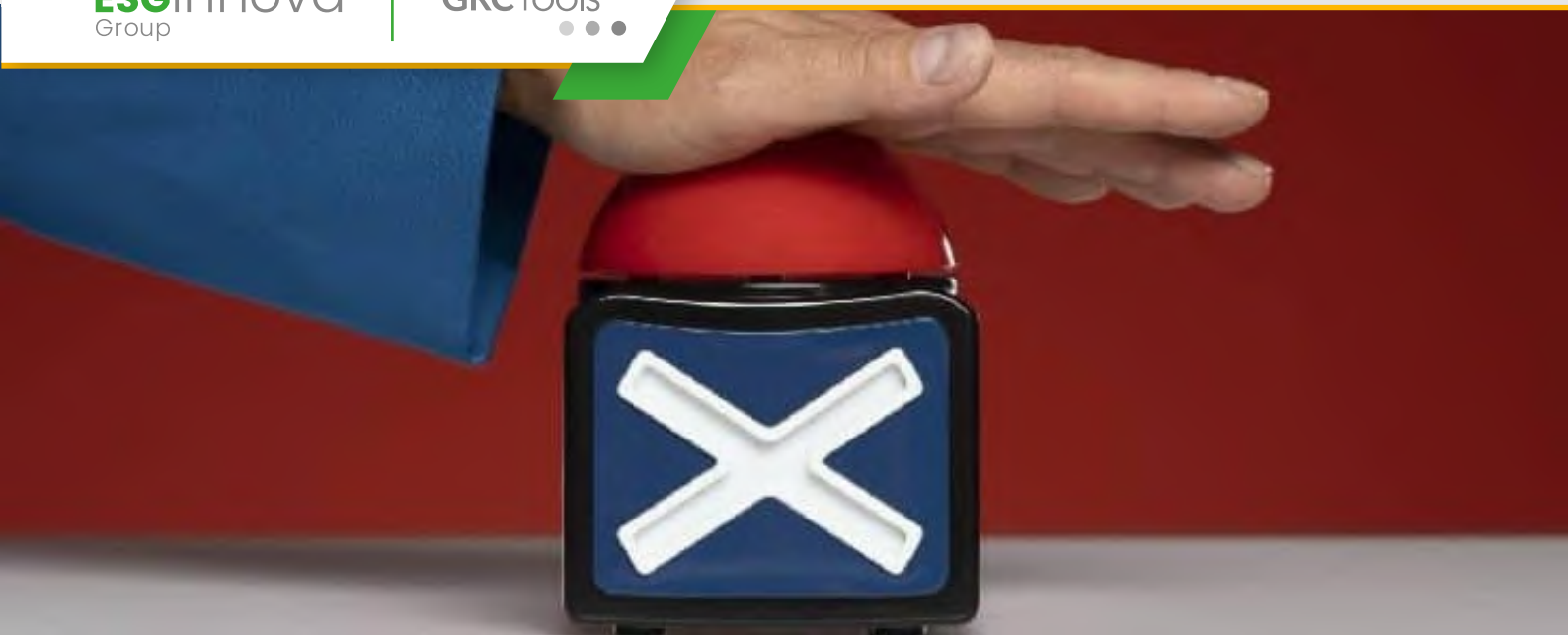
❖ Identificación de peligros y evaluación de **riesgos psicosociales**.

❖ Medidas de prevención concretas, medibles y con enfoque de género.

❖ Capacitación constante al personal.

❖ Garantías de confidencialidad y resguardo a las partes involucradas.

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO



Guía completa para implementar una matriz de peligros

En un entorno empresarial cada vez más dinámico y regulado, la **gestión efectiva de los riesgos operativos y laborales** se ha convertido en un componente esencial para garantizar la sostenibilidad y competitividad de las organizaciones. Entre las herramientas más eficaces para este fin se encuentra la **matriz de peligros**, un instrumento clave dentro de los sistemas de gestión de riesgos y cumplimiento normativo. Esta guía ofrece una visión profunda y práctica sobre cómo implementarla de forma eficiente, especialmente en el marco de la **transformación digital** impulsada por soluciones tecnológicas como **GRCTools**.

¿Qué es una matriz de peligros y por qué es tan importante?

La matriz de peligros es una herramienta sistemática que permite **identificar, analizar y priorizar los riesgos** derivados de los peligros presentes en las actividades de una organización.

Su implementación no solo responde a exigencias normativas (como las establecidas en normas ISO o legislaciones nacionales), sino que es una práctica estratégica que fortalece la **cultura preventiva**, minimiza incidentes y optimiza los procesos internos.

Al clasificar los peligros en función de su **probabilidad de ocurrencia** y su **nivel de severidad**, esta matriz orienta a los responsables de cumplimiento y riesgo a tomar decisiones más informadas y efectivas.

¿Cómo implementar una matriz de peligros en tu organización?

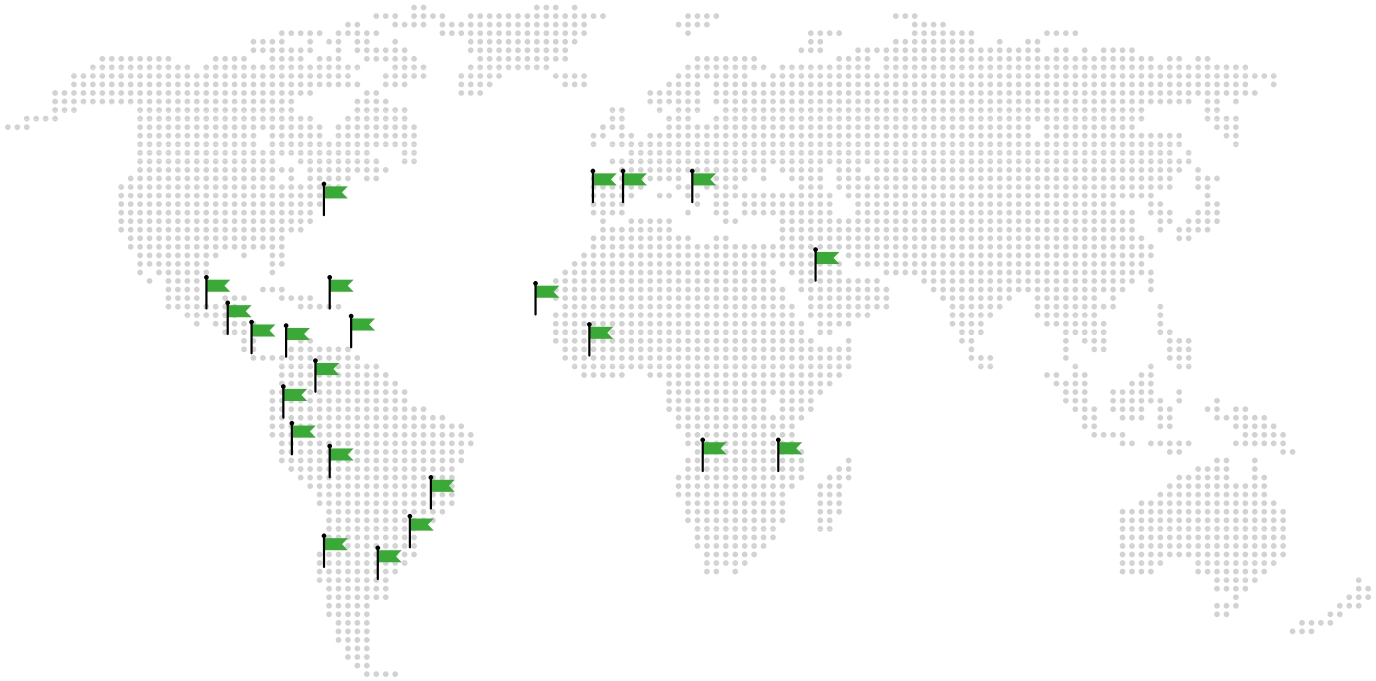
Definir el alcance

Toda **matriz** comienza con una delimitación clara: ¿Qué procesos, áreas o actividades se evaluarán? Este paso es crucial para enfocar los esfuerzos y recursos de forma eficiente.

Identificar los peligros

Mediante observación directa, entrevistas, revisión documental y análisis de datos históricos, se deben identificar los peligros asociados a cada actividad. Estos pueden ser:

- Físicos (ruido, vibraciones)
- Químicos (sustancias peligrosas)
- Biológicos (microorganismos)
- Ergonómicos, psicosociales, eléctricos, entre otros.



El camino hacia la Excelencia

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

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

+2.500 organizaciones

+25 años

+30 países

+240.000 usuarios

ESGinnova
Group

Córdoba, España

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

Écija, España

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

Santiago de Chile, Chile

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

Lima, Perú

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

Bogotá, Colombia

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

México DF, México

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