EMPRESA **EXCELENTE**

Las mejores temáticas sobre Normas ISO, HSE y GRC

MAYO 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.

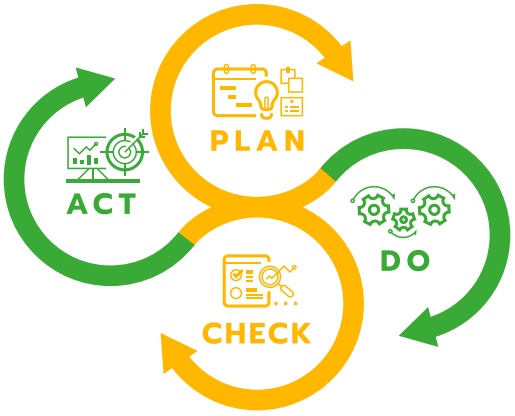
Plataforma ESG Innova

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

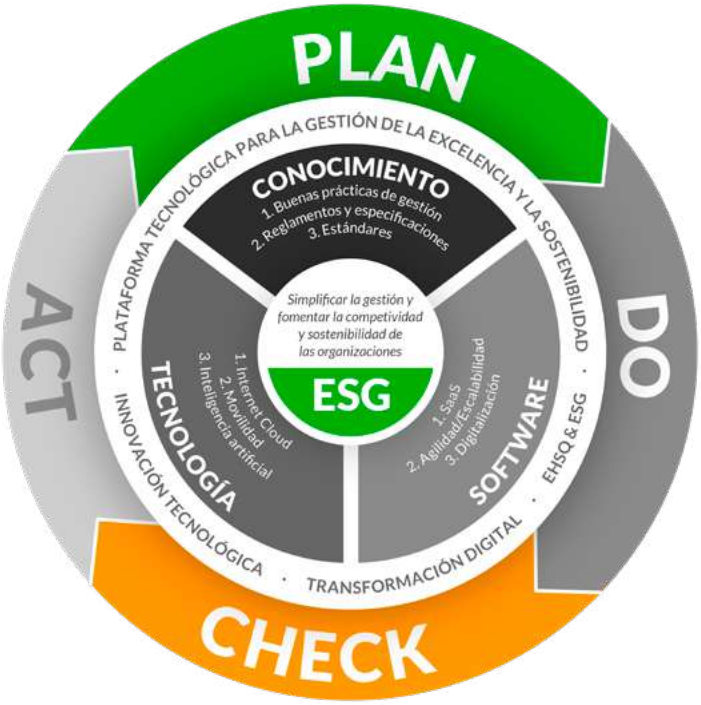
Simplificamos la monitorización y seguimiento, aportando información útil para la toma de decisiones.

❖ 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

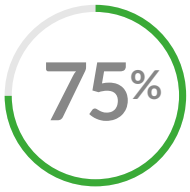
Transformación Digital para la gestión de Gobierno, Riesgo y Cumplimiento.

La Plataforma ESG aporta resultados en el corto plazo

Optimización del tiempo

Menos de tiempo de resolución de una acción correctiva

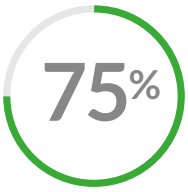
Menos de tiempo de preparación de las reuniones de gestión



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

Las **evaluaciones de riesgos de IA** se recogen en la cláusula 6.1.2 de la **norma ISO 42001**, publicada al final del año 2023. Este estándar es el primero en integrar directrices, controles y requisitos para evaluar y abordar los riesgos de la Inteligencia Artificial de forma eficaz, segura, transparente y ética.

Una norma asociada, ISO 23894, se ocupa de las evaluaciones de riesgos de IA. Quizá por ello, la mencionada cláusula 6.1.2. de ISO 42001 no entrega una guía detallada sobre la forma de desarrollar estas evaluaciones. **Solicita a las organizaciones diseñar e implementar procesos para ejecutar las evaluaciones de riesgos de IA**, pero no indica cómo hacerlo.

Una solución es, por supuesto, implementar ISO 23894. Pero, para aquellas organizaciones que no quieran extender a tal nivel el árbol de gestión con **normas ISO**, **la siguiente guía resultará de gran utilidad**.

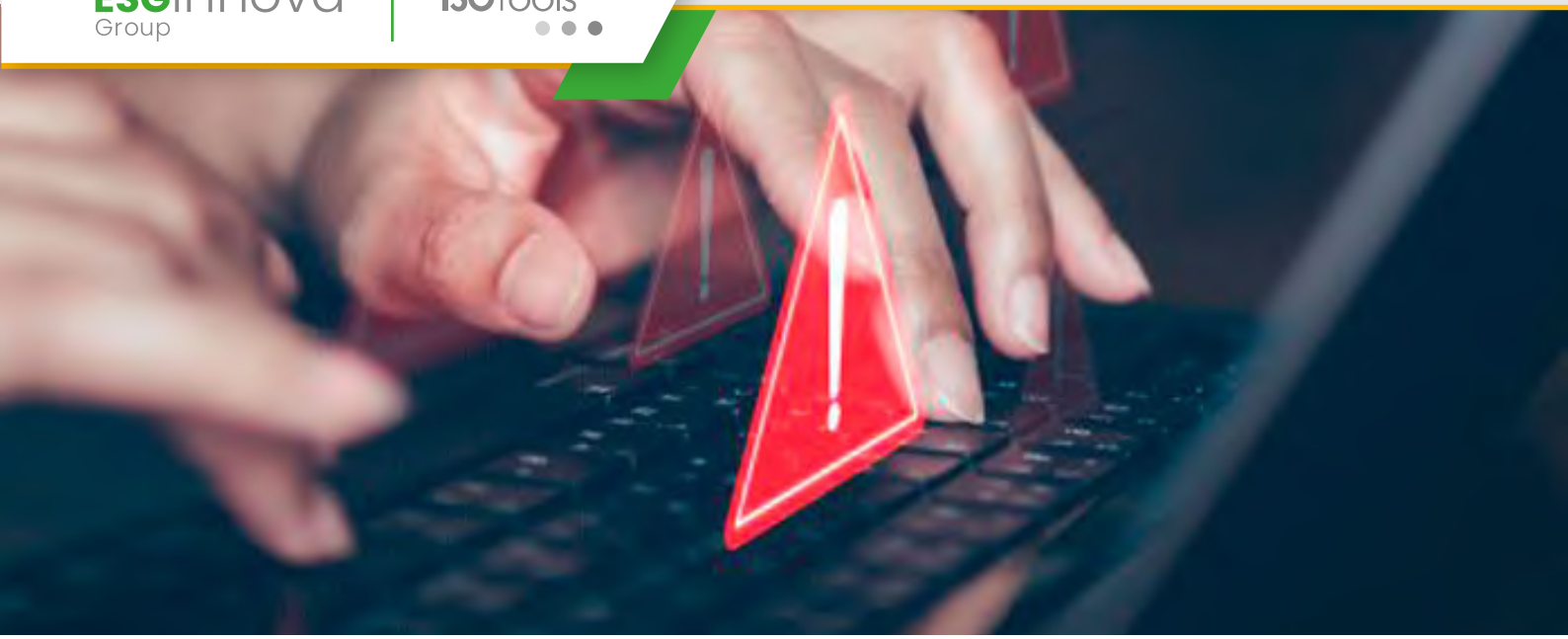
Cómo realizar evaluaciones de riesgos de IA de acuerdo con ISO 42001

No es necesario implementar ISO 23894 para aprovechar su contenido. Una de las consultas que bien vale la pena hacer en esta norma, antes de iniciar las evaluaciones de riesgos de IA, es el capítulo relacionado con las **fuentes de riesgos de IA, entre las que se pueden destacar**:

- Falta de transparencia.
- Incapacidad para rendir cuentas.
- Entornos complejos.
- Privacidad de datos.
- Problemas con el hardware.
- Sesgos en el entrenamiento.
- Problemas que surgen en el ciclo de vida que no está bajo el control de la organización.
- Arquitecturas con brechas de seguridad.
- Errores humanos.
- Vulnerabilidades del software.

ISO 23894, o por lo menos su texto, también ayuda a las organizaciones a identificar los activos de valor para la **gestión de riesgos de IA**.

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO



Informes de eventos de seguridad de la información según ISO 27001:2022

El reporte de **eventos de seguridad de la información** es el tema que aborda el control 6.8 del Anexo A del estándar internacional **ISO 27001:2022**. El control solicita a la empresa establecer mecanismos para que los empleados puedan notificar eventos de seguridad de la información sobre los que tengan evidencia o indicios, de manera inmediata y a través de canales apropiados.

Además, el control 6.8 pide a la organización **capacitar a las personas y documentar los eventos de seguridad de la información** de manera ágil, para garantizar la mitigación o la eliminación inmediata del riesgo.

Qué son eventos de seguridad de la información

Los eventos de seguridad de la información son hechos o situaciones evidenciadas u observadas en un servicio, una red, un sistema o un proceso que **indican o sugieren la existencia de un riesgo o de**

un fallo que puede comprometer la seguridad de la información o la privacidad de los datos de una organización o de sus terceros.

Los eventos de seguridad de la información son señales o alertas que avisan sobre la **presencia de una amenaza potencial**, antes de que el riesgo sea patente y cause un daño tangible.

Algunos **factores desencadenantes** de este tipo de eventos, recurrentes en muchas organizaciones son los siguientes:

- **Virus, malware u otro tipo de software malicioso** con propósitos similares.
- **Personas con acceso no autorizado** a los sistemas informáticos o a una red privada.
- **Contraseñas débiles o predecibles** que facilitan el acceso no autorizado de piratas informáticos o **incidentes de ciberseguridad**.
- **Negligencia en la protección de datos,** de contraseñas o de actualización oportuna de software, generando grietas de seguridad.
- **Ataques externos a la red** o al sistema informático interno de una organización que no utiliza los escudos apropiados.

Incluso las redes más seguras tienen un mínimo nivel de exposición a riesgos de seguridad de la información. En consecuencia, estas empresas también advierten amenazas, aunque lo hagan de forma esporádica. Estos eventos de seguridad de la información también se deben reportar utilizando el canal y el informe respectivo.

Sistema de Gestión de Inteligencia Artificial (SGIA): elementos clave según la norma ISO 42001

ISO 42001 es el estándar que con mayor velocidad ha logrado posicionarse en el panorama corporativo en las últimas décadas. Hay una explicación: cada vez más organizaciones usan la IA en sus procesos productivos o de prestación de servicios, o desarrollan este tipo de productos. De ahí surge la necesidad de implementar un **Sistema de Gestión de Inteligencia Artificial**.

En 2025, solo por tener una idea de la magnitud de la expansión de esta tecnología, el número de empresas que la utilizan triplica a las que lo hacían hace dos años. Las cifras sobre rendimientos financieros producto de la incursión de la IA en empresas de todos los sectores también son fabulosas.

Las oportunidades crecen, pero los riesgos también. ISO 42001 llega para **ayudar a las organizaciones a garantizar prácticas seguras, éticas, transparentes y legales** gracias a la implementación de un Sistema de Gestión de Inteligencia Artificial.

Qué es ISO 42001

ISO 42001 **es el primer estándar de gestión creado para tratar los riesgos asociados al uso o desarrollo de Sistemas de IA** y aprovechar las oportunidades que la tecnología ofrece, en un marco de seguridad, transparencia, legalidad y ética. Es el producto del trabajo durante de dos años de expertos que conformaron el Comité Técnico de ISO, en colaboración con representantes de empresas tecnológicas de todos los continentes.

La norma ISO 42001 **comparte la estructura de Alto Nivel** que caracteriza a las más importantes publicaciones ISO, entre ellas **ISO 9001**, ISO 45001, ISO 14001 o ISO 27001. Esta condición común hace que el estándar diseñado para la implementación de un Sistema de Gestión de Inteligencia Artificial pueda ser integrado a uno o a todos los sistemas mencionados.

Esta norma puede ser implementada por todo tipo de organizaciones, de cualquier tamaño, procedencia, industria o sector que utilicen o desarrollen sistemas de IA. Estas organizaciones demuestran con la certificación de su Sistema de Gestión de Inteligencia Artificial que adoptan las mejores prácticas de **gobernanza de la IA** en sus procesos administrativos, comerciales y productivos.

Como es natural, las organizaciones deben crear políticas, procesos, procedimientos, revisar, inspeccionar, auditar, siempre **sobre un modelo PDCA que garantice la mejora continua** del Sistema de Gestión de Inteligencia Artificial.

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO

¿Por qué usar un software de calidad para cumplir con ISO 9001?

Implementar un **software de calidad para cumplir con ISO 9001** es una necesidad esencial para las organizaciones en las que la gestión de la calidad es un área estratégica. Contribuye a optimizar procesos, automatiza tareas y fortalece la cultura de mejora continua,

El software de calidad para cumplir con ISO 9001 se convierte, además, en una herramienta imprescindible para **asegurar la conformidad con los requisitos de la norma** y transitar con éxito por las complejidades que plantea el estándar.

Cuáles son las características del software de calidad para cumplir con ISO 9001

Un software de calidad para cumplir con ISO 9001 necesita incorporar funcionalidades para **garantizar y agilizar el cumplimiento de los requisitos de la norma** y de los requisitos regulatorios que exige el estándar. Algunas de las más relevantes son las siguientes:

- **Gestión automatizada de documentos**: crea flujos de trabajo para la creación y actualización de la **documentación en ISO 9001**, entrega un repositorio central para la información, asegura el acceso con seguridad, controla versiones y almacena con seguridad las versiones obsoletas.

- **Mapas de calor y presentación de informes gráficos visuales**: permiten identificar puntos críticos o cuellos de botella y establecer en qué puntos pueden aparecer riesgos de cumplimiento.

- **Herramientas y funcionalidades inteligentes para la gestión de riesgos**: herramientas que permitan identificar, evaluar, categorizar y priorizar los riesgos, alineadas con el enfoque basado en el riesgo que caracteriza a la norma.

- **Gestión de auditorías**: desde la programación a la definición de objetivos, la planificación de las actividades sobre el terreno, la generación de informes y las actividades de seguimiento y monitoreo para verificar la eficacia de las acciones correctivas.

Beneficios que aporta el software de calidad para cumplir con ISO 9001

Un sistema de gestión es un tejido de procesos, procedimientos y actividades, diseñados para alcanzar un gran objetivo, algunos objetivos específicos y el cumplimiento de unos requisitos.

En el caso de la **gestión de la calidad**, el cumplimiento es uno de los conceptos más relevantes. Todo lo que se hace busca cumplir con una norma, una regulación, un requisito, un pedido de los clientes, etc. Solo por eso es importante contar con un software de calidad para cumplir con ISO 9001.

Ética de la inteligencia artificial: por qué es imprescindible para las organizaciones

En el entorno corporativo actual, la **ética de la inteligencia artificial** se convierte en factor de consideración en todas las decisiones y las etapas del desarrollo de los sistemas de IA. También ha sido determinante en el desarrollo de marcos normativos y estándares como **ISO 42001**.

Sin duda, la inteligencia artificial es un motor de crecimiento y desarrollo para las empresas. No se trata tan solo de evaluar la disminución de costes o el aumento de la productividad. **Se trata de pensar en innovación y eficiencia, pero también en riesgos**.

En esta última cuestión es donde entra en juego la ética de la inteligencia artificial. Amenazas como las que penden sobre la **privacidad de los datos, el derecho a igualdad de las personas, el empleo o los derechos de autor** justifican tomar decisiones que garanticen

el **uso responsable de las tecnologías de IA**. Un uso seguro, transparente y, sobre todo, ético.

¿Qué rol desempeña la ética de la inteligencia artificial en el mundo corporativo moderno?

Tomar decisiones basándose en un factor tan relevante como la ética de la inteligencia artificial llevará a las organizaciones a **aprovechar los beneficios y las oportunidades que propone la tecnología**. También permitirá **realizar evaluaciones de riesgos de IA** y producir bienes y servicios que contribuyan a lograr un mundo equitativo, inclusivo y sostenible.

La ética de la inteligencia artificial tiene mucho que aportar a la hora de alcanzar ese objetivo. Lo puede hacer de cinco maneras diferentes:

1. Gestionando los riesgos que pueden impactar en la organización

Adoptar prácticas responsables para el desarrollo y uso de soluciones de inteligencia artificial permite a las organizaciones **protegerse de litigios judiciales, multas** o, incluso, sanciones sociales.

Incorporar la ética de la inteligencia artificial genera una **gestión de riesgos de la IA** proactiva en la que **se evalúan las amenazas, a la luz de la ética**, en cada paso que se da para el uso o el desarrollo de sistemas de IA. Antes que protegerse, la empresa busca generar confianza en sus consumidores, su comunidad, sus inversores y sus reguladores.

Software de Gestión de SST: desafíos de los sistemas tradicionales y características de un software ideal

Las empresas que automatizan su gestión de seguridad y salud en el trabajo utilizando un **Software de Gestión de SST** basado en **ISO 45001** reducen el absentismo laboral, evitan multas y sanciones y aumentan la productividad. Pero todos esos beneficios se ven superados por el más importante: protegen la vida de sus trabajadores, ayudando a evitar y lesiones, accidentes o enfermedades.

Frente a los sistemas tradicionales, la gestión automatizada mediante un Software de Gestión de SST representa un avance fundamental. **Los métodos convencionales, aún vigentes en muchas organizaciones, presentan serias limitaciones** que comprometen la seguridad e integridad de los trabajadores y la estabilidad financiera de la empresa.

Problemas recurrentes en los sistemas tradicionales de gestión de seguridad y salud en el trabajo

Hasta la última década del siglo XX la seguridad de los trabajadores se gestionaba utilizando documentos en papel. **Reportes de incidentes, instrucciones de seguridad y todo lo relacionado con la gestión se procesaba en documentos impresos** y, en algunas ocasiones, a mano.

En los años 90, el uso de ordenadores introdujo una novedad que en su momento resultó interesante: la hoja de cálculo. Esto, que parece un avance notable, en la práctica resultó en **una sofisticación de la gestión manual, en la que prevalecieron los mismos problemas**:

1. Errores humanos y omisiones

Incluso con el apoyo de las hojas de cálculo, el error humano está presente en la gestión SST tradicional. Cifras invertidas, datos alojados en la columna equivocada, omisión de hechos relevantes, etc. generan **informes inexactos, conclusiones equivocadas y, por supuesto, toma de decisiones erróneas**. Todo ello sin mencionar que la información, deficiente o no, se obtenía después de varias semanas de ocurrido algún hecho fundamental.

2. Dificultad para integrar esfuerzos

Una de las grandes dificultades de la gestión manual está en la **incapacidad de obtener una visión integral del estado del sistema**. Los profesionales, en cada área, obtienen una visión parcial sobre lo que sucede en materia de seguridad porque solo tienen acceso a los documentos que se generan en su departamento.

¿Cuáles son los posibles riesgos de seguridad de la IA y cómo ayuda la norma ISO 42001?

Los **riesgos de seguridad de la IA** preocupan a las empresas que han basado sus proyectos estratégicos de crecimiento y expansión en la nueva tecnología. Hay sólidas razones para que eso sea así: esos riesgos tienen implicaciones regulatorias, éticas, de cumplimiento e, incluso, reputacionales. La norma **ISO 42001** nació como respuesta a esa realidad.

La inteligencia artificial ha tomado posiciones en todos los ámbitos industriales, comerciales o de servicios, utilizando como punta de lanza las indiscutibles oportunidades que ofrece. Sin embargo, de la mano de las oportunidades llegan los riesgos de seguridad de la IA. Estos derivan de un mal uso o gestión de la nueva tecnología y las organizaciones necesitan protegerse frente a ellos.

¿Cuáles son los riesgos de seguridad de la IA que es posible gestionar con la norma ISO 42001?

ISO 42001 es el primer **estándar para sistemas de gestión de inteligencia artificial** de alcance internacional. Está **diseñado específicamente para eliminar o mitigar los riesgos asociados al uso de la IA**: éticos, sociales, de privacidad de datos o, incluso, aquellos que vulneran los derechos a la igualdad de las personas. El que se aborda a continuación, sin restar importancia a otros tipos de amenazas, es el enfoque relacionado con los riesgos de seguridad de la IA.

1. Exposición de datos privados

La exposición de datos privados, **su manipulación o alteración y su uso con fines de entrenamiento** conforman el riesgo más natural y predecible asociado al desarrollo y empleo de la inteligencia artificial. Las causas de estos riesgos de seguridad de la IA suelen asociarse a la **ausencia de buenas prácticas** y de protocolos estrictos sobre la forma en que se recopilará y tratará la información. Tampoco suelen existir en estos casos procedimientos claros sobre el almacenamiento o no de los datos o sobre los controles que se utilizarán para evitar el acceso indebido.

¿Cómo ayuda ISO 42001?

La **gestión sistemática y estandarizada** es la herramienta que utiliza ISO 42001 para abordar el problema. La norma solicita a la organización que identifique, evalúe, priorice y gestione los riesgos, entre ellos los riesgos de seguridad de la IA relacionados con la privacidad de los datos.

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO

ESGinnova
Group

HSE Tools

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

Burnout en el trabajo: un reto para la seguridad y el bienestar laboral

Burnout en el trabajo es la expresión derivada del idioma inglés que se usa en el área de seguridad y salud en el trabajo para referirse al agotamiento laboral. Es una realidad que los profesionales especializados en la **gestión de personas** deben afrontar con diligencia, puesto que se trata de amenaza silenciosa, pero que amenaza al bienestar de los empleados.

Burnout en el trabajo se ubicaría cerca de otros **riesgos psicosociales** como el estrés o el acoso laboral. Sin embargo, las causas, las consecuencias y las características son diferentes. Por tanto, **las acciones para tratarlo deben ser específicas**.

Qué es el burnout en el trabajo y cómo se manifiesta

El burnout en el trabajo es agotamiento laboral. Esto implica que **el trabajador está cansado, fatigado, a nivel físico y mental**.

Es sensato pensar que la principal causa para que aparezca es la carga excesiva de trabajo. Y, en efecto, así es. Muchos de los trabajadores que experimentan un agotamiento laboral crónico lo hacen porque han sido **sometidos a cargas de trabajo superiores a sus capacidades**. Pero no es esa la única causa raíz del problema. En algunos ámbitos es usual que se confunda el burnout con el **estrés en el lugar de trabajo**. Este es un buen punto para hacer dos precisiones: se trata de dos riesgos y de dos síndromes diferentes, sin embargo, **es posible que el estrés sea una de las causas del burnout.** Los primeros síntomas del burnout en el trabajo son cansancio, agotamiento y la apatía evidente en el trabajador. Se trata de síntomas que aparecen día tras día y que evidencian una clara tendencia hacia el agravamiento. **Manifestaciones específicas son las siguientes**:

1. Agotamiento emocional

El agotamiento emocional, que puede hacerse evidente como **fatiga laboral** sin que represente exactamente lo mismo, se expresa como una sensación de desgaste que **hace que el trabajador esté irritable.** La consecuencia es que no manifiesta entusiasmo por cualquier actividad o por cualquier proyecto que se le proponga, tanto en el ámbito laboral como en el social o familiar. El agotamiento emocional **suele estar acompañado de problemas para concentrarse**, dificultad para conciliar el sueño o necesidad de aislarse y apartarse de todo y de todos.

2. Pérdida de iniciativa y entusiasmo

Trabajadores que se han caracterizado por su iniciativa, por sus propuestas innovadoras y entusiasmo para conformar grupos que acometen proyectos nuevos y luego **manifiestan una clara apatía** hacia ese tipo de comportamientos pueden estar sufriendo burnout en el trabajo.

Seguridad de contratistas: claves para una gestión eficaz con tecnología

La **seguridad de contratistas** es un área de la gestión HSE que merece especial atención y asignación de recursos propios, entre los que destacan los tecnológicos. Hay que tener en cuenta, en este aspecto, que la fuerza laboral externa suele seguir procedimientos y estándares de seguridad diferentes, de ahí la necesidad de una **gestión de contratistas** eficiente en todos los aspectos.

La fuerza laboral externa es diversa, pluricultural y dispersa. Por esas mismas razones los protocolos de seguridad de contratistas y los estándares de cumplimiento son disímiles y no siempre ajustados a las mejores prácticas. La seguridad de contratistas, no gestionada de forma adecuada, **podría afectar a los resultados del programa de seguridad para los empleados de la empresa**, generando riesgos adicionales y **brechas de cumplimiento** que pueden deteriorar el buen trabajo hecho hasta el momento por los equipos de seguridad y salud en el trabajo.

Cuáles son los desafíos que conlleva la seguridad de contratistas

Garantizar la seguridad de contratistas es una tarea que implica superar retos específicos. Se trata de desafíos que es preciso afrontar para poder **aprovechar las grandes oportunidades que la fuerza laboral externa representa** para un número creciente de empresas. El primer paso para hacer frente a los retos es conocerlos para después entender cómo **la tecnología puede convertirse en el mejor aliado** de cualquier organización en el propósito de garantizar la seguridad de contratistas. Entre esos desafíos cabe destacar los siguientes:

1. Diversidad de culturas de seguridad

Los protocolos de seguridad de contratistas son dispares. Pasan por muchos procesos de capacitación y por enfoques diferentes sobre la seguridad, algunos muy estrictos, otros más laxos. **Las diferencias generan grietas de seguridad** que pueden terminar afectando a los empleados directos de la empresa.

2. Desconocimiento del sitio y las condiciones de trabajo

Para muchos contratistas, el lugar en el que desarrollarán sus tareas es desconocido. En la misma medida, los riesgos son extraños, pero no por ello inexistentes. Si algo se debe reconocer en los contratistas, como fuerza de trabajo de excepcional capacidad, es la confianza en sí mismos y en sus capacidades. **El exceso de confianza, sumado al trabajo en un área desconocida**, **crea un escenario proclive a accidentes**, lesiones o incluso, consecuencias aún más graves.

Centralizar la documentación de seguridad laboral: cómo ahorrar tiempo y mejorar la seguridad en el trabajo

La gestión de la **documentación de seguridad** es una tarea que demanda un buen número de horas semanales para los equipos de HSE. Esa carga adicional de trabajo puede desviar la atención de otras cuestiones también importantes, de ahí la necesidad de apoyarse en una solución tecnológica que se centralice y facilite la **gestión de documentos y registros**.

Ocuparse de la documentación de seguridad es necesario, sin embargo, **almacenar, organizar y recuperar información requiere de innumerables recursos**. Si existe una manera de ahorrar tiempo y liberar espacio para investigar incidentes de seguridad o generar estrategias para mejorar los resultados de la gestión, es evidente que ese es el camino que hay que seguir. **La transformación digital ha permitido disponer de herramientas eficaces** para centralizar la documentación de seguridad y reducir

de forma ostensible el tiempo que consumen los equipos de HSE en gestión de documentos. Se liberan así horas y recursos para trabajar en estrategias para garantizar el cumplimiento y la eficiencia.

¿Por qué la gestión de documentación de seguridad laboral demanda tanto tiempo?

Un programa de seguridad laboral o un **Sistema de Gestión de Seguridad y Salud en el Trabajo** tienen una alta dependencia de la documentación de seguridad laboral por muchas razones. Esta se requiere para **alcanzar la conformidad con exigencias de un estándar como ISO 45001**, que establece requisitos para unos sistemas SST eficaces. Además de ello, también hay documentos que es preciso gestionar para **cumplir con exigencias regulatorias** o porque los procesos del área, o de otras relacionadas como Recursos Humanos o Contabilidad, así lo exigen.

El problema es que **todavía existen empresas que dependen de la documentación en papel** o que consideran que el uso de cuentas de correo electrónico y hojas de cálculo son suficientes para el tratamiento de la documentación de seguridad.

Esos sistemas tradicionales son proclives al extravío de documentos, al error humano, el retraso en las actividades o el trabajo con documentos desactualizados. Todo ello, sin olvidar la dificultad para acceder a la información correcta en el momento oportuno y, por supuesto, la degradación de las condiciones de seguridad de los trabajadores que puede suponer.

Plataforma HSE centralizada: la clave para gestionar operaciones en múltiples localizaciones

Una **plataforma HSE centralizada** es el elemento clave que hace posible a las empresas afrontar con éxito el desafío que representa atender la **Gestión HSE**. Esta se asocia a muchas obligaciones de cumplimiento, que se multiplican de acuerdo con el número de ubicaciones en las que opera una organización.

El incumplimiento en el área HSE tiene costes financieros y reputacionales importantes. Por supuesto, estandarizar los protocolos, los requisitos y las prácticas es la mejor forma de enfrentar el problema. Pero esto no será posible sin una plataforma HSE centralizada.

Por qué las empresas necesitan una plataforma HSE centralizada

Las empresas modernas se alejan del círculo local para ser globales. La operación en múltiples sitios **promueve la asociación con contratistas agregando un nuevo desafío para la Gestión HSE**, que necesita una herramienta efectiva para afrontar con éxito problemas como los siguientes:

1. Diversidad de marcos regulatorios

Las leyes y **regulaciones ambientales** o de seguridad y salud en el trabajo **aparecen en el ámbito local, regional, nacional o internacional**. Incluso empresas con ubicaciones en la misma ciudad pueden estar sometidas a regulaciones diferentes, de acuerdo con la zona en la que estén ubicadas sus instalaciones. El problema se magnifica con el crecimiento de la organización.

2. Diferentes formas de interpretar las normas

Cada ubicación crea un grupo humano diferente, con costumbres, comportamientos y niveles de conocimiento y concienciación diferentes en cuanto a las normas de seguridad o protocolos ambientales. **La ausencia de uniformidad genera riesgos de seguridad y de cumplimiento**.

3. Formación de silos de información

Las ubicaciones, filiales o sucursales de una organización muestran una tendencia natural para convertirse en islas. **Cada ubicación desarrolla procesos, procedimientos y, sobre todo, formas diferentes de recopilar datos y generar informes**.

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO

Semana de la Seguridad en la Construcción 2025

Del **5 al 9 de mayo de 2025**, el sector de la construcción se moviliza para celebrar la **Semana de la Seguridad en la Construcción**, una campaña anual que busca reforzar el compromiso con la **prevención de riesgos laborales**, el cuidado de la salud y la vida de los trabajadores. Esta iniciativa, impulsada desde 2014, se ha convertido en un **movimiento internacional**, con la participación de cientos de empresas y millones de personas involucradas.

La edición de este año se presenta bajo el lema **"All in Together: Plan. Own. Commit."** (Todos unidos: Planifica. Hazte responsable. Comprométete). Un mensaje claro que llama a la **acción colaborativa**, donde cada persona del equipo, desde la gerencia hasta el operario en obra, asume un rol activo en la **construcción de entornos laborales seguros, humanos y sostenibles**.

Este evento es impulsado por organizaciones como **Associated Builders and Contractors (ABC)** y **Associated General Contractors of America (AGC)**, y en 2025 contará con la participación de más de 900 empresas y el respaldo de casi 120 patrocinadores y aliados estratégicos.

Un enfoque renovado en cultura preventiva en la Semana de la Seguridad en la Construcción

La **seguridad en la construcción** no se limita a protocolos o normativas. Hoy se entiende como parte esencial de una **cultura organizacional consciente**, centrada en el bienestar físico, mental y emocional del trabajador. En este contexto, la Semana de la Seguridad se convierte en una oportunidad valiosa para **revisar prácticas**, **reconocer logros** y **fortalecer el liderazgo preventivo**.

Este año, la campaña destaca tres conceptos clave:

- **Planifica (Plan):** La seguridad comienza con una buena planificación. Identificar riesgos, asignar recursos, diseñar procedimientos y comunicar correctamente las tareas es esencial para prevenir accidentes.

- **Hazte responsable (Own):** La responsabilidad individual es el motor de la prevención. Cada persona debe asumir el deber de cuidarse y cuidar a los demás, más allá de lo que dicten las normas.

- **Comprométete (Commit):** El compromiso constante, visible y coherente con la seguridad es lo que consolida una cultura sólida. No basta con campañas puntuales; se requiere constancia, coherencia y liderazgo.

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO

Seguridad de contratistas: claves para una gestión eficaz con tecnología

La **seguridad de contratistas** es un área de la gestión HSE que merece especial atención y asignación de recursos propios, entre los que destacan los tecnológicos. Hay que tener en cuenta, en este aspecto, que la fuerza laboral externa suele seguir procedimientos y estándares de seguridad diferentes, de ahí la necesidad de una **gestión de contratistas** eficiente en todos los aspectos. [widget id=»custom_html-22″] **La fuerza laboral externa es diversa, pluricultural y dispersa**. Por esas mismas razones los protocolos de seguridad de contratistas y los estándares de cumplimiento son disímiles y no siempre ajustados a las mejores prácticas. La seguridad de contratistas, no gestionada de forma adecuada, **podría afectar a los resultados del programa de seguridad para los empleados de la empresa**, generando riesgos adicionales y **brechas de cumplimiento** que pueden deteriorar el buen trabajo hecho hasta el momento por los equipos de seguridad y salud en el trabajo.

Cuáles son los desafíos que conlleva la seguridad de contratistas

Garantizar la seguridad de contratistas es una tarea que implica superar retos específicos. Se trata de desafíos que es preciso afrontar para poder **aprovechar las grandes oportunidades que la fuerza laboral externa representa** para un número creciente de empresas. El primer paso para hacer frente a los retos es conocerlos para después entender cómo **la tecnología puede convertirse en el mejor aliado** de cualquier organización en el propósito de garantizar la seguridad de contratistas. Entre esos desafíos cabe destacar los siguientes:

1. Diversidad de culturas de seguridad

Los protocolos de seguridad de contratistas son dispares. Pasan por muchos procesos de capacitación y por enfoques diferentes sobre la seguridad, algunos muy estrictos, otros más laxos. **Las diferencias generan grietas de seguridad** que pueden terminar afectando a los empleados directos de la empresa.

2. Desconocimiento del sitio y las condiciones de trabajo

Para muchos contratistas, el lugar en el que desarrollarán sus tareas es desconocido. En la misma medida, los riesgos son extraños, pero no por ello inexistentes. Si algo se debe reconocer en los contratistas, como fuerza de trabajo de excepcional capacidad, es la confianza en sí mismos y en sus capacidades. **El exceso de confianza, sumado al trabajo en un área desconocida**, **crea un escenario proclive a accidentes**, lesiones o incluso, consecuencias aún más graves.

Centralizar la documentación de seguridad laboral: cómo ahorrar tiempo y mejorar la seguridad en el trabajo

La gestión de la **documentación de seguridad** es una tarea que demanda un buen número de horas semanales para los equipos de HSE. Esa carga adicional de trabajo puede desviar la atención de otras cuestiones también importantes, de ahí la necesidad de apoyarse en una solución tecnológica que se centralice y facilite la **gestión de documentos y registros**. [widget id=»custom_html-23″] Ocuparse de la documentación de seguridad es necesario, sin embargo, **almacenar, organizar y recuperar información requiere de innumerables recursos**. Si existe una manera de ahorrar tiempo y liberar espacio para investigar incidentes de seguridad o generar estrategias para mejorar los resultados de la gestión, es evidente que ese es el camino que hay que seguir. **La transformación digital ha permitido disponer de herramientas eficaces** para centralizar la documentación de seguridad y reducir de forma ostensible el tiempo que consumen los equipos de HSE en

gestión de documentos. Se liberan así horas y recursos para trabajar en estrategias para garantizar el cumplimiento y la eficiencia.

¿Por qué la gestión de documentación de seguridad laboral demanda tanto tiempo?

Un programa de seguridad laboral o un **Sistema de Gestión de Seguridad y Salud en el Trabajo** tienen una alta dependencia de la documentación de seguridad laboral por muchas razones. Esta se requiere para **alcanzar la conformidad con exigencias de un estándar como ISO 45001**, que establece requisitos para unos sistemas SST eficaces. Además de ello, también hay documentos que es preciso gestionar para **cumplir con exigencias regulatorias** o porque los procesos del área, o de otras relacionadas como Recursos Humanos o Contabilidad, así lo exigen. El problema es que **todavía existen empresas que dependen de la documentación en papel** o que consideran que el uso de cuentas de correo electrónico y hojas de cálculo son suficientes para el tratamiento de la documentación de seguridad. **Esos sistemas tradicionales son proclives al extravío de documentos**, al error humano, el retraso en las actividades o el trabajo con documentos desactualizados. Todo ello, sin olvidar la dificultad para acceder a la información correcta en el momento oportuno y, por supuesto, la degradación de las condiciones de seguridad de los trabajadores que puede suponer.

Cómo puede la centralización de la documentación de seguridad solucionar los problemas

Automatizar y digitalizar la gestión de la documentación de seguridad, utilizando un **software HSE** especializado en esta y en otras funcionalidades.

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO

Plataforma HSE centralizada: la clave para gestionar operaciones en múltiples localizaciones

Una **plataforma HSE centralizada** es el elemento clave que hace posible a las empresas afrontar con éxito el desafío que representa atender la **Gestión HSE**. Esta se asocia a muchas obligaciones de cumplimiento, que se multiplican de acuerdo con el número de ubicaciones en las que opera una organización. [widget id=»custom_html-23″] **El incumplimiento en el área HSE tiene costes financieros y reputacionales importantes**. Por supuesto, estandarizar los protocolos, los requisitos y las prácticas es la mejor forma de enfrentar el problema. Pero esto no será posible sin una plataforma HSE centralizada.

Por qué las empresas necesitan una plataforma HSE centralizada

Las empresas modernas se alejan del círculo local para ser globales. La operación en múltiples sitios **promueve la asociación con contratistas agregando un nuevo desafío para la Gestión HSE**, que necesita una herramienta efectiva para afrontar con éxito problemas como los siguientes:

1. Diversidad de marcos regulatorios

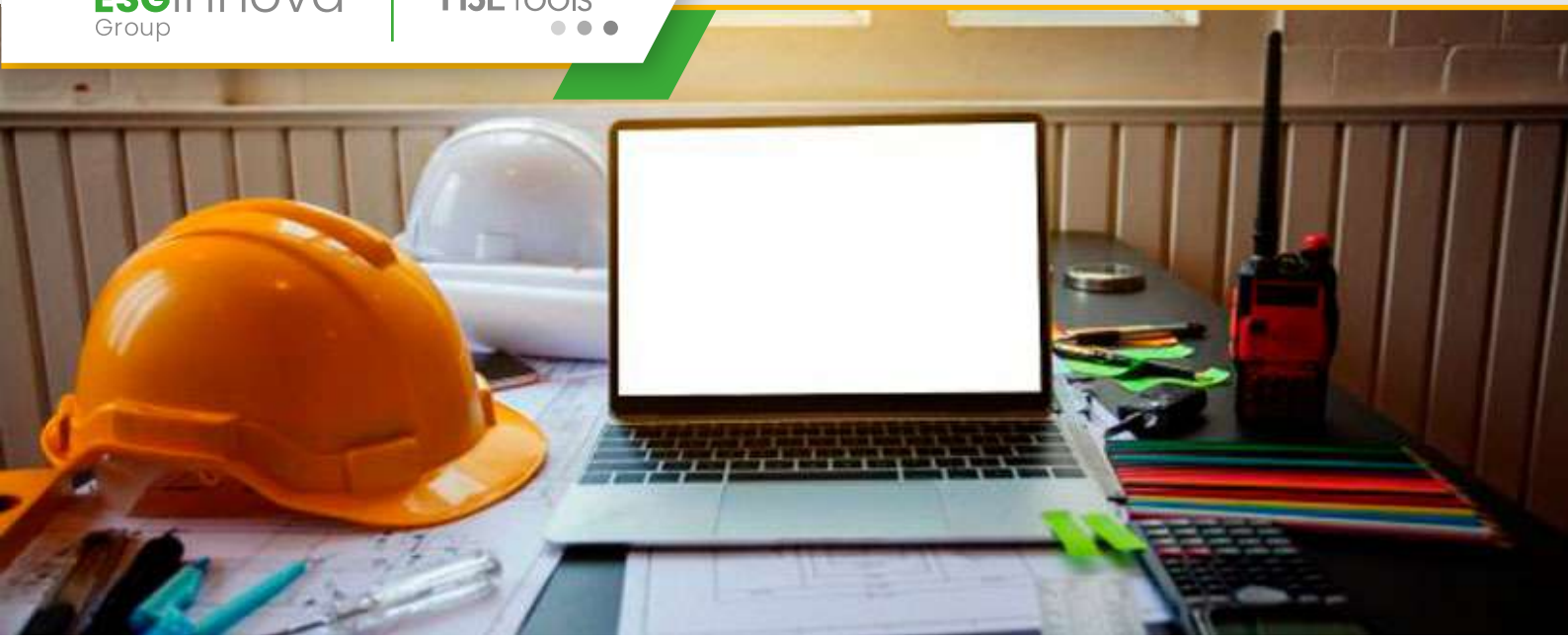
Las leyes y **regulaciones ambientales** o de seguridad y salud en el trabajo **aparecen en el ámbito local, regional, nacional o internacional**. Incluso empresas con ubicaciones en la misma ciudad pueden estar sometidas a regulaciones diferentes, de acuerdo con la zona en la que estén ubicadas sus instalaciones. El problema se magnifica con el crecimiento de la organización.

2. Diferentes formas de interpretar las normas

Cada ubicación crea un grupo humano diferente, con costumbres, comportamientos y niveles de conocimiento y concienciación diferentes en cuanto a las normas de seguridad o protocolos ambientales. **La ausencia de uniformidad genera riesgos de seguridad y de cumplimiento**.

3. Formación de silos de información

Las ubicaciones, filiales o sucursales de una organización muestran una tendencia natural para convertirse en islas. **Cada ubicación desarrolla procesos, procedimientos y, sobre todo, formas diferentes de recopilar datos y generar informes**.



Costes en la gestión de contratistas: consecuencias de una mala gestión (y cómo evitarlo)

La evaluación de **costes en la gestión de contratistas** suele reducirse a la tarifa que cobra esta fuerza laboral externa, imprescindible para muchas organizaciones. Sin embargo, el valor que se pagará a los **contratistas** por su trabajo es apenas uno de los diferentes componentes que conforman esta variable. [widget id=»custom_html-22″] Los costes en la gestión de contratistas **equivalen a la suma de varios elementos**. Sobre todo, necesitan considerar la probabilidad de pagar por la ineficiencia de la gestión, por la negligencia o por la omisión de tareas obvias. En la ejecución de un contrato en el que se utiliza fuerza laboral externa se presentan **situaciones que pueden sacar a la luz costes en la gestión de contratistas ocultos**, que no por tener ese carácter furtivo se pueden considerar menores o inocuos. Así, dentro de los costes en la gestión de contratistas, cuando esta es ineficiente, existen algunos que tienen la capacidad para **absorber la rentabilidad del proyecto, ocasionar daño**

reputacional a la empresa y causar problemas regulatorios que pueden culminar en la pérdida de licencias o la imposición de sanciones.

Costes en la gestión de contratistas que pueden permanecer ocultos

Los costes en la gestión de contratistas derivados de la ineficacia de esta y que pueden acabar con las expectativas planteadas en cualquier presupuesto **se pueden clasificar en cinco categorías**:

1. Costes de seguridad y salud en el trabajo

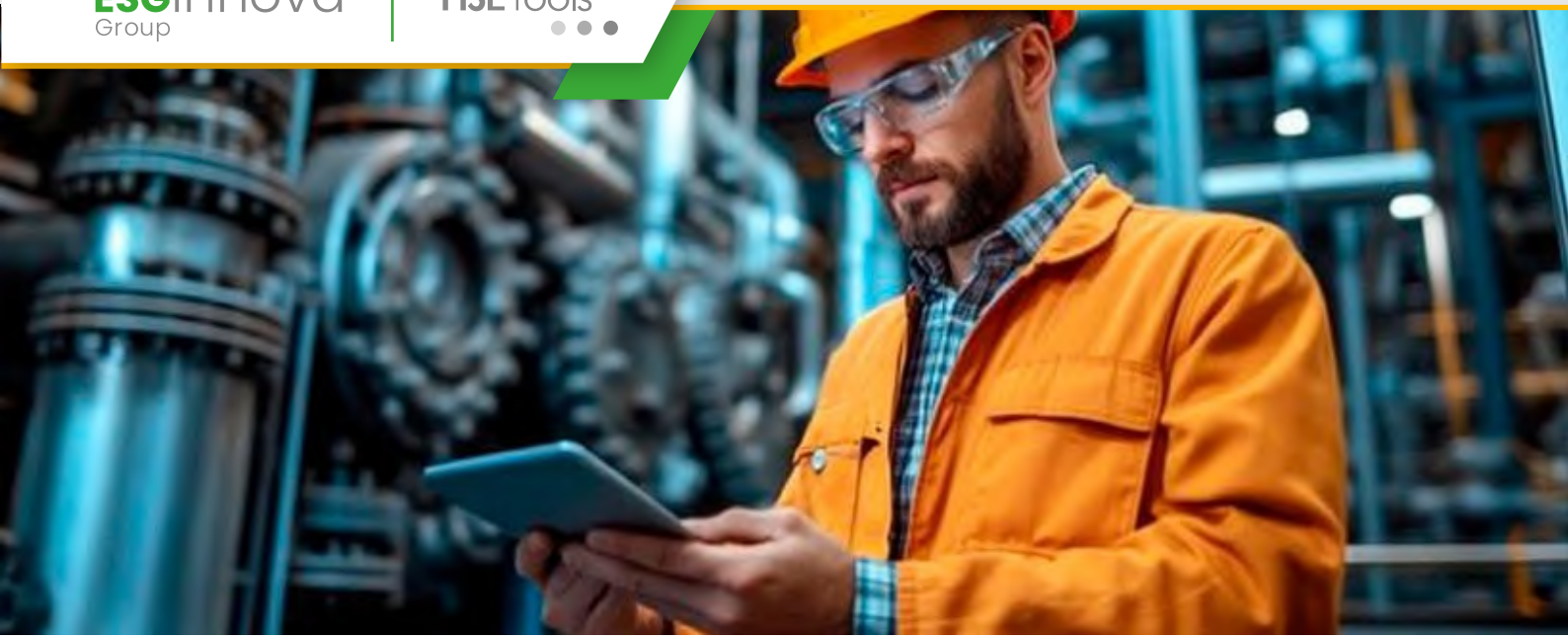
Se trata de los eventos que pueden incrementar costes en la gestión de contratistas asociados al contrato como consecuencia de **errores comunes** atribuibles a terceros o a la organización. Algunos ejemplos en esta categoría son los siguientes:

- **Incremento en el coste de las primas de seguro**, ocasionado por los antecedentes del contratista en otras empresas o la falta de certificaciones para realizar trabajos que implican riesgo, como trabajos en alturas o en espacios confinados.

- **Pago de indemnizaciones, reclamaciones de trabajadores o costes judiciales**, originados por accidentes, lesiones, heridas o enfermedades asociadas con el trabajo, derivadas de **brechas de cumplimiento** en seguridad.

- **Penalizaciones para la empresa** a causa del incumplimiento en los tiempos de ejecución, ocasionados por la falta de productividad del contratista, por lesiones o por negligencia en el desarrollo del contrato.

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO



Beneficios del Software de Gestión de Seguridad y Salud Laboral para el cumplimiento normativo

La seguridad en el trabajo es clave para el éxito operativo de cualquier empresa, pero garantizar el cumplimiento normativo puede ser un desafío. Un **Software de Gestión de Seguridad y Salud Laboral** optimiza procesos, reduce errores y mejora la protección en el entorno laboral. Además, una eficaz **gestión de documentos** centraliza información y facilita el acceso a registros clave, desafíos a veces insalvables para sistemas basados en papel o en hojas de cálculo. [widget id=»custom_html-22″] La importancia de la seguridad y la salud de los trabajadores no admite discusión. Además de las acciones obvias para mantener protegidos a sus trabajadores, **las organizaciones necesitan preocuparse por cumplir con las leyes**, con las regulaciones y con todo aquello que se conoce con el nombre de marco normativo y regulatorio. **Cumplir con las normas es una manera de mejorar la seguridad de los trabajadores**. El Software de Gestión de Seguridad y Salud Laboral

mejora las posibilidades que tiene la empresa para garantizar el **cumplimiento normativo**.

Importancia del cumplimiento para la seguridad y la salud de los trabajadores

El cumplimiento de las normas es una obligación legal y es también una solicitud en el estándar internacional **ISO 45001**. No cumplir con la ley, con las directivas en el caso europeo, con las normas o con los acuerdos en el área de seguridad en el trabajo genera consecuencias lesivas para los trabajadores, en primera instancia, y después para la organización. Es una de las razones por las que las empresas deben pensar en contratar un Software de Gestión de Seguridad y Salud Laboral. **Las secuelas del incumplimiento pueden ser muy lesivas** y afectar a las empresas de diferentes formas:

- **Afectación financiera**: las empresas pueden enfrentarse al pago de cantidades importantes de dinero en multas y sanciones.
- **Pérdida de contratos o licitaciones**: cuando las obligaciones de cumplimiento son contractuales, es probable que el incumplimiento lleve al contratista o al cliente a rescindir el contrato.
- **Deterioro de la reputación**: las organizaciones que incumplen pierden la confianza de sus empleados, de los consumidores y de los organismos reguladores.
- **Interrupción de la operación**: el incumplimiento puede interrumpir la operación por exigencia de un regulador, por iniciativa de los empleados o por decisión de la Alta Dirección.

Precalificación o clasificación de contratistas: áreas en las que realizar preguntas clave

La etapa de precalificación o **clasificación de contratistas** impacta directamente en todo el ciclo de vida del contrato. De lo que se haga bien o mal en este momento dependerán las condiciones de seguridad, el desarrollo técnico del proyecto, el cumplimiento normativo e incluso el bienestar financiero de la operación. De ahí su importancia dentro de la **gestión de contratistas.** [widget id=»custom_html-22″] El proceso **implica mucho más que revisar una lista de verificación con requisitos y documentos exigibles**. Si no se aplican criterios rigurosos de debida diligencia, enfocados en la seguridad, la capacidad técnica, la reputación y el cumplimiento, es poco probable que la clasificación de contratistas resulte en la contratación de la mejor fuerza laboral externa para realizar el trabajo.

Qué preguntar en la etapa de clasificación de contratistas

Muchos procesos de clasificación de contratistas fracasan porque se limitan a recopilar información superficial. No se enfocan en aspectos formales obvios y pasan por alto la investigación sobre posibles problemas que pueden trasladarse a la organización. En un buen proceso de clasificación de contratistas, **la clave está en la formulación de las preguntas acertadas**, sobre los temas correctos. Solo así se puede obtener una visión integral y realista del contratista, de su capacidad y del conocimiento que puede aportar para conducir el proyecto a buen término. Surge entonces la duda de qué preguntar en un proceso de clasificación de contratistas. **La siguiente lista de verificación aborda seis áreas con sus respectivas preguntas** y con un valor añadido interesante: el aporte que puede hacer la tecnología en cada una de las áreas de investigación.

1. Seguridad: cultura y antecedentes

El objetivo es indagar sobre la **cultura de seguridad** del contratista, así como **valorar su experiencia y conocimiento en el área de seguridad y salud en el trabajo**. Las preguntas que habría que realizar son las siguientes:

- ¿Cuál es su **concepción sobre la seguridad en el trabajo** y cómo la implementa?
- ¿Ha sufrido recientemente **accidentes, lesiones o heridas**, o ha estado involucrado en incidentes de seguridad?
- ¿Cómo ha actuado ante incidentes o accidentes, esté o no involucrado en ellos?

Compliance ambiental: principales elementos a considerar

Compliance ambiental es el nombre por el que se conoce al conjunto de estrategias, procesos y procedimientos que, dentro del área de gestión y los **planes de acción HSE**, se ocupa de garantizar que la organización cumpla con las regulaciones, leyes, acuerdos contractuales y solicitudes de las partes interesadas en relación con la protección del medio ambiente y mitigación de su impacto ambiental. Gran parte de las **obligaciones de cumplimiento ambiental** se resuelven **adoptando buenas prácticas, transparentes y responsables**. Algunas exigencias de los reguladores, que también lo son de los consumidores, incluyen la disminución de las emisiones de gases de efecto invernadero o la implementación de procesos de economía circular, por mencionar dos de las más comunes. Evitar la contaminación y preservar las fuentes de recursos naturales son también solicitudes que están asociadas a alguna obligación de cumplimiento. En consecuencia, el compliance ambiental se ocupa de **verificar que se alcance la conformidad con la exigencia regulatoria**, pero también

de recabar evidencia suficiente para comprobar que se hizo. Las organizaciones necesitan **estar al día con la evolución del marco regulatorio**. Esa es otra de las responsabilidades que asumen los encargados de compliance ambiental. Hacerlo requiere asumir un enfoque proactivo, anticiparse a los cambios y realizar evaluaciones y revisiones constantes.

¿Qué elementos considerar para garantizar el compliance ambiental?

La gestión eficiente y oportuna del compliance ambiental **reduce el riesgo de sanciones, multas, pérdida de licencias o cierre de la operación**. También es un elemento que influye en la percepción de los consumidores a la hora de elegir sus proveedores de productos y servicios. Las organizaciones que cumplen con sus obligaciones ambientales **tienden a crecer de forma sostenida y sostenible**, a ser más competitivas e innovar en tecnología. Es notable el incremento de equipos, software e, incluso, sistemas de IA vinculados a empresas que se esfuerzan por reforzar el compliance ambiental en áreas como la gestión operativa, contabilidad de la **huella de carbono** o control de emisiones. Lograrlo y mantenerlo requiere considerar los siguientes elementos esenciales:

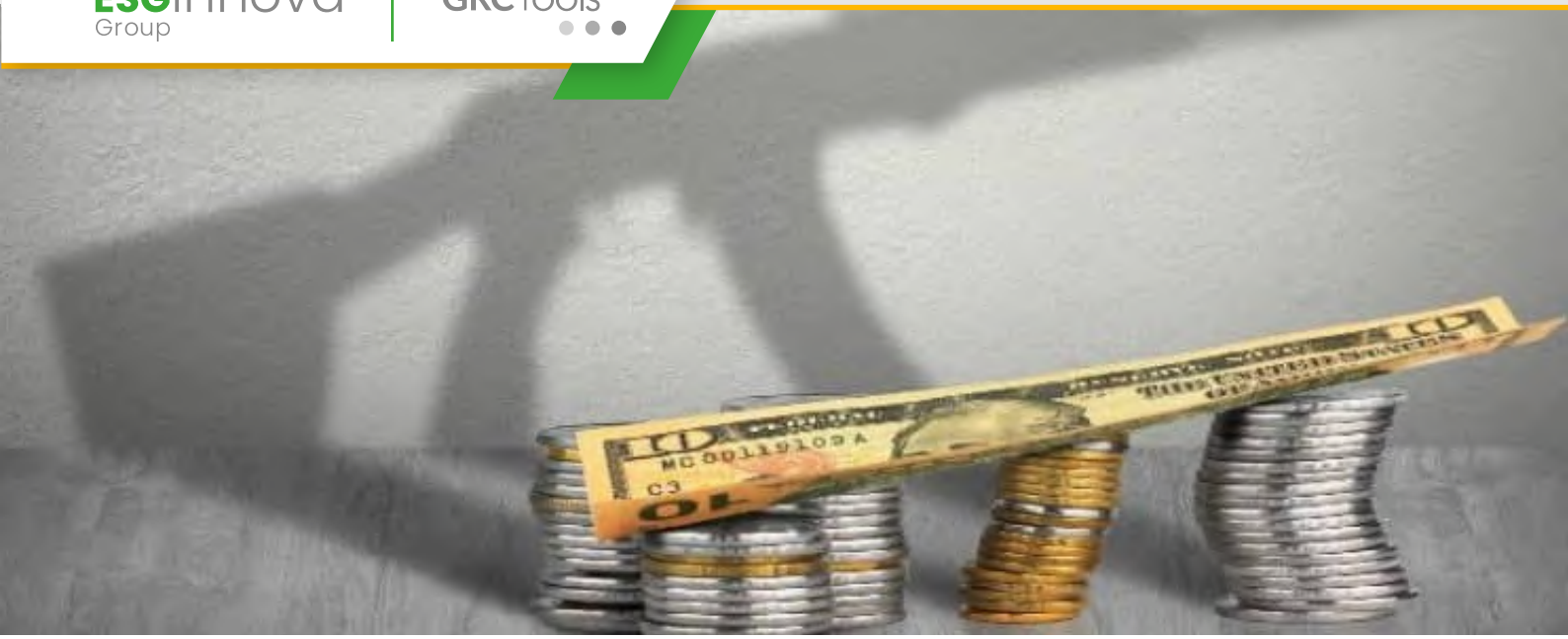
1. Implementar un sistema de gestión ambiental (SGA)

Un SGA es un conjunto de procesos diseñados para alcanzar objetivos ambientales, a la vez que cumplen con los requisitos de un estándar. **La norma internacional para gestión ambiental, que goza de mayor reconocimiento y aceptación es ISO 14001**. Eso no impide que existan **otros estándares que buscan objetivos similares.**

ESGinnova Group

GRCTools

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



Que es SAGRILAFT y quién lo debe implementar

La creciente presión regulatoria y las expectativas del mercado exigen a las empresas un compromiso real con la transparencia, la integridad y el cumplimiento normativo. En este contexto, entender **que es SAGRILAFT** se vuelve crucial, ya que muchas organizaciones aún enfrentan dificultades para identificar y gestionar eficazmente los riesgos asociados al Lavado de Activos y la Financiación del Terrorismo (**LA/FT**), exponiéndose a sanciones, pérdida de reputación y pérdida de confianza.

Ignorar o subestimar estos riesgos puede tener consecuencias devastadoras: bloqueos de operaciones, investigaciones judiciales, pérdida de socios estratégicos e incluso exclusión del sistema financiero. En un contexto donde los estándares internacionales son cada vez más estrictos, las empresas no pueden darse el lujo de operar sin mecanismos preventivos sólidos.

Para dar respuesta a este desafío, **Colombia ha implementado el SAGRILAFT** (Sistema de Autocontrol y Gestión del Riesgo Integral LA/FT), un modelo normativo robusto que exige a las empresas

identificar, evaluar, controlar y monitorear los riesgos LA/FT desde una perspectiva estratégica y basada en riesgos.

Cada vez más organizaciones del sector real reconocen que cumplir con el SAGRILAFT, además de permitirles evitar sanciones, fortalece su reputación, abre puertas a nuevos mercados e impulsa la madurez de su Gobierno Corporativo.

Adoptar este sistema es un paso fundamental, pero implementarlo de forma eficaz requiere tecnología especializada. **GRCTools** ofrece una plataforma integral para digitalizar y automatizar todos los procesos relacionados con el cumplimiento de SAGRILAFT, convirtiendo una obligación legal en una ventaja competitiva.

¿Que es SAGRILAFT?

El **SAGRILAFT** fue establecido por la **Superintendencia de Sociedades de Colombia** mediante la **Circular Externa 100-000016 de 2020**, y representa la evolución del anterior sistema **SARLAFT**. Se trata de un conjunto de políticas, procedimientos y mecanismos que deben adoptar ciertas empresas para prevenir que sus operaciones sean utilizadas como vehículo para el lavado de activos o la financiación del terrorismo.

Este sistema implica controles formales y una **gestión proactiva basada en el análisis de riesgos**, con componentes esenciales como:

- Identificación y evaluación de riesgos asociados a LA/FT.
- Diseño e implementación de medidas de mitigación.

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO

3 buenos consejos de gestión de riesgos

Los entornos volátiles, la incertidumbre regulatoria y los avances tecnológicos constantes, hacen que la gestión de riesgos se haya convertido en una pieza clave para garantizar la sostenibilidad y competitividad de las organizaciones. No basta con reaccionar ante las amenazas; es necesario anticiparse, prepararse y actuar con inteligencia. En este contexto, compartimos tres consejos de gestión de riesgos fundamentales para fortalecer la gestión de riesgos en cualquier organización moderna, especialmente en el sector empresarial.

1. Incorporar el análisis de riesgos en la toma de decisiones estratégicas

La transformación digital del Gobierno, Riesgo y Cumplimiento (GRC) exige repensar los modelos tradicionales, integrando nuevas prácticas, marcos normativos y herramientas tecnológicas. Uno de los mayores desafíos en las empresas es lograr que la gestión de riesgos no se limite a una función aislada, sino que se integre como una **herramienta de apoyo estratégico**.

Cada decisión empresarial —desde una expansión internacional hasta la adopción de una nueva tecnología— conlleva riesgos inherentes que deben ser identificados y evaluados.

¿Cómo lograrlo?

Adoptando un enfoque basado en datos, que utilice **matrices de riesgos**, escenarios prospectivos y mapas de calor como parte de los procesos de planificación y evaluación. Esto permite a los líderes visualizar el impacto potencial de cada decisión y adoptar planes de mitigación desde el inicio.

1. Beneficio clave:
Este es uno de los principales **consejos de gestión de riesgos** que toda organización debería aplicar. Una organización que integra la gestión de riesgos en su toma de decisiones es más ágil, resiliente y confiable frente a sus grupos de interés.

2. Fomentar una cultura organizacional orientada al riesgo

Más allá de los modelos y procedimientos, la verdadera fortaleza de un sistema de gestión de riesgos radica en su **cultura interna**. Una cultura organizacional orientada al riesgo se traduce en empleados conscientes, líderes comprometidos y procesos más transparentes.

Buenas prácticas para fortalecer la cultura de riesgos

- Capacitación continua sobre gestión de riesgos, cumplimiento normativo y ética organizacional.
- Espacios de reporte confidencial para alertar sobre incidentes o malas prácticas.

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO

Por qué el CISO y la Alta Dirección deben entenderse en materia de ciberseguridad

¿Qué pasaría si un ciberataque paralizara por completo tu operación mañana? No es una pregunta hipotética, sino un riesgo real que enfrentan miles de organizaciones cada día. El problema no es solo tecnológico, sino estratégico: en muchas empresas, el **CISO** y la Alta Dirección aún no hablan el mismo idioma cuando se trata de **ciberseguridad**.

La desconexión entre ambos niveles puede amplificar el impacto de una brecha digital. Cuando el **CISO** no logra traducir los riesgos técnicos en implicancias de negocio, y los líderes no comprenden la urgencia de fortalecer la protección digital, el terreno queda abonado para decisiones lentas, reactivas e ineficaces.

Pero hay una solución. Una relación sólida, basada en el entendimiento mutuo, puede transformar la ciberseguridad en una ventaja competitiva.

Cuando el **CISO** participa activamente en la estrategia corporativa y cuenta con herramientas para comunicar el valor de su trabajo en términos de riesgo y cumplimiento, todo cambia.

Cada vez más organizaciones están demostrando que este alineamiento es posible. Aquellas que promueven la integración entre el **CISO** y la Alta Dirección reportan mayor agilidad, mejor toma de decisiones y una postura digital más robusta.

En este artículo, te mostramos cómo lograrlo, qué prácticas lo hacen posible y cómo una solución como **GRCTools** puede ser el catalizador para convertir la ciberseguridad en un eje transversal del gobierno corporativo.

La ciberseguridad como prioridad estratégica

Durante años, la ciberseguridad fue considerada un tema técnico, relegado a los especialistas en sistemas. Sin embargo, con el crecimiento de los ataques sofisticados, la filtración de datos sensibles y las regulaciones más exigentes, la ciberseguridad se ha convertido en una **cuestión de gobierno corporativo**.

El **CISO** ya no solo protege infraestructuras tecnológicas; debe anticipar riesgos, interpretar el impacto en el negocio y establecer puentes con quienes toman decisiones estratégicas. Y es ahí donde entra en juego la Alta Dirección.

Por qué el CISO necesita hablar el lenguaje del negocio

Uno de los retos más grandes para el **CISO** es traducir las amenazas técnicas en términos comprensibles y relevantes para la dirección ejecutiva.

¿Cuál es el rol del Compliance Governance Specialist?

El cumplimiento corporativo ya no es lo que solía ser. En un mundo cada vez más interconectado, con regulaciones que evolucionan a ritmo acelerado y una creciente demanda de transparencia, las empresas necesitan mucho más que un enfoque reactivo para responder al entorno normativo. El compliance ha dejado de ser solo una barrera de protección legal: hoy es un pilar estratégico para la sostenibilidad y la gobernanza efectiva.

En este escenario, emerge una figura clave: el **Compliance Governance Specialist**. Lejos de limitarse a verificar listas de control o asegurar el cumplimiento formal, este perfil integra visión, análisis y tecnología para construir sistemas de cumplimiento robustos, adaptables y alineados con los objetivos del negocio.

En este artículo profundizaremos en sus funciones, competencias y valor añadido, con especial atención al papel de la tecnología —y en particular de plataformas como **GRCTools**— como aliada para potenciar su impacto dentro de la organización.

De la gestión del cumplimiento a la gobernanza del cumplimiento

Tradicionalmente, las funciones de **cumplimiento** han estado orientadas a garantizar que la organización actúe conforme a las **normativas externas e internas**. Sin embargo, este enfoque operativo ha demostrado ser insuficiente para enfrentar los desafíos actuales, donde los **riesgos éticos, regulatorios y reputacionales** están cada vez más interrelacionados y requieren una **visión holística**.

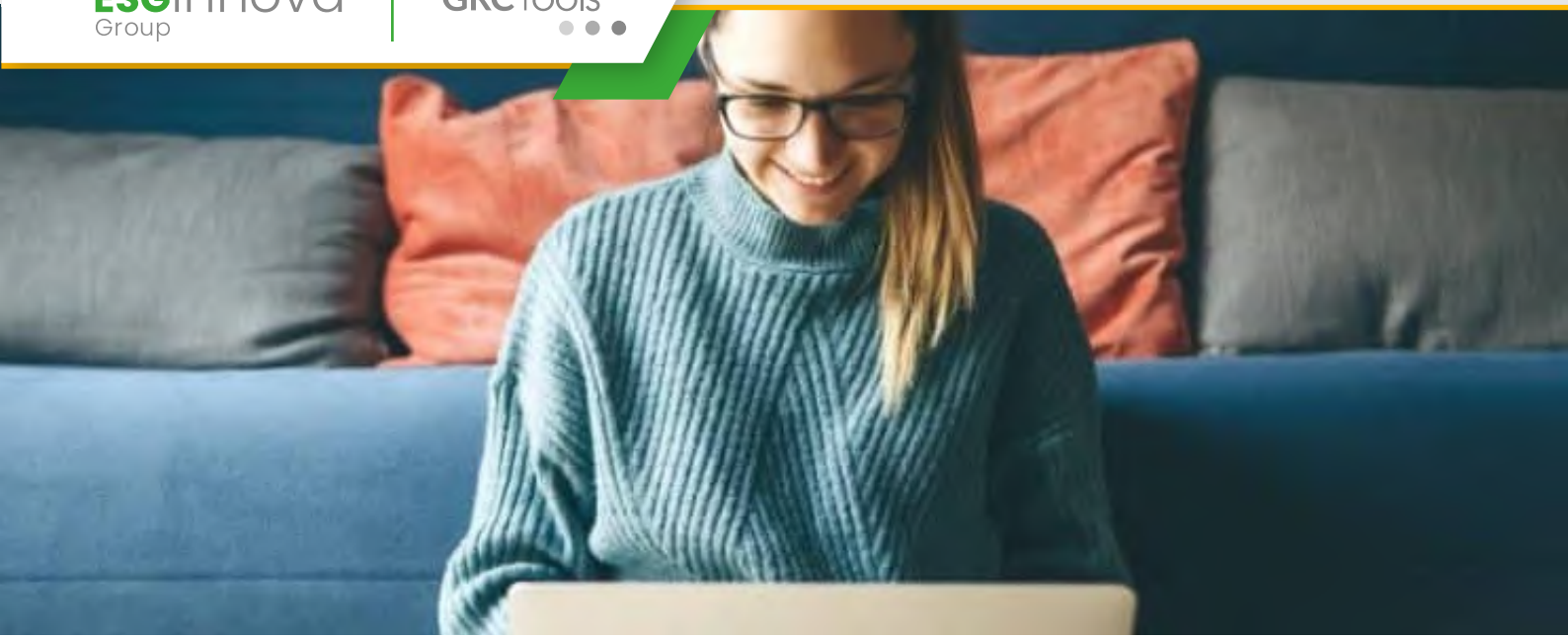
El **Compliance Governance Specialist** es un perfil estratégico que **diseña, articula y supervisa** la **estructura de gobernanza** del sistema de cumplimiento. Su enfoque no es únicamente operativo, sino estructural. Su misión es asegurar que el cumplimiento esté adecuadamente integrado a la **cultura**, a la **estrategia** y a los **procesos de toma de decisiones** de la organización.

Principales responsabilidades del Compliance Governance Specialist

Las funciones de este profesional abarcan múltiples dimensiones, que se entrelazan con otros sistemas de gestión y con los órganos de gobierno de la empresa.

Diseño del modelo de gobernanza del cumplimiento

Una de sus principales funciones es definir el **modelo de gobernanza** del sistema de cumplimiento. Esto incluye establecer **roles**, **responsabilidades**, **flujos de información**, **mecanismos de supervisión** y **canales de reporte**.



¿Qué son los riesgos invisibles del trabajo remoto?

En los últimos años, el trabajo remoto ha dejado de ser una medida excepcional para convertirse en una realidad permanente en muchas organizaciones. Aunque ofrece beneficios indiscutibles —como mayor flexibilidad, ahorro de costos y atracción de talento global— también ha traído consigo un conjunto de **riesgos no evidentes**, difíciles de medir y a menudo ignorados por los marcos tradicionales de gestión. Estos **riesgos invisibles del trabajo remoto**, si no se abordan adecuadamente, pueden comprometer la **gobernanza corporativa**, erosionar el cumplimiento normativo y debilitar los sistemas de gestión de riesgos.

Desde una perspectiva GRC (Gobierno, Riesgo y Cumplimiento), el desafío no radica únicamente en adaptar los procesos existentes al entorno digital, sino en **redefinir el perímetro del control**, considerando factores humanos, tecnológicos y organizacionales que antes eran marginales. Este artículo explora en profundidad qué son estos riesgos invisibles del trabajo remoto, por qué deberían preocupar a los líderes empresariales y cómo pueden ser gestionados desde un enfoque integrado GRC.

¿Qué entendemos por riesgos invisibles del trabajo remoto?

Los **riesgos invisibles** del trabajo remoto son aquellos que no se manifiestan con claridad inmediata, no dejan huellas tangibles en los sistemas de reporte tradicionales y, sin embargo, tienen un alto potencial disruptivo. En el contexto del trabajo remoto, estos riesgos no son nuevos, pero su **nivel de exposición ha aumentado significativamente** con la descentralización del entorno laboral.

A diferencia de los riesgos clásicos —como los financieros, operativos o regulatorios— estos no siempre se relacionan con eventos específicos, sino con **dinámicas organizacionales de fondo**, que si se descuidan pueden generar consecuencias acumulativas: reducción del compromiso, fuga de talento, incumplimientos regulatorios o pérdida de confianza en la marca.

Riesgos psicosociales y culturales: la amenaza silenciosa

Uno de los componentes más críticos de los riesgos invisibles del trabajo remoto es el factor humano. El trabajo remoto, si bien aumenta la autonomía, también **puede generar aislamiento**, debilitamiento de la cohesión del equipo y pérdida del sentido de pertenencia. El contacto humano espontáneo, que en el entorno presencial funcionaba como catalizador emocional y cultural, se ve limitado, lo que **afecta directamente la cultura organizacional**.

Además, la **autoexigencia** en contextos remotos puede derivar en jornadas más largas, con pausas menos frecuentes y una presión constante por demostrar productividad. Este fenómeno, conocido como **“presencialismo digital”**, está vinculado al agotamiento emocional y al síndrome de burnout, especialmente en equipos con liderazgo débil o poco empático.

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO

Lecciones acerca de la gestión de riesgos y resiliencia empresarial

La crisis sanitaria global, los conflictos geopolíticos, la disrupción digital y el cambio climático son apenas algunas de las fuerzas que han puesto a prueba la capacidad de las organizaciones para **anticipar, responder y recuperarse** ante lo inesperado. En este entorno incierto y complejo, la **gestión de riesgos y resiliencia empresarial** ya no puede ser un ejercicio técnico aislado, ni la **resiliencia empresarial** una simple aspiración: ambas se han convertido en **factores críticos de sostenibilidad**.

La gestión de riesgos y resiliencia empresarial

Desde la perspectiva GRC (Gobierno, Riesgo y Cumplimiento), las crisis recientes han dejado enseñanzas profundas que invitan a repensar la forma en que se **identifican amenazas**, se **gestionan vulnerabilidades** y se **fortalece la capacidad organizacional para resistir y adaptarse**.

Este artículo reúne algunas de las lecciones clave que deben tener en cuenta los líderes de hoy para construir organizaciones más preparadas y antifrágiles.

1. El riesgo ya no es estático ni predecible

Uno de los aprendizajes más evidentes es que **el riesgo ha dejado de ser una variable estable**. Ya no es posible pensar en amenazas aisladas, de aparición gradual o de impacto contenido. La realidad nos muestra un ecosistema de riesgos **interconectados, transversales y de alta velocidad**, donde un incidente local puede tener consecuencias globales en cuestión de horas.

La **gestión tradicional del riesgo**, centrada en eventos pasados y modelos probabilísticos, resulta insuficiente frente a crisis sistémicas como una pandemia, una guerra cibernética o un colapso climático. Por eso, las organizaciones deben evolucionar hacia **modelos dinámicos, integrados y prospectivos**, capaces de anticipar no solo lo probable, sino también lo posible y lo inesperado.

2. La resiliencia no es lo mismo que continuidad del negocio

Un error frecuente es confundir **resiliencia** con **planes de continuidad de negocio o recuperación operativa**. Aunque estos son componentes necesarios, la resiliencia implica algo más profundo: es la capacidad de una organización para **absorber impactos, aprender de la adversidad y transformarse de manera proactiva**.

Cómo afrontar los riesgos del RGPD en la Inteligencia Artificial

Pongamos sobre la mesa el contexto empresarial actual en torno a los riesgos del RGPD: la **automatización** y el uso de **tecnologías predictivas**, como la **Inteligencia Artificial (IA)**, se han consolidado como un motor de innovación. Sin embargo, este avance técnico plantea desafíos significativos para la **protección de datos personales**, especialmente en lo que respecta al cumplimiento del **Reglamento General de Protección de Datos (RGPD)**.

La IA depende de grandes volúmenes de información para generar patrones, tomar decisiones o anticipar comportamientos. Cuando esta información incluye datos personales —como hábitos de consumo, datos biométricos, ubicaciones o historiales clínicos—, surgen riesgos críticos que deben gestionarse con rigor. El incumplimiento del RGPD en proyectos de IA deriva en **sanciones económicas severas**, y también en una pérdida de **confianza pública** y en impactos éticos y reputacionales de gran alcance.

Riesgos del RGPD: La complejidad del cumplimiento en sistemas inteligentes

A diferencia de los sistemas tradicionales, los algoritmos de IA —especialmente los basados en **machine learning** o **deep learning**— presentan problemas de **opacidad**. Es frecuente que ni siquiera los desarrolladores puedan explicar con claridad cómo un modelo ha llegado a una decisión concreta, lo que dificulta garantizar los derechos reconocidos en el RGPD, como el derecho a la información, el acceso o la oposición.

Además, la IA suele requerir el tratamiento de **grandes volúmenes de datos**, lo que entra en tensión con principios como la **minimización del tratamiento** o la **limitación de la finalidad**. Esta situación obliga a las organizaciones a adoptar enfoques preventivos y estructurados para mitigar los riesgos y asegurar la **responsabilidad proactiva**.

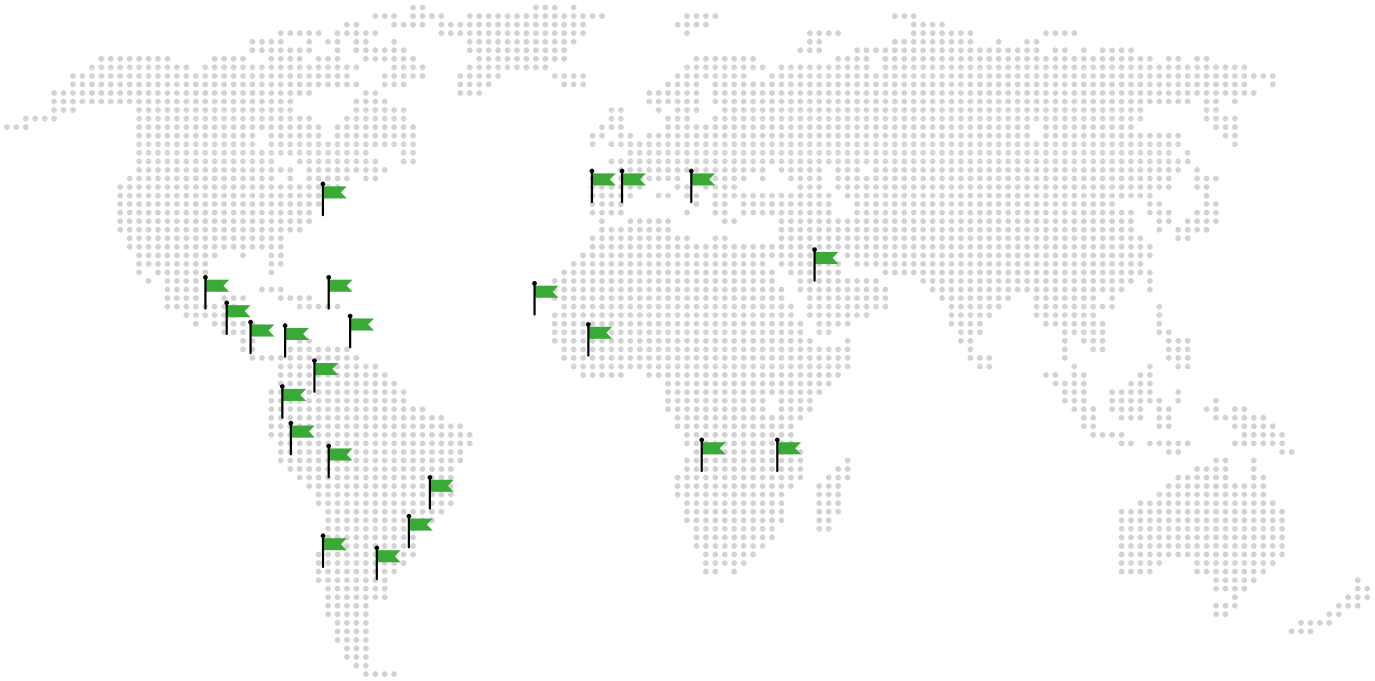
Principales riesgos del RGPD en la IA

Entre los riesgos más relevantes que plantea el uso de IA en relación con el RGPD, destacan:

- **Falta de transparencia**: La naturaleza técnica de los modelos puede impedir a los usuarios comprender cómo y por qué se han utilizado sus datos.

- **Decisiones automatizadas sin intervención humana**: El artículo 22 del RGPD limita este tipo de decisiones cuando pueden tener efectos significativos sobre el interesado.

- **Perfilados discriminatorios**: Si los datos de entrenamiento están sesgados, el algoritmo puede reproducir o amplificar esa discriminación.



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