

EMPRESA **EXCELENTE**

Las mejores temáticas sobre Normas ISO, HSE y GRC



2024
SEPTIEMBRE

ESGinnova
Group

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



Índice



ACERCA DE ESG INNOVA GROUP	04
NORMAS ISO	09
✓ Regulación IA en el mundo: panorama regulatorio de la inteligencia artificial actual.....	10
✓ Beneficios de ISO 27001:2022: factores clave del proyecto	12
✓ 5 formas en las que la ISO 37120 contribuye al ODS 11	14
✓ ¿Cómo se ve impactado el ODS 12 por la serie ISO 14020?	16
✓ ISO 42001: cómo implementar un Sistema de Gestión de Inteligencia Artificial en tu empresa	18
✓ Identificación de riesgos en ISO 14001: guía completa.....	20
✓ Tips para el sector marítimo: ISO 21070 y ODS 14	22
✓ ISO 14055-1: Protegiendo la vida en la tierra de la degradación del suelo para cumplir el ODS 15	24
✓ ISO 44001: Alianzas Colaborativas para el ODS 17	26
✓ Certificación de la norma ISO 42001: proceso a seguir paso a paso	28
✓ Cómo definir los objetivos y planes en ISO 45001	30
✓ 8 peculiaridades de la ISO 42001 que debes conocer	32
✓ Sistema de Gestión de Inteligencia Artificial (SGIA): definición y componentes clave	34
✓ Requisitos legales y reglamentarios en ISO 9001: cómo incluirlos en tu SGC.....	36
✓ 5 principales definiciones ISO 45001	38
✓ Como hacer auditoria interna ISO 45001	40
SEGURIDAD, SALUD Y MEDIOAMBIENTE	42
✓ Buenas prácticas en la gestión de equipos de protección personal para optimizar el programa SST	43
✓ ¿Cuál es la Definición de Control en el Contexto Empresarial?.....	45
✓ 7 desafíos comunes en la gestión de contratistas.....	47
✓ Minería y Conservación del Medio Ambiente: Desafíos y Soluciones Integradas.....	49
✓ 10 Pasos clave a la hora de seleccionar un software HSE.....	51
✓ Salud Ocupacional en la Minería: Claves para un Entorno Laboral Seguro	53
✓ 7 Consejos para elegir un Sistema de Gestión de Contratistas	55

Índice



✓ Implementar un software de gestión de incidentes y accidentes: 5 beneficios clave	57
✓ Gestión de contratistas digital: 5 beneficios para mejorar la sostenibilidad	59
✓ ¿Que son las charlas de 5 minutos?	61
✓ Cómo el software de cumplimiento ambiental puede ayudar a cumplir con las normativas	63
✓ 5 Pasos para gestionar contratistas de forma eficaz	65
✓ Arbol de Causas: Herramienta para la Mejora Continua	67
✓ ¿Que se conoce como gestión ambiental?	69
GOBIERNO, RIESGO Y CUMPLIMIENTO	71
✓ Cómo Fortalecer la Transparencia Corporativa con el Software GRC	72
✓ La Importancia de la Gestión Estratégica en Startups y PYMEs	74
✓ El rol del GRC en la prevención de ataques internos.....	76
✓ Gestión de Riesgos Asociados a la Privacidad de Datos	78
✓ Tendencias Actuales en la Gestión Estratégica	80
✓ Estrategias efectivas para mitigar los riesgos operacionales en el entorno empresarial actual	82
✓ Estrategias de Economía Circular con el apoyo de GRCTools	84
✓ Transformación Digital del Compliance: Cómo GRCTools Establece Nuevos Estándares	86
✓ Optimización de la respuesta a incidentes de ciberseguridad con GRC	88
✓ Pasos de la Gestión Estratégica: Guía completa para empresas.....	90
✓ Protección contra ataques de ransomware mediante GRC.....	92
✓ La importancia de la gestión de riesgos de terceros en la cadena de suministro.....	94
✓ Mejores Prácticas en la Gestión de Riesgos con Herramientas GRC.....	96
✓ Beneficios de implementar un programa de Compliance en tu organización	98
✓ Estrategias de Economía Circular con el Apoyo de GRCTools	100
✓ Automatización de políticas de ciberseguridad con GRC	102
✓ Certificación COBIT 5: principios y controles para la gestión de riesgos	104
✓ DORA: La nueva regulación de Ciberseguridad para el Sector Financiero.....	106
✓ El camino hacia la Excelencia	108

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.

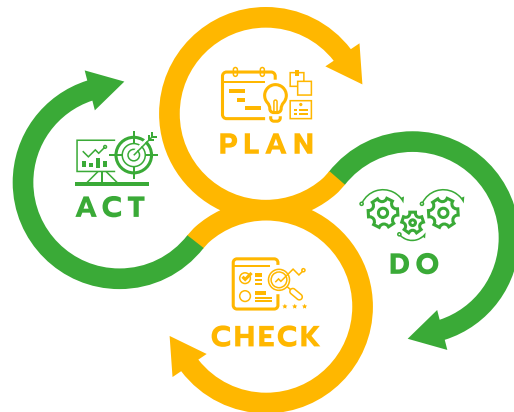
Plataforma ESG Innova

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

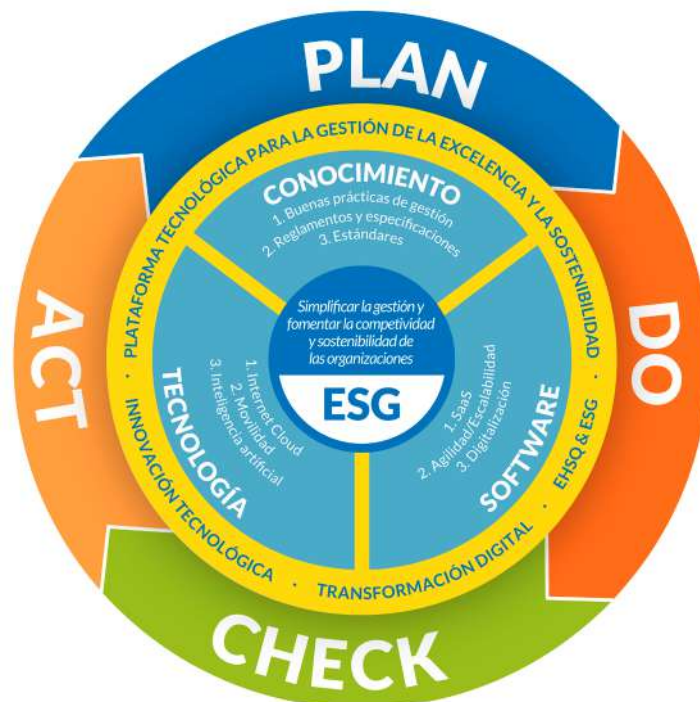
Simplificamos la monitorización y seguimiento, aportando información útil para la toma de decisiones.

❖ 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

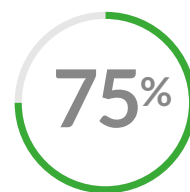
Optimización del tiempo



Menos de tiempo de resolución de una acción correctiva



Menos de tiempo de preparación de las reuniones de gestión

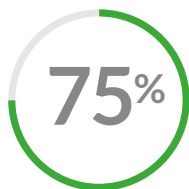


Menos de tiempo dedicado a recopilar y tratar indicadores

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

ISOTools



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



Regulación IA en el mundo: panorama regulatorio de la inteligencia artificial actual

La **regulación IA** es una de las cuestiones que hay que considerar de manera inexcusable cuando se habla de esta nueva tecnología. Los desarrollos de **Inteligencia Artificial** avanzan a una velocidad vertiginosa y es algo que **genera preocupaciones y un intenso debate** a nivel de países, organizaciones y sociedad en general.

Son, en cualquier caso, dudas y cuestionamientos válidos que **deben resolverse sin demora**. La regulación IA es el camino correcto para hacerlo y esa senda regulatoria ya se ha iniciado. A continuación, repasamos los avances que se han registrado ya en lo que a regulación IA se refiere.

Una aproximación a los avances en regulación IA

El desarrollo vertiginoso de la nueva tecnología no puede dejar a un lado las **preocupaciones éticas**, de seguridad, sociales e incluso de derechos humanos que genera.

Gobiernos, organismos no gubernamentales y organizaciones privadas trabajan con el objetivo de **crear escenarios regulatorios para hacer frente a los desafíos** que implica el uso de la Inteligencia Artificial.

En ese camino, **algunos esfuerzos son de orden supranacional**, como la **Ley de IA de la Unión Europea**, que vio la luz en diciembre de 2023. Otros son de alcance global y algunos más se desarrollan con carácter interno en diferentes países.

1. Ley de la Inteligencia Artificial de la Unión Europea

La regulación IA encuentra un hito en la que ha sido legislación pionera sobre la nueva tecnología. El objetivo de esta norma es **exigir el uso seguro, legal, confiable y respetuoso** con los derechos humanos, de los **sistemas de Inteligencia Artificial**.

La ley clasifica el uso de Inteligencia Artificial de acuerdo con tres niveles de riesgo: bajo, alto e inaceptable. Así, sectores como farmacéutico o sanitario son de riesgo alto, debido a las implicaciones que tienen sobre las personas.

La ley es de obligatorio cumplimiento en el territorio de la Unión Europea desde el 9 de diciembre de 2023, constituyéndose en el **primer marco regulatorio de alcance supranacional en el mundo**.

La tarea de los gobiernos de los Estados miembros ahora es adaptar sus legislaciones nacionales a lo dispuesto por la ley de la UE.



Beneficios de ISO 27001:2022: factores clave del proyecto

Conocer los **beneficios de ISO 27001:2022** es una estrategia efectiva para convencer a la Alta Dirección, de cualquier organización, para que asigne los recursos que requiere la implementación de un **sistema de gestión de seguridad de la información** basado en el estándar internacional.

Obtener el apoyo de la Alta Dirección es el primer paso y los beneficios de ISO 27001:2022 son un apoyo importante para afrontar el desafío inicial. Sin embargo, hay otros factores que determinan el éxito del proyecto y que también deben considerar quienes se ocupan de la seguridad de la información.

Beneficios de ISO 27001:2022 para una organización

Hablar de los beneficios de un proyecto, cuando este se expone a la Alta Dirección, suele centrarse en un tema: el retorno de la inversión. **Entre los beneficios de ISO 27001:2022 hay algunos de orden económico.** Sin embargo, y aunque todos los beneficios sean susceptibles de ser expresados en cantidades de dinero, algunos tienen un **impacto positivo** que se puede valorar más allá del mero aspecto económico.

1. Mejora el cumplimiento

La seguridad de la información involucra temas que se regulan en casi todos los países del mundo. Uno de ellos es la privacidad y confidencialidad de los datos y la **información sensible de las personas.** En la Unión Europea esta tarea la ejerce el RGPD.

El incumplimiento o **las infracciones de seguridad de los datos hacen mella en la reputación de la organización.** No solo eso, también pueden suponer un alto coste financiero por pérdida de credibilidad. En algunos casos pueden determinar el fin de una empresa. Uno de los beneficios de ISO 27001:2022 es, precisamente, que ayuda a las organizaciones a **cumplir con la normativa.**

2. Mejora de la percepción entre los consumidores

Atrás quedaron los tiempos en los que un solo fabricante o una empresa dominaban un mercado con exclusividad. Bienes de consumo tienen millones de proveedores y los consumidores buscan puntos de referencia diferenciadores.



5 formas en las que la ISO 37120 contribuye al ODS 11

ISO 37120

La **ISO 37120** es una norma internacional que proporciona indicadores clave para **medir el desempeño de los servicios y la calidad de vida en las ciudades**. Esta norma está estrechamente vinculada al **Objetivo de Desarrollo Sostenible 11 (ODS 11)**, que busca hacer que las ciudades y los asentamientos humanos sean **inclusivos, seguros, resilientes y sostenibles**.

Establece un conjunto estandarizado de **indicadores** para **medir y comparar el desempeño de las ciudades en diferentes áreas clave**. Fue desarrollada para ayudar a los gobiernos municipales a tomar decisiones informadas sobre **planificación y desarrollo urbano**, centrándose en aspectos como infraestructura, medio ambiente, educación, salud y gobernanza.

El **propósito** principal de la **ISO 37120** es permitir a las ciudades **monitorear su progreso y mejorar la calidad de vida** de sus habitantes, promoviendo la **sostenibilidad** y la **resiliencia urbana**.

Esto se alinea directamente con el **ODS 11**, que busca transformar las ciudades en espacios más inclusivos, seguros y ecológicamente responsables.

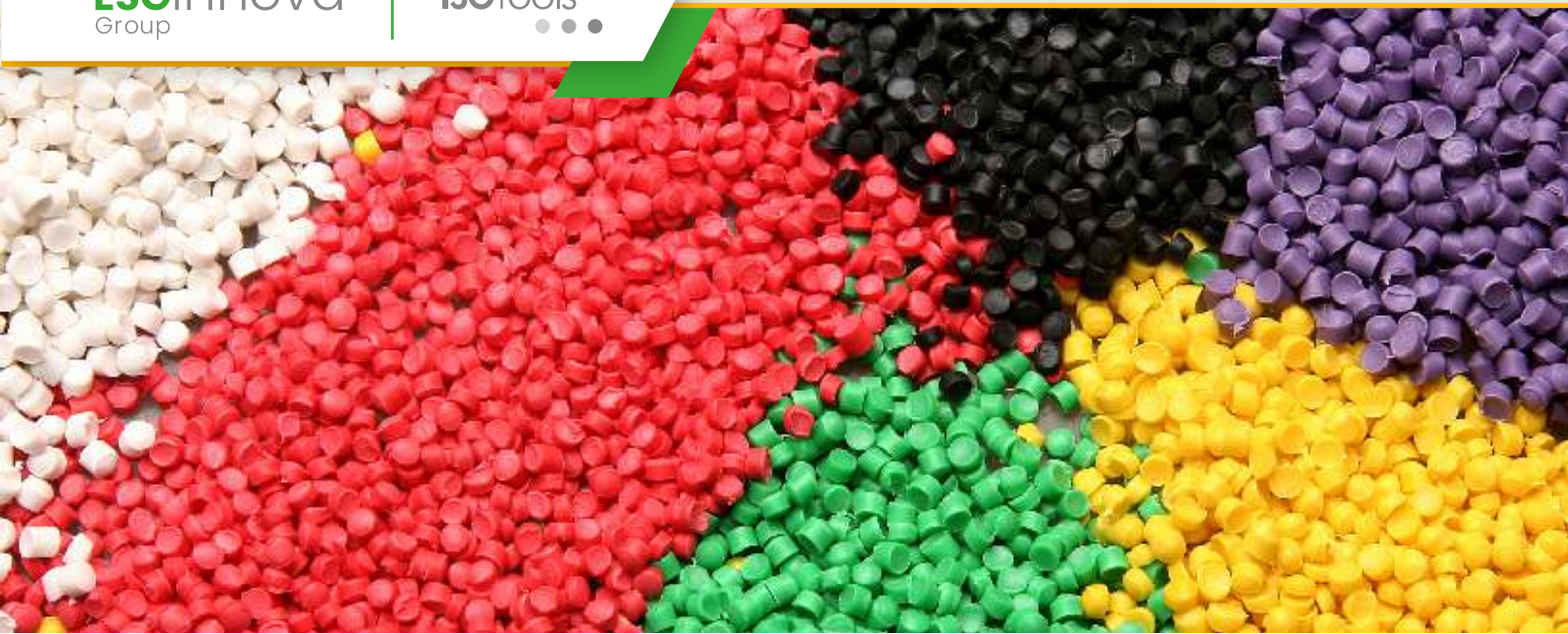
La **ISO 37120** utiliza un conjunto de más de 100 **indicadores** organizados en 19 áreas, como:

- **Vivienda y servicios básicos**
- **Energía**
- **Gestión de residuos**
- **Transporte**
- **Seguridad**
- **Educación**
- **Salud**

Estos indicadores proporcionan datos comparativos que permiten a las ciudades **identificar sus fortalezas y debilidades**, facilitando la implementación de políticas que contribuyan al **desarrollo sostenible y la mejora de la calidad de vida**.

Promueve ciudades inclusivas y equitativas

Una de las metas fundamentales del **ODS 11** es garantizar el **acceso a viviendas asequibles y servicios básicos** para todos. La **ISO 37120** incluye indicadores que miden la cantidad de personas que viven en **asentamientos informales**.



¿Cómo se ve impactado el ODS 12 por la serie ISO 14020?

ISO 14020

El **Objetivo de Desarrollo Sostenible 12** (ODS 12) de la **Agenda 2030 de la ONU** se centra precisamente en promover el uso eficiente de los recursos naturales y la reducción de desechos, a fin de mitigar el impacto ambiental de las actividades humanas. En este contexto, la serie de normas **ISO 14020** juega un rol crucial, proporcionando un marco para la evaluación y comunicación de la **gestión ambiental** de productos y servicios.

ODS 12: Consumo y producción responsables

El ODS 12 se propone garantizar que la gestión de los recursos naturales y los residuos se realice de manera **sostenible**, reduciendo el uso excesivo de materiales y minimizando los impactos negativos en el medio ambiente.

Para lograrlo, es necesario transformar tanto las **cadena de producción** como los hábitos de consumo, fomentando la adopción de productos más sostenibles y prácticas empresariales más responsables.

En este sentido, el **ODS 12** abarca desde la **eficiencia en el uso de recursos** hasta la **gestión adecuada de productos químicos y desechos**. Entre sus metas, destacan la reducción de desechos mediante la prevención, reducción, reciclado y reutilización, así como la incorporación de prácticas sostenibles por parte de las empresas, especialmente las grandes multinacionales.

ISO 14020: Declaraciones ambientales en el Centro de la Transparencia

La serie de normas **ISO 14020** es parte de la **familia de normas ISO 14000** orientada a la gestión ambiental. Esta serie se enfoca en proporcionar principios y procedimientos para las **declaraciones ambientales** de productos y servicios, fomentando la transparencia y la precisión en la información ambiental que se comunica al consumidor. La serie incluye tres normas principales:

- **ISO 14021** – Etiquetas y declaraciones ambientales: declaraciones ambientales tipo II (autodeclaraciones ambientales).
- **ISO 14024** – Etiquetas y declaraciones ambientales: Principios y procedimientos para las declaraciones ambientales tipo I (etiquetas ecológicas).
- **ISO 14025** – Etiquetas y declaraciones ambientales: Principios y procedimientos para las declaraciones ambientales tipo III (declaraciones de producto ambiental).



ISO 42001: cómo implementar un Sistema de Gestión de Inteligencia Artificial en tu empresa

Implementar un Sistema de Gestión de Inteligencia Artificial es una estrategia efectiva para no quedarse atrás una carrera vertiginosa liderada por la **nueva tecnología**. Las organizaciones necesitan **garantizar que el uso que hace de la IA es socialmente responsable**, ajustado a la ley, transparente e incluyente.

El **uso de la IA** ha revolucionado la forma de operar de las organizaciones, pero también implica **superar grandes retos y abordar riesgos** hasta hace poco desconocidos. Por ello, la mejor forma de avanzar hacia ese objetivo que es su uso responsable pasa por implementar un Sistema de Gestión de Inteligencia Artificial.

Qué hacer antes de implementar un Sistema de Gestión de Inteligencia Artificial

Las preocupaciones y las dudas que sobre el uso de la IA han surgido desde sus inicios no tardaron en despertar el interés de la Organización Internacional de Normalización. Interés que adquiere forma en **un estándar diseñado para la Gestión de Sistemas de Gestión de Inteligencia Artificial: ISO 42001**.

ISO 42001 es reciente, **se publicó en 2023**. Por ello, un primer paso, antes de implementar un Sistema de Gestión de Inteligencia Artificial, es conocer la norma y hacer que la conozcan personas con implicación directa dentro de la organización.

Ya entrando sobre el terreno, aparecen **dos pasos preliminares**, necesarios para implementar un Sistema de Gestión de Inteligencia Artificial:

1. Evaluar las prácticas de gestión de la IA

Es lo que se conoce como análisis de brechas. Las organizaciones que pretenden implementar un Sistema de Gestión de Inteligencia Artificial integran una de dos condiciones, o las dos: desarrollan productos de Inteligencia Artificial o hacen uso de ella.

Es predecible que esas organizaciones hayan tomado algunas precauciones para **tratar riesgos** ante las preocupaciones que han sido ampliamente divulgadas. Y es probable que **algunas de esas acciones se ajusten a lo que solicitará ISO 42001**, estándar de gestión que se implementará.



Identificación de riesgos en ISO 14001: guía completa

La **identificación de riesgos en ISO 14001** es una solicitud del estándar de **gestión ambiental**. Así lo expresa la **cláusula 6.1.1**: “la organización identificará y considerará los riesgos y oportunidades, teniendo en cuenta su contexto interno y externo, los aspectos e impactos ambientales, sus obligaciones de cumplimiento y cualquier otro factor o circunstancia que tenga la capacidad de generar un riesgo o una oportunidad.

El capítulo 6 incluye otros requisitos específicos sobre la identificación de riesgos en ISO 14001. De ello se desprende que **la gestión de riesgos es el punto medular en la gestión ambiental**. Por eso, el contenido de este capítulo de la norma se constituye en una guía confiable para avanzar en esa labor.

Cómo desarrollar la identificación de riesgos en ISO 14001

El propósito prioritario y esencial de **ISO 14001** es **mitigar el impacto de la operación de la organización en el medio ambiente**, a la vez que se asegura el cumplimiento regulatorio en el área ambiental, de orden local, regional, nacional o internacional.

Esto explica la importancia de la identificación de riesgos en ISO 14001, que, como se ha adelantado, está condicionada por los requisitos contenidos en el capítulo 6. **La siguiente guía se basa en él:**

1. Información documentada

Se relaciona con lo expresado en el apartado 6.1.1. del estándar. La organización debe mantener información documentada (documentos y registros) de todos los procesos, procedimientos y actividades solicitadas en este capítulo. La **documentación** necesita **describir los procedimientos y metodologías utilizados para identificar los riesgos ambientales o las oportunidades**.

La norma **no recomienda u obliga el uso de una metodología en particular**. Pero sí exige que se documente el sistema o la metodología que se utilizará en la identificación de riesgos en ISO 14001, asegurando las siguientes cuestiones:

- **El enfoque de la metodología debe basarse en evidencia comprobable.** Es necesario entregar documentos auditables y un plan de operación posible.



Tips para el sector marítimo: ISO 21070 y ODS 14

ISO 21070 y ODS 14

En el sector marítimo, la correcta **gestión de los desechos** es un tema crítico para **preservar la salud de los océanos y proteger los ecosistemas marinos**. La **ISO 21070** establece requisitos para la gestión y manipulación de los residuos generados a bordo de los buques, mientras que el **ODS 14** (Objetivo de Desarrollo Sostenible 14) se centra en la **conservación y el uso sostenible de los océanos, mares y recursos marinos**. Juntas, estas normativas son esenciales para **garantizar que las operaciones marítimas** se lleven a cabo de manera **sostenible y responsable**.

Norma ISO 21070

La **ISO 21070** es una norma internacional que especifica los requisitos para la **gestión y manipulación de los residuos a bordo de los buques**. Su principal objetivo es reducir el impacto ambiental de las actividades marítimas mediante la **correcta segregación, almacenamiento, manejo y disposición** de los

residuos generados durante las operaciones a bordo. Esta norma cubre una **amplia gama de residuos**, incluidos los residuos sólidos, líquidos y peligrosos, y se enfoca en garantizar que los procedimientos de **gestión sean seguros y respetuosos** con el medio ambiente.

Entre los principales **objetivos** se incluyen:

- **Prevenir la contaminación marina** mediante la correcta gestión de los desechos.
- **Fomentar prácticas de manipulación seguras y responsables** de los residuos a bordo de los buques.
- **Promover la sostenibilidad** en las operaciones marítimas, alineándose con los objetivos internacionales de conservación marina.

La **ISO 21070** es aplicable a todas las **embarcaciones comerciales y de transporte** que generan residuos durante sus operaciones, incluidas las **naves mercantes, cruceros, buques pesqueros y plataformas offshore**. La norma se complementa con otras regulaciones, como el **Convenio MARPOL**, que regula la **prevención de la contaminación en los mares**, pero la **norma** proporciona una **guía más específica** para la gestión de los residuos en el **día a día** de las operaciones marítimas.

ODS 14

El **Objetivo de Desarrollo Sostenible 14** (ODS 14) forma parte de los **17 Objetivos de Desarrollo Sostenible** establecidos por las Naciones Unidas y tiene como fin **conservar y utilizar de manera sostenible los océanos, mares y recursos marinos**.



ISO 14055-1: Protegiendo la vida en la tierra de la degradación del suelo para cumplir el ODS 15

ISO 14055-1

La **degradación del suelo** es uno de los desafíos ambientales más graves que enfrenta el mundo en la actualidad y la **gestión ambiental**. Esta problemática afecta la productividad agrícola, la biodiversidad y la capacidad de los ecosistemas terrestres para mitigar el cambio climático. Frente a esta situación, la norma **ISO 14055-1** surge como una herramienta esencial para abordar y frenar la degradación del suelo. La aplicación de esta norma es un paso decisivo hacia el cumplimiento del **Objetivo de Desarrollo Sostenible (ODS) 15: Vida de Ecosistemas Terrestres**, que promueve la protección, restauración y uso sostenible de los ecosistemas terrestres.

¿Qué es la ISO 14055-1?

La ISO 14055-1 es una norma internacional publicada por la **Organización Internacional de Normalización (ISO)** que establece un marco de referencia para gestionar y mitigar la degradación del suelo. Publicada en 2017, está diseñada para ser aplicada en cualquier parte del mundo y propone directrices que pueden adaptarse a distintos contextos geográficos, climáticos y socioeconómicos. La norma se centra en la **gestión sostenible de los suelos**, protegiendo no solo la capacidad productiva de la tierra, sino también su biodiversidad y su papel en la regulación de los ecosistemas.

¿Qué abarca la degradación del suelo?

La degradación del suelo se refiere a la **pérdida de calidad y funcionalidad** del suelo debido a factores como la **erosión**, la **desertificación**, la **salinización**, la **deforestación**, y el **mal uso agrícola o industrial**. Estos procesos no solo reducen la fertilidad del suelo, sino que también afectan la capacidad de los ecosistemas para sostener vida, almacenar carbono y filtrar agua. Se estima que más del 30% de las tierras del planeta ya están degradadas, lo que pone en peligro la sostenibilidad a largo plazo.

Relación de la ISO 14055-1 con el ODS 15

El **ODS 15** busca proteger y restaurar los ecosistemas terrestres, con una especial atención en la lucha contra la desertificación y la degradación del suelo, así como en la promoción de la gestión sostenible de los bosques y la preservación de la biodiversidad.



ISO 44001: Alianzas Colaborativas para el ODS 17

ISO 44001

La **ISO 44001** es una norma internacional diseñada para ayudar a las organizaciones a construir **relaciones colaborativas efectivas y duraderas**. En un mundo empresarial cada vez más globalizado e interconectado, las **alianzas colaborativas** son clave para el **éxito y la sostenibilidad a largo plazo**. Esta norma se alinea perfectamente con el **ODS 17** que **promueve alianzas** para el logro de los **Objetivos de Desarrollo Sostenible (ODS)**.

La norma **ISO 44001** es una norma internacional que proporciona un marco para **establecer, gestionar y mejorar relaciones colaborativas** entre organizaciones. Este estándar es aplicable a empresas de cualquier tamaño y sector que busquen **colaborar con otras organizaciones para alcanzar objetivos comunes**. La norma se basa en la creación de **valor mutuo, transparencia y confianza** entre las partes involucradas.

Los principales **objetivos** de la **ISO 44001** son:

- Facilitar la **colaboración efectiva** entre organizaciones.
- Mejorar la **comunicación** y la **transparencia** en las relaciones de negocio.
- Promover la **creación de valor** compartido a través de alianzas estratégicas.
- Establecer mecanismos para la **resolución de conflictos** y el cumplimiento de los objetivos comunes.

La **ISO 44001** es aplicable a cualquier tipo de **relación colaborativa**, ya sea entre empresas, gobiernos, instituciones académicas u **organizaciones no gubernamentales (ONGs)**. Se utiliza en una variedad de contextos, como el desarrollo de **proyectos conjuntos, alianzas público-privadas, consorcios industriales y acuerdos de cooperación** en sectores clave como la tecnología, la construcción y la salud.

El ODS 17 y su relación con la ISO 44001

El **ODS 17** es uno de los **Objetivos de Desarrollo Sostenible** establecidos por las Naciones Unidas para promover el **desarrollo global sostenible**. Su enfoque principal es fortalecer la implementación de los ODS a través de **alianzas entre los gobiernos, el sector privado y la sociedad civil**. Este objetivo se basa en la premisa de que los **desafíos globales** como la pobreza, el cambio climático y la desigualdad solo pueden resolverse mediante una **cooperación sólida** entre múltiples actores a nivel local, nacional e internacional.



Certificación de la norma ISO 42001: proceso a seguir paso a paso

La **certificación de la norma ISO 42001** garantiza que la **gestión de sistemas de Inteligencia Artificial** de una organización es adecuada, eficiente y cumple con los estándares internacionales generalmente aceptados.

Obtener la certificación de la norma ISO 42001 es el proceso que **cierra la etapa de implementación e inicia el de mejora continua y mantenimiento del sistema de gestión**. La organización que certifica su **sistema de gestión ISO 42001** no necesita hacer nada más para demostrar que hace uso responsable, transparente, ético y legal de la nueva tecnología.

Por qué es importante obtener la certificación de la norma ISO 42001

La Inteligencia Artificial es uno de los mayores avances tecnológicos desarrollados, pero también ha generado polémica debido a las **connotaciones éticas, legales y sociales** que le son inherentes. A pesar de las reservas, lo cierto es que un número importante de organizaciones ya hace uso de productos, aplicaciones y sistemas de **Inteligencia Artificial** o bien se dedica a desarrollar esos productos.

Esas organizaciones **necesitan demostrar que gestionan con eficacia los riesgos** que implica el uso de Inteligencia Artificial. Por eso es tan importante obtener la certificación de la norma ISO 42001.

Un sistema certificado no tiene que explicar nada más. **La certificación es prueba indiscutible de que la organización se compromete con la ética**, la ley, con su comunidad y con sus empleados, haciendo un **uso responsable de la tecnología**.

¿Cómo se obtiene la certificación de la norma ISO 42001?

Una organización que decide afrontar la **auditoría de terceros** para obtener la certificación de la norma ISO 42001 habrá concluido su trabajo de planificación e implementación.

Es probable que ya haya efectuado incluso una o más auditorías internas para evaluar la eficacia y la conformidad de su sistema. Si la organización está lista, solo queda dar algunos **pasos para obtener la certificación**.



Cómo definir los objetivos y planes en ISO 45001

Definir objetivos y planes en ISO 45001 **es la clave de la eficacia del sistema, si la tarea se ha realizado correctamente.** De no ser así, la integridad y la **salud de los trabajadores** estará expuesta. Por eso, el cumplimiento de este requisito es crítico y esencial.

El propósito es definir **objetivos y planes en ISO 45001 inteligentes y estratégicos**, que contribuyan al bienestar de los trabajadores y que, a la vez, consideren las expectativas de las partes interesadas.

Qué tener en cuenta para definir objetivos y planes en ISO 45001

Definir objetivos y planes en ISO 45001 **es una solicitud de la norma que integra dos elementos:** por una parte, objetivos; por otra, medidas para cumplir esos objetivos. Se deduce que lo primero es definir aquello que se pretende lograr, el **alcance**, para después determinar la forma en la que se trabajará para llegar a la meta. Dos solicitudes con un vínculo estrecho, pero diferentes.

1. Definición de objetivos

La definición de objetivos y planes en ISO 45001 es una solicitud que se incorpora en la cláusula 6.2 del **estándar ISO 45001**. Lo primero que hay que tener claro sobre los objetivos es que estos deben ser inteligentes: **específicos, medibles, alcanzables y realistas**. Además, deben fijarse para que puedan alcanzarse en un periodo de tiempo definido.

Por otra parte, necesitan alinearse con lo propuesto en la **política de seguridad y salud en el trabajo**. Es importante recordar que en ese documento **la Alta Dirección puede establecer uno o varios grandes objetivos**. Los que se definen aquí son los objetivos de medio y corto plazo.

El gran objetivo, o los grandes objetivos, propuestos en la política suelen ser inamovibles. Por contra, **los objetivos que solicita la cláusula 6.2. necesitan revisión periódica**. Además, es importante tener en cuenta algunos aspectos esenciales:

- **Obligaciones de cumplimiento:** es necesario hacer un inventario de obligaciones de cumplimiento en el área de seguridad y salud en el trabajo. Pueden ser regulatorias, legales, locales, nacionales, internacionales, pero también contractuales o voluntarias. Su cumplimiento se debe considerar objetivo esencial.
- **Expectativas de las partes interesadas:** la primera entre las partes interesadas es la fuerza laboral, que incluye a **contratistas** o subcontratistas. Organismos reguladores, Alta Dirección, asociaciones de trabajadores, etc. pueden también tener intereses en los resultados del sistema de gestión.



8 peculiaridades de la ISO 42001 que debes conocer

ISO 42001

La **inteligencia artificial (IA)** está transformando industrias a nivel global, desde el sector financiero hasta la salud y la manufactura. Sin embargo, a medida que su adopción se expande, también crecen los desafíos en torno a la **ética, seguridad y transparencia** de estos sistemas. La **ISO 42001** se posiciona como un estándar en desarrollo que busca ofrecer un marco robusto para la gestión de la IA.

A lo largo del siguiente artículo, exploraremos las **características clave de ISO/IEC 42001**, lo que promete ser un punto de referencia esencial para las organizaciones que buscan implementar IA de manera **responsable, segura y efectiva**.

1. Gobernanza de la IA: Control y supervisión en ISO 42001

Uno de los aspectos fundamentales de este estándar es la **gobernanza de los sistemas de IA**. ISO IEC 42001 establece directrices para la creación de políticas que regulen el uso y control de la IA en las

organizaciones. Esto implica asegurar que la IA esté alineada con los valores, objetivos y estrategias de la empresa. La gobernanza también incluye la asignación de **responsabilidades** claras para supervisar el desarrollo, uso y mantenimiento de los sistemas.

¿Por qué es importante? Una sólida gobernanza permite evitar el uso inapropiado de la IA, garantizando que sus resultados sean coherentes con los principios éticos y los objetivos de negocio.

2. Ética y responsabilidad: IA con impacto positivo

La **ética** es un componente crucial en cualquier sistema de IA. Este estándar asegura que las organizaciones tengan en cuenta el impacto que la IA puede tener en los derechos humanos, la privacidad y la igualdad. Esto incluye medidas para evitar **discriminación, sesgo** y **prácticas injustas**.

La responsabilidad de los resultados generados por la IA es otra área crítica. ISO 42001 enfatiza la necesidad de **asignar responsabilidades claras** por las decisiones tomadas por sistemas automatizados, asegurando que las organizaciones se hagan cargo de los posibles errores o consecuencias imprevistas.

3. Seguridad y confiabilidad: Sistemas IA a prueba de fallos

La IA, al igual que cualquier otra tecnología, presenta riesgos en términos de seguridad. **ISO/IEC 42001** establece directrices claras para que los sistemas de IA sean **seguros, confiables** y **robustos**. Esto implica minimizar la posibilidad de ciberataques, errores en los algoritmos o fallos que puedan comprometer la integridad de los resultados.



Sistema de Gestión de Inteligencia Artificial (SGIA): definición y componentes clave

Un uso adecuado de la nueva tecnología permite a organizaciones de todos los sectores **disminuir costes, aumentar la productividad e impulsar la innovación**. Sin embargo, existen **riesgos** que es necesario afrontar. Esas amenazas trasgreden los límites definidos por el uso de la IA para abordar temas de privacidad de datos y seguridad de la información. El Sistema de Gestión de Inteligencia Artificial deja entonces de ser una opción para convertirse en una necesidad.

Uno de los objetivos del SGIA es **alcanzar un equilibrio adecuado entre los riesgos y los beneficios**. Sin embargo, esta tecnología no para de desarrollarse, los riesgos evolucionan con ella y es preciso contar con un marco de operación que garantice el uso ético, transparente, legal y responsable de la IA. Es ahí donde un Sistema de Gestión de Inteligencia Artificial cobra especial valor.

Por qué se desarrolló un estándar para el Sistema de Gestión de Inteligencia Artificial

ISO 42001 es el estándar internacional para **Sistemas de Gestión de Inteligencia Artificial**. Se desarrolló en colaboración con expertos reconocidos a nivel internacional y representantes de diferentes partes interesadas, entre ellas, organizaciones del sector de la tecnología, ONGs, organismos estatales, grupos comunitarios y legisladores.

ISO consideró necesario integrar un comité técnico de Alto Nivel que tuviera la capacidad para abordar las preocupaciones de la comunidad internacional en cuanto al uso de Inteligencia Artificial. Así **se desarrolló un estándar de gestión que sigue el ciclo PDCA** y que garantiza el **uso ético**, seguro, legal, responsable y transparente de la IA.

Componentes clave del Sistema de Gestión de Inteligencia Artificial

Un sistema de gestión **es un engranaje sincronizado y armónico de procesos que se han diseñado para cumplir unos requisitos**. Los requisitos, a su vez, buscan dar cumplimiento a lo que se expresa en unas políticas. Y las políticas se basan en objetivos que pretende alcanzar la Alta Dirección con la implementación del sistema de gestión.

Se entiende así que una de las razones que justifican la existencia del sistema de gestión es la necesidad de **alcanzar unos objetivos**.



Requisitos legales y reglamentarios en ISO 9001: cómo incluirlos en tu SGC

Los **requisitos legales y reglamentarios en ISO 9001** se incluyen en el **sistema de gestión de calidad** porque así **lo solicita la norma en su revisión del año 2015**. Las organizaciones que en aquel entonces trabajaban con una edición anterior tuvieron que adaptarse, con las lógicas dudas iniciales sobre la forma de cumplir con la nueva exigencia.

Esas dudas, que todavía pueden surgir, tienen que ver con la definición exacta de lo que son requisitos legales y reglamentarios en ISO 9001, con **los detalles normativos contenidos en el estándar** y la forma práctica de cumplir con la exigencia.

Cuáles son los requisitos legales y reglamentarios en ISO 9001

Los requisitos legales y reglamentarios en ISO 9001 solicitan a la organización hacer algo de una forma determinada o entregar un

servicio o producto que cumpla con unas características mínimas. El **requisito legal** tiene origen en una ley, una directiva, un decreto o una solicitud de un organismo regulador. Es, además, mucho más relevante en sectores de alta regulación, como son el farmacéutico, el sanitario o el alimentario.

Dentro de los requisitos legales y reglamentarios en ISO 9001 **no se incluyen los compromisos que asume la organización de forma voluntaria** o aquellos a los que se obliga mediante la firma de un contrato. No son requisitos legales porque no los exige una ley u otro tipo de mecanismo gubernamental o estatal con carácter legal.

Qué dice la norma sobre requisitos legales y reglamentarios en ISO 9001

Los requisitos legales y reglamentarios aparecen en **ISO 9001:2015** a la vez que los requisitos del cliente: **“los productos y servicios de la organización deben cumplir requisitos legales y los del cliente”**. Esto significa que la norma concede la misma importancia a lo que solicita la ley y a lo que esperan o quieren los clientes. Además, recoge los aspectos prácticos que es obligatorio tener en cuenta dentro del sistema de gestión de calidad:

- **Comprender las necesidades y expectativas** de las partes interesadas.
- **Comprender los requisitos** para garantizar la atención del cliente.
- **Determinar y revisar los requisitos** de los productos y servicios.



5 principales definiciones ISO 45001

Definiciones ISO 45001

La norma **ISO 45001** es el estándar internacional para la gestión de la **seguridad y salud en el trabajo (SST)**, cuyo objetivo es **prevenir accidentes laborales** y **promover el bienestar** de los empleados. Para comprender su implementación, es crucial familiarizarse con algunas de las principales **definiciones ISO 45001**. A continuación, destacamos los cinco conceptos más relevantes de la norma y su importancia en la creación de **entornos laborales más seguros**.

1. Sistema de Gestión de Seguridad y Salud en el Trabajo (SG-SST)

El **Sistema de Gestión de Seguridad y Salud en el Trabajo (SG-SST)** es el conjunto de **políticas, procedimientos y procesos** implementados en una organización para **garantizar la protección de los empleados**. Este sistema se enfoca en la identificación de riesgos, el establecimiento de controles y la mejora continua de la seguridad laboral.

La implementación de un **SG-SST** bajo la norma **ISO 45001** tiene como objetivo **reducir los accidentes, enfermedades** laborales y **asegurar el cumplimiento** legal en materia de seguridad.

El sistema de gestión incluye:

- **Políticas de seguridad** que establecen los compromisos de la empresa.
- **Evaluación de riesgos laborales** para identificar posibles peligros.
- **Controles preventivos** y correctivos para gestionar los riesgos.

2. Peligro

En el contexto de la norma **ISO 45001**, un **peligro** se refiere a cualquier **fuente, situación o acto que puede causar daño, enfermedad o lesión** a los empleados. Los peligros pueden ser físicos, químicos, biológicos, ergonómicos, entre otros. **Identificar y evaluar los peligros** es esencial para crear un entorno laboral seguro.

Algunos ejemplos incluyen:

- **Peligros físicos:** Maquinaria en mal estado o condiciones inadecuadas de trabajo.
- **Peligros químicos:** Exposición a sustancias tóxicas.



Como hacer auditoria interna ISO 45001

Como hacer auditoria interna ISO 45001

La **auditoría interna ISO 45001** es un proceso clave para asegurar que el Sistema de Gestión de Seguridad y Salud en el Trabajo (SG-SST) cumpla con los estándares internacionales y mantenga un ambiente laboral seguro. Si tu organización busca mejorar la seguridad de los trabajadores y cumplir con las normativas, realizar auditorías internas efectivas es esencial.

En este artículo, te enseñamos **cómo hacer auditoria interna ISO 45001** paso a paso, para que tu empresa cumpla a la vez que mejora continuamente su desempeño en salud y seguridad ocupacional.

La auditoría interna es un mecanismo de **autoevaluación** que permite a las organizaciones verificar si su **Sistema de Gestión de Seguridad y Salud en el Trabajo** cumple con los requisitos de la norma ISO 45001. Este proceso ayuda a identificar **áreas de mejora** y a prevenir riesgos laborales, asegurando que las prácticas y procesos estén alineados con los estándares de seguridad.

1. Planificación de la Auditoría Interna

El primer paso para una auditoría interna efectiva es la **planificación adecuada**. Aquí es donde se definen aspectos clave como el **alcance de la auditoría**, los objetivos y el equipo auditor.

Algunos elementos importantes incluyen:

- **Objetivo:** Evaluar el cumplimiento del SG-SST y su eficacia en la prevención de accidentes y enfermedades laborales.
- **Alcance:** Determinar qué áreas y procesos de la empresa se auditarán.
- **Frecuencia:** La norma ISO 45001 sugiere realizar auditorías periódicas; se recomienda al menos una vez al año.

2. Selección del Equipo Auditor

Es crucial que el **auditor interno** o el equipo auditor esté debidamente capacitado y que tenga **independencia** respecto a las áreas que van a auditar. Un equipo imparcial garantizará que los resultados sean confiables y objetivos.

3. Revisión de la Documentación del SG-SST

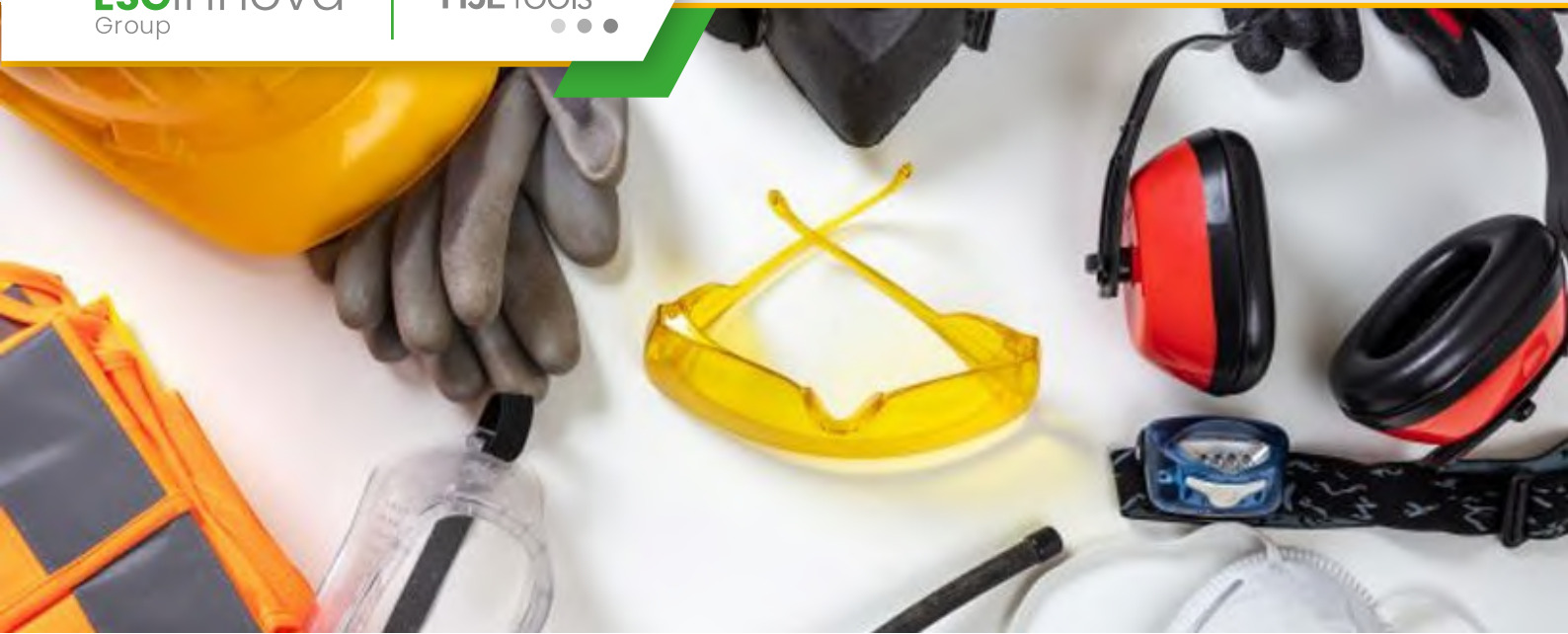
Antes de iniciar la auditoría, es necesario revisar toda la documentación relacionada con el SG-SST, incluyendo:

- **Políticas de seguridad y salud.**

HSETools



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



Buenas prácticas en la gestión de equipos de protección personal para optimizar el programa SST

Una **gestión de equipos de protección personal** efectiva es un elemento clave en el área SST de muchas organizaciones. Es, además, una tarea compleja porque cuando existe el compromiso y la obligación de garantizar la **salud y seguridad de los trabajadores** no es posible escatimar esfuerzos.

La gestión de equipos de protección personal se desarrolla día a día y **es un proceso cíclico**. Esto significa que, aunque se hayan asignado los equipos necesarios a todos los trabajadores de la organización, aún hay mucho que hacer.

En qué consiste la gestión de equipos de protección personal

La gestión de equipos de protección personal es un conjunto de procesos, procedimientos y tareas que se desarrollan con un objetivo claro: que **cada trabajador disponga y utilice equipos adecuados para la tarea que realizará** y que esos equipos reúnan las características de calidad mínimas para cumplir con su función. Esa función de los **EPPs** no es otra que **evitar que el trabajador resulte herido** o sufra consecuencias mayores a causa de un accidente. Por supuesto, también preservan la salud de los empleados de otro modo, ya que minimizan la exposición a agentes químicos, ruidos, exceso de luz o temperaturas altas o bajas en extremo. El uso de equipos de protección personal es responsabilidad del empleado. Proporcionar los equipos, exigir su uso e incluir la obligación en **políticas de empresa**, manuales o instrucciones de trabajo **es una responsabilidad del empleador**.

Qué se considera equipo de protección personal

Los equipos de protección personal son elementos diseñados y fabricados para proteger la integridad del trabajador y su salud ante el **riesgo que representa ejecutar una tarea determinada**. Los **riesgos laborales** pueden estar asociados a la manipulación de un material, a la altura, a las condiciones atmosféricas o climáticas o a la probabilidad de que se presente un accidente. El uniforme o las prendas de vestir habituales de un trabajador no son equipos de protección personal. De la misma forma, los EPPs no se utilizan en tareas, en situaciones o en actividades diferentes a las que representa el riesgo que minimizan o evitan.



¿Cuál es la Definición de Control en el Contexto Empresarial?

Definición de control

Nadie duda de la competencia tan feroz y los cambios son constantes a los que las organizaciones están expuestas. Es por ello que necesitan más instrumentos que aporten una visión clara para alcanzar el éxito. Requieren de herramientas y procesos que les permitan **monitorear, evaluar y ajustar su rumbo** continuamente. Para ello, el **control en el contexto empresarial**, se sitúa como una función esencial que asegura que la empresa avance en la dirección correcta, cumpliendo con sus **objetivos estratégicos** de manera eficiente.

A lo largo de las siguientes líneas nos gustaría hablar sobre la definición de control, un **concepto amplio** y **extremadamente útil**.

¿Qué es el control?

La definición de control en el ámbito empresarial es mucho más que un simple mecanismo de supervisión. Se entiende como el **proceso sistemático** mediante el cual una organización se asegura de que sus **actividades y recursos** están alineados con sus **objetivos previamente establecidos**. Este proceso involucra la **medición del desempeño**, la **comparación con estándares** previamente definidos y la **implementación de acciones correctivas** cuando sea necesario. En esencia, el control actúa como un **GPS corporativo**, orientando a la empresa y manteniéndola en el camino hacia el éxito.

Componentes clave del proceso de control

El proceso de definición de control empresarial se compone de varios elementos interconectados que garantizan su efectividad:

- 01. Establecimiento de estándares:** La base del control comienza con la definición de **estándares claros y medibles**. Estos estándares, que pueden estar relacionados con **costos, tiempos, calidad**, entre otros, sirven como punto de referencia para evaluar el desempeño de la organización.
- 02. Medición del desempeño:** Una vez establecidos los estándares, es crucial **medir el desempeño real**. Este paso implica recolectar **datos precisos** sobre las operaciones, procesos y resultados obtenidos.
- 03. Comparación con los estándares:** Con los datos en mano, el siguiente paso es **comparar el desempeño real** con los estándares definidos.



7 desafíos comunes en la gestión de contratistas

Colaborar con terceros ofrece numerosos beneficios a las organizaciones, entre ellos mayor flexibilidad en sus operaciones o ahorro de costes. Pero también implica algunos **desafíos que es necesario solventar para que esa relación sea fructífera y satisfactoria** para ambas partes. De ahí la necesidad de invertir en una adecuada y eficiente gestión de contratistas.

Desafíos habituales en la gestión de contratistas

Los desafíos suelen considerarse como obstáculos. Desde cierto punto de vista lo son, pero también son retos y, por ello, **oportunidades para mejorar y demostrar la capacidad de trabajo**. Desde ese enfoque, veamos cuáles son los siete retos que deben superar los encargados de la gestión de contratistas en una organización moderna y cómo una **herramienta tecnológica adecuada** puede ayudar en la tarea:

1. Cumplimiento legal y regulatorio

Los contratistas y los empleados directos de la empresa tienen aspectos en común. Sin embargo, también existe una brecha que los separa y en esa grieta están las leyes, las normas y las regulaciones. En temas como **seguridad y salud en el trabajo**, por ejemplo, no tiene por qué existir diferencia. En cambio, **en cuestiones salariales, laborales y contractuales**, las cosas son muy distintas. La organización necesita **conocer y monitorear todas las obligaciones de cumplimiento legales asociadas a su relación con contratistas**. Especial atención merece la vigilancia de un marco regulatorio y legal en constante evolución. La tecnología es un gran apoyo en ese sentido, puesto que herramientas como una plataforma especializada en la gestión de contratistas puede emitir notificaciones y alarmas.

2. Evaluación y selección de contratistas

Cuando una organización comienza un proyecto que requiere incorporar contratistas, aparecen con dos obstáculos: no contar con una base de datos verificada y no disponer de criterios y procesos de selección eficaces. Hay que tener en cuenta que **cada etapa de selección de contratistas se desarrolla como si fuera la primera vez que se realiza**. Tareas como revisar la experiencia, verificar calificaciones, comprobar capacidad y competencia e, incluso, indagaciones de debida diligencia pueden convertirse en un cuello de botella. Y, pese al esfuerzo y la buena voluntad, cabe la posibilidad de errar en la elección. De ahí la necesidad de **establecer procesos sistemáticos de evaluación e incorporación de contratistas**. A lo que habría que sumar la importancia de **conservar una base de datos y documentar todos los procesos de selección**.



Minería y Conservación del Medio Ambiente: Desafíos y Soluciones Integradas

Minería y Conservación del Medio Ambiente

La **minería** es una de las **actividades económicas más importantes** a nivel mundial, generando materias primas esenciales para diversas industrias. Sin embargo, también presenta **grandes retos en términos de sostenibilidad y conservación del medio ambiente**.

La explotación de recursos naturales puede tener un **impacto** significativo en los **ecosistemas**, la **biodiversidad** y las **comunidades** locales, lo que exige la implementación de **soluciones integradas** para equilibrar el desarrollo económico con la **protección ambiental**.

Desafíos ambientales en el sector

Deforestación y pérdida de biodiversidad

Uno de los principales impactos ambientales de la minería es la **deforestación**, que ocurre cuando se despejan grandes extensiones de terreno para la **explotación minera**. Esto lleva a la **pérdida** de **hábitats naturales** y la **disminución** de la **biodiversidad**, afectando a las especies que dependen de estos ecosistemas. La fragmentación de los hábitats puede hacer que ciertas especies se vean **amenazadas o desplazadas**, lo que genera **desequilibrios ecológicos** a largo plazo.

Contaminación del agua y suelos

La **contaminación del agua** es otro gran desafío en la minería. La descarga de productos químicos utilizados en el **procesamiento de minerales**, como el cianuro y el mercurio, puede afectar gravemente los cuerpos de agua cercanos, **poniendo en riesgo la vida acuática y el suministro de agua** potable para las comunidades locales. Además, el drenaje ácido de las minas, que ocurre cuando los minerales expuestos reaccionan con el agua y el oxígeno, puede causar **acidificación de suelos** y **contaminación de acuíferos subterráneos**.

Emisiones de gases de efecto invernadero

El proceso minero también está asociado con la **emisión de gases de efecto invernadero (GEI)**. La maquinaria pesada utilizada en las **operaciones y el consumo** energético necesario para la extracción y procesamiento de minerales contribuyen a la emisión de **CO₂** y otros gases nocivos.



10 Pasos clave a la hora de seleccionar un software HSE

Los encargados de **seleccionar un software HSE** en una organización buscan elegir una **herramienta tecnológica** que ofrezca soluciones, resuelva problemas y establezca una diferencia con respecto a la forma en la que se gestionan la protección del medio ambiente y la seguridad de los trabajadores.

Uno de los desafíos a los que se enfrentan los profesionales que deben seleccionar un software HSE es la **variada oferta de fabricantes y proveedores de soluciones informáticas** diseñadas para **automatizar la gestión**. Sus características y funcionalidades pueden ser muy diferentes, de ahí la importancia de elegir aquella herramienta que mejor se alinee con las necesidades de la organización.

Pasos para seleccionar un software HSE ideal para la organización

Los proyectos estratégicos en cualquier organización requieren planificación. Seleccionar un software HSE es, sin duda, un proyecto

estratégico para la empresa. La importancia y **el impacto que tendrá en todas las áreas justifica que se tome un tiempo para la planificación.** El proceso para seleccionar un software HSE que conduzca a la toma de la decisión más acertada para todos, incluidas las partes interesadas externas, **se desarrolla en 10 pasos.**

1. Crear un cronograma de actividades

Fijar un espacio de tiempo para **elegir la mejor solución** hace que el proyecto se materialice y que la persona encargada, o el equipo, entienda que hay una fecha límite. **El cronograma considera las diferentes etapas de investigación, depuración de proveedores, prueba** y los demás pasos que se mencionan a continuación.

2. Establecer el presupuesto

Seleccionar un software HSE es un proyecto que requiere el aval de la Alta Dirección. Si la tarea se hizo bien, ese órgano habrá fijado un presupuesto y habrá dispuesto los recursos. **Es importante fijar un presupuesto máximo, pero también uno mínimo.** Todo ello considerando que el mercado ofrece soluciones que, por su escaso valor, pueden no resultar de utilidad.

3. Identificar las necesidades de la organización

La gestión HSE involucra muchas áreas: gestión de documentos, de empleados, de **contratistas**, planes HSE, reportes de incidentes, investigaciones, etc. Quizá no todas son prioritarias para la organización. **Es posible que el proyecto haya sido concebido o aprobado, en términos financieros, para desarrollarse en escalas**, opción para la cual una solución modular resulta ideal.



Salud Ocupacional en la Minería: Claves para un Entorno Laboral Seguro

Salud ocupacional en la minería

La **salud ocupacional en la minería** es crucial para **garantizar la protección y el bienestar de los trabajadores** en un entorno que presenta numerosos **riesgos**. Las condiciones difíciles, como la exposición a polvo, ruido, vibraciones y sustancias tóxicas, requieren la **implementación de medidas de seguridad específicas**. A través de una **gestión efectiva de los riesgos laborales y la promoción de la salud**, las empresas mineras pueden no solo cumplir con las normativas vigentes, sino también crear un **ambiente laboral más seguro y productivo**.

El sector minero enfrenta **desafíos** únicos en términos de **condiciones laborales**, lo que convierte a la **salud ocupacional** en un tema crítico. Los trabajadores están expuestos a factores como el **polvo de sílice**, que puede causar enfermedades respiratorias crónicas, así como al **ruido extremo**, que puede provocar pérdida auditiva.

Además, el trabajo en zonas confinadas y con equipos pesados **incrementa el riesgo de lesiones**.

Implementar **controles efectivos** para mitigar estos riesgos, como el uso de **equipos de protección personal (EPP)** y la instalación de sistemas de ventilación adecuados, es fundamental para **prevenir problemas** de salud a largo plazo.

Entre las **enfermedades más comunes** en el sector minero se incluyen:

- **Neumoconiosis:** Causada por la inhalación de polvo de minerales, como el carbón o el sílice.
- **Pérdida auditiva inducida por ruido:** Resultado de la exposición constante a maquinaria ruidosa.
- **Estrés térmico:** El trabajo en condiciones de calor extremo puede causar agotamiento y deshidratación, lo que pone en riesgo la vida de los trabajadores.

Estas afecciones pueden **evitarse con la implementación** de programas de **salud ocupacional** enfocados en la **prevención y el monitoreo continuo** de los empleados.

Estrategias para mejorar la salud ocupacional en minería

Evaluación de riesgos laborales

Una de las primeras medidas para mejorar la **salud ocupacional** es realizar una **evaluación exhaustiva de riesgos** en el lugar de trabajo.



7 Consejos para elegir un Sistema de Gestión de Contratistas

Elegir un Sistema de Gestión de Contratistas es un proceso que necesita seguir un procedimiento minucioso, acorde con la complejidad del área que se va a automatizar. La abrumadora cantidad de **herramientas tecnológicas** disponibles para ello, así como las características y funcionalidades que necesita una organización para resolver sus problemas de gestión, agregan desafíos a la tarea.

Por otra parte, no hay que olvidar que **todas las empresas que trabajan con terceros no tienen las mismas necesidades**. Son elementos que deben valorar las personas encargadas de elegir un Sistema de Gestión de Contratistas para su organización.

Consejos para elegir un Sistema de Gestión de Contratistas

Un error frecuente en aquellas organizaciones que mantienen relaciones con contratistas es asumir que el mismo software que se

emplea en la gestión de los empleados funcionará para la **gestión de terceros**. En realidad, no suele ser así. Por ello, elegir un Sistema de Gestión de Contratistas adecuado es una buena decisión. Pero, **para acertar en la elección, es fundamental tener en cuenta algunos aspectos esenciales.**

1. Identificar las necesidades de gestión de la empresa

Las deficiencias en la gestión de contratistas o la ausencia de ella se muestran como problemas graves. **Una comunicación eficiente, gestión de documentos, supervisión y monitoreo del trabajo del contratista** o disponer de una base de datos de terceros actualizada son frentes de gestión que representan necesidades distintas. El primer paso para elegir un Sistema de Gestión de Contratistas pasa, de este modo, por identificar las necesidades específicas, **establecer los desafíos a los que hay que enfrentarse y elaborar un listado detallado.**

2. Pensar en el presente y en el futuro

Elegir un Sistema de Gestión de Contratistas que satisfaga las necesidades actuales de la organización es una buena idea, pero no siempre es suficiente. Lo ideal es optar por una **solución avanzada** que cubra también las necesidades que se puedan presentar en el futuro, sin tener que satisfacer los costes que eso supone desde un primer momento. La solución es contratar **un software modular y escalable**, basado en la nube. Con una herramienta de esas características, **la organización puede elegir lo que requiera en un momento concreto** y pagar solo por ello.



Implementar un software de gestión de incidentes y accidentes: 5 beneficios clave

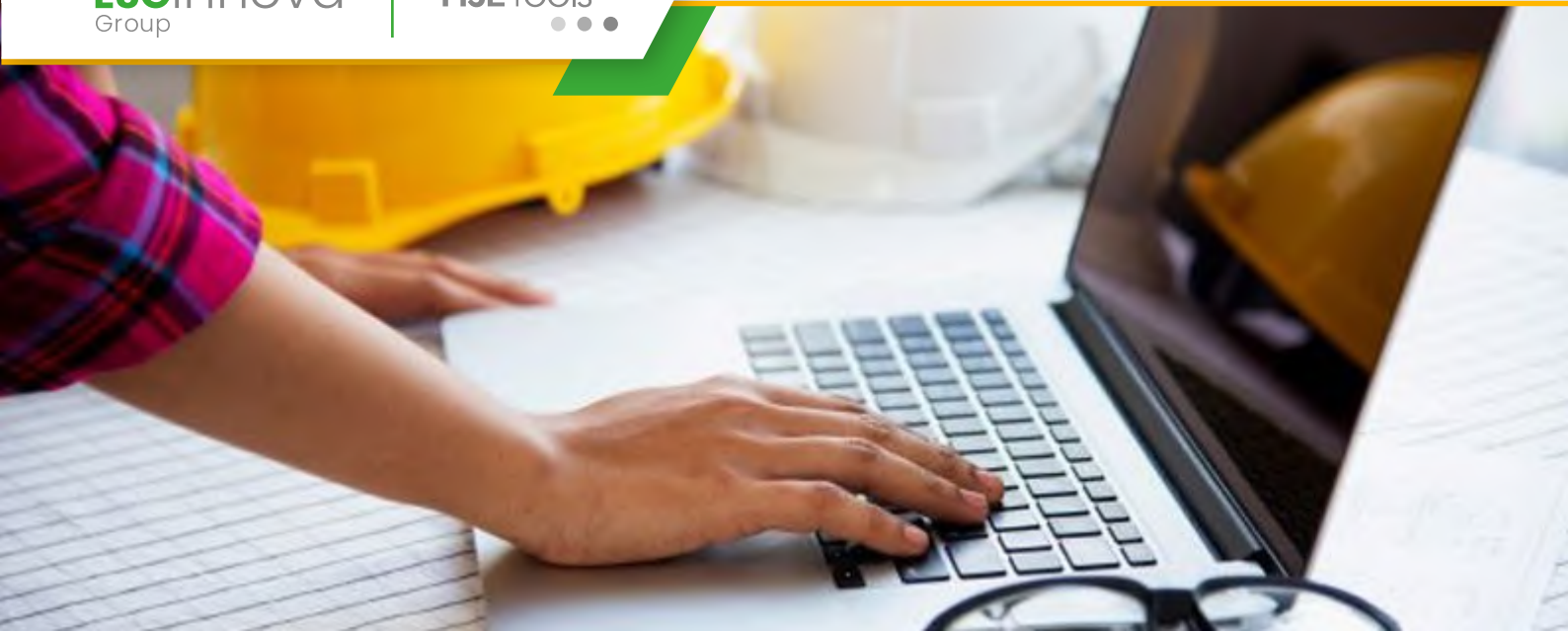
Un **software de gestión de incidentes y accidentes** contribuye a resolver uno de los grandes retos para el área de **Seguridad y Salud en el Trabajo**. Ese desafío son las dificultades que en ocasiones impiden que se notifiquen, con la inmediatez requerida, eventos que producen lesiones o pueden lesionar a los trabajadores. No es una cuestión menor: muchos **incidentes** no se notifican porque para ello es preciso seguir procedimientos burocráticos complejos que implican completar formularios en papel, elaborar informes y entregar la documentación en una oficina. Es un proceso que un software de gestión de incidentes y accidentes simplifica, con un primer beneficio para la Gestión SST: **los reportes de incidentes interrumpen un circuito que tiene un resultado inevitable: el accidente**. El software de gestión de incidentes y accidentes, **permite que la notificación se produzca casi de manera simultánea a los hechos** que lo motivan.

Esto evita que las personas pierdan esa iniciativa de informar que es tan importante, que olviden detalles esenciales o confundan la secuencia de los hechos, lo que suele suceder en los reportes extemporáneos en papel.

Qué es un software de gestión de incidentes y accidentes

El software de gestión de incidentes y accidentes es **una solución tecnológica diseñada para automatizar y digitalizar todo el proceso de reporte de eventos traumáticos** que afectan la **seguridad o la salud de los trabajadores**. Esta herramienta permite gestionar todo el ciclo de la eventualidad, desde su inicio hasta que se implemente una solución como resultado de una investigación previa. El uso de un software de gestión de incidentes y accidentes facilita, en primer lugar, que se pueda **informar del evento casi desde el mismo momento en que se produce**. Se puede hacer adjuntando información en archivos de audio, imágenes, vídeos, diagramas elaborados a mano sobre la marcha, etc.

El software inicia entonces un flujo de trabajo, alertando de forma automática a las personas indicadas, quienes inician el proceso de investigación, paso necesario para la resolución del problema. Durante todo el proceso se muestra el **avance de la gestión** y se producen notificaciones automáticas de acuerdo con el progreso de la tarea. Además de todo ello, **la documentación de cada investigación de incidentes y accidentes es almacenada de forma digital**, segura, en un repositorio central al que tienen acceso las personas autorizadas.



Gestión de contratistas digital: 5 beneficios para mejorar la sostenibilidad

Además de la mejora de la eficiencia, implementar un sistema de **gestión de contratistas digital** tiene un impacto positivo en los esfuerzos de sostenibilidad de las organizaciones. Sin embargo, y pese a los **beneficios ambientales** que ofrece, la **gestión digital de terceros** no se suele reconocer como un factor determinante en la mejora de la sostenibilidad.

Apesar de esa percepción, la gestión de contratistas digital **contribuye a mejorar los indicadores de sostenibilidad** en organizaciones de todos los sectores y todos los tamaños. Lo hace de formas muy diferentes que abordaremos a continuación.

Cómo contribuye la gestión de contratistas digital a mejorar la sostenibilidad

La gestión de contratistas digital ayuda a las organizaciones a **optimizar la relación con estos colaboradores estratégicos**. Esto es ya un motivo relevante para apostar por la automatización y **digitalización**. Pero hay otros beneficios para aquellas organizaciones que trabajan en mejorar sus indicadores de sostenibilidad:

1. Elimina el consumo de papel

Las relaciones y **el trabajo con terceros requiere una gran cantidad de documentos**: contratos, facturas, reportes de rendimiento, fichas para los trabajadores, resultados de evaluaciones, etc. Multiplicar este número de **documentos** por el de colaboradores bajo la modalidad de contratistas da una idea de las ingentes cantidades de papel que una organización puede llegar a consumir. **Con la gestión de contratistas digital desaparece la necesidad de utilizar papel en esos procesos**. Más allá del beneficio económico que supone, hay otro a nivel ambiental: ayudar a frenar la deforestación.

2. Reducción de consumo de energía

La gestión de contratistas digital implica un menor consumo de energía. La razón es que ya **no será preciso copiar, escanear o imprimir documentos**. La organización optimiza sus procesos al prescindir de dispositivos que consumen energía eléctrica, mejorando sus **indicadores de sostenibilidad**, y de paso, también los financieros.



¿Que son las charlas de 5 minutos?

Que son las charlas de 5 minutos

Las **charlas de 5 minutos**, un concepto que está muy de moda, pero, realmente, sabemos que son las charlas de 5 minutos. También conocidas como «5-minute safety talks», son **breves reuniones informativas** que se realizan en el lugar de trabajo para **mejorar la seguridad y concienciar** a los empleados sobre los **riesgos laborales**. Estas charlas se centran en temas clave de **seguridad, salud y prevención**, y están diseñadas para ser **concisas, directas y fáciles de aplicar**, ayudando a los trabajadores a **identificar riesgos y tomar medidas preventivas** de manera efectiva.

La característica más destacada de las **charlas de 5 minutos** es su **brevedad**. Al ser sesiones **cortas y enfocadas**, resultan **fáciles de integrar en la jornada** laboral sin interrumpir significativamente las actividades diarias. Este formato permite abordar **temas específicos** de seguridad de manera **clara y concisa**, manteniendo la atención de los empleados y reforzando su **compromiso con la prevención de riesgos**.

La clave de estas charlas es la **repetición periódica**, lo que ayuda a crear un **entorno laboral seguro** a través de la **concienciación continua** sobre posibles riesgos y la importancia de la prevención.

Una ventaja importante de las **charlas de 5 minutos** es su **flexibilidad**. Pueden abordar una **amplia gama de temas**, desde el uso correcto de **equipos de protección personal (EPP)** hasta la identificación de riesgos eléctricos o la ergonomía en el trabajo. Cada charla se adapta a las **necesidades específicas** del entorno laboral y los riesgos presentes en **cada área** de trabajo.

La **capacidad de personalización** asegura que los empleados reciban **información relevante para su puesto** y los riesgos que enfrentan en su día a día.

Estructura de las charlas de 5 minutos

Inicio de la charla

El **inicio de la charla** debe ser **claro y directo**, con una **breve explicación del tema** a tratar y su relevancia para el equipo. Es fundamental involucrar a los empleados desde el primer momento, **explicando cómo el tema impacta directamente** su **seguridad** y el **bienestar** general en el lugar de trabajo.

Explicación del riesgo o tema

Una vez introducido el tema, la charla debe enfocarse en la **explicación del riesgo o tema** central.



Cómo el software de cumplimiento ambiental puede ayudar a cumplir con las normativas

El **software de cumplimiento ambiental** aparece como respuesta a la necesidad que tienen las empresas de cumplir con un cúmulo de regulaciones, normativas, directivas, leyes y decretos en materia de **protección ambiental**.

La protección del medio ambiente y las acciones para detener el calentamiento global **son preocupaciones reales para la sociedad del siglo XXI**. El tema trasciende al ámbito político y se refleja en un aumento considerable de las obligaciones de cumplimiento para las empresas. **La carga reglamentaria recae en mayor proporción sobre las organizaciones**. Después de todo, son ellas las que mayor **impacto ambiental** causan. También son las que tienen mayores recursos y mejores argumentos para trabajar por la protección del planeta. Las empresas responden a ese compromiso, pero deben asumir mucho más.

El aumento de las obligaciones de cumplimiento ambiental implica **una considerable sobrecarga administrativa**. Es ahí donde un software de cumplimiento ambiental es de enorme valor.

Qué es un software de cumplimiento ambiental

El software de cumplimiento ambiental es una **solución tecnológica diseñada para automatizar un buen número de tareas** necesarias para cumplir con obligaciones ambientales y hacerlo de forma sistemática y transparente. El software de cumplimiento ambiental, además, **soluciona uno de los problemas más complejos que representa esta área: la volatilidad y el dinamismo de las reglas**. La solución tiene la capacidad para recoger información de diversas fuentes sobre obligaciones de cumplimiento ambiental o sobre su evolución y confrontarla con los permisos, licencias, auditorías, evaluaciones, indicadores o informes de **gestión ambiental**. Esta capacidad sirve para **establecer brechas de cumplimiento** y, en base a esa información, el software alerta a las personas indicadas para que puedan solventarlas. Para realizar su trabajo con la eficacia requerida, el software de cumplimiento ambiental **realiza varias operaciones autónomas**:

- **Recopilar documentos** e información.
- **Generar informes** que satisfacen las exigencias de los organismos reguladores.
- **Monitorea y revisa las actividades** de cumplimiento.
- **Emite alertas y notificaciones** automáticas.



5 Pasos para gestionar contratistas de forma eficaz

Gestionar contratistas de forma eficaz es un factor determinante para el éxito de muchas organizaciones. Aquellas que acuden a la **fuerza laboral subcontratada** lo hacen porque esta modalidad tiene para ellas un valor estratégico relevante.

Ese valor estratégico deja de existir si la empresa no encuentra los elementos necesarios para gestionar contratistas de forma eficaz. Tiene una explicación sencilla: solo una gestión eficiente hará que estén satisfechos. Además, hay que contar con **las condiciones de seguridad y salud en el trabajo**, que son un objetivo esencial en la relación con cualquier tipo de trabajadores.

Cómo gestionar contratistas de forma eficaz

La tarea de gestionar contratistas de forma eficaz, en cualquier área o en cualquier proyecto, cuenta con **una metodología que garantiza la efectividad** y, lo más importante, la mejora continua. Se trata del **ciclo PDCA** (planear, hacer, verificar y actuar, por sus iniciales en inglés). Ese método **lo diseñó Walter Shewarth**, ingeniero

norteamericano que lo aplicó en el proyecto de Control Estadístico de Procesos en los Estados Unidos. Sin embargo, fue el especialista en estadística William Edwards Deming quien lo popularizó, al aprovechar sus funcionalidades en trabajos de reconstrucción de Japón el siglo pasado. Ese es el motivo de que al ciclo PDCA se lo conozca como ciclo Deming. Esta breve introducción sirve para poner en contexto los **cinco pasos propuestos para gestionar contratistas de forma eficaz**, que se basan en cada una de las etapas del ciclo PDCA:

1. Planear

Gestionar contratistas de forma eficaz **implica una extensa y compleja etapa de planificación que se inicia con el diseño del proceso de selección y contratación**. Ese proceso debe actuar de manera sistemática para cada uno de los contratos en los que la organización decida **apoyarse en terceros**. En este proceso será importante **considerar qué tipo de tareas o proyectos requieren contratistas nuevos** y en cuáles es necesario acudir a una base de datos para elegir entre candidatos que ya tengan experiencia trabajando con la organización. La planificación también **identifica las áreas o las personas que intervendrán en el proceso para asignar recursos**, para capacitar o formar, para gestionar asuntos legales y contractuales o para vigilar el cumplimiento de las normas internas de la obligación y las directrices de **seguridad y salud en el trabajo**.

Finalmente, para completar la fase de planificación, es importante **definir cuál será la tarea específica de cada contratista**, qué maquinaria requerirá y si es preciso o no utilizar equipos de protección personal.



Arbol de Causas: Herramienta para la Mejora Continua

El **Arbol de Causas** es una herramienta ampliamente utilizada en la gestión de **seguridad y salud ocupacional** para identificar y analizar las **causas** de un incidente o accidente en el lugar de trabajo. A través de este enfoque, las empresas pueden comprender no solo el **evento principal**, sino también los factores subyacentes que lo desencadenaron. Este análisis permite implementar **acciones correctivas** y preventivas, mejorando la seguridad en el entorno laboral y contribuyendo a la **mejora continua**.

El **Árbol de Causas** es una técnica de análisis de incidentes que permite desglosar los **eventos previos y subyacentes** que llevaron a un accidente. Esta herramienta gráfica ayuda a **identificar conexiones causales**, organizando los hechos en una estructura jerárquica que va desde el **incidente principal** hasta sus causas básicas. Su principal objetivo es **identificar fallos** en el sistema o en los procedimientos que podrían haber sido **evitados**.

El análisis permite diferenciar entre dos **tipos de causas**:

- **Causas directas**: Son los factores inmediatos que desencadenaron el incidente.
- **Causas raíces**: Son los **factores subyacentes** que, si se hubieran abordado adecuadamente, habrían evitado que se produjera el incidente.

Pasos para realizar un análisis del Arbol de Causas

Recopilación de información

El primer paso para utilizar el **Árbol de Causas** es **recopilar información** sobre el incidente. Esto incluye entrevistas con los involucrados, revisión de informes de seguridad, análisis de datos históricos y observación directa. Es crucial tener una **comprensión detallada** de los **hechos** para construir un **análisis preciso**.

Identificación del evento principal

El siguiente paso es **identificar** el **evento principal** o el **accidente** en sí. Esto implica definir **qué incidente se analizará**, como una caída de un trabajador, un fallo en una maquinaria o una exposición a sustancias peligrosas. El incidente debe estar claramente descrito para **comenzar a desglosar las causas**.

Análisis de las causas directas

Con el evento principal definido, el siguiente paso es **identificar** las **causas directas**.



¿Que se conoce como gestión ambiental?

Que se conoce como gestión ambiental

La **gestión ambiental** es un concepto clave en el ámbito empresarial y gubernamental, especialmente en un mundo cada vez más enfocado en la sostenibilidad. Se trata de un **Plan de Acción dentro de las Políticas HSE** que busca minimizar los impactos negativos de las actividades humanas sobre el medio ambiente, al mismo tiempo que se optimiza el uso de recursos naturales. Pero, ¿en qué consiste realmente y por qué es tan relevante en la actualidad?

La gestión ambiental es el **conjunto de prácticas y políticas** que una organización implementa para controlar y reducir los efectos adversos que sus operaciones pueden tener sobre el medio ambiente. Esto incluye desde la reducción de emisiones de carbono hasta la optimización del uso de agua y energía. Es una herramienta que no solo promueve el desarrollo sostenible, sino que también mejora la eficiencia y la reputación de las empresas.

¿Por qué es importante la gestión ambiental?

Hoy en día, la conciencia sobre el cambio climático y la pérdida de biodiversidad ha puesto a la gestión ambiental en el centro de las agendas globales. **Las empresas que adoptan buenas prácticas ambientales no solo protegen el planeta, sino que también obtienen beneficios significativos**, tales como:

- **Cumplimiento legal:** Las regulaciones ambientales son cada vez más estrictas. Adoptar un sistema de gestión ambiental como la norma **ISO 14001** permite a las empresas asegurar que cumplen con las normativas vigentes.
- **Mejora de la reputación:** Los consumidores prefieren apoyar marcas responsables. Un enfoque sostenible puede incrementar la **confianza** y **fidelidad** del cliente.
- **Reducción de costos:** Optimizar el uso de recursos naturales, como el agua y la energía, puede disminuir los costos operativos, haciendo a la empresa más competitiva.

Componentes clave de una gestión efectiva

Una gestión ambiental eficiente debe basarse en varios componentes estratégicos:

- **Evaluación del impacto ambiental:** Antes de realizar cualquier actividad, es crucial evaluar sus posibles efectos en el medio ambiente. Esto permite identificar riesgos y tomar medidas preventivas.

GRCTools



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



Cómo Fortalecer la Transparencia Corporativa con el Software GRC

Transparencia Corporativa

En un entorno empresarial cada vez más complejo y regulado, la **transparencia corporativa** se ha convertido en un **pilar** fundamental para el **éxito y la sostenibilidad** de las organizaciones. La transparencia no solo **fortalece la confianza** entre los accionistas, empleados y clientes, sino que también **ayuda a las empresas a cumplir con las regulaciones y a prevenir fraudes y malas prácticas**.

La **transparencia corporativa** se refiere a la **claridad y apertura** con la que una empresa **comunica sus operaciones, decisiones y políticas** a sus accionistas, empleados, clientes y al público en general. Implica la **divulgación completa y precisa de la información financiera**, las prácticas de gobierno corporativo, los riesgos y cualquier otro dato relevante que pueda **afectar la percepción y las decisiones** de los stakeholders.

La relevancia de la **transparencia corporativa** radica en su capacidad para:

- **Fortalecer la confianza:** Las empresas transparentes tienden a ganar más confianza por parte de los inversores, empleados y clientes, lo que puede mejorar la lealtad y las relaciones a largo plazo.
- **Prevenir fraudes y malas prácticas:** La transparencia obliga a la organización a mantener estándares éticos altos, reduciendo el riesgo de fraudes y otras prácticas ilegales.
- **Cumplir con las regulaciones:** Las leyes y normativas modernas requieren altos niveles de transparencia en la gestión empresarial, y el incumplimiento puede llevar a sanciones severas.

Elementos Clave de la Transparencia Corporativa

Los elementos clave de la **transparencia corporativa** incluyen:

- **Divulgación financiera:** Información clara y precisa sobre el desempeño financiero de la empresa.
- **Gobernanza y estructuras de control:** Claridad sobre cómo se toman las decisiones dentro de la organización y qué mecanismos existen para garantizar la responsabilidad.
- **Gestión de riesgos:** Transparencia en cómo la empresa identifica, gestiona y comunica los riesgos a los que está expuesta.
- **Ética y cumplimiento normativo:** Divulgación de las políticas de ética, cumplimiento normativo y cómo se implementan y monitorean.



La Importancia de la Gestión Estratégica en Startups y PYMEs

Gestión Estratégica en Startups y PYMEs

Las **Startups** y **PYMEs** (Pequeñas y Medianas Empresas) enfrentan desafíos únicos por su condición y circunstancias. La competencia es feroz, los recursos son limitados y el entorno cambia rápidamente. En este contexto, la **gestión estratégica** en Startups y PYMEs se convierte en un pilar fundamental para asegurar la **supervivencia** y el **éxito sostenido** de estas organizaciones.

Visión y dirección: El punto de partida

Toda empresa exitosa comienza con una **visión clara**. La gestión estratégica en Startups y PYMEs ayudan a definir una misión y visión no solo a modo de formalismo; sería, pues, la brújula que guía cada decisión. Una visión bien articulada alinea al equipo con un **propósito común** y establece un marco para la **toma de decisiones coherente** con los objetivos a largo plazo.

Es la diferencia entre avanzar con rumbo firme o deambular sin dirección.

Adaptabilidad: Clave en un entorno cambiante

El mundo de los negocios es dinámico, especialmente para las Startups y PYMEs, que operan en mercados donde las **tendencias cambian rápidamente** y las innovaciones tecnológicas pueden redefinir industrias enteras de la noche a la mañana. La gestión estratégica permite a estas empresas ser más **adaptables y flexibles**. Al realizar un análisis constante del entorno, las empresas pueden **anticiparse a los cambios y ajustar su estrategia de manera proactiva**, aumentando así sus probabilidades de éxito.

Competitividad y diferenciación: Destacarse en el mercado

En un mercado saturado, diferenciarse es crucial. Una estrategia bien definida ayuda a las Startups y PYMEs a identificar y explotar sus **ventajas competitivas**. Ya sea descubriendo un nicho de mercado inexplorado o desarrollando productos y servicios únicos, la gestión estratégica les permite destacarse y construir una **marca sólida** que resuene con los clientes.

Eficiencia en el uso de recursos

Para las Startups y PYMEs, los recursos son valiosos y, a menudo, **limitados**. Aquí es donde la gestión estratégica juega un papel vital. A través de una **planificación estratégica**, estas empresas pueden priorizar sus inversiones y esfuerzos en áreas que ofrezcan el **mayor retorno**.



El rol del GRC en la prevención de ataques internos

En el mundo digital actual, **la ciberseguridad se ha convertido en una prioridad para las empresas** que desean proteger sus datos, reputación y competitividad. Uno de los aspectos más críticos dentro de este ámbito es la prevención de ataques internos, los cuales pueden ser devastadores para cualquier organización.

En este contexto, la gestión de riesgos y cumplimiento (GRC, por sus siglas en inglés) desempeña un papel fundamental. Este artículo **explora cómo el GRC puede ayudar a prevenir estos ataques internos** y fortalecer la ciberseguridad empresarial.

¿Qué es el GRC y por qué es importante?

El término GRC se refiere a un **enfoque integrado para la Gestión de la seguridad de la información**, riesgos y cumplimiento normativo en las organizaciones.

Este enfoque no solo abarca la implementación de medidas de seguridad, sino también la creación de una cultura corporativa que promueva la vigilancia constante y el cumplimiento de las normativas vigentes.

Las amenazas internas y su impacto en la ciberseguridad

Las amenazas internas son aquellas que provienen de dentro de la organización, ya sea de empleados actuales, ex empleados, contratistas o socios comerciales. Estas **amenazas pueden ser intencionales**, como el robo de datos, o no intencionales, como errores humanos que comprometen la seguridad de la información.

El impacto de estas amenazas puede ser significativo, **afectando no solo los datos confidenciales** sino también la reputación y la operatividad de la empresa.

Tipos de amenazas internas

- **Malintencionadas:** Empleados que deliberadamente buscan causar daño, como el robo de propiedad intelectual.
- **Accidentales:** Errores humanos, como enviar información sensible a la persona equivocada.
- **Negligentes:** Falta de cumplimiento de las políticas de seguridad, como el uso de contraseñas débiles.



Gestión de Riesgos Asociados a la Privacidad de Datos

En un entorno empresarial cada vez más digitalizado, la **privacidad de datos** se ha convertido en un aspecto crítico para todas las organizaciones. La exposición a riesgos asociados con la privacidad de datos puede tener consecuencias graves, incluyendo sanciones legales, pérdida de confianza por parte de los clientes y daño a la reputación. En este contexto, la **Gestión Integral de Riesgos** desempeña un papel esencial para prevenir y mitigar los impactos negativos relacionados con la privacidad de datos.

¿Qué son los riesgos asociados a la privacidad de datos?

Los **riesgos asociados a la privacidad de datos** se refieren a las posibles amenazas que pueden comprometer la integridad, confidencialidad y disponibilidad de la información personal que maneja una empresa. Estos riesgos incluyen, pero no se limitan a:

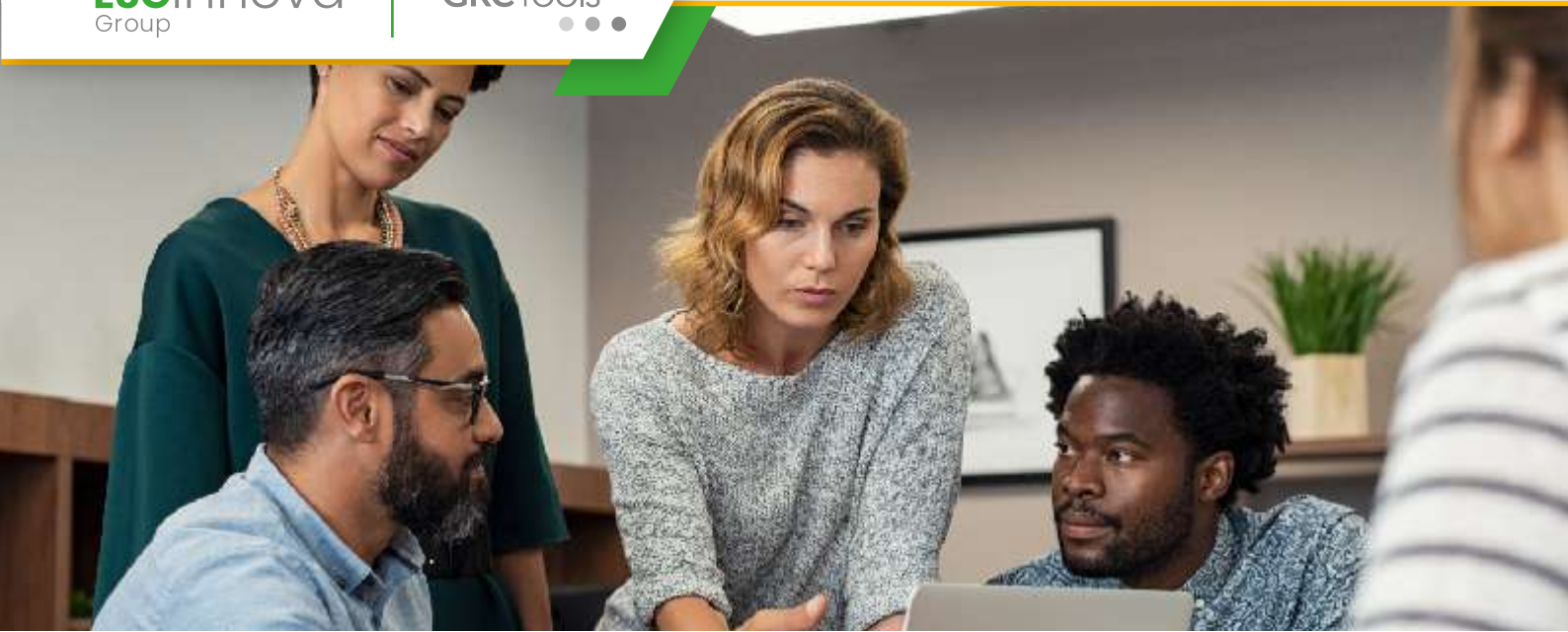
- **Riesgos de seguridad de la información:** Pérdida o robo de datos personales debido a fallos en la seguridad de los sistemas.

- **Riesgos de ciberseguridad:** Ataques cibernéticos como malware, phishing o ransomware que ponen en peligro la privacidad de la información.
- **Riesgos de compliance:** Incumplimiento de regulaciones como el RGPD, que puede resultar en sanciones severas.
- **Riesgos de terceros:** Fallos en la gestión de datos por parte de proveedores o socios comerciales que manejan información sensible en nombre de la empresa.

Importancia de la gestión integral de riesgos en la privacidad de datos

Implementar una **Gestión Integral de Riesgos** eficaz es crucial para proteger la privacidad de los datos en un entorno corporativo. Este enfoque permite a las empresas:

- ❖ **Identificar y evaluar riesgos:** Determinar cuáles son los riesgos más relevantes para la organización y priorizarlos según su probabilidad e impacto.
- ❖ **Mitigar riesgos:** Implementar controles y medidas preventivas que reduzcan la probabilidad de que ocurran incidentes relacionados con la privacidad de datos.
- ❖ **Cumplir con normativas:** Garantizar que la organización cumpla con todas las leyes y regulaciones aplicables, evitando sanciones y preservando la reputación corporativa.



Tendencias Actuales en la Gestión Estratégica

Gestión Estratégica

La **gestión estratégica** se ha convertido en un proceso vital para la supervivencia y el crecimiento de las empresas. Ya no basta con tener un plan a largo plazo; las organizaciones deben adaptarse constantemente a los **cambios tecnológicos, económicos y sociales**. En el siguiente texto puedes encontrar un análisis exhaustivo de las tendencias más importantes en la gestión estratégica que están marcando el rumbo de las organizaciones a nivel global.

1. Transformación Digital: El motor del cambio empresarial

El avance de la **inteligencia artificial (IA)**, el **big data** y la **automatización** ha cambiado las reglas del juego. Las empresas que han logrado integrar estas tecnologías en sus procesos están disfrutando de una mayor **eficiencia operativa** y una capacidad de respuesta más rápida a las demandas del mercado.

Por ejemplo, la IA permite analizar grandes volúmenes de datos en tiempo real, lo que proporciona a los líderes información precisa y oportuna para la toma de decisiones estratégicas.

Además, el surgimiento de **nuevas plataformas digitales** ha permitido a las empresas optimizar la experiencia del cliente y reducir los costos operativos. Estudios recientes indican que las organizaciones con una fuerte estrategia digital tienen un 50% más de probabilidad de superar a sus competidores en **crecimiento y rentabilidad**.

2. Sostenibilidad y Responsabilidad Social Corporativa (RSC): Un imperativo estratégico

Las empresas se están viendo obligadas a adoptar **prácticas más responsables** para reducir su impacto ambiental y contribuir positivamente a la sociedad. La gestión estratégica en este ámbito se traduce en la integración de principios sostenibles en toda la cadena de valor: desde la producción y el transporte hasta la gestión de residuos.

Un ejemplo notable es el aumento de la **economía circular**, un modelo que busca reducir el desperdicio al reutilizar recursos en la mayor medida posible.

Empresas líderes como **IKEA** y **Patagonia** ya están aplicando estos principios en sus operaciones. Además, la creciente demanda de **inversores responsables** está obligando a las empresas a demostrar su compromiso con los **Objetivos de Desarrollo Sostenible (ODS)**.



Estrategias efectivas para mitigar los riesgos operacionales en el entorno empresarial actual

En el mundo empresarial actual, la capacidad de una empresa para gestionar eficazmente sus **riesgos operacionales** marca la diferencia entre el éxito y el fracaso. Los riesgos operacionales son aquellos que surgen del funcionamiento diario de una empresa y pueden afectar su eficiencia, productividad e incluso su supervivencia. Estos riesgos pueden incluir desde fallos en los procesos internos, hasta problemas con la tecnología, errores humanos o interrupciones en la cadena de suministro.

En este post, veremos las estrategias más efectivas para mitigar los **riesgos operacionales** y cómo una **Gestión Integral de Riesgos** bien implementada puede ayudar a las empresas a mantenerse resilientes en un entorno cada vez más complejo.

¿Qué son los riesgos operacionales?

Los **riesgos operacionales** son aquellos riesgos que se derivan de las operaciones diarias de una empresa. Estos riesgos pueden estar relacionados con los procesos internos, la tecnología, el personal, los sistemas o eventos externos que afectan la capacidad de la empresa para operar de manera eficiente y cumplir con sus objetivos. Algunos ejemplos comunes incluyen:

- **Fallos en los sistemas tecnológicos:** Problemas con software o hardware que interrumpen las operaciones.
- **Errores humanos:** Decisiones equivocadas o acciones inadecuadas por parte del personal.
- **Problemas en la cadena de suministro:** Interrupciones o retrasos en la entrega de materiales o productos.
- **Desastres naturales:** Eventos inesperados como terremotos o inundaciones que afectan las instalaciones o los recursos.

Importancia de mitigar los riesgos operacionales

Mitigar los **riesgos operacionales** es fundamental para garantizar la continuidad del negocio. Un fallo en la gestión de estos riesgos puede resultar en pérdidas financieras significativas, daños a la reputación e incluso la quiebra de la empresa. Implementar una **Gestión Integral de Riesgos** permite a las organizaciones identificar, evaluar y mitigar estos riesgos de manera proactiva, reduciendo su impacto y asegurando que la empresa pueda seguir operando incluso en situaciones adversas.



Estrategias de Economía Circular con el apoyo de GRCTools

Estrategias de Economía Circular

Las **estrategias de economía circular** se han convertido en un pilar fundamental para garantizar la **sostenibilidad y el uso eficiente de los recursos**. En lugar del enfoque tradicional de producción y consumo lineal (extraer, producir, desechar), la economía circular propone un **modelo más regenerativo y eficiente**, donde los productos y materiales se mantienen en uso el mayor tiempo posible, **reduciendo los residuos** y el impacto ambiental.

La **economía circular** se basa en tres principios fundamentales:

- 01. Eliminar residuos y contaminación** desde el diseño de los productos.
- 02. Mantener productos y materiales en uso** durante el mayor tiempo posible.

03. Regenerar sistemas naturales, devolviendo recursos al ecosistema.

Este modelo no solo busca **reducir el impacto ambiental**, sino también optimizar la eficiencia de los **recursos a lo largo del ciclo de vida** de los productos. Al aplicar estos principios, las empresas pueden crear **sistemas más sostenibles** que beneficien tanto a la sociedad como al medioambiente.

Economía circular vs. economía lineal

En el modelo tradicional de **economía lineal**, los productos **siguen un ciclo de vida corto** que involucra la **extracción de materias primas**, la producción, el consumo y el descarte. Este modelo **no es sostenible a largo plazo** debido al agotamiento de los recursos y a la acumulación de residuos.

La **economía circular**, por el contrario, adopta un enfoque de «**cierre de ciclo**» donde los productos, componentes y materiales se **reciclan, reutilizan o se rediseñan** para **evitar el desperdicio**. Este enfoque no solo conserva los recursos naturales, sino que también **genera valor económico** a partir de los residuos.

Estrategias para implementar la economía circular en las empresas

- Rediseño de productos

Una de las primeras estrategias clave para adoptar la **economía circular** es el **rediseño de productos**. Este enfoque se centra en diseñar productos que sean **duraderos, reparables, reutilizables y reciclables**.

COMPLIANCE



Transformación Digital del Compliance: Cómo GRCTools Establece Nuevos Estándares

Transformación Digital del Compliance

La **transformación digital** ha traído consigo una evolución acelerada en muchos sectores, y el **compliance** no es una excepción. Las exigencias regulatorias, cada vez más complejas y diversas, han llevado a las organizaciones a buscar soluciones tecnológicas que optimicen sus procesos de cumplimiento normativo.

En este contexto, las plataformas de **Governance, Risk, and Compliance (GRC)** han ganado relevancia, y una de las herramientas que se ha posicionado como líder es **GRCTools**. Quédate con nosotros para explorar cómo esta solución está marcando un nuevo estándar en la transformación digital del compliance.

El desafío del Compliance en la era digital

El cumplimiento normativo es un **pilar crítico en la estructura de cualquier empresa**, especialmente en sectores altamente regulados como el financiero, el de la salud o el energético. A medida que las leyes se vuelven más complejas, las organizaciones deben asegurar que sus políticas, procedimientos y actividades cumplan con estas regulaciones. La transformación digital del compliance consiste en **aprovechar la tecnología para automatizar, simplificar y mejorar estos procesos**.

Tradicionalmente, la gestión del compliance ha estado plagada de ineficiencias debido a la dependencia de procesos manuales, hojas de cálculo y controles fragmentados. Sin embargo, la digitalización ha permitido automatizar tareas repetitivas, y ha brindado nuevas oportunidades para mejorar la **gestión de riesgos** y la **trazabilidad**.

GRCTools: Innovación en la gestión de GRC

GRCTools es una plataforma integral de gestión de **Governance, Risk, and Compliance (GRC)** que ha revolucionado la forma en que las empresas abordan sus procesos de cumplimiento. Esta solución tecnológica no solo simplifica el cumplimiento normativo, sino que también establece un estándar más alto en términos de eficiencia, escalabilidad y adaptabilidad a nuevas normativas.

Automatización y eficiencia

Uno de los mayores beneficios de GRCTools es su capacidad para **automatizar procesos clave**.



Optimización de la respuesta a incidentes de ciberseguridad con GRC

En el mundo digital actual, **la ciberseguridad es un aspecto crítico para cualquier organización**. No solo protege los datos sensibles, sino que también salvaguarda la reputación y la competitividad de una empresa. La gestión de incidentes de ciberseguridad se ha convertido en una prioridad para las empresas, y es aquí donde entra en juego el software GRC (Governance, Risk Management, and Compliance).

En este artículo, exploraremos **cómo optimizar la respuesta a incidentes de ciberseguridad utilizando herramientas GRC** y cómo estas pueden mejorar la eficacia de la gestión de riesgos en tu organización.

¿Qué es la ciberseguridad y por qué es importante?

La ciberseguridad **se refiere a la protección de sistemas, redes y datos** en el entorno digital contra ataques, daños o accesos no autorizados.

La importancia de **la ciberseguridad radica en su capacidad para proteger información sensible**, garantizar la continuidad del negocio, mantener la confianza de los clientes y socios, y cumplir con normativas y estándares de seguridad. Implementar una estrategia de ciberseguridad eficaz es esencial para mitigar riesgos y responder adecuadamente a incidentes de seguridad.

Gestión de la seguridad de la información

La **gestión de la seguridad de la información es un componente clave de la ciberseguridad**. Involucra la identificación, evaluación y mitigación de riesgos relacionados con la información. Esto incluye la implementación de políticas y procedimientos que aseguren la confidencialidad, integridad y disponibilidad de la información.

Una gestión efectiva de la seguridad de la información reduce riesgos mediante la identificación y mitigación de vulnerabilidades antes de que sean explotadas.

Además, **asegura el cumplimiento normativo al alinearse con regulaciones y estándares internacionales**, mejora la reputación al fortalecer la confianza de clientes y socios comerciales, y garantiza la continuidad del negocio al prepararse para responder y recuperarse rápidamente de incidentes de seguridad.



Pasos de la Gestión Estratégica: Guía completa para empresas

Gestión Estratégica

La **gestión estratégica** es el motor que impulsa el éxito a largo plazo de cualquier organización. En un entorno empresarial cada vez más competitivo y en constante cambio, contar con un plan estratégico sólido es esencial para **alcanzar los objetivos** y **adaptarse al mercado**. En este artículo, te presentamos los pasos clave para llevar a cabo una gestión estratégica efectiva, desde la **planificación** hasta la **evaluación continua**.

1. Definir la visión y misión de la empresa

El primer paso en la gestión estratégica es clarificar hacia dónde quieres llevar tu negocio. La **visión** es la imagen a largo plazo de lo que la empresa aspira a ser, mientras que la **misión** describe el propósito actual de la organización, respondiendo a preguntas como:

- ¿Qué hacemos?
- ¿Por qué lo hacemos?
- ¿Para quién lo hacemos?

Un buen ejemplo de una misión poderosa podría ser: «Nuestra misión es **proporcionar soluciones tecnológicas innovadoras** que transformen la manera en que las empresas gestionan sus recursos». Esta declaración no solo guía la estrategia, sino que también inspira a todo el equipo.

2. Análisis FODA: Conoce tu entorno

Antes de desarrollar cualquier estrategia, es crucial entender tanto el contexto externo como el interno de tu organización. El **Análisis FODA** (Fortalezas, Oportunidades, Debilidades y Amenazas) es una herramienta indispensable en este proceso.

- **Fortalezas y debilidades:** ¿En qué destaca tu empresa? ¿Dónde están las áreas de mejora?
- **Oportunidades y amenazas:** ¿Qué tendencias del mercado puedes aprovechar? ¿Qué riesgos debes mitigar?

Este análisis te dará una visión clara de **dónde estás** y **qué necesitas mejorar** para ser más competitivo.



Protección contra ataques de ransomware mediante GRC

La **ciberseguridad** se ha convertido en una prioridad esencial para las empresas que buscan proteger sus datos, mantener su reputación y asegurar su competitividad en un entorno digital cada vez más hostil.

Uno de los **mayores desafíos actuales es la protección contra ataques de ransomware**, que pueden paralizar las operaciones y resultar en pérdidas financieras significativas. Aquí es donde entra en juego el software GRC (Governance, Risk, and Compliance), una herramienta poderosa para gestionar y mitigar estos riesgos.

¿Qué es el ransomware y cómo afecta a las empresas?

El ransomware es un tipo de **malware que cifra los archivos de la víctima** y exige un rescate a cambio de la clave de descifrado. Este tipo de ataque puede tener consecuencias devastadoras para las empresas, desde la pérdida de datos críticos hasta la interrupción de operaciones y daños reputacionales.

Importancia de la ciberseguridad en la protección contra ransomware

La ciberseguridad **es crucial para defenderse contra el ransomware** y otros tipos de amenazas cibernéticas. Un enfoque integral de ciberseguridad incluye la implementación de políticas y prácticas robustas para prevenir, detectar y responder a incidentes de seguridad.

Aquí es donde el software GRC puede desempeñar un papel fundamental, proporcionando una **plataforma centralizada para gestionar todos los aspectos de la ciberseguridad** de una empresa.

Beneficios del uso de software GRC en ciberseguridad

El software GRC ofrece una serie de beneficios clave para la ciberseguridad empresarial, incluyendo:

- **Centralización de la gestión de riesgos:** Permite a las empresas gestionar todos sus riesgos desde una única plataforma, facilitando la identificación y mitigación de vulnerabilidades.
- **Cumplimiento normativo:** Ayuda a las empresas a cumplir con las normativas de ciberseguridad, evitando sanciones y protegiendo su reputación.
- **Automatización de procesos:** Reduce la carga de trabajo manual, permitiendo a los equipos de seguridad centrarse en tareas críticas.
- **Monitorización continua:** Proporciona una visión en tiempo real del estado de la seguridad.



La importancia de la gestión de riesgos de terceros en la cadena de suministro

En el mundo empresarial actual, la cadena de suministro se ha vuelto cada vez más compleja y globalizada. Con esta complejidad, surge una nueva serie de desafíos, especialmente en lo que respecta a la **gestión de riesgos de terceros**. Estos riesgos pueden tener un impacto significativo en la operación, reputación y rentabilidad de una empresa.

A continuación, explicaremos por qué es crucial gestionar los riesgos asociados a los terceros en la cadena de suministro y cómo una **Gestión Integral de Riesgos** puede ayudar a las empresas a mitigar estos riesgos de manera efectiva.

¿Qué son los riesgos de terceros en la cadena de suministro?

Los **riesgos de terceros** en la cadena de suministro se refieren a los riesgos que surgen del uso de proveedores, subcontratistas y otros socios comerciales. Estos riesgos pueden incluir problemas de calidad, interrupciones en el suministro, incumplimiento de normativas y riesgos financieros. También incluyen otros desafíos que podrían afectar la capacidad de una empresa para operar de manera eficiente.

Tipos de riesgos de terceros

- 01. Riesgos de cumplimiento normativo:** Los proveedores o subcontratistas que no cumplen con las normativas locales o internacionales exponen a la empresa a sanciones legales y daños a la reputación.
- 02. Riesgos financieros:** La insolvencia de un proveedor clave puede interrumpir la cadena de suministro y afectar la producción.
- 03. Riesgos de calidad:** Productos o servicios de baja calidad suministrados por terceros pueden perjudicar la reputación de la empresa y generar costos adicionales.
- 04. Riesgos de ciberseguridad:** Los proveedores que manejan datos sensibles pero no cuentan con medidas de seguridad adecuadas pueden convertirse en un punto vulnerable para ciberataques.



Mejores Prácticas en la Gestión de Riesgos con Herramientas GRC

Gestión de Riesgos con herramientas GRC

La **gestión de riesgos** con herramientas GRC es una disciplina crítica que permite a las organizaciones **identificar, evaluar y mitigar posibles amenazas** a su operación. Implementar herramientas **GRC (Governance, Risk, and Compliance)** optimiza este proceso, asegurando un enfoque sistemático para **gestionar los riesgos de manera efectiva**.

La **gestión de riesgos** implica la **identificación, análisis y control** de las amenazas potenciales que podrían afectar los **objetivos** de una organización. Estas amenazas pueden ser de origen financiero, operativo, de cumplimiento, tecnológico o ambiental. El objetivo es **reducir la incertidumbre** y **minimizar el impacto negativo** de los eventos inesperados mediante la **implementación de estrategias y medidas preventivas**.

La **gestión de riesgos** no se limita a la **mitigación de amenazas**; también implica aprovechar oportunidades, mejorar la **resiliencia organizativa** y garantizar el **cumplimiento normativo**.

La correcta **gestión de riesgos** ayuda a las empresas a:

- **Identificar posibles vulnerabilidades** antes de que se conviertan en problemas mayores.
- **Reducir pérdidas** financieras y operativas.
- Cumplir con las **normativas y regulaciones** vigentes.
- Mejorar la **toma de decisiones** al basarse en un análisis sólido de los riesgos.

Las empresas que no cuentan con un proceso adecuado de gestión de riesgos están expuestas a **sanciones**, pérdidas **financieras** y **daños reputacionales** significativos.

Herramientas GRC para la gestión de riesgos

Las **herramientas GRC (Governance, Risk, and Compliance)** son plataformas que permiten a las empresas gestionar de manera integrada sus procesos de gobierno corporativo, gestión de riesgos y cumplimiento normativo. Estas soluciones **automatizan** la **identificación de riesgos**, la **evaluación** de su impacto y la implementación de controles para **mitigar dichos riesgos**.

Además, las herramientas GRC facilitan la **creación de informes**, el **monitoreo** de indicadores clave y la **integración** de todas las **áreas involucradas** en la gestión de riesgos.



Beneficios de implementar un programa de Compliance en tu organización

Programa de Compliance

Los entornos empresariales cada vez están más regulados y es necesario **implementar un programa de Compliance** para salvaguardar los intereses de la organización. Esta opción te protege contra riesgos legales a la vez que aporta múltiples beneficios estratégicos. ¿Te has planteado alguna vez establecer uno de estos programas? A continuación, te contamos por qué deberías considerar seriamente su implementación en tu organización.

1. Reducción de riesgos legales y sanciones

Uno de los principales objetivos de un programa de Compliance es **garantizar el cumplimiento de leyes y regulaciones**. Esto te protege de sanciones que pueden ser muy costosas, tanto en términos económicos como reputacionales.

Multas, cierres temporales y litigios son riesgos que puedes mitigar si tu empresa opera dentro de un marco normativo adecuado.

2. Mejora de la reputación corporativa

Las empresas que muestran un compromiso sólido con las **buenas prácticas y la transparencia** ganan la confianza de sus clientes, proveedores e inversores. Un buen programa de Compliance refuerza tu marca como una organización ética, lo que no solo atrae más negocio, sino que también la protege en tiempos de crisis.

3. Fomento de una cultura organizacional ética

El Compliance además de favorecer el cumplimiento con la ley, **promueve una cultura ética** dentro de la empresa. Un programa sólido establece un estándar claro de conducta para los empleados, desde el nivel más alto hasta el más bajo. Por lo tanto, estaremos trabajando para prevenir fraudes internos, conflictos de interés y malas prácticas.

4. Mayor eficiencia operativa

Implementar un programa de Compliance mejora los **procesos internos y los controles** de la organización. Al establecer procedimientos claros para cumplir con las normativas, se evitan interrupciones, sanciones y auditorías externas que pueden afectar la productividad. Además, facilita la identificación de áreas de mejora continua, optimizando el rendimiento general.



Estrategias de Economía Circular con el Apoyo de GRCTools

Estrategias de economía circular

La **economía circular** es un enfoque que busca optimizar el **uso de los recursos, reduciendo al mínimo los desechos y reutilizando productos y materiales**. Las empresas que adoptan estrategias de economía circular no solo **generan beneficios ambientales**, sino también ventajas económicas al **disminuir costos y mejorar la eficiencia** operativa.

La **economía circular** se basa en tres principios clave:

- 01. Eliminar residuos y contaminación:** En lugar de generar productos desechables, el diseño debe enfocarse en crear bienes que puedan reutilizarse o reciclarse de manera eficiente.

02. Mantener los productos en uso: Este principio fomenta la creación de productos duraderos que se puedan reparar o reciclar fácilmente.

03. Regenerar los sistemas naturales: Se trata de devolver a los ecosistemas lo que se toma, ya sea mediante la agricultura regenerativa o la restauración de recursos naturales.

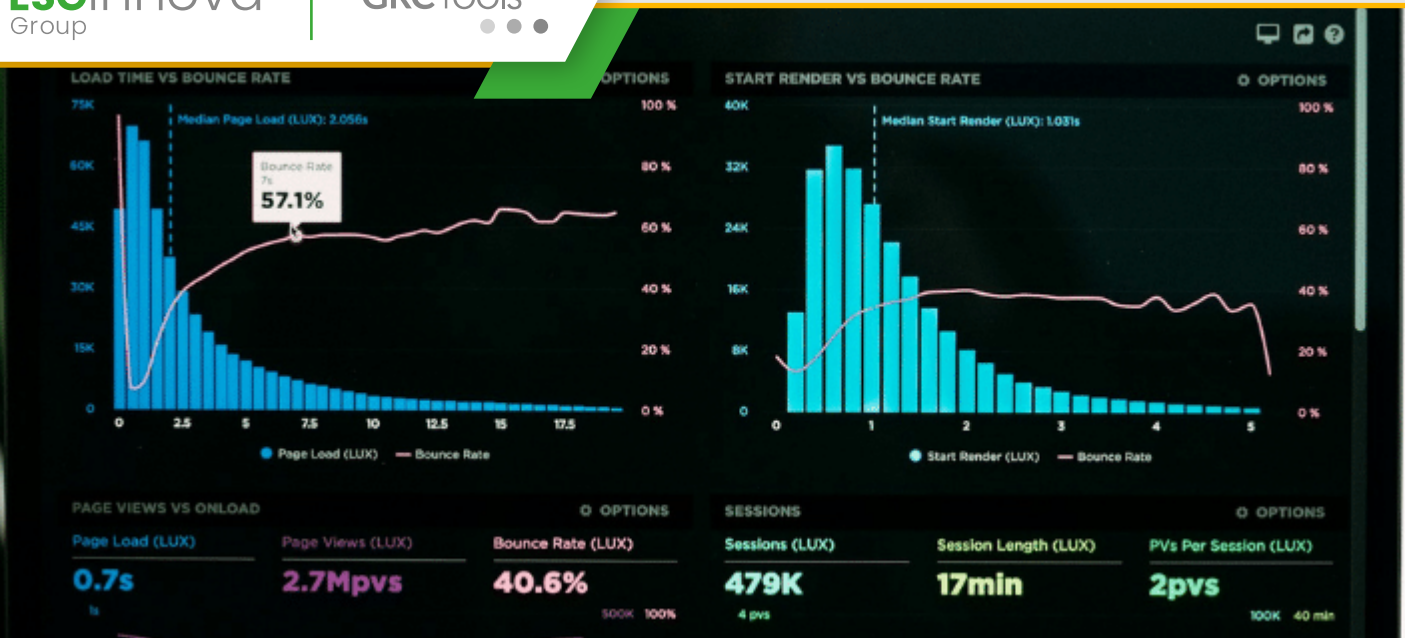
La economía circular representa un **cambio** significativo frente a la **tradicional economía lineal**, donde los productos se fabrican, se consumen y luego se desechan. En cambio, las estrategias de economía circular promueven la **maximización del valor de los productos y materiales** a lo largo del tiempo.

La transición hacia las estrategias de **economía circular** ofrecen múltiples beneficios para las empresas. Primero, permite una **reducción de costos** a través de la **reutilización** de materiales y productos, disminuyendo la dependencia de materias primas vírgenes. Además, mejora la **reputación corporativa**, ya que cada vez más consumidores valoran las marcas que **aplican prácticas sostenibles**. Finalmente, reduce la exposición a los riesgos asociados con la **escasez de recursos y las fluctuaciones** en los precios de las materias primas.

Estrategias de economía circular que son clave

Rediseño de productos

El **rediseño de productos** es una de las primeras acciones que deben adoptar las empresas que buscan implementar la **economía circular**.



Automatización de políticas de ciberseguridad con GRC

La **ciberseguridad** es fundamental para proteger los datos, la reputación y la competitividad de las empresas en el entorno digital actual. Con la creciente sofisticación de las amenazas cibernéticas, la implementación de políticas de ciberseguridad robustas y efectivas se ha convertido en una necesidad imperante.

La automatización de estas políticas mediante **herramientas de Governance, Risk, and Compliance (GRC)** es una solución que permite a las empresas gestionar y controlar sus riesgos de manera centralizada, eficiente y adaptada a sus necesidades específicas.

¿Qué es la automatización de políticas de ciberseguridad?

La **automatización de políticas de ciberseguridad** implica el uso de tecnologías avanzadas para desarrollar, implementar, supervisar y actualizar automáticamente las políticas de seguridad.

Esto reduce la carga de trabajo manual y mejora la precisión y consistencia de las medidas de seguridad.

Con un enfoque automatizado, **las empresas pueden responder rápidamente a las amenazas** y garantizar el cumplimiento normativo continuo.

Beneficios de la automatización de políticas de ciberseguridad con GRC

Eficiencia y reducción de costes

La automatización de políticas de ciberseguridad **permite a las empresas ahorrar tiempo y recursos** al eliminar la necesidad de tareas manuales repetitivas. Esto no solo reduce costos, sino que también permite al personal de TI enfocarse en tareas más estratégicas.

Mejora de la precisión y consistencia

Las herramientas GRC garantizan que las políticas de seguridad **se apliquen de manera uniforme en toda la organización**. Esto reduce el riesgo de errores humanos y asegura que todas las medidas de seguridad sean coherentes y efectivas.

Respuesta rápida a incidentes

La automatización facilita una detección y respuesta más rápida a los incidentes de seguridad. Las herramientas GRC pueden **monitorear continuamente el entorno de TI**, identificar anomalías y activar automáticamente las respuestas adecuadas para mitigar amenazas potenciales.



Certificación COBIT 5: principios y controles para la gestión de riesgos

La **certificación COBIT 5** es un marco de trabajo ampliamente utilizado para la gestión y el gobierno de las TI en las organizaciones. Desarrollado por ISACA, COBIT 5 ofrece un enfoque integral para alinear los objetivos de TI con las metas empresariales, ayudando a las empresas a gestionar los riesgos y maximizar el valor de sus inversiones tecnológicas. En este artículo, exploraremos los principios clave de **COBIT 5** y cómo su implementación puede optimizar la gestión de riesgos.

¿Qué es COBIT 5 y por qué es relevante para la gestión de riesgos?

COBIT 5 (Control Objectives for Information and Related Technology) es un marco de referencia diseñado para guiar a las empresas en la administración de TI, ayudando a las organizaciones a equilibrar la creación de valor y la **gestión de riesgos**.

Su enfoque es especialmente útil para empresas que operan en entornos altamente regulados, donde la seguridad de la información y la gestión del riesgo son fundamentales.

Una de las principales razones por las que **COBIT 5** es relevante en la gestión de riesgos es su capacidad para establecer controles claros y medibles, lo que permite a las empresas identificar, evaluar y mitigar riesgos asociados con sus sistemas de información y procesos tecnológicos.

Principios de COBIT 5

COBIT 5 se basa en cinco principios fundamentales que sirven de base para la implementación efectiva de la gobernanza de TI. Estos principios no solo permiten una gestión eficiente, sino que también contribuyen directamente a la **mitigación de riesgos**.

Satisfacer las necesidades de los interesados

Toda organización debe alinear sus objetivos de TI con los intereses de las partes interesadas. **COBIT 5** proporciona un enfoque estructurado para identificar y satisfacer estas necesidades, garantizando que las iniciativas tecnológicas aporten valor y controlen los riesgos relevantes.

Cubrir la empresa de extremo a extremo

COBIT 5 considera todos los aspectos de la empresa en su conjunto, y no solo la función de **TI**. Esto es crucial para la gestión de riesgos, ya que permite un enfoque integral que asegura que todas las áreas operativas estén alineadas con los objetivos de negocio y que los riesgos se gestionen de manera coherente.



DORA: La nueva regulación de Ciberseguridad para el Sector Financiero

DORA

El sector financiero está enfrentando uno de los retos más importantes de la era digital: **protegerse contra las crecientes amenazas cibernéticas**. Con la transformación digital acelerada y la dependencia de las **Tecnologías de la Información y la Comunicación (TIC)**, las organizaciones financieras necesitan reforzar su resiliencia ante interrupciones y ciberataques.

Para abordar este desafío, la Unión Europea ha lanzado el **Digital Operational Resilience Act (DORA)**, una regulación clave que promete transformar la **Gestión de la Seguridad de la Información (GSI)** en todo el sector.

¿Qué es DORA y por qué es importante para las organizaciones financieras?

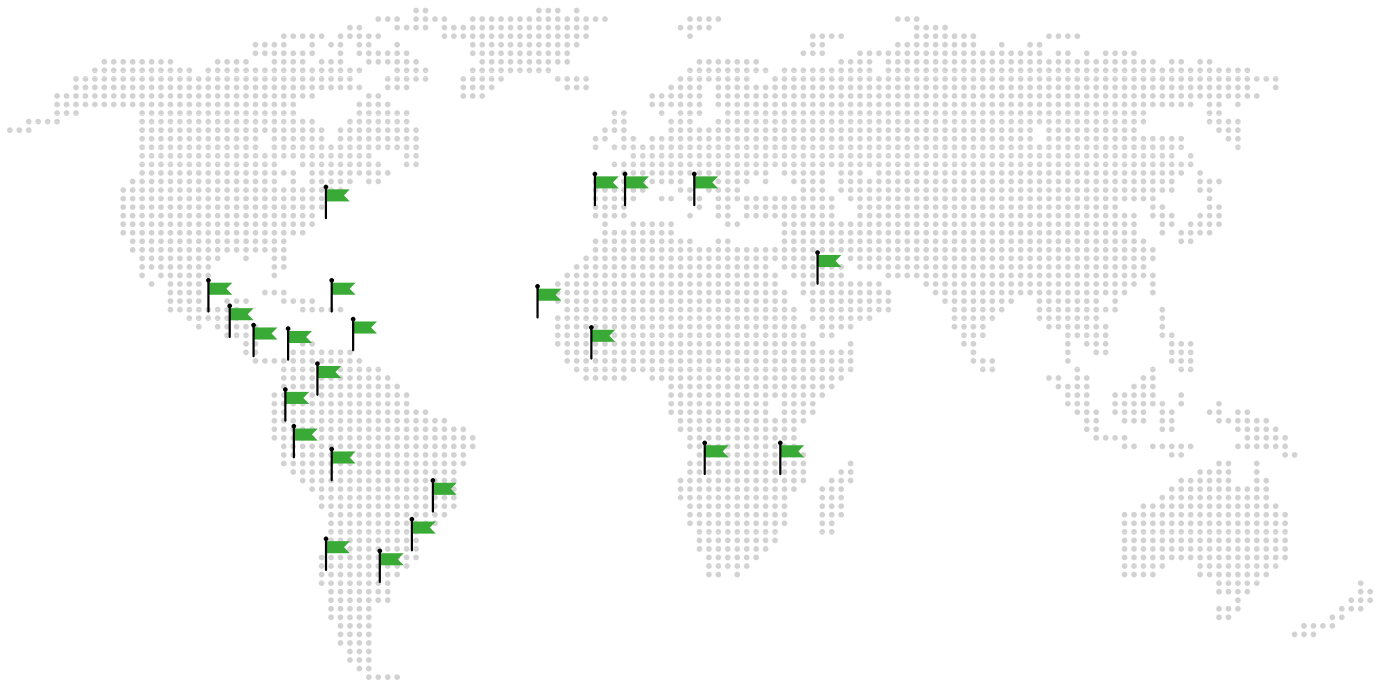
DORA, que entrará en vigor en enero de 2025, establece un **marco integral** para gestionar el riesgo relacionado con las TIC en el sector financiero. Con una cobertura amplia que incluye **bancos, aseguradoras, firmas de inversión y proveedores de servicios tecnológicos**, esta regulación busca asegurar que las organizaciones no solo puedan prevenir ciberataques, sino también **responder y recuperarse rápidamente** en caso de que ocurra un incidente.

El impacto de DORA será significativo. Las empresas deberán adoptar una **estrategia de ciberseguridad robusta** que abarque no solo sus operaciones internas, sino también sus relaciones con proveedores externos. Si tu empresa está vinculada al sector financiero, es el momento de prepararse.

Principales requisitos de DORA para empresas

Gestión del riesgo TIC

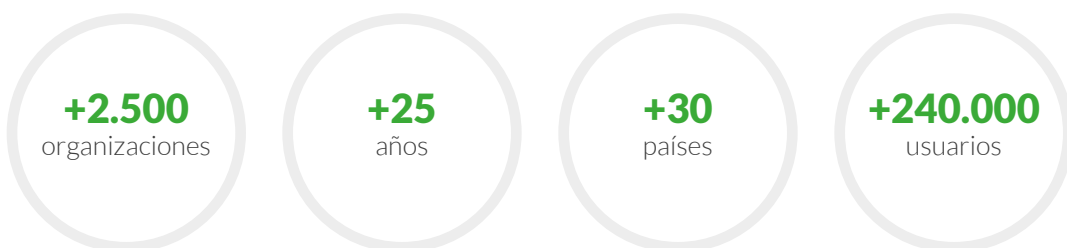
Las organizaciones deben establecer **políticas y procedimientos claros** para identificar, gestionar y mitigar los riesgos relacionados con las tecnologías de la información y la comunicación. Esto incluye no solo amenazas internas, sino también aquellas derivadas de terceros que proporcionan servicios esenciales, como plataformas en la nube o proveedores de software.



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.



ESGinnova Group

Córdoba, España

C. Villnius, P.I. Tecnocórdoba,
Parcela 6-11 Nave H, 14014
Tel: +34 957 102 000

Écija, España

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

Santiago de Chile, Chile

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

Lima, Perú

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

Bogotá, Colombia

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

México DF, México

Av. Darwin N°. 74, Interior 301,
Colonia Anzures, Ciudad de México
11590 México
Tel: +52 5541616885

