ESG INNOVA GROUP

Empresa excelente

Las mejores temáticas sobre Normas ISO, HSE, GRC y ESG



Índice

ACERCA DE ESG INNOVA GROUP 04

NORMAS ISO 09

- Cómo implantar compliance en empresas que trabajan con grandes clientes o sector público 10
- Rol de ISO 42001 para la inteligencia artificial sin cajas negras 12
- 5 pasos para elaborar un programa de auditoría 14
- Qué debe incluir un código ético o de conducta empresarial 16
- Programa de auditoría vs. plan de auditoría 18
- 7 tips para auditar indicadores de calidad 20
- Cómo prevenir conflictos de interés en la empresa: política, claves y ejemplos 22
- 10 errores frecuentes al definir indicadores de calidad 24
- Claves del liderazgo de la alta dirección ISO 37001 26
- Canal de denuncias ISO 37301: ¿cómo impulsarlo? 28
- Qué debe incluir un programa de compliance en una empresa: estructura normativa de cumplimiento 32

SEGURIDAD, SALUD Y MEDIOAMBIENTE 34

- ¿Qué es la gestión de emergencias? 35
- 8 pasos para llevar a cabo la prevención de riesgos en SSO 37
- Cómo evitar la dependencia de un solo proveedor 39
- Protocolo de prevención de riesgos en SSO en caso de inundacion 41
- El riesgo legal de intentar ahorrar con proveedores informales 43
- Cómo blindar la cadena de suministro ante economías ilícitas 45
- ¿Qué es y cómo optimizar la cadena de abastecimiento? 47
- ¿Qué es el control documental?: objetivos y cómo implantarlo 49
- Cómo identificar y prevenir el fraude en proveedores 51
- ¿Cuáles son las medidas de Prevención de riesgos en SSO en caso de terremoto? 53
- Tercerización y obligaciones laborales: homologación de proveedores 55
- ¿Qué es y cómo hacer un plan de continuidad operacional? 57

Índice

GOBIERNO, RIESGO Y CUMPLIMIENTO 59

- ¿En qué consiste el diseño de producto centrado en el cumplimiento? 60
- Plan anual de auditoría interna: cómo elaborarlo paso a paso 62
- Inventario de controles internos: qué es y cómo mantenerlo actualizado 64
- Estrategia y establecimiento de objetivos en COSO ERM: alineando riesgo y negocio 66
- Categoría básica ENS: requisitos y medidas de seguridad aplicables 68
- Política de seguridad de la información: cómo elaborarla y mantenerla actualizada 70
- Seguimiento de hallazgos de auditoría: cómo garantizar el cierre de acciones 72
- Responsables de los controles internos: roles y funciones en la organización 74
- El componente desempeño en COSO ERM y su papel en la respuesta al riesgo 76
- Categoría media ENS: requisitos y controles del Esquema Nacional de Seguridad 78
- Entidades importantes en NIS2: requisitos y diferencias respecto a las esenciales 80
- Cómo elaborar un inventario de activos de información eficaz 82

SOSTENIBILIDAD MEDIANTE SOFTWARE ESG 84

- GRI 1: fundamentos clave para elaborar informes de sostenibilidad 85
- GRI 2: contenidos generales para reportar la información corporativa 87
- GRI 3: cómo identificar y reportar los temas materiales 89

EL CAMINO HACIA LA EXCELENCIA 91

ESG Innova Group

ESG Innova es un grupo de empresas con **más de 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.

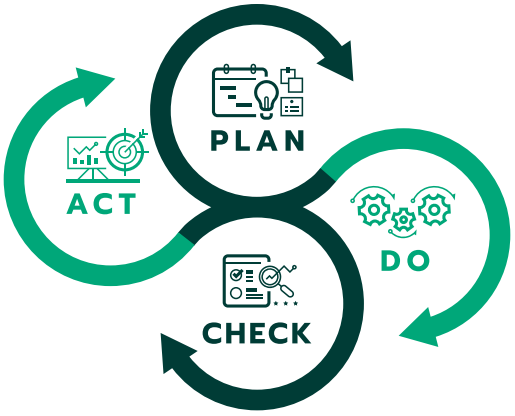
Plataforma ESG Innova

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.

ESG INNOVA 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.**

ISO TOOLS

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

HSE TOOLS

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

GRC TOOLS

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

ESG TOOLS

Transformación Digital para la gestión de la Sostenibilidad mediante Software ESG con Inteligencia Artificial

La Plataforma ESG aporta resultados en el corto plazo

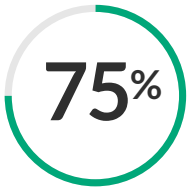
Optimización del tiempo



Menos de tiempo de resolución de una acción correctiva



Menos de tiempo de preparación de las reuniones de gestión

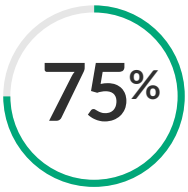


Menos de tiempo dedicado a recopilar y tratar indicadores

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

ESG INNOVA GROUP



ISO TOOLS

Transformación Digital para la gestión de Sistemas Normalizados ISO



Cómo implantar compliance en empresas que trabajan con grandes clientes o sector público

Implantar compliance en empresas que trabajan con grandes clientes o el sector público exige sistemas robustos, documentados y trazables, y la norma ISO 37301 ofrece un marco claro para lograrlo. Aplicar de forma estratégica cómo implantar compliance en empresas que trabajan con grandes clientes o el sector público reduce riesgos legales y reputacionales y, además, fortalece la competitividad en licitaciones y contratos clave.

Cuando defines cómo implantar compliance en empresas que trabajan con grandes clientes o el sector público, debes partir de una realidad sencilla: estos grupos de interés exigen evidencias sólidas,

y ya no basta con códigos éticos genéricos. **Los departamentos de compras, compliance y contratación pública piden pruebas documentadas de integridad, controles preventivos y una cultura real de cumplimiento**, porque se juegan su propia reputación.

Si te preguntas cómo implantar compliance en empresas que trabajan con grandes clientes o el sector público, la respuesta más sólida pasa por un sistema alineado con la norma internacional de sistemas de gestión de compliance **ISO 37301**. **Este estándar define requisitos verificables para identificar riesgos de incumplimiento, establecer controles, formar a las personas y generar evidencias auditables**, lo que encaja muy bien con pliegos de licitación y procesos de homologación de proveedores.

La norma adopta la estructura de alto nivel de otros estándares ISO, así que se integra con facilidad con sistemas de calidad, seguridad de la información o antisoborno. Gracias a esta compatibilidad, **puedes aprovechar políticas, procesos y canales ya existentes y reforzarlos con un enfoque específico de cumplimiento normativo**, evitando duplicidades y reduciendo la carga operativa para las áreas implicadas en el día a día.

Diversas administraciones están incorporando requisitos de integridad, prevención de corrupción y control de conflictos de interés en sus marcos de contratación, y esto impacta en tu organización. **Contar con un sistema alineado con ISO 37301 facilita demostrar diligencia debida ante organismos de control y órganos de contratación**, lo que aumenta tu puntuación técnica y la confianza de los evaluadores en la fase de adjudicación.

El primer paso para cómo implantar compliance en empresas que trabajan con grandes clientes o el sector público consiste en entender qué espera cada grupo de interés.

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO



Rol de ISO 42001 para la inteligencia artificial sin cajas negras

La inteligencia artificial sin cajas negras exige transparencia, trazabilidad y control sobre datos, modelos y decisiones, porque solo así genera confianza. ISO 42001 aporta un marco de gestión que ordena responsabilidades, riesgos y controles, y te permite integrar la IA en tu organización de forma ética, segura y alineada con objetivos de negocio.

Cuando hablas de inteligencia artificial sin cajas negras, te refieres a sistemas donde entiendes cómo se toman las decisiones, quién las supervisa y qué límites existen. **La opacidad técnica ya no es aceptable en sectores regulados o con alto impacto en personas**, porque genera desconfianza, riesgos legales y resistencia interna al uso de la IA.

La implantación de la norma **ISO 42001** para sistemas de gestión de inteligencia artificial te permite pasar de pruebas aisladas a un modelo gobernado y repetible. **La norma define políticas, roles y procesos para que cada caso de uso de IA tenga objetivos claros, controles definidos y métricas que respalden su desempeño** con una visión integral del ciclo de vida.

Para lograr inteligencia artificial sin cajas negras, necesitas documentar qué datos usas, cómo los procesas y qué algoritmos aplicas. ISO 42001 exige inventarios de sistemas, descripciones de modelos y registros de entrenamiento, así que **puedes reconstruir por qué un sistema generó una salida concreta y quién aprobó ese comportamiento** durante su diseño o en cada cambio relevante.

Esta norma anima a definir criterios de calidad de datos, sesgos aceptables y límites de uso, y a mantener evidencias. Gracias a ello, cuando un auditor, un regulador o una persona afectada pide explicaciones, tienes argumentos sólidos. **El resultado es una IA más trazable y alineada con expectativas éticas**, incluso cuando empleas modelos complejos como redes neuronales profundas.

Una inteligencia artificial sin cajas negras no solo explica decisiones, también gestiona riesgos de forma continua. ISO 42001 se apoya en metodologías de análisis de riesgos conocidas y las adapta al contexto de la IA, así que **puedes identificar amenazas técnicas, legales, reputacionales y de seguridad desde la fase de diseño** y no solo cuando la solución está en producción.

Cuando estableces un proceso cíclico de identificación, evaluación, tratamiento y seguimiento, vinculas cada control a un riesgo concreto.

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO



5 pasos para elaborar un programa de auditoría

Diseñar un programa de auditoría sólido te permite controlar riesgos, demostrar cumplimiento con las normas ISO, alinear áreas dispersas y sostener la mejora continua, porque transforma la auditoría en una actividad planificada, orientada a resultados y alineada con la estrategia de tu organización.

Un programa de auditoría bien construido unifica criterios, prioriza riesgos y ordena todas las auditorías internas y externas que requiere tu organización durante un periodo concreto. **Funciona como hoja de ruta que conecta estrategia, procesos y resultados de auditoría**, y te ayuda a decidir qué auditar, cuándo, con qué recursos y con qué profundidad en cada ciclo.

El programa de auditoría es el conjunto coordinado de una o varias auditorías planificadas en un periodo, con sus objetivos, alcance,

criterios, métodos y recursos definidos. **No es solo un calendario, sino un marco de gestión que integra riesgos, prioridades y resultados esperados**, y que se revisa periódicamente para ajustarse a los cambios del contexto y de la estrategia.

Cuando tu organización gestiona varias **normas ISO** de referencia en distintos sistemas de gestión, el programa cobra aún más importancia, porque permite integrar auditorías, reducir duplicidades y coordinar equipos. Esto se traduce en menos esfuerzo, más coherencia entre requisitos y una visión global del desempeño de procesos y áreas clave en cada ciclo de auditoría.

La ISO 19011:2018 establece directrices claras para estructurar un programa de auditoría eficaz en cualquier tipo de sistema de gestión, tanto de calidad como ambiental o de seguridad. **Esta guía se ha convertido en el marco de referencia principal para alinear objetivos de auditoría, competencias de auditores y enfoque basado en riesgos**, por lo que conviene conocer sus principios y recomendaciones antes de diseñar tu propio esquema.

Si quieres profundizar en la guía específica para auditar sistemas de gestión, resulta clave revisar el enfoque y los principios descritos en la **norma internacional ISO 19011:2018 y sus directrices** actualizadas. Este estándar explica cómo estructurar programas de auditoría, cómo seleccionar equipos competentes y cómo usar hallazgos para impulsar la mejora continua dentro de la organización.

El punto de partida del programa de auditoría es comprender qué te preocupa realmente y dónde se concentran los riesgos de incumplimiento o fallo operativo.

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO



Qué debe incluir un código ético o de conducta empresarial

Contar con un código ético sólido reduce riesgos legales, refuerza la confianza y ordena el comportamiento interno, y la norma ISO 37301 ofrece un marco para integrarlo en el sistema de compliance. Si te preguntas **qué debe incluir un código ético o de conducta empresarial**, necesitas alinear principios, reglas y controles con la estrategia y la cultura corporativa.

Un código ético o de conducta empresarial es mucho más que un documento para cumplir expediente, porque define el estándar mínimo de comportamiento esperado y orienta tus decisiones diarias. Cuando este código se integra en un sistema de gestión basado en la norma **ISO 37301** de compliance, se convierte en una herramienta viva que previene incumplimientos, canaliza dilemas éticos y refuerza tu reputación ante clientes, socios y autoridades.

Cuando defines qué debe incluir un código ético o de conducta empresarial, necesitas partir de tu realidad organizacional, porque no existe un modelo único válido para todos. Es clave vincular la cultura corporativa, el mapa de riesgos de cumplimiento y los compromisos con grupos de interés para que el código sea coherente, aplicable y medible, y no un simple documento teórico.

Un enfoque maduro sitúa al código ético como elemento central del sistema de compliance, ya que alinea políticas, procedimientos e indicadores con principios y valores. Así logras que las decisiones complejas se apoyen en criterios claros y que los equipos entiendan **cómo traducir los valores en conductas observables** durante su trabajo diario, incluso en situaciones de presión comercial o de plazos.

La ISO 37301 exige que el órgano de gobierno y la alta dirección asuman liderazgo en materia de cumplimiento, y esto incluye aprobar y respaldar el código ético. La norma pide roles definidos, recursos adecuados y supervisión continua, así que tu código debe reflejar esta gobernanza y concretar quién aprueba, revisa y comunica sus contenidos, y cómo se evalúa su efectividad.

Además, la norma impulsa la mejora continua del sistema, por lo que el código no puede ser estático y debe revisarse cuando cambie el contexto, la legislación o los riesgos clave. De este modo, el código pasa a ser un instrumento dinámico que integra lecciones aprendidas, hallazgos de auditorías e incidencias reales, y así **evoluciona al ritmo de la organización**.

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO



Programa de auditoría vs. plan de auditoría

Las organizaciones que buscan certificar y mantener sus sistemas de gestión necesitan distinguir con precisión entre programa de auditoría y plan de auditoría, porque esa claridad mejora la planificación, reduce riesgos de incumplimiento y potencia el valor de las auditorías internas como herramienta de mejora continua.

Entender con claridad Programa de auditoría vs. plan de auditoría evita malentendidos entre equipos, auditores y dirección, y te ayuda a alinear recursos, tiempos y competencias con los riesgos reales del negocio, cumpliendo las directrices de auditoría establecidas y conectando cada revisión con los objetivos estratégicos de la organización.

El programa de auditoría es la hoja de ruta global de auditorías para un periodo determinado, que suele abarcar un año o más, e integra todos

los sistemas de gestión presentes en la organización, como calidad, medio ambiente o seguridad de la información.

Cuando diseñas el programa, defines qué procesos se auditan, con qué frecuencia, bajo qué criterios y qué competencias necesita cada auditor, de forma que **las actividades de auditoría se priorizan según riesgos, impacto y contexto del negocio**, y se garantiza una cobertura sistemática sin improvisaciones ni vacíos de control.

La primera decisión clave consiste en alinear el programa con los riesgos y oportunidades que marcan las **normas ISO** de referencia en tu organización, porque así integras las actividades de auditoría con tus objetivos de cumplimiento y con las obligaciones regulatorias que afectan a procesos críticos.

Para estructurar de forma rigurosa el programa de auditoría vs. plan de auditoría, necesitas comprender las directrices de ISO 19011 y su enfoque basado en riesgos, que orienta la selección de auditorías, la definición de objetivos y la asignación de recursos hacia las áreas con mayor impacto sobre el desempeño y la conformidad.

La norma ISO 19011:2018 describe los principios de auditoría, la gestión del programa y la realización de auditorías, y resulta una referencia básica para responsables de calidad, coordinadores de sistemas integrados y auditores internos, porque **ofrece un lenguaje común y un método probado para planificar, ejecutar y mejorar las auditorías** en cualquier organización.

Si quieres profundizar en la actualización de los lineamientos para auditar sistemas de gestión integrada, es especialmente útil revisar el alcance, los cambios y el enfoque de la guía ISO 19011:2018, que se detallan en el contenido sobre **qué es la norma internacional ISO 19011:2018** y cómo orienta las auditorías.

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO



7 tips para auditar indicadores de calidad

Auditar indicadores de calidad te permite saber si tu sistema realmente mejora, si los datos son fiables y si cumples los requisitos de ISO 9001, porque conecta la estrategia con la operación diaria y reduce decisiones basadas en intuición.

Cuando auditas indicadores de calidad, tienes que tener en cuenta que es mucho más que revisar cuadros de mando bonitos, porque implica verificar cómo se definen, cómo se calculan y cómo se usan para mejorar procesos. Si descuidas esta revisión, puedes tomar decisiones equivocadas, generar desconfianza en los resultados y frenar la mejora continua, aunque aparentemente cumplas objetivos en tus informes mensuales.

El primer tip para auditar indicadores de calidad consiste en definir bien el alcance, porque necesitas saber qué procesos revisar, qué datos

analizar y qué decisiones se apoyan en cada métrica. **Si no acotas el sistema que vas a auditar, terminas dispersando esfuerzos**, perdiendo foco y generando informes que no aportan información útil a la dirección ni a los responsables de proceso.

Cuando estructuras el programa de auditoría, incluye siempre los indicadores estratégicos, de proceso y operativos, y no dejes fuera los indicadores de experiencia de cliente. Es clave que el auditor conozca la cadena causa-efecto entre indicadores, porque un mal resultado en satisfacción suele tener su origen en fallos de proceso, tiempos de respuesta o defectos de producto, y debes seguir ese rastro durante la auditoría.

Para seleccionar qué indicadores revisar, resulta muy útil apoyarte en una clasificación clara de métricas de calidad, porque así relacionas eficacia, eficiencia, cumplimiento y percepción del cliente. Es especialmente práctico revisar los principales tipos de indicadores de calidad descritos en esta **guía sobre tipos de indicadores de calidad**, y contrastarlos con los que tú utilizas en tus procesos.

La primera vez que menciones la norma en tu planificación de auditoría, asegúrate de relacionar los requisitos aplicables con cada indicador clave, porque la norma **ISO 9001** para la gestión de la calidad exige demostrar resultados medibles. **Esto te ayuda a vincular cada KPI con un requisito concreto**, como enfoque al cliente, mejora continua o evaluación del desempeño, y refuerza la trazabilidad durante la auditoría interna.

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO



Cómo prevenir conflictos de interés en la empresa: política, claves y ejemplos

La clave sobre **cómo prevenir conflictos de interés en la empresa** está en combinar una política clara, controles eficaces y una cultura de integridad alineada con ISO 37301, lo que reduce riesgos legales, protege la reputación y fortalece la toma de decisiones.

Evitar que los intereses personales de directivos, empleados o socios influyan en decisiones corporativas es un reto constante, porque afecta a la confianza de clientes, reguladores y del propio equipo. Si defines criterios objetivos, documentas los vínculos relevantes y reaccionas con rapidez ante incidentes, resulta más sencillo demostrar que gestionas los riesgos de integridad de forma profesional.

Si quieres saber **cómo prevenir conflictos de interés en la empresa**, necesitas primero distinguirlos con claridad. Un conflicto de interés aparece cuando un vínculo personal, económico o familiar puede influir, o parecer que influye, en una decisión profesional, incluso si finalmente no hay beneficio real para la persona implicada.

Estos conflictos pueden ser actuales, potenciales o aparentes, y cada tipo exige una respuesta distinta, porque no es lo mismo un directivo que ya contrata a la empresa de un familiar que una empleada que valora invertir en un proveedor aún no seleccionado. La percepción externa importa mucho, ya que los reguladores y terceros analizan el impacto reputacional.

La norma **ISO 37301 sobre sistemas de gestión de compliance** propone abordar el conflicto de interés como un riesgo de cumplimiento integrado en un ciclo de mejora continua. No solo se trata de prohibir conductas, sino de identificar escenarios, valorar impactos y establecer respuestas coherentes con la estrategia de la organización.

Dentro del ecosistema de normas de compliance, la ISO 37009 refuerza aspectos de gobierno corporativo relacionados con la independencia y la objetividad. Resulta especialmente útil conocer las **claves del nuevo marco sobre conflicto de interés ISO 37009** para alinear la gestión de incompatibilidades con las mejores prácticas de estructura y supervisión.

Una política eficaz explica con palabras sencillas qué es un conflicto de interés, a quién aplica y qué comportamientos esperas. Es recomendable que establezcas **principios como transparencia, lealtad, independencia y trazabilidad de las decisiones**, porque así alineas la política con tu código ético y con el sistema de compliance.

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO



10 errores frecuentes al definir indicadores de calidad

Definir bien los indicadores de calidad evita esfuerzos estériles, reportes irrelevantes y decisiones erróneas, y permite cumplir los requisitos de la norma ISO 9001 con datos fiables. Comprender los errores frecuentes al definir indicadores de calidad te ayuda a orientar recursos, procesos y equipos hacia la mejora continua basada en evidencia.

Los errores frecuentes al definir indicadores de calidad aparecen cuando mezclas intuición con presión por medir, pero sin un método claro. Necesitas alinear cada indicador con los objetivos estratégicos, los requisitos de clientes y los compromisos del sistema de gestión de la calidad, y así podrás priorizar lo que realmente importa.

La gestión por indicadores es un requisito clave de la **norma ISO 9001** para sistemas de gestión de la calidad, porque conecta la planificación con los resultados reales. Si eliges mal qué medir, tu sistema cumplirá en apariencia, pero no generará conocimiento accionable ni sostendrá la mejora continua.

Un error muy habitual consiste en confundir tipos de métricas y perder el equilibrio entre indicadores de resultado, proceso y percepción del cliente. Resulta útil revisar los principales tipos de indicadores de calidad y su propósito para seleccionar qué seguir en cada nivel organizativo, y así construir un cuadro de mando coherente y manejable.

Cuando te preguntas por qué ciertos indicadores no cambian pese a muchas acciones, revisa primero la cadena causa-efecto. Un buen sistema separa indicadores lagging y leading, porque los primeros describen lo ocurrido y los segundos actúan como palancas que puedes mover con rapidez.

Uno de los errores frecuentes al definir indicadores de calidad es empezar desde los datos disponibles, en lugar de partir de los objetivos. **Cuando mides lo que puedes y no lo que necesitas, llenas informes y vacías la estrategia**. Cada indicador debe responder a una pregunta clave sobre el desempeño y tener dueño claro.

Para evitarlo, vincula cada indicador con un objetivo específico, un requisito de cliente o un riesgo prioritario. Escribe la relación de forma explícita, revisa la coherencia en revisiones por la dirección y elimina indicadores que no apoyan decisiones concretas, porque solo generan ruido y resistencia.

Definir indicadores técnicamente brillantes, pero incomprensibles para los equipos operativos, genera desconfianza y uso superficial.

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO



Claves del liderazgo de la alta dirección ISO 37001

Una alta dirección ISO 37001 comprometida marca la diferencia entre un sistema antisoborno formal y uno que previene riesgos reales, protege la reputación corporativa y refuerza la confianza de clientes, inversores y reguladores al integrar el cumplimiento en la estrategia y la cultura.

La alta dirección ISO 37001 asume un rol de liderazgo que trasciende la simple aprobación del sistema, porque define el tono ético, asigna recursos y exige resultados medibles que alinean el control del soborno con la estrategia de negocio.

Cuando la alta dirección ISO 37001 lidera con coherencia, la integridad deja de ser un eslogan y se convierte en un criterio real de decisión diaria en proyectos, contrataciones y relaciones con terceros, lo que genera una cultura difícil de vulnerar por prácticas de soborno o conflictos de interés.

La primera responsabilidad es la fijación del tono desde la cúpula, así que resulta clave que el comité ejecutivo transmita con hechos que el cumplimiento no es negociable y que los objetivos comerciales nunca justifican atajos, porque **el comportamiento observable de la alta dirección modela lo que la organización entiende por aceptable**.

El estándar **ISO 37001** sobre sistemas de gestión antisoborno exige que el liderazgo defina una política clara, establezca roles, impulse la mejora continua y demuestre compromiso visible con el sistema, de modo que el programa antisoborno tenga autoridad para cuestionar decisiones y detener operaciones de riesgo.

Para que la alta dirección ISO 37001 resulte creíble, el liderazgo debe asumir acciones visibles y frecuentes que dejen claro el compromiso, como sesiones abiertas con equipos, mensajes directos sobre incidentes y participación activa en los comités, porque **las personas confían más en decisiones observadas que en documentos publicados**.

Algunas prácticas concretas son las revisiones periódicas del sistema en reuniones de dirección, la aprobación personal de sanciones disciplinarias por soborno y la presencia de directivos en formaciones clave, ya que esto vincula el desempeño ético con la evaluación del talento y los incentivos internos.

Otra señal potente es que la alta dirección asuma la responsabilidad última en caso de fallos graves y no delegue la culpa en mandos intermedios, porque ese comportamiento refuerza que el sistema antisoborno es estructural y **no un simple requisito de cumplimiento adjunto al área de cumplimiento o auditoría interna**.

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO



Canal de denuncias ISO 37301: ¿cómo impulsarlo?

Un canal de denuncias ISO 37301 sólido permite detectar incumplimientos antes de que dañen tu reputación, refuerza la cultura ética y reduce sanciones regulatorias, siempre que combine confidencialidad, tecnología adecuada y una gestión ágil de los casos.

El canal de denuncias ISO 37301 no es un buzón pasivo; es el mecanismo que transforma inquietudes individuales en información clave para tu Sistema de Gestión de Compliance y te permite anticipar riesgos legales, éticos y reputacionales.

La norma **ISO 37301 de sistemas de gestión de compliance** define el canal de alertas como parte de la infraestructura que soporta la función de cumplimiento, por lo que exige accesibilidad, protección de denunciantes, respuesta documentada y una trazabilidad total de todo el ciclo de la denuncia.

Un canal de denuncias ISO 37301 debe permitir que cualquier persona vinculada a tu organización comunique hechos de riesgo de forma segura y sin temor a represalias, así que necesitas políticas claras, múltiples vías de comunicación y registros que acrediten cómo recibes, analizas y cierras cada caso.

Para que tu canal de denuncias ISO 37301 aporte valor real, debe regirse por principios muy concretos: accesibilidad permanente, confidencialidad estricta y neutralidad en la gestión, porque si las personas perciben sesgos o falta de protección, el flujo de alertas se reducirá de forma drástica.

También es clave que el canal se integre con tu mapa de riesgos, ya que cada denuncia debe relacionarse con obligaciones específicas, procesos afectados y responsables asignados, lo que exige procedimientos escritos, matrices de clasificación y plazos de respuesta definidos por niveles de criticidad.

ISO 37301 refuerza que el órgano de gobierno y la alta dirección respalden el canal de denuncias ISO 37301 con una postura de tolerancia cero frente a represalias, así que necesitas evidencias de comunicación interna, formación y seguimiento de incidentes disciplinarios asociados a denuncias.

La norma también espera que realices revisiones periódicas de la eficacia del canal, de modo que analices tendencias, tiempos de resolución, reincidencias y nivel de utilización por colectivo, y que ajustes recursos, formación y controles según los hallazgos de cada revisión programada.

Un canal de denuncias ISO 37301 cumple su función solo cuando se usa.

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO



Cómo hacer auditorías 4.0 con ISO 19011:2026

Las Auditorías 4.0 con ISO 19011:2026 permiten transformar las auditorías tradicionales en procesos digitales, conectados y predictivos que refuerzan la eficacia del sistema de gestión de calidad basado en ISO 9001 y multiplican el valor de cada hallazgo para la mejora continua.

Las Auditorías 4.0 con ISO 19011:2026 combinan tecnología, datos y enfoque basado en riesgos para convertir la auditoría en un proceso verdaderamente estratégico, y ya no en un simple requisito de cumplimiento documental.

Cuando alineas las Auditorías 4.0 con ISO 19011:2026 con los requisitos de un sistema de gestión de calidad **ISO 9001** moderno, consigues que la auditoría se convierta en un motor de decisiones basadas en datos y no solo en un informe anual que revisas de forma reactiva.

ISO 19011:2026 se perfila como la guía que traduce los requisitos de ISO 9001 al lenguaje digital, porque orienta la planificación, la ejecución y el seguimiento de auditorías que usan herramientas colaborativas, analítica de datos y trabajo remoto sin perder rigor ni independencia técnica.

Este nuevo enfoque exige que la alta dirección se implique más en la definición de objetivos de auditoría, y que los equipos de calidad trabajen muy cerca de IT, ciberseguridad y responsables de datos, porque las Auditorías 4.0 con ISO 19011:2026 se apoyan en información distribuida por múltiples sistemas.

El salto a Auditorías 4.0 con ISO 19011:2026 no se limita a usar herramientas digitales; implica asumir principios que cambian la cultura de auditoría y obligan a repensar cómo recopilas evidencia y cómo priorizas los riesgos.

Uno de los cambios más relevantes es que el programa de auditoría se diseña usando información histórica, indicadores clave y mapas de riesgo, así que **las áreas con mayor impacto en el cliente obtienen más peso y frecuencia en el plan anual**.

Ya no tiene sentido auditar todos los procesos con la misma profundidad, porque las Auditorías 4.0 con ISO 19011:2026 impulsan que utilices métricas de desempeño, reclamaciones, tiempos de ciclo y fallos internos para definir prioridades, y eso mejora el retorno de cada hora de auditoría invertida.

Este enfoque requiere que tus procesos de medición y análisis de datos funcionen bien, porque si los indicadores no son fiables, el riesgo de enfocar la auditoría en zonas equivocadas aumenta y pierdes efectividad en la mejora continua.

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO



Qué debe incluir un programa de compliance en una empresa: estructura normativa de cumplimiento

Diseñar correctamente qué debe incluir un programa de compliance en una empresa reduce sanciones, protege la reputación y ordena el gobierno corporativo, porque incorpora políticas, controles y cultura ética alineados con ISO 37301 para asegurar un cumplimiento sistemático, medible y mejorable que responda a las expectativas regulatorias, a los riesgos reales del negocio y a las exigencias de tus grupos de interés.

Cuando te preguntas **qué debe incluir un programa de compliance en una empresa, necesitas una estructura normativa clara que conecte riesgos, controles y liderazgo**. La ISO 37301, como estándar

internacional de sistemas de gestión de compliance, ofrece esa columna vertebral para integrar políticas, procesos y responsabilidades en un marco único, alineado con la estrategia y el contexto regulatorio de tu organización.

La primera respuesta a qué debe incluir un programa de compliance en una empresa es un sistema de gestión basado en riesgo que cumpla el ciclo PDCA. La norma internacional **ISO 37301** para sistemas de gestión de compliance define requisitos para entender el contexto, establecer liderazgo visible y desplegar controles eficaces que prevengan infracciones y conflictos éticos de forma demostrable.

Para que esa estructura normativa funcione, necesitas alinear políticas, procedimientos y registros con el mapa de riesgos de cumplimiento. De esta manera, **la organización documenta decisiones clave y demuestra diligencia debida frente a autoridades, clientes y socios**. El programa deja de ser una colección aislada de documentos y se convierte en un sistema vivo que se revisa, se audita y se mejora de forma constante.

Un programa de compliance sólido parte del compromiso inequívoco del órgano de gobierno y de la alta dirección. Esto implica aprobar una política de compliance clara, asignar recursos y nombrar un responsable con autoridad real. Además, **el liderazgo debe integrar la ética en la estrategia, los objetivos y la toma de decisiones diarias**, para que no se perciba el cumplimiento como un mero requisito legal desconectado del negocio.

La gobernanza del programa también exige estructuras de supervisión y reporte con independencia funcional.

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO

ESG INNOVA GROUP



HSE TOOLS

Transformación Digital para la gestión de Seguridad, Salud y Medioambiente



¿Qué es la gestión de emergencias?

La gestión de emergencias protege a las personas, el medio ambiente y la continuidad del negocio, pero exige procesos claros, coordinación y datos en tiempo real. Un software de preparación y respuesta ante emergencias permite anticipar escenarios críticos, estandarizar planes, automatizar comunicaciones y mejorar la trazabilidad, para que tu sistema HSE responda con eficacia cuando cada segundo cuenta.

La gestión de emergencias es el conjunto de procesos, recursos y decisiones que preparan a tu organización para responder ante incidentes críticos, reducir sus impactos y recuperar la actividad. Abarca desde la identificación de amenazas hasta el restablecimiento de operaciones, y conecta de forma directa con la seguridad laboral, el medio ambiente y la reputación corporativa.

Cuando piensas en gestión de emergencias, sueles imaginar solo la fase de respuesta, pero la disciplina abarca todo el ciclo de vida. **Un modelo maduro incluye la anticipación de riesgos, la planificación, el entrenamiento, la intervención estructurada y la vuelta controlada a la normalidad**. Cada fase necesita roles definidos, recursos asignados y criterios claros de activación y cierre.

Dentro de este ciclo, la **preparación y respuesta ante emergencias** como proceso digitalizado se convierte en el esqueleto operativo que sostiene decisiones rápidas y coherentes. Permite unificar criterios entre sedes, estandarizar protocolos y minimizar variaciones que generan fallos durante situaciones críticas y escenarios de alta presión.

Antes de diseñar procedimientos, necesitas saber a qué te enfrentas y con qué probabilidad. **La gestión de emergencias parte de un análisis sistemático de peligros internos y externos**, que incluye procesos industriales, ubicación geográfica, proximidad a comunidades, proveedores clave y regulaciones sectoriales, entre otros factores relevantes para tu tipo de actividad.

Este análisis no se limita a una matriz estática, porque los riesgos evolucionan con cambios operativos, clima extremo o nuevas tecnologías. Un enfoque robusto incorpora revisiones periódicas, participación de mandos y trabajadores, y conexión con el sistema de gestión de riesgos corporativo, para que los escenarios de emergencia se mantengan actualizados y alineados con la realidad.

Una vez definidos los escenarios, necesitas planes específicos y realistas. **Un buen plan de gestión de emergencias establece cadenas de mando, niveles de alerta, rutas de comunicación y umbrales claros para la toma de decisiones**, y se adapta a las particularidades de cada centro de trabajo sin perder coherencia global.

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO



8 pasos para llevar a cabo la prevención de riesgos en SSO

La prevención de riesgos en SSO exige coordinación, datos fiables y acciones sistemáticas para reducir accidentes, enfermedades laborales e impactos ambientales, y una buena gestión de riesgos digitalizada integra personas, procesos y tecnología para anticipar peligros, priorizar controles y asegurar cumplimiento normativo.

La prevención de riesgos en SSO solo genera resultados sostenibles cuando sigues una metodología clara que conecte evaluación, control y mejora continua, así que estos 8 pasos te ayudan a ordenar el trabajo, implicar a toda la organización y medir el impacto real de tus decisiones preventivas.

El primer paso para una prevención de riesgos en SSO efectiva es **definir el contexto interno y externo de tu organización** porque necesitas entender procesos, cultura, perfil de la plantilla, partes interesadas y requisitos legales antes de priorizar peligros y recursos preventivos.

En este marco, el liderazgo juega un papel decisivo y debe asumir responsabilidades claras, así que es clave nombrar una persona o equipo referente, fijar objetivos medibles de seguridad y salud, asignar recursos y establecer un marco de **gestión de riesgos** integral alineado con la estrategia corporativa.

Cuando el liderazgo se implica de verdad, tú percibes coherencia entre discurso y práctica, y esto refuerza la participación porque las personas técnicas HSE obtienen respaldo para implantar medidas, exigir cumplimiento y coordinar acciones con operaciones, mantenimiento, recursos humanos y medio ambiente.

Tras definir el contexto, necesitas identificar las partes interesadas clave, porque **la prevención de riesgos en SSO afecta a trabajadores, subcontratas, clientes, comunidad y autoridades**, y cada grupo aporta requisitos, expectativas y condicionantes que influyen directamente en tu nivel de exposición al riesgo.

En paralelo, actualiza el inventario de requisitos legales y otros compromisos aplicables a seguridad, salud y medio ambiente, y enlaza cada requisito con procesos, responsables y evidencias, porque así reduces desviaciones en inspecciones, auditorías y visitas de la autoridad laboral.

Antes de evaluar peligros, define qué consideras un riesgo aceptable, porque **sin criterios de aceptación, la prevención de riesgos en SSO se vuelve subjetiva**.

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO



Cómo evitar la dependencia de un solo proveedor

La dependencia de un solo proveedor en entornos con alta contratación externa incrementa el riesgo operativo, legal y reputacional, porque concentra decisiones críticas en un único actor. Un enfoque estratégico de compras y una gestión de contratistas digitalizada permiten diversificar, controlar el desempeño y asegurar continuidad del negocio, reforzando la cultura HSE y el cumplimiento normativo en seguridad, salud laboral y medio ambiente.

Confiar la continuidad de tus operaciones a una sola empresa externa aumenta la vulnerabilidad HSE, porque cualquier fallo se multiplica en toda la cadena. Un retraso, un accidente grave o una sanción ambiental de ese proveedor impactan directamente en tus plazos, tus costes y tu reputación, así que necesitas anticiparte y diseñar una estrategia consciente para reducir esa exposición.

La dependencia de un solo proveedor suele nacer de decisiones bienintencionadas pero poco analizadas, como simplificar la gestión, aprovechar economías de escala o mantener una relación histórica. Con el tiempo pierdes información de mercado, negocias con menos fuerza y aceptas condiciones que no revisarías si tuvieras alternativas claras y datos comparables.

En muchos entornos industriales, un proveedor se convierte en el "de confianza" porque responde rápido y conoce tus procesos, y eso genera inercia. **La falta de recursos internos para buscar, evaluar y homologar nuevos contratistas refuerza esta comodidad**, y el área HSE queda atada a la capacidad preventiva de una sola empresa, incluso cuando surgen señales de alerta.

Otra causa habitual es la ausencia de una estrategia formal de compras y de un modelo definido de **gestión de contratistas**, donde se delimiten niveles de criticidad, requisitos HSE mínimos y proveedores alternativos. Sin ese marco, cada área negocia por su cuenta, aparecen acuerdos informales y se consolidan dependencias que nadie ha medido ni controlado.

Cuando concentras en un único contratista servicios críticos, como mantenimiento, trabajos en altura o gestión de residuos, cualquier desviación se amplifica. Si ese proveedor descuida la formación, la coordinación de actividades empresariales o las evaluaciones de riesgo, tus indicadores de siniestralidad empeoran, y tu exposición legal aumenta. **La dependencia de un solo proveedor también limita la mejora continua**, porque solo ves una forma de trabajar.

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO



Protocolo de prevención de riesgos en SSO en caso de inundacion

La prevención de riesgos en SSO en caso de inundación exige anticipar escenarios críticos, coordinar a todas las áreas y apoyarte en datos en tiempo real. Un enfoque digital de **prevención de riesgos en SSO en caso de inundación** refuerza la continuidad del negocio y la protección de las personas.

Las inundaciones se encuentran entre los desastres naturales más frecuentes en entornos industriales y urbanos, y afectan tanto a trabajadores como a activos críticos. Por eso, una estrategia de **prevención de riesgos en SSO en caso de inundación** requiere protocolos claros, formación continua y herramientas digitales que integren la información preventiva.

La primera decisión clave consiste en incluir el riesgo de inundación en tu sistema de **gestión de riesgos** corporativo, no tratarlo como un evento aislado. Así aseguras que la identificación de peligros, la valoración de probabilidad y el impacto sobre las personas y el entorno se documenten, revisen y actualicen con la misma disciplina que el resto de riesgos laborales.

Para realizar una buena **prevención de riesgos en SSO en caso de inundación,** necesitas cartografiar dónde puede entrar el agua y qué actividades resultarían más comprometidas. Analiza sótanos, salas de bombas, archivos, laboratorios o cámaras frigoríficas, y vincula cada zona a tareas específicas y turnos, porque la exposición real cambia según el momento del día y la ocupación.

Es recomendable que adoptes criterios de clasificación homogéneos para estimar criticidad, ya que eso facilita priorizar inversiones. Puedes usar escalas cualitativas basadas en impacto sobre la seguridad, la salud, el medio ambiente y la continuidad operativa, y luego relacionarlas con controles técnicos, organizativos y formativos que **refuercen la toma de decisiones**.

Las autoridades hidrológicas y meteorológicas publican avisos oficiales que debes incorporar en tus protocolos de alerta temprana, porque reducen la improvisación y los tiempos de reacción. Define quién monitoriza esos avisos, con qué frecuencia y qué umbrales activan cada nivel de respuesta, desde la prealerta hasta la evacuación parcial.

Un sistema digital te ayuda a registrar el histórico de episodios, compararlo con daños sufridos y afinar escenarios. De este modo, puedes ajustar mapas de inundabilidad internos, comprobar qué controles han sido eficaces y reforzar los más débiles, mientras **mejoras continuamente tus barreras de protección** frente a futuras crecidas.

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO



El riesgo legal de intentar ahorrar con proveedores informales

Elegir proveedores informales parece una vía rápida para reducir costes, pero multiplica el riesgo legal, eleva la exposición a accidentes y debilita tu cultura preventiva, mientras que una gestión de contratistas digital y trazable protege tu responsabilidad, refuerza el control operativo y convierte la selección de terceros en un aliado estratégico para tu sistema HSE.

Cuando trabajas con proveedores informales, asumes riesgos que no controlas y que terminan impactando en tu sistema de seguridad, salud laboral y medio ambiente. Suelen operar sin contratos robustos, con documentación insuficiente y sin evidencias claras de cumplimiento HSE, así que cualquier incidente se puede trasladar a tu organización, tanto a nivel reputacional como jurídico.

Muchos proveedores informales trabajan sin procedimientos formales de seguridad, planes de trabajo escritos ni análisis de riesgos documentados. **Cuando les abres la puerta a tus instalaciones, introduces sus carencias dentro de tu propio sistema** porque pasan a formar parte de tu cadena de valor, y la autoridad laboral o ambiental te exigirá evidencias de control que no podrás acreditar con facilidad.

En sectores con actividades peligrosas o reguladas, como industria, energía o construcción, el impacto se multiplica porque cualquier accidente grave investigará el rol de la empresa principal. Si el tercero era informal, con registros débiles y sin seguimiento, tú cargarás con buena parte de la responsabilidad, y la discusión sobre quién causó el daño tendrá poco peso frente a la falta de diligencia demostrable.

Cuando estructuras tu modelo de **gestión de contratistas** con criterios claros y digitales, reduces al mínimo el espacio para improvisación y acuerdos informales. **Transformas la relación con proveedores en un proceso controlado, auditable y alineado con tu Sistema HSE**, porque defines requisitos, verificas evidencias y mantienes una trazabilidad que antes dependía de correos dispersos o archivos en papel.

Esta gestión profesional no se basa solo en pedir documentos, sino en integrar el desempeño de terceros en tu ciclo de mejora continua. Evalúas su comportamiento en seguridad y medio ambiente, decides si mantienen la homologación y estableces planes de acción cuando detectas desviaciones. Y todo esto se fortalece con una solución tecnológica que centraliza y automatiza la información crítica.

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO



Cómo blindar la cadena de suministro ante economías ilícitas

Blindar la cadena de suministro frente a economías ilícitas exige conocer tus vulnerabilidades, controlar a proveedores y contratistas y automatizar la vigilancia continua, porque solo así reduces riesgos reputacionales, legales y operativos mientras alineas tu estrategia HSE con un enfoque de gestión de riesgos basado en datos.

Para blindar la cadena de suministro frente a economías ilícitas, es necesario ir más allá del puro control documental y entender cómo se combinan riesgos legales, operativos, HSE y reputacionales. El crimen organizado aprovecha puntos ciegos en contratación, transporte o subcontratación, así que tu modelo de supervisión debe anticipar escenarios, priorizar focos críticos y conectar la información dispersa de compras, prevención, seguridad y sostenibilidad.

Si quieres blindar la cadena de suministro, el primer paso es mapear los eslabones críticos, porque ahí se concentran las oportunidades para economías ilícitas. **Las fases con mayor exposición suelen ser la selección de proveedores, la contratación de transporte, la gestión de subcontratas y la manipulación de mercancías**. Cada una implica riesgos distintos y requiere controles específicos y trazables.

La primera vez que diseñas este mapa es habitual descubrir procesos opacos, hojas de cálculo desconectadas y responsabilidades difusas, y todo esto fomenta brechas de control. Un enfoque de **gestión de riesgos** estructurado y digitalizado te permite listar amenazas, valorar impacto y probabilidad y priorizar acciones, integrando requisitos legales, estándares HSE y políticas internas de compliance.

Para que el análisis no se quede en papel, necesitas clasificar riesgos por tipologías operativas y HSE. **Riesgos como la introducción de mercancía ilícita, corrupción en la contratación o uso de mano de obra no declarada se conectan con incidentes de seguridad, accidentes laborales o incumplimientos ambientales**. Esta visión integrada ayuda a romper silos y a justificar inversiones en tecnología, formación y controles preventivos.

Una vez identificados los puntos débiles, el foco pasa a proveedores y contratistas, porque su comportamiento puede introducir economías ilícitas en tu operación. Es clave que definas criterios de homologación que integren solvencia económica, reputación, histórico HSE, licencias, certificaciones y posibles sanciones. **Sin una matriz clara de evaluación, la selección basada solo en precio amplifica la exposición**.

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO



¿Qué es y cómo optimizar la cadena de abastecimiento?

La cadena de abastecimiento condiciona tus riesgos HSE porque concentra proveedores críticos, operaciones dispersas y exigencias normativas crecientes, y un buen control operacional digitalizado permite anticipar fallos, reducir incidentes y asegurar trazabilidad ambiental y de seguridad en cada eslabón.

La cadena de abastecimiento es el entramado de procesos que conecta a tus proveedores con tus clientes, desde la planificación de la demanda hasta la entrega final, y en cada fase se generan riesgos de seguridad, salud ocupacional y medio ambiente. **Si no integras estos riesgos en la gestión operativa, terminas reaccionando tarde, con incidencias costosas y pérdida de confianza**.

Si quieres optimizar tu cadena de abastecimiento desde la mirada HSE, necesitas mapear procesos, actores y flujos físicos e informacionales,

porque cada nodo puede convertirse en un punto de fallo. **Cuando defines con precisión quién hace qué, dónde y con qué recursos, puedes asignar responsabilidades HSE claras y diseñar controles operativos eficaces**.

En términos prácticos, la cadena de abastecimiento suele dividirse en planificación, aprovisionamiento, producción, almacenamiento, distribución y logística inversa, y en cada etapa existen riesgos específicos, como exposición a sustancias peligrosas, accidentes en maniobras de carga o emisiones asociadas al transporte. **La clave es que tus criterios de seguridad, salud y medio ambiente viajen junto con el material y la información, no solo con el contrato**.

Los estándares de gestión ISO 45001 e ISO 14001 insisten en el control de procesos externalizados y actividades contratadas, y eso te obliga a mirar la cadena de abastecimiento como extensión de tu propio sistema de gestión HSE. **No basta con declarar requisitos en pliegos; necesitas evidencias, auditorías y seguimiento continuo de los proveedores que más impacto generan**.

Para llevar estos requisitos a la práctica, la digitalización del **control operacional** de actividades y proveedores es fundamental porque unifica procedimientos, registros y flujos de aprobación en una sola capa de gestión. **Sin esta visión integrada, cada área decide por su cuenta y se multiplican las brechas entre compras, logística, seguridad y medio ambiente**.

Un sistema de control operacional bien diseñado te permite definir matrices de riesgos por tipo de proveedor, actividad y ubicación, así que puedes desplegar medidas preventivas específicas, como permisos de trabajo, listas de verificación o formaciones obligatorias.

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO



¿Qué es el control documental?: objetivos y cómo implantarlo

El control documental es la base para que tu sistema HSE funcione, porque asegura que los procedimientos críticos estén actualizados, disponibles y trazables, y el gestor de documentos y registros permite transformar documentos dispersos en información fiable que reduce riesgos, evita sanciones y mejora el cumplimiento normativo en seguridad, salud laboral y medio ambiente.

El control documental organiza, gobierna y protege toda la información que sostiene tu gestión de seguridad, salud y medio ambiente, y actúa como columna vertebral del sistema porque conecta procedimientos, evidencias y registros con la realidad operativa, así que sin un enfoque estructurado resulta casi imposible garantizar coherencia entre lo que defines en tus normas internas y lo que ocurre en campo.

El primer objetivo del control documental es evitar errores derivados de información desactualizada o contradictoria, porque un procedimiento obsoleto en una planta o centro de trabajo puede derivar en un accidente grave o en una no conformidad crítica, y por eso necesitas identificar qué documentos son críticos, quién los aprueba y cómo se comunican las revisiones para que siempre se aplique la última versión.

Otro objetivo clave es asegurar el cumplimiento legal y normativo, ya que normas como ISO 45001 o ISO 14001 exigen control efectivo de información documentada, y el **gestor de documentos** y registros corporativo permite demostrar trazabilidad de cambios, accesos y aprobaciones, algo esencial cuando afrontas auditorías internas, certificaciones o inspecciones de la autoridad laboral o ambiental.

El control documental también busca reducir tiempos muertos y fricción operativa, porque cuando cada persona sabe dónde encontrar formularios, instrucciones de trabajo o registros HSE, dedicas menos minutos a buscar y más a prevenir, así que mejoras la productividad del área de prevención y refuerzas la confianza de los equipos de operación en la información que consultan a diario.

Una implantación seria de control documental empieza por definir el ciclo de vida de cada tipo de documento, y para ello necesitas decidir cómo se crean, revisan, aprueban, publican, distribuyen y finalmente archivan o eliminan, de forma que cada fase tenga un responsable asignado, plazos claros y criterios objetivos para saber cuándo un documento sigue siendo válido o cuándo debe actualizarse.

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO



Cómo identificar y prevenir el fraude en proveedores

El fraude en proveedores erosiona tus márgenes, distorsiona la seguridad de tus operaciones y puede bloquear contratos críticos, pero una gestión robusta del ciclo de vida del contratista y el uso de software de gestión de contratistas permiten detectar patrones anómalos, reforzar el cumplimiento HSE y reducir de forma drástica los riesgos económicos, legales y reputacionales asociados.

El fraude en proveedores no es solo un problema financiero, porque también impacta en la seguridad, la salud laboral y el medio ambiente. **Cuando un proveedor manipula datos o incumple requisitos HSE, introduce un riesgo oculto en tu operación** y dificulta cualquier estrategia de mejora continua. Detectar estas prácticas de forma temprana se convierte en una prioridad estratégica para cualquier organización.

Hablar de fraude en proveedores implica mucho más que facturas infladas o comisiones ocultas, porque abarca cualquier conducta engañosa que distorsiona la relación contractual. En entornos HSE, estas prácticas suelen ir vinculadas a la ocultación de incumplimientos en seguridad, salud y medio ambiente, lo que se traduce en riesgos operativos que los indicadores económicos no muestran de inmediato.

Un caso frecuente son los proveedores que declaran certificaciones caducadas, seguros inexistentes o personal sin la formación preventiva requerida. Aquí el fraude en proveedores se materializa cuando la información documental no refleja la realidad operativa y tú tomas decisiones apoyadas en datos falsos. Este desfase genera un espejismo de cumplimiento y mina tu sistema de gestión HSE desde dentro.

También aparecen esquemas más sofisticados, como redes de empresas vinculadas que rotan empleados sancionados o con historial de accidentes entre distintas razones sociales. **Este tipo de fraude en proveedores busca esquivar los filtros de homologación y evaluación**, mientras mantiene en tu planta a personas y equipos que aumentan la probabilidad de incidentes graves y paradas de producción.

En cadenas de suministro con muchos contratistas y subcontratas, el fraude en proveedores suele seguir patrones reconocibles. Se repiten desajustes entre la documentación presentada y los datos oficiales, variaciones bruscas en costes de servicios similares y coincidencias sospechosas entre representantes legales de distintas empresas. **Identificar estos patrones exige centralizar la información y cruzarla de forma sistemática**.

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO



¿Cuáles son las medidas de Prevención de riesgos en SSO en caso de terremoto?

La prevención de riesgos en SSO en caso de terremoto exige anticipación, planificación y automatización para reducir daños personales, materiales y ambientales, y un enfoque sistemático basado en datos. Integrar la **prevención de riesgos en SSO en caso de terremoto** en una estrategia global de gestión de riesgos permite reaccionar con rapidez, coordinar recursos y aprender de cada incidente.

Cuando tu organización se ubica en una zona sísmica, ignorar ese contexto ya es un riesgo crítico, porque un terremoto impacta personas, procesos, activos y reputación. **Necesitas una estrategia que conecte la evaluación de amenazas sísmicas con la planificación de emergencias, la formación y la digitalización de la respuesta**, para que cada minuto durante el seísmo cuente de verdad.

La primera medida clave de prevención de riesgos en SSO en caso de terremoto es identificar qué puede fallar en tu entorno físico, organizativo y tecnológico durante un seísmo. Una **metodología estructurada de gestión de riesgos** te ayuda a clasificar amenazas, valorar impactos en personas y activos, y priorizar inversiones preventivas con criterios claros.

No basta con revisar la resistencia de la construcción porque muchos accidentes graves ocurren por elementos secundarios que se desplazan, se caen o bloquean rutas de evacuación. **Incluye en tu inventario de peligros todo aquello que pueda convertirse en un proyectil o un obstáculo**, como estanterías altas, maquinaria suspendida, conducciones, falsos techos o sistemas de almacenamiento en altura.

Realiza inspecciones específicas en zonas de alto tránsito, almacenes, laboratorios y áreas con sustancias peligrosas, y documenta fotografías, responsables y acciones correctivas con un criterio homogéneo. **Cuando integras estas inspecciones en un ciclo de revisión periódica, el riesgo se mantiene visible y gestionable**, y no queda oculto en documentos que nadie actualiza.

Una vez identificados los peligros, clasifícalos por probabilidad de daño humano, económico y ambiental para enfocar recursos en lo esencial. **Los riesgos con impacto potencial sobre múltiples personas o sobre procesos críticos del negocio deben ir primero**, porque ahí un fallo puede dejar inoperativa tu organización durante mucho tiempo.

Este análisis de criticidad tiene que considerar también la continuidad operacional, así que evalúa qué instalaciones son esenciales para reanudar actividades y cuáles pueden pararse más tiempo.

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO



Tercerización y obligaciones laborales: homologación de proveedores

La tercerización y obligaciones laborales exigen hoy una gestión rigurosa de proveedores y contratistas, porque tu empresa retiene responsabilidades solidarias en seguridad, salud y aspectos laborales. Un modelo robusto de homologación, apoyado en un software de gestión de contratistas, permite reducir riesgos legales, prevenir accidentes y asegurar continuidad operativa desde el primer día de trabajo externo.

Cuando decides subcontratar actividades críticas, **no externalizas tus responsabilidades legales en materia laboral ni preventiva**, solo delegas la ejecución operativa.

La ley mantiene tu obligación de garantizar condiciones seguras, controlar el cumplimiento de requisitos laborales básicos y asegurar que cada contratista actúe alineado con tus estándares HSE y de compliance, desde la selección hasta la liquidación.

La tercerización y obligaciones laborales forman un binomio delicado, porque una mala elección de contratistas se traduce en sanciones, accidentes graves y conflictos con la autoridad laboral. **Si un proveedor incumple pagos, cotizaciones o medidas de seguridad, tu organización puede responder solidaria o subsidiariamente**, y sufrir impactos en reputación, continuidad del negocio y clima interno.

La legislación laboral y de prevención de riesgos establece esquemas de responsabilidad solidaria o subsidiaria entre empresa principal y contratistas. Por eso, **el precio ya no puede ser el criterio dominante en tus decisiones de contratación**, porque eliges también el nivel de riesgo jurídico y operativo que asumes al incorporar una empresa externa a tu cadena de valor.

En este contexto, una solución específica para **gestión de contratistas** te permite estandarizar requisitos, centralizar documentación y automatizar alertas, y así reduces el margen de error humano en procesos repetitivos. Esta digitalización crea trazabilidad probatoria, muy útil ante inspecciones de trabajo o auditorías de certificación en seguridad y salud.

Cuando un trabajador externo sufre un accidente grave en tus instalaciones, la opinión pública y las autoridades no distinguen fácilmente entre personal propio y de terceros. **A nivel reputacional, el incidente se asocia a tu marca y a tus estándares de seguridad**, por lo que necesitas integrar a contratistas en tu cultura preventiva y en tus controles operativos diarios.

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO



¿Qué es y cómo hacer un plan de continuidad operacional?

La continuidad operacional garantiza que tu negocio siga funcionando ante emergencias, incidentes HSE o fallos críticos de infraestructura, y exige anticipar escenarios, formalizar planes y apoyarte en un software de preparación y respuesta ante emergencias para coordinar recursos, comunicar de forma efectiva y reducir el impacto sobre las personas, el medio ambiente y la cadena de valor.

La continuidad operacional es la capacidad de tu organización para mantener procesos críticos ante interrupciones significativas y recuperar el funcionamiento normal en plazos aceptables.

No se limita a tener un plan de emergencia, sino que integra riesgos HSE, tecnología, proveedores y cultura interna, porque una crisis afecta a toda la organización y no solo a un área concreta.

Para diseñar un plan sólido de continuidad operacional, necesitas partir de un análisis estructurado del negocio y de su entorno. **Identifica procesos esenciales, dependencias tecnológicas, proveedores clave y amenazas HSE como incendios, vertidos, explosiones o fenómenos meteorológicos extremos**, porque cualquier interrupción relevante en estos puntos puede detener tu operación o generar impactos graves sobre las personas.

Un primer paso práctico es definir criterios claros para clasificar procesos según criticidad, tiempo máximo de interrupción admisible y recursos necesarios. Así podrás priorizar esfuerzos y destinar recursos a lo que realmente sostiene tu operación diaria. **Este enfoque te ayuda a relacionar continuidad operacional con objetivos de negocio, indicadores financieros y metas de seguridad**, y facilita el compromiso de la dirección con inversiones específicas.

La continuidad operacional y la gestión de crisis se apoyan en una buena gobernanza de riesgos, y ahí el sistema de **preparación y respuesta ante emergencias** actúa como columna vertebral operativa. **Cuando integras ambos ámbitos, alineas evaluaciones de riesgos, procesos de notificación y procedimientos de respuesta**, y consigues que los equipos trabajen con la misma información durante una emergencia real.

Resulta clave mapear dependencias externas como suministros de energía, telecomunicaciones, logística o servicios críticos contratados. Muchas interrupciones prolongadas surgen por fallos fuera de tu instalación, pero terminan afectando tu reputación y tu cumplimiento legal.

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO

ESG INNOVA GROUP



GRC TOOLS

Transformación Digital para la gestión de Gobierno, Riesgo y Cumplimiento



¿En qué consiste el diseño de producto centrado en el cumplimiento?

El diseño de producto centrado en el cumplimiento integra requisitos legales, regulatorios y de riesgo desde la concepción de la solución, evitando retrabajos, sanciones y vulnerabilidades. Esta aproximación permite reducir costes de auditoría, acelerar lanzamientos seguros al mercado y fortalecer la confianza de cliente, regulador y consejo de administración frente a un entorno normativo y de ciberamenazas cada vez más exigente.

El diseño de producto centrado en el cumplimiento convierte el cumplimiento normativo en un criterio de diseño igual de importante que experiencia de usuario, rendimiento o coste. **Cuando incorporas requisitos legales, regulatorios y de ciberseguridad en las primeras fases del ciclo de vida, reduces fricciones posteriores y mejoras la**

competitividad. Esta visión encaja de forma natural con marcos GRC y con prácticas de seguridad desde el diseño.

Cuando integras un programa de gestión de **compliance** corporativo en tus decisiones de diseño, dejas de ver el cumplimiento como un freno al negocio y lo conviertes en brújula estratégica. **Esto implica mapear normativas, traducirlas a requisitos funcionales y no funcionales, y asignar responsables claros por cada exigencia**, desde privacidad hasta resiliencia operacional o requisitos sectoriales críticos.

El diseño de producto centrado en el cumplimiento exige estrecha colaboración entre legal, ciberseguridad, tecnología y negocio. Necesitas identificar regulaciones aplicables a cada solución, como protección de datos, prevención de blanqueo o requisitos financieros, y desglosarlas en historias de usuario y criterios de aceptación. **Así garantizas que cada entrega incremental avanza en paralelo en funcionalidad, seguridad y conformidad regulatoria**.

Para que esta integración funcione en entornos reales, el área de riesgos debe priorizar obligaciones según impacto y probabilidad de incumplimiento. Los criterios de priorización deben considerar sanciones potenciales, daño reputacional y afectación al cliente. **Cuando enlazas este análisis con tus decisiones de producto, el backlog refleja riesgos reales y no una lista abstracta de controles**, lo que aumenta la alineación con la estrategia corporativa.

Un diseño de producto centrado en el cumplimiento necesita tres pilares: gobierno, procesos y herramientas. El gobierno define roles, responsabilidades y foros de decisión, como comités de producto con participación de Compliance y seguridad. **Los procesos describen cómo se incorporan requisitos regulatorios en discovery, definición, desarrollo, pruebas y despliegue**, asegurando evidencias trazables en cada fase del ciclo de vida.

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO



Plan anual de auditoría interna: cómo elaborarlo paso a paso

Un plan anual de auditoría bien definido alinea riesgos clave, prioridades de negocio y obligaciones regulatorias para asegurar un control interno robusto. Permite anticipar debilidades, priorizar recursos de revisión y coordinar mejor las funciones de Gobierno, Riesgo, Cumplimiento y ciberseguridad, generando información fiable para el consejo y la alta dirección en cada ciclo anual de planificación.

El plan anual de auditoría sirve como hoja de ruta estructurada que conecta la estrategia corporativa con el día a día del control interno. Define qué procesos auditarás, con qué alcance, en qué momentos del año y con qué recursos, para que tus revisiones no dependan de urgencias improvisadas ni de percepciones subjetivas del riesgo.

Para que el plan anual de auditoría tenga impacto real, debes empezar por entender el mapa de riesgos estratégicos. Identifica procesos críticos, activos de información clave y obligaciones regulatorias exigentes, y cruza esa visión con la capacidad de tu equipo interno y los compromisos con auditores externos.

Una **auditoría de control interno** estructurada refuerza ese análisis de riesgos, porque te ofrece criterios claros para clasificar procesos por materialidad, probabilidad de fallo y nivel de exposición. Así consigues que el plan anual de auditoría se apoye en métricas objetivas y no solo en la intuición de los responsables de área.

Es clave que involucres a la alta dirección y a los dueños de proceso en esa priorización. De ese modo, el plan anual de auditoría refuerza las iniciativas estratégicas vigentes, como proyectos de transformación digital, programas de ciberseguridad o despliegues de nuevas líneas de negocio, en lugar de convertirse en una agenda paralela desconectada de la realidad operativa.

Para definir prioridades sólidas, combina varias fuentes de información de forma sistemática. Analiza resultados de auditorías anteriores, incidentes de seguridad, brechas de cumplimiento, reclamaciones relevantes y observaciones de supervisores o reguladores. Cada hallazgo se transforma en un input para valorar el riesgo residual asociado al proceso.

Integra también indicadores cuantitativos, como volumen de transacciones, criticidad del sistema, dependencia tecnológica o impacto financiero potencial. De esta manera, **el plan anual de auditoría se convierte en una herramienta basada en evidencia**, capaz de justificar por qué un área entra o no entra en el calendario del año.

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO



Inventario de controles internos: qué es y cómo mantenerlo actualizado

Un inventario de controles internos sólido evita brechas de riesgo, duplica menos esfuerzos y facilita la trazabilidad ante auditorías y reguladores, incluso en entornos multinorma exigentes. Permite alinear seguridad, cumplimiento y gobierno corporativo con decisiones ágiles y medibles. Diseñar, catalogar y mantener vivo ese inventario convierte el control interno en un activo estratégico y no en una carga documental.

El inventario de controles internos es mucho más que una lista de políticas o procedimientos, ya que **funciona como mapa operativo de cómo tu organización gestiona sus riesgos clave**. Conecta procesos, amenazas, responsables, evidencias y normativa, lo que permite entender de forma estructurada dónde se apoya realmente

tu sistema de gobierno, riesgo y cumplimiento. Cuando está bien diseñado, se convierte en una fuente única de verdad para negocio, TI, auditoría y ciberseguridad.

Un inventario de controles internos es el repositorio estructurado donde registras cada control asociado a tus procesos, riesgos y requisitos normativos. **Debe permitir saber qué control existe, por qué existe, quién lo ejecuta y cómo se demuestra su eficacia**. Sin esa visión canónica, los equipos trabajan con hojas de cálculo aisladas, definiciones distintas y lagunas que solo descubres cuando llega una auditoría o un incidente.

La primera mención al marco de **Control Interno** alineado con modelos como COSO es clave para entender el alcance del inventario, ya que no se limita al área financiera. Se extiende a tecnología, ciberseguridad, ESG, privacidad y continuidad de negocio, por lo que conviene usar una taxonomía común de riesgos y procesos en toda la organización. Esa taxonomía simplifica el enlace entre controles, evidencias y métricas de desempeño.

Para que tu inventario de controles internos sea utilizable en el día a día, conviene definir un modelo de datos mínimo y coherente. **Cada control debería tener atributos como objetivo, tipo, frecuencia, responsable, sistema involucrado, riesgos mitigados, evidencias y normativas relacionadas**. Cuando capturas esa información de forma homogénea, abres la puerta al análisis avanzado, al reporting automatizado y a la priorización basada en riesgo real y no en percepciones.

El diseño de un inventario de controles internos eficaz empieza por delimitar su alcance en términos de procesos, unidades y marcos regulatorios.

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO



Estrategia y establecimiento de objetivos en COSO ERM: alineando riesgo y negocio

La gestión estratégica del riesgo solo genera ventaja competitiva cuando conectas decisiones, apetito de riesgo y métricas con tus objetivos corporativos, integrando estrategia y establecimiento de objetivos dentro de un modelo COSO ERM que estructure gobernanza, priorización y respuesta ante la incertidumbre en entornos GRC y de ciberseguridad.

Cuando defines estrategia y establecimiento de objetivos en clave COSO ERM, decides cómo tu organización se relaciona con la incertidumbre, qué nivel de exposición estás dispuesto a aceptar y qué riesgos asumes para crecer. Si esa definición no es clara, cada área interpretará el riesgo a su manera y tu sistema GRC se fragmentará.

Necesitas traducir propósito, misión y expectativas de partes interesadas en objetivos tangibles, medibles y coherentes entre sí.

El primer bloque del modelo COSO ERM se centra en gobierno y cultura porque condiciona toda decisión estratégica. Si el consejo, la alta dirección y los comités de riesgo no comparten un lenguaje común sobre riesgo y valor, la estrategia y establecimiento de objetivos se convierte en un ejercicio teórico. Define estructuras de supervisión, roles GRC, canales de reporte y criterios claros para escalar decisiones críticas relacionadas con el apetito de riesgo.

Un elemento clave es el apetito de riesgo corporativo, que debe expresarse en términos cuantitativos y cualitativos alineados con los objetivos estratégicos. **Cuando defines umbrales, límites y tolerancias, ayudas a cada área a decidir qué riesgos aceptar, mitigar o transferir**. Esto reduce discusiones subjetivas y da coherencia a la asignación de recursos en proyectos, ciberseguridad y transformación digital.

Sin una cultura de riesgo consistente, la estrategia y el establecimiento de objetivos se quedan en papel. **La cultura se traduce en cómo se toman decisiones diarias, cómo se tratan las alertas y qué ocurre ante un incidente**. Necesitas mensajes claros desde la dirección, incentivos alineados y formación continua para que el riesgo se perciba como factor de negocio, no como freno a la innovación.

Un diseño maduro de **gestión integral de riesgos** fomenta esa cultura porque conecta mapas de riesgo, controles y KPIs con planes estratégicos y presupuestos. **Cuando los responsables de negocio ven el impacto económico de cada riesgo en sus objetivos, se implican más en su tratamiento**.

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO



Categoría básica ENS: requisitos y medidas de seguridad aplicables

La categoría básica ENS marca el nivel mínimo de seguridad exigible a muchos sistemas públicos y proveedores TIC, y condiciona cómo gestionas riesgos, controles y evidencias de cumplimiento. Entender bien sus requisitos te permite priorizar inversiones, evitar sanciones y alinear ciberseguridad, continuidad y gobierno corporativo bajo un mismo modelo de gestión.

La categoría básica ENS se aplica a sistemas cuya afectación sobre la organización, los derechos de las personas o la prestación de servicios esenciales se considera limitada. **Eso no implica baja relevancia, sino un conjunto concreto de medidas organizativas, operacionales y de protección que debes implantar y demostrar**.

Clasificar bien cada sistema y sus datos es el primer paso para decidir controles, presupuesto y priorización.

El primer bloque clave de la categoría básica ENS es la clasificación de la información y de los servicios. Necesitas valorar de forma estructurada la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de los activos. **Si esa valoración es superficial, terminarás sobredimensionando controles o dejando brechas sin cubrir**. Aquí el trabajo conjunto entre responsables de seguridad, negocio y TI es imprescindible.

La primera mención al **Esquema Nacional de Seguridad** en su conjunto debe servirte como marco de referencia para todo el ciclo de vida del sistema. A partir de esa clasificación inicial, defines si cada sistema encaja en categoría básica ENS, media o alta, y adaptas los requisitos proporcionales para cada dimensión. Esta coherencia reduce conflictos entre proyectos y auditorías.

El análisis para decidir si un sistema está en categoría básica ENS empieza por entender qué servicio soporta y qué datos trata. **Debes valorar el impacto real sobre la ciudadanía, obligaciones legales, reputación y continuidad del servicio**. No te quedes en etiquetas genéricas como “aplicación interna”, porque suelen ocultar información sensible o procesos críticos que cambian la clasificación.

Cuando cartografías servicios, procesos y flujos de información, se aclaran casos híbridos en los que parte del sistema puede mantenerse en categoría básica ENS y otra parte exige requisitos de nivel medio. Mantener esta granularidad, junto con un inventario vivo de activos, facilita justificar decisiones frente a auditorías y reduce tensiones entre cumplimiento y operativa diaria.

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO



Política de seguridad de la información: cómo elaborarla y mantenerla actualizada

Una política de seguridad de la información clara y actualizada reduce incidentes, ordena decisiones de ciberseguridad, alinea negocio y TI y demuestra diligencia ante auditorías, clientes y reguladores, convirtiéndose en el marco de referencia práctico que guía controles, responsabilidades y prioridades de inversión en entornos cada vez más expuestos.

La política de seguridad de la información traduce la estrategia corporativa en reglas operativas que definen qué proteger, cómo hacerlo y quién es responsable. Sin este marco, cada área actúa por intuición, los controles se solapan o quedan huecos y resulta casi

imposible demostrar cumplimiento frente a ISO 27001, ENS, NIS2 o el propio consejo de administración.

Antes de escribir una sola línea, necesitas acotar a qué información y procesos aplicará la política de seguridad de la información. **Define si cubrirá solo el perímetro corporativo clásico o incluirá teletrabajo, proveedores, nube pública, desarrollos internos y dispositivos personales**, porque esa decisión condiciona recursos, controles y obligaciones contractuales.

Los objetivos deben ser medibles y conectarse con el negocio. Es muy distinto decir que la política busca "proteger la información" a establecer metas como reducir incidentes de confidencialidad, acortar tiempos de respuesta ante brechas o mejorar la trazabilidad de accesos críticos, lo que **permite justificar inversiones de seguridad frente a finanzas y dirección general** con indicadores claros.

En este contexto, resulta clave encajar la política dentro de la **gestión de la seguridad de la información corporativa**, donde convergen riesgos, controles, proyectos, proveedores y métricas. Este encaje garantiza que lo que defines por escrito se traduzca en procesos repetibles, auditorías internas estructuradas y decisiones coherentes a lo largo del tiempo.

Una política de seguridad de la información madura parte de un análisis formal del contexto interno y externo. **Revisa tipo de negocio, apetito de riesgo, regulaciones aplicables, madurez tecnológica y dependencia de terceros**, porque cada elemento modifica el nivel de protección exigible y la tolerancia a interrupciones o fugas.

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO



Seguimiento de hallazgos de auditoría: cómo garantizar el cierre de acciones

Un seguimiento de hallazgos disciplinado convierte observaciones de auditoría en mejoras reales de control, reduce riesgos operacionales y fortalece la confianza regulatoria. Integrar la Auditoría de Control Interno con flujos de trabajo, métricas y gobierno de datos permite priorizar acciones, gestionar responsables y vencer la resistencia al cambio, generando una cultura de cierre efectivo y aprendizaje continuo en tu organización.

El valor de una auditoría se materializa cuando los hallazgos se transforman en acciones corregidas y verificadas. Sin un proceso de seguimiento de hallazgos estructurado, las observaciones se diluyen,

los riesgos permanecen y el comité de auditoría pierde visibilidad. En entornos de Gobierno, Riesgo y Cumplimiento, necesitas demostrar trazabilidad desde el hallazgo hasta la evidencia de cierre, con responsables claros, plazos realistas y controles reforzados.

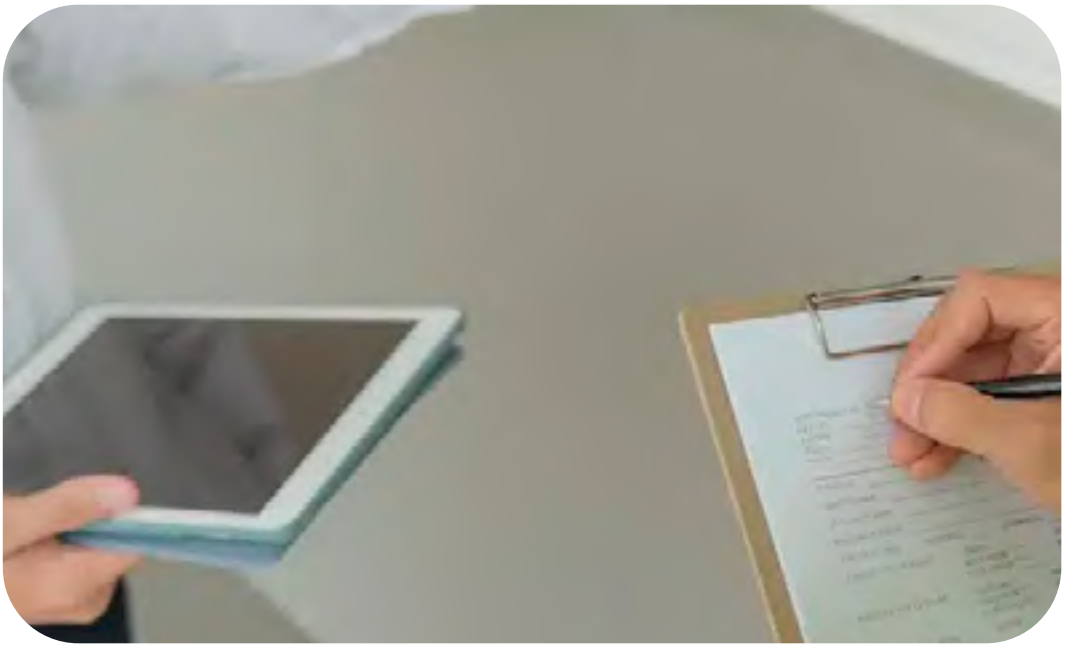
Cuando diseñas tu estrategia de seguimiento de hallazgos, el primer paso es vincular cada observación con el marco de control que uses, ya sea COSO, ISO 27001 o marcos sectoriales. **Esto permite evaluar no solo el incidente puntual, sino la fortaleza sistémica del entorno de control.** Así detectas patrones, áreas recurrentes y procesos donde los controles siempre fallan o son insuficientes.

El rol de la **Auditoría de Control Interno** es articular esta estrategia con una visión integral, conectando riesgos, controles, indicadores y acciones. La unidad de auditoría debe patrocinar criterios homogéneos de clasificación de hallazgos, niveles de criticidad y tipos de acción, para que toda la organización entienda el impacto y la urgencia asociada a cada caso.

Para que el seguimiento de hallazgos funcione, necesitas una taxonomía clara. Clasifica por tipo de riesgo, proceso, causa raíz y grado de exposición. **De esta forma, los comités pueden comparar hallazgos entre áreas diferentes con un lenguaje común** y priorizar recursos donde el riesgo residual sea inaceptable. Esta normalización es clave en grupos empresariales complejos o multinacionales.

Un flujo end-to-end de seguimiento de hallazgos debe cubrir desde la emisión del informe hasta la verificación del cierre y la medición de efectividad. **Cada etapa necesita responsables definidos, plazos, criterios de aceptación y evidencias mínimas requeridas** para considerar que una acción correctiva está realmente implantada y no solo documentada en papel.

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO



Responsables de los controles internos: roles y funciones en la organización

Los responsables de los controles definen la eficacia real del sistema de control interno, porque traducen la teoría en acciones diarias, evidencias trazables y decisiones informadas que reducen riesgos, aseguran cumplimiento normativo y fortalecen la ciberseguridad de toda la organización.

La figura de los propietarios de controles se ha vuelto crítica en entornos con alta presión regulatoria, transformación digital acelerada y mayor exposición a ciberamenazas. Estos responsables vinculan la estrategia con la operación diaria y permiten que la organización responda con agilidad ante auditorías, incidentes y cambios regulatorios sin perder foco en los objetivos de negocio.

Todo sistema de **control interno** **robusto y alineado con el negocio necesita roles claros y trazables** para cada actividad de mitigación. Si nadie asume la titularidad de un control, ese control es débil, se ejecuta de forma irregular o no genera evidencias suficientes para auditoría y supervisores. Esa falta de dueño funcional se traduce en riesgos financieros, reputacionales y tecnológicos.

El propietario de controles es la persona que asume la responsabilidad de que un control exista, funcione y se mantenga actualizado. No tiene por qué ejecutar todas las tareas, pero sí debe asegurar su diseño adecuado, su implementación correcta y su monitorización continua. Desde una perspectiva GRC, este rol se sitúa entre la primera y la segunda línea de defensa, colaborando con negocio, riesgo, cumplimiento y tecnología.

La estructura de reporting también es esencial para que los propietarios de controles actúen con autoridad. Sin un respaldo claro de la alta dirección, sus decisiones sobre priorización, refuerzo o automatización de controles pierden peso. Por eso, muchas organizaciones integran estos roles en comités de riesgo y compliance, donde se discuten debilidades detectadas, planes de remediación y necesidades de inversión tecnológica.

Una responsabilidad central consiste en que el diseño del control sea coherente con el riesgo que busca mitigar. Esto implica **definir objetivos, alcance, periodicidad, responsables operativos, evidencias requeridas y criterios de éxito**. Sin ese nivel de detalle, la organización entra en zonas grises que complican auditorías internas, revisiones regulatorias y análisis forenses tras incidentes de seguridad o fraude.

La documentación debe estar viva y accesible.

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO



El componente desempeño en COSO ERM y su papel en la respuesta al riesgo

El componente desempeño en COSO ERM transforma la gestión del riesgo en una ventaja competitiva, porque conecta objetivos, apetito de riesgo y respuesta operativa diaria. Una gestión integral de riesgos madura integra métricas, KRI y análisis dinámico para alinear decisiones, priorizar recursos y anticipar impactos en ciberseguridad, cumplimiento y estrategia corporativa.

El componente desempeño en COSO ERM se centra en cómo identificas, evalúas y priorizas los riesgos en relación con tus objetivos estratégicos, operativos y de cumplimiento. No se limita a un inventario estático; exige análisis dinámicos, criterios claros de impacto y probabilidad, y una conexión explícita con el apetito de riesgo aprobado por la alta dirección.

Cuando integras el componente desempeño en un enfoque de **gestión integral de riesgos corporativos**, conviertes la información de riesgo en un ciclo continuo de aprendizaje. Ese ciclo alimenta planificación, inversión en controles, priorización de proyectos y definición de límites de exposición aceptables por negocio y por unidad organizativa.

El marco COSO ERM exige que el desempeño del riesgo se mida en relación con objetivos definidos, porque **solo así puedes decidir si asumir, mitigar, transferir o evitar una exposición concreta**. Esa visión orientada a desempeño rompe la lógica puramente documental y te obliga a vincular cada decisión de riesgo con resultados tangibles, tanto financieros como no financieros.

La forma en que evalúas el riesgo condiciona la calidad de tus decisiones, por eso la estructura de COSO facilita un enfoque consistente. Si quieres profundizar en la aplicación práctica del modelo en tu organización, resulta clave entender **cómo gestionar riesgos con el modelo COSO en el día a día** y cómo conectar cada componente con la gobernanza y el reporting.

Sin objetivos claros, el desempeño en COSO ERM se vuelve un ejercicio teórico y desconectado del negocio. Debes definir metas estratégicas, operativas, de información y cumplimiento, y descomponerlas en objetivos específicos por área. Cada objetivo define qué riesgos son relevantes, qué métricas necesitas y qué nivel de tolerancia puedes aceptar.

Este enfoque obliga a que la función de riesgos trabaje muy cerca de estrategia, finanzas, TI y ciberseguridad. La evaluación ya no se centra solo en amenazas, sino en cómo esas amenazas alteran ingresos, continuidad de servicio, reputación o cumplimiento regulatorio.

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO



Categoría media ENS: requisitos y controles del Esquema Nacional de Seguridad

La categoría media ENS concentra el grueso de sistemas públicos y proveedores críticos, y exige una gestión madura de riesgos, gobierno y ciberseguridad. Entender bien sus requisitos te permite priorizar controles, dimensionar inversiones y evitar sanciones, incidentes graves y reproches de los órganos de control, mientras alineas tecnología, negocio y cumplimiento en una misma hoja de ruta.

La categoría media ENS se sitúa entre los sistemas básicos y los de nivel alto, y concentra servicios con impacto relevante en la continuidad operativa y la confianza ciudadana. **Su objetivo es asegurar que la degradación de la confidencialidad, integridad o disponibilidad no**

derive en daños inaceptables, pero sin exigir los controles extremos propios de sistemas muy críticos. Por eso requiere una aproximación de gestión de riesgos muy estructurada.

Para asignar la categoría media ENS debes valorar de forma sistemática el impacto potencial sobre confidencialidad, integridad y disponibilidad. **El análisis no se queda en la tecnología, se centra en cómo afectaría un incidente a los procesos de negocio, a las personas y a las obligaciones legales de la organización.** Esa visión integral evita infracategorizar sistemas que parecen secundarios, pero sostienen servicios prioritarios.

Los criterios habituales consideran el daño económico, la afectación a derechos de las personas, las consecuencias reputacionales y la interrupción de servicios esenciales. En categoría media, el daño esperado resulta relevante y sostenido en el tiempo, pero no alcanza escenarios catastróficos asociados a la categoría alta. **Por eso encaja en muchos sistemas transaccionales, portales ciudadanos, backoffice y soluciones compartidas entre varias entidades.**

Resulta clave alinear la categorización con lo que certifica el ENS y su alcance real dentro de la organización. El contenido sobre qué certifica el **ENS** en relación con los sistemas y servicios afectados te ayuda a evitar que queden fuera activos críticos aparentemente periféricos, como integraciones o servicios en la nube.

El marco de referencia obligatorio lo establece el Real Decreto 311/2022, que regula los principios básicos, requisitos mínimos y medidas de seguridad del Esquema Nacional de Seguridad en sistemas de información del sector público. **Este decreto vincula directamente el nivel de categorización con el conjunto de controles a implantar, el modelo de gobierno y la supervisión continua.**

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO



Entidades importantes en NIS2: requisitos y diferencias respecto a las esenciales

La categoría de entidades importantes en NIS2 redefine cómo gestionas riesgos, ciberseguridad y cumplimiento en sectores estratégicos. Comprender tus obligaciones, el alcance real de los controles y las diferencias frente a las entidades esenciales es clave para priorizar inversiones, evitar sanciones elevadas y usar el cumplimiento como palanca para fortalecer tu gobierno corporativo.

Como responsable de seguridad, riesgo o cumplimiento, necesitas saber si tu organización encaja en la categoría de **entidades importantes NIS2 y qué implicaciones reales tiene para tu modelo de gobierno**. Esta clasificación determina el nivel de supervisión, los plazos de reporte

de incidentes, la profundidad de los controles de ciberseguridad y la exposición regulatoria de tu Consejo de Administración.

La Directiva europea **NIS2** **define un marco común de requisitos de ciberseguridad y resiliencia** para sectores críticos y relevantes. Dentro de ese marco, distingue entre entidades esenciales y entidades importantes, con obligaciones similares pero con un nivel distinto de supervisión y de intervención de la autoridad competente.

Desde un punto de vista práctico, las entidades importantes NIS2 son organizaciones que prestan servicios relevantes para la economía y la sociedad, pero cuyo fallo tiene un impacto menor que el de una entidad esencial. Esta diferencia de impacto esperado justifica una supervisión más reactiva, aunque la exigencia de medidas técnicas y organizativas sigue siendo alta y alineada con buenas prácticas internacionales.

Los Estados miembros se apoyan en criterios armonizados para decidir si una organización encaja en esta categoría, combinando sector, tamaño y criticidad del servicio. **Suelo, facturación y número de empleados actúan como umbrales de entrada**, junto con el impacto potencial de una interrupción en la prestación de servicios digitales o físicos relevantes.

En general, muchas medianas y grandes empresas de sectores como servicios digitales, alimentación, fabricación de equipos o proveedores de servicios B2B entran como entidades importantes NIS2. Esto implica revisar tus datos de plantilla y volumen de negocio, pero también la dependencia que terceros y ciudadanos tienen de tus servicios para su actividad diaria.

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO



Cómo elaborar un inventario de activos de información eficaz

Un inventario de activos de información sólido reduce incidentes, acelera auditorías y permite controlar el riesgo tecnológico con criterio. Alinea a TI, negocio y cumplimiento, conecta la Gestión de la Seguridad de la Información con la realidad operativa y se convierte en la base para clasificar, proteger y monitorear cada activo crítico que sostiene tus procesos claves.

Un inventario de activos de información eficaz no es un listado técnico aislado, sino un mapa de valor del negocio. **Su objetivo es vincular cada activo con procesos, riesgos, propietarios, controles y cumplimiento regulatorio**, para que puedas priorizar inversiones en ciberseguridad, justificar presupuestos y demostrar trazabilidad ante auditorías internas y externas.

La primera condición para proteger algo es saber que existe. En cualquier programa de **gestión de la seguridad de la información** alineado con buenas prácticas, el inventario de activos se considera un requisito estructural. Sin un inventario actualizado, los análisis de riesgos, los controles y los planes de respuesta a incidentes se basan en supuestos incompletos.

Cuando vinculas el inventario de activos de información con procesos GRC, transformas una hoja de cálculo en un modelo vivo. **Cada activo se asocia a un responsable, un nivel de criticidad, dependencias técnicas y requisitos normativos específicos**, lo que facilita priorizar vulnerabilidades, seleccionar salvaguardas y justificar decisiones frente a la dirección o el comité de riesgos.

El inventario es además el punto de partida para una clasificación efectiva de activos, tanto por valor de negocio como por sensibilidad de la información. Si quieres profundizar en criterios, etiquetas y niveles, puedes apoyarte en el enfoque descrito en **cómo clasificar los activos de seguridad de la información** dentro de un marco corporativo.

El inventario de activos de información debe ir más allá de registrar servidores y aplicaciones. **Necesita capturar datos que permitan tomar decisiones de riesgo, cumplimiento y continuidad de negocio**, equilibrando detalle y mantenibilidad. Diseñar bien los campos desde el inicio reduce retrabajos y mejora la calidad del dato a lo largo del ciclo de vida del activo.

Para que el inventario sea accionable, cada activo debería incluir un conjunto estándar de campos. **Estos campos permiten relacionar la información con procesos, riesgos, contratos, proveedores y controles**, y dan coherencia al modelo de datos, incluso cuando distintos equipos colaboran en la actualización diaria del inventario.

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO

ESG INNOVA GROUP



ESG TOOLS

Transformación Digital para la gestión de Sostenibilidad mediante Software ESG con IA



GRI 1: fundamentos clave para elaborar informes de sostenibilidad

GRI 1 define los fundamentos que necesitas para estructurar informes de sostenibilidad rigurosos, alineados con expectativas de grupos de interés, estándares internacionales y marcos regulatorios, facilitando decisiones empresariales informadas y comparables, y preparando a tu organización para integrar la materialidad, la gobernanza ESG y la transparencia en la gestión diaria.

El estándar GRI 1 introduce los principios, definiciones y requisitos generales que sostienen toda la arquitectura de los Estándares GRI. Explica qué información debes divulgar, cómo aplicarla de forma sistemática y qué criterios garantizan que un informe de sostenibilidad sea comprensible, equilibrado, fiable y comparable para tus grupos de interés.

Cuando aplicas GRI 1, entiendes que un informe de sostenibilidad no es solo un documento, sino **una herramienta de gestión estratégica que conecta impactos, riesgos y oportunidades ESG**. Este enfoque impulsa decisiones de negocio más coherentes, mejora el diálogo con inversores y refuerza la confianza de clientes, talento y comunidades donde operas.

La arquitectura de los Estándares GRI combina GRI 1 con los estándares universales y temáticos, lo que exige comprender cómo se relacionan entre sí. Si quieres profundizar en esa lógica de conjunto, puedes apoyarte en una guía detallada sobre **cómo funcionan los estándares GRI**, sus requerimientos y conceptos principales, que ayuda a conectar la teoría con la operativa diaria.

GRI 1 se apoya en una serie de principios que orientan la elaboración de informes de sostenibilidad útiles. **Estos principios actúan como criterios de calidad** para seleccionar la información, estructurarla y revisarla antes de su publicación. Si los integras desde el inicio, reduces retrabajos y refuerzas la credibilidad frente a auditorías y revisiones externas.

Entre los principios clave de GRI 1 destacan la relevancia, la completitud y el equilibrio entre información positiva y negativa. **Aplicar relevancia implica priorizar los impactos significativos sobre detalles marginales**, lo que ahorra esfuerzo y evita informes extensos pero poco útiles. El equilibrio reduce el riesgo de greenwashing y mejora la confianza de los lectores.

La completitud exige cubrir el alcance adecuado de actividades, geografías y periodos. Este enfoque evita lagunas de información que puedan distorsionar el análisis.

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO



GRI 2: contenidos generales para reportar la información corporativa

GRI 2 define los contenidos generales que aseguran una información corporativa coherente, transparente y comparable. Aplicarlo bien refuerza la confianza de tus grupos de interés, facilita el cumplimiento regulatorio y ordena tu gobernanza ESG. Esta guía práctica te ayuda a entender sus requisitos, estructurar datos clave y convertir tu reporte en una herramienta real de gestión sostenible.

GRI 2 funciona como el esqueleto del informe de sostenibilidad, porque reúne los contenidos generales que explican quién eres, cómo te gobiernas y cómo decides. Sin esta pieza, los indicadores temáticos pierden contexto y tus grupos de interés no pueden interpretar bien los datos de desempeño ni tu grado real de compromiso con la sostenibilidad.

La primera capa de GRI 2 se centra en la identidad corporativa, la estructura del grupo y la cadena de valor. **Describir de forma clara tu perfil y operaciones crea el marco mínimo** para entender los impactos posteriores. Aquí defines sede, países donde operas, actividades principales, entidades incluidas y relación entre estados financieros y reporte de sostenibilidad.

Aplicar GRI 2 exige que expliques cómo determinas el alcance de la información corporativa. Describe si cubres solo la empresa matriz o también filiales, joint ventures y otras unidades relevantes. **Esta delimitación evita interpretaciones erróneas**, porque quienes leen el informe saben qué parte del grupo está detrás de cada dato que presentas.

Otro bloque clave de GRI 2 se centra en la gobernanza y el liderazgo en sostenibilidad. El estándar pide detallar la composición máxima de los órganos de gobierno, sus comités y sus responsabilidades relacionadas con ESG. **Cuando clarificas quién decide sobre sostenibilidad, demuestras coherencia entre discurso y estructura** y facilitas la rendición de cuentas interna.

GRI 2 también te pide explicar procesos de supervisión de riesgos, conflictos de interés, políticas de ética y mecanismos de denuncia. Aquí se observa si la sostenibilidad forma parte del control interno o si se trata de iniciativas aisladas. **Una gobernanza bien descrita genera confianza** porque muestra procedimientos concretos para gestionar impactos y riesgos materiales.

El estándar GRI 2 insiste en que tu estrategia y tus políticas se vinculen con impactos significativos sobre personas, medio ambiente y economía.

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO



GRI 3: cómo identificar y reportar los temas materiales

GRI 3 te ayuda a definir con claridad qué temas ambientales, sociales y de gobernanza son críticos para tu negocio, cómo priorizarlos y cómo reportarlos de forma consistente, comparable y alineada con las expectativas de reguladores, inversores y grupos de interés, para que tu memoria de sostenibilidad genere decisiones mejor informadas y resultados tangibles.

El estándar **GRI 3 establece el marco para identificar, priorizar y explicar los temas materiales** que una organización debe incluir en su reporting de sostenibilidad. Encaja dentro de la familia GRI 2021 y se centra en el contenido, no en los indicadores concretos. GRI 3 responde a dos preguntas críticas: qué asuntos importan de verdad y por qué esos asuntos son materiales para el modelo de negocio.

Con GRI 3, la materialidad se basa en los **impactos reales o potenciales que la organización causa, contribuye o está conectada a través de su cadena de valor**. Importa la magnitud, el alcance, la remediabilidad y la probabilidad del impacto, no solo la visibilidad mediática. Esta mirada evita sesgos cortoplacistas y ayuda a centrar recursos donde el negocio genera más efectos positivos o negativos.

Cuando trabajas con GRI 3, necesitas distinguir entre importancia para la empresa e importancia para las personas y el entorno. Esa discusión se enriquece si dominas las diferentes definiciones de materialidad que usan marcos como GRI, ESRS o SASB, algo que se explica con detalle en el recurso sobre **qué es la materialidad, por qué es importante y qué definiciones existen**.

GRI 3 propone un proceso estructurado en etapas que va desde la identificación amplia de temas hasta la validación final. **El objetivo es que puedas demostrar cómo llegaste a la lista de asuntos materiales**. Esta trazabilidad es crítica cuando dialogas con auditores, inversores o supervisores que quieren entender las decisiones detrás de tu memoria de sostenibilidad.

La primera etapa del estándar consiste en elaborar un listado amplio de temas potencialmente relevantes. Para ello, **GRI 3 recomienda analizar normativa, marcos internacionales, benchmarking sectorial, riesgos, oportunidades y feedback de grupos de interés**. Conviene incluir aspectos ambientales, sociales y de gobernanza ligados a toda la cadena de valor, desde proveedores hasta el fin de vida del producto.

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO



El camino hacia la Excelencia

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

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

+2.500 organizaciones

+25 años

+30 países

+240.000 usuarios

ESG INNOVA