ISOTools EXCELLENCE

EMPRESA EXCELENTE

Los mejores artículos técnicos publicados en el blog de ISOTools Calidad y Excelencia

Grupo ESGinnova

Sistemas de Gestión Normalizados

Modelos de Gestión y Excelencia

Plataforma tecnológica para la gestión de la excelencia

Recursos gratuitos

FEBRERO 2023

El camino hacia la Excelencia

Somos una empresa consultora que ayuda a las organizaciones comprometidas con la **calidad y la excelencia** a:

Optimizar sus modelos y sistemas de gestión, aportando soluciones innovadoras para la gestión de la estrategia, los procesos y las personas. Facilitando su aplicación, haciéndolos accesible, ágiles y medibles, y aportando resultados en el corto plazo, gracias a una plataforma tecnológica de desarrollo propio llamada **ISOTools.**

Servicio de llave en mano

Para que el el software pueda ser implementado y mantenido de forma rápida y sin incidencias, ofrecemos esta lista de servicios y servicios complementarios a todos nuestros clientes:

Capacitación

Los consultores expertos de ISOTools Excellence ofrecen una formación personalizada a los clientes para que se familiaricen rápidamente con el manejo del software.

Soporte

Contamos con profesionales disponibles a través de vía telefónica y online para resolver cualquier duda / incidencia que pueda surgir acerca del uso de la herramienta.

Consultoría

Nuestro equipo de consultores puede ayudarle a sacarle el máximo partido a ISOTools Excellence en su organización, antes, durante y después de la implementación.

Integración

Puede convivir con otras aplicaciones que ya estén funcionando en tu organización. Dispone de mecanismos para cambio de datos con soluciones de otros proveedores.

Adaptaciones

Toda organización posee sus particularidades, que muchas veces son la razón de la eficiencia de sus procesos. Por ello, ofrecemos la posibilidad de desarrollos a medida.

Migración de datos

El proceso de migración de datos tiene como objetivo principal importar a ISOTools Excellence los datos de su sistema de gestión actual.

Una herramienta a la medida de su organización

Estamos ante un sistema modular y altamente parametrizable, que se adapta a las necesidades de cada organización. Cuenta con un módulo base que sirve como cimiento de otros módulos de soluciones que cubren distintas áreas, pensados para facilitar y agilizar la gestión de gobierno, riesgo y cumplimiento. Sea cual sea su sector.

ISOTools Excellence aporta resultados en el corto plazo

Optimización del tiempo

50%
Menos de tiempo de resolución de una acción correctiva

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

75%
Menos de tiempo dedicado a recopilar y tratar indicadores

Optimización de los costes

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

75%
Menos de costes indirectos derivados de la gestión documental

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

Optimización del rendimiento

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

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

100%
Más de trabajadores implicados en la gestión del sistema

Control de Prevención de fugas de datos en la nueva ISO 27002.

Una fuga de datos se provoca cuando los datos que son sensibles están expuestos en público de forma involuntaria. **Esta exhibición de datos puede ocurrir en el tránsito, en sosiego o en usanza.**

Los datos que son expuestos en tránsito pueden contener los datos enviados por medio de correos electrónicos, salas de chat, llamadas, etc. Los datos expuestos en reposo resultan del almacenamiento en la nube configuraciones mal elaborados, también de una base de datos mal protegida o de dispositivos perdidos. **Los datos que son expuestos en uso, pueden proceder a ejecutar de capturas de pantalla, impresoras, unidades USB o portapapeles.** Una fuga de datos no se compra con una brecha de datos, aunque la primera pueda dar lugar a la segunda. La diferencia es que una fuga de datos no es el resultado de un intento de pillaje informático, sino que se origina por errores humanos.

Formas de prevenir fugas de datos

1. Las técnicas y tecnologías que utilizan para prevenir fugas de datos son, en la mayoría, los mismos que las que se utilizan para prevenir brechas también. En su mayoría las estrategias para advertir las pérdidas de datos sensibles inician con la ejecución de evaluaciones de riesgo (se incluyen las evaluaciones de riesgo de terceros) y la elaboración de políticas y procedimientos que se basan en dichas evaluaciones.

2. No obstante, para llevar una correcta **evaluación de riesgos,** primero hay que tener en cuenta es qué datos se tienen y dónde se encuentran ubicados.**Detección de clasificación de Datos:** Usa una solución que pueda detectar y clasificar datos sensibles de forma automática. Una vez realizado esto, se pueden eliminar datos **ROT** (redundantes, obsoletos y triviales) con el objetivo de optimizar las estrategias para proteger los datos. Catalogar los datos hace más sencillo asignar los controles adecuados y así monitorear cómo interactúan los usuarios con los datos sensibles. **Restringir los derechos de Acceso:** Siempre es una buena idea limitar el número de usuarios que tienen acceso a datos sensibles, ya que esto reduce el riesgo de sufrir una fuga.

3. **Filtrado del contenido de los Emails:** Utiliza una solución de filtrado de contenido que se apoye en una tecnología de inspección profunda de contenidos para encontrar datos sensibles en el contenido, las imágenes y los archivos adjuntos que se ubican en los correos electrónicos. Si este filtro se encuentran los datos sensibles, se enviará una alerta al administrador para que este pueda realizar verificación de la legitimidad del uso de estos datos.

Cómo verificar el Sistema de Gestión de Riesgos

La verificación del **sistema de gestión de riesgos** corresponde a la tercera etapa del **ciclo PHVA.** La idea de verificar la gestión de riesgos implica, primero que nada, **constatar que se haya completado el proceso de gestión del riesgo.**

Como ese proceso es transversal a la organización, es posible que no se haya completado el ciclo en la ejecución del proceso. De allí la importancia de verificar que cada etapa sea superada, desde identificar y analizar hasta evaluar y tratar los riesgos.

¿Qué más debemos verificar? Que se usen los métodos adecuados para la ejecución de cada una de las fases mencionadas. Por ejemplo, **en la identificación, ¿se están usando las fuentes adecuadas, o se omitió alguna? ¿la organización es lo suficientemente ágil para incluir los nuevos riesgos que surgen del contexto? También es menester revisar que los involucrados cuenten con las competencias pertinentes.**

Hay que tomar en cuenta que dentro de las organizaciones ocurren muchos cambios: constantemente hay nuevas funciones, procesos, productos y personas. Si hay individuos que se van de la empresa o que se integran a ella, necesitamos verificar que los roles y responsabilidades son asignadas acertadamente a personas que cuenten con las competencias requeridas para cumplir con sus funciones y actividades.

El análisis también es susceptible a la verificación. Si bien suelen estar en manos de comités especializados, existe la posibilidad de que se presenten fallas instrumentales o al emplear algún criterio. Por ejemplo, si utilizamos ofimática o alguna hoja en Excel **hay que verificar que las fórmulas que permiten hacer los análisis no se hayan dañado.** Si se usa una plataforma tecnológica, se verifica que se usen adecuadamente los principios de funcionamiento de las aplicaciones o de la tecnología que se ocupa para ello. El verificador, risk manager o control interno (además de auditores internos) tienen que conocer claramente cómo funcionan las herramientas para poder verificar que se usen correctamente.

La verificación nos lleva a enfocarnos en la evaluación, **hay que determinar si las evaluaciones están acordes a la política de gestión de riesgos de la organización, también si lo que se aceptó como riesgo está dentro del apetito por el riesgo.** Hay que considerar si se aplicaron niveles de riesgo altos, medios o bajos, si se abordaron adecuadamente los que se consideran mayores a lo señalado en el apetito por el riesgo... Además, se debe verificar que todos los elementos que fueron analizados en la evaluación de riesgos sean bien evaluados, puesto que podemos encontrar que hay niveles de análisis que probablemente den un resultado, pero si los comparamos con el mapa de calor, tal vez no haya coincidencias.

Cómo da cumplimiento la ISO 45001 al Decreto 1072

La **ISO 45001** es un estándar internacional para la gestión de la seguridad y salud en el trabajo. El objetivo de este estándar es mejorar la seguridad y salud de los trabajadores en todo el mundo al establecer un marco para la **gestión de riesgos y la prevención de accidentes en el lugar de trabajo.** El Decreto 1072 de Colombia, por su parte, es una regulación de seguridad laboral del gobierno colombiano.

El Decreto 1072, regula la seguridad y salud en el trabajo en Colombia y establece las obligaciones para las empresas en cuanto a prevenir accidentes y mejorar la seguridad en el lugar de trabajo. **La ISO 45001 se alinea con el Decreto 1072 en varios aspectos importantes.** En primer lugar, ambos establecen la necesidad de que las empresas establezcan una política de seguridad y salud en el trabajo, y establezcan objetivos para mejorar la seguridad en el lugar de trabajo. Ambos requieren que las empresas realicen evaluaciones de riesgos y establezcan controles para mitigar los

riesgos identificados. **La ISO 45001** también requiere la realización de auditorías internas periódicas para evaluar la eficacia de las medidas de seguridad y salud en el trabajo, lo que también está contemplado en el Decreto 1072.Otra área en la que se alinean ambos estándares es en la importancia de la participación y consulta de los trabajadores en la gestión de la seguridad y salud en el trabajo. La ISO 45001 establece que los trabajadores deben ser consultados y participar en la identificación de riesgos y en la toma de decisiones relacionadas con la seguridad y salud en el trabajo, mientras que **el Decreto 1072 establece que los trabajadores deben tener un papel activo en la promoción de la seguridad y salud en el trabajo y en la prevención de accidentes.**

Otro aspecto importante es la documentación, **El Decreto 1072 requiere que las empresas mantengan registros de los accidentes y enfermedades relacionadas con el trabajo,** así como de las medidas tomadas para prevenir accidentes y mejorar la seguridad en el lugar de trabajo, La ISO 45001 también requiere la documentación detallada de los procesos de seguridad y salud en el trabajo.

La ISO 45001 también promueve la continuidad de mejora en la gestión de la seguridad y salud en el trabajo, a través de la evaluación continua del desempeño y la identificación de áreas para mejorar. Esto es esencial para cumplir con el Decreto 1072, ya que **el gobierno colombiano establece la obligación de las empresas de mejorar continuamente sus sistemas de gestión de seguridad y salud en el trabajo.**

Además, la ISO 45001 promueve la colaboración con otras partes interesadas, como proveedores, clientes y autoridades reguladoras, para mejorar la seguridad y salud en el trabajo.

BPR (Business Process Reengineering). La reingeniería de procesos y mejora continua

En un entorno cada vez más competitivo, las organizaciones competitivas emplean gran parte de sus recursos en la optimización de procesos de negocio con el fin de ser más eficientes, rentables y con ello contar con **más capacidad para aportar valor al cliente.**

Existen una gran cantidad de metodologías para la **mejora de procesos** y quizás la más conocida sea el **Ciclo PHVA** o las **metodologías Lean** que han proliferado en los últimos años, sin embargo, existen más opciones igualmente válidas y con enfoques parecidos para alcanzar una eficiencia cada vez mayor.La reingeniería de procesos es una de las más utilizadas por las organizaciones en la búsqueda de la mejora continua.

¿Qué es BPR o Business Process Reengineering?

Se trata de una metodología que busca una mejora radical en el rendimiento empresarial en busca de la máxima eficiencia mediante el rediseño completo de los **procesos que aportan directamente e indirectamente al cliente.**

Al igual que otras metodologías de mejora continua, se basa en la búsqueda de la simplicidad y la eficiencia, rediseñando si es necesario totalmente un proceso o una dinámica de trabajo para conseguirlo, siendo en este punto donde se diferencia del resto.

Sus autores, Michael Hammer y James Champy apostaban por el rediseño radical y afirman que en esa radicalidad es donde está la clave para la mejora.

¿Mejoras radicales o mejoras paso a paso?

Es posible que **muchos lectores no comparten el concepto de radicalidad** en el cambio, pero, antes de emprender un proceso de mejora, sería importante reflexionar acerca de cómo llegó el proceso actual a ser como es.

En muchas empresas, sobre todo aquellas que están **comenzando con la mejora continua**, se puede ver como el proceso actual simplemente se ha ido conformando solo, fruto de agregar actividades y subprocesos (muchas veces con poco orden). El resultado es un proceso anticuado, lleno de desperdicios y con muchas posibilidades de ser un cuello de botella para otros procesos. En estos casos, el pensamiento de cambio radical, de reingeniería de procesos o Business Process Reengineering si comienza a tener sentido.

Gestión de activos según la ISO 27002

El objetivo de este punto de la norma **ISO 27001** es la preservación de los **activos de información** como soporte del negocio algunos ejemplos activos son los siguientes que mostraremos a continuación.**Recursos de información:** Las bases de datos y registros, documentación del sistema, los manuales de usuario, los materiales de capacitación, los diferentes procedimientos operativos o de soporte, los diversos planes de continuidad y contingencia, la información archivada, etc.

- **Recursos de software:** Los software de las aplicaciones, los sistemas operativos, las herramientas del desarrollo y la publicación de contenidos, proficientes, etc.

- **Activos físicos:** esta formado por el equipamiento informático, los equipos de comunicaciones, los medio u otros equipos técnicos, moblaje, lugares de instalación, etc.

- **Servicios:** prestación de servicios informáticos y de comunicaciones, proficientes generales.

Los activos de la información deben estar clasificados teniendo en cuenta la sensibilidad y criticidad de la información que contenga o que cumplan con **los objetivos de señalar cómo ha de ser trata y protegida la información.**

Los pasos de la clasificación tienen que predecir y examinar el hecho de que dicha clasificación de un ítem de información determinando no es precisamente tiene que mantener invariable por siempre, y que se puede variar según la política explícita por la propia organización. **Es ineludible que se considere las cantidades de categorías para definir la clasificación dado que los esquemas son demasiado complejos y estos pueden volverse difíciles o resultar poco prácticos.**

Responsabilidad sobre los activos

Los activos de la información según la norma **ISO 2700,** tienen que ser comprendidos y tener asignados un responsable y deberán identificar a los responsables o propietarios para todos los activos y asignarles la responsabilidad del mantenimiento en los dibersos controles adecuados.La ejecución estos controles específicos puede ser encargada por el mismo propietario de forma provechosa, Sin embargo, el propietario permanece como el responsable de la adecuada resguardo de los activos.El término identifica a individuos o entidades de forma comprometida, que cuente con la aprobación por parte de la dirección, para el controlar la producción, desarrollos, mantenimientos, la utilización y seguridad de los activos. El vocablo propietario no figura que la persona disponga de los derechos de propiedad reales del activo.

Mejora continua del PGR

El pensamiento basado en riesgos es vital para el éxito sostenido. Las empresas que transitan el éxito sostenido requieren un proceso de **gestión riesgo** eficaz y con el compromiso de la **mejora continua.** A continuación se explica como se relacionan estos conceptos.**El proceso de gestión de riesgos según la ISO 31000:2018**

- **La norma ISO 31000:2018** establece un marco para la gestión de riesgos en todo tipo de organizaciones. El **proceso de gestión de riesgos** según esta norma se compone de varios pasos:**Establecimiento del contexto:** se establece el alcance y los objetivos de la gestión de riesgos, así como el contexto en el que se llevará a cabo.

- **Identificación de riesgos:** se identifican los riesgos potenciales que pueden afectar a los objetivos de la organización.

- **Análisis de riesgos:** se para determinar su probabilidad y su impacto.

- **Evaluación de riesgo:** que permite ubicar al riesgo en una sección del mapa de calor y en consecuencia conocer el nivel de riesgo

- **Tratamiento de riesgos:** se establecen medidas para controlar o mitigar los riesgos evaluados.

- **Comunicación y consulta:** se comunican los resultados de la gestión de riesgos a las partes interesadas y se lleva a cabo una consulta con ellas.

- **Monitoreo y evaluación:** consiste en monitorizar los riesgos y las medidas de tratamiento implementadas para medir su eficacia.

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO

Matriz IPER para ISO 45001. Estructura e instrucciones para completarla.

Las matrices de riesgos son instrumentos de gran utilidad ya que nos permite identificar todo tipo de riesgos concurrentes con la actividad de la organización. El uso de esta herramienta está muy desarrollado, principalmente en las empresas certificadas por la norma **ISO 45001,** esta nos muestra en su punto 6.1 que se ha ejecutar una serie de acciones para plantear los riesgos y oportunidades, con el objetivo de aseverar la obtención de objetivos, evitar riesgos y, en resumen, conseguir la mejora continua del **(SGSST).** Todo ello pasa por la identificación de riesgos y oportunidades y la evaluación de su impacto en la empresa y contexto para su acción. **Una de los equipos más útiles con las que cuentan las sociedades para identificar, evaluar y gestionar los riesgos a los que se enfrentan es la matriz de riesgos.**

Esta específicamente es un documento que permite realizar la identificación de las actividades que realiza una empresa, los riesgos inherentes a las mismas y la probabilidad de que estos riesgos se concreten. **Para que sea eficaz es preciso que colaboren en su confección todas las partes interesadas, procesos y áreas productivas, operativas y funcionales de la organización además de que sea sujeta a revisiones periódicas.**

1. **Se debe identificar los riesgos y oportunidades** que se presentan tanto en los procesos de una organización, como aquellos referentes al contexto interno o externo que logren afectar al sistema o a sus partes interesadas. Para tener en consideración revisemos los siguientes puntos:

Seguimiento general: El contexto interno y externo, necesidades y expectativas de las partes interesadas, además del alcance del **SGSST.** Determinar qué estimamos como riesgo u oportunidad: **peligros, riesgos y oportunidades para la SST** y el sistema de gestión, los requisitos legales y otros que pueden impactar. Se han de tener en cuenta aspectos como: estrategia, estructura, recursos humanos, procesos, competitividad, aspectos sociales y políticos, innovación, desarrollo tecnológico, proveedores entre otros.

1. Se deberán evaluar los riesgos y oportunidades, en contextos normales, como en un escenario de emergencia (6.1.2.3 Evaluación de las oportunidades para la **SST**).

2. Este punto es a la acción. Se deben identificar y programar todas las acciones derivadas de los distintos análisis de riesgos y oportunidades (procedimientos, instrucciones, formaciones) y evaluar su eficacia. (6.1.4 Planificación de acciones).

Normas ISO de Gestión de Riesgos. ¿Cuáles son y por qué tenerlas en cuenta?

En lo que se refiere a la **Gestión de Riesgos, hay muchas normas ISO que los expertos del área deben estar al tanto**. Estas normativas **están encaminadas a establecer la gestión de las empresas en diferentes sectores** y son expresadas por el Organismo Internacional de Estandarización (ISO). Su beneficio reside en que funcionan como un lenguaje común entre organizaciones. De este modo, la ejecución de una ISO permite a una organización evidenciar que cumple con unos requisitos de calidad que son registrados internacionalmente. No obstante, son diversas las normas de gestión de riesgos, si más, hay algunas cuya comprensión es indispensable para los profesionales del sector.

A continuación, nombraremos algunas de las normas relacionadas con la gestión de los riesgos.

ISO 31000 Gestión de Riesgos

Evidentemente, la norma más significativa en **Gestión de Riesgos es la ISO 31000**. Esta norma instaura las directrices y principios que debe cumplir un **Sistema de Gestión de Riesgos**. La actual versión actualizada de esta norma es del año 2018.

ISO 9001

Esta normativa ordena cómo debe ser un **Sistema de Gestión de la Calidad** en la organización. En su última versión, I**SO 9001:2015**, incluye el pensamiento basado en riesgos.

Norma ISO 55000 de Gestión de Activos

A lo referente a la ISO 55000 **es conjunto de tres normas** que aprueban establecer un Sistema de Gestión de Activos en las empresas. Se define como de una norma de Gestión de Riesgos **principalmente beneficiosa en el ámbito económico**. El estándar está encaminado a todo tipo de activos, incluyendo los intangibles.

ISO 27001 Seguridad de la Información

Otra norma que corresponde conocer es la ISO 27001. Este estándar internacional forma las claves para establecer un **Sistema de Gestión de Seguridad de la Información (SGSI).** En otras palabras, ayuda a resguardar toda la información sensible que manejan las organizaciones, como por ejemplo pueden ser los datos de los clientes.

Gestión de riesgos en proyectos como parte del Riesgo Operacional

Una aproximación al riesgo operacional

En la **ejecución de los procesos**, las organizaciones están expuestas dificultades que tienen el potencial de afectar su operación normal, además de **exponer su imagen y afectar su capacidad de crecimiento** o peor aún de mantenerse ofertando bienes y servicios al mercado. El riesgo se puede definir como

"El potencial de pérdida financiera o daño a la reputación que puede surgir de problemas internos, incluyendo fallos en los procesos, errores humanos, o problemas con sistemas o tecnologías."

En otras palabras, **se refiere a los riesgos asociados con la ejecución de actividades de operación de una empresa.**

Estos riesgos son los resultados de errores humanos, fallas de sistemas, actos de mala fe o cambios en los entornos reguladores o de mercado. El riesgo operacional puede tener un impacto directo en los ingresos, los beneficios, la reputación y la capacidad de una empresa para cumplir con sus **responsabilidades reguladoras**.

Tipos de riesgos operacionales

Los tipos de riesgos operacionales incluyen:

1. **Errores humanos**
2. **Fallos en los procesos.**
3. **Problemas con las TIC.**
4. **Incumplimiento de regulaciones y leyes.**
5. **Fraude y corrupción.**
6. **Desastres naturales y eventos inesperados.**
7. **Mala gestión de proyectos.**
8. **Problemas de ciberseguridad, privacidad y seguridad de la información.**
9. **Interrupciones en la cadena de suministro y logística.**

Una de las actividades más comunes para gestionar una organización es la gestión de proyectos, los cuales se emprenden principalmente para Alcanzar objetivos estratégicos.

Certificado ISO 14001. Claves para conseguirlo.

La certificación **ISO 14001** tiene como objetivo de **apoyar las diferentes aplicaciones de un plan ambiental en cualquier organización.**

Esta norma ha sido creada por la organización internacional para normalización, este es una red internacional de institutos de normas nacionales que trabajan en alianza con los gobiernos, la industria y los diferentes representantes de los consumidores. **La norma ISO 14001 se puede utilizar como un complemento para proteger el medio ambiente.**

La realización de la norma **ISO 14001**, proporciona controles de las actividades, productos o servicios de una empresa y la interacción con el medio ambiente. A su vez, puede aumentar la viabilidad a largo plazo de la empresa y una mayor consideración de su valor patrimonial. Si las organizaciones tienen interés en conseguir la certificación ISO 14001, deben cumplir con los parámetros establecidos de forma

internacional relativos al sistema de gestión de medio ambiente. **Esta certificación se puede obtener con el objetivo de generar nuevos negocios, debido a que resulta interesante acceder un contrato, vinculaciones y estar a un buen nivel competitivo en el mercado.**

Debemos tener en cuenta los siguientes puntos:

- Contexto de la empresa.Liderazgo.Concepto de riesgos y oportunidades.Ciclo de vida.Controles de documentos.Evaluación de desempeño ambiental.Orientación a la mejora continua de los procesos.**Para comenzar con la implementación, se puede ejecutar con el personal o con recursos internos, además de contratar una consultoría ambiental ISO 14001.**

- Existen diversos cambios en la gestión de los recursos que se llevan a cabo en la organización. Un ejemplo claro, tiene que mejorar las gestiones de aguas servidas y blancas, donde se busca disminuir la producción de residuos.

- Es importante que cambie la difusión del tema dentro de los negocios. **El liderazgo,** la dirección tienen que involucrarse en el tema, e incrementar la importancia de todos los procesos de negocios.

- Si decide implementar la norma **ISO 14001**, habrá que revisar procesos, crear cultura con el personal, involucrar a la dirección, se puede iniciar un proceso de auditoría interna con el objetivo de verificar la implementación. **El sistema de gestión ISO 14001 contiene reglas que igualan los parámetros de trabajo en el tema ambiental, la auditoria busca cumplir con las reglas y las pautas.**

Resumen de la ISO 31000 para la Gestión de Riesgos

La **ISO 31000** es una norma internacional cuyo objetivo es la **gestión del riesgo.** Al suministrar los elementos integrales y orientaciones, **esta norma es de bastante utilidad y a las organizaciones con sus análisis y evaluaciones de riesgos.**

Sea que trabaje en entidades públicas, privadas o comunitarias, se logran beneficiar de **ISO 31000**, porque esta norma es aplicada a la mayoría de las actividades de comercio, donde incluye la planeación, las operaciones de gestión y los procesos de la comunicación. **Todas organizaciones manejan el riesgo en cierta medida, las recomendaciones de las mejores prácticas de esta norma internacional se desenvolvieron para mejorar las técnicas de gestión y asi garantizar la seguridad y la protección en todo momento en el área de trabajo.**

Las diferentes organizaciones, afrontan de manera constante a imprevistos de todo tipo, pueden ser económicos, técnicos o estratégicos. Las organizaciones no pueden eliminar estos riesgos sin más, sino que tienen que contender con ellos. Los **SGR** suministran directivas y procesos que indican como toma decisiones en situaciones de riesgo para limitar los daños potenciales lo mejor posible. **Hay que tener en cuenta que la norma ISO 31000 no considera todos los riesgos como negativos, sino que, de acuerdo a esta, también hay riesgos positivos.** Es más, siempre que surja la perplejidad de que un acontecimiento futuro pueda provocar que la empresa se desvíe de sus objetivos, se hablará de un riesgo.

Al ejecutar la implementación, los principios y directivas de la ISO 31000 en su organización, **tendrá la capacidad de mejorar la eficiencia operacional, gobernanza y confianza de las partes interesadas, a su vez que minimiza las pérdidas.** Esta norma internacional también le ayuda a impulsar el desempeño de salud y seguridad, establecer un dinámico fundamento para la toma de decisiones y incitar la gestión proactiva en todas las áreas.

Principios para la gestión de riesgos de la ISO 31000

- **Implementar un valor:** hace que sea sencillo el cumplimiento de los objetivos que se plantean y de los requisitos legales que se asocian a la seguridad, salud laboral, protección ambiental, entre otros.

- **Integración en los procesos de la organización:** No es una gestión que se realiza separadamente, por el contrario, está implicada en las diversas actividades primordiales de la organización.

Enterprise Risk Management (ERM). ¿Qué es y cómo implementarlo en la organización?

La gestión de riesgos y oportunidades son uno de los factores diferenciadores de las organizaciones, el hecho de que se gestionen no garantizan el éxito (porque esto depende de muchos factores), pero si no se gestionan, el fracaso de la propuesta es inminente. También hay que destacar que muchas organizaciones son nativos del cambio y, por lo tanto, han sabido gestionar el riesgo y las oportunidades de forma natural, no obstante el uso de marcos normativos son muy útiles, de manera que esas lecciones aprendidas sean de fácil aplicación en el resto del ecosistema, porque un ecosistema organizacional con riesgos debidamente tratados también es parte del recorrido del camino del éxito, pues, las organizaciones no surgen solas ni se sustentan de la nada.

5 marcos normativos para gestionar riesgos y oportunidades

Los marcos normativos más comunes en los que se afianzan las organizaciones para abordar los riesgos son:

1. COSO: es un acrónimo que se refiere al **Comité de Organización y Supervisión de los Sistemas de Control Interno (COSO)**, corresponde al marco de control interno de la Comisión de Valores de los Estados Unidos en 1992 y su última versión es de 2017.

2. ISO 31000: Este marco normativo internacional proporciona una guía para la gestión de riesgos y está diseñado para ser aplicable a cualquier organización, independientemente de su tamaño o sector. Es de la ISO y su última versión es del 2018.

3. **NIST**: El marco de seguridad de la información del Instituto Nacional de Estándares y Tecnología (NIST) es un marco de seguridad de la información ampliamente utilizado para la gestión de riesgos en el sector de la tecnología y cuenta con varias publicaciones especiales que ayudan a la mitigación de riesgos. Estas publicaciones están en constante revisiones.

4. Basilea III: es un conjunto de regulaciones y recomendaciones sobre la regulación bancaria desarrolladas por el Comité de Basilea sobre Supervisión Bancaria (BCBS). Estas regulaciones fueron diseñadas para mejorar la estabilidad y la calidad de los bancos y las finanzas globales. Su implementación está vigente desde el 01 de enero de 2019.

5. COBIT: Es un marco normativo empleado para la gestión de los riesgos relacionados con la tecnología de la información.

Gestión documental en ISO 45001. ¿Qué dice la norma al respecto?

Se debe entender y anotar en primera instancia, lo primero es que el **estándar publicado en febrero de 2018 excluye la selección entre registros y documentos**. Uno y otro, ahora, se nombran "*información documentada*".Asimismo, en este momento **ISO 45001 todavía accede a permisividad en el cómo, qué y cuándo documentar un proceso**. Lo cual no es solo para aproximar a formas más recientes de comunicación, como audio, video y otros registros electrónicos, sino para permitir a la organización la habilidad de aprovechar información conveniente, conservar versiones actuales con más facilidad y facilitar capacidad de acceso y disposición más amplia, aminorar los costes añadidos a la obligatoriedad de la documentación en ISO 45001.

Conforme con la información disposición 7.5.3 de ISO 45001, "*la información documentada solicitada por el sistema y el estándar debe*

chequearse para avalar que esté disponible y sea apropiado para su uso cuando y donde sea necesario, y que esté apropiadamente resguardada contra la pérdida de integridad o el uso indebido"Por lo tanto, ¿cuál sería la documentación necesaria y **obligatoria que ISO 45001** a la que debemos de fijarnos? Podemos informar que hoy en día, **hay una lista completa de los documentos requeridos** y también de algunos que, no siendo obligatorios, son de uso habitual.

Lista de documentación obligatoria en ISO 45001

Varias empresas **forman excesivos documentos**, tratando de no incidir en una **No Conformidad** que dificulte el logro de la certificación. Esto si puede mostrar algún beneficio, pero en términos generales, representa una carga administrativa para los profesionales en seguridad y salud en el trabajo.

Las empresas deberían aprovechar aquella oportunidad que ofrece la norma de establecer **un sistema manejable, práctico, eficiente y provechoso**. De ahí la importancia de contar con una lista detallada de la **documentación obligatoria** en ISO 45001.

No obstante, como ya lo hemos registrado, la norma no hace la selección en relación con documentos y registros, para proporcionar el conocimiento de quienes trabajan en la migración desde OHSAS 18001, aquí vamos a presentar una lista en dos secciones, iniciando por los documentos:

1. Alcance del Sistema de Gestión de Seguridad y Salud en el Trabajo.

2. Política de seguridad y salud en el trabajo.

3. Definir los roles y responsabilidades dentro de la organización.

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

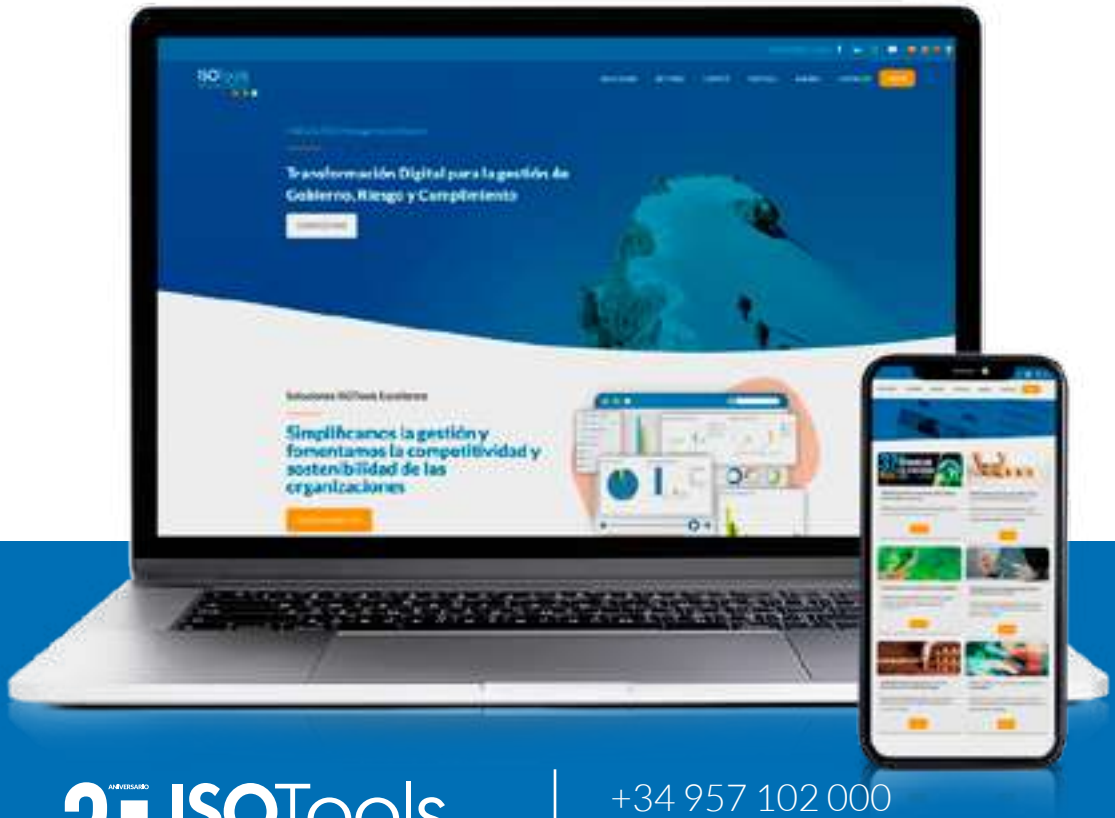
+30 países

+240.000 usuarios

PLATAFORMA TECNOLÓGICA PARA LA GESTIÓN DE LA EXCELENCIA

Software que agiliza los sistemas de gestión y los modelos de excelencia de la gestión empresarial

Es un sistema modular, flexible, altamente parametrizable y adaptable a las necesidades de cada empresa u organización independientemente del tamaño y del sector en el que opere.



+34 957 102 000
www.isotools.us