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

ENERO 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

Gestión de Riesgos Según ISO 45001. Tipos de riesgos y cómo tratarlos adecuadamente.

Los peligros y riesgos en el escenario laboral están presentes en todo nivel y en cualquier sector económico, por lo que es necesario poder identificarlos, tratar los riesgos eficazmente y colocar controles para poder prevenir los accidentes de trabajo y las enfermedades ocupacionales. **La ISO 45001, en su versión 2018**, se basa en el ciclo de mejora continua PHVA, nos muestra una metodología para poder gestionar los riesgos en seguridad y salud en el trabajo.

La gestión de riesgos es un proceso efectuado por la alta dirección de la organización y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de objetivos. Para gestionarlos adecuadamente debemos tomar en cuenta 6 factores, lo cual explicaremos a continuación.

Misión, visión y objetivos

Misión, visión y objetivos, conocer los procesos a todo nivel, establecimiento de **Política y lineamientos SST, Identificación de riesgos**, Evaluación de riesgos, Medidas de control. Los objetivos estratégicos, misión, visión de la organización deben estar bien definidos, puesto que son los pilares para las decisiones y delegación de responsabilidades en la gestión de los riesgos en todos los niveles. Estos representan los valores y el compromiso de la organización para la obtención de objetivos.Al tener claro la estrategia y los objetivos se plasmará posteriormente la **Política de Seguridad y salud en el trabajo,** donde los representantes de la organización manifestarán su compromiso con la identificación, evaluación y de los peligros y riesgos, y la mejora continua.

Conocer los Procesos a todo nivel

En la **gestión de los riesgos laborales** es necesario conocer los procesos y subprocesos claves en los cuales se identificarán los peligros y riesgos en la estructura de la organización, los cuales deben estar identificados y plasmados en un mapa de procesos para facilitar la gestión de los mismos.**Establecimiento de una política y lineamientos SST**

Al establecer la política de Seguridad y Salud (SST) se establecen los objetivos en seguridad y el compromiso de la empresa con la gestión de riesgos, deben considerarse los siguientes puntos:

- **Objetivos**: Se debe establecer su alineación con los objetivos estratégicos de la organización y gestionar.

Políticas que no te deben faltar en tu SGSI

Las políticas de seguridad de la información son reglas que tenemos que cumplir todo el personal relacionado con una empresa. Así se garantiza la **rectitud, la privacidad y la disponibilidad de las infraestructuras informáticas y de los datos que contienen**. En este artículo se explica **qué son las políticas de seguridad informática y sus aplicaciones prácticas** en la empresa en distintos ámbitos.

Una política de **seguridad de la información** es un documento que instituye los designios y objetivos de una empresa en relación con este componente. Un ejemplo claro es que una política puede precisar las **necesidades de establecer contraseñas seguras que cumplan con explícitos requisitos** para toda clase de dispositivos, y especialmente para los móviles que se utilizan externamente de las instalaciones. A diferencia de los procesos y procedimientos, las políticas no contienen instrucciones específicas y puntuales sobre cómo llevar a cabo estas actividades.

Las políticas son un conjunto de **normas importantes decretadas** por una organización con el objetivo de garantizar que todos los empleados, usuarios o partes interesadas las acojan y delineen procesos y procedimientos que alcancen estos principios de modo ordenado.

La **ISO 27001** no cuenta las dificultades específicas que deben abordarse en la política comprendiendo que cada organización tiene sus propias metas y exigencias. Pero sí debe proporcionar un marco cerca del que se debe trabajar.

¿Cómo debería ser una Política SGSI?

Una política de seguridad de la información apropiada debería:

- Suministrar una **directriz** clara sobre el tratamiento de la seguridad de la información en la organización.
- Enseñar los **objetivos** del sistema.
- Agregar información sobre cómo se efectuará junto con los objetivos comerciales y con los requisitos establecidos, legales. Adjudicarse a los **compromisos** de optimar de forma continua el SGSI.
- Determinar el **alcance** del sistema.
- Establecer los **responsables** de las operaciones, las coordinaciones en el día laboral de la realización general, las evaluación de riesgos y de las prácticas de auditorías, intervenciones e indagación de incidentes.

Estándares de sostenibilidad GRI asociados a la Seguridad y Salud Laboral

Los estándares de sostenibilidad GRI simbolizan las mejores prácticas que se pueden aplicar para comunicar los impactos generados por una organización en el ámbito económico, ambiental y social.

Cuando las organizaciones llevan a cabo la **elaboración de informes de sostenibilidad** recurren a estos estándares para proporcionar información sobre sus aportaciones en el desarrollo sostenible.Los Estándares GRI se organizan en tres series:

- 200 (aspectos económicos).
- 300 (aspectos ambientales).
- 400 (aspectos sociales).

¿Qué estándar de sostenibilidad GRI está asociado a la Seguridad y Salud Laboral?

El estándar de sostenibilidad GRI que está asociado a la Seguridad y Salud Laboral es el GRI 403, se trata de un Estándar GRI temático de la serie 400 (aspectos sociales).

Este Estándar de sostenibilidad GRI asociado a la Seguridad y Salud Laboral considera a los siguientes trabajadores, de los cuales se espera que la organización se implique en la protección de la seguridad y salud laboral.

- Todo trabajador que sea empleado, es decir, aquellas personas que tengan un vínculo laboral con la organización según esté establecido en la legislación aplicable.

- Todo trabajador que no sea empleado pero su trabajo está controlado por la organización.

- Todo trabajador que no sea empleado y que su trabajo no está controlado por la organización pero que están sometidos a impactos relevantes para la seguridad y salud laboral por el desarrollo de la organización y las relaciones con ella.

Las organizaciones que determinen que la seguridad y salud laboral se encuentran entre sus temas materiales, **estarán obligadas a mostrar el enfoque de gestión de estos temas haciendo uso de los contenidos del GRI 103** y también los contenidos sobre el enfoque de gestión de este ámbito.

ISO 45001 y la Ley 29783. Cómo darle cumplimiento.

La norma **ISO 45001** establece un marco de referencia para un sistema de gestión de Seguridad y Salud en el trabajo en la gestión de los riesgos laborales y se basa en el ciclo de mejora continua, manteniendo una correlación con otros sistemas de gestión. Esta normativa se publicó en el año 2018 **para sustituir a OHSAS 18001**, pues esta es una norma no pertenece a la **familia ISO**, y viene cargada de potencial para disminuir el número de accidentes, salvar vidas y aumentar la moral de los trabajadores.**La Ley 29783, Ley de Seguridad y Salud en el Trabajo,** es el requisito fundamental que **da las directrices para la gestión de Seguridad y Salud para las entidades particulares y privadas en el Perú, es obligatorio y sujeto a sanciones económicas** por no implementarlas adecuadamente.

En ella se establecen criterios generales para la protección de los trabajadores en las distintas empresas peruanas. **Es un requerimiento obligatorio de esta ley que todas las empresas**

tanto públicas como privadas implementen un sistema de gestión de seguridad y salud en el trabajo para la prevención de los accidentes, incidentes y enfermedades ocupacionales generando una cultura de prevención de riesgos, planificando las actividades a través de planes y programas de seguridad y salud, evaluando los riesgos y colocando controles para estos mismos de forma de minimizar el impacto de cada riesgo para las diferentes actividades, luego generando mecanismos de verificación de los mismos a través de mecanismos como la supervisión o auditorías, inspecciones periódicas que permitan obtener datos para la mejora continua de los procesos en el sistema de gestión.

La ley 29783, ley de Seguridad y Salud en el trabajo, tiene los siguientes principios como base:

- **Asegurar un compromiso** visible del empleador con la salud y seguridad de los trabajadores.
- **Lograr coherencia** entre lo que se planifica y lo que se realiza.
- **Propender al mejoramiento continuo**, a través de una metodología que lo garantice.
- **Mejorar la autoestima y fomentar el trabajo en equipo** a fin de incentivar la cooperación de los trabajadores.
- **Fomentar la cultura de la prevención** de los riesgos laborales para que toda la organización interiorice los conceptos de prevención y proactividad, promoviendo comportamientos seguros.

Los 50 artículos más Excelentes de ISOTools en 2022

Otro año más nos llena de orgullo presentaros los **50 Excelentes de ISOTools.** Esta publicación anual consiste en una recopilación de los 50 artículos más vistos y valorados durante el pasado año 2022.

De este modo, podrás disponer de este contenido de valor de manera unificada en un ejemplar único y gratuito.

Desde **ISOTools Excellence, como parte del grupo ESGinnova,** consideramos que el conocimiento es uno de los elementos principales que podemos ofrecerte. Año tras año, hemos conseguido posicionarnos como fuente de conocimiento en la materia con nuestras publicaciones diarias.

Con el fin de facilitar la lectura y de que puedas contar con el conjunto de artículos seleccionados en un solo documento, ponemos a tu

disposición esta edición. Hemos preparado un ejemplar en formato PDF, con enlaces al blog Calidad y Excelencia, por si deseas realizar la lectura desde nuestra web **www.isotools.us**. Nuestro blog es totalmente accesible para que aquellas personas con dificultades sensoriales vinculadas con la visión. De esta forma el contenido puede ser disfrutado sin requerir de la lectura por parte de un tercero.

Estos son algunos de los títulos que vas a encontrar dentro de este recopilatorio:

- Éxito en la 28ª Semana de la Salud Ocupacional de Colombia.
- ISOTools obtiene el certificado en Continuidad de Negocio ISO 22301.
- Resumen de nuestro paso por PERUMIN 2022.
- ISOTools celebra un evento sobre Tendencias y Claves HSE en empresas Sostenibles en República Dominicana.
- ISOTools presente en el webinar «Experiencia de Éxito Empresarial» organizado por TALMA.
- ISOTools presente en la Jornada de Capacitación de Calidad organizada por la Municipalidad de Vitacura.
- ISOTools colabora con la Cámara de Comercio e Industria de Arequipa.
- ISOTools presente en Transfiere 2022. Principal encuentro i+D+i del sur de Europa.

QUIERO SEGUIR LEYENDO ESTE ARTÍCULO

Buenas prácticas en la gestión de Compliance

El compliance (cumplimiento), es la práctica de adherirse al **marco legal y regulatorio** que ha sido establecido por un gobierno u organización. Existen un conjunto de **reglas y regulaciones que rigen cómo operan las organizaciones** dentro de su industria. Estas tienen como objetivo **garantizar que las organizaciones cumplan con la ley** mientras operan dentro de su industria. Los estándares de cumplimiento los establecen las propias empresas, pero también dependen de agentes externos, como agencias gubernamentales u organismos reguladores, para hacerlos cumplir.

La ley de cumplimiento regula cómo las empresas realizan negocios **con clientes, empleados, proveedores y otras partes interesadas** para cumplir con requisitos específicos. Por ejemplo, las normas de cumplimiento pueden exigir que una empresa proporcione un seguro de salud a los empleados que trabajan más de 40 horas a la semana; esas regulaciones serían aplicadas por una agencia como el Ministerio de Trabajo en España o alguna otra

entidad que tenga autoridad sobre estos asuntos dentro de su jurisdicción.

El hecho de **no tener un proceso de control del cumplimiento puede traer consecuencias** de extrema gravedad para la organización, no solo económicas, también de pérdida de negocio, imagen corporativa, reputación o apoyo de accionistas y otras terceras partes que son necesarias para la continuidad de la organización. Esto hace que las organizaciones deban establecer estrategias para conseguir un cumplimiento excelente tanto en el ámbito legal como normativo. En este sentido, seguir una serie de buenas prácticas será de especial utilidad.

Buenas prácticas relacionadas con el cumplimiento

1. Crea una estructura de datos común

El primer paso para evitar riesgos por cumplimiento es construir una estructura de datos común. Una estructura de datos común es una base de datos que contiene toda la información relevante para los esfuerzos de cumplimiento normativo de una organización. Esto incluye información sobre regulaciones, cambios que pueden ocurrir y prácticas generales de gestión de riesgos. Para ello será de especial utilidad contar con un software que permita una gestión excelente de matrices de riesgos, incluido el legal.

2. Rastrea los cambios regulatorios

Una vez que tengas construida su estructura de datos común, es hora de comenzar a rastrear los cambios regulatorios. Los reguladores cambian constantemente las reglas para asegurarse de que las empresas aprovechen al máximo sus oportunidades comerciales y al mismo tiempo cumplan con las regulaciones.

Control de Encriptación de datos en la nueva ISO 27002

Como se sabe, en el mes de febrero del presente año, fue publicado por parte del comité técnico de seguridad de la información, ciberseguridad y protección de la privacidad, por medio de la organización de estándares internacionales, la norma **ISO/IEC 27002:2022 seguridad de la información, ciberseguridad y protección de la privacidad**.

Cabe mencionar que la **ISO 27002** no es el estándar certificable, esta norma es un complemento para implementar las mejores prácticas y controles más eficaces para prevenir ataques o la vulneración de la privacidad de la información de los clientes y las partes interesadas. Dentro de los principales cambios que ofrece la versión 2022 de la norma ISO 27002, se tienen los siguientes:

La actualización presenta cuatro secciones de forma organizacional y dos anexos:

1.1.— **Cláusula 5: Controles Organizacionales.**

1.2.— **Cláusula 6: Controles de Personas.**

1.3.— **Cláusula 7: Controles Físicos.**

1.4.— **Cláusula 8: Controles Tecnológicos**.

Los dos anexos se ocupan para el uso de atributos y de la correspondencia con los controles de la anterior edición de la ISO 27002 del año 2013.

1.5.— La nueva edición, ISO 27002:2022, **reduce el número de controles de 114 a 93**.

1.6.— **La implementación de los controles es ahora justificada en esta actualización con una tabla de atributos asociados con el control y con su función,** los cuales pueden ser de tipo preventivo, de detección o correctivos.

La actualización a ISO 27002:2022 **se agregan 11 nuevos controles**:

1. Inteligencia de Amenazas.

2. Seguridad de la información en la nube.

3. Continuidad del negocio.

4. Seguridad física y su supervisión.

5. Configuración.

Capacitaciones SST según ISO 45001. ¿Qué hay que tener en cuenta?

La **Norma 45001** cumple su objetivo que es facilitar a una empresa la investigación de alto rango sobre los asuntos significativos que pueden inquietar, hasta tal punto de forma positiva como de forma negativa, y cómo se tramita sus responsabilidades de salud y seguridad en el trabajo hacia sus trabajadores.La norma 45001, así como otras directrices, **implica que se certifique que los trabajadores se hallen capacitados y sean consecuentes de lo que deben hacer para respaldar el sistema de gestión**.

Debe entregarse la capacitación ideal y competente para que el trabajador lleve a cabo todas las tareas necesarias que requiere el trabajo estipulado.

Es esencial que un trabajador tenga alguna **información para protegerse y mantenerse ileso en el trabajo**, para eso se ejecutan

las capacitaciones. Esta es una de las motivaciones principales para establecer un Sistema de Gestión de Seguridad y Salud en el Trabajo (SG-SST), esto para poder intervenir y controlar los riesgos en sus procesos.

Por lo demás, es el medio que se empleará para asegurar que todos los trabajadores de las diferentes áreas aprendan la manera correcta de ejecutar las labores productoras y habituales, por medio del conocimiento de los procedimientos que apliquen a sus áreas, manejar su capacitación de forma apropiada para afirmar este objetivo.

Para concientizar el Sistema de gestión de Seguridad y Salud en el trabajo. ¿Qué capacitación SST es necesaria?

Corresponderá facilitar la capacitación necesaria para que un trabajador efectué completamente todos los trabajos necesarios que requiere el trabajo establecido y además convendrá definir la capacitación para cada trabajo en su empresa. Existen seis áreas primordiales de capacitación en concientizar que **ISO 45001 decide en la sección 7.3 de la norma**, siendo:

1. Por lo tanto, son los objetivos y las políticas de seguridad y salud en el trabajo que inquietan a su trabajo. Esto quiere decir saber lo que crean que **afecta la capacidad de la empresa para cumplir con la política y los objetivos**.

2. Aportación al sistema de gestión de seguridad y salud en el trabajo. **Los trabajadores tienen que saber sus propias políticas y procedimientos** para seguridad y salud en el trabajo y percibir cómo el cumplimiento de estas obligaciones los conserva seguros. Asimismo, incluye los beneficios de un excelente desempeño de seguridad y salud en el trabajo.

¿Qué es una empresa B Corp y cómo conseguir el certificado?

Las **empresas B Corp** son aquellas que centran su esfuerzo en la **sostenibilidad,** no solo para la propia organización, sino también para la **sociedad y el medio ambiente**. Hasta aquí, como muchas otras que disponen de **estrategias de sostenibilidad** o están certificadas bajo marcos de trabajo de **responsabilidad social** o sostenibilidad, la diferencia está en las **exigencias y alcance de estas certificaciones**. Veamos las diferencias.

El movimiento B Corp

Se trata de un movimiento iniciado en Estados Unidos en 2006, bajo la iniciativa de la **ONG B Lab,** con el firme propósito de impulsar un **nuevo tipo de economía** alrededor de todo el mundo en el que la rentabilidad pudiera convivir con **impactos positivos en la sociedad y el medioambiente.** Sin duda se trata de un sueño esperanzador, pero esto se consigue solo si existen estándares, exigencias y marcos regulatorios que acompañen y a los que las organizaciones estén dispuestas a sumarse.

B Lab desarrolló un **estándar, el certificado B Corporation,** ahora mundialmente conocido como **B Corp**, de modo que la organización pueda certificar a efectos de todas sus terceras partes que cumplen con las políticas, directrices y valores que promulga B Lab.

La certificación B Corp (B Corporation)

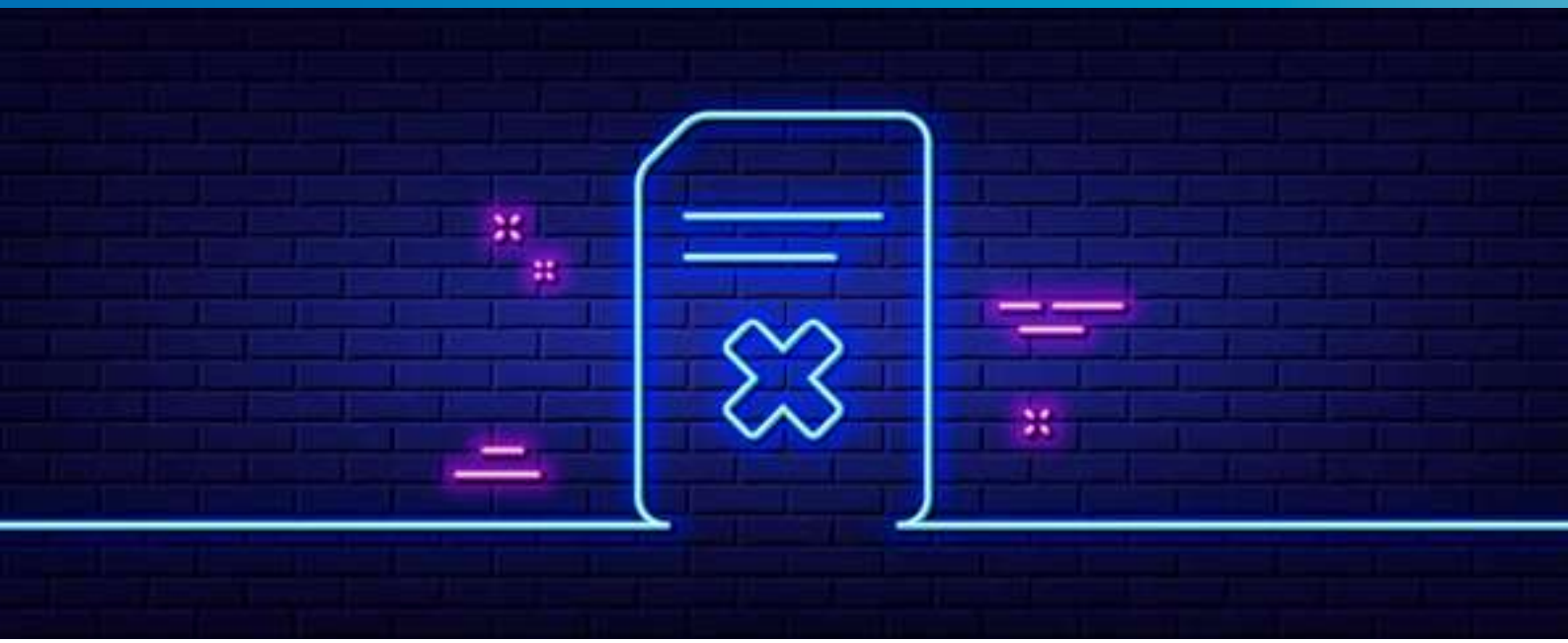
La certificación B Corp **no es sencilla de conseguir.** Implica altos estándares que deben ser verificados en las organizaciones y con ello obtener el sello que acredita que cumplen con las políticas y aplican los valores de B Lab en favor de un mundo mejor, una economía sostenible, ética y capaz de cambiar el mundo.

En resumen, acredita que la empresa se suma al **conjunto de organizaciones que hacen fuerza para el bien común,** no solo actual sino a futuro.

Pasos para la obtención del certificado B Corp

La única organización que puede conceder el **certificado B Corp** es B Lab, para lo que somete a las organizaciones que lo solicitan a una evaluación exhaustiva del "Impacto B", que toma indicadores en aspectos clave como los siguientes:

- Comunidad
- Trabajadores
- Medioambiente
- Gobernanza



Control de eliminación de la información en la nueva ISO 27002

Hasta hace un tiempo las organizaciones tenían un gran reto de buscar información para mejorar y así crecer. Con el tiempo, el uso de redes amplió la forma de comunicarnos y por ende a disponer información de manera cada vez más rápida. De esta forma, en la actualidad se cuenta con información para diferentes campos de interés, desde lo directamente obtenido por la organización hasta lo utilizado o generado por empresas terceras que contrata la organización.

Es así, como **no solo surgió la necesidad de proteger la información desde el punto de vista de conservarlos, sino también para eliminarlos**. Esto último, en caso se presenten algunas situaciones como:

- **La información ya no es relevante** para la continuidad de las operaciones de la organización.

- **La información nunca fue importante** para las operaciones de la organización.

- **La información ha pasado por revisiones para su mejora**, por lo que existen versiones anteriores que ya no forman parte de la actual gestión

La **norma ISO 27002:2022** propone no únicamente el cuidado de la información desde el punto de vista de preservarla para los intereses de la organización, sino también de eliminarla en caso esta ya no tenga un aporte para sus intereses de la organización. Es así como antes de proceder a eliminar, se debe proceder a establecer criterios de tiempo y utilidad. Esto es, no **se debe conservar una información que resulta totalmente irrelevante en las operaciones de la organización**. Esto reduce en gran manera el filtrado de información no deseada externamente a la organización.

Métodos a usar en el control de eliminación de la información

Una vez definido que se cuenta con información que no aporta en la actualidad en la organización se ubica el método adecuado para proceder con su eliminación. De antemano para estas gestiones, si hablamos de información que actualmente no aporta en la organización que, pero es de muy alto impacto en caso se filtre a personas que no le competen, se recomiendan métodos más estrictos que únicamente eliminarlo de forma convencional. Entre estos métodos contamos con algunos ejemplos que abordaremos a continuación.

Cómo planificar un sistema de gestión de riesgos

Planificar un Sistema de Gestión de Riesgos es el primer paso para comenzar un ciclo **PDCA** eficaz para que la gestión de riesgos en la organización sea cada ve más eficaz y eficiente.

El ciclo PDCA (plan, do, check, act) aporta **orden a la gestión de riesgos**, ya que esta se suele considerar una forma de acción muy improvisada, entonces el PDCA le confiere orden y estructura – y por consiguiente la optimización de recursos - para responder a un conjunto de factores que pueden ser muy caóticos. También **orienta hacia lo relevante**: contar con una forma de priorizar el uso de los recursos y las acciones que se deben tomar para ejecutar un proceso es importante para generar los resultados esperados, que es que la organización proteja y genere valor en función a la gestión de riesgos. A continuación, veremos cómo aplicarlo:

Ciclo PDCA

Planificar la gestión de riesgos

Tiene que ver con la **definición del método de gestión de riesgos,** normalmente por medio de un procedimiento. También en esta etapa **se definen los roles:** quiénes van a participar y cuáles serán sus funciones dentro de la gestión de riesgos. Además, se decide la frecuencia con la que se van a aplicar los controles y el modelo de gestión de los resultados, puesto que los resultados de la gestión de riesgos simplemente son una entrada para la gestión del resto de los procesos **(como el modelo de las 3 líneas de defensa, y otros que elija la organización)**.

Elementos clave de la planificación: recursos, tiempo, el método y la tecnología.

Do (Hacer)

La ejecución está referida a la **recolección de información** sobre el contexto, requisitos de las partes interesadas, los objetivos y metas de la organización... De allí se hace la identificación de los riesgos, que fundamentalmente sucede gracias a la tormenta de ideas de los equipos que constituimos en la fase de planificación. Luego **analizamos los riesgos identificados en una relación de probabilidad – impacto,** comparamos contra un mapa de calor que permita saber cuáles son los riesgos bajos, medios y altos (dependiendo de una política de apetito por el riesgo que se define en la planificación). De esa evaluación y comparación se establece un tratamiento que se basa en aceptar, mitigar o transferir los riesgos. Esto nos lleva a lo que **llamamos "miniproyectos",** que son los planes de tratamiento de riesgos.

¿Qué dice ISO 45001 sobre liderazgo visible?

La norma ISO 45001 es un estándar internacional de gestión de seguridad y salud en el trabajo. Establece requisitos para un sistema de gestión de seguridad y salud en el trabajo y proporciona un marco para su implementación y mejora continua. Uno de los requisitos clave de ISO 45001 es la necesidad de **liderazgo visible** para garantizar la efectividad del sistema de gestión de seguridad y salud en el trabajo.

Norma ISO 45001 y liderazgo visible

El liderazgo visible se refiere a **la capacidad de un líder para mostrar su compromiso con la seguridad y la salud en el trabajo** y para guiar y apoyar a su equipo en la implementación de medidas de seguridad y salud. Esto incluye **tomar decisiones** informadas sobre la seguridad y la salud en el trabajo, **establecer objetivos y metas** claros y alcanzables y **proporcionar los recursos necesarios** para lograrlos.

Implica estar disponible y accesible para el equipo y estar abierto a recibir y considerar sus ideas y preocupaciones, deben promover una cultura de seguridad y salud en el trabajo y fomentar una comunicación abierta y transparente sobre el tema, requiere un compromiso activo por parte de los líderes para llevar a cabo investigaciones y **análisis de riesgos** y para tomar medidas correctivas cuando sea necesario, deben estar dispuestos a asumir la responsabilidad de la seguridad y la salud en el trabajo y a hacer que sea una prioridad en la toma de decisiones.Los líderes **deben ser un modelo a seguir** y demostrar su compromiso con la seguridad y la salud en el trabajo a través de su propia conducta y decisiones. Esto puede incluir llevar equipo de protección personal adecuado, seguir los procedimientos de seguridad establecidos y participar activamente en la identificación y evaluación de riesgos.

Además, el liderazgo visible **implica la capacidad de un líder para motivar y apoyar a su equipo** en la implementación de medidas de seguridad y salud. Esto puede incluir proporcionar formación y orientación adecuadas, fomentar la participación activa del equipo en la identificación y evaluación de riesgos y proporcionar los recursos necesarios para implementar medidas de seguridad y salud adecuadas.

Un líder visible también debe ser capaz de reconocer y valorar el trabajo de su equipo en materia de seguridad y salud en el trabajo. Esto puede incluir el reconocimiento formal, como premios o reconocimientos, o simplemente expresar gratitud y reconocimiento por el esfuerzo y el compromiso del equipo. **Es esencial para garantizar la efectividad de un sistema de gestión de seguridad y salud en el trabajo**.

Elementos del Control Interno en la ogranización

Control Interno

El **sistema de Control Interno** de la organización establece los medios necesarios para garantizar que la organización marche en la **línea correcta para alcanzar los objetivos**, haciendo una utilización eficiente de los recursos, obteniendo una productividad acorde con lo esperado, prevenir el fraude y errores o violaciones de normas y principios.

Se trata de algo que **compete a toda la organización**, desde la alta dirección hasta ciertos colaboradores externos, por lo que exigirá que los medios empleados por los responsables del Sistema de Control Interno sean eficaces y extremadamente eficientes para obtener un buen equilibrio entre control y operatividad, no incurriendo en excesiva burocracia ni en actitudes laxas ante lo definido.

Si nos fijamos en lo comentado anteriormente, el Control Interno implicará a la totalidad de áreas de la organización y, por tanto, deberá contar con estructura suficiente para realizar su labor respecto a tres elementos principales:

Control Estratégico:

Dentro del ámbito estratégico, la función del Control Interno es la de definir el **Plan de Control Interno,** un documento que recoge los objetivos del Sistema de Control Interno (aquellos que deben perseguirse en la organización), las funciones asignadas a cada área dentro del mismo y las metas que se pretenden conseguir. No se debe olvidar que el Plan de Control Interno se basa en el **Plan Estratégico de la empresa.**En este sentido, los responsables deberán:Definir el riesgo y las políticas de control que se seguirán, acorde siempre con los objetivos.Vigilar el rendimiento de la organización en el alto nivel con relación a la marcha de la consecución de objetivos.Evaluar los **riesgos estratégicos** del negocio y definir los puntos de control necesarios para mantenerlos bajo control.Aportar en la mejora continua del negocio a todos los niveles como parte del avance global de la empresa.Vigilar los factores externos a la organización que pueden tener un efecto sobre la misma.Asignar los recursos necesarios para que se avance hacia la consecución.

Control en Procesos o nivel operativo:

Esto dependerá mucho de la propia estructura de la organización, pero en líneas generales, el Sistema de Control Interno deberá:

Evaluar los **riesgos asociados a cada proceso**, con especial atención en aquellos que forman parte de la cadena de valor o pueden llegar a ser especialmente críticos para la actividad.

Control de Seguridad de la información en la nube de la nueva ISO 27002

El control de seguridad de la información y su acceso es un elemento esencial de la seguridad que **determina quién tiene permiso estipulado para tener el acceso a determinados datos, aplicaciones, recursos y en qué circunstancias**. El objetivo principal es limitar el acceso a la información y a las instalaciones de procesamiento de información de la igual representación que las claves y listas de asistentes con aprobación anterior resguardan las plazas físicas, las directivas de los controles de acceso que protegen las plazas digitales. Es decir, permiten que las personas o usuarios adecuados ingresen y que la que es ajena a las plazas digitales se queden fuera.

Las directivas de **control de acceso** dependen de medidas técnicas como la autenticación y la autorización, que es el que permiten a las diferentes organizaciones **comprobar de forma evidente que**

los usuarios son quienes dicen ser y que cuentan con el nivel apropiado de acceso con base en elementos contextuales como el dispositivo, la ubicación, el rol, la responsabilidad entre otros.

El **control de seguridad de la información** impide que los infiltrados u otros usuarios no autorizados se hagan con la información confidencial, como por ejemplo los datos de clientes y la propiedad intelectual. También apoya a la reducción de riesgos de filtración de datos por parte de los empleados y mantiene controlado las amenazas web. En vez de manipular los diversos permisos manualmente, las empresas con mayor seguridad dependen de soluciones de administración de identidad y acceso para las implementaciones directivas de control de acceso.

ISO 27002

La **norma ISO 27002:2022** propone **no únicamente el cuidar la información desde la perspectiva de resguardar la información** para los intereses de las diversas organizaciones, sino que también de controlar en caso este tenga información confidencial para los intereses de la organización. Se procede a establecer criterios de controles de la información. Esto se debe conservar debido a que es una información que resulta totalmente relevante en las operaciones de la organización. Esto reduce en gran manera el filtrado de información no deseada, malwares que provienen de forma externa a la organización.

Una vez teniendo definida la información controlada y actualizada en la organización, **se debe implementar los métodos adecuados para proceder con los diversos controles de la información**.

Cómo operar en el día a día con un sistema de gestión de riesgos

Uno de los conflictos que tenemos cuando pensamos en riesgos es que **creemos que se trata de problemas puntuales** que requieren una gran planificación y que las autoridades más relevantes deben hacerse cargo de ellos. A manera de ejemplo, supongamos que muchas veces en nuestros vecindarios vemos una tubería rota y no lo denunciamos ni avisamos a las autoridades pertinentes porque suponemos que alguna suerte de alarma les va a indicar que esa tubería está fallando, pero si nosotros no nos ocupamos esto se puede convertir en un desastre y en un desperdicio importante. Lo mismo sucede en la **gestión de riesgos**.

Una de las primeras cosas que debemos tomar en cuenta es tener consciencia de que **en la vida organizacional no hay nada que esté escrito en piedra, todos los días nos exponemos a posibles fraudes, ataques informáticos, pérdidas de recursos,**

tiempo, productividad, de clientes... Como estamos expuestos a diario a estas situaciones, debemos tener claro cómo reaccionar ante esos eventos, que son potenciales hasta que no ocurren. Pero como pueden ocurrir, constituyen riesgos. Ese es el componente de probabilidad que tiene el riesgo. Dada la variante de riesgo tenemos que concentrarnos en la ejecución de dos grandes componentes de la gestión del riesgo, que forman parte del día a día de una organización:

1. **Desarrollo de los planes de tratamiento de riesgos**: Estos son los que primero debemos formular, son una suerte de "mini proyectos" que le permiten a la organización construir la forma de reaccionar ante un riesgo cuya evaluación ya conocemos, y es la que se hace durante la gestión de riesgos. En esa construcción **tendríamos que actuar a diario**. Es vital que el conjunto de actividades que forman parte del **plan de tratamiento de riesgos** tenga responsables, horas, fechas y recursos establecidos, incluyendo los hitos que nos permitirán avanzar dentro del PTR.

2. **La ejecución de los controles**: esta es una actividad cotidiana, que se relaciona con la ejecución de los procesos, es decir, los controles deben estar insertos en los procesos y tienen que estar tan bien diseñados que nos permitan ir ejecutando el proceso junto con los controles. Es decir, que no hagamos un paréntesis solamente para ejecutar controles, sino que se ejecuten mientras se lleva a cabo el proceso. Un ejemplo sería que cuando usemos un sistema haya un control de acceso lo **suficientemente ágil para identificar claramente a la persona que tiene privilegios y que puede acceder solo gracias a ellos**. Que cuando se transfiera la información o se opere y estemos expuestos al riesgo, el control esté incorporado.

Automatización de procesos para la gestión de ISO 45001

En el año 2018, se publicó **la norma ISO 45001 para los Sistemas de Gestión de Seguridad y Salud en el Trabajo**. Con anterioridad, la única norma que se aplicaba a nivel internacional en materia de seguridad y salud en el trabajo era la OHSAS 18001. Esta norma de origen británico fue empleada durante muchos años como norma de referencia por las organizaciones de todo el mundo.

Con la publicación de la ISO 45001, los sistemas de gestión basados en la norma OHSAS 18001, deberán adoptar los requisitos de la norma ISO 45001 lo antes posible, para que, de este modo, sea posible mantener la certificación de dicho sistema.

Además de que **la ISO 45001 reemplaza a la OHSAS 18001**, también está elaborada según la estructura del Anexo L, lo que facilita su integración con el resto de sistemas de gestión.

Se estableció un periodo de 3 años para realizar la migración de OHSAS 18001 a ISO 45001**. Debido a la situación actual de pandemia la IAF (International Accreditation Forum) ha ampliado el plazo**. Antes de esto, el plazo de migración a ISO 45001 terminaba el 11 de marzo de 2021. Con la ampliación, la fecha se amplía durante seis meses más, **hasta el 11 de septiembre de 2021**.

¿Cuáles son los beneficios de obtener el certificado ISO 45001?

- **Minimiza el periodo de baja laboral** al que tienen que enfrentarse los trabajadores con motivo de la reducción de accidentes laborales, lo que repercute directamente en disminuir los costos operativos de seguridad y salud laboral.

- **Convierte en prioridad la seguridad y salud de los trabajadores**, y cualquier parte interesada de la organización o stakeholders como los clientes o proveedores, logrando mejoras en la seguridad y salud.

- **Ayuda a en la gestión riesgos de seguridad y salud,** identificando riesgos e implementando controles para reducir sus consecuencias.

- **Favorece el cumplimiento legal**, a través de los requisitos normativos.

- **Potencia la obtención de nuevos contratos,** ya que la certificación en muchos casos es un requisito para optar a contrataciones.

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

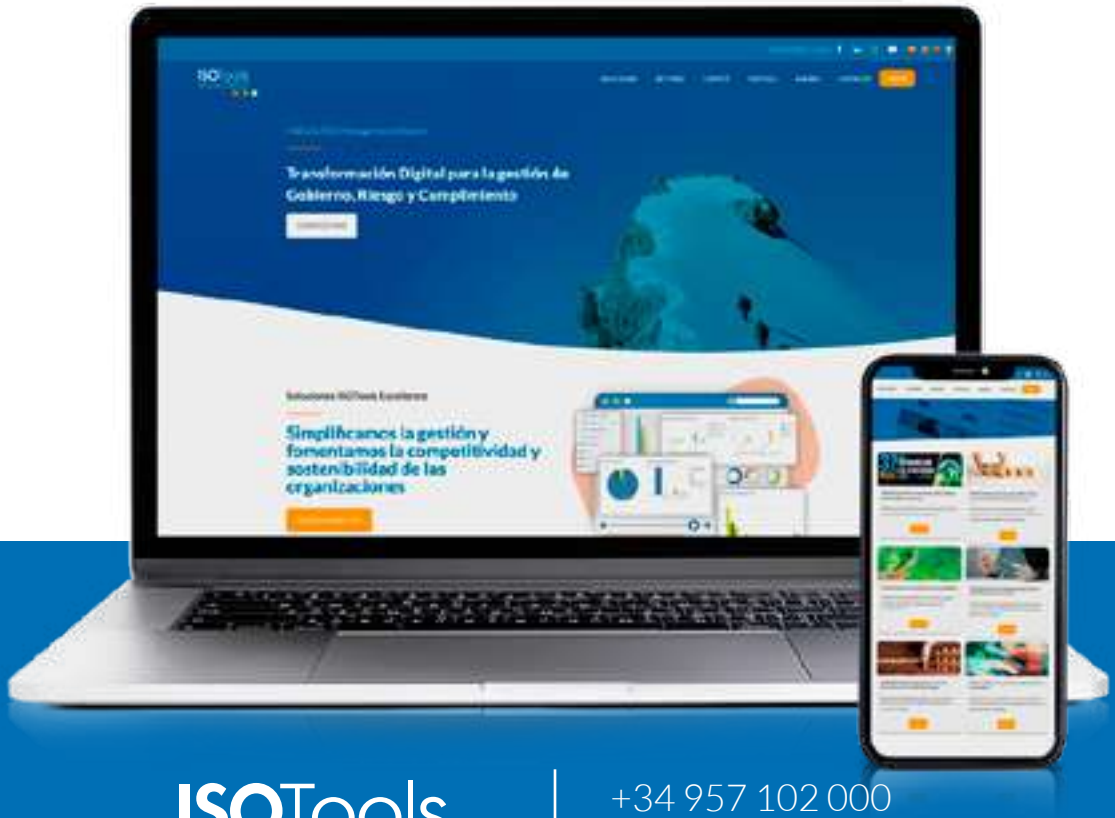
+240.000 usuarios

ISOTools EXCELLENCE

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.



ISOTools EXCELLENCE

+34 957 102 000
www.isotools.us