nqa.

ISO 45001:2018

GUÍA DE IMPLANTACIÓN PARA SEGURIDAD Y SALUD LABORAL



43,000 CERTIFICATES GLOBALLY

100% ALL INCLUSIVE FEES

1000+ EMPLOYEES WORLDWIDE

AVERAGE CUSTOMER PARTNERSHIP 10 YEARS

OPERATING COUNTRIES OVER 90



nqa.

> ISO 45001:2018

GUÍA DE IMPLANTACIÓN PARA SEGURIDAD Y SALUD LABORAL

Contenido

Introducción a la norma	P04
Beneficios de la implantación	P06
Ciclo PHVA	P07
Mentalidad/auditoría basada en riesgos	P08
Anexo SL	P09
SECCIÓN 1: Alcance	P10
SECCIÓN 2: Referencias normativas	P11
SECCIÓN 3: Términos y definiciones	P12
SECCIÓN 4: Contexto de la organización	P14
SECCIÓN 5: Liderazgo	P16
SECTION 6: Planificación	P18
SECCIÓN7: Soporte	P20
SECCIÓN 8: Operación	P22
SECCIÓN 9: Evaluación del desempeño	P24
SECCIÓN 10: Mejora	P28
Sacar el máximo de su sistema de gestión	P30
Pasos tras la implantación	P32
¿Cómo podemos ayudarle?	P33

TRUSTED GLOBALLY
30
YEARS
SINCE 1988

INTRODUCCIÓN A LA NORMA

La ISO 45001:2018 es la nueva norma internacional que proporciona un marco para gestionar y mejorar continuamente la seguridad y salud laboral (SSL) dentro de la organización, independientemente de su tamaño, actividad y ubicación geográfica.

El enfoque basado en riesgos introduce la estructura común del "Anexo SL" que proporciona compatibilidad con otras normas ISO, incluidos los sistemas de gestión ISO 9001, ISO 14001 e ISO 27001.

Al adoptar un enfoque sistemático que incluye la participación de los trabajadores, la organización puede integrar la SSL dentro de sus procesos comerciales, lo que contribuirá en la prevención de accidentes y efectos a largo y corto plazo sobre la salud. La norma proporciona una plataforma para desarrollar una cultura de seguridad positiva que conduzca al bienestar de los trabajadores.

Una vez que se haya establecido la política, junto con los procesos para facilitar el compromiso de la organización, la norma le pide a la organización que audite, revise y mejore el sistema, incluyendo la evaluación de las obligaciones de cumplimiento. Este enfoque proporciona a la organización seguridad y continuidad de negocio.

Los requisitos de la norma pueden ayudar significativamente a la organización a mejorar internamente, al incorporar una cultura de desafío y mejora continua.





Breve historia de la ISO 45001

La OHSAS 18001:2007 (versión inicial OHSAS 18001:1999) es la predecesora de la nueva ISO 45001: 2018. La norma OHSAS es reconocida internacionalmente pero no es una norma ISO.

Con el tiempo, se ha vuelto cada vez más evidente que muchos trabajadores sufren enfermedades, lesiones y defunciones relacionadas con la SSL, lo que representa una carga inaceptable para las personas, sus familias y conlleva costes morales y de bienestar para la sociedad en general.

Esto fomento la necesidad de tener una estructura sistemática para la gestión de estas actividades. La ISO 45001:2018 es una norma ISO y ha sido diseñada para tener una mayor compatibilidad con las revisiones existentes de sistemas de gestión ISO 9001:2015 e ISO 14001:2015.

Utiliza la misma estructura y refleja los requisitos identificados por la guía de la Organización Internacional del Trabajo para los sistemas de SSL. Ha sido desarrollada durante varios años por organismos internacionales y expertos de la industria.

Debido a esta compatibilidad, la ISO 45001:2018 debería superar los beneficios de la OHSAS 18001 y facilitar la integración con otras normas de sistemas de gestión ISO.

En 2021, se retirará la OHSAS 18001, dejando a ISO 45001 como la principal norma internacional de sistemas de gestión de seguridad y salud laboral.

BENEFICIOS DE LA IMPLANTACIÓN

Con o sin un sistema formal de gestión de SSL, las organizaciones tienen el deber moral y legal de proteger a los trabajadores de accidentes y enfermedades. La siguiente sección proporciona una visión general aobre los beneficios positivos de la implantación de la ISO 45001. Estos beneficios positivos no son exhaustivos.



La adopción de la estructura de alto nivel del "Anexo SL" permite a las organizaciones integrar la ISO 45001 con los sistemas de gestión de calidad ISO 9001 e ISO 14001. Este enfoque ha reducido la complejidad de los requisitos de múltiples cláusulas en diferentes normas, ahorrando tiempo y recursos.



El estándar proporciona un enfoque sistemático hacia liderazgo de la gerencia para evaluar el riesgo y las oportunidades de SSL, monitorizar y revisar el desempeño y establecer objetivos para la mejora continua dentro del "contexto" de las actividades de la organización. Esto puede incluir campañas de promoción SSL o el seguimiento de los efectos de SSL de los productos y servicios.



La implantación demuestra el compromiso por parte de la gerencia con las partes interesadas internas y externas, con la intención de proteger a los trabajadores de los accidentes, incluidos los efectos a corto y largo plazo sobre la salud. Esto puede reducir el tiempo de inactividad, conducir a la reducción de bajas y a un posible juicio.



Este compromiso también brinda garantías a la junta directiva o propietarios de que los controles de SSL de la gerencia son inherentes a la organización.



La norma promueve la participación de los trabajadores al identificar peligros y eliminar o reducir riesgos mediante la implementación de controles integrados con otros procesos comerciales. Este enfoque puede mejorar la cultura de seguridad, minimizar el riesgo e integrar las mejores prácticas, lo que resulta en una mayor productividad.



Además de los controles internos del proceso, la norma dictamina requisitos para evaluar la adquisición de productos y servicios que pueden afectar a la SSL. Por ejemplo, la gestión estructurada de contratistas basada en el riesgo. Dicho proceso puede proporcionar controles para reducir riesgos de SSL y promover una cultura de seguridad positiva.



La norma proporciona una estructura para monitorizar y revisar las obligaciones de cumplimiento y garantizar que la organización cumpla legalmente con los requisitos de productos y servicios. Es importante que la organización entienda lo que quiere lograr, por qué necesita lograrlo y si lo ha logrado.



Los programas de auditoría interna y externa revisan la eficacia del sistema de gestión, incluidos los procesos. El programa promueve la comunicación y la participación de los trabajadores a través de la identificación de brechas que conduzcan a la mejora continua.



El énfasis en los trabajadores que desempeñan un papel activo en SSL, puede tener beneficios en la reputación de una organización. Un lugar de trabajo seguro conduce a la retención y motivación del personal y a una mayor productividad.



La implantación también es un reconocimiento al haber alcanzado un marco de referencia internacional que puede tener una influencia positiva en los clientes existentes y potenciales y en el cumplimiento de sus propios compromisos de responsabilidad social.

Para mayor información sobre los beneficios de la ISO 45001 y su implantación, dirijase a la sección 1 Alcance.

CICLO PHVA

La ISO 45001 ha adoptado el ciclo PHVA para lograr la mejora continua. Esta es una parte inherente del enfoque sistemático para determinar soluciones viables, evaluar los resultados e implementar las soluciones que han demostrado funcionar.

El ciclo PHVA puede aplicarse no solo a los sistemas de gestión en su conjunto, sino también a cada elemento individual para proporcionar un enfoque continuo en la mejora continua. En el centro de cada etapa se encuentra la "Gerencia", que es fundamental para garantizar que el sistema de SSL se gestiona de manera efectiva.

En el contexto de la ISO 45001, consulte el siguiente ciclo PHVA:

Planificar:

Comprender el contexto de la organización, incluidos los riesgos y oportunidades. Establecer los objetivos, procesos y recursos necesarios para entregar resultados acorde a la política de SSL.

Hacer:

Implemente los procesos, incluyendo: participación de trabajadores, identificación de peligros y preparación ante emergencias.

Verificar:

Realice un seguimiento, medición y evaluación de las actividades y procesos de SSL.

Actuar:

Tome medidas para mejorar continuamente, incluyendo incidentes, no conformidades y hallazgos de auditoría.



Establecer los objetivos, procesos y recursos de SSL necesarios para entregar resultados acorde a la política de SSL de las organizaciones.

HACER:
Implemente procesos: participación de trabajadores, identificación de peligros y preparación ante emergencias.

VERIFICAR: Monitoizar, medir y evaluar las actividades y procesos de SSL.

ACTUAR:
Tome medidas para mejorar continuamente, incluyendo incidentes, no conformidad y hallazgos de auditoría.

MENTALIDAD/ AUDITORÍAS BASADAS EN RIESGOS

Cualquier empresa que opere un sistema de gestión de SSL debe asegurarse de que existan medidas efectivas para evaluar el desempeño que permitan la mejora continua interna. Esta sección describe las diferentes metodologías de auditoría en relación con el sistema SSL para garantizar que sea efectivo a todos los niveles de la organización y cumpla con los requisitos de la norma.

Mentalidad basada en riesgos

La mentalidad basada en riedgos (MBR) es un principio central de la ISO 45001. La MBR requiere que el equipo de gestión evalúe continuamente los problemas que afectan los aspectos de SSL de una organización y se asegure de que existan objetivos, recursos y controles apropiados. La MBR permite realizar cambios dinámicos en objetivos y enfoque, al tiempo que garantiza los recursos para controlar los cambios y las circunstancias imprevistas. La MBR se extiende a áreas externas a la organización que pueden influir en la SSL.

Por ejemplo, la adquisición de productos y servicios (incluidos los contratistas) y el impacto de los productos y servicios suministrados. La organización debe determinar la metodología para la MBR teniendo en cuenta las obligaciones de cumplimiento y la participación de los trabajadores. Para los aspectos operativos, la norma define claramente la jerarquía de control para la identificación de peligros y la reducción de riesgos con la participación de los trabajadores. Esta metodología requiere que una reducción de riesgos asociados.

1º Parte: Auditoría interna

Las auditorías internas se realizan en un momento determinado para determinar si las políticas y prácticas son efectivas y si logran el objetivo previsto. La auditoría interna es una oportunidad para comprometerse con los trabajadores y capturar un reflejo de los procesos. Las auditorías pueden identificar evidencias de conformidad, incluidas las obligaciones de cumplimiento. También pueden identificar oportunidades de mejora e incumplimiento con respecto a la norma aplicable.

Planificación de la auditoría

El desarrollo de un plan de auditoría no tiene que ser un proceso complicado. A través de la MBR, se puede programar una serie de auditorías para enfocar áreas de mayor riesgo y para comprometerse con grupos identificados de trabajadores. Depende de la organización determinar la frecuencia, siempre que esta esté definida. Además de los aspectos operativos, el plan cubrirá los procesos centrales, incluidas las obligaciones de cumplimiento, la revisión por la dirección y la información documentada.

Auditorías intermedias

Puede adoptar un enfoque menos formal mediante la realización de auditorías intermedias. Pueden ser realizadas por altos directivos o a nivel operativo para inspeccionar áreas de la organización a preguntas predeterminadas. Es una oportunidad adicional para interactuar con los trabajadores, promover la comunicación y construir una cultura de seguridad positiva.

2ª Parte: Auditorías externas

Las auditorías de 2ª parte generalmente son realizadas por clientes u organizaciones en su nombre, sin embargo, pueden ser realizadas por los reguladores para garantizar que la organización cumpla con los requisitos legales. Las auditorías externas son una forma útil de corroborar un reclamo de SSL de la organización y recopilar información de primera mano y contactar a los trabajadores antes de una relación comercial. Se pueden planificar auditorías de segunda parte, sin embargo, es posible que los reguladores no se lo notifiquen. Mas vale estar preparados.

3º Parte: Auditoría de certificación

Las auditorías de 3ª parte son realizadas por organismos de certificación acreditados por UKAS como NQA. Dependiendo de la cantidad de empleados, sedes, riesgo y complejidad de la organización, el organismo de certificación determinará un número de días de auditoría necesarios para cubrir el alcance completo de la norma. Antes de la certificación, la organización puede considerar realizar un análisis de deficiencias por un consultor o un organismo de certificación para identificar las deficiencias con respecto a la OHSAS.

La certificación es una demostración a las partes interesadas, incluidos los trabajadores, clientes y reguladores, de que existe:

- Un mecanismo de evaluación regular para controlar e implantar las obligaciones de cumplimiento.
- Una evaluación regular para controlar y mejorar los procesos de SSL.
- Identificación de peligros y reducción de riesgos de SSL
- Revisiones y evaluación regulares de los riesgos de SSL y oportunidades
- Participación de los trabajadores en el proceso de toma de decisiones para asegurar un entorno de trabajo seguro, mejora continua y una cultura de seguridad.

ANEXO SL

Antes de la introducción del Anexo SL (anteriormente conocido como Guía 83 ISO), cualquier organización que implantara las normas ISO 9001, ISO 14001 e ISO 27001 tenía dificultades para integrar los sistemas de gestión. La ausencia del Anexo SL podría conducir a posibles brechas entre los sistemas de gestión y llevar a una carga innecesaria de recursos. La introducción del Anexo SL, que incluye la ISO 45001, ha permitido la adopción de una estructura de alto nivel en varias normas con el fin armonizar las 10 cláusulas centrales, lo que facilita la integración de las normas.

Estructura de alto nivel

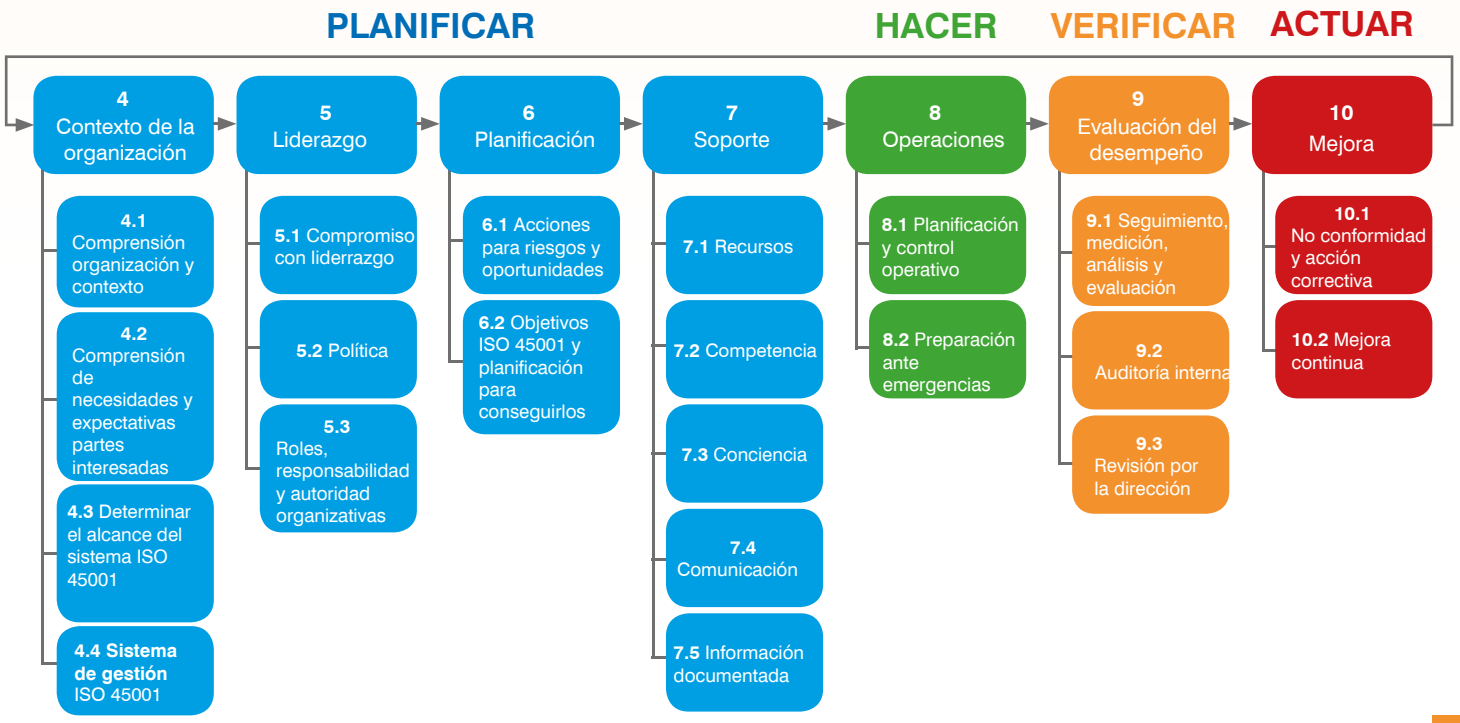
EL Anexo SL incluye 10 cláusulas principales:

1. Alcance
2. Referencias normativas
3. Términos y definiciones
4. Contexto de la organización
5. Liderazgo
6. Planificación
7. Soporte
8. Preparación de emergencias
9. Evaluación del desempeño
10. Mejora

Las primeras tres cláusulas proporcionan información útil que incluye términos y definiciones. El fundamento del "contexto de la organización" (cláusula 4) es que el sistema se centre en los procesos y requisitos necesarios para alcanzar los objetivos de la política de la organización. Esto se logra al comprender la organización y el contexto en el que opera. Dicha cláusula establece los requisitos para que la organización defina el "Alcance" del sistema y la planificación posterior del sistema.

Las cláusulas 5 a 10 son comunes a todas las normas ISO. La ISO 45001 se refiere específicamente a cuestiones de seguridad y salud laboral. Si bien hay algo en común, hay que establecer, implementar y mantener procesos de SSL que incluyen la comprensión del marco de políticas, la identificación de los peligros, el control y gestión de los riesgos y la participación de los trabajadores. La inclusión del Anexo SL permite un sistema de gestión integrado (SGI) que maneja simultáneamente los requisitos de la ISO 45001, ISO 9001 e ISO 14001. Esto incluiría un proceso armonizado de información documentada, adquisición, auditoría y revisión de por la dirección sin necesidad de duplicación.

VISTA GENERAL DEL ANEXO SL



SECCIÓN 1: ALCANCE

Conseguir la certificación requiere de la aplicación de todas las cláusulas de requisitos. Esta sección establece el propósito y parámetros del sistema de gestión ISO 45001 para conseguir los resultados esperados.

El resultado previsto del sistema de gestión de SSL es que la organización:

- Proporcione un espacio de trabajo seguro y saludable.
- Prevenga los accidentes y enfermedades laborales.
- Controle y mejore proactivamente el desempeño de SSL
- Elimine los peligros y minimice los riesgos de SSL(incluidas las deficiencias del sistema)
- Aproveche las oportunidades de SSL y aborde las no conformidades del sistema de gestión asociadas a sus actividades.
- Cumpla con los requisitos legales y otros
- Consiga los objetivos de SSL
- Integre otros aspectos de seguridad y salud, incluyendo el bienestar de los trabajadores

Esta sección deja claro que la norma no aborda cuestiones como la seguridad del producto, daños a la propiedad o impactos ambientales más allá de los riesgos que presentan para los trabajadores y para otras partes interesadas relevantes.



SECCIÓN 2: REFERENCIAS NORMATIVAS

La alusión a las referencias normativas es común a todas las normas de sistemas de gestión, no obstante, la ISO 45001 no dispone de referencias normativas.

Si corresponde a un estándar, las referencias normativas son documentos esenciales utilizados para la aplicación del documento. En otras palabras, el documento de referencia se considera esencial para la aplicación del estándar referenciado.

La ISO 45001 proporciona una bibliografía con más información, incluidas las normas de gestión ISO asociadas.



SECCIÓN 3: TÉRMINOS Y DEFINICIONES

Las normas ISO están redactadas de tal manera que su significado puede estar abierto a interpretación. Como con todos las normas, dicha interpretación puede generar confusión. Para ayudar al usuario, la sección 3 de la norma proporciona términos y definiciones prescriptivos para evitar una interpretación incorrecta.

Recomendamos que las personas responsables de la implantación de la norma aclaren y comprendan claramente loa términos descritos en esta sección.

Por ejemplo, "trabajador" puede ser interpretado sin orientación como un operador que trabaja en una fábrica, cuando en realidad un trabajador cubre muchos aspectos laborales, incluyendo agencias, contratistas, empleados, gerencia y el personal de proveedores externos.

Cada término se enumera de acuerdo con la jerarquía de conceptos que refleja la secuencia de la introducción de la norma.

Además del término o definición, las notas pueden proporcionar más información y claridad.

Si ha adquirido una versión electrónica de la norma, podrá ver que las definiciones se vinculan a otras definiciones para poder ver sus interrelaciones.

Anexo A Guía

El anexo A de la norma proporciona clarificaciones sobre conceptos de SSL para eviar confusiones. Los conceptos incluyen:

- **Continuidad**
- **Aseguramiento**
- **Parte interesada**
- **Información documentada**

Si la organización requiere el uso de términos específicos de la industria y sus significados en relación con el sistema de SSL, puede utilizarlos, pero deben cumplir con el documento ISO 45001.




WORK
SAFETY

SECCIÓN 4: CONTEXTO DE LA ORGANIZACIÓN

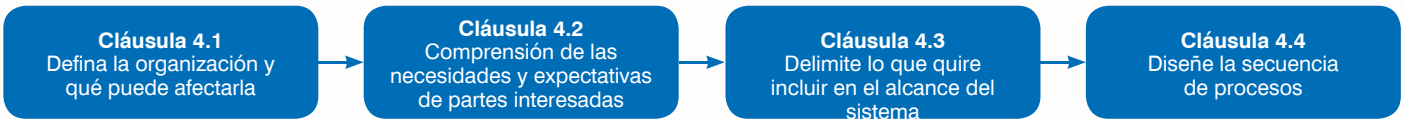
La razón de esta cláusula es que el sistema se centre en los procesos y requisitos necesarios para lograr los objetivos de la política de SSL. Esto se puede lograr mediante la comprensión de la organización y su contexto. La cláusula 4 también establece los requisitos para el "Alcance" y el sistema a definir, y la posterior planificación del sistema para lograr los objetivos.

La comprensión del contexto de la organización se lleva a cabo por la gerencia con información sobre el negocio y las actividades de todos los niveles de la organización. Los puntos de discusión se centran en cuestiones internas y externas que tienen un impacto en el sistema de SSL.

La cláusula 4 tiene cuatro subcláusulas que establecen elementos necesarios para definir el contexto de la organización y para diseñar el sistema de gestión de SSL.

Estos 4 requisitos siguen una secuencia:

- 4.1: Aclarar los objetivos estratégicos de la organización y determinar cualquier problema que pueda afectar la consecución de estos objetivos.
- 4.2: Consideración de las partes interesadas, incluidos los trabajadores y cómo pueden afectar al funcionamiento de la organización.
- 4.3: Establecer el alcance del sistema de gestión de SSL a partir de la información de los requisitos 4.1 y 4.2
- 4.4: Elaborar un diseño para el sistema de gestión SSL y su planificación de alto nivel.



4.1 Comprensión de la organización y su contexto

La cláusula 4.1 requiere una comprensión de alto nivel de los problemas clave que pueden afectar a la SSL, tanto positiva como negativamente. El uso de esta información ayudará a desarrollar una mejor comprensión de los problemas internos y externos y la interacción de actividades para ayudar a planificar y desarrollar controles dentro del sistema.

¿CUÁLES SON LOS PROBLEMAS INTERNOS Y EXTERNOS?

Los problemas internos y externos son circunstancias, características y cambios que pueden influir positiva o negativamente en el sistema de gestión de SSL. El "Anexo A" de la norma se ha desarrollado para proporcionar ejemplos de problemas internos y externos. A continuación se presentan algunos ejemplos:

Problemas externos

- Entorno cultural, social, político, legal, financiero, tecnológico, económico y natural en el que opera la organización.
- Quiénes son los competidores, subcontratistas, proveedores y socios.
- Leyes nacionales e internacionales.
- Motores de la industria y tendencias que influyen en la organización.
- Los productos y servicios de la organización y su influencia en la salud y seguridad laboral.

Problemas internos

- Gobierno, estructura organizativa, roles y responsabilidades
- Políticas, objetivos y estrategias establecidas para lograrlos.
- Recursos (incluidos humanos), conocimiento y competencia.
- La cultura de SSL dentro de la organización y la relación con los trabajadores.
- Proceso para la introducción de productos, materiales, servicios, herramientas, software, locales y equipos.
- Condiciones laborales

Recomendamos incluir la información que se recopila a todos los niveles de la organización para determinar el contexto en un informe. El beneficio de esto es que proporciona una explicación coherente y una buena referencia para apoyar la estrategia comercial actual y futura. (Para la revisión del contexto, consulte la sección 9).

4.2 Comprensión de necesidades y expectativas de trabajadores y partes interesadas

"Partes interesadas" es el término preferido introducido por la norma ISO. A diferencia de otras nomras comunes, esta cláusula introduce el término "trabajadores", que es un término amplio como se describe en la sección 3 "Términos y definiciones".

Esta sección requiere la determinación de, además de los trabajadores, las partes interesadas que pueden influir positiva y negativamente en la SSL. Una vez que se ha decidido qué partes interesadas son relevantes y significativas, se deben abordar sus necesidades y expectativas dentro del sistema de gestión de SSL.

Recuerde que al considerar a las partes interesadas, algunas necesidades y expectativas son obligatorias por ley y, por lo tanto, deben considerarse en los requisitos reglamentarios.

Una vez definidas las partes interesadas, la ISO 45001 requiere que determine sus efectos potenciales y reales.

Las partes interesadas pueden documentarse en un mapa:



4.3 Determinación del alcance del sistema de gestión de SSL

A partir de la información de contexto del 4.1 y la comprensión de las necesidades y expectativas de los trabajadores y partes interesadas del 4.2, se puede desarrollar el "alcance".
El alcance establece las áreas del negocio que se gestionarán en el sistema de gestión de SSL.

Esto incluirá los procesos y actividades clave que se dedican al servicio o la producción de bienes, incluida cualquier actividad de cara al cliente y el trabajo de garantía post-entrega.
Cuando una organización es compleja, el alcance se usa para limitar las actividades o ubicaciones donde se aplica el sistema, son "límites de aplicabilidad". Sin embargo, las áreas de negocio no pueden excluirse del alcance para evitar procesos de SSL o evadir el cumplimiento legal.

Cuando solicite a NQA la auditoría de certificación de sus sistema, será necesario declarar el alcance.

Esto asegurará que enviemos al auditor correcto y con experiencia en el sector de su industria. Por ejemplo:

"Fabricación y venta de lavavajillas".

En este ejemplo puede ver que el proceso principal es la fabricación, que incorporará muchos procesos, incluidos trabajadores, maquinaria, requisitos reglamentarios, proveedores externos, clientes (usuarios finales) y competencia a auditar.

4.4 Sistema de gestión de SSL

A partir de la información recopilada en 4.1, 4.2 y 4.3, la norma requiere el diseño e integración de procesos dentro del sistema de gestión para satisfacer los requisitos de la ISO 45001. Esto puede incluir procesos tales como diseño y desarrollo, adquisición, comercialización y fabricación.

SECCIÓN 5: LIDERAZGO

El liderazgo y el compromiso de la gerencia es vital para el éxito del sistema de gestión de SSL. La expectativa de los líderes dentro de una organización es convertirse en líderes del sistema y proporcionar los recursos necesarios para proteger a los trabajadores de daños.

Esta sección proporciona el tono y las expectativas sobre el liderazgo de la gerencia para participar activamente en el sistema SSL y generar una cultura positiva de salud y seguridad dentro de la organización.

A continuación, se muestran ejemplos de demostración del liderazgo dentro del sistema SSL:

- Asumir la responsabilidad respecto a la prevención de lesiones/enfermedades laborales, así como la provisión de un entorno laboral seguro y saludable.
- Facilitar la cultura positiva y la mejora continua.
- Garantizar que el sistema SSL esté integrado en los procesos comerciales.
- Promover la comunicación interna y externa y a todos los niveles, empezando desde la gerencia.
- Proteger a los trabajadores de represalias cuando denuncien incidentes, peligros, riesgos y oportunidades.
- Provisión y apoyo a comités de seguridad.

De cara a una auditoría externa, la expectativa es que el liderazgo sea el centro del sistema de gestión de SSL y haya una demostración clara de la comprensión del sistema.

Política de SSL

La política de SSL es una "declaración de intencione o misión" que establece el marco para administrar el sistema de gestión de seguridad y salud laboral. La política de SSL debe estar arobada por la gerencia, quien impulsará los controles existentes y las acciones que se llevan a cabo para mejorarla.

La norma requiere específicamente que la política de SSL incluya compromisos para:

- Proporcionar un marco para establecer objetivos.
- Proporcionar condiciones de trabajo seguras para la prevención de lesiones y/o enfermedades ocupacionales.
- Eliminar peligros y reducir riesgos de SSL.
- Mejora continua del sistema de SSL.
- Consulta y participación de los trabajadores y los representantes de los trabajadores.
- Cumplimiento de requisitos legales y otros requisitos.

Una vez que la política de SSL haya sido aprobada, debe comunicarse a las partes interesadas, incluidos los trabajadores. Debe estar disponible para las partes interesadas, incluyendo a clientes y proveedores externos.

Además, la política de SSL debe ser revisada periódicamente por la gerencia para garantizar que siga siendo aplicable al contexto de la organización.



Roles, responsabilidades y autoridades organizativas

Esta sección requiere que la organización defina roles, responsabilidades y autoridades claras en toda la organización. Se reconoce que la responsabilidad general del sistema de gestión de SSL recae en la gerencia, sin embargo, las personas deben tener en cuenta su propia salud y seguridad y la de los demás.

Documente los roles, responsabilidades y autoridades dentro de organigramas. Las políticas y las instrucciones de trabajo también pueden incluir responsabilidad y autoridad, y debe considerarse la competencia.

Consulta y participación de los trabajadores

Un factor clave para el éxito del sistema de SSL es garantizar que haya líneas claras de comunicación, consulta y participación de los trabajadores con suficiente asignación de tiempo y recursos. Esta sección requiere el desarrollo de procesos para garantizar que la información que afecta a la SSL se comunica a todos los niveles de la organización.

Esto se puede lograrse de muchas maneras, según el alcance y la escala de su organización.

A continuación sugerimos una serie de medidas para promocionar la consulta y participación de trabajadores.

- Reuniones periódicas con la gerencia para discutir procesos que incluyen cuestiones de SSL.
- Comité de seguridad con representantes de los trabajadores (cuando sea necesario).
- Iidentificación y eliminación de peligros (evaluación riesgos).
- Desarrollo de charlas y presentaciones sobre formación (incluso trabajadores fuera de su organización, como contratistas o visitantes).
- Desarrollo de sistemas e instrucciones de trabajo seguros.
- Comunicación cruzada dentro de la organización.
- Esquemas de informes de fallos potenciales con acciones de seguimiento que incluyen análisis de causa raíz.
- Visitas de sedes.
- Política de puertas abiertas para hablar con sindicatos.
- Buzón de sugerencias parsa SSL.
- Comunicación: tablones de anuncios, boletines, correos electrónicos, blogs, campañas de promoción de la salud...

Una vez que se haya elegido una selección de métodos de consulta y participación de los trabajadores, considere documentar las metodologías dentro de un proceso. Esto permitirá a la organización verificar periódicamente el proceso dentro de su programa de auditoría para garantizar el cumplimiento de los requisitos.



SECCIÓN 6: PLANIFICACIÓN

La planificación es uno de los componentes clave de cualquier sistema de gestión. La ISO 45001 se basa en el ciclo "Planificar-Hacer-Verificar-Actuar", donde la planificación se utiliza para poner en marcha las acciones de funcionamiento del sistema.

La planificación ocurre en varios puntos del marco del sistema de gestión de SSL. Para establecer el sistema de gestión, la planificación requiere utilizar la información recopilada en la cláusula 4. En varios momentos habrá la necesidad de 'planificar' nuevamente. Esto incluye la planificación periódica para alcanzar los objetivos establecidos y revisados. También en el caso de cambios por eventos planificados o no.

Los requisitos son:

- Planifique acciones basadas en la evaluación de riesgos para gestionar riesgos y oportunidades en la prevención de efectos no deseados (lesiones o enfermedades).
- Administre eventos y determine continuamente riesgos y oportunidades para los trabajadores y el sistema de SSL.
- Establezcar y gestione objetivos.
- Planifique y gestione cambios en el sistema y vuelva a evaluarlos una vez que se hayan realizado.
- Considerar las relaciones e interacciones entre actividades.
- Defina una metodología para la identificación de peligros.
- Defina la metodología para la identificación y gestión de los requisitos legales y de otro tipo.
- Considere el conocimiento de la organización para gestionar actividades de forma segura.

Identificación de peligros

La identificación de peligros es fundamental en el proceso de planificación para priorizar acciones a la hora de abordar riesgos y oportunidades. El uso de la "jerarquía de control" requiere que la organización realice una evaluación de riesgos basada en actividades internas y externas. La identificación de peligros permitirá a la organización reconocer y comprender los peligros en el lugar de trabajo. También permitirá a los trabajadores evaluar, priorizar y eliminar peligros o reducir los riesgos de SSL que pueden aparecer en muchas circunstancias, incluidas las físicas, químicas, biológicas, psicosociales, fisiológicas, mecánicas, eléctricas o basadas en el movimiento y la energía.

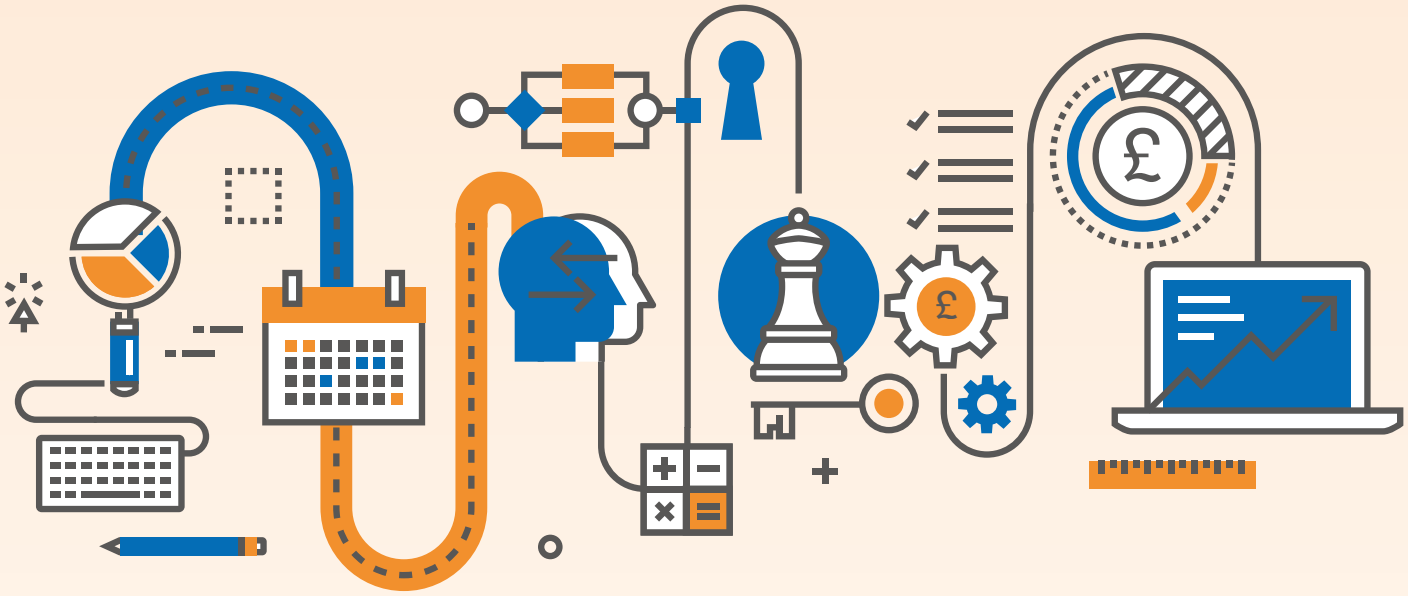
También se debe tener en cuenta los tipos de actividad, incluyendo:

- Grupos de trabajadores expuestos al peligro.
- Trabajo por turnos o soliartio, horas de actividad y supervisión.
- Factores humanos que incluyen actividades físicas exigentes.
- Diseño del lugar de trabajo, por ejemplo, segregación de tráfico y rutas peatonales.
- Cambios en el patrón de trabajo, incluido el aumento o la disminución de la productividad.
- Ruido, frío, calor.
- Requisitos legales y mecanismo para adaptarse a los cambios en los mismos.
- Cómo se comunicará la evaluación de riesgos y la posterior formación sobre las medidas de control.
- Situaciones de emergencia, como eventos no planificados, incluidos incendios y pérdida de energía.
- Los recursos para garantizar la jerarquía de control puede aplicarse a los resultados de la evaluación de riesgos.



Utilizando la jerarquía de control, la organización necesitará determinar la metodología para registrar hallazgos como información documentada y su comunicación a los trabajadores y partes interesadas. La persona competente llevará a cabo una evaluación de riesgos y calificará los hallazgos en función de su probabilidad y la gravedad del daño. Esta metodología se aplicará de manera coherente y se basará en los requisitos legales/reglamentarios, el tipo y las circunstancias de la actividad (ruido, fuego, vibración, riesgo de altura...)

Se recomienda que la evaluación de riesgos comience en la fase de diseño de cualquier actividad e involucre a los trabajadores que están o estarán directamente involucrados en el proceso.



Determinación de requisitos legales y otros

La organización necesita asegurar que durante el proceso de evaluación de riesgos se adhiere a los últimos requisitos legales y otros requisitos aplicables. El proceso de evaluación de requisitos legales y de otro tipo variará según la complejidad del negocio.

Las fuentes de información pueden incluir:

- Suscripción a boletines de actualización legal del editor
- Membresía de asociaciones comerciales
- Investigación a través de sitios web gubernamentales
- Uso de consultores competentes
- Membresía de empleados en institutos de salud y seguridad ocupacional
- Asistencia de los empleados a cursos de capacitación en seguridad y salud ocupacional.

Tras la evaluación inicial de obligaciones de cumplimiento, la organización puede considerar colocar la información relevante en un documento, como una hoja de cálculo.

El documento puede incluir la siguiente información y ser referenciado en evaluaciones de riesgo individuales:

- Nombre y número de referencia de regulación/requisito
- Estatus de revisión
- Fecha de última revisión de la regulación
- Persona competente responsable de revisar el requisito
- Área a la que afecta el requisito, incluida una breve descripción de la actividad y la información documentada asociada
- Un hipervínculo o descripción de la fuente de información.
- Nombre y detalles de contacto del cliente/proveedor externo si son relevantes para otro requisito
- Próxima fecha de revisión.

Acción de planificación

Después del proceso de identificación de peligros, la organización debe planificar acciones en orden de prioridad para reducir el riesgo. Estos deben considerar las consecuencias de estas acciones antes de que se introduzcan las acciones. Las acciones de planificación e incluso la introducción de medidas de control deben estar dentro del marco del sistema de gestión de SSL.

Las medidas de control pueden integrarse en las instrucciones de trabajo del sistema existente o basarse en el riesgo y desarrollarse en un sistema de trabajo seguro. Las tareas pueden ser delegadas por la gerencia individual o colectivamante. Las tareas se asignarán a las personas en función de su competencia, teniendo en cuenta cómo se impartirá la formación de los trabajadores.

Objetivos

Es un requisito del estándar establecer objetivos alcanzables de SSL con los medios para medir periódicamente el progreso, demostrando una mejora continua. A menudo, los objetivos se establecen y revisan en la revisión por la dirección (cláusula 9.3) o en reuniones departamentales. Una vez establecido, debe haber medios para comunicar los objetivos en toda la organización para generar una cultura de SSL.

Si se han identificado muchos requisitos, la organización puede considerar desarrollar un plan estratégico documentado de SSL. El plan debe ser acordado por la gerencia e incluir tareas de calificación de riesgo, en orden de prioridad, y la alineación con la gerencia responsable de supervisar la tarea.

Un plan estratégico de SSL es un documento en vivo y debe revisarse periódicamente para controlar el progreso hacia el logro de objetivos y la mejora continua.

Los documentos pueden incluir:

- Temas estratégicos priorizados
- Acciones, como realizar evaluaciones de acuerdo con las obligaciones de cumplimiento.
- Método para lograr la acción.
- Recursos necesarios para lograr la acción. Por ejemplo: Humanos, equipo, proveedores, financieros y externos.
- El indicador clave de desempeño para demostrar el logro de la acción.
- Responsabilidad general
- Responsabilidad de la gerencia
- Calendario
- Clasificación del riesgo.

SECCIÓN 7: SOPORTE

Esta sección analiza los requisitos que sustentan el sistema de gestión de SSL para garantizar que funciona de manera efectiva.

Recursos

Se necesitarán recursos para cumplir con los requisitos identificados durante las etapas de planificación del sistema para mantener la mejora continua. Estos incluyen recursos humanos, naturales, infraestructura, tecnológicos y financieros.

La asignación de recursos debe contar con el apoyo de la gerencia, bajo los requisitos de la Cláusula 5, para impulsar el mantenimiento de un entorno de trabajo seguro y saludable. Como parte de la identificación de recursos, la organización necesita considerar la información de la sección 6 para reconocer el riesgo, las oportunidades y los objetivos. Luego necesitará asignar recursos suficientes para mitigarlos o gestionarlos.

Competencia

Una organización efectiva y eficiente debe tener trabajadores competentes. En términos de SSL, es esencial que los trabajadores tengan acceso a la información y que hayan recibido la capacitación adecuada para evitar accidentes o enfermedades. La competencia puede incluir:

- Capacidad para cumplir los roles laborales definidos y una comprensión de los aspectos de SSL requeridos.
- Métodos definidos de reclutamiento con consideración para trabajadores temporales o de agencias.
- Conciencia de los peligros asociados con el medio ambiente y los procesos.
- Requisitos legales.
- Capacidades individuales que incluyen experiencia, habilidades lingüísticas, alfabetización y diversidad.

La diversidad de actividades dentro de la organización determinará el nivel de capacitación requerido para cumplir con la competencia. Las deficiencias de capacitación se identifican con el desarrollo de nuevos procesos, por ejemplo, la introducción de nueva maquinaria o el cumplimiento de los requisitos reglamentarios.

Independientemente del tamaño de la organización, los registros de capacitación son esenciales como referencia y evidencia del cumplimiento de la misma Considere una matriz de capacitación general que identifica las deficiencias, incluidas las fechas de actualización de capacitación. Además, considere los registros de capacitación individual con evidencia firmante del trabajador para reconocer la finalización y comprensión de la capacitación, incluida la conciencia de los peligros.

La organización debe considerar la competencia de los proveedores externos, incluidos los contratistas que realizan tareas en sus instalaciones. El proceso de contratación de la organización puede proporcionar la estructura para la gestión de proveedores externos, incluyendo evidencia de capacidad, competencia. Esto puede ser apoyado con formación extra.

Ya sea interna o externamente, la gerencia de la organización debe confiar que existen mecanismos para brindar a los trabajadores capacitación adecuada y suficiente basada en la competencia de SSL.

Concienciación

La concienciación sobre requisitos del sistema de SSL es fundamental para los trabajadores internos y externos. Debe haber una comprensión clara de dicha política, incluyendo el requisito de que las personas se protejan a sí mismas y a otros de los peligros. La concienciación comienza antes del comienzo del trabajo para los trabajadores internos y externos y puede incluir:

- Política y requisitos de SSL.
- Peligros asociados con el medio ambiente y los procesos.
- Medios para reportar incidentes y recibir información tras su investigación
- Medios para reportar fallos o defectos potenciales o críticos
- Estructura de supervisión
- Suministro de información, incluidos sistemas seguros de trabajo o instrucciones de trabajo.
- Comprensión clara de que no hay recriminaciones por informar sobre peligros. Esto debe fomentarse activamente como parte de una cultura de seguridad positiva.

Se recomienda que exista evidencia de la capacitación en concienciación. Esto se describe en la sección 7 "Competencia".

Communicación interna y externa

Los canales de comunicación definidos son clave para el éxito del sistema de gestión de SSL. Se recomienda que exista una política clara sobre la comunicación respaldada por la gerencia que identifique el proceso de comunicación. La organización deberá determinar:

Pregunta	Ejemplos
¿Qué se comunicará?	Política de SSL, responsabilidades, riesgos, evaluación de riesgos, instrucciones de trabajo, actas de reuniones, resultados de investigación, estructura organizacional, desempeño...
¿Cuándo se comunicará?	Contratación permanente o temporal, formación interna y externa, sesión informativa, reuniones del comité de seguridad, requisitos legales...
¿A quién irá destinada la información?	Trabajadores, contratistas, proveedores externos, usuarios finales y otras partes interesadas.
¿Cómo se comunicará la información?	Tablón de anuncios, charlas, e-mail, sitio web, boletines informativos, supervisión...

Información documentada

El alcance de la información documentada variará según el tamaño, alcance y complejidad de los procesos dentro de la organización. Un enfoque práctico para el desarrollo y control de la información documentada ayudará en la protección del negocio y proporcionará fuentes de información para los trabajadores relacionadas con la identificación de peligros. Considere un enfoque basado en riesgos para el nivel de información documentada requerida, incluida la consideración de la alfabetización y el lenguaje. La información documentada puede disponerse en formao impreso o electrónico. A continuación se muestran ejemplos de información documentada:

Fuentes internas y externas	Tipo	Uso
Externa	Regulación	Instrucciones de la web del gobierno, códigos de prácticas
Externa	Información	Hojas de datos de seguridad del material del proveedor externo, certificados de conformidad
Externa	Información	Instrucciones de instalación y especificaciones técnicas de proveedores externos
Externa	Información	Evaluación de riesgos y métodos de declaración
Externa	Certificados	Sistema contra incendios, registros de cableado, seguro de responsabilidad
Externa	Formación	Certificados de competencia (carretilla, concienciación SSL)
Interna	Formación	Presentaciones de formación, actas de charlas
Interna	Formación	Registros de formación individual
Interna	Trabajo	Sistemas de trabajo seguros, instrucciones de trabajo
Interna	Inspecciones	Evidencia de mantenimiento e inspección rutinarias

Métodos de control de la Información documentada

Es esencial tener un sistema de control robusto y simple para la información documentada. Esto asegurará que los trabajadores estén siempre al tanto de los últimos requisitos respecto a SSL. Para respaldar la última revisión de la información documentada, deben existir medios para comunicar las últimas políticas, prácticas e instrucciones de trabajo. La información documentada provendrá de fuentes internas y externas. A continuación se presentan los medios sugeridos para controlar la información documentada.

Internos

- Desarrolle un sistema de referencia dentro del encabezado o pie. Ejemplo: Procedimiento de mantenimiento Nº1 - MP01, Formulario de mantenimiento 01 - MF01, etc.
- IIdentifique el estado de revisión, la fecha de revisión y el autor dentro del pie de página del documento.
- Utilice la misma metodología de control de documentos para documentos y datos electrónicos.
- Desarrolle una hoja de cálculo que identifique las razones por las cuales se han actualizado las revisiones anteriores.
- Determinar el método de emisión de información documentada, incluyendo recuperación de información y comunicación documentada previamente modificada.
- Archivar en formato electrónico revisiones previas de documentos basadas en el riesgo, asegurando que haya un medio para hacer copias de seguridad y recuperar datos.
- Determine e identifique en una hoja de cálculo la escala de tiempo de retención de los documentos. Esto puede basarse en requisitos legales como la documentación del seguro.

Externos

- Determinar qué se debe comunicar y retener según el riesgo.
- Considere escanear para reducir la dependencia del papel.
- Mantenga la integridad de la información documentada.

Recuerde crear un sistema simple para que todos lo comprendan y sea accesible. Considere apoyar el método elegido con un procedimiento de instrucción y una formación en su uso.

SECCIÓN 8: OPERACIÓN

Una vez identificados los procesos dentro de la organización (ver cláusula 4.4) y planificados, así como el método de operación del negocio (ver cláusula 6.0), la compañía necesitará planificar y controlar cada proceso dentro del sistema de gestión de SSL.

La planificación y el control operativos es el método en que la organización determina qué se requiere para cada proceso y el método de control para garantizar que los trabajadores estén protegidos contra daños. La planificación y el control operativos se logran identificando los criterios para cada proceso, que pueden incluir:

- **Los límites de cada proceso y cómo interactúan.**
- **Recursos requeridos para gestionar el proceso, incluidos liderazgo, equipo, tiempo, humanos (aspectos de competencia y formación) y financieros.**
- **Información documentada requerida para la gestión del proceso, incluidos los procedimientos y los sistemas de trabajo seguros.**
- **El método de planificación y control de cambios en los procesos, incluidos los eventos no deseados.**
- **Aplicación de requisitos legales y de otro tipo o instrucciones del fabricante para el equipo.**
- **Controles de ingeniería, por ejemplo, protecciones entrelazadas y sistemas de escape.**

La organización también debe considerar la adaptación del ambiente de trabajo para garantizar que sea adecuado para los trabajadores. La adaptación puede consistir en la formación de nuevos trabajadores o la modificación ergonómica de procesos para proteger a los trabajadores de daños y mejorar la eficiencia del proceso.

Eliminación de peligros y reducción de riesgos de SSL

Una vez elegida la metodología para la evaluación de riesgos determinada en la cláusula 6.0, la organización utilizará el la "jerarquía de control" para eliminar o reducir los peligros al menor riesgo posible. Es esencial que al realizar la evaluación de riesgos, los trabajadores y proveedores externos, sean competentes. Los resultados de la evaluación de riesgos deben comunicarse a los trabajadores directamente afectados, para ayudar a desarrollar medidas de control. Los trabajadores deben ser incluidos en el proceso de evaluación y otros elementos del sistema.

Gestión del cambio

Todos sabemos que pueden ocurrir accidentes cuando los procesos se desvían de las medidas de control establecidas. Esto puede incluir cambios en la supervisión, trabajadores o en la introducción de nuevos materiales, maquinaria y procesos.
La organización debe definir e implementar un proceso que considere el cambio en todo el negocio. Esta puede ser una política escrita que explique diferentes escenarios basados en el riesgo y la oportunidad. El proceso de cambio puede estar respaldado por un sistema documentado para acusar recibo y recibir la notificación para garantizar que se comunique y se entienda. La notificación de cambio puede estar respaldada por requisitos de capacitación y competencia. El proceso de cambio podría incorporar un mecanismo para evaluar y prevenir la introducción de nuevos peligros. Entre los ejemplos de eventos en los que podría ser necesaria la gestión del cambio se incluyen:

Evento cambio	Método de gestión
Pérdida de empleados competentes	Organización de la formación del personal existente apoyado con un proveedor externo hasta que el empleado sea competente.
Ausencia de personal de primeros auxilios	Capacite temporalmente al personal en medios alternativos para recibir tratamiento de primeros auxilios.
Introducción de nueva maquinaria	Designe un gerente de proyecto para coordinar la implementación, la evaluación de riesgos, la instrucción, la capacitación y la supervisión. Provisión de evaluación de riesgos y declaración del método de instalación. Documentos de control basados en recomendaciones del fabricante.
Inundación en instalaciones	Nombre un representante para evaluar riesgos y coordinar la reubicación del personal a un entorno seguro.
Introducción de nuevo software	Coordinación de gestión de proyectos, presentaciones y charlas, formación de competencia y concienciación.

General

La compra de bienes y servicios es un requisito para el funcionamiento de cualquier negocio. La norma requiere que la organización establezca controles para garantizar que los bienes y servicios adquiridos no presenten riesgos y no expongan a los trabajadores a daños, incluyendo contratistas.

Contratación

Un proceso de contratación robusto es esencial para controlar las entradas de productos y servicios en una organización. Los insumos pueden incluir materias primas para productos, equipos que incluyen maquinaria, consumibles como productos de limpieza y trabajadores que realizan tareas de mantenimiento. Se requiere que la organización desarrolle un proceso que incluya una evaluación del impacto en la seguridad de los productos y servicios antes de la compra. Esto requiere datos de seguridad del producto o material del proveedor o realizar una evaluación de riesgos. La evaluación identificaría los peligros potenciales y las medidas de control adecuadas para proteger tanto a los trabajadores de la organización como a los contratistas.

Considere la entrega de productos dentro del proceso, para asegurarse de que se inspeccionan según los requisitos especificados antes del lanzamiento. También servirá para garantizar que dichos productos y servicios cumplen legalmente. Esto puede hacerse a través de la evaluación de las hojas de datos de seguridad, declaraciones de conformidad o registros con asociaciones comerciales. El personal responsable de la adquisición debe asegurarse de utilizar trabajadores competentes para ayudar con las evaluaciones y comunicar la información del producto o servicio. Dicha información puede incluir hojas de datos de seguridad, formación, competencia e instrucciones de uso.

Contratistas y externalización

Muchas empresas utilizan los servicios de contratistas para cubrir ciertos procesos. La norma requiere que la organización realice una evaluación de esos contratistas, incluyendo verificaciones de competencia. La organización puede considerar el uso de criterios de selección de contratistas para garantizar que los servicios estén dentro del alcance.

La organización debe estar satisfecha de que exista un proceso para proteger a los contratistas y trabajadores que puedan estar expuestos a riesgos debido a sus actividades. Durante el proceso de contrataciónn, puede establecer acuerdos escritos entre la organización y el contratista que especifiquen las reglas de la organización. Esto puede estar respaldado por evaluaciones de riesgos y declaraciones de métodos realizadas por ambas partes y con comunicación de resultados.

Es vital realizar las verificaciones necesarias para garantizar que los contratistas sean competentes y que se cumplen los requisitos legales. Por ejemplo, solicitar la certificación para trabajar en un interruptor eléctrico o para trabajar en una caldera de gas.

Una vez se haya completado el proceso de contratación, habrá que implantar un programa de formación. Esto proporcionará a los contratistas una comprensión de las reglas y requisitos específicos, por ejemplo, los riesgos del sitio, las áreas autorizadas, los procesos de informes de fallos, los planes de acción en caso de emergencia, la supervisión y los permisos necesarios para trabajar.

Información documentada

La norma requiere que la organización mantenga información documentada relacionada con la adquisición de productos y servicios, incluidos contratistas.
A continuación se muestra una lista de ejemplos de información documentada:

- Evaluación de riesgos y método de declaración entre la organización y el contratista.
- Hojas de información de material de seguridad.
- orrespondencia relativa a temas de seguridad.
- Certificados de conformidad: Arneses, protección, parada de emergencia, equipos de protección personal...
- Permisos y licnecias del contratista.
- Cuestionario de proveedor completo.
- Registros de formación del trabajador.

Preparación y respuesta ante emergencias

La planificación de eventos inesperados es una buena disciplina organizativa. El proceso de evaluación de riesgos según la ISO 45001 puede haber puesto en relieve posibles situaciones de emergencia con posibles consecuencias catastróficas. Por lo tanto, es necesario establecer medidas de control para mitigarlos.

Una vez identificadas las situaciones de emergencia, que puede solicitar de trabajadores a todos los niveles, se necesitará formualr un plan y probarlo.Compruebe la preparación y respuesta ante emergencias dentro del plan de auditorías internas.

Las pruebas a los planes de respuesta ante emergencias son críticas para crear conciencia sobre posibles eventos y garantizar el funcionamiento de las medidas de control, incluyendo supervisión, responsabilidades,formación y comunicación. A continuación se presentan algunos ejemplos de situaciones y planes de emergencia:

Evento	Recomendación
Provisión de primeros auxilios	Prueba de respuesta de primeros auxilios (turnos, disponibilidad de equipo, personal competente...)
Simulacro de evacuación	Alarma, contacto con los servicios de emergencia, responsabilidad de los trabajadores, evacuación, cambios en el diseño del edificio...
Amenza de bomba	Activar alarma, evacuación a un área segura, método controlado para activar la alarma.
Fuga de productos químicos	Activar alarma, evacuación, contención, disponibilidad de hojas de datos de seguridad del material.

Una vez que el plan haya sido probado, es importante proporcionar a los trabajadores retroalimentaión sobre los resultados. Es un requisito disponer de información y registros adecuados como información documentada.

SECCIÓN 9: EVALUACIÓN DEL DESEMPEÑO

La evaluación del desempeño es un proceso constructivo que tiene como objetivo mejorar la operación de una organización y es crucial para el modelo PHVA prescrito por la ISO 45001. Estos procesos deberían ayudar a lograr y apoyar la estrategia y los objetivos de la organización.

Seguimiento, medición, análisis y evaluación

Una organización debe verificar, revisar, inspeccionar y observar sus actividades planificadas para asegurarse de que ocurren según lo previsto. También debe asegurarse de haber determinado los procesos apropiados, para evaluar el desempeño en función del riesgo y las oportunidades. Generalmente, el seguimiento indica procesos que pueden verificar si algo está ocurriendo según lo previsto.

Las siguientes tablas muestran ejemplos de seguimiento y medidas de control específicas:

Evento	Sistema de ventilación local
Seguimiento	Persona designada para inspeccionar semanalmente el sistema de ventilación para eliminar los humos.
Medición	Uso de un medidor calibrado para verificar el flujo de aire en dos ubicaciones del sistema de acuerdo con una Instrucción de trabajo especificada. (El empleado está capacitado y es competente para usar el equipo).
Análisis	Revisión de los datos que determinan la eficiencia del flujo de aire del sistema para garantizar la seguridad de los trabajadores. Debe cumplir con las especificaciones del fabricante y los requisitos reglamentarios.
Evaluación	El análisis de tendencias indica una reducción en el flujo de aire, por lo tanto, el mantenimiento se activa para aislar e inspeccionar el sistema.

Evento	Salidas de emergencia
Seguimiento	Persona designada para la inspección diaria de salidas de emergencia para asegurarse de que estén en condiciones y evitar resbalones, tropiezos y caídas.
Medición	Inspección visual para asegurar que no haya obstrucciones en las salidas definidas. (Por lo general, la medición se asocia con equipos de medición para obtener datos).
Análisis	Examen de los resultados de las inspecciones.
Evaluación	Determinación de la causa raíz.



Cualquier equipo utilizado para determinar el "indicador" de medición debe calibrarse y mantenerse de modo que se gane un alto grado de confianza en la credibilidad de los datos. La norma requiere que la organización implemente un proceso para evaluar el cumplimiento legañ, que incluya:

- Frecuencia y método de evaluación.
- En caso de requirir acción, el proceso en que será evaluado e implantado.
- Mantener conocimiento y comprensión del estatus de cumplimiento.
- Retener información documentada para soportar la evaluación legal y de otros requisitos.

Puede considerar incluir una lista de obligaciones de cumplimiento dentro de una hoja de cálculo como se describe en la sección 6 de este documento. Este proceso debe auditarse dentro del programa de auditoría interna para garantizar que se hayan cumplido todas las obligaciones de cumplimiento. Los resultados de la auditoría, incluido el estado de cumplimiento, deben comunicarse a la gerencia. Cualquier requisito pendiente o pendiente puede ser procesado por el equipo de liderazgo. Esto garantizará el cumplimiento de las obligaciones y la reducción del riesgo, incluido el posible juicio.

Auditoría interna

Una auditoría interna es un método sistemático para verificar los procesos y requisitos de la organización, así como los detallados en la norma ISO 45001. Esto asegurará que los procesos sean efectivos y que se cumplan los procedimientos. El programa de auditoría interna ayudará a la organización a alcanzar los objetivos y metas de SSL. Ayuda con:

- Monitorear el cumplimiento de la política y los objetivos.
- Proporcionar evidencia de todos los controles necesarios
- Asegurar cumplimiento derequisitos legislativos y de otro tipo .
- Evluar la efectividad de la gestión de riesgos.
- Compromiso de los trabajadores hacia la cultura de seguridad.
- Identificar la mejora para revisar un proceso desde otro ángulo.
- Ayuda con la mejora continua.

Las auditorías internas deben ser realizadas por personal competente con cierto grado de imparcialidad en el área auditada. Se puede aplicar un enfoque basado en riesgos a las áreas que se auditan con un mayor enfoque o en las actividades de mayor riesgo. Las auditorías internas deben planificarse para ser auditadas a intervalos regulares.

Además se pueden realizar auditorías no planificadas en áreas problemáticas, informes de posibles fallos o datos de incidentes con enfoque en la prevención de accidentes.

Es beneficioso comunicar los resultados de la auditoría a las partes interesadas, y establecer plazos de finalización realistas para las "oportunidades de mejora" o "no conformidades" identificadas. La grerencia debe ser consciente de las deficiencias del sistema para garantizar que se puedan asignar los recursos para mitigar los hallazgos. Los resultados de la auditoría se revisarán en la revisión por la dirección.

Revisión por la dirección

La Revisión por la dirección es un elemento esencial del Sistema de Gestión de SSL. El objetivo de la revisión es que la gerencia evalúe el rendimiento del sistema de gestión para garantizar que haya sido eficaz y adecuado para las necesidades del negocio, evitando en última instancia lesiones o daños a los trabajadores. También es una actividad planificada para revisar los objetivos, incluido el cumplimiento, y para establecer nuevos objetivos.

Por lo general, las reuniones de revisión por la dirección se llevan a cabo anualmente, sin embargo, muchas organizaciones realizan revisiones cada seis o tres meses para rastrear el desempeño del sistema. Si se llevan a cabo reuniones más frecuentemente, la agenda de la reunión se verá reducida.

La tabla de la página siguiente proporciona una descripción general de los requisitos de la agenda de revisión por la dirección.

9.3 Referencia normativa	Sumario de requisitos para la agensión por la dirección/cláusula de referencia
a)	Proporcione un resumen del estado de las acciones de la revisión por la dirección anterior. Esto incluirá tareas completadas o incompletas y justificaciones para su estado. Esta información se puede preparar previo a la reunión.
b1)	Explique cualquier cambio en los problemas internos y externos relevantes para el contexto de la organización para garantizar que se cumplan las necesidades y expectativas de las partes interesadas y trabajadores.
b2)	Además del B1, tenga en cuenta los cambios o cambios pendientes en los requisitos legales y otros requisitos y acciones para abordar las obligaciones de cumplimiento.
b3)	Si existen diferencias o cambios en el riesgo y las oportunidades de la organización, se deben anotar, explicar y discutir en la sección siguiente.
c)	Revise si se ha logrado el cumplimiento de la política y los objetivos de SSL. Es una buena práctica colocar los objetivos dentro de una tabla, alinear los indicadores clave de desempeño para lograrlos y comentar si se han logrado o no. Esto también indicará el estado de cumplimiento de la mejora continua.
d1)	Discuta cualquier incidente o no conformidad que haya ocurrido desde el último período de revisión. ¿Hay alguna tendencia y qué medidas se han tomado para evitar que vuelva a ocurrir?
d2)	Determine si el seguimiento y la medición han sido efectivos para cumplir con las expectativas. Si la evidencia sugiere que no han sido eficaces, la gerencia podrá influir en la mejora.
d3)	Discuta el estado de cumplimiento de los requisitos legales y de otro tipo. Esto puede incluir evidencia para respaldar el cumplimiento, incluidos los métodos de determinación y las fuentes de información. Discuta los requisitos legales y otros requisitos pendientes.
d4)	Discuta los resultados de las auditorías internas y las acciones que se han tomado para resolver cualquier no conformidad. Discuta las áreas de mejora y las áreas que funcionan correctamente.
d5)	Consulta de trabajadores a través de retroalimentación de las reuniones y acciones del comité de seguridad para abordar riesgos y oportunidades. Otros procesos para garantizar la seguridad de los trabajadores.
d6)	Analice los riesgos y oportunidades, incluido el desempeño de la identificación de peligros y oportunidades para mitigar el daño a los trabajadores. Puede revisar los hallazgos significativos de las evaluación de riesgos.
e)	Considerando la información discutida en las secciones anteriores, ¿hay suficientes recursos para mantener y mejorar continuamente el sistema de gestión? La gerencia es clave para influir en la mejora en este área.
f)	Discuta las comunicaciones con las partes interesadas, esto puede incluir autoridades reguladoras o proveedores externos que proporcionan materiales que tienen un impacto en la seguridad.
g)	Discusión general con la provisión de información sobre cómo funciona el sistema de gestión de SSL y cómo puede mejorar continuamente en el futuro.

Al finalizar la reunión de revisión por la dirección, la organización debe decidir lo que se necesita para mejorar continuamente la SSL y cumplir con la norma. Los siguientes puntos resumen los requisitos de salida de la reunión de revisión por la dirección:

- Proporcionar una conclusión amplia de la estabilidad, adecuación y efectividad continuas para lograr los resultados previstos.
- Identificar oportunidades de mejora continua.
- Identifique cualquier cambio requerido en el sistema de gestión de SSL.
- Identifique los recursos necesarios.
- Identifique las acciones necesarias.
- Identifique cualquier mejora de integración con otros procesos comerciales. Esto puede incluir una mejor armonización con los sistemas de gestión ISO 9001 o ISO 14001.
- Cualquier implicación para la dirección estratégica del negocio. Este es un requisito de amplio alcance para capturar cualquier tema para mejorar el sistema de gestión de SSL.

La organización debe registrar las actas de la reunión dentro de la información documentada. Esta información debe comunicarse a las partes interesadas relevantes y, cuando corresponda, a los representantes de los trabajadores.

Recomendfamos transferir los objetivos de la revisión por la dirección a un documento separado con indicadores clave de desempeño identificados, plazos de tiempo esperados y responsabilidades delegadas. Estos objetivos pueden comunicarse a través del correo electrónico de la organización o colocarse en tablones de anuncios.


C
D
E
600
550
400
900
760
650
600
300
200
240
1000

SECCIÓN 10: MEJORA

- Resultados discutidos en la Sección 9 Revisión por la dirección, incluido el análisis y la evaluación del desempeño de SSL, la auditoría interna y la retroalimentación del compromiso de los trabajadores
- No conformidad y acción correctiva
- Investigación del incidente y acción correctiva
- nvestigación del accidente y acción correctiva
- Obligaciones de cumplimiento, incluidos los resultados de la introducción de una nueva regulación.

Se pueden diseñar varios métodos diferentes para capturar oportunidades de mejora en el sistema en función de la estructura, las actividades y el riesgo dentro del negocio. Los métodos elegidos deben considerar lo siguiente:

- Medios de notificación, incluyendo incidentes de trabajadores y partes interesadas.
- Tiempo para la comunicación.
- Cómo se registrará la información documentada, por ejemplo, boletin de calificaciones, informes de accidentes, informes de defectos, informes a la gerencia...

- Uso de trabajadores para participar en investigaciones para determinar el análisis de causa raíz.
- Sistema estructurado para prevenir la recurrencia.
- Jerarquía de medidas de control para reducir el riesgo.

- Evaluación de riesgos de SSL antes de la introducción de una acción correctiva para prevenir la introducción de nuevos peligros.
- Capacitación y competencia para los trabajadores y las partes interesadas sobre los medios para informar sobre riesgos, incidentes y oportunidades de mejora en al SSL.



Incidente

A diferencia de los sistemas de gestión ISO 9001 e ISO 14001, la ISO 45001 presenta el "incidente" junto con la no conformidad y la acción correctiva. La cláusula 3 "Términos y definiciones" proporciona los parámetros en los que se puede interpretar e informar de un "incidente". Un "incidente" es un suceso que no resulta en una lesión y/o enfermedad. Por lo tanto, la organización debe implementar un sistema de informes que recoja los eventos que no se han previsto dentro de los procesos del sistema de gestión. A menudo, estos se denominan "incidentes potenciales". Cuando se informa de un incidente potencial, puede darse un proceso en el que se registran dentro de un informe de no conformidad, mientras se invetigan los resultados.

Ejemplo básico de proceso de comunicación de incidente que conduce a no conformidad, acción correctiva y mejora continua.

Proceso	Evento	Sistema de gestión
Incidente	• Durante una maniobra de marcha atrás un vehículo de reparto casi atropella a untrabajador.	• El conductor ha realizado la formación de entrada, incluyendo el mapa de la sede.
Informe de fallo potencial	• El trabajador rellena un boletin de calificaciones que describe la ocurrencia con la ayuda del supervisor.	• Documento de potencial fallo disponible en toda la sede y entregado durante la formación inicial.
Acción correctiva	• Se colocan conos inmediatamente para evitar que el supervisor ingrese al área del incidente.	• Acción correctiva temporal.
Investigación	• El supervisor tiene una charla con el conductor en relación con las circunstancias. • El gerente del alamcén discutee el incidente y revisa la evaluación de riesgos asociada. • Trabajadores del área proporcionan información.	• Detalles registrados como parte de investigación • Revisión de evaluación de riesgos.
Solución de mentalidad basada en riesgo	• Después de la revisión de la evaluación de riesgos, se colocan barreras físicas en la pasarela peatonal a mode de separación. • Instalación de luces adicionales. • Las barreras se incorporan al programa de mantenimiento.	• Evaluación de riesgos revisada. • Formación del conductor modificada para incluir las barreras. • Informe de no conformidad completado con análisis de causa raiz. • Registrado en el informe de incidentes. • Actualización del programa de mantenimiento.
Comunicación	• Se informa al conductor de retoalimentación sobre el incidente y su cierre. • Lo mismo sucede con el empleado sufre el potencial accidente.	• Informe de incidente para la empresa transportes • El trabajador denunciante firma la acción correctiva como evidencia de retroalimentación positiva.
Revisión	• Se discute del incidente en el comité de seguridad y reuniones de la dirección. • El supervisor informa de la efectividad de los cambios introducidos.	• Actas de reunión del comité de seguridad y gerencia. • Actas del comité publicadas en boletines informativos.
Revisión por la dirección	• Resultado del incidente y resultado positivo dentro de las estadísticas.	• Revisión de fallo potencial. Comunicación de la minuta de revisión por la dirección. • Se agrega una auditoría regular de rutas peatonales al programa de auditoría interna como parte de un objetivo de mejora.
Resultado en la mejora continua		

SACAR EL MÁXIMO DE SU SISTEMA DE GESTIÓN

Los consejos clave para sacar el máximo de su sistema de gestión de SSL son:

1. Para tener un sistema de gestión de SSL efectivo, la gerencia debe comprometerse con la implantación y mejora continua del mismo.

2. Desarrolle el sistema de gestión como una herramienta para proteger a los trabajadores y los intereses del negocio, no solo para satisfacer la norma.

3. Utilice el contexto para comprender cómo puede la organización afectar interna y externamente a la SSL, incluyendo a los trabajadores.

4. Informe a las partes interesadas y trabajadores de sus objetivos al implantar la norma con el fin de desarrollar una cultura de seguridad positiva.

5. Al diseñar los procesos, asegúrese de que estos son relevantes para su contexto. En otras palabras, no complique demasiado el sistema.

6. Construya los requisitos de la norma en procesos y controles. La seguridad no es un complemento.

7. Considere integrar la norma en un sistema de gestión integrado con ISO 9001 (calidad) o ISO 14001 (medioambiente). Esto ayudará a integrar la mentalidad de la gerencia y trabajadores respecto a la cultura de seguridad y salud en el trabajo.

8. La implantación de la norma no debe ser una carga para su organización. La mentalidad basada en riesgos y la participación de los trabajadores mejorarán la cultura de seguridad y la productividad de su organización.



PASOS TRAS LA IMPLANTACIÓN

1 FORMACIÓN DE CONCIENCIACIÓN

- Su organización debe crear conciencia sobre los diversos estándares cubiertos por el sistema
- Debe celebrar reuniones de capacitación separadas para los diferentes niveles de la gerencia, lo que ayudará a crear un ambiente motivador, listo para la implantación.

2 POLÍTICA Y OBJETIVOS

- Su organización debe desarrollar una política de SSL/integrada y objetivos relevantes para ayudar a cumplir los requisitos.
- Al trabajar con la gerencia, su empresa debe realizar talleres con todos los niveles de personal de gestión para delinear los objetivos integrados.

3 ANÁLISIS DE DEFICIENCIAS INTERNO

- Su organización debe identificar y comparar el nivel de cumplimiento de los sistemas con los requisitos de las normas de su nuevo sistema.
- Todo el personal relevante debe comprender las operaciones de la organización y desarrollar un mapa de procesos para las actividades del negocio.

4 DOCUMENTACIÓN/PROCESO DE DISEÑO

- La organización debe crear documentación de los procesos según los requisitos de las normas relevantes.
- Debe redactar e implantar un manual, procedimientos funcionales, instrucciones de trabajo, procedimientos del sistema y proporcionar los términos asociados

5 DOCUMENTACIÓN/PROCESO DE IMPLANTACIÓN

- Los procesos/documentos desarrollados en el paso 4 deben implementarse en toda la organización y abarcar todos los departamentos y actividades.
- La organización debe realizar un taller sobre la implementación según corresponda para los requisitos de la norma ISO.

6 AUDITORÍA INTERNA

- Un sistema de auditoría interna robusto es esencial. Recomendamos la formación de auditor interno y NQA puede proporcionar dicha formación para las normas que esté implantando.
- Es importante implementar acciones correctivas para las mejoras, en cada uno de los documentos auditados, a fin de cerrar las deficiencias y garantizar la eficacia del sistema de gestión.

7 ORGANIZAR LA REVISIÓN POR LA DIRECCIÓN DEL SISTEMA

- La gerencia de debe revisar varios aspectos comerciales de la organización, que son relevantes para las normas a implantar.
- Revise la política, los objetivos, los resultados de la auditoría interna, los resultados del desempeño del proceso, los resultados de las quejas, el cumplimiento legal, los resultados de la evaluación de riesgos/incidentes y desarrolle un plan de acción y un acta de revisión.

8 ANÁLISIS DE DEFICIENCIAS DE SISTEMAS IMPLANTADOS

- Debe realizar un análisis de deficiencias para evaluar la efectividad y el cumplimiento de la implantación del sistema en la organización.
- Este análisis de deficiencias preparará a su organización para la auditoría de certificación final.

9 ACCIONES CORRECTIVAS

- La organización estará lista para la auditoría de certificación final, siempre que el análisis de deficiencias y todas las no conformidades (NC) hayan recibido acciones correctivas.
- Verifique que todas las NC significativas estén cerradas y que la organización esté lista para la auditoría de certificación final.

10 AUDITORÍA DE CERTIFICACIÓN FINAL

- Una vez completada la auditoría de forma satisfactoria, su organización recibirá el certificado.
- ¡Enhorabuena!



USEFUL LINKS

Health and Safety Management Training
https://www.nqa.com/training/health-safety-management

The Institution of Occupational Safety and Health
https://www.iosh.co.uk/

The Health and Safety Executive
http://www.hse.gov.uk/

Authored on behalf of NQA by: Alister Constantine