

The LRQA logo is enclosed in a teal square border. The letters 'LRQA' are in white, with a teal diagonal line through the 'A'.

LRQA

Un enfoque integrado a los sistemas de gestión

Agregando un elemento de seguridad
de la información



El cambio hacia la estandarización

Los mercados actuales requieren que las empresas tengan en cuenta un amplio rango de componentes que definen el éxito. Los sistemas y procesos de gestión implementados en forma efectiva pueden respaldar todos los impulsores de la efectividad organizacional. También ayudan a introducir una mentalidad de mejora continua, que se encuentra en la base de cualquier buena empresa.

Desde que se introdujo la ISO 9001, la norma internacional que define los requisitos de un sistema de gestión de la calidad, más de un millón de organizaciones ha alcanzado la certificación. En la actualidad es uno de los documentos empresariales más importantes que se hayan escrito jamás.

Después del éxito de la ISO 9001, se han publicado muchas normas adicionales, y más organizaciones comenzaron a implementar varios sistemas de gestión; y cada uno de ellos requiere la certificación independiente de una tercera parte. Como resultado, queda claro que la falta de consistencia en la estructura y el contenido de diferentes normas de la ISO dificultan en gran medida un enfoque más integrado. A modo de solución, la ISO introdujo el Anexo SL.



El rol del Anexo SL

El Anexo SL es el marco que deben respetar todas las normas de sistemas de gestión ISO nuevas y revisadas.

Para asegurarse de que las normas son consistentes y compatibles entre sí, el Anexo SL incluye cuatro temas clave:

Estructura de alto nivel

Esta es la base del Anexo SL y contiene diez cláusulas, desde alcance hasta planificación y mejora.

Reduce drásticamente la duplicación del esfuerzo y tiene sistemas de gestión que siguen el mismo conjunto de requisitos básicos.

Texto principal idéntico

Como mínimo, las normas de los sistemas de gestión tendrán al menos 84 requisitos genéricos, más cualquier requisito adicional específico de cada disciplina.

Esto ayuda a garantizar que los materiales relacionados con las normas sean claros, repetibles y fáciles de entender para las personas que trabajan en varias áreas.

Términos y definiciones comunes

Hay 22 términos y definiciones que deben abordarse en todas las normas. Por ejemplo, “parte interesada” es el término que se prefiere a “accionista”, y “liderazgo” reemplaza a “responsabilidad gerencial”.

Enfoque basado en riesgo

El Anexo SL ayuda a que las organizaciones adopten un enfoque sistemático y proactivo hacia el riesgo. Esto reduce la ocurrencia y el impacto de eventos no deseados y promueve la mejora continua.

Cláusula 1	Alcance
Cláusula 2	Referencias normativas
Cláusula 3	Términos y definiciones
Cláusula 4	Contexto de la organización
Cláusula 5	Liderazgo
Cláusula 6	Planificación
Cláusula 7	Soporte
Cláusula 8	Operación
Cláusula 9	Evaluación del rendimiento
Cláusula 10	Mejora

La estructura de alto nivel del Anexo SL

Implementación fácil

La compatibilidad que introduce el Anexo SL facilita la integración de los requisitos de varias normas en un único sistema. Como resultado, para una organización ahora es mucho más directo agregar nuevos sistemas de gestión basados en el Anexo SL y combinarlos con los existentes.

Este es un enfoque más práctico que reduce la duplicación y crea un sistema en el cual las numerosas partes trabajan en pos del mismo conjunto de metas estratégicas. El Anexo SL brinda a las organizaciones un marco de mejor práctica para gestionar otros procesos que no se han elegido para la certificación.

Por medio de la integración, las organizaciones pueden usar sus recursos con más eficiencia y adoptar un enfoque estandarizado hacia la documentación. También pueden mejorar la gestión de operaciones y procesos esenciales.

Caso de estudio

Terex Trucks

Terex Trucks fue una de las primeras organizaciones en hacer la transición hacia la ISO 9001:2015.

Gracias al Anexo SL, Terex Trucks obtuvo beneficios de los puntos en común entre las normas. Esto permitió la integración de los sistemas de gestión de calidad (SGC) y de medioambiente (SGA).

“ Hay muchos puntos en común entre las dos normas (ISO 9001 e ISO 14001); y ahora, con las dos siguiendo la estructura introducida por el Anexo SL, pudimos aprender del trabajo que terminamos en nuestro SGC para integrar nuestro SGA al mismo tiempo.

Nuestras estadísticas de rendimiento confirman que cumplimos con éxito nuestras metas para el SGC y el SGA; y seguiremos construyendo sobre esto en el futuro a través del desarrollo de nuestro sistema de gestión.”

Un proceso de certificación optimizado

Las ventajas de la integración no se limitan a la implementación de sistemas de gestión.

Cuando una organización designa a un organismo de certificación, como LRQA, las auditorías integradas impulsan un enfoque más eficiente. Por ejemplo, es posible que la estructura de alto nivel se revise solo una vez, lo cual podría reducir la cantidad requerida de visitas al sitio.

Por medio de la integración, las organizaciones también establecen relaciones a largo plazo con los organismos de certificación y los auditores.

Debido a la exposición a varios sistemas, los auditores desarrollan un conocimiento profundo y holístico de la empresa y sus metas, así como de su modus operandi. Esto permite entregar perspectivas más profundas, que conllevan un mayor impacto.

Evaluación remota

Al trabajar con LRQA, en muchos casos las organizaciones pueden elegir que sus auditorías se entreguen de forma remota utilizando tecnología segura. Esta opción brinda el mismo servicio de alta calidad con muchos beneficios adicionales, que incluyen flexibilidad, entrega rápida y acceso a conocimientos técnicos globales.

Las empresas pueden elegir también un enfoque combinado que optimiza el proceso general mediante auditorías remotas y, al mismo tiempo, utilizar opciones en sitio para construir relaciones sólidas.

Todos los clientes de LRQA que optan por una auditoría remota se benefician de la flexibilidad y conveniencia que brinda.

Sin embargo, esta les muestra también a las organizaciones cómo la tecnología generalizada puede aprovecharse para realizar una auditoría efectiva que no se vea limitada por las fronteras geográficas. Esto ayuda a que algunas empresas identifiquen cómo pueden utilizar la tecnología y plataformas similares para sus propios programas internos de supervisión y auditoría.



Incluir la ISO 27001 en su sistema de gestión integrado

La ISO 27001 es la norma internacional que describe los requisitos para un sistema de gestión de la seguridad de la información (SGSI).

Para cualquier organización, sin que importe su tamaño o sector, la ISO 27001 proporciona una base sólida para una estrategia completa de información y ciberseguridad. Describe un marco de mejor práctica que mitiga los riesgos y protege información fundamental para la empresa por medio de identificación, análisis y controles útiles.

Incluir la ISO 27001 en un sistema de gestión integrado más amplio es una forma ideal de garantizar que, como área de enfoque estratégico, se incorpore la mejor práctica de seguridad de la información en la organización.

Integrar la ISO 27001 con la ISO 9001

Gracias al Anexo SL, integrar la ISO 27001 con la ISO 9001 es cosa cada vez más popular. Ambas normas comparten una estructura similar y se enfocan en temas internos y externos, a pesar de los diferentes ángulos específicos de cada disciplina.

La integración de los requisitos de las dos normas en un único sistema asegura que los procesos de la organización estén alineados. Asimismo las similitudes entre las normas brindan la oportunidad de acelerar la implementación y usar los recursos con más eficiencia.

Los requisitos específicos son diferentes para cada norma. Sin embargo, a modo de ejemplo, las siguientes áreas comunes pueden abordarse con los mismos procesos y sistemas, y generar diferentes resultados:

- Partes interesadas
- Responsabilidades
- Sistema de gestión de la documentación
- Auditoría interna y revisión de gestión
- Sistemas para no conformidades y acciones correctivas

Extender su sistema para gestionar riesgos específicos de la seguridad de la información

En función del perfil de riesgo de una organización, otras normas y pautas ofrecen la oportunidad de expandir el sistema para tratar amenazas más específicas.

La ISO 27001 forma parte de la serie de normas ISO 27000. Dentro de la familia de la ISO 27000, hay varias otras normas y pautas, que son extensiones de la ISO 27001.

Estas normas y pautas adicionales describen controles relacionados con áreas como privacidad y protección de datos (ISO 27701, ISO 27018), y seguridad en la nube (ISO 27017). La conformidad con normas adicionales como estas fortalece aún más el elemento de seguridad de la información en un sistema integrado. Garantiza que haya un enfoque más robusto y extenso hacia la gestión de riesgo en funcionamiento.

También es común que las organizaciones expandan su sistema integrado para que abarque la continuidad del negocio (ISO 22301) y, donde corresponda, la gestión del servicio de TI (ISO 20000-1).

Caso de estudio

OCTO Telematics

OCTO Telematics (OCTO) es un proveedor líder de servicios de telemática y análisis avanzado de datos para el sector de seguros.

OCTO implementó un sistema de gestión completo e integrado que fue auditado de forma remota y certificado por LRQA. Ayuda a la organización a mantener el ritmo con un panorama de amenazas a la seguridad de la información en constante evolución, mitigando los riesgos de forma proactiva antes de que ocurran.

“La estructura de alto nivel del Anexo SL, con su texto básico idéntico, términos y definiciones comunes, facilitó la integración de nuestros sistemas de gestión.”

“A través de la integración, OCTO pudo reducir el conflicto entre los sistemas individuales. También redujo la duplicación de los procesos, el trabajo administrativo y la burocracia en general. Esto permitió un enfoque mucho más fuerte en las necesidades de toda la empresa, y no solo en un área en particular.”

“Un SGSI certificado es una puerta de acceso para garantizar negocios con clientes importantes. Sin embargo, también le permitió a OCTO adoptar un enfoque orgánico hacia la seguridad del sistema, al extender el SGSI para gestionar adecuadamente las amenazas y oportunidades relacionadas con nuestro negocio.”

Attilio De Bernardo | Diretor de Segurança da Informação OCTO Telematics

Construir su sistema de gestión integrado con LRQA

Entendemos que su organización tiene requisitos únicos. Ya sea que se trate de una pequeña o mediana empresa que desea dar los primeros pasos hacia un sistema de gestión integrado o una gran empresa que busca niveles adicionales de evaluación, nuestro equipo de expertos trabajará de cerca con usted para comprender sus necesidades específicas.

LRQA brinda un rango de servicios de auditoría, certificación y capacitación acreditados en relación con las normas y esquemas líderes en el mundo: desde seguridad de la información hasta calidad y salud y seguridad.

Obtenga más información

Comuníquese con un miembro del equipo y programe una consulta gratuita para hablar sobre los requisitos de su organización y generar su solución de garantía.



YOUR FUTURE. OUR FOCUS.

Acerca de LRQA:

Al reunir una experiencia inigualable en certificación, garantía de marca y capacitación, LRQA es uno de los principales proveedores mundiales de soluciones de garantía y seguridad alimentaria. Trabajando junto con granjas, pesquerías, fabricantes de alimentos, restaurantes, hoteles y minoristas globales, ayudamos a gestionar los riesgos de seguridad alimentaria y sostenibilidad en todas las cadenas de suministro y nos hemos convertido en un proveedor líder de aseguramiento global.

Estamos orgullosos de nuestra herencia, pero lo que realmente importa es quiénes somos hoy, porque eso es lo que determina la forma en que nos asociamos con nuestros clientes en el futuro. Al combinar valores sólidos, décadas de experiencia en la gestión y mitigación de riesgos y un gran enfoque en el futuro, estamos aquí para ayudar a nuestros clientes a construir negocios más seguros y sostenibles.

De auditoría, certificación y capacitación de terceros independientes; a los servicios de asesoría técnica; a la tecnología de aseguramiento en tiempo real; a la transformación de la cadena de suministro impulsada por datos, nuestras soluciones innovadoras de extremo a extremo ayudan a nuestros clientes a negociar un panorama de riesgos que cambia rápidamente, asegurándose de que estén dando forma a su propio futuro, en lugar de dejar que él les dé forma a ellos.

Póngase en contacto

LRQA México

www.lrqa.com/mx
+52 (81) 8152-1000

LRQA Sudamérica

www.lrqa.com/cl
+56 (32) 221-7665



Se tiene el cuidado de garantizar que toda la información brindada sea precisa y actualizada. Sin embargo, LRQA no acepta ninguna responsabilidad por imprecisiones o cambios en la información.

Para obtener más información, consulte

www.lrqa.com/entities

© LRQA Group Limited 2021