


PREPARACIÓN PARA EL PROYECTO DE IMPLEMENTACIÓN ISO: UNA GUÍA EN UN LENGUAJE SENCILLO




ISO

SERIES
LIBROS
DE BOLSILLO

05

Un manual paso a paso para
profesionales ISO en pequeñas empresas



DEJAN KOSUTIC

Preparación para el proyecto de implementación ISO: una guía en un lenguaje sencillo

También de Dejan Kosutic:

[Ciberseguridad en 9 pasos: El manual sobre seguridad de la información para el gerente](#)

[Seguro & Simple: Una guía para la pequeña empresa para la implementación de la ISO 27001 con medios propios](#)

[Becoming Resilient: The Definitive Guide to ISO 22301 Implementation](#)

[ISO 27001 Risk Management in Plain English](#)

[ISO 27001 Annex A Controls in Plain English](#)

[Preparación para la auditoría de certificación ISO: Una guía en un lenguaje sencillo](#)

[Gestión de documentación ISO: Una guía en un lenguaje sencillo](#)

Dejan Kosutic

Preparación para el proyecto de implementación ISO: una guía en un lenguaje sencillo

*Un manual paso a paso para profesionales ISO en
pequeñas empresas*

Advisera Expert Solutions Ltd
Zagreb, Croatia

Copyright ©2017 by Dejan Kosutic

Todos los derechos reservados. Ninguna parte de este libro puede ser reproducida, almacenada en un sistema de recuperación, o transmitida en cualquier forma o por cualquier medio, electrónico, mecánico, fotocopia, grabación u otro tipo, sin el permiso escrito del autor, exceptuando la inclusión de breves citas en un informe.

Límite de responsabilidad / exención de garantía: Aunque que el editor y el autor han utilizado sus mejores esfuerzos en la preparación de este libro, no hacen ninguna representación o garantía con respecto a la exactitud o la exhaustividad de los contenidos de este libro, y específicamente niegan cualquier garantía implícita de comerciabilidad o idoneidad para un propósito en particular. Este libro no contiene toda la información disponible sobre el tema. Este libro no ha sido creado para ser específico para cualquier individuo, o para situaciones o necesidades específicas de una organización. Usted debe consultar con un profesional para cada caso. El autor y el editor no tendrán ninguna obligación o responsabilidad de cualquier persona o entidad con respecto a cualquier pérdida o daño incurrido, o alegado de haber incurrido, directa o indirectamente, por la información contenida en este libro.

Publicado por primera vez por Advisera Expert Solutions Ltd
Zavizanska 12, 10000 Zagreb
Croacia
Unión Europea
<http://advisera.com/>

ISBN: 978-953-8155-06-2

Primera edición, 2017

Título original: "Preparations for ISO Implementation Project: A Plain English Guide"

Traducido del Inglés por Antonio José Segovia

SOBRE EL AUTOR



Dejan Kosutic es autor de numerosos artículos, video tutoriales, plantillas de documentos, webinars y cursos sobre gestión de seguridad de la información, y sobre gestión de continuidad del negocio. Él también es el autor del blog líder sobre ISO 27001 & ISO 22301 y otros estándares ISO, y ha ayudado a varias organizaciones, incluyendo instituciones financieras, agencias gubernamentales, y empresas de TI, a implementar la gestión de la seguridad de la información según estos estándares. Tiene numerosos certificados, entre ellos el de Auditor Líder ISO 27001 y Auditor Líder ISO 9001.

Click aquí para ver su [Perfil en LinkedIn](#).

TABLA DE CONTENIDOS

SOBRE EL AUTOR	5
PREFACIO	8
1 INTRODUCCIÓN	10
1.1 LOS 5 MITOS MÁS COMUNES RELACIONADOS CON LOS ESTÁNDARES ISO / POR QUÉ ES NECESARIO LA PREPARACIÓN	10
1.2 ¿QUIÉN DEBERÍA LEER ESTE LIBRO?	13
1.3 LO QUE NO ES ESTE LIBRO	14
1.4 RECURSOS ADICIONALES	14
2 OBTENER LA PARTICIPACIÓN DE LA ALTA DIRECCIÓN Y OTROS EMPLEADOS	16
2.1 CÓMO CONVENCER A LA ALTA DIRECCIÓN PARA IMPLEMENTAR UN ESTÁNDAR ISO	17
2.2 CÓMO PRESENTAR LOS BENEFICIOS A LA ALTA DIRECCIÓN	20
2.3 EJEMPLO DE RETORNO DE LA INVERSIÓN (ROI) PARA SEGURIDAD DE LA INFORMACIÓN	22
2.4 TRATAR CON LA LÍNEA DE RESPONSABLES Y OTROS EMPLEADOS	24
2.5 FACTORES DE ÉXITO	25
3 PREPARACIÓN PARA EL PROYECTO DE IMPLEMENTACIÓN	27
3.1 ESTRATEGIA PARA LA IMPLEMENTACIÓN ISO: TRES OPCIONES..	27
3.2 CÓMO SELECCIONAR UN CONSULTOR	30
3.3 ¿DEBERÍA USAR UN ANÁLISIS DE BRECHA?	32
3.4 SECUENCIA DE IMPLEMENTACIÓN DE LOS ESTÁNDARES ISO & RELACIÓN CON EL CICLO PDCA.....	33
3.5 ESTABLECIENDO UNA ESTRUCTURA DE GESTIÓN DE PROYECTO..	34
3.6 QUIÉN DEBERÍA SER EL RESPONSABLE DE PROYECTO	36
3.7 ¿CUÁNTO PUEDE DURAR?	39
3.8 ¿CUÁNTO PUEDE COSTAR?.....	40
3.9 USAR HERRAMIENTAS Y PLANTILLAS.....	43
3.10 DECIDA SU ESTRATEGIA DE DOCUMENTACIÓN.....	46
3.11 FACTORES DE ÉXITO	49

4 MINI CASO DE ESTUDIO: OBTENER EL APOYO DE LA ALTA DIRECCIÓN EN UNA COMPAÑÍA DE PROPIEDAD ESTATAL.....	50
APÉNDICE A – LISTA DIAGRAMA DE IMPLEMENTACIÓN ISO 9001:2015.....	52
APÉNDICE B – DIAGRAMA DEL PROCESO DE IMPLEMENTACIÓN ISO 14001:2015.....	54
APÉNDICE C – DIAGRAMA DEL PROCESO DE IMPLEMENTACIÓN DE LA NORMA ISO 27001:2013	56
APÉNDICE D – DIAGRAMA DEL PROCESO DE IMPLEMENTACIÓN DE ISO 22301	58
APÉNDICE E – DIAGRAMA DEL PROCESO DE IMPLEMENTACIÓN OHSAS 18001:2007	60
APÉNDICE F – DIAGRAMA DEL PROCESO DE IMPLEMENTACIÓN ISO 13485:2016.....	62
APÉNDICE G – PLANTILLA: PROPUESTA DE PROYECTO PARA LA IMPLEMENTACIÓN ISO	64
APÉNDICE H – PLANTILLA: PLAN DE PROYECTO PARA LA IMPLEMENTACIÓN ISO.....	70
APÉNDICE I – LISTA DE PREGUNTAS PARA HACERLE A SU CONSULTOR ISO.....	77
BIBLIOGRAFÍA	81
ÍNDICE.....	83

Listado de Figuras

Figura 1: Palabras a evitar y palabras a usar cuando se presenta un proyecto ISO	21
--	----

PREFACIO

Cuando publicamos mi libro *Seguro & Simple: Una guía para la pequeña empresa para la implementación de la ISO 27001 con medios propios* el año pasado, me di cuenta rápidamente que mucha gente estaba buscando información sobre lo que necesitan para realizar su implementación de ISO 27001 adecuadamente.

Por lo tanto, he creado este libro más corto, una parte de una serie de libros de bolsillo, que se centra exclusivamente en cómo prepararse para la implementación. Este libro no se centra únicamente en ISO 27001 – la preparación para la implementación es igual para cualquier otro estándar, por lo que he adaptado este libro de tal manera que es perfectamente aplicable para ISO 9001, ISO 14001, ISO 27001, ISO 20000, ISO 22000, OHSAS 18001, ISO 13485 y IATF 16949.

Este libro, *Preparación para el proyecto de implementación ISO: una guía en un lenguaje sencillo*, es realmente un fragmento del libro *Seguro & Simple*, que ha sido editado con pequeños cambios. De esta manera, si compara las secciones de *Seguro & Simple* que hablan sobre la preparación para la implementación, podrá ver aquí en este libro las mismas secciones, con casi el mismo texto – como ya he mencionado, el texto ha sido adaptado de manera que pueda ser válido para cualquier ISO.

Pero, ¿por qué tener dos libros con casi el mismo texto? Porque quería proporcionar una lectura rápida a las personas que se centran exclusivamente en la preparación para la implementación, y no tienen tiempo (o necesidad) para leer un libro completo sobre la implementación de la ISO, es decir, un libro como *Seguro & Simple*.

También podría confundirle la longitud de este libro, que es bastante corto, dado que hay otros libros en el mercado que son mucho más extensos y detallados. ¿Es realmente posible explicar un tema tan complejo en un breve libro como este? Bueno, hay dos respuestas para esto:

En primer lugar, este libro se centra en la preparación para la implementación en empresas pequeñas - por lo tanto, he simplificado intencionadamente los pasos, para que de esta manera su preparación pueda ser más rápida, por lo que he dejado fuera todos los elementos que serían necesarios sólo en empresas grandes.

En segundo lugar, y lo más importante, he seguido mi misión de empresa: "Hacer fácil de entender, y fácil de usar, los entornos complejos." En otras palabras, es fácil complicar las cosas, pero es difícil hacer las cosas fáciles de entender. Por lo tanto, cuando empiece a leer este libro notará que eliminé todas las cuestiones que son difíciles de entender, todos los detalles innecesarios, y también se dará cuenta de que me he centrado exactamente en lo que hay que hacer, en un lenguaje entendible para principiantes, sin experiencia previa en la implementación del estándar ISO.

Por lo tanto, puede estar seguro: Si usted es una organización pequeña, usando este libro podrá conseguir usted mismo estar preparado para la implementación de su estándar ISO, incluso si es la primera vez que hace un proyecto de este tipo.

1

INTRODUCCIÓN

¿Cuáles son los errores más costosos que se pueden cometer con una implementación ISO? ¿Por qué es importante la preparación para el proyecto ISO? Y, ¿Este libro es la mejor elección para usted?

Este libro cubre la preparación para cualquier estándar ISO de gestión – ISO 9001, ISO 14001, ISO 27001, ISO 20000, ISO 13485, pero también para OHSAS 18001 e IATF 16949 (antiguamente ISO/TS 16949), por lo tanto, en el libro me referiré a “estándar ISO”, o simplemente “estándar”, para referirme a cualquiera de estos estándares.

Por otra parte, en lugar de usar por ejemplo “SGC” para “Sistema de Gestión de Calidad”, o “SGSI” para “Sistema de Gestión de Seguridad de la Información”, simplemente usaré la frase “sistema de gestión”.

1.1 Los 5 mitos más comunes relacionados con los estándares ISO / Por qué es necesario la preparación

Hay muchos conceptos erróneos sobre los estándares ISO, que muy a menudo dificultan que conozca y considere esos estándares, y que usted considere una implementación real del estándar. En realidad, podríamos decir que estos mitos son el mayor enemigo de los estándares ISO.

Esto es lo que oigo muy a menudo:

“Bien, dejaremos al administrador manejarlo”

Esta es la favorita de la dirección – “Bien, le daremos este proyecto ISO al administrador; de todos modos, él no nos cuesta mucho”. Bien, el problema de este enfoque es que el proyecto nunca finaliza – debido a que este administrador no tiene los conocimientos necesarios para este tipo de proyecto, probablemente no tenga tiempo suficiente, y ciertamente tampoco tiene suficiente autoridad.

“Bien, lo implementaremos en un par de semanas”

Usted podría implementar su estándar ISO en 2 ó 3 semanas, pero no funcionará - sólo obtendrá un montón de políticas y procedimientos de las que nadie se preocupará. La implementación del sistema de gestión significa que tiene que implementar cambios, y toma tiempo que estos cambios sean aceptados por sus empleados.

Sin dejar de mencionar que debe implementar sólo los controles o procesos que realmente se necesitan, y el análisis de lo que se necesita realmente lleva tiempo.

“Este estándar es todo sobre documentación”

La documentación es una parte importante de la implementación de cualquier estándar ISO, pero la documentación no es un fin en sí mismo. El punto principal de una implementación ISO es que los empleados realicen sus actividades de una manera definida, y la documentación está para ayudarle a hacer esto. Además, los registros que se generen le ayudarán a medir si usted alcanza los objetivos que ha establecido para su sistema de gestión, y permitirá corregir aquellas actividades que no se han realizado.

Así podría considerar la documentación como una herramienta para manejar la calidad para la ISO 9001, el ambiente para la ISO 14001, o la seguridad para la ISO 27001, en lugar de considerar que es una sobre carga de trabajo para sus operaciones.

“El único beneficio del estándar es marketing”

"Estamos haciendo esto sólo para obtener el certificado, ¿no?" Bien, (por desgracia) esta es la manera de pensar del 80 por ciento de las empresas. No estoy tratando de argumentar aquí que un estándar ISO no debe ser utilizado para propósitos promocionales y de ventas, pero también puede obtener otros beneficios muy importantes - los principales beneficios se enumeran en la sección 2.1.

“Necesitamos una herramienta GRC para implementar el estándar ISO”

Las herramientas de gobernanza, riesgo y cumplimiento pueden ser útiles, sin embargo no son requeridas de ninguna manera para la implementación de una ISO. Usted puede albergar toda su documentación en un servidor existente, o en algún servicio en la nube como Dropbox, o en su computadora; deben mantenerse registros automáticos en los sistemas que los creó – encontrará una guía más detallada en la sección 3.9.

El punto aquí es – Lea primero este libro para ver lo que es realmente necesario y lo que no, y por tanto decida dónde invertir la mayor parte de tiempo y dinero para su proyecto ISO.

La principal idea de este libro es ayudar a evitar algunos errores – en otras palabras, prepárese para su proyecto ISO, en lugar de correr de manera precipitada.

1.2 ¿Quién debería leer este libro?

Este libro está escrito principalmente para los principiantes en este campo y para las personas con un conocimiento moderado sobre una implementación ISO – estructuré este libro de tal manera que alguien sin experiencia previa ni conocimientos sobre estándares ISO pueda comprender rápidamente cómo prepararse para un proyecto de implementación. Sin embargo, si tiene experiencia con una implementación ISO, pero siente todavía que tiene lagunas en su conocimiento, también encontrará este libro muy útil.

Por tanto, si usted es un responsable de producción, ingeniero, oficial de cumplimiento, profesional de seguridad de la información, director de departamento de TI, ejecutivo, o un responsable de proyecto con la responsabilidad de implementar un estándar ISO en una empresa pequeña o mediana, este libro es perfecto para usted.

Este libro ofrece ejemplos de preparación para la implementación de un estándar ISO en organizaciones pequeñas y medianas (es decir, empresas con hasta 500 empleados.) Todos los principios aquí descritos también son aplicables a organizaciones más grandes, así que si trabaja para una empresa grande puede encontrar este libro útil; sin embargo, tenga en cuenta que en algunos casos las soluciones tendrán que ser más complejas que las descritas en este libro – por ejemplo, puede utilizar una estructura de gestión de proyectos más compleja que la que se sugiere en el capítulo 3.5 Estableciendo una estructura de gestión de proyecto.

Resumiendo, este libro le da una imagen sistemática de las actividades que necesita hacer y las decisiones que necesita tomar antes de empezar la implementación de su estándar ISO –

usando este libro puede estar seguro de que no cometerá ningún error desde el principio.

1.3 Lo que no es este libro

Este libro se centra en las actividades y decisiones que necesita considerar antes de empezar su proyecto de implementación ISO, pero no explica la implementación efectiva de un estándar ISO en particular. (En la próxima sección podrá encontrar referencias a materiales que le ayudarán con la implementación)

Este libro no le dará las plantillas finales para todas las políticas, procedimientos y planes; sin embargo, en los apéndices de este libro encontrará un par de plantillas, por ejemplo, el Plan de Proyecto.

Este libro no es una copia de un estándar ISO concreto – no puede reemplazar el estándar mediante la lectura de este libro. Por lo tanto, por favor, no caiga en el error de empezar la implementación de un estándar sin antes leerlo – Creo que encontrará este libro y su estándar ISO, como la perfecta combinación para su futuro trabajo. Puede comprar el estándar en [Portal ISO oficial](#).

1.4 Recursos adicionales

Aquí tiene algunos recursos que le ayudarán, junto con este libro, a aprender sobre varios estándares ISO:

- [Cursos en línea ISO](#) – cursos online gratuitos que le enseñarán cómo implementar ISO 9001, ISO 14001 e ISO 27001, incluyendo trucos sobre cómo ir hacia la certificación.

- [Descargas gratuitas ISO 27001](#), [descargas gratuitas ISO 9001](#), [descargas gratuitas ISO 14001](#), [descargas gratuitas OHSAS 18001](#) y [descargas gratuitas ISO 20000](#) – colección de documentos, listas de chequeo, diagramas, plantillas, etc.
- [Conformio](#) – sistema de gestión de documentos basado en la nube (DMS), y herramienta de gestión de proyectos enfocada en estándares ISO.
- [Paquete de Documentación ISO 9001](#) – Conjunto de todas las plantillas de documentos requeridas por ISO 9001, incluyendo soporte de expertos que te guiarán paso a paso en la implementación; existen paquetes de documentos similares para otros estándares ISO.
- [Portal ISO oficial](#) – aquí puede comprar una versión oficial de cualquier estándar ISO.

2

OBTENER LA PARTICIPACIÓN DE LA ALTA DIRECCIÓN Y OTROS EMPLEADOS

La mayoría de profesionales de estándares ISO destacan una razón principal como la responsable del fracaso de sus proyectos: la falta de comprensión de la alta dirección y, en consecuencia, la falta de su apoyo continuo.

Sin embargo, la alta dirección no es el único problema. Muy a menudo, los profesionales de estándares ISO son, si no totalmente incomprendidos, al menos evitados por otros empleados en una empresa. Por “profesional de estándar ISO”, me refiero a alguien que está a cargo de la implementación de un estándar ISO específico.

¿La solución a este problema? A usted probablemente no le va a gustar esto: tiene que ser una combinación de una persona diplomática y un vendedor: va a tener que vender la idea del estándar en el que está trabajando a su dirección, a sus empleados y a sus socios, y usted tendrá que usar todo su poder de persuasión para convencerlos. Y no, su trabajo como profesional de estándares ISO no es sólo sobre políticas y procedimientos – tiene que ver sobre todo sobre psicología y sobre ser convincente con la gente de su alrededor.

Este capítulo le mostrará cómo hacerlo.

2.1 Cómo convencer a la alta dirección para implementar un estándar ISO

Si usted piensa que a su dirección le encanta conocer cuál es su gran idea sobre una nueva política, o una nueva tecnología, está equivocado - simplemente no les importa.

Lo que la dirección quiere escuchar (y entender) son beneficios, cuota de mercado, satisfacción del cliente, disminución de costes, estrategias de negocio, y riesgos empresariales. Y no les puede culpar – después de todo, este es su trabajo.

Por lo tanto, si usted no puede cambiar esto, tendrá que cambiarse a sí mismo. Desde el principio, si quiere que le escuchen, tiene que empezar a hablar un idioma que entiendan - y ellos le entenderán solamente si presentan cuales son los beneficios para el negocio de la implementación de su estándar.

En mi experiencia, hay cuatro beneficios potenciales que usted debe considerar:

1. **Cumplimiento.** Cada vez existen más y más leyes y reglamentos en casi todos los países que pueden ser cumplidas con la implementación de un estándar específico (por ejemplo, la protección de datos personales, y la protección de información clasificada por el gobierno, puede ser resuelta implementando la ISO 27001); pero lo que es aún más interesante, es que hay un creciente número de clientes que requieren a sus proveedores y socios implementar un estándar en particular (por ejemplo, una compañía de construcción puede requerir a sus proveedores estar certificados en ISO 9001). La buena noticia es que los estándares ISO son perfectos marcos de trabajo para cumplir con todos estos requisitos, en parte porque estos estándares

internacionales fueron un modelo en el que se basaron esas leyes y reglamentos cuando se desarrollaron. Esto significa por una parte menos esfuerzo en el proceso de cumplimiento, y por otra parte, menos sanciones a pagar.

2. **Ventaja competitiva.** Si su empresa tiene un certificado ISO y sus competidores no, en realidad podría ganar a nuevos clientes porque usted será capaz de convencer a los potenciales clientes que tiene mayor capacidad que la competencia (por ejemplo, si tiene ISO 9001 puede demostrar que tiene capacidad para el manejo de los requerimientos del cliente, o si tiene ISO 22301 podría demostrar que tiene una alta resiliencia). Esto significa mayor mercado y mayores ganancias.
3. **Reducción de gastos.** Los estándares ISO se consideran generalmente como un coste con ninguna ganancia financiera palpable. Sin embargo, hay beneficios financieros si usted reduce sus gastos ocasionados por, por ejemplo, incidentes, o quejas de cliente. Usted probablemente tenga algún tipo de incidente de seguridad, o de salud, ambiente, u otro tipo de incidente; probablemente también tenga quejas de clientes – todo esto cuesta dinero. Y es cierto, es difícil de calcular cuánto dinero podría ahorrar si usted previene estos incidentes/quejas - pero siempre suena bien si atrae la atención de la dirección exponiendo estos casos. (Más adelante en este capítulo voy a explicar cómo calcular la cantidad de dinero que puede ahorrar por un incidente de seguridad de la información, en la sección 2.3.)
4. **Optimización de procesos de negocio.** Este es probablemente el más subestimado – si usted es una empresa que ha ido creciendo considerablemente en los últimos años, es posible que experimente problemas

como - quién tiene que decidir qué, quién tiene que reportar a quién, quién es responsable de qué. Los estándares ISO son particularmente buenos en arreglar estas cosas - ya que le obligan a definir con mucha precisión los roles y responsabilidades, lo que le puede ayudar a fortalecer su organización interna.

No estoy diciendo que estos cuatro beneficios puedan ser aplicables a su organización, pero lo más probable es que encuentre al menos dos que sean realmente relevantes para su organización. Y tiene que consultar a sus colegas de empresa, porque en definitiva tiene que averiguar cuál de estos beneficios son los más interesantes para la alta dirección de su empresa, y para aquellos que apoyan su estrategia. La mejor manera de hacer esto podría ser realizar una lluvia de ideas de estos beneficios con sus colegas desde el lado del negocio de la organización, y con aquellas funciones corporativas.

Por supuesto, también tendrá que encontrar los caminos de cómo usted puede relacionar su proyecto ISO con la estrategia de negocio de la empresa. Aquí tiene un ejemplo: digamos que su empresa quiere comenzar a ofrecer servicios en la nube, lo que significa que la información sensible del cliente necesita ser protegida; Si comienza a implementar ISO 27001, no sólo disminuirá la probabilidad de que algunos datos se puedan revelar, también disminuirá la indisponibilidad del servicio - por lo tanto, este proyecto apoyará el paso estratégico que su empresa decidió tomar.

Vea también este mini caso de estudio en el capítulo 4: Mini caso de estudio: Obtener el apoyo de la alta dirección en una compañía de propiedad estatal.

El siguiente paso es averiguar cómo llegar a la mente de su dirección.

2.2 Cómo presentar los beneficios a la alta dirección

No espere que su dirección pueda captar todos los beneficios después de una reunión de 20 minutos, no importa lo bonito que se vea su presentación de PowerPoint. Por desgracia, a su dirección le tomará tiempo entenderlo.

Aquí tiene algunas técnicas que puede utilizar para presentar su caso de forma más efectiva:

Discurso motivador. Es probable que usted logre mucho más en ocasiones informales que en reuniones formales - por ejemplo, cuando accidentalmente tropieza con su CEO en una cafetería, un ascensor, o similar. Si no están preparados para esta ocasión, probablemente conseguirá confundir - por lo tanto, tiene que preparar un supuesto discurso de ascensor, un discurso de 30 a 60 segundos donde presente intensamente su caso. Si usted ensaya bien, sonará seguro y convincente. Por ejemplo, mi discurso de ascensor (como consultor tratando de vender mis servicios): *la inversión en ISO 27001 será rentable si usted evita solamente un incidente mediano, sin mencionar los grandes incidentes.*

Encontrar un aliado. Usted necesita encontrar personas que estén cerca de su CEO y que naturalmente estén interesadas en lo que está haciendo - por ejemplo, su director financiero podría ver la implementación del estándar ISO como una forma de disminuir el riesgo financiero de la compañía, así que esta persona puede decidir apoyar su esfuerzo; el director de cumplimiento podría ver su proyecto como una forma de aliviar una parte de su carga de trabajo, mientras que los chicos de marketing podrían ver esto como un punto de venta clave adicional. En cualquier caso, haga su tarea e investigue quién estaría interesado en las ventajas mencionadas en la sección previa.

Estas personas no sólo darán una percepción adicional sobre cómo un estándar ISO específico ayudará a la empresa, también hará más fácil llegar a la agenda de la alta dirección más rápidamente.

Regla 30-20-10. Cuando hagas tu presentación en PowerPoint, olvídate de todas esas estadísticas de lujo que has encontrado, y las cientos de diapositivas que usted preparó. En su lugar, use la regla 30-20-10: use fuentes tamaño 30, máximo 20 minutos, y hasta 10 diapositivas. Y céntrese en los beneficios – este es el mensaje principal que usted necesita dar. (Vea también el Apéndice G para una plantilla de propuesta de proyecto.)

Cuidado con las palabras. Recuerde, su grupo objetivo son directivos que no entienden o no les gusta sus expresiones friki. Por ejemplo, a la hora de presentar la seguridad de la información / ISO 27001:

En lugar de:	Use esto:
Backup, sistema de extinción de incendios (y otras salvaguardas)	Prevención (<i>Nos evitará...</i>)
Coste	Inversión (Invirtiendo en ..., ahorraremos xyz dólares...)
Probabilidad	Riesgo (Reduciremos el riesgo de...)
Incidente	Daño (Reduciremos el daño implementando...)
Desastre	Pérdida/tiempo de inactividad (Perderemos xyz dólares; nuestro tiempo previsto de inactividad durará...)

Figura 1: Palabras a evitar y palabras a usar cuando se presenta un proyecto ISO

Y, sobre todo, sea paciente y persistente - compórtese como un vendedor real. Después de un tiempo, usted seguramente empiece a notar algunos progresos – quizás no en el primer par de días o incluso en los primeros meses, pero no deje que esto le desaliente.

2.3 Ejemplo de Retorno de la Inversión (ROI) para seguridad de la información

El siguiente ejemplo es sobre seguridad de la información; sin embargo, puede ser aplicado de forma similar a incidentes ambientales, y quizás incluso también a incidentes de salud y seguridad.

Muy a menudo le preguntarán, "Si invertimos xyz dólares en la seguridad de la información, ¿cuánto ganaremos? ¿Cuál es el RIS?"

En lugar de mostrar una teoría profunda sobre cómo calcular el ROI, déjeme darle un ejemplo sencillo.

Digamos que usted tiene un servidor que, si es destruido, el daño (tanto en hardware, datos y tiempo de inactividad) sería de \$100.000 – esto también se denomina como Expectativa de Pérdida Simple, o en inglés Single Lost Expectancy (SLE). Digamos que tienes una amenaza de incendio, y que tal incidente puede suceder una vez en 20 años - esto significa que la tasa anualizada de ocurrencia (ARO) sería 5%. Por lo tanto, ahora tiene que calcular el valor del riesgo (o, utilizando esta terminología complicada – Expectativa de Pérdida Anual, o en inglés Annualized Lost Expectancy ALE) que se calcula multiplicando el SLE por el ARO.

Esto significa que el riesgo tiene un valor de \$5.000 anualmente.

¿Qué significa esto? Esto significa que mientras usted invierta menos de \$5.000 en los sistemas de prevención de incendios y extinción de incendios, hará que esto sea un beneficio. Por lo tanto, digamos que invierte \$4.000 en esos sistemas al año, lo cual significa que obtendrá un beneficio de \$1,000 cada año. Esta es la cantidad de dinero que ha ahorrado su empresa en promedio, por año, porque con esos sistemas nunca debe producirse un fuego (es decir, ha eliminado el riesgo).

Si obtuvo un beneficio de \$1,000 en una inversión de \$4.000, esto significa que su RIS es 25% – bastante bueno, ¿no?

Sin embargo, es cierto: sí, es difícil calcular el daño que ocurriría; sí, no hay estadísticas fiables sobre la frecuencia de estos incidentes. Pero, con esfuerzo, se puede calcular el daño con una relativa exactitud y puede hacer una suposición inteligente con la frecuencia – y sí, podría perder 50 ó 70 por ciento, que es todavía mucho mejor que una pura conjetura, por lo que puede perder 50 ó 70 veces.

Por lo tanto, el punto principal aquí es – a no ser que como mínimo de alguna estimación a su dirección, no tendrán la menor idea acerca de los beneficios de su estándar ISO en términos económicos. Y si usted habla con dólares y porcentajes, este es el lenguaje que entiende la dirección, y eso hará que comiencen a escuchar.

Sin embargo, la inexactitud en estos cálculos no es el único problema - otro problema es que toma tiempo y mucho esfuerzo. Por esta razón le recomiendo usar este cálculo de retorno de la inversión sólo si están proponiendo inversiones grandes (por ejemplo, la compra de algunos equipos caros) – en

este caso, tiene sentido, para demostrar a su dirección la lógica de los números.



Herramienta libre: Este [Calculador del Retorno sobre la Inversión en Seguridad](#) le da la fórmula par calcular el daño de un incidente, y le ayuda a calcular el RIS total.

2.4 Tratar con la línea de responsables y otros empleados

La mayoría de los empleados de su empresa serán bastante escépticos acerca de lo que hace, así que tiene que vender mucho la idea sobre la implementación ISO. Y la buena noticia es – conseguirlo no es muy diferente de obtener el compromiso de alta dirección. Otra vez, tiene que encontrar beneficios que sean relevantes a los departamentos, o a las personas de manera independiente, y presentar los beneficios de una manera convincente.

Por ejemplo, si el jefe del Departamento de ventas considera que la seguridad de la información es absolutamente innecesaria, pregúntele lo siguiente: "¿Qué habría sucedido durante el proceso de licitación si filtra los datos de su propuesta a sus competidores"? Probablemente le contestarían: "esto nunca ha sucedido hasta ahora, confío en mi gente". Pero luego puede proporcionarle ejemplos de cómo esto ha sucedido por ejemplo a otras empresas de su industria, o tal vez como datos de su empresa se han filtrado a algún otro departamento.

Usted puede seguir la conversación con un dato más. Digamos que su Departamento de ventas desea enviar una propuesta a un concurso a través del cual adquiriría el cliente más grande de los últimos 3 años. ¿Qué pasa si la revelación de datos ocurre en medio de este proceso?

Una vez que pueda abrir una ventana de oportunidad, tiene que explicar qué es lo que puede hacer para él y para su Departamento: se puede definir exactamente quién puede acceder a los datos, dónde se almacenan los datos, y cómo se transmiten - el punto es, con relativamente poco esfuerzo se puede prevenir un gran incidente.

Y así es como esto funciona con cualquier otro estándar, con cualquier departamento, con cualquier persona individual - desde mi experiencia, hasta el momento, no he encontrado ningún departamento de cualquier empresa que no se beneficie de los estándares ISO.

Así que, ¿qué significa esto para usted? Haga su tarea primero. Estudie sus procesos de negocio, sus productos principales, lo que es crítico en todos los departamentos, las fechas importantes, etc. Una vez esté armado con este conocimiento, usted será capaz de conseguir convencer a casi cualquier persona.

Por supuesto, tiene que seguir repitiendo estas actividades de convencimiento de una manera sistemática - esto normalmente se hace a través de un programa de desarrollo de concienciación, pero esto es algo que hará durante la implementación inicial del estándar (y también luego).

2.5 Factores de éxito

En Resumen, para obtener el compromiso de sus directivos y sus colegas, usted debe hacer lo siguiente:

- Empiece a pensar desde la perspectiva de beneficios, no desde la perspectiva técnica

(Esta parte del libro no se muestra en la vista previa gratuita)

BIBLIOGRAFÍA

ISO 9001:2015, Quality management systems – Requirements, International Organization for Standardization, 2015

ISO 14001:2015, Environmental management systems – Requirements with guidance for use, International Organization for Standardization, 2015

ISO/IEC 20000-1:2011, Information technology – Service management – Part 1: Service management system requirements, International Organization for Standardization, 2011

ISO 22301: 2012, Societal security – Business continuity management systems – Requirements, International Organization for Standardization, 2012

ISO/IEC 27001:2013, Information technology – Security techniques – Information security management systems – Requirements, International Organization for Standardization, 2013

ISO/DIS 45001, Occupational health and safety management systems – Requirements with guidance for use, International Organization for Standardization, 2015

ITIL 2011, Axelos, 2011

Kosutic, Dejan, *9 Steps to Cybersecurity*, Zagreb: EPPS Services Ltd, 2012

Kosutic, Dejan, *Becoming Resilient*, Zagreb: EPPS Services Ltd, 2013

OHSAS 18001:2007, Occupational health and safety management systems – Requirements, BSI, 2007

<http://advisera.com/27001academy/blog/> *ISO 27001 & ISO 22301 Blog*, Advisera.com

<http://training.advisera.com/course/iso-27001-foundations-course/> *ISO 27001 Foundations Course*, Advisera.com

ÍNDICE

- administrador, 27
- alta dirección, 16, 21, 24, 35
- anualizada de ocurrencia, 22
- Auditor Jefe, 30, 78
- beneficio, 23
- beneficios, 19, 21, 24, 26
- Business continuity, 81
- CEO, 20
- certificado ISO, 18
- certificados, 30
- clientes, 17, 30
- compromiso, 24
- concienciación, 25, 43
- consecuencia, 33
- consultor, 31
- consultores, 29
- consultoría, 30
- Coste, 21
- costes, 41
- cumplimiento, 12, 66
- Cumplimiento, 17
- cuota de mercado, 17
- cursos, 30, 42
- Declaración de Aplicabilidad, 32
- Departamento de TI, 35
- Departamento de ventas, 24
- diagrama de Gantt, 36
- director de cumplimiento, 20
- director de departamento de TI, 13
- director general, 50
- Discurso motivador, 20
- disminución de costes, 17
- ejecutivos, 43
- empresa de TI, 30
- equipo de proyecto, 35
- estrategia, 19, 51
- Estrategia, 27
- evaluación del riesgo, 48
- Expectativa de Pérdida Anual, 22
- herramientas de software, 31
- herramientas online, 43
- Information security, 81
- Invirtiendo, 21
- ISO, 81, 82
- ISO 13485, 33
- ISO 14001, 33, 37
- ISO 20000, 37
- ISO 22301, 33, 81, 82
- ISO 27001, 33, 37
- ISO 9001, 5, 33, 37, 81
- ITIL, 81
- jefe de departamento, 41
- leyes y reglamentos, 17
- línea de responsables, 26
- los beneficios, 17
- medición, 45
- nube, 12, 19
- objetivos, 34
- Oficial de Seguridad de la Información, 35
- organizaciones más grandes, 13
- Patrocinador, 35
- PDCA, 33, 34, 39

Pérdida/tiempo de inactividad, 21	riesgo financiero, 20
Plan de Proyecto, 35	riesgos empresariales, 17
Presupuestar, 42	ROI, 26
Prevención, 21	roles y responsabilidades, 19, 72
profesional de seguridad de la información, 13	satisfacción del cliente, 17
protección de datos	SGSI, 10
personales, 17	sistema de extinción de incendios, 21
proveedores, 17	sistema de gestión de documentos, 15
recursos, 27	tratamiento de riesgos, 67
responsable de proyecto, 13, 30, 35	tratamiento del riesgo, 33
Retorno de la Inversión, 22	Visitas de seguimiento, 43

Preparación para el proyecto de implementación ISO: una guía en un lenguaje sencillo

Una guía paso a paso para principiantes en estándares ISO de pequeñas empresas.

Piense y actúe como un implementador experimentado con esta guía comprensiva y práctica que le enseñará qué preparación necesita antes de empezar su proyecto de implementación de la ISO 9001, ISO 14001, ISO 27001 o cualquier otro estándar de gestión ISO.

El autor y consultor experimentado Dejan Kosutic comparte su conocimiento y sabiduría práctica con usted en este libro de valor incalculable. Usted aprenderá:

- ✓ Cómo convencer a su alta dirección para implementar el estándar
- ✓ Cómo presentar los beneficios del negocio para la implementación ISO
- ✓ Cómo obtener el compromiso de otros empleados en su compañía
- ✓ Cómo desarrollar su estrategia para la implementación ISO – aprenda las 3 opciones que tiene
- ✓ Cómo seleccionar un consultor
- ✓ Cómo configurar una estructura de gestión del proyecto
- ✓ Cuánto ocupará el proyecto, y cuánto costará
- ✓ Decidir si debe utilizar herramientas y plantillas
- ✓ Todo esto, y mucho más...

Escrito en un lenguaje sencillo de entender, *Preparación para el proyecto de implementación ISO: una guía en un lenguaje sencillo* está escrito para personas que van hacia una implementación ISO por primera vez, y necesitan una guía clara sobre qué tienen que hacer antes de que comience el proyecto. Si usted es un principiante con algo de experiencia, o es nuevo en este campo, este es el único libro que necesitará sobre este tema.