SEGURO & SIMPLE

Una Guía Para La Pequeña Empresa Para La Implementación De La ISO 27001 Con Medios Propios

EL MANUAL, CON UN IDIOMA PLANO, PASO A PASO, PARA LOS PROFESIONALES DE SEGURIDAD DE LA INFORMACIÓN

DEJAN KOSUTIC

Dejan Kosutic

Seguro & Simple:

Una guía para la pequeña empresa para la implementación de la ISO 27001 con medios propios

El manual, con un idioma plano, paso a paso, para los profesionales de seguridad de la información

Advisera Expert Solutions Ltd
Zagreb, Croatia

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

ISBN: 978-953-57452-7-3

Primera edición, 2016

Título original: "Secure & Simple: A Small-Business Guide to Implementing ISO 27001 On Your Own"

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 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.

Click aquí para ver su perfil de LinkedIn profile.

TABLA DE CONTENIDOS

LISTADO DE FIGURAS

PREFACIO

Veo miles de visitantes leyendo diariamente mis artículos en el blog ISO 27001 Blog, y aunque muchos de ellos están agradecidos, algunos se quejan un poco – dicen "Sí, sus artículos son útiles, pero hay muchos, y simplemente no se por donde empezar y donde terminar." Y en efecto – en el momento de escribir este libro, había casi 200 artículos publicados en 27001Academy; por tanto, tienen razón, es difícil usar todo este conocimiento de una manera sistemática.

Por esta razón me decidí a escribir este libro – quería proporcionar a guía completa, paso a paso, para la ISO 27001, escrita en un lenguaje sencillo, que pueda ser entendido por principiantes sin conocimientos previos de este estándar, escrito de una forma estructurada para que sepa dónde comenzar y cómo terminar la implementación de la ISO 27001 de una manera exitosa.

Y sí, lo admito – muchos de los contenidos de este libro están tomados de los artículos más populares del blog, de mi libro Becoming Resilient, de nuestros cursos online, y de otros materiales, porque pensé que un libro que presente estos materiales de una manera estructurada, proporcionaría un buen valor.

Pero lo que creo que más le gustará de este libro es que le doy respuestas prácticas a situaciones de la vida real, a la hora de implementar la ISO 27001. Estos consejos vienen principalmente de mi interacción con muchas personas que están haciéndome preguntas diariamente – Fui lo suficientemente afortunado para impartir muchos cursos presenciales, y webinars online, y contestar miles de preguntas a través de foros, llevar a cabo muchos trabajos de consultoría, y hablar en una serie de conferencias. En todas estas ocasiones me vi obligado a pensar en muchas cuestiones relacionadas con la ISO 27001, y a proporcionar las mejores prácticas sobre cómo manejarlas.

Por lo tanto, después de leer este libro, usted será capaz de implementar el estándar, ya que le proporcionará suficientes conocimientos y consejos para implementar el estándar en una pequeña o mediana empresa.

Espero haber tenido éxito en esto. ¡Disfrute su libro!

1
INTRODUCCIÓN

¿Por qué su organización necesitaría tener su información a salvo? ¿Cómo puede la ISO 27001 ayudarle a conseguir la seguridad de la información? ¿Este libro es la mejor opción para ti?

1.1 ¿Por qué la seguridad de la información? ¿Por qué ISO 27001?

La seguridad de la información, la cyberseguridad, o la protección de datos no son cosas que estén reservadas sólo para expertos de TI, esto es algo que concierne a prácticamente cualquier persona en este planeta, así como a cualquier empresa.

Si usted fuera un ejecutivo de una organización de hace diez años, probablemente no estaría tan preocupado con cualquiera de estas cosas. Hoy en día, está en la segunda década del tercer milenio y no puede ignorar las amenazas a sus datos. Además, en el futuro tendrá más protección. ¿Por qué? Porque la mayoría de organizaciones está ahora en el negocio de procesamiento de información.

La mayoría de nosotros imagina que un banco maneja grandes cantidades de dinero en efectivo todos los días. Y aunque los bancos todavía manejan muchas transacciones de dinero en efectivo, la realidad actual es que las transacciones de dinero electrónicas superan las transacciones de efectivo – en algunos casos por más de 1 millón a uno. Por lo tanto, esto significa que un banco típico está en el negocio de procesamiento de la información – es una gran fábrica de información. Y adivinen qué; desde hace algún tiempo hasta la fecha robar un banco hackeando los sistemas informáticos es mucho más rentable que caminar con una máscara sobre el rostro y robar físicamente los cajeros. El hacking es mucho menos arriesgado, demasiado.

Piense en su negocio; ¿es una fábrica de información, también? Es probable que su negocio, si no totalmente, entonces parcialmente esté basado en el procesamiento de información. Esto significa que su negocio es más vulnerable. Su información, su conocimiento, su know-how y la propiedad intelectual están en riesgo. Y ahora la pregunta del millón de dólares, o si estás en un negocio más grande esta podría ser una pregunta de mil millones de dólares: ¿Qué necesita hacer para proteger la información de su empresa?, y ¿por dónde comenzar?

El problema es que en la actualidad hay una abundante información sobre seguridad de la información; probablemente sea bombardeado con información sobre nuevo cortafuegos, software antivirus, frameworks, metodologías, legislación y así sucesivamente. Muchas empresas ofrecen servicios que pretenden ser la solución a todos sus problemas de seguridad. Sin embargo, estas soluciones individuales no van a protegerle completamente. Por ejemplo, no puede resolver el problema de un empleado disgustado con un firewall, de la misma manera que no puede resolver el problema de un hacker solo por cumplir con una ley.

Por lo tanto, es obvio que necesita algo más, algo integral. Pero el desafío es cómo comenzar, qué pasos tiene que seguir para proteger de la mejor manera su negocio.

Aquí es donde ISO 27001 entra – como se explica a lo largo de este libro, ofrece un marco integral que le ayudará con este proceso crucial. Le da la orientación necesaria y los cimientos para proteger su empresa. ISO 27001 le indica por dónde empezar, cómo ejecutar su proyecto, cómo adaptar la seguridad a las cuestiones específicas de su empresa, cómo controlar lo que hacen los expertos de seguridad y de TI, y mucho más.

Por lo tanto, lo principal es – ISO 27001 no tiene que ser un trabajo de cumplimiento burocrático – si se aplica correctamente, puede ser una herramienta muy eficiente no sólo para proteger su empresa, sino también para obtener algunos beneficios.

1.2 Principios básicos de seguridad de la información

Primero definamos qué es información. La información es un activo de la organización, que tiene valor para la organización y debe ser protegido adecuadamente. La información puede tener diversas formas y se puede almacenar en diferentes medios.

Por otra parte, la seguridad de la información se puede definir como la protección de la confidencialidad, la integridad y la disponibilidad de la información en diversas formas, tales como escrita, hablada, impresa, electrónica y así sucesivamente.

Veamos las definiciones oficiales de estos términos en ISO 27000: confidencialidad es "propiedad que hace que la información no esté disponible o sea revelada a individuos no autorizados, entidades o procesos", integridad es "propiedad de exactitud e integridad", y la disponibilidad es "propiedad de ser accesible y usable bajo demanda por una entidad autorizada".

Sí, a veces es difícil entender esta terminología de la ISO, así que aquí está una explicación fácil de estos conceptos básicos: si llego a un banco y hago un depósito de $10.000, en primer lugar no quiero que nadie sepa nada sobre este dinero excepto el Banco y yo. (Esto es confidencialidad).

Dentro de unos meses cuando vuelva a retirar mi depósito, quiero la cantidad de $10.000 más los intereses; No quiero que la cantidad sea $1000 porque alguien ha jugado con mi cuenta. (Esto es integridad).

Por último, si quiero retirar mi dinero no quiero que el empleado del banco me diga que los sistemas del Banco están sin funcionar y que tengo que volver mañana. (Esto es la disponibilidad.)

ISO 27001 tiene exactamente el mismo enfoque – la protección de la confidencialidad, integridad y disponibilidad (también conocido como las 3 dimensiones CID); pero además va un paso más allá, explica cómo hacerlo sistemáticamente en una empresa de cualquier tipo.

1.3 ISO 27001 lo une todo

Lo que me gusta de ISO 27001 es que lo que tiene es comprensible, y al mismo tiempo, tiene un enfoque equilibrado para construir un sistema de gestión de seguridad de información (SGSI) – no sólo proporciona un perfecto equilibrio entre la parte de TI y el negocio de la organización, también requiere la participación directa de la alta dirección en la implementación de la seguridad de información, asegurando que dicho proyecto no sólo tiene todos los recursos necesarios, sino que además es compatible con los objetivos estratégicos de la empresa.

ISO 27001 explica cómo estructurar la documentación de la seguridad de la información, y también cómo aplicar solamente aquellos controles de seguridad (salvaguardas) que son realmente necesarios para la empresa. Te da las herramientas para revisar permanentemente todo el sistema y mejorarlo siempre que sea posible; le proporciona un sistema que capacita a sus empleados para que sean conscientes de la importancia de la seguridad de la información; esto incluye los requisitos sobre cómo planificar los recursos, incluyendo los recursos financieros.

Como explicaré más adelante en mayor detalle, ofrece un camino de implementación perfecta – está escrito de manera secuencial, de manera que sólo tiene que seguir la estructura de la norma para implementar su SGSI de la manera más lógica.

Finalmente, ofrece un marco de gestión sobre cómo evaluar si la seguridad de la información ha logrado algún valor para el negocio – estableciendo objetivos y midiendo si se cumplen estos objetivos. Se puede sorprender, pero me gusta mucho esta parte, porque si la dirección ve beneficios concretos de la inversión en seguridad de información, puede ser la mejor manera para asegurar una larga y exitosa vida del SGSI en su empresa.

1.4 ¿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 ISO 27001 – estructuré este libro de tal manera que alguien sin experiencia previa ni conocimientos sobre seguridad de la información pueda comprender rápidamente de lo que trata y cómo implementar todo el proyecto; sin embargo, si tiene experiencia con el estándar, y siente todavía que tiene lagunas en su conocimiento, también encontrará este libro muy útil.

Este libro ofrece ejemplos de la implementación de la norma 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 metodología de análisis de riesgo más compleja que la que se sugiere en el capítulo 7 Gestión del riesgo.

Así que si usted es un administrador de TI, un profesional de seguridad de la información, un jefe de departamento o jefe de proyecto con la tarea de implementar ISO 27001 en una empresa pequeña o mediana, este libro es perfecto para usted.

Creo que este libro también será muy útil para consultores – siendo también consultor hice un esfuerzo para presentar en este libro el camino más lógico para implementar un sistema de gestión de seguridad de información (SGSI), así que leyendo con cuidado este libro obtendrá los conocimientos para sus futuros contratos de consultoría.

Este libro no está escrito como una guía para la realización de auditorías, pero podría ser útil para los auditores internos o incluso auditores de certificación, porque les ayudará a comprender todos los requisitos de la norma y también presentará la mejor práctica para la implementación, esto será útil cuando el auditor deba proporcionar algunas recomendaciones en su informe de auditoría.

Por último, creo que este libro puede ser una especie de lista de verificación para los profesionales de seguridad de la información experimentados – lo digo porque he tenido muchos de esos profesionales en mis cursos de ISO 27001, y aunque no aprenden nada especialmente nuevo, agradecen el obtener una visión completa y estructurada de cómo debería implementarse la seguridad de la información.

Y así es exactamente cómo está escrito este libro - da una imagen sistemática sobre todo lo que es la ISO 27001, y le ayuda a asegurarse de que no se olvida nada. Realmente no importa si su empresa va a por la certificación o no - este libro le explicará cómo utilizar ISO 27001 como marco de trabajo, y cómo llegar a cumplir totalmente con este estándar.

1.5 Cómo leer este libro

Este libro está escrito como una guía de implementación paso a paso, y la forma es leer los capítulos 3 al 11 en el orden en el que están escritos, porque esta secuencia representa la forma más óptima de implementación de la norma.

Aquí también tiene algunas otras características de este libro que le harán más fácil leerlo y utilizarlo en la práctica:

- Cuando ciertas secciones de este libro estén relacionadas con una cláusula específica del estándar, entonces la cláusula del estándar estará escrita en el título de la sección.
- Dado que los capítulos del 5 al 8 y 10 describen la implementación de cláusulas particulares del estándar, cada sección tiene estos elementos:
    - **Propósito** – describe brevemente por qué existe la cláusula y cómo puede utilizarse para su SGSI
    - **Entradas** – qué insumos necesita tener para poder implementar el requisito

- **Opciones** – qué opciones debe de considerar a la hora de implementar el requisito
- **Decisiones** – qué decisiones necesita tomar para avanzar
- **Documentación** – describe cómo documentar los requisitos de la ISO 27001
- **Truco de documentación** – resume brevemente los documentos que necesita para cada requisito

- Algunas secciones contienen consejos de herramientas libres, que le permitirán implementar la norma de una manera más fácil – por ejemplo, en el apartado 3.3, se habla de convencer a la alta dirección, y encontrará un enlace a una herramienta gratuita de cálculo del retorno de la inversión en seguridad.
- Al final de los capítulos más importantes verá una sección llamada Factores de éxito, que hará hincapié en lo que necesita centrarse.
- Al final del libro, en el capítulo 14 verá un par de pequeños casos de estudio que explican cómo determinados elementos del estándar ISO 27001 se implementan en situaciones reales.
- Encontrará mucha información útil en los apéndices - glosario, diagrama de implementación, lista de verificación de la documentación obligatoria, matrices de comparación, plantillas para planificación de proyectos, etc.

1.6 Lo que no es este libro

Este libro se centra en la gestión de la seguridad, en la gestión de proyectos, la documentación, cómo conseguir el apoyo para su proyecto, etc., pero no se centra en la tecnología. Este libro no explica qué tipo de sistemas de backup necesita comprar, qué tecnologías de comunicación se deben utilizar, o qué tipo de firewall debe instalar. Sin embargo, este libro le dará una metodología sobre cómo conseguir las entradas para

que puedan tomar decisiones relevantes sobre la tecnología, cómo determinar qué datos sensibles tiene compartiendo con sus colegas desde el lado del negocio, y cómo asegurarse de que está respaldada regularmente, qué información necesita comunicar y a quién, cuáles son las amenazas a los sistemas que su firewall debe proteger, etc.

Este libro no le dará las plantillas finales para todas las políticas, procedimientos y planes; sin embargo, este libro le explicará cómo estructurar todos los documentos requeridos por el estándar ISO 27001, qué opciones tiene para escribir dichos documentos, quienes deberían participar en la elaboración y toma de decisiones relacionados con cada documento, dónde se encuentra los insumos, etc.

Este libro no es una copia del estándar ISO 27001 – no puede reemplazar el estándar mediante la lectura de este libro. Este libro pretende explicar cómo interpretar el estándar (ya que el estándar está escrito de una manera bastante antipática) y cómo implementar cada elemento del estándar utilizando mejores prácticas basadas en la experiencia; sin embargo, este libro no es un reemplazo de la ISO 27001 en sí mismo.

Por lo tanto, por favor, no caiga en el error de empezar la implementación del estándar sin antes leerlo – Creo que encontrará el estándar ISO 27001 y este libro, como la perfecta combinación para su futuro trabajo. Puede comprar el estándar en el sitio oficial de ISO, existe también una alternativa económica en website de ANSI.

1.7 Recursos adicionales

Aquí tiene algunos recursos que le ayudarán, junto con este libro, a aprender todo sobre cómo implementar ISO 27001:

1) ISO 27001 online courses – cursos online gratuitos que le enseñarán las bases de ISO 27001, cómo implementar el estándar, cómo realizar una auditoría, etc.

2) ISO 27001 Descargas gratuitas – colección de documentos, listas de chequeo, diagramas, plantillas, etc.

3) Herramientas ISO 27001 – par de herramientas gratuitas como la Calculadora de Inversión en Seguridad, la Calculadora de la Duración de la implementación y la herramienta de Análisis de brecha.

4) Conformio – sistema de gestión de documentos basado en la nube (DMS), y herramienta de gestión de proyectos enfocada en estándares ISO.

5) ISO 27001 Paquete de documentos – Conjunto de todas las plantillas de documentos requeridas por ISO 27001, incluyendo soporte de expertos para la implementación.

6) El sitio oficial de ISO sobre ISO 27001 – aquí puede comprar una versión oficial del estándar ISO 27001.

¿Le interesó? Bien, vamos a ver más de cerca todo lo que es la ISO 27001.

7
GESTIÓN DE RIESGOS

La evaluación y el tratamiento son, sin duda, la parte más compleja de la implementación del estándar ISO 27001, pero no puede dejar de realizarlos – sin estos pasos (evaluación y tratamiento) no sabrá dónde enfocar sus esfuerzos con respecto a la seguridad de la información, lo que significa que perderá algo importante.

Por suerte, este proceso puede agilizarse bastante – si no se complica con elementos innecesarios, se puede acabar en un tiempo bastante aceptable y con un esfuerzo razonable. Además, usted se sorprenderá con lo que aprenderá acerca de su empresa con este proceso.

7.1 Abordar riesgos y oportunidades (cláusula 6.1.1)

Además del mencionado análisis del contexto de la organización y las partes interesadas, en el proceso de planificación del SGSI, las empresas deben identificar los riesgos y oportunidades que se deben abordar. Se trata de la única manera de impedir que sucedan incidentes, al mismo tiempo que se consiguen los objetivos del SGSI. Por cierto, el abordar los riesgos y oportunidades, tiene un papel similar al de las acciones preventivas que existían en la antigua revisión 2005 de la ISO 27001.

Los riesgos se refieren a eventos no deseados que pueden tener impacto negativo en la seguridad de la información, y por lo tanto en la empresa, tales como una inundación que podría destruir información en papel. Las oportunidades se refieren a las acciones que podría emprender la empresa con el fin de mejorar la seguridad de la información, como la contratación de un experto en seguridad de la información como CISO.

Voy a explicar cómo hacer frente a los riesgos en las siguientes secciones; por otro lado el abordar oportunidades puede integrarse en

el proceso de mejora continua, que significa que son oportunidades que pueden ser documentadas y evaluadas como las iniciativas para la mejora continua del SGSI, como voy a describir en la sección 10.6; abordar oportunidades también puede ser parte de la configuración de los objetivos de seguridad y la medición de su cumplimiento.

Por ejemplo, si la empresa decide elegir a uno de sus empleados para que sea el CISO, podría ser una oportunidad para esta persona mejorar su conocimiento de seguridad de la información. Para ello la empresa puede iniciar la acción de la mejora de este conocimiento de la persona y puede establecer un objetivo para el CISO, que puede ser obtener certificados de seguridad.

7.2 Cinco pasos en el proceso de gestión de riesgos (cláusula 6.1)

La evaluación y el tratamiento (juntos se llaman gestión del riesgo) son los pasos más importantes al principio de su proyecto de seguridad de la información – establecen las bases de la seguridad de la información en su empresa.

La pregunta es – ¿por qué son tan importantes? La respuesta es muy sencilla aunque no es entendida por muchas personas: la filosofía principal del estándar ISO 27001 es averiguar qué incidentes pueden ocurrir (es decir, evaluar los riesgos) y luego encontrar la manera más adecuada para evitar estos incidentes (es decir, tratar los riesgos). No sólo esto, también tiene que valorar la importancia de cada riesgo para que usted pueda centrarse en los más importantes.

Aunque la gestión del riesgo es un trabajo complejo, muy a menudo innecesariamente se transfigura. Estos 5 pasos básicos arrojará luz sobre lo que tiene que hacer:

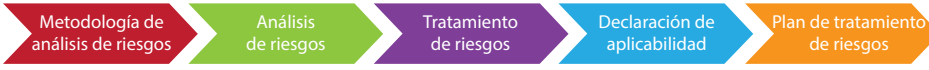

Figura 5: Cinco pasos en el proceso de gestión del riesgo

1) Metodología de análisis de riesgos. Este es el primer paso en su viaje a través de la gestión del riesgo. Es necesario definir las reglas sobre cómo va a realizar la gestión del riesgo, dado que desea que su organización lo haga siempre del mismo modo, ya que el mayor problema con la evaluación del riesgo ocurre si diferentes partes de la organización lo realizan de una manera diferente. Por lo tanto, es necesario definir qué escala usas para la evaluación cualitativa, cuál será el nivel aceptable de riesgo, etc.

2) Implementación del análisis de riesgos. Una vez que conoce las reglas, puede empezar a averiguar qué problemas podrían sucederle – generalmente mostrará una lista de todos sus activos, y las amenazas y vulnerabilidades relacionadas con estos activos, la evaluación del impacto y la probabilidad para cada combinación de activos/amenazas/vulnerabilidades, y finalmente el cálculo del nivel de riesgo.

3) Implementación del tratamiento de riesgos. Por supuesto, no todos los riesgos son iguales – usted tiene que centrarse en los más importantes, llamados "riesgos inaceptables". Hay cuatro opciones que usted puede elegir para mitigar cada riesgo inaceptable: aplicar controles de seguridad, transferir el riesgo, evitar el riesgo y aceptar el riesgo.

4) Declaración de aplicabilidad. Este documento realmente muestra el perfil de seguridad de su empresa - basándose en los resultados del tratamiento de riesgo, necesitará una lista de todos los controles que ha implementado, por qué se han aplicado y cómo. Este documento también es muy importante porque el auditor de certificación lo usará como guía principal para la auditoría.

5) Plan de tratamiento de riesgos. El propósito de este documento es definir exactamente quién va a implementar cada control, en qué tiempo, con qué presupuesto, etc. Yo prefiero llamar a este documento "Plan de implementación" o "Plan de acción", pero vamos a usar la terminología de ISO 27001.

Como verá en otras secciones, este proceso es bastante sencillo y realmente no es tan difícil como podría parecer al principio. Lo bueno es – ISO 27001 le obliga a realizar esta gestión de riesgos de forma sistemática.

Es muy importante entender que estos cinco pasos deben realizarse secuencialmente - no puede implementar los controles de seguridad a menos que sepa que estos son los más adecuados; no puede saber qué salvaguardias son apropiadas, antes de encontrar dónde están los potenciales problemas; Si primero no define las reglas para todo el proceso, simplemente fallará.

En las secciones siguientes voy a explicar cada uno de estos pasos, utilizando también las directrices de ISO 27005.

7.3 Escribir la metodología de análisis de riesgos (cláusula 6.1.2)

Propósito. Como dice el viejo refrán, si no sabe dónde va, probablemente acabará en algún lugar a donde no esperaba llegar. Por lo tanto, no debe empezar a evaluar los riesgos con ninguna metodología en mente, o con alguna hoja que descargaste en algún lugar de Internet (esta hoja podría utilizar una metodología que es completamente inadecuada para su empresa); del mismo modo no debería empezar a utilizar la metodología descrita por la herramienta de evaluación de riesgos que ha adquirido (en su lugar, usted debe elegir la herramienta de evaluación de riesgos que se adapte a su metodología, o puede decidir que no necesita una herramienta, y que lo puede hacer mediante sencillas hojas de Excel).

Lo que debe hacer es – debe desarrollar o adaptar la metodología a sus circunstancias específicas y a sus necesidades.

Entradas. Existen muchos mitos con respecto a lo que la evaluación del riesgo debe ser, pero en realidad los requisitos de la ISO 27001:2013 no son muy difíciles - aquí tiene lo que la cláusula 6.1.2 requiere:

1) Definir cómo identificar los riesgos que podrían causar la pérdida de confidencialidad, integridad y/o disponibilidad en su información.

2) Definir cómo identificar a los propietarios de riesgos

3) Definir los criterios para evaluar las consecuencias y evaluar la probabilidad del riesgo

4) Definir cómo será calculado el riesgo

5) Definir los criterios para la aceptación de riesgos

Por tanto, esencialmente, debe definir estos 5 elementos en su metodología – cualquier otra cosa no será suficiente, pero más importante aún - no es necesario nada más, lo cual significa: no se complique demasiado la vida.

También, debe asegurarse de que los resultados de la evaluación de riesgos son consistentes, es decir, tiene que definir que dicha metodología produce resultados comparables en todos los departamentos de su empresa.

Opciones. Por supuesto, hay muchas opciones disponibles para los 5 elementos de arriba – aquí tiene lo que puede escoger:

- **Identificación de riesgos.** En la revisión del 2005 de la ISO 27001, fue descrita la metodología para la identificación: necesita identificar activos, amenazas y vulnerabilidades. La actual revisión del 2013 de la ISO 27001 no requiere tal identificación, lo que significa que puede identificar los riesgos basándose en sus procesos, en sus departamentos, utilizando sólo las amenazas y vulnerabilidades, o cualquier otra metodología que le gusta; sin embargo, mi preferencia sigue siendo el viejo buen método de activos-amenazas-vulnerabilidades – por ejemplo este método le permitirá identificar, por ejemplo, todas las personas que crean altos riesgos en su empresa, y las personas muy a menudo son el eslabón más débil de seguridad.

- **Propietarios de riesgos.** Básicamente, usted debe elegir a una persona que esté interesada en la resolución de un riesgo y esté bien posicionada en la organización para hacer algo al respecto.

- **Evaluando consecuencias y probabilidad.** Se deben evaluar por separado las consecuencias y la probabilidad para cada uno de sus riesgos; Usted es totalmente libre de usar cualquier escala que le guste – por ejemplo, Bajo-Medio-Alto, o de 1 a 5, o de 1 a 10, etc. - lo que más le convenga. Por supuesto, si quiere hacerlo simple, utilice Bajo-Medio-Alto.

- **Método de cálculo del riesgo.** Esto habitualmente se realiza mediante la suma de las consecuencias y la probabilidad (por ejemplo, 2 + 5 = 7) o a través de la multiplicación (por ejemplo, 2 x 5 = 10). Si utiliza escalas de Bajo-Medio-Alto, esto es lo mismo que utilizar la escala 1-2-3, por lo que de nuevo tendrás números para el cálculo.

- **Criterio para aceptar riesgos.** Si su método de cálculo del riesgo no produce los valores de 1 a 10, puede decidir que un nivel aceptable de riesgo es, por ejemplo, 7 – esto significa que sólo los riesgos valorados con 8, 9 y 10, necesitan un tratamiento. Como alternativa, puede examinar cada riesgo individual y decidir cuál necesita un tratamiento, basándose en su conocimiento y experiencia, usando valores no predefinidos. En cualquier caso, el nivel de riesgo aceptable debe estar en consonancia con su estrategia de negocio – si usted por ejemplo es una organización conservadora como un banco, entonces su nivel de riesgo aceptable será menor.

La decisión de elegir entre estas opciones dependerá de lo siguiente:

- Tamaño y complejidad de su empresa – mientras más pequeña y menos compleja sea su organización, más simple deberá ser su metodología

- Legislación y obligaciones contractuales – si las leyes y requerimientos (también contratos con sus clientes) le requieren que use una determinada metodología, entonces no tienes nada que hacer.

- Reglas existentes para la gestión de riesgos – si usted es una empresa grande, o un banco, es probable que ya tenga algunas políticas para la gestión de riesgos empresariales – su gestión de riesgos de seguridad de la información debe cumplir con estas políticas.

Decisiones. Ya que este tipo de metodología tendrá consecuencias en los empleados involucrados, y también puede tener consecuencias en la precisión de los resultados, se recomienda que la aprobación final de este documento sea realizada por la alta dirección. Por supuesto, antes de enviarlo para su aprobación, usted debe enviarla para su revisión a un par de jefes de departamentos y a los miembros de su equipo de proyecto.

Documentación. El documento de su metodología tiene que describir lo siguiente:

- El proceso de evaluación de riesgos, incluyendo el método de identificación de riesgos, cómo se determina el nivel de riesgos, escalas de evaluación, método para el cálculo del riesgo, cómo determinar el propietario del riesgo, el nivel de riesgo aceptable, cómo realizar la decisión del tratamiento del riesgo, qué herramientas utilizar, etc.

- El proceso de tratamiento de riesgos, incluyendo responsabilidades y documentación.

- Leyes, regulaciones, requerimientos contractuales relacionados con la gestión de riesgos.

- El periodo de revisión – normalmente una vez al año, o con más frecuencia si existen cambios importantes. Vea también la sección Revisión periódica del análisis y tratamiento de riesgos (cláusula 8.2)8.9 para más detalles.

- Roles en el proceso completo – por favor, sea las secciones sobre la realización del análisis y tratamiento de riesgos.

- Qué documentos tienen que producirse – por favor, sea las secciones sobre la realización del análisis y tratamiento de riesgos.

- Quién debe comunicar qué información a quién, y qué reportes serán necesarios.

- Cómo proteger la confidencialidad de la información producida durante el análisis.

Consejo de documentación: (obligatorio) Un documento denominado *Metodología de evaluación de riesgos* o *Metodología de gestión de riesgos*.

7.4 Análisis de riesgos parte I: Identificando riesgos (cláusulas 6.1.2 y 8.2)

Propósito. Basándome en mi experiencia, los empleados y toda la organización en su conjunto son generalmente conscientes de sólo un 25 a 40% de los riesgos – por lo tanto, un proceso minucioso y sistemático debe llevarse a cabo para averiguar todo lo que podría poner en peligro la confidencialidad, integridad y disponibilidad de su información.

Opciones. Puesto que este paso en el proyecto podría ser bastante largo y complejo, debe decidir si será coordinado por el CISO, o por algunos expertos contratados (por ejemplo, un consultor) - por simplicidad, voy a mencionar sólo el CISO en esta sección. En cualquier caso, esta persona tiene que desarrollar hojas de recogida de información (o si se utiliza una herramienta, configurarla), organizar entrevistas o talleres, compilar toda la información y producir el informe.

Si elige la manera más fácil y envía la metodología y las hojas de evaluación de riesgos a las personas responsables de cada departamento, y les dice que las deben devolver, por ejemplo, el próximo Lunes, puede estar seguro que los resultados que obtendrá de ellos serán inservibles (si los obtiene). Esto es porque resulta muy difícil entender lo que es la evaluación de riesgos, incluso si ha escrito muy bien su metodología.

Por lo tanto, si quiere tener éxito, básicamente tiene 2 opciones:

a) **Realizar el análisis de riesgos a través de entrevistas** – Esto significa que el CISO entrevistará a la persona responsable de cada departamento, y en primer lugar explicará el propósito de la evaluación de riesgos, y por otra parte se asegurará de que todas las decisiones, sobre el nivel de riesgo, de la persona responsable (consecuencia y probabilidad), tienen sentido y no son parciales.

b) **Realizar talleres con las personas responsables** – en estos talleres el CISO explica a todas las personas responsables el objetivo de la evaluación de riesgos, y a través de varios ejemplos de la vida real, muestra cómo identificar los riesgos y evaluar su nivel.

BIBLIOGRAFÍA

ISO 9001:2015, Quality management systems – Requirements

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

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

ISO 22301: 2012, Societal security – Business continuity management systems – Requirements

ISO/IEC 27000:2016, Information technology – Security techniques – Information security management systems – Overview and vocabulary

ISO/IEC 27001:2005, Information technology – Security techniques – Information security management systems – Requirements

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

ISO/IEC 27002:2013, Information technology – Security techniques – Code of practice for information security controls

ISO/IEC 27004:2009, Information technology – Security techniques – Information security management – Measurement

ISO/IEC 27005:2011, Information technology – Security techniques – Information security risk management

ISO/IEC 27017:2015, Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services

ISO/IEC 27018:2014, Information technology – Security techniques – Code of practice for protection of personally identifiable information

(PII) in public clouds acting as PII processors

ISO/IEC 27032:2012, Information technology – Security techniques – Guidelines for cybersecurity

ISO 31000:2009, Risk management – Principles and guidelines

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

COBIT 5, ISACA, 2012

ITIL 2011, Axelos, 2011

PCI DSS version 3.2, Payment Card Industry Security Standards Council, 2016

SP800 series, NIST

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

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

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

SEGURO & SIMPLE: UNA GUÍA PARA LA PEQUEÑA EMPRESA PARA LA IMPLEMENTACIÓN DE LA ISO 27001 CON MEDIOS PROPIOS

El manual, con un idioma plano, paso a paso, para los profesionales de seguridad de la información

Piense y actúe como un consultor con esta guía comprensiva, y práctica, para la implementación de la ISO 27001.

El autor Dejan Kosutic, consultor experimentado en seguridad de la información, comparte con usted todo su conocimiento, y su experiencia práctica en este libro invaluable.

- ✓ Consiga una explicación simple sobre el estándar ISO 27001
- ✓ Aprenda cómo empezar el proyecto de implementación
- ✓ Aprenda cómo escribir la política de seguridad de la información, y otras políticas y procedimientos
- ✓ Realice el análisis y tratamiento de riesgos
- ✓ Aprenda cómo estructurar la documentación obligatoria
- ✓ Aprenda el proceso de certificación, y el criterio de las entidades certificadoras
- ✓ Todo esto y mucho más…

Escrito en español y evitando la jerga técnica de los frikis, Seguro & Simple, está escrito para personas normales, con un lenguaje llano, simple. Si usted es un profesional de seguridad de la información, o es nuevo en este campo, este el único libro que necesitará.