Nueve pasos para el éxito

Una visión de conjunto para la aplicación de la ISO 27001:2013

Alan Calder

Nueve pasos para el éxito

Una visión de conjunto para la aplicación de la ISO 27001:2013

ALAN CALDER

IT Governance Publishing

IT Governance Publishing
IT Governance Limited
Unit 3, Clive Court
Bartholomew's Walk
Cambridgeshire Business Park
Ely, Cambridgeshire
CB7 4EA
Reino Unido

www.itgovernance.co.uk

Publicada por primera vez en el Reino Unido en 2017
por IT Governance Publishing: ISBN: 978-1-84928-929-0

ÍNDICE

INTRODUCCIÓN

El ciberriesgo se ha convertido en un problema empresarial serio, con la alta gerencia cada vez más bajo presión, por parte de clientes, reguladores y socios, para garantizar que su organización puede defenderse, responder y recuperarse de un ciberataque.

La resistencia contra ciberataques requiere que una organización haga algo más que solo colocar defensas digitales; un porcentaje considerable de los ataques con éxito se originan en al mundo físico análogo o reciben ayuda y se agravan por vulnerabilidades físicas y ambientales. Una ciberseguridad eficaz requiere por tanto un sistema de gestión de la seguridad de la información fuerte, sistemático e integral; los consejos, los clientes y los reguladores todos buscan una garantía de que se han identificado los riesgos de la información y están siendo gestionados.

La norma internacional ISO/IEC 27001:2013 *Tecnología de la información – Técnicas de seguridad – Sistemas de gestión de la seguridad de la información – Requisitos* es el plan para gestionar la seguridad de la información en línea con los requisitos reglamentarios, contractuales y empresariales de una organización, y su apetito de riesgo La seguridad de la información siempre ha sido un problema internacional y esta versión de la Norma refleja ocho años de mejoras en el entendimiento de la gestión de la seguridad de la información eficaz. Además, tiene en cuenta el progreso en el panorama de las ciberamenazas en ese periodo y permite un amplio abanico de controles de mejores prácticas.

La seguridad de la información es ahora también claramente un problema de gestión y una responsabilidad de la

gobernanza. El diseño y la implementación de un sistema de gestión de la seguridad de la información (SGSI) es una función de la gerencia y no tecnológico. Requiere todo el abanico de habilidades y atributos gerenciales, desde la gestión de proyectos y priorización pasando por la comunicación, habilidades de ventas y motivación hasta la delegación, monitorización y disciplina. Un buen gerente que no tenga experiencia o conocimientos tecnológicos puede liderar una implementación de SGSI con éxito, pero sin las habilidades de gestión, el especialista en seguridad de la información más tecnológicamente sofisticado fallará en la tarea.

Esto es particularmente así si la organización quiere derivar el máximo valor a largo plazo de la implementación de un SGSI. Lograr una certificación externa es cada vez más un coste estándar de hacer negocios; alcanzar el nivel de conocimiento de seguridad de la información y una buena práctica interna que permita que una organización surque los mares tormentosos y crueles de la edad de la información requiere un nivel de cambio de cultura no menos profundo que aquel necesario para el cambio de las operaciones industriales a posindustriales.

Sé todo esto porque mi experiencia es de administrador general y no de tecnólogo. Entré en la seguridad de la información en 1995 porque estaba preocupado sobre las exposiciones de la seguridad de la información afrontadas por una empresa en la que era director ejecutivo. Cuando uno es el director ejecutivo y está interesado en esto, puede hacer que ocurra un SGSI, como he demostrado en varias ocasiones. Aunque este libro reducirá la curva de aprendizaje para otros directores ejecutivos en mi posición, está dirigido realmente al gerente, a menudo un gerente de seguridad de la información o de TI, algunas veces un gerente de calidad,

que esté encargado de emprender una implementación del ISO 27001 y que quiere entender la ruta a un resultado positivo. Se basa en la experiencia de muchas implementaciones de ISO 27001 y refleja la metodología de implementación en nueve pasos que ahora respalda todos los productos y servicios de ISO 27001 que se pueden acceder a través de IT Governance Ltd, la empresa que fundé allá en 2005. Estos nueve pasos funcionan en cualquier organización: sector público, sector voluntario y privado, en cualquier parte del mundo. La infraestructura de tecnología, el modelo empresarial, la arquitectura organizativa y los requisitos reglamentarios todos informan del contexto para la implementación de un SGSI de la ISO 27001 pero no limitan su aplicabilidad. Hemos ayudado a implementar un SGSI de la ISO 27001 en empresas que tenían solo dos personas, en empresas globales gigantescas que trabajan en varios países y en organizaciones de todos los tipos y tamaños en medio.

El segundo mayor reto que, en mi experiencia, afrontan los tecnólogos en seguridad de la información en todas partes del mundo es conseguir y mantener la atención del consejo. El mayor reto es ganarse, y mantener, el *interés de la organización en el proyecto y la aplicación en este*. La atención en curso de la prensa y el público acerca del ciberriesgo está llevando el problema a las órdenes del día de los consejos, y cuando los consejos entiendan finalmente que tienen que actuar, sistemática e integralmente, frente a las amenazas de seguridad de la información, se interesan mucho en oír a sus especialistas de seguridad de la información. Incluso desarrollan un apetito en investir dólares organizativos en soluciones de hardware y software y en encargar el desarrollo de un nuevo SGSI, o intensificar el existente.

Un proyecto de SGSI con éxito resulta y depende de un apoyo genuino de la alta gerencia. El progreso es más rápido si el proyecto se ve como algo que tiene una necesidad empresarial creíble: para ganar subcontratación u otro contrato con el cliente, por ejemplo, o para cumplir un requisito de financiación pública, mejorar la competitividad o reducir los costes de cumplimiento reglamentario y las exposiciones.

Cuando decidimos por primera vez abordar la seguridad de la información, allá en 1995, se exigió que mi organización lograse tanto la certificación ISO 9001 como el reconocimiento de Investors in People (IiP) como condición de su licencia de comercio y desarrollo de marca. Además, pretendíamos vender servicios de gestión medioambiental y de seguridad de la información y, con el deseo de poner en práctica lo que predicábamos, así como con una determinación por lograr los beneficios identificables de abordar todos estos componentes de nuestro negocio, decidimos aplicar tanto la BS 7799 como la ISO 14001 al mismo tiempo.

La certificación BS 7799 solo existía entonces en una forma sin acreditar y era, esencialmente, un Código de Prácticas. Solo había una parte para esto y, aunque la certificación no era técnicamente posible, algunos organismos certificadores estaban interesados en expedir declaraciones de conformidad. Las otras normas en las que estábamos interesados existían pero, en aquel tiempo, se esperaba que una organización abordaría cada norma por su cuenta, desarrollando manuales y procesos independientes. ¡Esto fue apenas sorprendente, ya que era inusual que cualquier organización buscara más de una norma en cualquier momento!

Tomamos la decisión trascendental de abordar el tema desde una perspectiva empresarial principalmente, más que una de calidad. Decidimos que queríamos crear un sistema de gestión integrado único que funcionara para nuestra empresa, y que fuera capaz de lograr múltiples certificaciones. Aunque esto parecía ir en contra de la práctica estándar acerca de la implementación del sistema de gestión, parecía estar en línea con el espíritu de las normas mismas.

Además, decidimos que queríamos que todos en la organización participaran en el proceso de crear y desarrollar el sistema de gestión integrado que concebimos. Creímos que era la manera más rápida y más certera de hacer que se convirtieran en auténticos contribuidores en el proyecto, tanto a corto como a largo plazo. Utilizamos consultores externos para parte del proyecto de la ISO 9001 pero simplemente no había conocimientos de la BS 7799 disponibles externamente.

Esta falta de especialistas de BS 7799 era un reto menor en comparación con la falta de libros o herramientas útiles. En la actualidad, puede comprar libros tales como *Una introducción a la ISO27001 y la seguridad de la información de la seguridad*; de aquella había estanterías llenas de libros gruesos centrados en la tecnología sobre toda clase de problemas de la seguridad de la información, pero nada que pudiera decirle a un gerente comercial cómo implementar sistemáticamente un sistema de gestión de la seguridad de la información. No tuvimos otra opción que intentar solucionarlo nosotros mismos.

En realidad hicimos el trabajo dos veces, una vez en el programa sin acreditar y la segunda vez después de que la Norma se convirtiera en dos partes y se hubiera acreditado

(la anterior parte sencilla se había convertido en un Código de Prácticas y se había introducido una parte nueva, una especificación para un sistema de gestión de la seguridad de la información). De hecho, nuestra auditoría acreditada también fue la primera auditoría observada de un nuestro organismo de certificación para su propia acreditación de UKAS. ¡Aunque fue una experiencia interesante, significó que nuestros sistemas tenían que ser particularmente fuertes si tenían que resistir el escrutinio simultáneo de dos niveles de auditores externos!

Nos sometimos a un examen externo en cinco ocasiones separadas en unos meses y nuestro sistema de gestión integrado logró todas las certificaciones y reconocimientos externos necesarios. Hicimos esto sin nada más que la asistencia a tiempo parcial de un consultor de ISO 9001 y un equipo de gestión de calidad interna formado por una persona. Steve Watkins, ahora director de IT Governance Ltd y Asesor Técnico de UKAS para ISO 27001, fue ese gerente de calidad e hizo la mayor parte del trabajo real para crear nuestro sistema de gestión integrado para múltiples normas. Es verdad que la organización era relativamente pequeña pero, aunque solo empleábamos unas 80 personas (en tres sitios), también teníamos un equipo de consultores asociados que eran un grupo de casi cien. Y de aquella, probablemente no podríamos haber hecho algo tan complejo como esto en una organización mucho más grande.

Las lecciones que Steve y yo aprendimos en nuestras dos primeras implementaciones, y nuestra experiencia con las implementaciones de ISO 27001 desde entonces, a menudo en organizaciones del sector público y privado muy importantes, nos han permitido cristalizar las nueve claves para una implementación de SGSI con éxito.

Dirigido y gestionado adecuadamente, cualquier proyecto de ISO 27001 puede tener éxito. Nosotros lo hemos demostrado.

Con el paso de los años, mi organización (IT Governance Ltd: *www.itgovernance.co.uk*) ha desarrollado enfoques para implementar un SGSI que pueden ayudar a los gerentes de proyecto a identificar y superar muchos de los problemas muy reales que afrontan al lograr un resultado con éxito. Además, hemos desarrollado herramientas y técnicas únicas que simplifican el proceso, que encajan en los nueves pasos descritos en este libro y que permiten que las organizaciones tengan éxito sin ayuda externa adicional. El éxito en la seguridad de la información, a largo plazo, no tiene que depender de un consultor; depende de la organización misma. Este libro describe los problemas clave, los componentes básicos del éxito, y le dicen cómo abordarlos.

El libro está pensado para ser una guía de nivel bastante alto para el proceso de implementación de nueve pasos y por tanto hace referencia, de vez en cuando, a libros más detallados o herramientas que se han desarrollado o publicado por mi empresa. En particular, hace referencia a menudo a *Normas de TI – Una guía internacional a la seguridad de los datos e ISO27001/ISO27002, sexta edición* considerablemente más detallada y exhaustiva, que Steve y yo escribimos originalmente para llenar la laguna evidente en orientación disponible en la materia. Ese libro es ahora también un libro de texto de posgrado en la Universidad Abierta sobre seguridad de la información.

En cada caso en el que he hecho una referencia específica, el libro o herramienta es único y se desarrollaron para hacer el trabajo específico que describo que hace. Desarrollamos estos libros, herramientas y servicios porque sencillamente

no había nada disponible en el mercado que hiciera un trabajo comparable o que ofreciera la rentabilidad de la inversión que sabemos que nuestros clientes están buscando.

La familia de la ISO 27000

La norma de la seguridad de la información es, de hecho, una norma con dos partes que ha sufrido una evolución considerable. Una parte de la norma (ISO 27001:2013) proporciona una especificación para el SGSI (utiliza palabras como "debe", concretamente en el Anexo A, que es la lista de los controles). La otra parte (ISO 27002:2013) tiene el estado de Código de prácticas; la orientación reunida sobre la seguridad de la información de las mejores prácticas de todo el mundo.

La diferencia entre una especificación y un Código de prácticas, en el mundo de las normas de los sistemas de gestión, es que una especificación contiene la palabra "debe" y especifica que es obligatorio para un sistema si quiere cumplir la norma, mientras que un Código de prácticas ofrecer una orientación y usa palabras como "debería" para indicar que el cumplimiento no es obligatorio. Las organizaciones pueden elegir los controles de este Código de prácticas o de cualquier otra parte, siempre y cuando se cumplan los requisitos de la especificación. La certificación acreditada tiene lugar frente a una especificación de requisitos y no un Código de prácticas.

La ISO 27001 está vinculada a la ISO 27002 y, cuando la organización utiliza los controles del Anexo A, la ISO 27002 proporciona una directriz sobre cómo implementar esos controles.

Estas dos normas están respaldadas por la ISO 27000, que proporciona las definiciones en las que dependen. Esta es una obra ligera, pero contiene una directriz útil y todas las definiciones esenciales que ayudarán a todos los que participen en el proyecto de implementación están en la misma página.

Tienen que obtener, y estudiar, las copias de tanto la *ISO/IEC 27001:2013* como la *ISO/IEC 27002:2013*. Es específicamente la ISO 27001 que se medirá el cumplimiento y las palabras exactas en esa norma tienen precedencia sobre cualquier otra directriz o comentario. Se pueden obtener copias de las normas en su organismo de normalización nacional o en *www.itgovernance.co.uk* (IT Governance Ltd es una distribuidora de normas autorizada para una serie de organismos de normalización).

En los casos de duda o incertidumbre, su auditor de la certificación hara referencia a las normas para aclaración; si todo lo que hace se puede relacionar con palabras concretas en la norma estará en una posición fuerte. Por otro lado, no suponga que si hace algo que no está especificado en la norma, su acción es incorrecta. La norma es un requisito *mínimo* y no el máximo.

Vínculos con otras normas

La ISO 27001 está respaldada por una familia de normas de mejores prácticas relacionadas, cada una de las cuales proporciona una directriz adicional sobre un aspecto concreto de la gestión de la seguridad de la información. Esta familia de normas está creciendo y desarrollándose continuamente; la información actualizada está disponible en *www.itgovernance.eu/iso27000-family*.

La ISO 27001:2013 armonizará con la ISO 9001:2015 y la ISO 14001:2015, así como con la ISO 22301, ISO 20000-1 y la ISO 50001, para que los sistemas de gestión se puedan integrar con eficacia.

La ISO 27001 reconoce implícitamente que la seguridad de la información y un SGSI deberían formar parte integral de cualquier sistema de control interno creado como parte de los procedimientos del gobierno corporativo. La norma encaja con el enfoque adoptado en el Reino Unido por la Directiz sobre gestión del riesgo de FRC.

Hay más debate sobre las relaciones con estas otras normas, más detalles sobre la relación con la ISO 27002 y una orientación inicial sobre cómo los marcos tales como el ITIL (y la ISO 20000) y COBIT se podrían utilizar en la implementación de la ISO 27001 en *Una introducción a la ISO27001 y la seguridad de la información*.

Antes de empezar

Valdría la pena recibir una formación adecuada antes de empezar su proyecto de SGSI.

Los cursos de formación más útiles son aquellos que ofrecen una introducción al tema completo, aquellos que cubren la implementación y aquellos que cubren la auditoría. Todos los cursos buenos están acreditados por una junta de examen externo, tal como IBITGQ (la junta internacional para cualificaciones en gobierno de TI – *www.ibitggq.org*).

Un curso básico sobre SGSI de la ISO27001 es un curso de un día que ofrece conocimientos amplios sobre el tema y es adecuado para todos los miembros del equipo del proyecto.

Un curso de Implementador líder en ISO27001 es el curso ideal para aquellos que serán responsables de llevar adelante el proyecto. Es un curso de tres días que proporciona una orientación práctica sobre la implementación eficaz. La cualificación de Implementador líder en seguridad de la información certificado (CIS LI, por sus siglas en inglés) está reconocido ampliamente, y los cursos y exámenes de CIS LI reflejan el enfoque de nueve pasos que describo.

Todos los sistemas de gestión tienen que estar sujetos a una auditoría interna (gestión) y un curso de Auditor líder de SGSI (o, posiblemente, un SGSI interno) proporcionará a aquellos dentro de su organización a los que se les encargará el diseño y la gestión de su proceso de auditoría de la seguridad de la información las habilidades que necesiten para hacerlo eficazmente.

Puede ver más información detallada sobre estos, y otros, cursos aquí: *www.itgovernance.eu/itg-training-courses*. Estas cualificaciones se puede lograr atendiendo un curso en aula (gastos de viaje u hotel diarios) o uno en directo por internet (se prepara sus propias bebidas y comidas).

La formación será también, por supuesto, un facilitador importante de los tipos de cambios que su organización tenga que hacer en cuanto a la gestión de la seguridad de la información. Exponer a todo el equipo del proyecto a los principios de la ISO 27001 mediante un curso de formación básica sobre la ISO 27001 es un paso sensato después de haber proporcionado la formación para el crucial implementador líder y el auditor líder. El personal en toda la empresa también necesitará formación específica en aquellos aspectos de la política de seguridad que afecte su trabajo cotidiano. El gerente informático y el personal informático todos necesitarán competencias específicas en seguridad de

la información (ver ISO 27001 cláusula 7.2) y, si esto hay que mejorarlo con formación, debería ser ofrecido por una organización que reconozca y entienda los aspectos técnicos de la formación sobre la ISO 27001. Se puede encontrar más información sobre la formación adecuada aquí: *www.itgovernance.eu/itg-training-courses*.

CAPÍTULO 1: ENCARGO DEL PROYECTO

Puede sonar un poco a cliché pero, para los proyectos del sistema de gestión de la seguridad de la información (SGSI), es desde luego cierto que "empezar bien es tener la mitad hecha". La persona encargada de liderar un proyecto de SGSI de la ISO/IEC 27001:2013 tiene que reducir que parece potencialmente complejo, difícil y caro en cuanto a tiempo y recursos, a algo que todos creen que se puede lograr en el marco de tiempo asignado y con los recursos permitidos. ¡Y entonces tiene que asegurarse de que se entrega realmente!

Lo que esto significa en realidad es que el líder del proyecto de SGSI tiene que crear el proyecto de tal manera que cuente con los fondos adecuados, que hay tiempo suficiente (incluyendo para todo lo que puede salir mal) y que todos entiendan los riesgos en el proyecto y acepten los controles que se están utilizando para minimizarlos.

A casi todo el mundo le desagrada el cambio. Muy pocas personas disfrutan tratando lo desconocido. La mayoría de las personas ven un proyecto de SGSI como algo que trae tanto cambio como lo desconocido a su vida laboral, y no todos se alegrarán. Eso es normal; lo asimilarán al final.

El líder del proyecto, en la primera fase del proyecto, es la persona al que todos los demás en la organización acuden en busca de conocimientos, consuelo y apoyo. Tiene que ser la persona que ofrezca entusiasmo, certeza y entendimiento de lo que implica.

Esto significa que el aprendizaje en el puesto de trabajo de manera transparente no es aconsejable. No quiero decir que tiene que saber todas las respuestas al comienzo, porque eso

no es realista. Mientras tenga un claro entendimiento de los problemas estratégicos y el conocimiento práctico de dónde acudir para conseguir asesoramiento y orientación, puede ser eficaz, incluso si solo está un día o dos por delante de todos los demás en el conocimiento detallado necesario para el proyecto.

Se sorprendería con la cantidad de veces que alguien ha iniciado un proyecto de SGSI sin preparación adecuada, ha fallado al responder una serie de preguntas o retos sobre problemas específicos adecuadamente y entonces se ha sorprendido de que el proyecto haya perdido credibilidad bastante rápido.

El apoyo de su director ejecutivo para el proyecto es incluso más importante que su propio entendimiento de lo que está intentando lograr. La seguridad de la información es tanto una cuestión de gestión como de gobierno. La implementación con éxito de un SGSI depende absolutamente de que el proyecto tenga apoyo verdadero de la cúpula de la organización. Con este, tiene una oportunidad verdadera de éxito; sin él, nada de nada. *Asegurar el apoyo verdadero de la alta gerencia,* no aceptar meramente de boquilla, es clave para el éxito de la ISO 27001. En este contexto, no estoy hablando necesariamente sobre el director ejecutivo de una gran organización con múltiples filiales; estoy hablando de la persona que es responsable del éxito o fracaso empresarial de la entidad comercial que esté considerando la ISO 27001. Esto podría ser una división comercial, una empresa filial, una unidad independiente o una organización virtual.

Es importante ser claro acerca del significado de "responsable" en este contexto. Estoy hablando de la persona cuyo trabajo y carrera depende en última instancia del éxito

de la entidad empresarial que esté considerando la ISO 27001; esta persona no siempre ocupa la función que es formalmente "donde recae la responsabilidad". Todas las organizaciones saben exactamente dónde recae la responsabilidad realmente, y esta es la persona a la que me refiero como el director ejecutivo en este capítulo.

Alineamiento estratégico

La primera razón de por qué el director ejecutivo tiene que apoyarle totalmente y el proyecto de SGSI es que es un proyecto empresarial y no un proyecto informático. Tiene que estar completamente en línea con el modelo empresarial, la estrategia empresarial y las metas y tiene que priorizarse para la empresa y asignarse un nivel adecuado de recursos. Aunque es improbable que el director ejecutivo sea el líder del proyecto de SGSI, la única persona que puede priorizar eficazmente la seguridad cibernética es el director ejecutivo. Ningún simple líder de proyecto está en una posición para tener claro las metas y necesidades estratégicas de la organización pero, como este es un proyecto estratégico que afecta a todos, tiene que estar "al tanto" para que pueda personalizar sus propios planes para cumplir las prioridades empresariales de la organización.

Además, tiene que saber qué riesgos estratégicos son afrontados por la organización y cómo estos se reflejan y priorizan en los riesgos de la seguridad de la información. Hay muchas preguntas posibles, cuyas respuestas serán cruciales para su enfoque y plan detallado. Por ejemplo, ¿es el riesgo de robo de propiedad intelectual más significativo, con un potencial de impacto mayor, que el riesgo, por ejemplo, de cierre del negocio durante tres días? ¿Es el cumplimiento reglamentario más, o menos, importante que

reducir el coste de las ventas? ¿Van a ser la seguridad de la información y el cumplimiento reglamentario importantes en las soluciones de subcontratación (o, cuando se afronte una elección entre una opción de subcontratación con un coste más bajo, pero menos segura, y uno más segura pero más cara, cuál elegirá la organización)? ¿Cómo se debería resolver el conflicto entre los requisitos reglamentarios de dos jurisdicciones distintas en las que la organización comercia? ¿Cuál es la compensación entre la flexibilidad operativa que se permite a las organizaciones filiales y la implementación de un nivel mínimo y sistemático de seguridad de la información y la fiabilidad de los servicios informáticos? ¿Cuáles son los planes a largo plazo para los servicios de apoyo específicos (si se van a subcontratar, entonces va a enfocar la implementación del SGSI de manera diferente que si se quedan en la organización)? Hay muchas preguntas así, cuyas respuestas tiene que saber antes de que pueda incluso empezar a planificar; hay muchas otras que surgirán en el curso del proyecto.

Priorización y respaldo

La segunda razón de que necesite este tipo de apoyo es que, sin él, el proyecto simplemente no ocurrirá. No es suficiente que el director ejecutivo y la gerencia ejecutiva simplemente reconozcan que el proyecto es importante. No es suficiente que meramente hablen de él. No es suficiente que usted sepa las prioridades estratégicas de la organización y que sea capaz de alinear el proyecto con el plan empresarial.

Si va a suceder de verdad, la alta gerencia tiene que comprometerse, determinados realmente a lograrlo. El compromiso de la alta gerencia significa que el proyecto consiga los recursos humanos y financieros que necesita.

Consigue la supervisión, "tiempo dedicado a la comunicación personal" y los plazos de comunicación interna que necesita. A menos que tenga esta clase de compromiso, van a haber muchas cosas que las personas en toda la organización verán como con mayores prioridades que su proyecto. Por supuesto, van a haber *algunas* prioridades mayores; lo que necesita es una clara priorización que se entienda en toda la empresa y que se respalde continuamente por el director ejecutivo.

La priorización relativa de las necesidades de su proyecto tienen que ser entendida claramente. Dentro de este contexto, tiene que tener el respaldo firme y absoluto del director ejecutivo. Por "respaldo" quiero decir que, cuando aparezcan ocasionalmente esas barreras internas innecesarias, las palabras: "Este es un proyecto respaldado/ordenado por el director ejecutivo" deberían contribuir a superarlas.

Gestión del cambio

La tercera razón por la que necesita el apoyo del director ejecutivo es que un proyecto de SGSI es probable que sea un proyecto de gestión de cambio. La implementación de un SGSI no es una actividad de impacto bajo. Puede requerir cambios sobre cómo los usuarios de los ordenadores hacen una serie de cosas y también afecta a aspectos de las actividades cotidianas de los gerentes. Un proyecto de SGSI con éxito es, en otras palabras, un perfil bajo, pero no obstante un proyecto de gestión del cambio de gran alcance y la manera de enfocarlo tiene que aprender de la experiencia de programas de gestión del cambio con éxito.

Han habido muchos libros escritos acerca de la gestión del cambio. Muchos de estos proyectos no dan los beneficios que

se han utilizado para justificar el gasto de empezarlos y llevarlos a cabo. La implementación con éxito de un SGSI no requiere un programa de gestión del cambio estratégico y detallado, concretamente no uno concebido e impulsado por consultores externos. Lo que necesita es una claridad completa entre la alta gerencia, aquellos encargados con impulsar el proyecto hacia delante y aquellos cuyas prácticas de trabajo se verán afectadas, en cuanto a por qué es necesario el cambio, cómo será el resultado final y por qué este resultado es esencial. Los aspectos de la gestión del cambio de esto son la tercera razón de por qué el apoyo y el respaldo del director ejecutivo son esenciales: quiere que él dé ejemplo, haciendo todas las cosas que va a querer que alguien más haga.

El hecho es que la norma misma exige este nivel de apoyo. No permitirá que ningún organismo de certificación certifique un SGSI sin conseguir pruebas firmes de que la alta gerencia está comprometida. La razón para esto es sencilla: si falta compromiso, el SGSI no será adecuado; los riesgos para la organización no se reconocerán propiamente ni se abordarán totalmente; y es improbable que se hayan considerado las metas empresariales estratégicas y los consiguientes requisitos futuros de la seguridad de la información.

La función del director ejecutivo

Idealmente, el director ejecutivo debería ser la fuerza impulsora detrás del programa y el logro de la certificación de la ISO 27001 debería ser una meta indicada claramente en el plan empresarial actual. El director ejecutivo tiene que entender completamente los problemas estratégicos acerca del gobierno de TI y la seguridad de la información y el valor

para la empresa de la certificación con éxito. El director ejecutivo tiene que ser capaz de expresar esto al consejo y la alta gerencia, y abordar las objeciones y problemas que surjan. Sobre todo, tiene que tener suficientemente al cargo de esta parte del plan empresarial para ser capaz de mantenerlo enfocado frente a las metas estratégicas.

El presidente y el consejo deberían prestar tanta atención al progreso de la monitorización frente al plan de implementación de la ISO 27001 como lo hacen con la monitorización de todas las demás metas empresariales clave. La cláusula 5.1 de la norma requiere específicamente pruebas de este compromiso desde la cúpula: "La alta gerencia demostrará liderazgo y compromiso con respecto al sistema de gestión de la seguridad de la información". Si el director ejecutivo y el consejo no están detrás de este proyecto no tiene mucho sentido seguir; la certificación no ocurrirá sin pruebas claras de dicho compromiso. Este principio de liderazgo de la cúpula es, por supuesto, también fundamental para todos los proyectos de cambio importantes.

Si usted ya es el director ejecutivo de la organización, entonces está haciendo exactamente lo correcto leyendo este libro y preparándose para impulsar el proyecto de la seguridad de la información usted mismo. Si usted no es el director ejecutivo, entonces tiene que asegurarse la clase de compromiso y apoyo que describí anteriormente.

El líder ideal de un proyecto de SGSI es un líder empresarial, un COO (director de operaciones) o una línea de líder empresarial; adoptar un SGSI es un proyecto empresarial y por tanto el liderazgo empresarial es fundamental para su éxito. A menudo es el caso que un proyecto de SGSI falla porque se ha creado como un proyecto de tecnología y por

tanto se ve y trata como un proyecto limitado que no merece el compromiso total de la empresa. "Simplemente otro proyecto informático" es el mensaje equivocado para impulsar un SGSI en la cultura de la organización.

Hay, por supuesto, organizaciones en las que el director de informática es un miembro del equipo de alta gerencia, es responsable de una función integrada que incluye la seguridad de la información y ya tiene la confianza y apoyo plenos del director ejecutivo y el consejo. En dicha organización, el director de informática podría ser el impulsor del proyecto, pero todavía necesitará el compromiso y el apoyo del director ejecutivo, por lo menos para que todos en la organización entienda que asegurar el reconocimiento es una prioridad empresarial. El director de informática también necesitará urgentemente establecer un equipo del proyecto interempresarial; volveré sobre esto más tarde.

El encargo del proyecto

El encargo del proyecto es donde captura la prueba inicial de este compromiso en un formato utilizable. Un encargo de proyecto (o PID por sus siglas en inglés) es un documento que se utiliza ampliamente para capturar los elementos clave de cualquier proyecto complejo. Asegura que haya un punto de referencia único y original que exponga los tres puntos clave para el éxito del proyecto: productos finales, plazo y presupuesto.

Los proyectos complejos fallan porque uno o más de estos tres variables del proyecto se identifican y/o gestionan deficientemente. Los "requerimientos imprevistos" son una de las causas más comunes del fallo de un proyecto. Los

encargos de proyecto, por tanto, buscan identificar claramente el alcance del proyecto y precisar las tres variables con el fin de apoyar un proceso de gobierno del proyecto eficaz.

Su encargo de proyecto debe abordar estos cuatro puntos:

1. Productos finales: identifique el objetivo como el logro de la certificación ISO 27001 para una parte específica o el conjunto de la organización y, si es posible, identifique por qué la seguridad de la información es tan importante para su organización.
2. Plazo: cree un plan del proyecto resumido y fecha de finalización del objetivo basándose en los nueve pasos para el éxito.
3. Presupuesto: identifique los recursos, tanto internos como externos, así como la formación, el software y las herramientas que va a necesitar para el proyecto.
4. Autorización para continuar: el encargo debería contener el respaldo de la gerencia del proyecto y la autorización para continuar, para lograr los objetivos identificados utilizando los recursos presupuestados.

Productos finales y el objetivo del proyecto

Aunque el producto final del proyecto es relativamente fácil de definir (por ejemplo, lograr la certificación ISO 27001 en el plazo de cuatro meses), todavía tendrá que ser claro sobre las razones de buscar ese objetivo así como aclarar la diferencia entre objetivo del proyecto y objetivos de la seguridad de la información.

El propósito de un sistema de gestión de la seguridad de la información es, por supuesto, reducir y controlar los riesgos

en su información. El objetivo real (u objetivos) de su proyecto de SGSI puede ser diferente a los propósito del SGSI mismo, y debería ser claro sobre estas diferencias si se va a centrar adecuadamente tanto en el proyecto como el SGSI. El objetivo del proyecto puede ser, por ejemplo, para asegurar la certificación de la ISO 27001 dentro de un marco de tiempo dado con el fin de cumplir un requisito reglamentario o contractual, para mejorar la competitividad comercial o reducir el coste y la complejidad de las respuestas de ventas y marketing a las invitaciones de licitación. Los objetivos del proyecto, en otras palabras, se vinculan específicamente a beneficios empresariales que se van a derivar de su logro. Los objetivos del proyecto normalmente serán de alto nivel y rendimiento frente a ellos fáciles de seguir.

Los objetivos de la seguridad de la información pueden estar relacionados, pero no necesariamente, con los objetivos del proyecto. Los objetivos de la seguridad de la información se vincularán definitivamente con el mantenimiento de la confidencialidad, la integridad y la disponibilidad de la información dentro de un contexto de la organización y en relación con su apetito de riesgo. El progreso hacia el logro de los objetivos de la seguridad de la información deben ser mensurables, lo cual significa que los objetivos mismos tienen que ser específicos, mensurables, alcanzables, realistas y de tiempo limitado. Los objetivos típicos podrían ser, por ejemplo, reducir la cantidad de incidentes perjudicales de la seguridad de la información de 14 al año a dos por año, o aumentar la disponibilidad de la red del 97 % y 20×7×360 a 99,99999 % y 24×7×365. Dichos objetivos se desglosarán en objetivos de niveles inferiores, con responsabilidad de su logro asignada a los departamentos y niveles adecuados dentro de la organización.

Análisis de las deficiencias

La mayoría de las organizaciones ya están tomando medidas para gestionar su seguridad de la información. Aunque pueden haber vulnerabilidades importantes, ¡no es como si no se estuviera haciendo nada en la actualidad! El punto de partida para su proyecto normalmente es, por tanto, entender lo alejadas que están sus prácticas actuales de los requisitos expuestos en la ISO 27001, y la mejor manera de hacer esto es con lo que llamamos un "análisis de las deficiencias". Esto es una auditoría rápida de nivel razonablemente alto sobre sus prácticas actuales de gestión de la seguridad de la información frente a los requisitos expuestos en la ISO 27001, la cual identifica dónde hay una carencia y también identifica qué recursos y capacidades tiene implantados para solucionar la deficiencia, o que recursos podría necesitar para traerlos de fuera.

Si tiene objetivos de la seguridad de la información ya definidos, su análisis de las deficiencias podría identificar también qué medidas tendrá que tomar aún para lograr esos objetivos.

Podría llamar al resultado del análisis de las deficiencias un "plan de mejora de la seguridad" o "SIP". Este plan de mejora de la seguridad se convierte, en efecto, en su plan de proyecto del SGSI.

Presupuesto y recursos

No puede implementar un SGSI de la ISO 27001 por su cuenta, o sin alguna inversión en herramientas y formación. Para la ISO 27001, "recursos" significa recursos humanos, técnicos, informáticos y financieros. Las herramientas diseñadas para ese propósito es probable que reduzcan

tiempo, errores y coste. Las dos herramientas más útiles son las plantillas de documentación y el software de evaluación del riesgo. La solución de la evaluación del riesgo que más recomendamos está disponible directamente de Vigilant Software, aquí: *www.vigilantsoftware.co.uk*.

Una serie de personas a través de la organización, y desde distintos niveles dentro de ella, tendrán que contribuir. Puede que también quiera traer consultores externos, para orientación o porque necesite un recurso adicional para ejecutar el plan del proyecto.

Hay una serie de áreas especializadas en las que los consultores pueden ser útiles:

- Puede utilizar consultores, terceros de confianza, para comunicar la gravedad de los riesgos de la información afrontados por la organización y la necesidad, por tanto, de un SGSI.
- Puede usar consultores para dar asesoramiento sobre problemas específicos (más a menudo técnicos), por ejemplo estudio del alcance y cómo las amenazas internas o externas podrían afectar sus decisiones sobre el alcance del proyecto, para llevar a cabo una evaluación del riesgo, para ocuparse de la documentación, o para asesorar sobre la integración con otros sistemas de gestión.
- Puede (y podría ser muy sensato) emplear consultores para ayudarle a identificar controles técnicos apropiados para los riesgos específicos que haya identificado. Esto es cierto siempre y cuando los consultores no tengan interés financiero en cualquier solución que podrían recomendar y entienden completamente y pueden ayudarle a aplicar las dos medidas clave de rentabilidad de la inversión (ROI) y el coste total de la propiedad (TCO) en cualquier solución que propongan.


image
not
available

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.


image
not
available


image
not
available

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.


image
not
available

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.


image
not
available

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.


image
not
available

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.