EL VALOR DE NEGOCIO DE ISO 27K – UN CASO DE ESTUDIO

Por Gary Hinson, CEO de IsecT Ltd

Traducido por: iso27000.es

SUMARIO

Este caso de estudio toma en consideración a una empresa que presta servicios TIC y que ha implantado ISO/IEC 27002:2005, código de buenas prácticas para la Gestión de la Seguridad de la Información, y que fue certificada en ISO/IEC 27001:2005, especificaciones de un Sistema de Gestión de la Seguridad de la Información, obteniendo como resultado ventajas significativas para el negocio. El caso desvela algunas relaciones sorprendentes entre la gestión de la seguridad de la información y la gestión general de negocio y muchos beneficios indirectos de negocio que raramente suelen mencionarse.

INTRODUCCIÓN

ESTE CASO DE ESTUDIO

Este caso se deriva de la presentación que el Director General de la empresa ficticia "ServiceCo", una compañía de servicios TIC, realizó a una audiencia compuesta por especialistas en seguridad de la información y de auditorías TI. El DG fue el único ponente (estaba programada la intervención del CIO responsable de la seguridad de la información pero no fue posible finalmente y en el último momento). El DG explicó su satisfacción de poder hablar sobre esta materia dada la ilusión por los resultados de negocio generados en la compañía aportados por la seguridad de la información.

SITUACIÓN DE NEGOCIO DE SERVICECO

ServiceCo proporciona servicios TIC, hardware y software a sus clientes. Una vez ganada la certificación en ISO 9001 hace ya 10 años aproximadamente, los empleados se acostumbraron a trabajar de un modo adecuado y en relación a los procedimientos de calidad documentados y a las guías establecidas. Hace un par de años, sin embargo, el ambiente laboral empezó a cambiar de forma negativa. Las decisiones de la Gerencia fueron acometidas de manera instintiva y con poca base de análisis en datos reales mayoritariamente. Con una rotación de la plantilla en aumento, la Gerencia reconoció la necesidad de aplicar cambios y acometer un análisis serio de las debilidades y fortalezas de la organización.

La Gerencia de ServiceCo decidió implantar un ISO27k (que implica tanto ISO/IEC 27001 como 27002). Según las palabras del Gerente de ServiceCo, "la implantación de ISO27k tenía sentido en el negocio. La seguridad en la información interna de ServiceCo reduciría el riesgo y, en consecuencia, el coste relacionado con infracciones serias. ISO27k es un conocido marco de seguridad desarrollado originalmente por algunas de las compañías líderes a nivel internacional (BT, HSBC, Shell international y Unilever, entre otras), por tanto nos proporcionaría los medios para implantar los controles de seguridad según las mejores prácticas.".

BENEFICIOS DE NEGOCIO DE ISO27K

El DG manifestó “ISO27k no es únicamente seguridad de la información o TIC, actualmente ayuda a la organización a ahorrar y a ganar dinero.”. Indicó asimismo los siguientes beneficios directos e indirectos de ISO27k en ServiceCo.

BENEFICIOS DIRECTOS

Aumento de la fiabilidad y seguridad de los sistemas: “Como ocurre en cualquier otro negocio, ServiceCo depende de sus sistemas de información. ISO27k ha garantizado que nosotros tengamos ahora establecidos controles que mantienen la disponibilidad de los sistemas y que reducen el riesgo de que las vulnerabilidades puedan ser aprovechadas. Las visitas de seguimiento tras la certificación y las auditorías de recertificación en ISO/IEC 27001 aseguran que la organización se mantiene actualizada en relación a las más recientes vulnerabilidades y mejoras prácticas.”.

Aumento de beneficios: “Las ventas y los márgenes han aumentado y las percepciones de los clientes sobre nuestro negocio han mejorado. Nuestro certificado en ISO/IEC 27001 demuestra que somos de confianza en relación a garantizar los datos de nuestros clientes, además de los nuestros propios. Nuestros clientes no sólo comprenden que nuestra inversión en ISO27k les aporta beneficios sino que además están preparados para gastar una pequeña diferencia a favor de una infraestructura TI segura. Desde la obtención de la certificación ISO/IEC 27001, hemos visto un incremento importante en nuestra línea base de beneficios y algunos nuevos clientes nos indican que prefieren mantener relaciones con compañías que disponen de una certificación en seguridad reconocida. Adicionalmente, estamos viendo más invitaciones a presentación de ofertas desde empresas que incorporan ISO/IEC 27001 como uno de los prerrequisitos de la lista a cumplir. Y, por cierto, nuestros empleados están desperdiciando menos tiempo en Internet navegando por sitios no relevantes para su trabajo.

Seguridad de la información rentable y consistente: “Hemos implantado medidas de seguridad rentables y adaptadas a las necesidades de nuestro negocio. ServiceCo tenía muchas protecciones técnicas desplegadas por toda la organización pero la valoración del riesgo descubrió que algunas de nuestras protecciones ofrecían poco o ningún beneficio y proporcionarían un mejor retorno de la inversión si fueran reconfiguradas para proteger aquellos activos que requerían un nivel más alto de protección. Todas las divisiones y departamentos en ServiceCo habían desarrollado previamente sus propias guías de seguridad. ISO27k nos ayudó a desarrollar un enfoque consistente de la seguridad mediante la creación de políticas uniformes que incorporasen las mejores prácticas de la industria. Donde ha sido necesario, el cumplimiento de las políticas por parte de los empleados se sustenta con un proceso disciplinario de refuerzo.

Racionalización de los sistemas: “El análisis adecuado de nuestra información y los requisitos de la seguridad de la información indican que gastamos nuestro dinero de un modo prudente. Fuimos capaces de eliminar el 50% de nuestros sistemas y datos cuando fuimos conscientes que no aportaban valor y actualmente hemos reducido los controles aplicados en algunos sistemas de riesgo bajo.”.

Cumplimiento con la legislación: “Implantar ISO27k nos forzó a cumplir con la legislación de UK en áreas como la protección de datos y derechos de autor del software.”.

BENEFICIOS INDIRECTOS

Mejora en el Control de la Gerencia: “Los Gerentes disponen de un mayor control sobre la organización y una mejor calidad de la información con la que gestionarla. El esfuerzo de la Gerencia ha sido por tanto reducida.”.

Mejora en las relaciones humanas: “Políticas, procedimientos y guías claras facilitan las cosas a nuestro empleados; la atmosfera ha mejorado y se ha reducido el cambio negativo iniciado por la plantilla. ISO27k ha diferenciado ServiceCo de nuestros competidores y ha proporcionado a la compañía de una marca única para la venta y que ha llevado a la compañía a un mejor entorno de trabajo para toda nuestra plantilla. Los empleados reconocen ahora que su ganancia del potencial depende de cómo los clientes perciben la marca de la compañía y que cualquier publicidad negativa podría afectarles. El nivel de profesionalidad ha mejorado en todas la compañía. Dado que gran parte de la seguridad se basa en los controles internos, necesitamos comprobar con mayor detenimiento a quién vamos a emplear. Mediante ISO27k introdujimos procesos de contratación más completos con

el objeto de reducir el riesgo de contratar personal no adecuado al puesto o que potencialmente podría poner nuestro negocio en riesgo. Ahora sí sabemos quien trabaja con nosotros!".

Mejora en la gestión del riesgo y planes de contingencia: "Mediante el proceso de certificación en ISO/IEC 27001, ServiceCo identificó sus vulnerabilidades, amenazas e impactos potenciales al negocio. Como resultado de esta actividad y mediante la implantación de controles de ISO/IEC 27002, ServiceCo ahora dispone de un enfoque más estructurado de gestión de riesgos. Por ejemplo, nosotros disponemos ahora de un proceso racional para decidir qué riesgos transferir a nuestras aseguradoras. También disponemos de un plan de continuidad de negocio que comprende todo el negocio, no sólo al departamento TI. La evaluación de riesgos identificó los activos de información que son críticos para el éxito del negocio. Esto nos ha habilitado para producir un plan de continuidad de negocio que ha priorizado estos activos y reduce nuestro potencial exposición a pérdidas financieras o publicidad negativa.".

Mayor confianza de clientes y de socios comerciales: "Con el aumento de la sensibilidad a las brechas de seguridad, los socios comerciales, clientes y vendedores buscaban evidencias de seguridad. La certificación en ISO/IEC 27001 nos ha proporcionado esta garantía. En cualquier industria debes de permanecer en una posición destacada en relación a tus competidores. Convertirse en el primer Reventa TI con Valor Agregado del mundo en obtener ISO/IEC 27001 es un hecho destacado y único que siempre estará ligado a ServiceCo. Disponer de logos ISO/IEC 27001 dentro de nuestra información corporativa es un recordatorio constante a los clientes potenciales y los ya existentes de que somos una organización profesional que gestiona y considera la confidencialidad, integridad y disponibilidad de su información, así como de la nuestra propia, de forma seria.".

COSTES ISO27K

"En contra de lo que se dice habitualmente, los costes de implantación de ISO27k son muy modestos. El mayor elemento de coste fue el miedo al cambio cultural (tuvimos que permitir que un par de nuestros empleados "se marcharan" por no cumplir con nuestras políticas y procedimientos). Las revisiones regulares de cumplimiento para mantener nuestra certificación sólo nos suponen sobre 3.000 libras esterlinas (aprox. 3.500 EUR) al año, por tanto, el ISO27k es muy rentable. Estamos ahora en conversaciones con nuestros asesores sobre la posibilidad de combinar las auditorías de ISO/IEC 27001 y de ISO 9001 para ahorrar tiempo y dinero.".

PARA MÁS INFORMACIÓN

Para encontrar más sobre el valor de negocio de la familia de estándares ISO/IEC 27000, por favor visite www.iso27001security.com. El caso de negocio genérico "Las implicaciones financieras de implantar ISO 27001 & ISO27002: un modelo de rentabilidad genérico" incorpora y extiende las ideas de este caso de estudio y supone una buena base para una propuesta de inversión. Otros documentos disponibles en el website describen los procesos de implantación y certificación y describen posibles métricas.