HISTORIA DE UNA CERTIFICACION BS 7799-2

Un relato personal del Dr. David Brewer, presidente de Gamma Secure Systems Limited

El objetivo de este artículo es la narración del proceso de certificación de Gamma en BS 7799-2, con la intención de que otras organizaciones, en particular las pequeñas como Gamma, puedan sacar provecho de nuestras experiencias.

Mi historia comienza unos dos años atrás, en el momento en que Gamma decidió que debía ampliar el alcance de su sistema de control interno (SCI) para adoptar la norma BS 7799-2:2000. Recuerdo la fecha con precisión: 12 de septiembre de 2002. Presidía una reunión directiva de revisión interna y debatíamos sobre una revisión recientemente finalizada de nuestros procedimientos de seguridad. Acordamos la necesidad de completar en primer lugar la transición del SCI de ISO 9001:1994 a ISO 9001:2000, lo cual logramos posteriormente en Noviembre de 2002.

La seguridad de la información no es algo que sea nuevo para Gamma. De hecho, es nuestro sustento, debido a que somos consultores en seguridad de la información; ha sido siempre una parte integral de nuestro SCI desde el inicio de la empresa en 1988 y somos algunos de los colaboradores principales en el desarrollo del estándar. Sin embargo, cualquier esperanza de ir a por la certificación en otoño de 2003 quedó rota con la llegada de un

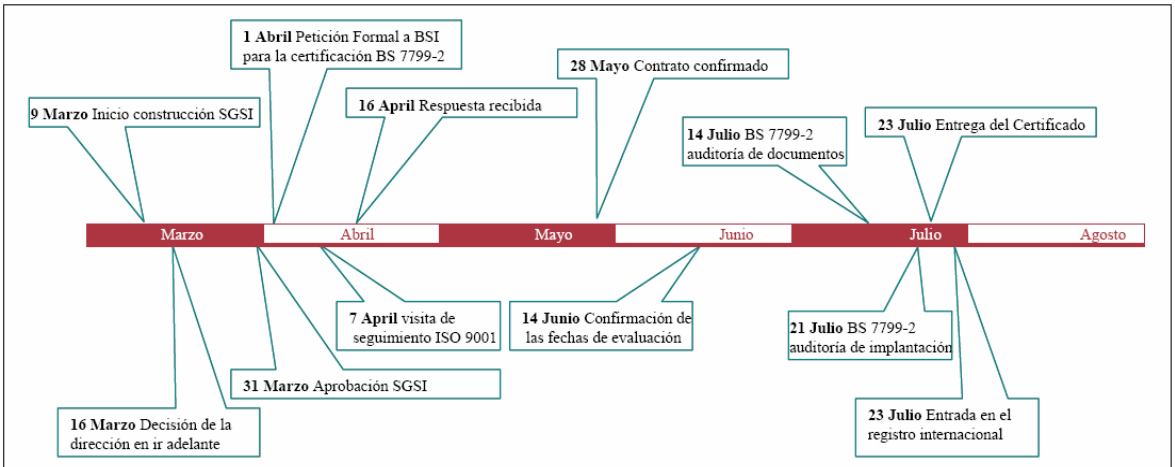

Figura 1: Hitos Principales

número de compromisos inesperados que me llevaron a mí, en particular, a salir del Reino Unido por varios meses seguidos. La primera oportunidad que tuvimos para reestablecer nuestro objetivo fue el 5 de marzo de 2004. Relataré a continuación los acontecimientos desde aquel día hasta la entrega de nuestro certificado en BS 7799-2.

LA DECISION

El 5 de Marzo, durante la comida, mi codirector, Mike Nash, me preguntó cuánto tiempo llevaría ampliar nuestro sistema de gestión basado en tecnología web para cubrir BS 7799-2. Yo imaginaba que unos pocos días pero, antes de ofrecer cualquier promesa o compromiso aparentemente desmesurado, contesté que vería cuánto tiempo llevaría completar la SOA [N. del T.: Statement of Applicability - Declaración de Aplicabilidad].

Normalmente, yo no comenzaría con la SOA pero, en calidad de director y fundador de la empresa, tengo un profundo conocimiento de sus riesgos y del tratamiento de los mismos. También dispongo de un íntimo conocimiento de nuestro sistema de gestión y de los controles existentes. Por ser uno de los autores de BS 7799-2, también sabía que existen 127 controles catalogados en BS 7799-2 y que, al ritmo de un minuto por cada uno, me llevaría 2 horas. Esta es, posiblemente, una de las actividades que más tiempo requiere durante el establecimiento de un SGSI. Por supuesto, el manual con el esqueleto de un SGSI que Gamma utiliza para crear el SGSI de sus clientes [1] me daría ventaja.

Inicié el trabajo el 9 de Marzo, dedicando la primera parte de la mañana a integrar el esqueleto del SGSI en una copia del sistema de gestión actual de Gamma. Para última hora del día siguiente, la SOA estaba lista para una revisión formal, con excepción de algunos hipervínculos que tendrían que ser añadidos más tarde. Es importante entender que, como consultora en seguridad que practica lo que predica, todos los controles de seguridad estaban en su sitio y documentados. Al completar la SOA, lo único que necesitaba saber era qué controles había y dónde estaban documentados. Había necesitado un promedio de unos 6 minutos por control.

Mike repasó la SOA el 12 de marzo y, tras unas modificaciones menores, la consideró apta para el propósito. El Esqueleto había hecho su trabajo y la parte más difícil del desarrollo del SGSI de Gamma estaba superada.

Nuestra siguiente auditoría de seguimiento de ISO 9001 estaba prevista para el 7 de Abril. Mike insistía especialmente en tener nuestro SGSI preparado para enton-

ces, y con preparado quería decir: finalizado, aprobado y operativo. Una vez completada la SOA, ni Mike ni yo teníamos ninguna reserva sobre la consecución de este objetivo. Comprometimos formalmente los recursos en la reunión de revisión del sistema por parte de la Dirección el 16 de Marzo y fijamos el 2 de Abril como fecha final para la terminación.

COMPLETANDO EL SGSI

Ahora que disponía de la aprobación de la dirección, podría completar y autorizar los cambios requeridos, meter el proyecto dentro de la "lista de tareas" e integrar adecuadamente la SOA dentro del sistema de desarrollo. Comencé el 22 de Marzo. Todos los cambios estaban completados y aprobados para el 31 de Marzo. El esfuerzo total que supuso, incluyendo el trabajo en la SOA, fue únicamente de seis días - prueba del duro trabajo de nuestra plantilla a lo largo de años en el establecimiento del Sistema de Gestión de la Calidad inicial en 1994, de nuestro reciente trabajo de conversión a un sistema basado en tecnología web y del desarrollo del Manual con el Esqueleto de un SGSI. Se proporciona una descripción completa del SCI en [2].

NEGOCIACION DEL CONTRATO

El siguiente paso era negociar el contrato para la certificación. Nuestro objetivo era un sistema de gestión, una auditoría, pero dos normas - ISO 9001 y BS 7799-2. Me puse en contacto con nuestra entidad de certificación, BSI, por correo electrónico, el 1 de Abril. Resaltamos nuestro nuevo sistema de gestión durante la visita de seguimiento de ISO 9001 y contamos con la ayuda de nuestro auditor en la obtención de una respuesta positiva. Recibimos un presupuesto el 16 de Abril, pero suponía que solamente íbamos a por la certificación en BS 7799-2 y no consideraba nuestra certificación en ISO 9001. Volvimos a llamar la atención de BSI sobre nuestro requisito (un sistema de gestión, una auditoría, pero dos normas). BSI se disculpó profusamente por el malentendido y recibimos un presupuesto aceptable el 28 de Mayo, que confirmamos por nuestra parte.

Estábamos ya en condiciones de fijar las fechas para la auditoría. Las más cercanas que BSI podía ofrecer eran el 14 y 21 de julio. Accedimos a su propuesta.

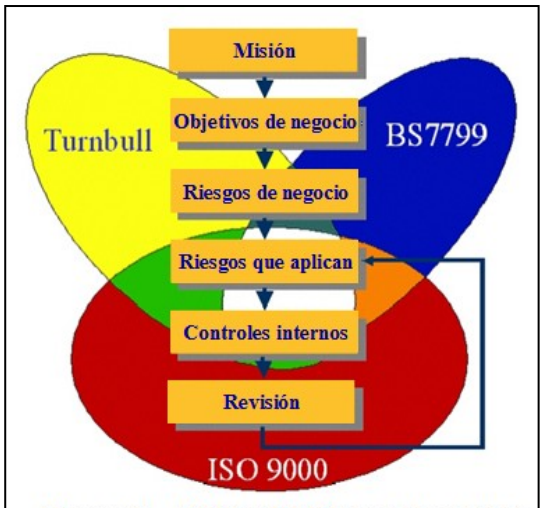

Figura 2 – SGSI y SGQ son sólo partes del sistema general de control interno

1ª VISITA DE CERTIFICACION

Daba la sensación de haber transcurrido mucho tiempo desde que me había puesto por primera vez en contacto con BSI, 3 meses y medio para ser exacto, pero por fin llegó el día. Tuvimos un inicio gracioso cuando BSI llamó para decir que nuestro nuevo auditor se había perdido y no podía encontrar la oficina. Mike le telefoneó y le proporcionó instrucciones. Al rato estábamos todos juntos tomando una taza de café y la auditoría de media jornada para la revisión de la documentación se puso en marcha. ¡Se supo que la persona en BSI responsable de programar las auditorías había dado a nuestro auditor una dirección incorrecta!

Primeras impresiones

Mi primera impresión fue que estaba tratando con un auditor sumamente competente tanto en BS 7799-2 como en ISO 9001. Esto empezaba a poner cómodamente a nuestro alcance la consecución de nuestro objetivo de "una auditoría, dos normas".

El objetivo de la auditoría de revisión de documentación es el de confirmar que el sistema de gestión, tal y como está documentado, está conforme con el estándar. Mi labor era la de guiar al auditor por el sistema de gestión. Al ser un sistema de gestión integrado, pasaríamos de forma natural de un estándar al otro durante la navegación a través del sistema.

A un solo clic de distancia

Al ser un sistema basado en tecnología web, la navegación por el manual SGSI se realiza pulsando sobre los enlaces de hipertexto. En una secuencia concreta, mostré cómo las observaciones de las auditorías internas, las acciones de la revisión del sistema por parte de la dirección, las entradas de la “lista de tareas”, los formularios de petición de cambios y los registros de control de documentos encajaban adecuadamente unos con otros. En el breve espacio de unos pocos minutos, había demostrado cómo nuestro sistema de gestión reunía aproximadamente el 50% de los requisitos de BS 7799-2. El auditor me realizó una nueva pregunta. Pulsé el hipervínculo. La respuesta apareció en una nota a pie de página de la ventana (ver [1]). Mike observó con regocijo la sonrisa del auditor.

De hecho, prácticamente todo lo que consultábamos estaba accesible inmediatamente en la pantalla de mi ordenador.

El único registro en papel que miramos fue mi archivo de correo con BSI en relación a nuestra certificación original de ISO 9001:1994.

Evaluación de riesgos

Miramos detalladamente la evaluación de riesgos. Como el sistema de gestión cubre todo nuestro sistema de control interno, la evaluación de riesgos sigue la “Guía del Comité de Prácticas de Auditoría del Reino Unido [3]” y

comienza con la declaración de la misión de la empresa y objetivos de negocio (véase Figura 2). Se realiza mediante un análisis de eventos e impactos (ver [4]), a partir de los cuales se *derivan* los activos y las amenazas. Las vulnerabilidades son tratadas sobre la marcha mediante la realización de planes para el tratamiento del riesgo. Este enfoque no sorprendió a nuestro auditor. Me dijo que varios de sus clientes habían descubierto que era mejor comenzar con los eventos e impactos y que comprendía claramente que tenía sentido para la buena gestión del negocio hacerlo así.

Documentación

Revisando nuestra Política del Sistema de Gestión (que es nuestra implantación del requisito de BS 7799-2 de disponer de una política del SGSI), nuestro auditor se fijó en nuestra declaración de política de documentación, donde establecemos las reglas sobre lo que debe estar documentado y lo que no necesita estarlo. Esto condujo a una interesante conversación sobre la cultura, donde el auditor indicó que, en algunas organizaciones, procedimientos que deben seguirse por muchas personas no están documentados, pero que, aún así, cada persona continúa sabiendo qué es lo que tiene hacer. Indiqué que, al menos, uno debía documentar, p. ej. en la SOA, el hecho de que el procedimiento es parte de la cultura de la organización, pero que se puede auditar. "*Sí*", dijo nuestro auditor, "*pregunte a una selección de personas en qué consiste el procedimiento y, si todas ellas dan una respuesta correcta, existe una buena evidencia para demostrar que todos ellos lo están siguiendo.*"

¿Por qué se hace esto así?

En respuesta a otra pregunta, Mike contestó, "*Por razones históricas*.". Claramente, fue la respuesta correcta. La pregunta que el auditor estaba haciendo en realidad era "*¿sabe por qué hace usted esto de esta forma?*"

SOA

Después de aproximadamente dos horas, habíamos dado un buen repaso a la evaluación de riesgos y a todos los procesos de gestión. Sólo faltaba la SOA.

Una vez que había demostrado cómo funcionaba, con sus hipervínculos hacia atrás, hasta los planes de tratamiento del riesgo y declaración de políticas aplicables, y hacia delante, hasta los procedimientos documentados (ver [1], [2]), lo repasamos rápidamente desde el inicio hasta el final. El auditor se interesó en particular en los controles que habíamos marcado como no-aplicables. Para cada uno de ellos, realizó una diversidad de preguntas perspicaces, quedando satisfecho con nuestras respuestas.

Obviamente, nuestro auditor contaba con que algunos controles figuraran sin excepción, como los de continuidad de negocio, y, efectivamente, allí estaban.

Finalmente, comprobamos una selección de procedimientos. Aquí fui capaz de mostrarle el control de cambios y el histórico de aprobaciones, así como varias referencias cruzadas adicionales a las acciones de revisión y auditoría del sistema de gestión.

Conclusión

La auditoría de la documentación finalizó sobre las 12:30. Habíamos repasado el sistema de gestión completo en relación a la conformidad con el estándar y, en su transcurso, se habían descubierto muchas evidencias de la implantación (el objetivo real de la segunda auditoría), tales como las auditorías internas y las revisiones del sistema de gestión.

Desde luego, no todas las auditorías de la documentación discurren así de apacibles. Nosotros conocemos BS 7799-2 a fondo, lo que significa que el auditor tuvo que dar pocas explicaciones y nuestros procedimientos de gestión estaban bien establecidos, documentados con precisión y ya certificados para la gestión de la calidad.

2ª VISITA DE CERTIFICACION

La segunda visita de certificación tuvo lugar una semana más tarde. Comenzó puntualmente a las 09:15 (todo el mundo sabía esta vez dónde ir) y se concentró, naturalmente, en la SOA. Esto era terreno conocido para todos nosotros y el tiempo transcurrió rápidamente.

Permanecer tranquilos

Esta evaluación también tuvo un principio divertido, cuando al auditor comenzó pidiendo una impresión en papel de la SOA. No resultó ser sencillo. El ordenador desde el cual controlaba el sistema de gestión parecía ser capaz de imprimir todo lo que le pedía excepto el sistema de gestión -todavía no sé por qué; posteriormente, fui incapaz de reproducir el problema-. Finalmente, decidí lanzar la impresión desde mi ordenador portátil. Después de lo que parecieron ser diez minutos, pero probablemente fueron sólo unos pocos segundos, la impresora se puso en marcha y sacó la impresión esperada. "*¿Por qué quiere usted una impresión de un documento electrónico?*", indagué con una sonrisa. "*¡Ah!*", contestó el auditor, reparando en la parte divertida de su petición. Obviamente, la impresión de documentos electrónicos no era el tipo de actividad de la que nos ocupáramos con regularidad.

De hecho, cuando terminábamos de examinar cada punto, él lo tachaba sobre su copia impresa como recordatorio y evidencia de que cada una de las secciones había sido cubierta.

Número de versión

Su siguiente pregunta fue "*¿Cuál es el número de versión de la SOA?*" BSI necesita este dato para el certificado, lo cual es un fastidio, ya que implica que la SOA debe ser necesariamente un elemento único de configuración y en el sistema de gestión de Gamma cada página web es un elemento independiente. Por casualidad, todas ellas, salvo la página índice, tenían idéntico número de versión, así que tomamos éste.

A largo plazo, voy tener que encontrar alguna solución más elegante que permita una revisión y mejora continua, pero que disponga de un número de versión fijo para mantener contenta a la certificación.

Proceso de auditoría

Comenzando por la sección de política de seguridad, el auditor seleccionaría un número de controles, nos haría varias preguntas sobre su implantación, para seguir entonces adelante con la siguiente sección de la SOA.

Tendía a contestar las preguntas reforzando lo que estaba escrito en la SOA y utilizando los hipervínculos para proporcionar evidencias de apoyo. Recuerde, esto era una auditoría de implantación y, por lo tanto, el auditor busca pruebas de que los controles, así como otros componentes del sistema de gestión, hayan sido implantados.

Figura 3 – Certificados Gamma ISO 9001 y BS 7799-2

Registros

A menudo el auditor preguntaba qué registros mantenía. La respuesta a esta pregunta, en el contexto de los procesos de gestión, fue directa, ya que están todos, salvo el registro de incidentes, en el manual electrónico (y por tanto a un solo clic de distancia). Las preguntas más significativas del auditor, en mi opinión, concernían a los controles. Por ejemplo, en los controles relacionados con el control de accesos, preguntó "*¿Qué registros mantiene usted?*". Mi respuesta fue decir "*Aquí está la política*", pulsando sobre el hipervínculo que descubría la política aplicable de control de accesos, "*y la evidencia de su puesta en práctica está en este ordenador*", señalando a mi ordenador portátil. "*Echemos un vistazo.*" Me enseñaron hace mucho tiempo que el control de acceso en un ordenador se rige por lo que contienen sus tablas internas, no lo que un gerente dice que debería ser – así que el registro es lo que está en el ordenador. Di respuestas similares a sus preguntas acerca de los registros de cortafuegos y antivirus.

Era el enfoque tradicional de auditoría. El auditor hacía preguntas aparentemente inocentes sobre cómo funcionaba la tecnología, por ej. "actualización directa" y una vez comprobado que yo conocía la respuesta, continuaba adelante con otro asunto. Exactamente del mismo modo que en una auditoría de ISO 9001.

Un comentario que haría en esta etapa concierne al consejo dado en el Anexo B de BS 7799-2 sobre la comprobación rutinaria. No es una exigencia obligatoria, pero es algo que yo practico con regularidad: conozca cuáles son sus políticas y compruebe con regularidad que son llevadas a cabo por el ordenador.

Métricas

Después de una agradable comida con nuestro auditor, conversando sobre problemas prácticos de interpretación de BS 7799, estábamos en la recta final y a falta de sólo tres secciones de la SOA para la finalización de la auditoría. El auditor había comprobado durante la visita previa y en el transcurso de este día cómo habíamos puesto en práctica muchos otros requisitos de BS 7799-2. Finalmente, llegamos a la última sección de la SOA. Paramos por un momento en el apartado legal, ya que habíamos identificado una serie de leyes aplicables. El punto de interés de la discusión, sin embargo, se centro en el cumplimiento, donde entramos en un útil debate sobre métricas. Las métricas son una exigencia de ISO 9001, pero no de BS 7799-2. Sin embargo, estoy trabajando en ellas usando nuestra "teoría [4] del tiempo" como guía.

La hora final

Acabamos con la SOA aproximadamente a las 14:30. El auditor pasó la siguiente hora completando su informe, que nos presentó después a Mike y a mí de la manera acostumbrada. Era un informe positivo, recomendando la certificación sin restricciones, al no existir ninguna no-conformidad que atender. Una vez tratado este asunto, dedicamos los siguientes veinte minutos a hablar de algunas cuestiones prácticas, que Mike y yo encontramos considerablemente más interesantes, tales como ¿cuándo recibiremos el certificado? y ¿puede ayudarnos BSI con los comunicados de prensa?, además de algunos detalles prácticos adicionales sobre BS 7799 desde el punto de vista de un auditor.

ENTREGA DEL CERTIFICADO

La promesa era de dos semanas, una mejora significativa desde los primeros días de certificación en BS 7799, cuando nos indicaron que podría llevar tres meses. El registro tuvo lugar, de hecho, dos días más tarde, el 23 de julio. BSI se ocupó de nuestra entrada en el Registro Internacional y lo pude ver antes de que el certificado llegara por correo. Buen trabajo por parte de todos.

CONCLUSIONES FINALES

Importancia del control interno

Estoy convencido de que la clave de nuestro éxito reside en dar al sistema de control interno un lugar de privilegio. Su objetivo es ayudarnos a Mike y a mí en la gestión de nuestro negocio, asegurar la calidad de nuestro trabajo y gestionar nuestros riesgos de negocio. Lo usamos a diario. Las auditorías internas y revisiones del sistema de

gestión son parte integrante de nuestra convicción y ejercicio de técnicas de gestión prudentes, tales como el ciclo Deming (Plan-Do-Check-Act). No es algo que resucitemos y limpiemos justo antes de una auditoría, para después guardarlo y olvidarlo hasta la próxima ocasión.

El poder de la tecnología web

Nuestro sistema de gestión es fácil de usar y mantener, al igual que todos los controles internos. No existe burocracia. Nada interrumpe el curso del negocio. Tanto las auditorías internas como externas son muy rápidas, permaneciendo todo a una distancia de tan solo "un clic".

¿Podría haberse hecho más rápido?

Hace tres años, negocié la certificación BS 7799-2 con BSI para los Sistemas de Información de Vodafone en Rattingen, Alemania. Desde el contacto inicial hasta la presentación de la certificación en el Cebit del año 2001 transcurrieron 42 días, así que la respuesta es posiblemente que sí. Si Gamma se hubiera contentado con el tratamiento de ISO 9001 y BS 7799-2 como sistemas de gestión separados, posiblemente podríamos haber ahorrado seis semanas pero, en ese caso, no habríamos logrado nuestro objetivo de "un sistema de gestión, una auditoría, dos normas".

¿Mereció la pena?

Como uno de los autores de la norma, fui inflexible desde el principio en garantizar que las grandes organizaciones no obligasen al cumplimiento del estándar a sus proveedores de menor tamaño sin haber logrado el estándar ellos mismos en primer lugar. Junto a mis colegas del BDD/2 (el comité de BSI responsable de BS 7799-2 en aquel momento) presionamos vehementemente para lograrlo y sentí una gran satisfacción cuando el responsable de Administraciones Públicas del Reino Unido ordenó a todos los departamentos gubernamentales tener incorporada BS 7799 para finales del año 2000. Liderazgo desde lo más alto. Siempre menciono este hecho en los distintos seminarios y cursos de formación que he impartido sobre el estándar por todo el mundo. Refuerzo mis comentarios señalando la necesidad del compromiso y aprobación del estándar por parte de la dirección. Tiene mucho sentido seguir esta misma práctica y disponer de nuestro propio SGSI y ser una parte integral de su dirección y administración.

Algunas personas dirán que la certificación en BS 7799 para una organización del tamaño de Gamma resulta excesiva. Mi respuesta es preguntar siempre cómo puede usted confiar en un consultor de BS 7799 que no puede demostrar que él o ella cumplen sus requisitos para ellos mismos. Una cosa es haber ayudado a escribir el estándar y haber ayudado a otros a ponerlo en práctica; pero otra muy distinta es usar, mantener y mejorar tu propio SGSI a diario. En los servicios de consultoría que proporcionamos, podemos de verdad decir que "estuvimos allí, lo hicimos, escribimos el libro…". En definitiva, tenemos nuestras propias historias de certificación que contar.

REFERENCIAS

[1] “Fast Track ISMS Certification”, Brewer, D.F.C., List, W., Agosto 2004, www.gammassl.co.uk/topics/ics/FTISMS.pdf

[2] “A description of Gamma’s internal control system”, www.gammassl.co.uk/topics/ics/gamma.html

[3] “Briefing paper - Providing Assurance on the effectiveness of Internal Control” publicado por el Comité de Prácticas de Auditoría en Julio de 2001, www.apb.org.uk.Copias disponibles de ABG Professional Information

[4] “Measuring the effectiveness of an internal control system”, Brewer, D.F.C., List, W., Marzo de 2004, www.gammassl.co.uk/topics/time/RTPs.html

Traducción de "A tale of BS 7799-2 certification" (http://www.gammassl.co.uk/topics/ics/Certification%20v02.pdf). Realizada por Agustín López Neira (www.iso27000.es).