Implantando ISO17799: ¿Placer o Dolor?

Por Carl Thorp, CISM, CISSP

Con sistemas dispares, información y amenazas emergentes impactando en las organizaciones desde todos los ángulos y con muchos sistemas de seguridad heredados incapaces de afrontar tales ataques, puede que las organizaciones estén lejos de encontrarse a salvo.

Hoy es casi imposible evitar el leer acerca de riesgos en las tecnologías de la información y comunicaciones, evaluación de riesgos, análisis de riesgos, comunicación de riesgos, gestión de riesgos, concienciación del riesgo, asunción de riesgos, buen gobierno y aversión por el riesgo. Los medios, Internet y, prácticamente, cada foro comercial, industrial o gubernamental se hacen eco de estos temas.

Esta atención creciente no ha producido aún estándares y guías de seguridad universalmente consensuados. A pesar de las numerosas recomendaciones de organizaciones gubernamentales y asociaciones profesionales, no existe un lenguaje común para la medida y gestión de los riesgos de seguridad de la información, ni hay métricas formalmente establecidas para evaluar el rendimiento de la gestión del riesgo.

No obstante, a pesar de lo dicho, ISO/IEC17799 es un estándar de seguridad ampliamente seguido que proporciona una buena guía y un marco útil dentro del cual construir un sistema de seguridad de la información.

Dicho en dos palabras, ISO17799, o la más familiar BS7799, es la documentación de procesos y procedimientos rigurosos que ayudarán a garantizar la seguridad de la información en toda una organización. En cita textual de British Standards, "el establecimiento de un sistema de gestión es fundamental para la correcta gestión de cualquier cosa".

Para asegurar una gestión efectiva de la información en una organización, al menos tienen que estar implantados controles en las tres áreas siguientes:

- Confidencialidad: Implementación de controles, p. ej., contraseñas, biometría o una simple cerradura, para prevenir el acceso no autorizado a información confidencial.
- Integridad: Garantía de que la información es exacta y completa, sea durante su almacenamiento, proceso o transmisión. Ejemplos son dos personas revisando mutuamente sus entradas de datos o el uso de sumas de comprobación [*checksums*].
- Disponibilidad: Asegurar que la información está disponible para el personal autorizado cuando y donde quiera. Esto lo puede facilitar el uso de equipos de sustitución en caliente o en frío, *backups*, almacenamiento externo, recuperación de desastres, planes de contingencia, etc.

El sistema de gestión de seguridad de la información (SGSI) de una organización refleja el enfoque y evaluación del nivel de riesgo/confidencialidad que da a su información y su asignación de prioridades de personal y recursos.

Inconvenientes percibidos o ideas preconcebidas

Los inconvenientes percibidos para implantar ISO17799 incluyen:

- El tiempo requerido para documentar aparta de las tareas a realizar.
- Documentar aburre; sacar trabajo adelante es "divertido".
- No es más que una pesadilla; implica política y tratar con las cuestiones emocionales de seres humanos.
- Será necesario quitar valiosos recursos de "apaga-fuegos".

Ventajas observadas

Las ventajas observadas de implementar ISO17799 incluyen:

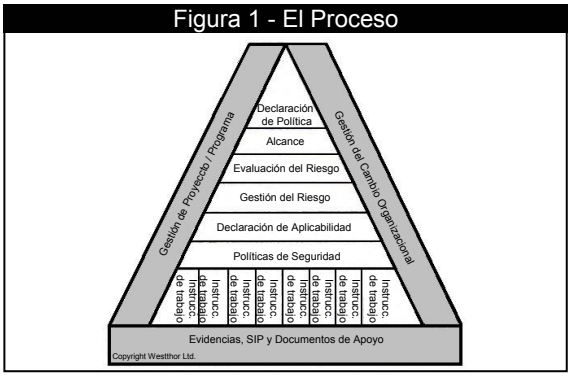
- Un acceso rápido a la información requiere una documentación clara y un enfoque coherente en las tareas.
- Inculca disciplinas tales como la gestión del riesgo y el mantenimiento de registros, que pueden convertirse en ventajas.
- El ser humano trabaja de forma natural más eficientemente en un marco ordenado y estructurado, al reducirse las suposiciones y la duplicación de esfuerzos y facilitarse el intercambio de información.
- Proporciona herramientas y métodos para que la gerencia y los usuarios compartan una parte de la responsabilidad sobre sus acciones.
- Aporta la base para defender el uso de buenas prácticas.

Consejos principales

Así pues, ¿es dolor o placer? Dolor suele ser la respuesta cuando uno considera que los sistemas de control pueden engendrar burócratas y que el papeleo puede servir de excusa para no acabar las tareas. No obstante, el dolor se puede minimizar y se pueden obtener claros beneficios siguiendo cuidadosamente los estándares ISO17799 con algunas simples recomendaciones:

1) Simplifique. A no ser que se esté implantando ISO17799 en un entorno pequeño y compacto, es poco probable que uno consiga la certificación si toda la organización se incluye en el alcance a la primera. Mantenga el alcance reducido y ajustado; incluya sólo controles que necesite (sin olvidarse de justificar por qué los demás se han quedado fuera). Restrinja el alcance a una unidad manejable, es decir, un solo centro de datos, un área donde el personal debería tener al menos algo de comprensión por la necesidad de seguridad. Una vez que se ha tenido éxito aquí, debería ser posible mostrar beneficios probados, lo que ayudará a extenderlo a otras áreas en fases controladas.
2) Comprenda el proceso. Muchos proyectos progresan con dificultad porque la decisión de implementar ISO17799 se toma sin comprender totalmente la cuestión. No se meta de lleno y empiece a tratar los temas técnicos. El director del proyecto quedará rápidamente sobrecargado con la enormidad del problema. Comprenda la estructura; comience por arriba y siga el flujo hacia abajo en una secuencia lógica y bien pensada (véase **Figura 1**). Aprenda de los errores de otros, asista a cursos de formación, pregunte en su sector de actividad, hable con consultores experimentados (pero no se deje controlar por ellos), fíjese en buenos y malos ejemplos de implantaciones de SGSIs, analice cualquier lección aprendida e impleméntela.
3) Dirección de proyecto. Este es un proyecto como otro cualquiera, así que concéntrese en controles adecuados de dirección de proyectos. Se necesita un mandato de proyecto que muestre el respaldo de la gerencia. También se necesita un plan de proyecto para establecer metas y entregables. Fije objetivos e hitos que le permitan llevar el proyecto adelante. Sin éstos, seguro que perderá el rumbo y se quedará sin fuelle gradualmente.

Figura 1 - El Proceso



4) Gestión del cambio organizacional (GCO). Con un curso de GCO o de ventas/negociación, la mayoría de las personas de seguridad pueden adquirir destreza en vender los beneficios de ISO17799 y de la seguridad de la información en general. Adicionalmente, hay que asegurarse de convencer a los que disienten y convertirlos en defensores del proyecto. Sin estas habilidades, la seguridad de la información se percibe, en el mejor de los casos, como un mal necesario, o, en el peor, como una carga adicional a evitar. Al menos, asista a un curso de técnicas de auditoría porque, al implementar ISO17799, uno deberá poner en práctica habilidades no asociadas normalmente a una función técnica de "trastienda". Tendrá que dirigir grandes reuniones, entrevistarse con miembros de la gerencia, documentar tareas, efectuar evaluaciones de riesgo, formar personal, superar objeciones y, sobre todo, vender ideas.
5) Comprensión y apoyo de la dirección. Incluso si, inicialmente, se restringe el alcance a un sistema TI, es importante involucrar a la dirección al nivel más alto de la organización. Sin este respaldo, buena voluntad general y autoridad, uno se enfrentará a un muro de excusas y razones para no implementar las buenas prácticas. Es importante implantar ya en las fases iniciales del proyecto un programa de formación continua en seguridad y un comité de gestión de la seguridad.
6) Vaya por la certificación. Muchas organizaciones van sólo a por el cumplimiento. Esto es una zona gris y confusa. ¿Por qué pasar por todo el esfuerzo de implantar un SGSI y no ser capaz de alcanzar el éxito total? Perseguir la certificación proporciona un enfoque mejor, metas más claras y, por tanto, mayores probabilidades de éxito.
7) No reinvente la rueda; aprenda de otros métodos de gestión de la seguridad. Si la certificación es el objetivo, hay que cumplir con ISO17799, pero merece la pena investigar otros estándares y métodos útiles, como los *Control Objectives for Information and related Technology* (COBIT ®) de ISACA, *IT Infrastructure Library* (ITIL) de la *Office of Government Commerce* del Reino Unido, ISF, etc. Éstos pueden traer plantillas hechas de procesos y procedimientos, para cuando se es auditado.
8) Construya sobre lo que ya dispone internamente. Si ya se han implantado estándares tales como ISO9000, utilícelos para crear el marco. Cuanto menos, le ayudará a asegurar si las normas de control de documentación resistirán la certificación.
9) Hable con auditores. Si existe un equipo de auditoría interna, puede que éste tenga ya mucha de la información necesaria para crear un análisis diferencial [*gap analysis*] de controles de seguridad. Puede que incluso esté dispuesto a realizar dicho análisis. Esto puede resultar en ayuda adicional, un punto de vista independiente y ahorro de tiempo, y se podrá tener más confianza en el SGSI, facilitando por tanto futuras auditorías. No obstante, como con todos los consultores y auditores, éstos deberán comprender y estar versados en los estándares que van a ser implantados.
10) Libere recursos. Asuma que ISO17799 será una inversión considerable para la organización. Aísle los recursos necesarios para conseguirlo y no les permita ser distraídos con tareas de "apaga-fuegos". Puede ser necesario devolver personal a tareas operacionales ciertos días de la semana para mantener habilidades técnicas, atender la demanda, etc., pero la plantilla del proyecto debe ser capaz de trabajar tranquila la mayor parte de la semana en implantar ISO17799, o el proyecto fracasará.
11) Pruebe los controles. ¿Para qué sirve un control si no se puede demostrar que realmente funciona? Es necesario recopilar evidencias, mostrando que los controles funcionan desde al menos tres meses antes de intentar la certificación. Hay certificaciones que han fracasado, no porque hubiese nada incorrecto en el SGSI, sino por no existir suficientes evidencias de que el plan de recuperación de desastres había sido probado.

Implantada con éxito, ISO17799 proporciona las herramientas para justificar la necesidad de recursos, priorizar cargas de trabajo y, lo más importante, impulsar las mejoras en gestión de seguridad de la información.

Carl Thorp, CISM, CISSP
lleva dedicándose a la gestión de sistemas de información desde hace 18 años, desempeñando diferentes puestos técnicos y de gestión. En 2001, fundó Westthor Ltd., con el objetivo de desarrollar estrategias que protejan de los riesgos de seguridad de la información y se integren y sean consideradas parte de la gestión general de riesgos de la organización.