La gestión de la seguridad en la empresa:

Introducción

Vivimos en un mundo globalizado y cada vez más competitivo, en el que las empresas se encuentran con nuevos desafíos que hacen necesaria la búsqueda de nuevas vías que les permitan obtener una ventaja sostenible. En el presente artículo pretendemos facilitar algunas de las claves para gestionar la seguridad de la información en la empresa.

Los Sistemas de Gestión de Seguridad de la Información (en adelante SGSI), así como las redes de trabajo de dichas organizaciones, se están viendo afectadas por amenazas de seguridad, ataques y fraudes informáticos, problemas de sabotajes, virus informáticos y otro tipo de contingencias, imprevistos y catástrofes mayores, con el posible riesgo de eliminación y pérdida de información.

La relación entre las tecnologías de la información, la seguridad de las instalaciones, el personal y su *know how,* la protección de la información y los procesos de negocio es cada vez más estrecha. La clave está en que las organizaciones inviertan en aplicar herramientas que mejoren su seguridad, que les permitan proteger y evitar en lo posible que los activos de mayor valor se pierdan ante cualquier eventualidad, y en desarrollar e implementar enfoques y esquemas para el control y gestión de las amenazas presentes y futuras.

Si analizamos las tendencias actuales, y los diferentes esquemas y normas existentes a nivel mundial para gestionar la seguridad de la información en la empresa, podemos ver que existe toda una "sopa de letras y números":

- Referenciales nacionales e internacionales específicos.
- Normas creadas por agentes privados para la protección de datos.

"… como consecuencia de estas situaciones, así como de la vulnerabilidad, dependencia e inestabilidad actual de las organizaciones de sus SGSI, la seguridad de la información es uno de los retos más acuciantes para las empresas…"

de la información
ISO 27001

- UNE 71502
- ISO / IEC 17799
- BS 7799
- BS 15000
- ISO 27001

que crean confusión si no se está verdaderamente apoyado y asesorado por expertos a la hora de poder seleccionar una norma o un sistema, que permita rentabilizar todas sus inversiones en seguridad en términos de infraestructura, consultoría para la implementación, formación continua del personal, mejora tanto del hardware como del software, envío periódico de información a grupos de interés (clientes, proveedores, empleados, accionistas, administración, etc.).

A finales del año 2005 fue publicada oficialmente la norma ISO 27001: "Tecnologías de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos", norma internacional que pretende sustituir a las anteriores y ser líder de los SGSI.

Antecedentes: de los comienzos de la gestión de seguridad de la información hasta la ISO 27001:2005

A primeros de la década de los 90, el Departamento de Comercio e Industria del Reino Unido inició el desarrollo de una norma británica (en adelante BS), para proteger y regular la gestión de la seguridad en la empresa, y como respuesta a las peticiones de la industria, el gobierno y los comerciantes para crear una estructura común de seguridad de la información. La primera norma fue aprobada oficialmente en 1995 (BS 7799:95) y nace como un código de buenas prácticas para la gestión de seguridad de la información.

Cronológicamente a este primer gran hito en la normalización de la gestión de la seguridad de la información le han seguido las siguientes normas y etapas:

- En 1998, tres años después, se publica la norma BS 7799-2, en la que se recogen especificaciones para la gestión de la seguridad de la información y se "lanzan" requerimientos certificables por primera vez.
- En el año 1999, se lanza la segunda edición, en la que se añade "e-commence" al alcance de la norma. En aquella época, la Organización Internacional de Normalización (ISO) comienza a interesarse ya por los trabajos publicados por el Instituto inglés.
- Tras una revisión de ambas partes de la norma, en diciembre del año 2000, ISO aprueba la norma ISO 17799 Parte 1, que es el Código de Práctica para los requisitos

de gestión de seguridad de la información (no certificable). Esta norma está formada por un conjunto completo de controles que conforman las buenas prácticas de seguridad de la información, y que pueden ser aplicadas por toda organización con independencia de su tamaño.

- En el año 2002 se realiza la revisión de la parte 2 —la certificable— de la BS (BS 7799-2:2002), con el fin de armonizarla con otras normas de gestión tales como la ISO 9001:2000 y la ISO 14001:1996, así como con los principios de la Organización para la Cooperación y el Desarrollo Económicos (OCDE).
- Ese mismo año la norma es publicada norma UNE (UNE-EN ISO/IEC 17799/1:2002) sin apenas modificación y se establece exclusivamente en España otra norma, la UNE 71502.
- En el año 2005 se publica la norma ISO 27001, norma certificable y que reemplazará a la actual BS 7799-2.

  Finalmente, cabe señalar dos aspectos también novedosos y muy interesantes, dado que está previsto igualmente la aprobación de la norma ISO 27002, el Código de Práctica que sustituirá a la actual ISO 17799: 2005 y otra norma que ampliará a las existentes (ISO 27004), que establecerá las métricas y medidas del sistema de gestión de la seguridad, buscando su eficiencia. Por lo tanto, en un futuro cercano existirán las Normas 27001-Certificable; 27002-Código de Práctica y 27004-Métricas y Medidas del Sistema de Gestión de la Seguridad.
- Únicamente como referencia complementaria hemos creído interesante incluir a nuestros lectores, algunas de las normas y modelos relacionados con las Tecnologías de la Información, y que existen mundialmente además de la ISO 27001 y que la complementan en función de la organización y del alcance de los procesos de negocio a implantar y, en su caso, certificar:
  - ISO/IEC 15408: Information Technology-security techniques-evaluation criteria.
  - ISO/IEC 12207: Software life cycle processes.
  - ISO/IEC 18045: Methodology for IT security evaluation.
  - ISO/IEC 13569: Banking and related financial services-information security guidelines.
  - ISO/IEC TR 13335: Information technology guidelines for the management of IT security.
  - ISO/IEC TR 15504: Software process assessment.
  - BS ISO/IEC 90003:2004: Software engineering. Guidelines for the application of ISO 9001:2000 to computer software.
  - TickIT V5.0: Using ISO 9001:2000 for software quality management system construction, certification and continual improvement.
  - BS 15000: IT Service Management.

Desglose y análisis de los aspectos más relevantes de la norma ISO 27001

La ISO 27001 proporciona requisitos para un SGSI que permitirán a la organización establecer, implantar, operar, supervisar o en términos de norma "monitorizar", revisar, mantener y mejorar un SGSI documentado en el contexto de la actividad de la organización, teniendo en cuenta sus problemáticas y riesgos de seguridad o de otro tipo, intrínsecos a su negocio. La ISO 27001 se ha creado entre otras cuestiones para garantizar su adecuación y proporcionar controles de seguridad que protejan adecuadamente los activos de la información y proporcionar confianza a los consumidores, clientes y otras partes interesadas.

¿Cuál es la relación existente entre ISO 27001 e ISO/IEC 17799?

ISO 27001 lanza y prepara los requisitos para un SGSI; ISO/IEC 17799 debe ayudar a preparar todo lo concerniente desde un punto de vista de partida para el desarrollo específico de mejoras y pautas aplicables para cada organización y alcance específico del SGSI.

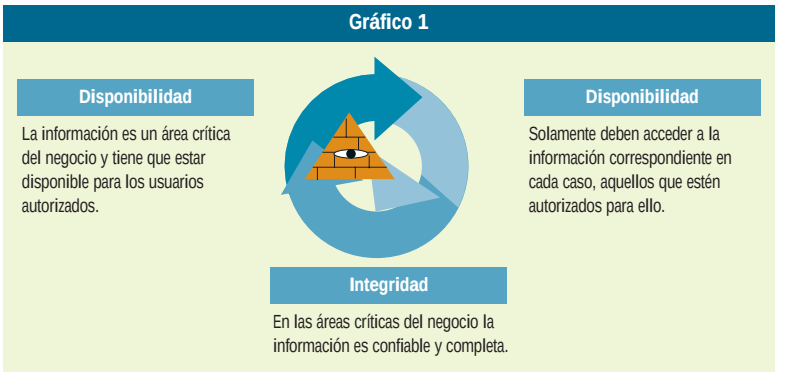
No todos los controles que aparecen documentados en la Guía o Código de Práctica, serán aplicables, y dependerá del tamaño y tipo de organización, complejidad, productos, niveles de competencia de su personal, etc. La guía puntualiza además que las recomendaciones deberán ser elegidas y utilizadas siempre contemplando la legislación reglamentaria aplicable a la organización en función del alcance del SGSI.

SGSI: Tres conceptos básicos

Los tres conceptos básicos o "pilares" de la seguridad de la información son "C-I-D":

- confidencialidad
- integridad y
- disponibilidad

Gráfico 1



El SGSI es la mejor manera de supervisar, controlar, revisar periódicamente el trabajo de la organización en materia de seguridad de la información, proporcionando una dirección de las actividades relacionadas con la seguridad de la información en respuesta a los factores de cambio por agentes internos o externos. Todo individuo dentro de la organización debe aceptar su responsabilidad para mejorar el SGSI.

Compatibilidad con otras normas internacionales

Una de las fortalezas y claves del éxito de la nueva ISO 27001 es que la estructura de la norma está relacionada, construida y documentada, como el resto de las siguientes normas ISO de gestión:

1. Serie ISO 9000, tanto la norma ISO 9001, como las Directrices de mejora del desempeño (9004) como el vocabulario y terminología (ISO 9000).
2. Norma ISO 14001 para Sistemas de Gestión Medioambiental.
3. Norma ISO 19011, que proporciona las guías para auditores de sistemas de calidad y/o medio ambiente.

Con la ISO 27001 y en función del alcance del SGSI, la organización deberá controlar y garantizar igualmente el cumplimiento de las leyes y reglamentaciones aplicables (por ejemplo: medidas de nivel bajo-medio-alto aplicables a la organización establecidos por la Ley Orgánica de Protección de Datos en España).

Mejora continua basada en el ciclo P-D-C-A

Es evidente que la seguridad de la información no se termina en la implementación de un "firewall" o con la contratación de una empresa de seguridad. Es necesario integrar las múltiples iniciativas puestas en ejecución dentro de una estrategia global con el fin de que cada elemento ofrezca un nivel óptimo de protección. Es a este nivel que intervienen los sistemas de gestión de la seguridad de la información permitiendo coordinar los esfuerzos para alcanzar una seguridad óptima *(ver gráfico 2)*.

Un sistema de gestión debe incluir un método de evaluación, medidas de protección y un proceso de documentación y de revisión. Esto último es el principio del Modelo del PDCA (Establecer-Implantar-Monitorizar y Verificar-Actuar, manteniendo y mejorando el SGSI). Este modelo popularizado por W. Edwards Deming (y conocido como el "Ciclo Deming") recuerda fuertemente al modelo de gestión de la calidad ISO 9001 *(ver gráfico 3)*.

- PLAN. En esta fase necesaria para la planificación, definición y el establecimiento del SGSI, es importante considerar el entorno de la actividad de la organización que implementará el Sistema. Se deberían identificar, por ejemplo, directrices corporativas aplicables y requisitos legales. Además de esto, el contexto de la actividad de la organización debería quedar reflejado en las políticas y objetivos de seguridad y se debería considerar al definir el alcance del SGSI. Durante esta fase la organización también diseña un procedimiento formal para la continua identificación y evaluación de riesgos y la selección de los objetivos de control y controles que le permitirán gestionar estos riesgos. Al final de este proceso, la organización prepara la declaración de aplicabilidad.
- DO. Hacer, implementar. Es importante centrarse inicialmente en el desarrollo e implementación de un plan efectivo y a medio y largo plazo para la atenuación de los riesgos. Durante esta fase, los controles

Gráfico 2

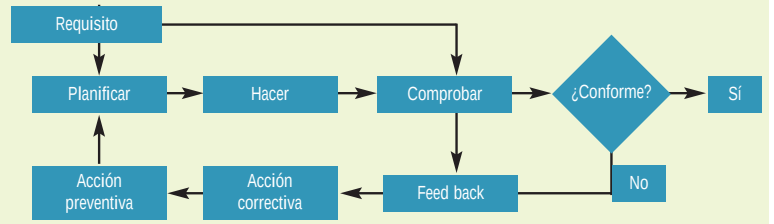
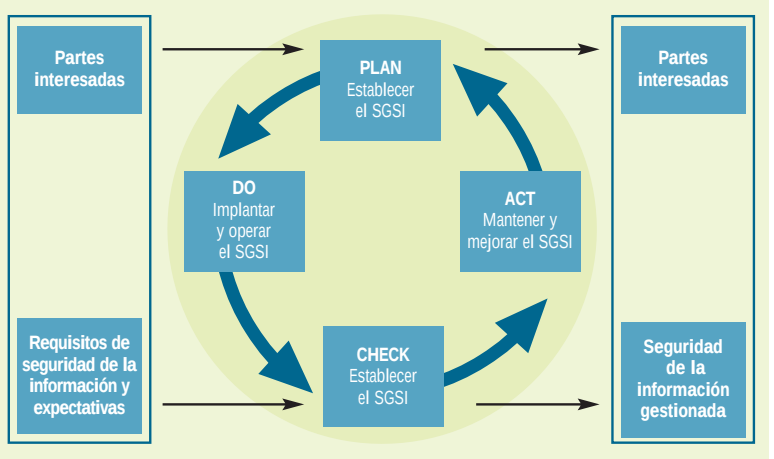


Gráfico 3



seleccionados en la fase de planificación se implementarán para alcanzar los objetivos de control. En esta fase se inicia el Plan de Formación para incrementar la concienciación y conocimiento del personal que garantice la correcta implementación de los controles.

- CHECK. Seguimiento, monitorización y revisión del SGSI. Realización periódica de auditorías internas del SGSI y seguimiento regular de la eficiencia del sistema. La organización también revisa el nivel de los riesgos residuales.
- ACT. Actuar, mantener y mejorar el SGSI. Cuando se han identificado las vulnerabilidades y debilidades, se deben llevar a cabo las medidas correctivas y preventivas apropiadas para mejorar el SGSI, así como las planificaciones temporales de estas mejoras.

¿Cómo crear e implementar su Sistema de Gestión de Seguridad de la Información?

Los siguientes pasos exponen, de modo sucinto y muy práctico, el método que habitualmente han venido utilizando las organizaciones que han implantado y posteriormente certificado BS7799 con éxito, los cuales son aplicables igualmente para el desarrollo de la ISO 27001.

PASO 1: Inicio del proyecto

En esta primera etapa se pretende asegurar para el éxito de todo el proyecto, el compromiso de la dirección general y seleccionar y formar a los miembros del equipo inicial del proyecto.

Para reducir la duración del proceso, el apoyo de la dirección debe estar presente a todos los niveles: operativo, técnico y presupuestario, así como en el de la planificación temporal. La dirección general debe comprender que su apoyo necesariamente conlleva un esfuerzo continuo. La infraestructura establecida requerirá con toda seguridad ajustes, así como una mejora continua.

Gráfico 4: índice de la estructura de la ISO 27001

1. Alcance
   1.1. General
   1.2. Ámbito de aplicación
2. Referencias normativas
3. Términos y definiciones
4. Elementos del Sistema de Gestión de Seguridad de la Información
   4.1. Requisitos generales
   4.2. Establecimiento y gestión del SGSI
   4.2.1. Establecimiento del SGSI
   4.2.2. Implantación y operativa del SGSI
   4.2.3. Revisión y monitorización del SGSI
   4.2.4. Mantenimiento y mejora del SGSI
   4.3. Requisitos de la Documentación
   4.3.1. General
   4.3.2. Control de los documentos
   4.3.3. Control de los registros
5. Responsabilidad de la Dirección
   5.1. Compromiso de la Dirección
   5.2. Gestión de Recursos
   5.2.1. Provisión de recursos
   5.2.2. Formación, conocimiento y competencia
6. Auditorías internas del SGSI
7. Revisión del SGSI
   7.1. General
   7.2. Entradas para la revisión
   7.3. Salidas a la revisión
8. Mejora continua del SGSI
   8.1. Mejora continua
   8.2. Acción correctiva
   8.3. Acción preventiva

Hay también tres anexos:

- Anexo A: Objetivos de Control y Controles (incluidos en una tabla)
- Anexo B: OECD principios de la norma internacional
- Anexo C: Relación entre ISO 9001, 14001 y la norma internacional ISO 27001

Respecto al equipo inicial del proyecto (coordinadores, grupos de trabajo, etc.), se debe formar un comité de dirección del proyecto que puede estar compuesto por un director ejecutivo, el director del proyecto y representantes de las diferentes unidades operativas implicadas. Es habitual que en algunas organizaciones grandes, el responsable de seguridad pueda llevar a cabo gran parte de las tareas del director del proyecto. En la mayoría de los casos, la implementación de la norma ISO 27001 en una organización requiere la implicación de todas las unidades operativas.

PASO 2: Alcance del SGSI

Definición del alcance del SGSI, etapa clave para el éxito posterior del proyecto:

- Alcance del SGSI: ¿qué unidades operativas y actividades estarán dentro del entorno de seguridad de la información?
- Limitaciones del SGSI: características específicas de la organización (tamaño, campo de acción, etc.), ubicación de la organización, activos (inventario de todos los datos críticos), tecnología.
- Conexiones o Interfaces: se deberán tener en cuenta por parte de la organización las relaciones con otros sistemas, otras organizaciones y proveedores externos.
- Requerimientos de Seguridad del SGSI: de naturaleza legal o del negocio.
- Exclusiones y justificación de las exclusiones (Declaración de aplicabilidad).
- Contexto estratégico: las medidas de seguridad planificadas deben tener en cuenta la posición actual y futura de la organización para alcanzar las metas fijadas por la dirección.
- Recopilación de la documentación existente: para simplificar y mejorar la eficacia del proceso desde el inicio, es necesaria una revisión de la documentación existente para evaluar el alcance de las medidas existentes, como el manual de gestión de calidad de la norma ISO 9001, el de la 14001 en su caso, o el manual de políticas de seguridad.
- Redacción de un inventario documental por los responsables de departamento (ejemplos):
  a. Documentos de la política de seguridad.
  b. Normas y procedimiento de las políticas (administrativos o técnicos).
  c. Informes de evaluación de riesgos.

d. Planes de tratamiento de riesgos.
e. Documentos que indiquen la existencia de controles de seguridad y su gestión; por ejemplo, informes y planes de auditoría, informes de incidencias, etc.

PASO 3: Evaluación de riesgos

Con independencia del tipo o tamaño de la empresa, todas las organizaciones son vulnerables a las amenazas que ponen en peligro la confidencialidad, integridad y disponibilidad de la información importante.

Cuanto antes se adopten las medidas correctivas, la seguridad representará un menor coste y será más efectiva. Para poder realizar una identificación y selección de controles más sencillos que permitan una mejor gestión de los recursos humanos y financieros se debe conocer la fuente y naturaleza de las amenazas.

- Aplicabilidad de los controles de la ISO 17799: diagnóstico preliminar.
- Identificación y evaluación de activos, datos a proteger.
- Identificación y evaluación de amenazas y vulnerabilidades.

PASO 4: Tratamiento y administración del riesgo

En este paso es básico conocer cómo la selección y la implantación de los controles permite reducir los riesgos a un nivel aceptable por la organización. Esta gestión generalmente es una función de la:

- Política de seguridad inicial.
- Nivel de seguridad requerido.
- Resultados de la evaluación de riesgos.
- Reglamentación y legislación aplicable.
- Regulaciones y restricciones del negocio existentes.

En general existen cuatro opciones para el tratamiento del riesgo: reducir el riesgo, aceptar el riesgo, evitar el riesgo y transferencia del riesgo.

PASO 5: Programa de Formación y Sensibilización para el Personal

La organización debe asegurarse de que todos los miembros del personal con responsabilidades específicas en el SGSI están debidamente formados, cualificados y capacitados para realizar sus funciones. La organización debe también asegurarse de que el personal necesario está concienciado de la importancia de sus actividades en la seguridad de la información y de cómo contribuyen ellos a alcanzar los objetivos del SGSI.

Es importante desarrollar un programa de formación y sensibilización con el fin de "educar" a todos los empleados. Los empleados tienen que entender y respetar las buenas prácticas de seguridad de la información.

PASO 6: Documentación e implantación del SGSI

La documentación de un SGSI es una exigencia necesaria y previa a la implantación del sistema y se articula en torno a dos puntos estratégicamente claves:

- La descripción de la estrategia de la organización, sus objetivos, la evaluación de riesgos y las medidas adoptadas para evitar o atenuar los mismos.
- El control y el seguimiento del funcionamiento del SGSI. Es usual plantear por lo menos cuatro niveles de documentación como muestra el gráfico 5:

Una vez realizado lo anterior, o en paralelo, se lleva a cabo la implantación de los documentos creados y se complementa con la formación del personal en las etapas en que sea necesario.

PASO 7: Ajustes y preparación para la Auditoría de Certificación

El Diagnóstico es uno de los pasos "previos e imprescindibles" de toda organización que desee y tenga como objetivo la certificación de acuerdo a la norma ISO 27001, con el fin de validar si el sistema sigue las especificaciones necesarias para la implantación de su marco de gestión.

Otro de los pasos que es un requisito *sine qua non* para el éxito de la auditoría es la Declaración de Aplicabilidad, que deberá ser obligatoriamente realizada antes de la auditoría.

Este documento (que se convertirá en un registro imprescindible del SGSI de cara a la auditoría de certificación) proporciona la justificación para la aplicabilidad o no aplicabilidad de cada control ISO 27001 del SGSI en cuestión, incluyendo también dónde es aplicable el estado de implantación de cada control.

En la Declaración de Aplicabilidad deben ser explicados los objetivos, los controles seleccionados, y las razones para su selección, como así también las razones para la exclusión de cualquier medida de la norma ISO 27001.

PASO 8: Control y mejora continua

Control y mejora continua del SGSI de acuerdo al Ciclo de DEMING (P-D-C-A) establecido en la norma debiéndose realizar antes de la Auditoría de Certificación en función de los resultados del diagnóstico.

Gráfico 5

Nivel 1	Manual de seguridad	Política, evaluación de riesgo, declaración de aplicabilidad
Nivel 2	Procedimientos	Procesos: ¿Qué-quién-cuándo-dónde?
Nivel 3	Fichas de trabajo, formularios, etc.	Descripción de cómo se realizan los trabajos y actividades
Nivel 4	Registros	Este nivel proporciona pruebas objetivas de conformidad con las exigencias del SGSI

¿Cómo se desarrolla el proceso de certificación?

Es indudable que una de las grandes ventajas para una empresa certificada es su reconocimiento externo. Disponer de la certificación supone que una tercera parte independiente y acreditada para ello, avala que los niveles del SGSI cumplen los estándares internacionalmente aceptados de buenas prácticas para la gestión de la seguridad de la información.

El proceso de certificación ISO 27001 es muy sencillo y es completamente voluntario. Las organizaciones que hayan completado con éxito el proceso de certificación pueden obtener una mayor confianza en su capacidad para gestionar la seguridad de la información. La auditoría se realiza en dos fases:

1. Revisión de la documentación (fase 1):

Uno de los objetivos de la auditoría fase 1 es la revisión de la documentación, que permite a la Entidad de Certificación la comprensión del SGSI dentro del contexto de la política de seguridad, objetivos y aproximación a la gestión de riesgos. Ésta también sirve como un punto de referencia útil a la hora de preparar la auditoría de fase 2 y ofrece una oportunidad para evaluar el grado de preparación de la organización.

Dicha fase puede complementarse, en función de la complejidad del SGSI, con una visita a las instalaciones de la organización con el fin de comprobar y/o aclarar diferentes aspectos del SGSI que sean requisitos obligatorios para el éxito de la auditoría de certificación.

2. Auditoría "in situ" (fase 2)

Esta auditoría está guiada por las conclusiones del informe de auditoría de fase 1. Se redactará el plan de auditoría basándose en estas conclusiones, y se enviará con la debida antelación a la organización proponiendo el equipo auditor, itinerario, tiempos, recursos necesarios, etc.

En la fecha programada se llevará a cabo la auditoría en la instalación/instalaciones de la organización donde esté desplegado e implantado el SGSI.

Ventajas de los Sistemas de Gestión de Seguridad de la Información

Evidentemente sólo por el hecho de utilizar la norma ISO 17799 o de obtener la certificación ISO 27001 no es razón suficiente para establecer que una organización está segura al 100%; la seguridad completa no existe a menos que se dé una inactividad total... No obstante, la adopción de esta norma proporciona de un modo indiscutible ventajas que todo buen directivo debería tener en cuenta.

1. Aumenta el compromiso de la organización, dado que el sistema permite garantizar y demostrar la eficacia de los esfuerzos desarrollados para asegurar la organización en todos sus niveles.
2. Salvaguarda ventajas competitivas sobre técnicas avanzadas en gestión, mejora de procesos, nuevos desarrollos de software, etc.
3. Incrementa la confianza de los clientes, usuarios y otras partes interesadas con respecto a la información (por ejemplo de carácter personal, confidencial, etc.) que maneja la empresa.
4. Obtiene reducciones en las primas de su seguro, vinculadas a una posible disminución de los incidentes en materia de seguridad de la información.
5. Permite acceder a concursos públicos, selección de proveedores, etc., al tener un SGSI certificado.
6. Mejora la eficacia de las operaciones, personas y procesos relacionados con la seguridad de la información; la gestión de los riesgos, pudiendo obtener un mejor conocimiento de los sistemas de información, sus debilidades y los medios de protección.
7. Garantiza una mejor disponibilidad de los documentos, información y datos.
8. Evita pérdidas, robos, descuidos, etc., con los activos de información en la organización.
9. Garantiza la conformidad y el cumplimiento a las autoridades competentes de los aspectos referentes a la reglamentación y leyes aplicables, pudiendo evidenciarlo mediante registros. En este aspecto la norma es complementaria a su vez de otras normas y legislaciones ya existentes: por ejemplo, en España para la protección de los datos de carácter personal, auditando además su cumplimiento periódico (cada año), por una entidad de Certificación Independiente; y otras a nivel internacional como: HIPAA, Privacy Act of 1974, Computer Security Act of 1987, National Infrastructure Act of 1996, Gramm-Leach-Bliley Act of 1999, Government Information Security Reform Act of 2001.
10. Facilita los procesos de formación y conocimiento del personal en materia de seguridad de la información, siendo una herramienta compatible y complementaria con otros Sistemas de Gestión (ISO 9001 e ISO 14001) y pudiendo realizarse una Auditoría Integrada de su Sistema de Gestión (por ejemplo calidad e información) por un auditor independiente calificado para ambas normas.
11. Genera confianza entre organizaciones que intercambian información, tanto a nivel nacional como internacional.

Ramón Robles, Álvaro Rodríguez de Roa / Comité de Entidades de Certificación de la AEC