

Sociedad General de Autores y Editores: implantación y certificación del SGSI

La Sociedad General de Autores y Editores (en adelante SGAE), basándose en la experiencia de la certificación del Sistema de Gestión de Calidad ISO 9001:2000, abordó el proyecto de certificación UNE 71502:2004 con el objetivo de mejorar la gestión de la información desde el punto de vista de la seguridad. ESA Security participó en diferentes partes del proyecto, apoyando a la SGAE con el objetivo de prepararla para obtener la citada certificación bajo el sello de Aenor.



José Miguel Moneo / Miguel Ángel Aguilar

SGAE

La SGAE se configura como una asociación sin ánimo de lucro, constituida para la protección y gestión de los derechos de propiedad intelectual de los autores, editores y demás administrados que forman parte del colectivo social de la compañía. Su marco legal de actuación está regulado fundamentalmente por el Texto Refundido de la Ley de Propiedad Intelectual, y su funcionamiento interno se recoge en sus Estatutos y Reglamento General.

SGAE administra la explotación de los derechos de comunicación pública, reproducción, distribución y remuneración de los diferentes tipos de obras que le ceden sus administrados, propietarios de las mismas. El repertorio o conjunto de obras administrado por SGAE se compone de obras literarias, musicales, teatrales, cinematográficas y cualesquiera otras obras audiovisuales y multimedia.

Los clientes o usuarios de la Sociedad son aquellas personas físicas o jurídicas que hacen uso del repertorio administrado por SGAE a través de la correspondiente autorización o licencia de uso.

Pueden citarse, entre otros, los siguientes: entidades de radiodifusión, entidades públicas o privadas que organicen cualquier tipo de espectáculo en que se haga uso del repertorio, productores de soportes fonográficos, videográficos y multimedia, redes digitales, cines, teatros, compañías de transportes, grandes almacenes, hoteles, bares, discotecas.

Cabe reseñar que en el año 2004, SGAE repartió 295 millones de euros entre 513.041 obras distintas, de 26.928 socios autores y editores. Cuenta con representación en todas las Comunidades Autónomas y delegaciones

en USA, México, Cuba, Brasil, Argentina, China y Japón. La plantilla está constituida por 485 personas, distribuida en 13 centros de trabajo.

NECESIDADES DEL SGSI

Las obligaciones derivadas del cumplimiento de la ley 15/1999 de Protección de Datos de Carácter Personal (en adelante LOPD) y del Real Decreto 994/1999 relativo al Reglamento

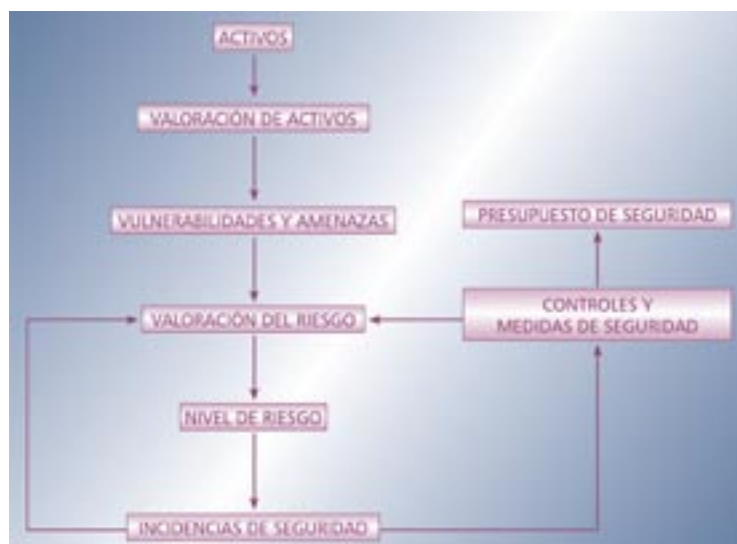


Figura 1

de seguridad de los ficheros automatizados que contengan datos de carácter personal, hicieron plantearse a la organización la conveniencia de ampliar el ámbito de aplicación, desde el estricto cumplimiento de las medidas y requisitos de seguridad exigidos en la normativa citada hasta el diseño e implantación de un sistema global que gestionase los riesgos de seguridad de la información.

Para ello, se tomó como modelo de referencia la guía de buenas prácticas en materia de seguridad ISO 17799.

SGSI

Se ha definido el siguiente esquema de seguridad: (Ver Figura 1)

Activos. Los activos de la Organización se agrupan en categorías, subcategorías y tipos de tratamiento. Las categorías son: documentación, hardware, software, servicios, recursos humanos y edificios y equipamiento. Han sido identificados más de 15.000 activos.

Valoración de activos. Cada uno de los activos encuadrados en cada subcategoría se valoran de acuerdo a cuatro parámetros: confidencialidad, integridad, disponibilidad (accesibilidad) y legalidad.

Vulnerabilidades y amenazas. Se procede a identificar las vulnerabilidades y amenazas a las que está sometido cada uno de los activos señalados. El acceso no autorizado físico a las instalaciones y a la información, errores, código malicioso, robo, fuego son algunos ejemplos.

Controles y medidas de seguridad. La Organización, de acuerdo con la norma ISO 17799, tiene implantados una serie de controles y medidas de seguridad que actúan sobre las vulnerabilidades y amenazas disminuyendo los niveles de riesgo. Hay un total de 127 medidas de seguridad.

Algunas medidas son de tipo organizativo: comité de seguridad, responsables de actividades de seguridad, asesoramiento y revisión de organizaciones externas, exigencias de seguridad a terceras partes con las que se contrata, entre otros.

Otro tipo de medidas hacen referencia al acceso físico: el acceso a la entrada a instalaciones, al CPD mediante tarjeta codificada, suministro eléctrico mediante UPS y condiciones de temperatura y humedad en CPD, entre otros.

Otras medidas tienen que ver con el establecimiento de procedimientos: procedimientos y responsabilidades documentadas en materia de seguridad, antivirus y copias de salvaguarda hasta en tres emplazamientos distintos, manipulación y seguridad en los soportes de información e intercambio de software, entre otros.

Algunas medidas más se refieren al control de accesos: accesos a los sistemas con contraseñas caducables (1 mes) y denegación de servicio al tercer intento no correcto, o seguridad en los servicios de red, entre otros.

Medidas de seguridad relacionadas con el desarrollo de sistemas: los requisitos de seguridad en el software que se desarrolla, el control de paso de las aplicaciones de desarrollo a explotación mediante su correspondiente protocolo y la protección de los datos de prueba de las aplicaciones, son algunos ejemplos.

Finalmente, existen controles para verificar la conformidad del Sistema: controles de cumplimiento de legalidad, auditorías y pruebas de intrusión al sistema, llamadas de *hacking* ético interno y externo, que miden la robustez de los sistemas.

Todos los controles citados tienen un procedimiento que los regula, e incluyen, además, los requisitos recogidos en la ley de protección de datos, así como la normativa en la utilización de las tecnologías de información y comunicación.

Valoración del riesgo. Se define como la probabilidad de materializarse cada una de las vulnerabilidades o amenazas de cada uno de los activos, teniendo en cuenta la valoración de cada activo y los controles y medidas de seguridad implantadas. Se establece una escala de 1 a 3 dependiendo de si el riesgo es bajo, medio o alto respectivamente.

Incidencias de seguridad. Todos los incidentes de seguridad se registran. Con carácter semestral se revisan y se evalúa la eficacia de los controles y medidas adoptadas. Anualmente, en la revisión del sistema que hace la Dirección General, el análisis de las incidencias se utiliza como "entrada" para revisar el nivel de riesgo de la Organización, decidiendo sobre la implantación de nuevas medidas con el correspondiente reflejo en el presupuesto de seguridad, o bien asumiendo el nivel de riesgo para el caso de que el coste de implantar una nueva medida de seguridad sea superior al impacto de materializarse el riesgo.

EXPERIENCIA DE SGAE

Para acometer el proyecto de implantación de SGSI se contó con la aprobación de la política de Seguridad por parte del Consejo de Dirección, la involucración y liderazgo del Presidente del Consejo de Dirección y Director General, y la colaboración y participación de toda la compañía, con mención especial del departamento de Sistemas de Información.

Para poder acometer las diferentes partes del SGSI, se establecieron las diferentes etapas que se debían realizar: (Ver **Figura 2**)

A través del asesoramiento de un consultor jurídico experto que había intervenido como guía en la implantación de las medidas exigidas por la LOPD, se inició el proceso de diseño e implantación del SGSI.

SGAE, a partir del referencial ISO17799, formalizó y sistematizó las medidas de seguridad que venía aplicando, complementando aquellas con las exigidas por la citada norma. Se requirió la colaboración de una compañía con experiencia

en el sector, ESA Security, quien ayudó a completar el diseño del sistema de gestión de riesgos, formalizar e implantar los procedimientos y controles de carácter más técnico.

Asimismo, se realizó la preceptiva auditoría interna del sistema, que incluyó el test de intrusión al sistema para verificar la respuesta ante posibles ataques externos e internos. Estas pruebas tuvieron un resultado satisfactorio, adoptándose las recomendaciones de seguridad que se derivaron de las mismas.

Después de año y medio de trabajos, se

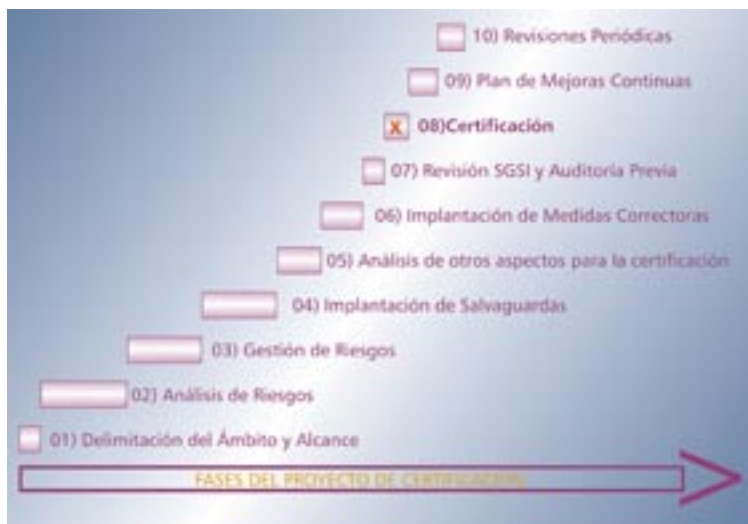


Figura 2

contactó con Aenor para iniciar el proceso de certificación bajo la norma UNE 71502, basado en el análisis de la documentación y la visita *in-situ* a las instalaciones, que concluyó el pasado 7 de abril de 2005 con la concesión del certificado.

PUESTA EN PRÁCTICA

SGAE entró en contacto con ESA Security debido a la necesidad de realizar una auditoría interna de su SGSI conforme al punto 7.2 de la UNE 71502:2004. ESA Security aportó al proyecto dos auditores expertos en SGSI y un experto en implantación UNE 71502:2004.

El proyecto se realizó en dos partes. En la primera, se solicitó la entrega por parte de la SGAE de documentación para una revisión general y la determinación del alcance del SGSI objetivo de la certificación, que en este caso era toda la SGAE (Delegación central y sus delegaciones nacionales). Gracias a la revisión general, siempre dentro del marco del alcance, se pudo obtener una idea clara de la situación del SGSI en ese momento.

En la segunda parte de la auditoría, se realizaron diferentes entrevistas (desde el Director General hasta los responsables de las diferentes áreas de la SGAE). En ellas se pudo comprobar el alto grado de compromiso y sensibilización que la Dirección General de la SGAE tiene con

sus procesos de negocio desde el punto de vista de la seguridad. Se constató que era necesario complementar el SGSI desde el punto de vista técnico informático.

SGAE solicitó la colaboración de ESA Security para complementar el SGSI con las partes técnicas que faltaban. Para el desarrollo del nuevo proyecto se aportó un jefe de proyecto experto en SGSI y dos expertos implantadores de SGSI para UNE 71502.

Se abordaron las siguientes tareas:

1. Complementar el Inventario de activos con nuevos activos y categorías.
2. Complementar el análisis de riesgos con los nuevos activos.
3. Gestión de vulnerabilidades y amenazas a través de ficheros de uso interno.
4. Selección de controles ISO 17799.
5. Estudio de estado de Implantación de los controles ISO 17799.
6. Creación de la declaración de aplicabilidad.
7. Complementar procedimientos técnicos de SGSI.

El objetivo final fue entregar una metodología que no necesitara de la adquisición de ninguna herramienta específica para la gestión del Análisis y Gestión del Riesgo. Para cumplir dicho criterio, se utilizaron para la creación y gestión del proyecto las herramientas estándar del mercado del paquete Microsoft Office (Word, Excel, etc).

CONCLUSIÓN

A modo de resumen cabe indicar que, al igual que en el Sistema de Calidad, el contar con un referente de buenas prácticas en materia de seguridad, tal que la ISO 17799, facilita el camino a la hora de sistematizar y disciplinar actividades.

En el caso de seguridad, por razón de materia de contenido jurídico y técnico, resulta de gran utilidad contar con expertos en ambos campos, además de la convicción de la propia Organización, para garantizar el éxito del proyecto acometido. ■

JOSÉ MIGUEL MONEO PÉREZ
Director de Innovación y Calidad
**SOCIEDAD GENERAL DE AUTORES
Y EDITORES**
jmoneo@sgae.es

MIGUEL ÁNGEL AGUILAR
Experto en Implantación SGSI
ESA SECURITY
maaguiar@esa-security.com