ESQUEMA NACIONAL DE SEGURIDAD

El Esquema Nacional de Seguridad persigue fundamentar la confianza de los ciudadanos en que los sistemas de información prestan sus servicios y custodian la información de acuerdo con sus especificaciones funcionales, sin que pueda llegar al conocimiento de personas no autorizadas. AENOR ha concedido el primer Certificado de Conformidad en el cumplimiento de este esquema.

Confianza en los sistemas de información

Carlos Manuel Fernández
Gerente TIC AENOR
Andres Cebriá
Manuel Viscasillas
Auditores Jefe de SGSI-ENS por AENOR

La Ley 11/2007 de acceso electrónico de los ciudadanos a los Servicios Públicos consagra el derecho de éstos a comunicarse electrónicamente con la Administración en el marco del principio fundamental de la conservación de las garantías constitucionales y legales de sus derechos, cuya exigencia se deriva del artículo 18.4 de nuestra Carta Magna (*La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos*).

Para dar cumplimiento a esta exigencia, el citado cuerpo legal en su artículo 42.2 establece el Esquema Nacional de Seguridad, que tiene por objeto establecer la política de seguridad en la utilización de medios electrónicos en el ámbito de la presente Ley. Asimismo, está constituido por los principios básicos y requisitos mínimos que permitan una protección adecuada de la información.

ESQUEMA NACIONAL DE SEGURIDAD

El Esquema Nacional de Seguridad persigue fundamentar la confianza de los ciudadanos en que los sistemas de información prestarán sus servicios y custodiarán la información de acuerdo con sus especificaciones funcionales, sin interrupciones o modificaciones fuera de control, y sin que la información pueda llegar al conocimiento de personas no autorizadas.

Para generar y acreditar esta confianza, el propio Esquema Nacional de Seguridad define unos mecanismos de verificación (artículo 34 y Anexo III *Auditoría*) y transparencia (artículo 41 *Publicación de conformidad*). Así pues, el mecanismo de verificación es la auditoría de seguridad descrita en el mencionado artículo 34 y Anexo III. Y es que, el punto 4 de este artículo dice: *En la realización de esta auditoría se utilizarán los criterios, métodos de trabajo y de conducta generalmente reconocidos, así como la normalización nacional e internacional aplicables a este tipo de auditorías de sistemas de información.*

Primera auditoría de seguridad

AENOR, como entidad independiente de certificación con más de 28 años de experiencia y cerca de 300 certificados vigentes de acuerdo con la Norma UNE-ISO/IEC 27001 de Sistemas de Gestión de Seguridad de la Información, abordó el reto de realizar esta auditoría de seguridad. El proceso culminó de forma satisfactoria con la entrega el pasado 14 de marzo del primer Certificado de Conformidad con el Esquema Nacional de Seguridad al Consejo General de la Abogacía Española y Red Abogacía. El alcance de esta certificación incluye los sistemas de información que dan soporte a los servicios del Expediente Electrónico de Justicia Gratuita, el portal www.justiciagratuita.es y la Ventanilla Única de la Abogacía www.ventanillaunicaabogados.org.

Para llevar a cabo esta auditoría de conformidad del Esquema Nacional de Seguridad con los requisitos exigidos por la ley, AENOR ha actuado considerando la Norma ISO/IEC 17021:2011 *Evaluación de la Conformidad. Requisitos para los organismos que realizan la auditoría y certificación de sistemas de gestión* como en otros esquemas de certificación (ver figura 1).

El Anexo III del Esquema Nacional de Seguridad (1. Objeto de la auditoría), en su punto 1 dice: *La seguridad de los sistemas de información de una organización será auditada en los siguientes términos:*

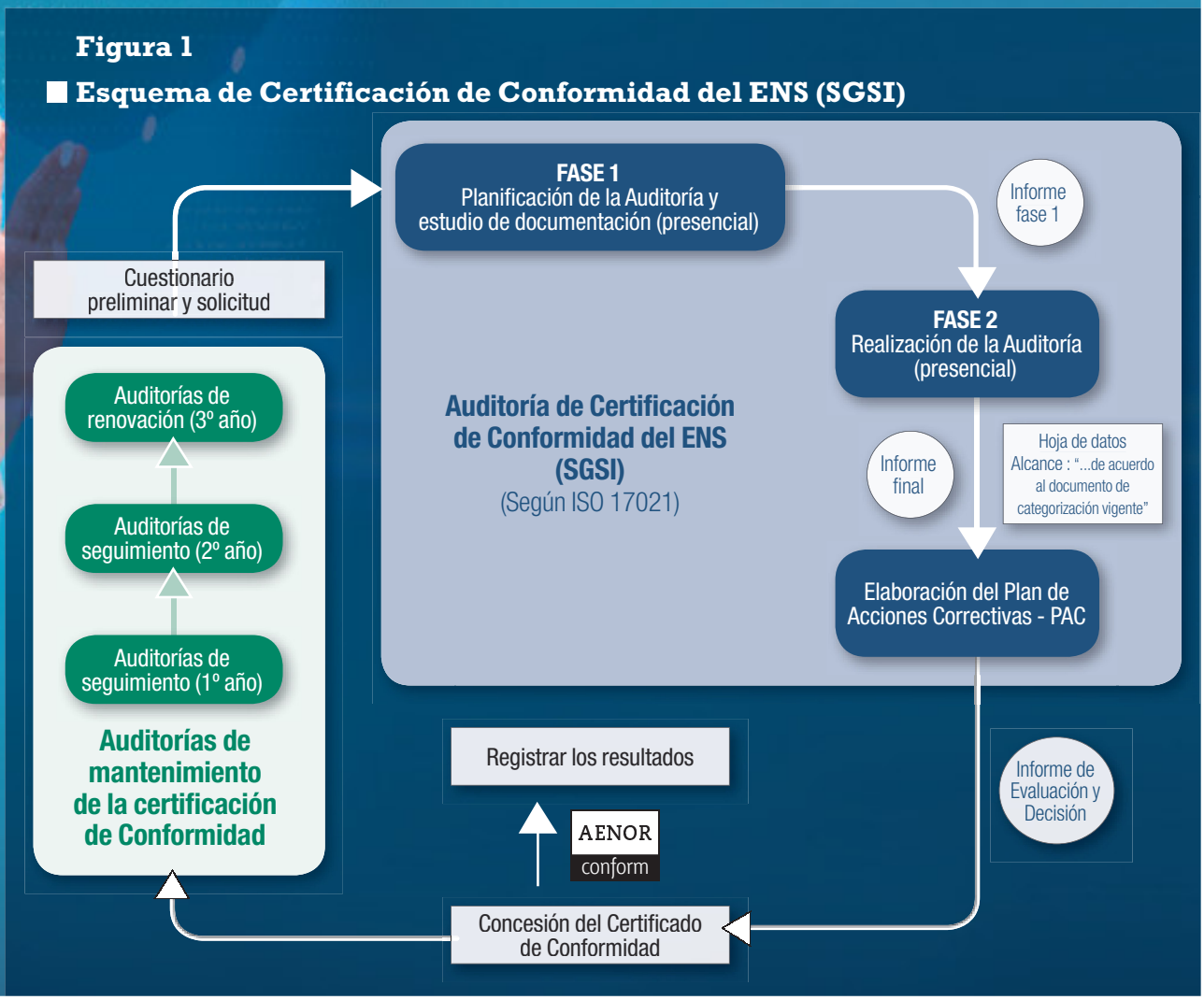
f. Que existe un sistema de gestión de la seguridad de la información, documentado y con un proceso regular de aprobación por la dirección.

Entonces, ¿cómo relacionar los requisitos de un Sistema de Gestión de Seguridad de la Información (SGSI) con el Esquema Nacional de

Tanto el SGSI como el Esquema Nacional de Seguridad utilizan un enfoque basado en la gestión de los riesgos con la mejora continua como marco de referencia

Figura 1

Esquema de Certificación de Conformidad del ENS (SGSI)



Seguridad?, ¿resulta más sencillo implantar el Esquema Nacional de Seguridad en el marco de un SGSI?, ¿puede un SGSI sustituir al Esquema Nacional de Seguridad? Para intentar responder a estas cuestiones, en primer lugar no hay que perder de vista las claras diferencias en origen existentes entre el SGSI y el Esquema Nacional de Seguridad. Respecto a su carácter, un SGSI está basado en una norma internacional ISO de adscripción voluntaria, y el Esquema Nacional de Seguridad viene definido por un Real Decreto de obligado cumplimiento en las Administraciones Públicas en el marco de la administración electrónica. Si tenemos en cuenta su ámbito de aplicación, un SGSI se puede aplicar a todas las organizaciones, cualquiera que sea su tipo, tamaño y naturaleza. Por su parte, el Esquema Nacional de Seguridad, de acuerdo con el artículo 2 de la Ley 11/2007, afecta a las Administraciones Públicas, sus relaciones y al ciudadano en sus relaciones con las Administraciones Públicas. Por último, el alcance en un SGSI lo define la organización y en el Esquema Nacional de Seguridad viene condicionado por los servicios prestados al ciudadano de modo electrónico y las comunicaciones entre Administraciones Públicas.

Similitudes con el SGSI

Sin embargo, todas estas diferencias pueden eliminarse si las opciones que se definen en el SGSI se concretan con las requeridas en el Esquema Nacional de Seguridad. Y es que no todo son diferencias. Tanto uno como otro utilizan para lograr sus objetivos de seguridad de la información un enfoque basado en la gestión de los riesgos con la mejora continua como marco de referencia.

Estableciendo más paralelismos, un sistema de gestión define una política, unos objetivos y el modo de conseguirlos. En el caso del SGSI hablaríamos de política de seguridad de la información, requisitos u objetivos de seguridad de la información y la aplicación de un conjunto de controles técnicos y organizativos para conseguirlos. En el Esquema Nacional de Seguridad, la definición de la política

ESQUEMA NACIONAL DE SEGURIDAD

de seguridad de la información es un requisito exigido. Los niveles de seguridad que hay que lograr se derivan de la categorización de los sistemas y en función de ésta el Anexo II define las medidas de seguridad (controles que hay que implantar).

Tanto el SGSI como el Esquema Nacional de Seguridad formalizan en el documento *Declaración de Aplicabilidad* la relación de controles/medidas de seguridad que hay que implantar. Ante la posibilidad de disparidad o diferencia entre los controles propuestos por la Norma UNE-ISO/IEC 27001 y las medidas de seguridad identificadas en el Anexo II del Esquema Nacional de Seguridad, la propia norma elimina esta posible barrera que aparece en el párrafo 6.1.3 *Tratamiento de los riesgos de seguridad de la información,* en su punto b, que dice: *Determinar todos los controles que sean necesarios para poner en práctica la opción de tratamiento de riesgos de seguridad de la información elegida.*

NOTA: Las organizaciones pueden diseñar controles según sea necesario, o identificarlos a partir de cualquier fuente.

Si la fuente utilizada para implantar los controles es el Anexo II del Esquema Nacional de Seguridad, la superposición es completa.

Con más fines prácticos, se pueden señalar estas sencillas pero clarificadoras conclusiones:

- Es perfectamente factible implantar el Esquema Nacional de Seguridad en el marco de un SGSI basado en la Norma UNE-ISO/IEC 27001.
- Se deberá comprobar que dentro del alcance del SGSI se incluyen todos los sistemas de información objeto del Esquema Nacional de Seguridad (utilización de medios electrónicos en el ámbito de la Administración).
- En la valoración de los activos se deberán considerar dos nuevas dimensiones, como son la trazabilidad y la autenticidad, además de los ya considerados de confidencialidad, disponibilidad e integridad.
- Se deberá realizar una categorización de los sistemas de acuerdo con la valoración de los activos.
- La declaración de aplicabilidad del Esquema Nacional de Seguridad vendrá determinada por la categorización establecida e indica las medidas de seguridad aplicables.
- El Esquema Nacional de Seguridad detalla más explícitamente los controles y medidas de seguridad que hay que aplicar.
- Toda la experiencia acumulada en la implantación y certificación de Sistemas de Gestión de la Información según la Norma UNE-ISO/IEC 27001 es exportable y adaptable al entorno de las Administraciones Públicas para facilitar la implantación y certificación del cumplimiento del Esquema Nacional de Seguridad.

Por supuesto estas conclusiones no tienen ningún ánimo de exhaustividad, siendo un punto de inicio para futuras reflexiones.

Para llevar a cabo esta auditoría de conformidad del Esquema Nacional de Seguridad con los requisitos exigidos por la ley, AENOR ha actuado considerando la Norma ISO/IEC 17021:2011

Carlos Carnicer

Presidente
Consejo General de la Abogacía Española

“Los ciudadanos pueden confiar en que sus datos se gestionan con garantías de seguridad”

¿En qué medida esta certificación contribuye a homogeneizar la calidad del servicio que la abogacía presta a los ciudadanos? ¿Cómo contribuye a agilizar y modernizar la justicia?
Nos hemos propuesto el reto de conseguir que toda la gestión asociada al servicio de la Justicia Gratuita y las comunicaciones entre los diversos actores involucrados se realice sin papeles, de forma electrónica, pero con plenas garantías en cuanto a confidencialidad, integridad y disponibilidad. Para ello, el Consejo General de la Abogacía Española cuenta con RedAbogacía, empresa encargada de ejecutar y mantener los proyectos e iniciativas tecnológicas de la Abogacía.

Nuestra apuesta por las nuevas tecnologías y la seguridad en las comunicaciones se puede comprobar en la tramitación de la solicitud de Justicia Gratuita. Antes de la entrada en funcionamiento de nuestro servicio de Expediente Electrónico de Justicia Gratuita, para recabar los datos obligatorios en su tramitación, se podría llegar a tardar hasta 15 días; ahora en 24 horas se dispone de la misma información y sin que el ciudadano tenga que perder su tiempo en realizar las gestiones en los distintos organismos.

¿De qué forma los clientes percibirán la implantación y certificación de este esquema?
Que la Abogacía Española haya sido la primera entidad en ser auditada y certificada en el Esquema Nacional de Seguridad (ENS) por AENOR expresa la voluntad que existe de estar mejorando continuamente. Esta certificación se convierte en beneficios para los ciudadanos, para nuestros abogados, para los Colegios de Abogados y para los Consejos Autonómicos. Con ella, los usuarios de los servicios que presta la Abogacía Española tienen una prueba de nuestra apuesta por la confidencialidad, integridad y disponibilidad de la información.

Durante el año pasado se han tramitado a través del Expediente Electrónico de Justicia Gratuita más de 525.000 solicitudes de ciudadanos sin recursos económicos, haciendo que se resuelva de forma mucho más rápida su expediente y, ahora, con las recientes certificaciones, estarán aún más confiados en que sus datos se gestionan con plenas garantías de seguridad.

¿Cómo ha sido el proceso de implantación del Esquema Nacional de Seguridad? ¿Qué retos se han encontrado?
Muchos de los requisitos que nos encontramos en el Esquema Nacional de Seguridad son exigencias que ya estaban implantados en la operativa de los servicios de tecnología de la información. El ENS ha sido un estímulo para validar nuestra operativa en cuanto a seguridad se refiere. Sobre todo, los aspectos de auditoría interna y externa, que están avalados por las prácticas que veníamos realizando, incorporando claro está, nuevos aspectos que han mejorado nuestra gestión de la seguridad.

Nuestro Centro de Proceso de Datos (CPD) es relativamente reciente, esto nos ha beneficiado en la implantación del Esquema porque tenemos una infraestructura muy cohesionada que incorpora las funcionalidades más modernas, como son la virtualización total de los servidores o la dotación de altas prestaciones.

Otro aspecto también muy relevante son las labores de concienciación del personal involucrado en la gestión de la seguridad. Nuestro personal está altamente cualificado y nos preocupamos de proporcionar una formación continuada para mantener estos niveles.

El Consejo ha implantado también un sistema de Gestión de Seguridad de la Información según la ISO 27001. ¿Cómo convive el Esquema Nacional de Seguridad con este sistema de gestión? ¿Se apoyan el uno en el otro, se complementan?
Son dos metodologías que se complementan, allí donde una deja los temas de forma más difusa la otra llega con más detalle y profundidad. Para facilitar el compromiso con la Norma ISO 27001 y el Esquema Nacional de Seguridad hemos elaborado una lista de comprobación conjunta para identificar qué requisitos son comunes y cuáles son específicos de cada una de ellas. De esta forma hemos simplificado la implementación y hemos logrado mayor claridad a la hora de realizar el seguimiento del cumplimiento de las mismas.