Título: EL ESQUEMA NACIONAL DE SEGURIDAD

Punto del temario: 4. Iniciativas legales y tecnológicas - Seguridad, conservación y normalización de la información, formatos, y aplicaciones.

Miguel A. Amutio Gómez
Jefe de Área de Planificación y Explotación
Ministerio de la Presidencia
miguel.amutio@mpr.es

Javier Candau
Jefe del Área de Políticas y Servicios
Centro Criptológico Nacional
infosec@areatec.com

Resumen: El Real Decreto 3/2010, de 8 de enero (BOE de 29 de enero), por el que se regula el Esquema Nacional de Seguridad en el ámbito de la administración electrónica, regula el citado Esquema previsto en el artículo 42 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos. Su objeto es establecer la política de seguridad en la utilización de medios electrónicos y está constituido por principios básicos y requisitos mínimos que permitan una protección adecuada de la información. En esta comunicación se exponen los aspectos principales del Esquema Nacional de Seguridad, elaborado con la participación de todas las Administraciones públicas.

1. CREACIÓN DEL ESQUEMA NACIONAL DE SEGURIDAD

La *Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos*, reconoce que la necesaria generalización de la sociedad de la información es subsidiaria, en gran medida, de la confianza que genere en los ciudadanos la relación a través de medios electrónicos.

En consecuencia, esta Ley 11/2007 **tiene entre sus objetivos crear las condiciones de confianza en el uso de los medios electrónicos**, estableciendo las medidas necesarias para la preservación de la integridad de los derechos fundamentales, y en especial de los relacionados con la intimidad y la protección de datos de carácter personal, por medio de la garantía de la seguridad de los sistemas, los datos, las comunicaciones y los servicios electrónicos.

En efecto, la consagración del derecho a comunicarse con las Administraciones públicas a través de medios electrónicos comporta una **obligación** correlativa de éstas **en cuanto a la promoción de las necesarias condiciones de confianza y seguridad** mediante la aplicación segura de las tecnologías.

En este contexto, **se entiende por seguridad** la capacidad de las redes o de los sistemas de información para resistir, con un determinado nivel de confianza, los accidentes, acciones ilícitas o malintencionadas, que comprometan la disponibilidad, autenticidad, integridad, confidencialidad y trazabilidad de los datos almacenados o transmitidos y de los servicios que dichas redes y sistemas ofrecen, o a través de los que se realiza el acceso.

Dicho lo anterior, **diversos principios de la Ley 11/2007, de 22 de junio, se refieren a la seguridad**:

- **El principio de derecho a la protección de los datos de carácter personal** en los términos establecidos en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de carácter personal.

- **El principio de seguridad** en la implantación y utilización de los medios electrónicos por las Administraciones públicas, en cuya virtud se exigirá al menos el mismo nivel de garantías y seguridad que se requiere para la utilización de medios no electrónicos en la actividad administrativa.
- **El principio de proporcionalidad**, en cuya virtud sólo se exigirán las garantías y medidas de seguridad adecuadas a la naturaleza y circunstancias de los distintos trámites y actuaciones.

También **figura la seguridad entre los derechos de los ciudadanos recogidos en la citada Ley**, de forma que se contempla el derecho a la garantía de la seguridad y confidencialidad de los datos que figuren en los ficheros, sistemas y aplicaciones de las Administraciones públicas.

Además, a lo largo del texto de la Ley 11/2007 **el requisito de seguridad está presente** en el tratamiento de la sede electrónica, de las transmisiones de datos entre administraciones, de los registros electrónicos, de las comunicaciones electrónicas, del archivo electrónico de documentos y del procedimiento por medios electrónicos.

Viene a dar respuesta a todo lo anterior el **artículo 42 de la Ley 11/2007 de 22 de junio, mediante la creación del Esquema Nacional de Seguridad (ENS)**, cuyo objeto es **establecer la política de seguridad** en la utilización de medios electrónicos en el ámbito de la citada Ley y que está constituido por **los principios básicos y requisitos mínimos que permitan una protección adecuada de la información**.

Dicho Esquema Nacional de Seguridad, al igual que el Esquema Nacional de Interoperabilidad, se debe **elaborar con la participación de todas las Administraciones públicas** y **aprobar por Real Decreto** del Gobierno, a propuesta de la Conferencia Sectorial de Administración Pública y previo informe de la Comisión Nacional de Administración Local. Este mandato se ha materializado en el *Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.*

El ámbito de aplicación del Esquema Nacional de Seguridad es el de las Administraciones públicas, los ciudadanos en sus relaciones con las mismas y el de las relaciones entre ellas, según se establece en el artículo 2 de la Ley 11/2007. Estarán excluidos de su ámbito de aplicación los sistemas que tratan información clasificada regulada por Ley 9/1968 de 5 de abril, de Secretos Oficiales y sus normas de desarrollo.

Como resultado de un proceso coordinado por el Ministerio de la Presidencia con el apoyo del Centro Criptológico Nacional (CCN) en el que han participado todas las Administraciones públicas, a través de los órganos colegiados con competencia en materia de administración electrónica (Comisión Permanente del Consejo Superior de Administración Electrónica, Conferencia Sectorial de Administración Pública, Comisión Nacional de Administración Local), se ha obtenido el citado real decreto 3/2010 por el que se regula el Esquema Nacional de Seguridad. También se ha sometido al previo informe de la Agencia Española de Protección de Datos y del Consejo de Estado. Se ha recibido además la opinión de numerosos expertos a través de las asociaciones profesionales del sector de la industria de tecnologías de la información y las comunicaciones.

El Esquema **se ha elaborado atendiendo a la normativa** nacional sobre Administración Electrónica, Protección de Datos de Carácter Personal, Firma Electrónica y Documento Nacional de Identidad Electrónico, Centro Criptológico Nacional, Sociedad de la Información, Reutilización de la Información en el Sector Público y Órganos Colegiados responsables de la Administración Electrónica; así como a la regulación de diferentes Instrumentos y Servicios de la Administración, a las Directrices y Guías de la OCDE y a la normalización en la materia.

También han inspirado el contenido del Esquema Nacional de Seguridad documentos de la Administración en materia de seguridad de tecnologías de la información, tales como los Criterios de Seguridad, Normalización y Conservación de las aplicaciones utilizadas para el

ejercicio de potestades, las Guías CCN-STIC de Seguridad de los Sistemas de Información y las Comunicaciones, la metodología MAGERIT de análisis y gestión de riesgos y las herramientas para su aplicación.

Junto con lo anterior, se han tenido presentes las recomendaciones de la Unión Europea (Decisión 2001/844/CE CECA, Euratom de la Comisión de 29 de noviembre de 2001, por la que se modifica su Reglamento interno y Decisión 2001/264/EC del Consejo de 19 de marzo de 2001, por la que se adoptan las normas de seguridad del Consejo), la situación tecnológica de las diferentes Administraciones públicas, así como los servicios electrónicos existentes en las mismas, la utilización de estándares abiertos y, de forma complementaria, estándares de uso generalizado por los ciudadanos; también se han tenido presentes documentos previos de la Administración en materia de seguridad de los medios electrónicos, informáticos y telemáticos.

En particular, un referente que merece una mención singular entre los manejados al elaborar el Esquema Nacional de Seguridad es la conocida *Federal Information Security Management Act* (FISMA) de los Estados Unidos de América, por su naturaleza de texto legal, por su alcance y por su enfoque.

Finalmente, cabe decir que la regulación del Esquema Nacional de Seguridad constituye un hito en nuestro ordenamiento jurídico pues concreta las condiciones relativas a la protección de los sistemas, los datos, las comunicaciones y los servicios electrónicos en el ámbito administrativo, dando respuesta a retos complejos derivados del alto grado de sofisticación de las tecnologías aplicadas a la prestación de servicios públicos por los medios electrónicos.

2. OBJETIVOS

El Esquema Nacional de Seguridad persigue fundamentar la confianza 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. Por lo que sus objetivos son los siguientes:

- **Crear las condiciones necesarias de confianza en el uso de los medios electrónicos**, a través de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones, y los servicios electrónicos, que permita a los ciudadanos y a las Administraciones públicas, el ejercicio de derechos y el cumplimiento de deberes a través de estos medios.
- **Establecer la política de seguridad** en la utilización de medios electrónicos en el ámbito de la Ley 11/2007, que estará constituida por los **principios básicos** y los **requisitos mínimos** para una **protección adecuada** de la información.
- **Introducir los elementos comunes** que han de guiar la actuación de las Administraciones públicas en materia de seguridad de las tecnologías de la información.
- **Aportar un lenguaje común** para facilitar la interacción de las Administraciones públicas, así como la comunicación de los requisitos de seguridad de la información a la industria.

En el Esquema Nacional de Seguridad se concibe la seguridad como una actividad integral, en la que no caben actuaciones puntuales o tratamientos coyunturales, debido a que la debilidad de un sistema la determina su punto más frágil y, a menudo, este punto es la coordinación entre medidas individualmente adecuadas pero deficientemente ensambladas.

Dada la naturaleza de la seguridad, la consecución de estos objetivos requiere un desarrollo que tenga en cuenta la complejidad técnica, la obsolescencia de la tecnología subyacente y el

importante cambio que supone en la operativa de la administración la aplicación de la Ley 11/2007, de 22 de junio.

3. ESTRUCTURA Y CONTENIDO

El Esquema Nacional de Seguridad establece los principios básicos y requisitos mínimos que, de acuerdo con el interés general, naturaleza y complejidad de la materia regulada, permiten una protección adecuada de la información y los servicios en el ámbito de la Ley 11/2007.

Sus elementos principales son los siguientes:

- Los **principios básicos** a ser tenidos en cuenta en las decisiones en materia de seguridad.
- Los **requisitos mínimos** que permitan una protección adecuada de la información.
- El mecanismo para lograr el cumplimiento de los principios básicos y requisitos mínimos mediante **la adopción de medidas de seguridad proporcionadas** a la naturaleza de la información, el sistema y los servicios a proteger.
- La **auditoría de la seguridad**.

El aspecto principal del ENS es, sin duda, que **todos los órganos superiores de las Administraciones públicas deberán disponer de su política de seguridad** que se establecerá en base a los principios básicos y que se desarrollará aplicando los requisitos mínimos, según se expone a continuación.

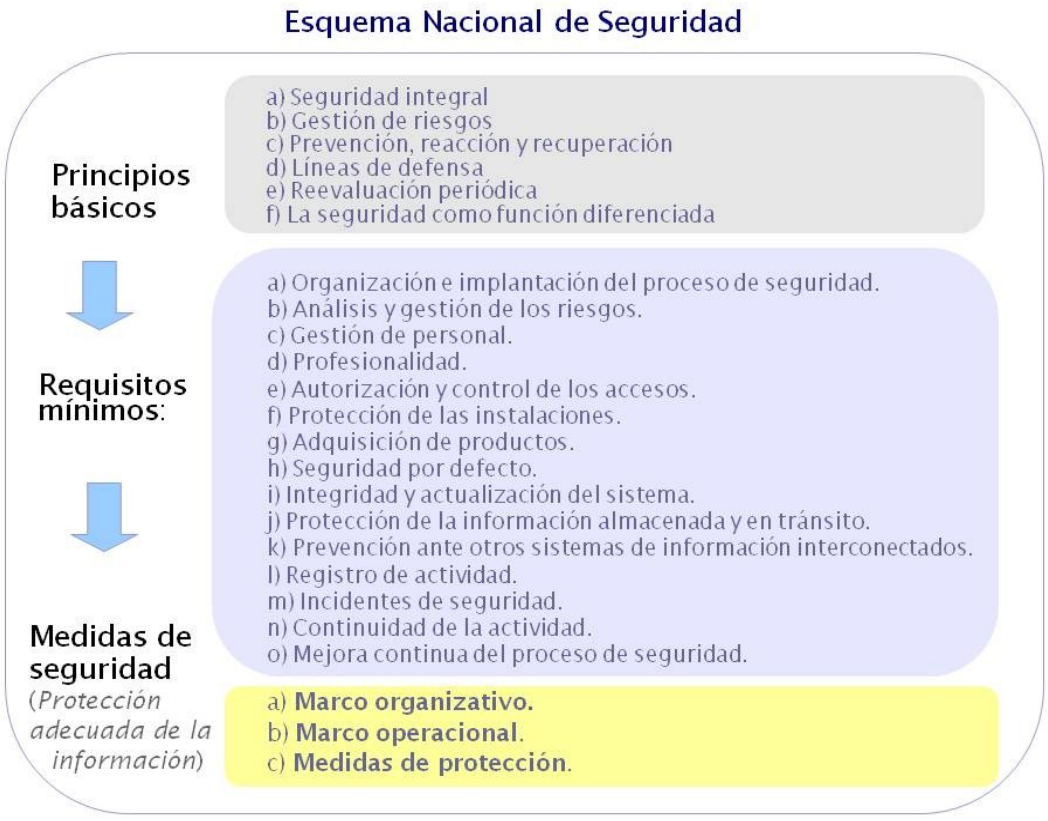

Figura 1: Principios básicos, requisitos mínimos y medidas de seguridad.

En primer lugar se introducen **los principios básicos** que deben tenerse en cuenta en las decisiones en materia de seguridad:

- La seguridad se entiende como un *proceso integral*, constituido por todos los elementos técnicos, humanos, materiales y organizativos relacionados.
- La *gestión de riesgos* permite el equilibrio entre la naturaleza de los datos y los tratamientos, los riesgos a los que están expuestos y las medidas de seguridad.
- La seguridad debe contemplar *la prevención, reacción y recuperación* para conseguir que las amenazas no se materialicen o no afecten gravemente a la información y los servicios.
- Las *líneas de defensa* permiten ganar tiempo, reducir la posibilidad de que el sistema sea comprometido en su conjunto y minimizar el impacto final sobre el mismo.
- Las medidas de seguridad requieren de la *reevaluación y actualización periódicas* para adecuar su eficacia a la evolución de los riesgos y de los sistemas de protección.
- *La seguridad como función diferenciada* de forma que es necesario distinguir las responsabilidades relativas a la información, a los servicios y a la seguridad.

En segundo lugar, se introducen los siguientes quince **requisitos mínimos:**

- *Organización e implantación del proceso de seguridad*, de forma que la política de seguridad deberá identificar unos claros responsables de velar por su cumplimiento y ser conocida por todos los miembros de la organización administrativa.
- Análisis y gestión de los riesgos, de forma que las medidas adoptadas para mitigar o suprimir los riesgos deberán estar justificadas y, en todo caso, existirá una proporcionalidad entre ellas y los riesgos.
- *Gestión de personal*, de forma que todo el personal relacionado con la información y los sistemas deberá ser formado e informado de sus deberes y obligaciones en materia de seguridad.
- *Profesionalidad*, de forma que la seguridad de los sistemas estará atendida, revisada y auditada por personal cualificado, dedicado e instruido en todas las fases de su ciclo de vida.
- *Autorización y control de los accesos*, de forma que el acceso al sistema de información deberá ser controlado y limitado a los usuarios, procesos, dispositivos y otros sistemas de información, debidamente autorizados, restringiendo el acceso a las funciones permitidas.
- *Protección de las instalaciones*, de forma que los sistemas se instalarán en áreas separadas, dotadas de un procedimiento de control de acceso.
- *Adquisición de productos*, de forma que en la adquisición de productos de seguridad de las tecnologías de la información y comunicaciones que vayan a ser utilizados por las Administraciones públicas se valorarán positivamente aquellos que tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición.
- *Seguridad por defecto*, de forma que los sistemas deben diseñarse y configurarse de forma que garanticen la seguridad por defecto.
- *Integridad y actualización del sistema*, de forma que todo elemento físico o lógico requerirá autorización formal previa a su instalación en el sistema. Y se deberá conocer en todo momento el estado de seguridad de los sistemas, en relación a las especificaciones de los fabricantes, a las vulnerabilidades y a las actualizaciones que les

afecten, reaccionando con diligencia para gestionar el riesgo a la vista del estado de seguridad de los mismos.

- *Protección de la información almacenada y en tránsito*, de forma que se prestará especial atención a la información almacenada o en tránsito a través de entornos inseguros.
- *Prevención ante otros sistemas de información interconectados*, de forma que el sistema ha de proteger el perímetro, en particular, si se conecta a redes públicas.
- *Registro de actividad*, de forma que, con plenas garantías del derecho al honor, a la intimidad personal y familiar y a la propia imagen de los afectados, y de acuerdo con la normativa sobre protección de datos personales, de función pública o laboral, y demás disposiciones que resulten de aplicación, se registrarán las actividades de los usuarios, reteniendo la información necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa.
- *Incidentes de seguridad*, de forma que se establecerá un sistema de detección y reacción frente a código dañino. Y se registrarán los incidentes de seguridad que se produzcan y las acciones de tratamiento que se sigan.
- *Continuidad de la actividad*, de forma que los sistemas dispondrán de copias de seguridad y establecerán los mecanismos necesarios para garantizar la continuidad de las operaciones, en caso de pérdida de los medios habituales de trabajo.
- *Mejora continua del proceso de seguridad*, de forma que el proceso integral de seguridad implantado deberá ser actualizado y mejorado de forma continua. Para ello, se aplicarán los criterios y métodos reconocidos en la práctica nacional e internacional relativos a gestión de las tecnologías de la información.

En tercer lugar, se señala **el mecanismo para lograr el cumplimiento de los requisitos mínimos**, a través de las correspondientes medidas de seguridad, teniendo en cuenta que es necesario modular el equilibrio entre la importancia de la información que se maneja, los servicios que se prestan y el esfuerzo de seguridad requerido, en función de los riesgos a los que se está expuesto, bajo el criterio del principio de proporcionalidad.

Para facilitar la aplicación del principio de proporcionalidad se contempla la categorización de los sistemas en tres escalones, en función de la valoración del impacto que tendría un incidente que afectara a la seguridad de la información o de los servicios con perjuicio para la disponibilidad, autenticidad, integridad, confidencialidad o trazabilidad, atendiendo a la repercusión en la capacidad de la organización para el logro de sus objetivos, la protección de sus activos, el cumplimiento de sus obligaciones de servicio, el respeto de la legalidad y de los derechos de los ciudadanos.

Hecha esta valoración, **la selección de las medidas de seguridad apropiadas** se ha de realizar de acuerdo con las dimensiones de seguridad y sus niveles, y, para determinadas medidas de seguridad, de acuerdo con la categoría del sistema.

Se contemplan medidas de seguridad relacionadas con la organización global de la seguridad, con la protección de la operación del sistema como conjunto integral de componentes para un fin y con la protección de activos concretos, según su naturaleza y la calidad exigida por el nivel de seguridad de las dimensiones afectadas. Así, las medidas de seguridad se estructuran, por tanto, en tres grupos:

a) *Marco organizativo*: Constituido por el conjunto de medidas relacionadas con la organización global de la seguridad.

b) *Marco operacional*: Formado por las medidas a tomar para proteger la operación del sistema como conjunto integral de componentes para un fin.

c) *Medidas de protección*: Se centran en proteger activos concretos, según su naturaleza y la calidad exigida por el nivel de seguridad de las dimensiones afectadas.

La articulación entre la protección de datos de carácter personal y el Esquema Nacional de Seguridad se plantea según la mecánica siguiente: **cuando un sistema al que afecte el Esquema Nacional de Seguridad maneje datos de carácter personal** le será de aplicación lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, y normativa de desarrollo, sin perjuicio de los requisitos establecidos en el Esquema.

Figura 2: Medidas de seguridad.

Para lograr un mejor cumplimiento del Esquema se hace referencia a la utilización de los servicios e infraestructuras comunes y a las guías de seguridad de las tecnologías de la información y las comunicaciones que elaborará y difundirá el Centro Criptológico Nacional (CCN).

Adicionalmente se tratan otros aspectos tales como los que se indican a continuación.

En cuarto lugar, se establece la auditoría de la seguridad que verifique el cumplimiento del Esquema al menos cada dos años. Dicha auditoría se realizará en función de la categoría del sistema y para la misma se utilizarán los criterios, métodos de trabajo y de conducta generalmente reconocidos, así como la normalización nacional e internacional aplicable a la misma. El informe de auditoría deberá dictaminar sobre el grado de cumplimiento del Esquema, identificar las deficiencias y sugerir las posibles medidas correctoras o complementarias necesarias, así como las recomendaciones que se consideren oportunas; deberá, igualmente, incluir los criterios metodológicos de auditorías utilizados, el alcance y el objetivo de la auditoría, y los datos, hechos y observaciones en que se basen las conclusiones formuladas.

Junto con las cuestiones anteriores se tratan diversos aspectos que también tienen relevancia como los que se exponen a continuación.

Se tratan las comunicaciones electrónicas contemplando las condiciones técnicas de seguridad de este tipo de comunicaciones, los requerimientos técnicos de notificaciones y publicaciones electrónicas y la firma electrónica:

- Se establece un mandato para que las condiciones técnicas de seguridad de las comunicaciones electrónicas en lo relativo a la constancia de la transmisión y recepción, de sus fechas, del contenido integro de las comunicaciones y la identificación fidedigna del remitente y destinatario de las mismas, sean implementadas de acuerdo con lo establecido en el Esquema Nacional de Seguridad.
- En cuanto a los requerimientos técnicos de las notificaciones y publicaciones electrónicas, se establecen exigencias técnicas relativas al aseguramiento de la autenticidad del organismo que lo publique, de la integridad de la información publicada, de la constancia de fecha y hora de puesta a disposición del interesado y acceso al contenido, así como de la autenticidad del destinatario.
- En cuanto a la firma electrónica, se contempla que los mecanismos de firma electrónica serán establecidos de acuerdo con lo previsto en las medidas de seguridad, con la política de firma electrónica que concretará los procesos de generación, validación y conservación de firmas electrónicas, así como las características y requisitos exigibles a los sistemas de firma electrónica, los certificados, los servicios de sellado de tiempo, y otros elementos de soporte de las firmas.

Se trata la respuesta a incidentes de seguridad donde se recoge como capacidad de respuesta a los incidentes de seguridad de los sistemas en las Administraciones públicas, la estructura CCN-CERT del Centro Criptológico Nacional que actuará sin perjuicio de las capacidades de respuesta que pueda tener cada administración pública, y de su función como coordinador a nivel nacional e internacional, prestando los siguientes servicios a las Administraciones públicas:

- *Soporte y coordinación* para el tratamiento de vulnerabilidades y la resolución de incidentes de seguridad o agresiones recibidas por las distintas Administraciones públicas (general, autonómica y local) y las Entidades de Derecho público con personalidad jurídica propia dependientes de éstas.
- *Investigación y divulgación de las mejores prácticas* sobre seguridad de la información entre todos los miembros de la Administración.
- *Formación* destinada al personal de la Administración especialista en el campo de la seguridad de las tecnologías de la información.
- *Información sobre vulnerabilidades, alertas y avisos* de nuevas amenazas a los sistemas de información, recopiladas de diversas fuentes de reconocido prestigio, incluidas las propias.

De igual modo, se regulan el desarrollo por parte del CCN-CERT de un programa que ofrezca apoyo a las Administraciones públicas para que desarrollen sus propias capacidades de respuesta a incidentes de seguridad.

Figura 3: Portal CCN-CERT, disponible en https://www.ccn-cert.cni.es/

El Esquema también destaca la importancia de la **certificación** a la hora de adquirir productos de seguridad por parte de la Administración. Se contempla que se valorarán positivamente aquellos que tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición. En este sentido se cita al **Organismo de Certificación del Esquema Nacional de Evaluación y Certificación de Seguridad de las TIC** (el propio Centro Criptológico Nacional) como aquel encargado de determinar el criterio a cumplir en función del uso previsto del producto, en relación con el nivel de evaluación, otras certificaciones de seguridad que se requieran adicionales, así como en aquellos casos en los que no existan productos certificados. Asimismo, en diversas ocasiones, el Esquema señala la recomendación y, o bien, obligación de utilizar algoritmos certificados por el Centro Criptológico Nacional a la hora de utilizar diferentes productos o características de los sistemas, como en el caso de utilización de dispositivos físicos (tokens), de la protección de claves criptográficas, protección de la confidencialidad, la autenticidad y de la integridad o en los medios utilizados en la firma electrónica.

Figura 4: Portal del Organismo de Certificación del Esquema Nacional de Evaluación y Certificación de Seguridad de las TIC, disponible en https http://www.oc.ccn.cni.es/index_es.html

Se tratan también las normas de **conformidad** con el Esquema Nacional de Seguridad en cuanto a sedes y registros electrónicos; la inclusión de las especificaciones de seguridad en el ciclo de vida de los servicios y sistemas; los mecanismos de control para garantizar el cumplimiento del Esquema; así como la publicidad de las declaraciones de conformidad, y de los distintivos de seguridad, obtenidos respecto al cumplimiento del Esquema.

Finalmente, las disposiciones adicionales inciden en las cuestiones siguientes:

- **La formación necesaria** para garantizar el conocimiento del Esquema Nacional de Seguridad por parte del personal de las Administraciones públicas.
- INTECO, y otras entidades análogas, podrán desarrollar proyectos de innovación y programas de investigación dirigidos a la mejor implantación de las medidas de seguridad contempladas en el Esquema.
- Se establece un órgano colegiado para la cooperación de las Administraciones públicas en materia de adecuación e implantación de lo previsto en el Esquema.
- Se articula **un mecanismo escalonado para la adecuación** a lo previsto en el Esquema Nacional de Seguridad, de forma que los sistemas existentes se deberán adecuar al Esquema en doce meses, aunque si hubiese circunstancias que impidan la plena aplicación, se dispondrá de un plan de adecuación que marque los plazos de ejecución, en ningún caso superiores a 48 meses desde la entrada en vigor del Esquema.

Más información

- Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos <http://www.boe.es/boe/dias/2007/06/23/pdfs/A27150-27166.pdf>.
- Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos <http://www.boe.es/boe/dias/2009/11/18/pdfs/BOE-A-2009-18358.pdf>.
- Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica. <http://www.boe.es/boe/dias/2010/01/29/pdfs/BOE-A-2010-1331.pdf>.
- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica <http://www.boe.es/boe/dias/2010/01/29/pdfs/BOE-A-2010-1330.pdf>.
- CCN-CERT <http://www.ccn-cert.cni.es/>.
- Series CCN-STIC <http://www.ccn-cert.cni.es/>.
- Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información <http://www.oc.ccn.cni.es/index_es.html>.
- MAGERIT – versión 2. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información <http://www.csae.map.es/csi/pg5m20.htm>.