ESTUDIO DEL ESQUEMA NACIONAL DE SEGURIDAD

Por Joseba Enjuto

AGRADECIMIENTOS

El presente documento forma parte del Trabajo Fin de Master realizado por el autor, titulado "*Modelo de Aplicación Práctica del Real Decreto 3/2010*", en el marco de sus estudios de postgrado en el Máster en Derecho de Internet y Nuevas Tecnologías del **Instituto Europeo Campus Stellae**.

El autor desea agradecer a los tutores, formadores y compañeros del Master su disposición y apoyo en el desarrollo del citado Trabajo y en la redacción del presente documento.

Así mismo, el autor desea agradecer a **CriptoRed**, la Red Temática Iberoamericana de Criptografía y Seguridad de la Información, la oportunidad de difundir el presente estudio.

ÍNDICE DE CONTENIDOS

ESTUDIO DEL ESQUEMA NACIONAL DE SEGURIDAD I
AGRADECIMIENTOS II
ÍNDICE DE CONTENIDOS III
ÍNDICE DE TABLAS IV
1. Introducción 5
1.1. Antecedentes 5
1.2. Situación actual del ENS 6
1.2.1. La realidad de las Administraciones Públicas 7
1.2.2. Dificultades para su acometida 8
1.2.3. Deseos y previsiones 10
1.2.4. Panorama previsto 11
2. Justificación 13
3. Objetivos 14
4. El Esquema Nacional de Seguridad 15
4.1. Descripción del Esquema Nacional de Seguridad 15
4.1.1. Estructura del Esquema Nacional de Seguridad 16
4.2. Análisis del Esquema Nacional de Seguridad 22
4.2.1. Ámbito de aplicación 22
4.2.2. Clasificación de la información 23
4.2.3. Categorización de sistemas 23
4.2.4. Identificación de las líneas base de seguridad 24
4.2.5. Análisis y gestión de riesgos 24
4.2.6. Aplicación de las medidas de seguridad 25
4.2.7. Articulación de las medidas de seguridad 26
4.2.8. Mantenimiento de la Seguridad 30
4.3. Dificultades para la aplicación práctica del ENS 31
5. Conclusiones 34
6. Bibliografía 35

ÍNDICE DE TABLAS

Tabla 1 – Medidas de Seguridad del ENS 22
Tabla 2 – Articulación de las Medidas de Seguridad 30

1. Introducción

1.1. Antecedentes

El 22 de Junio de 2007 vio la luz la Ley 11/2007 de Acceso Electrónico de los Ciudadanos a los Servicios Públicos (LAECSP), que reconoce el derecho de los ciudadanos a relacionarse con las Administraciones Públicas por medios electrónicos y regula los aspectos básicos de la utilización de las tecnologías de la información en la actividad administrativa, tanto en las relaciones de los entes públicos con el exterior (ciudadanos, empresas, Administraciones Públicas y otros entes públicos) como en el funcionamiento interno de los mismos allí donde actúan en régimen de derecho público. Dentro de dicha regulación, la citada Ley establece la necesidad de asegurar la disponibilidad, el acceso, la integridad, la autenticidad, la confidencialidad y la conservación de los datos, informaciones y servicios en el uso de las tecnologías de la información.

Con el fin de crear las condiciones de confianza necesarias en el uso de los medios electrónicos, esta Ley establece, en el artículo 42.2, la creación del denominado Esquema Nacional de Seguridad, cuyo objeto es el establecimiento de los principios básicos y requisitos mínimos de seguridad en la utilización de medios electrónicos, permitiendo la adecuada protección de la información.

El Real Decreto 3/2010 por el que se regula el Esquema Nacional de Seguridad (ENS) en el ámbito de la Administración Electrónica 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. En ese contexto se entiende por seguridad la capacidad de las redes y 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/o trazabilidad de los datos almacenados,

procesados y/o transmitidos y de los servicios que dichas redes y sistemas ofrecen o a través de los que se realiza el acceso.

El Esquema Nacional de Seguridad establece los principios básicos y requisitos mínimos necesarios para proporcionar una protección adecuada de la información y los servicios, definiendo un denominador común normativo en materia de seguridad electrónica de los sistemas que tratan información administrativa en el ámbito de la LAECSP. Esta regulación concibe la seguridad como una actividad integral, consistente en analizar los riesgos de seguridad a los que están expuestos las redes y sistemas considerados, diseñar y desplegar las medidas de seguridad (tanto de carácter organizativo como de carácter operativo y tecnológico) necesarias para mitigar los riesgos identificados, desarrollando estas tareas de forma cíclica, de modo que las medidas de seguridad adoptadas se puedan ir adecuando a la situación cambiante de los servicios prestados.

1.2. Situación actual del ENS

El próximo 30 de Enero de 2014 se cumplirá el periodo máximo legalmente establecido para que las administraciones públicas hayan completado su adecuación al ENS. Su aprobación supuso un importante respaldo a las disciplinas relacionadas con la seguridad de la información, ya que exigía que todas las Administraciones Públicas nacionales desarrollasen un proceso formal para gestionar la seguridad de los servicios electrónicos que prestan a través de Internet en el marco de sus competencias, aplicando una serie de medidas de seguridad específicas y reglamentariamente estipuladas. Sin embargo, a unos meses de que se cumpla el plazo máximo establecido, existen ciertas lagunas acerca del grado de adopción del ENS en la actualidad, debido a las circunstancias que han condicionado la adecuación de las Administraciones Públicas, lo que genera importantes dudas acerca de la consecución real de sus objetivos.

1.2.1. La realidad de las Administraciones Públicas

La realidad es que el panorama actual en relación al grado de adopción del ENS por parte de las Administraciones Públicas es, lamentablemente, poco alentador, como se ha podido comprobar en el último Congreso Nacional de Interoperabilidad y Seguridad. Sin que por el momento existan estadísticas oficiales al respecto, la información pública disponible deja entrever que la adecuación a las exigencias del Esquema Nacional de Seguridad por parte de las Administraciones Públicas es más la excepción que la regla. Son principalmente los ministerios y entes públicos asociados a ellos los que más iniciativas han abordado al respecto, publicado la preceptiva declaración de conformidad con el ENS (la Seguridad Social), creando el correspondiente Comité de Seguridad (el Ministerio de Trabajo e Inmigración) o aprobando la correspondiente Política de Seguridad al respecto (el Ministerio de Ciencia e Innovación, el Ministerio del Interior, el Ministerio de la Presidencia, el Ministerio de Industria, Turismo y Comercio o el Consejo Superior de Deportes), aunque también podemos encontrar alguna universidad o gobierno autonómico tanto en el primer caso (la Universidad Pablo de Olavide) como en el segundo (la Junta de Andalucía o la Universidad de Murcia). También hay diputaciones (la Diputación de Cádiz, la Diputación de Zamora, la Diputación de Burgos, …) y ayuntamientos (el Ayuntamiento de Chiclana de la Frontera, el Ayuntamiento de Majadahonda, el Ayuntamiento de Pozuelo de Alarcón, …) que han iniciado el correspondiente proceso de adecuación, pero en general todos estos procesos están en fases iniciales y cuentan con amplios plazos para su ejecución, que en general se prolongarán más allá de la fecha límite establecida.

Un caso especialmente destacable lo podemos encontrar en el Gobierno Vasco, que no sólo desarrolló a principios de 2010 su Política de Seguridad sino que a mediados del año pasado ya inicio la ejecución de su Plan de Adecuación, con previsión de que esté completamente finalizada para Diciembre del presente año. No obstante, más allá de estos casos puntuales, cuya relevancia relativa en el conjunto de las Administraciones Públicas nacionales es bastante limitada, el panorama es poco halagüeño. Los proyectos no ya de adecuación a las exigencias del Esquema Nacional de

Seguridad, sino sencillamente de elaboración del correspondiente Plan de Adecuación, brillan por su ausencia, sin que ni siquiera figuren, en muchos casos, en la lista de proyectos previstos o pendientes de ejecución.

1.2.2. Dificultades para su acometida

Es evidente que la situación económica por la que está pasando el sector público nacional dificulta enormemente el abordaje de proyectos de este tipo. En general, la adecuación a las exigencias del Esquema Nacional de Seguridad requiere de la dedicación de unos recursos particularmente escasos en estos tiempos, lo cual supone un importante hándicap a la hora de materializar las iniciativas que cualquier Administración Pública pueda tener en esta materia. Sin embargo, no deberíamos quedarnos en el mero argumento económico para justificar esta situación, ya que creo que existen otra serie de motivos igualmente significativos a la hora de entender las causas de este panorama tan poco alentador.

Uno de los principales motivos por los que este tipo de proyectos no acaba de ver la luz es la falta de concienciación de gran parte de las Administraciones Públicas en torno a la seguridad de la información. En general, la seguridad no es vista como un aspecto prioritario, y en muchos casos ni siquiera es tenida en cuenta como un elemento preocupante a la hora de desarrollar servicios públicos, lo que hace que, a la hora de seleccionar los proyectos que finalmente se van a acometer, los relacionados con la seguridad queden dentro del gran grupo de “proyectos deseables pero no prioritarios”. La percepción generalizada de que el nivel de riesgo en materia de seguridad de la información es relativamente bajo –que sea o no correcta dicha percepción queda fuera del objetivo del presente trabajo– hace que este tipo de cuestiones pierda importancia dentro del plan de proyectos de cualquier Administración Pública.

Otro de los motivos que es necesario considerar a la hora de analizar esta situación es la falta de un régimen sancionador asociado al incumplimiento de las exigencias del ENS. Más allá de las responsabilidades genéricas derivadas de infringir los dictámenes de un Real Decreto, la falta de un régimen

sancionador específico hace que esta regulación “pierda peso” en comparación con otro tipo de legislación que también tiene repercusiones directas en materia de seguridad, como es la referida a la protección de datos personales. Pese a que el incumplimiento de la Ley Orgánica 15/1999 de Protección de Datos de carácter personal (LOPD) por parte de las Administraciones Públicas no conlleva una sanción económica asociada, la asociación existente en el imaginario colectivo entre incumplimientos de la LOPD y multas de elevada cuantía ha hecho que dicha regulación cobre un importante peso específico en la actuación de las Administraciones Públicas, y ese es un potente impulsor del que carece el ENS.

Sin embargo, uno de los factores más determinantes en el limitado nivel de implantación del ENS en las Administraciones Públicas se debe, curiosamente, a algo que no tiene nada que ver con la propia seguridad. No debemos olvidar que el Esquema Nacional de Seguridad se enmarca en el ámbito de la Administración Electrónica, como bien indica el título del Real Decreto, y ese es precisamente uno de los principales frenos para la expansión del cumplimiento del ENS. Pese a los plazos definidos en la Disposición final tercera de la Ley de Acceso Electrónico de los Ciudadanos a los Servicios Públicos (Ley 11/2007, de 22 de Junio) y los programas de ayuda desarrollados dentro del marco del Plan Avanza, todavía existe una gran cantidad de Administraciones Públicas que no ha concluido (y en algunos casos, ni siquiera comenzado) el proceso de digitalización de sus servicios, principalmente entre las comunidades autónomas y los entes locales, para quienes dicha obligación quedaba condicionada, según la citada Ley, por la disponibilidad presupuestaria. Pese a lo indicado por el ENS, las Administraciones Públicas que están en la actualidad desarrollando sus servicios electrónicos no se están preocupando por cumplir con las exigencias de seguridad del ENS desde su concepción, sino que están centrando sus esfuerzos en desarrollar exclusivamente el apartado funcional de los mismos. Como se ha indicado anteriormente, la escasa concienciación en materia de seguridad provoca que la misma no sea tenida en cuenta durante el desarrollo de los servicios, cerrando de este modo un círculo vicioso del que se hace difícil encontrar una salida.

1.2.3. Deseos y previsiones

Con estos condicionantes, el panorama que se extiende en torno a la adopción generalizada del ENS por parte de las Administraciones Públicas para los próximos años es complejo. En un escenario de dificultades económicas y escasa cultura y preocupación por la seguridad de la información, es probable que los próximos años no vayan a ser un camino de rosas para el futuro del ENS. Sin embargo, este panorama tampoco debe desalentar, ya que también hay signos positivos que dejan entrever un futuro prometedor, aunque quizás no tan cercano como se hubiera deseado. Nadie dijo que fuese fácil, pero tampoco que fuese imposible.

La realidad tampoco es tan cruda como parece. Que todavía haya muchas Administraciones Públicas que no han iniciado su adecuación a las exigencias del ENS no significa que esas Administraciones Públicas no se preocupen por la seguridad de su información. La seguridad siempre ha sido una de las preocupaciones clásicas de los técnicos informáticos, incluso en aquellas Administraciones Públicas con menor capacidad económica, como son las entidades locales (tal y como refleja, por ejemplo, el estudio de Inteco de 2007 sobre la Seguridad de la Información y eConfianza en el ámbito de las Entidades Locales). Por otro lado, hemos visto que cada vez va habiendo más Administraciones Públicas que inician su andadura en pos del cumplimiento de las exigencias del Esquema Nacional de Seguridad; cada vez hay más funcionarios que van interiorizando la necesidad de ofrecer servicios electrónicos confiables, y poco a poco las Administraciones Públicas van avanzando en la digitalización de sus servicios (así lo demuestran los estudios del Observatorio de Administración Electrónica en sus informes periódicos del grado de avance de la Administración Electrónica en la Administración General del Estado y en las Comunidades Autónomas). Este panorama nos debe llevar a ser optimistas, aunque todavía veamos lejana la luz al final del túnel.

Frente a estas perspectivas, la introducción de algún elemento externo capaz de romper el círculo vicioso que frena la evolución del ENS sería algo totalmente deseable. Cualquier factor capaz de alterar alguno de los frenos expuestos anteriormente supondría un punto de inflexión en el progresivo (aunque lento) proceso de adecuación generalizada a las exigencias del ENS.

La aparición de un programa de ayudas para la adecuación al ENS equivalente al desarrollado dentro del Plan Avanza para el desarrollo de la administración digital sería una gran noticia, pero iniciativas menos ambiciosas como la aparición de algún programa de auditoría externa de verificación del cumplimiento del ENS por parte del Comité Sectorial de Administración Electrónica o de algún programa potente de concienciación en materia de seguridad para toda la Administración Pública constituirían igualmente un revulsivo de cara a la mejora de la seguridad en todas nuestras Administraciones Públicas.

1.2.4. Panorama previsto

En definitiva, tras más de tres años de andadura del Esquema Nacional de Seguridad las sensaciones son ambiguas. Por una parte se percibe un interés creciente por parte de las Administraciones Públicas de ofrecer unos servicios electrónicos seguros, pero por otro lado las dificultades existentes para lograr una adopción generalizada de las exigencias del ENS hacen que ese crecimiento sea tan lento que en ciertos momentos puede llegar a ser desesperante. No obstante, iniciativas como el proyecto de modificación del propio Esquema Nacional de Seguridad que está promoviendo el Ministerio de Hacienda y Administraciones Públicas permiten demostrar que el interés del legislador en torno a la seguridad de la información no ha decaído.

Y en medio de esta situación están, no lo olvidemos, los ciudadanos, que si bien no son todavía una mayoría los que utilizan la administración electrónica, representan una cantidad suficiente de personas (más de 9.000.000) como para atender con la necesaria diligencia las necesidades de seguridad de esos trámites. No podemos perder de vista que el objetivo del Esquema Nacional de Seguridad es crear las condiciones de confianza necesarias en el uso de los medios electrónicos, y más allá de presupuestos, prioridades o concienciación, la confiabilidad de esos medios debería ser un pilar fundamental en el funcionamiento de cualquier Administración Pública. Por lo tanto, parece inevitable que durante los próximos años todos deberemos hacer un esfuerzo adicional para lograr avances en esta materia, puesto que la modernización de

nuestros servicios públicos, y por ende de nuestra sociedad, dependerá en gran medida de ese avance.

2. Justificación

A la vista del panorama existente en torno a la adecuación de las Administraciones Públicas a las exigencias del Esquema Nacional de Seguridad, parece evidente que cualquier iniciativa relacionada con su impulso puede tener una buena acogida en un sector público tan necesitado como interesado en cualquier tipo de ayuda relacionada con la seguridad. Tal y como se ha indicado en el apartado anterior, existe un sentimiento ambivalente al respecto dentro del sector público, normalmente interesado en los beneficios que proporciona la seguridad de la información y el cumplimiento legal pero poco dispuesto a invertir los recursos necesarios para lograr dichos resultados.

En este ámbito, el presente trabajo trata de dar un pequeño impulso a esta situación, tratando de proporcionar a cualquier administración pública interesada en lograr los beneficios que supone la adecuación a las exigencias del ENS un análisis detallado de sus implicaciones.

Con este fin, tras la descripción de la situación actual existente en torno al Esquema Nacional de Seguridad realizada en la introducción, y plantear a continuación la motivación y objetivos del presente trabajo, se lleva a cabo una descripción detallada del Real Decreto y sus exigencias, desmenuzando las principales exigencias recogidas por el ENS en cada uno de los ámbitos cubiertos y detallando las principales dificultades prácticas que cualquier Administración Pública se puede encontrar a la hora de desarrollar un proyecto de adecuación a las mismas.

3. Objetivos

Tal y como se ha señalado, el principal objetivo del presente trabajo es el de presentar un análisis detallado de las exigencias del Esquema Nacional de Seguridad, con el fin de que cualquier organismo público pueda utilizarlo como aclaración a la hora de llevar a cabo su proceso de adecuación.

De forma más específica, los diferentes apartados que se desarrollan en el presente trabajo dan respuesta a objetivos más específicos, como son los siguientes:

- Llevar a cabo una descripción de la situación existente en la actualidad en relación al grado de cumplimiento de las exigencias del Esquema Nacional de Seguridad por parte del sector público nacional.
- Realizar un análisis de las exigencias recogidas por el Esquema Nacional de Seguridad y detallar, en cada uno de los ámbitos cubiertos por el Real Decreto, las implicaciones prácticas que puede tener su cumplimiento.
- Describir las principales dificultades que se puede encontrar un organismo público a la hora de desarrollar las medidas de seguridad planteadas, considerando el marco socio-laboral en el que hay que llevar a cabo la adecuación.

4. El Esquema Nacional de Seguridad

El presente apartado describe el Esquema Nacional de Seguridad, aclarando tanto su estructura y contenido como sus implicaciones y forma de aplicación, así como las principales dificultades que existen en las Administraciones Públicas para lograr un adecuado cumplimiento de sus exigencias.

4.1. Descripción del Esquema Nacional de Seguridad

El objeto del ENS es el establecimiento de los principios básicos y requisitos mínimos de seguridad en la utilización de medios electrónicos, permitiendo la adecuada protección de la información, con el fin de crear las condiciones de confianza necesarias en el uso de los medios electrónicos por parte de los ciudadanos. Por tanto, 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. Para ello, este Real Decreto regula, principalmente, los siguientes aspectos:

- Los principios básicos de seguridad que deben regir su aplicación.
- Los requisitos mínimos que debe garantizar la política de seguridad.
- El deber de categorizar los sistemas de información considerados en función de la información tratada.
- La aplicación de las medidas de seguridad apropiadas en cada caso.
- La posibilidad de utilizar recursos externos específicos para articular la respuesta ante incidentes de seguridad.
- La necesidad de realizar auditorías de seguridad periódicas.
- La obligación de disponer de informes periódicos de estado de la seguridad.
- La necesidad de garantizar la conformidad con el ENS.

De este modo, el Esquema Nacional de Seguridad establece el conjunto de elementos necesarios para garantizar una adecuada gestión de la seguridad de la información en las redes y sistemas involucrados en la prestación de servicios públicos de manera electrónica.

4.1.1. Estructura del Esquema Nacional de Seguridad

El Esquema Nacional de Seguridad se estructura en 10 capítulos y 44 artículos, a lo largo de los cuales se determinan las obligaciones básicas que deben cumplir todas las Administraciones Públicas en materia de seguridad de la información. Así mismo contiene una disposición transitoria que establece los plazos de adecuación, otra derogatoria que anula cualquier disposición contraria al ENS y tres disposiciones finales que establecen sus capacidades normativas. También cuenta con 5 anexos en los que se recogen las medidas de seguridad específicas a aplicar, el procedimiento para determinar cuáles de esas medidas deben ser aplicadas, el procedimiento a seguir para auditar el cumplimiento del ENS, un glosario de términos y un modelo de cláusula administrativa particular a utilizar.

El primer capítulo del ENS, que consta de tres artículos, determina y regula su marco de aplicación, referenciando a la LAECSP. El segundo consta de siete artículos, y establece los principios básicos de seguridad de la información que debe cumplir cualquier Administración Pública para asegurar que podrá seguir funcionando y utilizando sus sistemas de información:

- Gestionar la seguridad de forma integral.
- Analizar y gestionar los riesgos de seguridad.
- Establecer medidas de seguridad que prevengan la aparición de incidentes de seguridad, permitan reaccionar si ocurren y faciliten la recuperación.
- Desarrollar estrategias de protección basadas en la aplicación de múltiples líneas de defensa superpuestas.
- Reevaluar periódicamente la situación de seguridad y los riesgos asociados.

- Definir funciones específicas y diferenciadas para el responsable de la seguridad y los responsables de la información, los servicios y los sistemas de información.

El tercer capítulo del ENS está compuesto por veintinueve artículos, a lo largo de los cuales determina los requisitos mínimos que debe cumplir cualquier Administración Pública para garantizar que su política de seguridad va a poder satisfacer los principios básicos anteriormente indicados:

- Disponer de un proceso de seguridad que cubra a toda la organización y comprometa a todos los implicados en ella.
- Desarrollar periódicamente un análisis y gestión de los riesgos que permita aplicar las medidas de seguridad definidas en el Anexo de forma proporcionar a los riesgos identificados.
- Garantizar la formación de todo el personal en materia de seguridad de la información.
- Garantizar la profesionalidad y capacitación en materia de seguridad de la información tanto del personal propio como del subcontratado.
- Garantizar que a los sistemas de información sólo accede el personal autorizado, y se controlan dichos accesos.
- Disponer de sistemas de control de acceso físico en los CPDs (Centros de Procesamiento de Datos) de las Administraciones Públicas.
- Adquirir productos de seguridad certificados bajo Common Criteria (ISO/IEC 15408) siempre que sea posible.
- Desarrollar los sistemas de información de forma que garanticen su seguridad por defecto.
- Mantener la integridad de los sistemas de información, garantizando que cualquier cambio está autorizado y que se controlan las vulnerabilidades que puedan aparecer.
- Proteger la información tanto cuando está almacenada en los sistemas de información como cuando está almacenada en equipamiento portátil o incluso impresa.

- Proteger el perímetro lógico de los sistemas de información, controlando todas sus conexiones con el exterior.
- Registrar la actividad de los sistemas de información y de sus usuarios, salvaguardando su intimidad y sus derechos.
- Registrar y resolver cualquier incidente de seguridad que se pueda producir, aprendiendo de los mismos.
- Disponer de copias de seguridad y de soluciones que permitan garantizar la continuidad de la actividad en caso de pérdida de los medios habituales de trabajo.
- Garantizar la mejora continua del proceso de seguridad.

Así mismo, el tercer capítulo determina cómo se deben cumplir estos requisitos mínimos y en particular cómo se deben aplicar las medidas de seguridad contempladas en el anexo y qué excepciones se pueden realizar, además de regular el uso de medios comunes y el desarrollo de guías específicas que amplíen o detallen la aplicación de estos requisitos mínimos.

El capítulo cuatro del Esquema Nacional de Seguridad consta de sólo tres artículos, en los que se indica cómo las Administraciones Públicas deben desplegar sus comunicaciones electrónicas.

El quinto capítulo, de un único artículo, indica cómo las Administraciones Públicas deben llevar a cabo las auditorías del ENS, mientras que el sexto, también de un solo artículo, regula el informe de cumplimiento que deben desarrollar y poner a disposición del Comité Sectorial de Administración Electrónica.

El séptimo capítulo, que consta de dos artículos, no regula el funcionamiento de las Administraciones Públicas, sino que establece el funcionamiento del CCN-CERT y las posibilidades que tienen las Administraciones Públicas para utilizar sus servicios.

El capítulo octavo consta de cuatro artículos, en los que se establecen las normas de conformidad que deben seguir las Administraciones Públicas para cumplir con el ENS.

El capítulo noveno, de un solo capítulo, regula el procedimiento de actualización del propio ENS, mientras que el último capítulo, de dos artículos, determina el método de categorización de los sistemas de información que se debe seguir a la hora de llevar a cabo el análisis de riesgos definido en los principios básicos y requisitos mínimos.

El primer anexo del ENS desarrolla la metodología de categorización definida por el décimo capítulo, estableciendo tres niveles (BAJO, MEDIO y ALTO) para los sistemas de información en función de la criticidad de los servicios que proporcionan, analizada por cada una de las dimensiones (propiedades) de seguridad que determina el ENS:

- **Disponibilidad [D]**: Aseguramiento de que los usuarios autorizados tienen acceso cuando lo requieran a la información y sus activos asociados.
- **Integridad [I]**: Garantía de la exactitud y completitud de la información y los métodos de su procesamiento.
- **Confidencialidad [C]**: Aseguramiento de que la información es accesible sólo para aquellos autorizados a tener acceso.
- **Autenticidad [A]**: Aseguramiento de la identidad u origen.
- **Trazabilidad [T]**: Aseguramiento de que en todo momento se podrá determinar quién hizo qué y en qué momento.

El segundo anexo recoge el catálogo de medidas de seguridad a aplicar en función de la categoría que se ha establecido para cada uno de los sistemas de información, y se organizan en:

- Medidas de carácter organizativo, relativas a la organización del proceso de seguridad.
- Medidas de carácter operacional, referentes a las actividades de gestión a llevar a cabo en torno a los sistemas de información.
- Medidas de protección específicas para cada uno de los diferentes ámbitos en los que se requiere actuar para lograr una seguridad integral.

La tabla que figura a continuación recoge el listado de todas las medidas de seguridad definidas por el ENS.

NIVEL			CÓDIGO	MEDIDA DE SEGURIDAD
BAJO	MEDIO	ALTO		
			org	Marco organizativo
Aplica	=	=	org.1	Política de Seguridad
Aplica	=	=	org.2	Normativa de seguridad
Aplica	=	=	org.3	Procedimientos de seguridad
Aplica	=	=	org.4	Proceso de autorización
			op	Marco operacional
			op.pl	Planificación
Aplica	+	++	op.pl.1	Análisis de riesgos
Aplica	=	=	op.pl.2	Arquitectura de seguridad
Aplica	=	=	op.pl.3	Adquisición de nuevos componentes
n.a.	Aplica	=	op.pl.4	Dimensionamiento / Gestión de capacidades
n.a.	n.a.	Aplica	op.pl.5	Componentes certificados
			op.acc	Control de acceso
Aplica	=	=	op.acc.1	Identificación
Aplica	=	=	op.acc.2	Requisitos de acceso
n.a.	Aplica	=	op.acc.3	Segregación de funciones y tareas
Aplica	=	=	op.acc.4	Proceso de gestión de derechos de acceso
Aplica	+	++	op.acc.5	Mecanismo de autenticación
Aplica	+	++	op.acc.6	Acceso local (local logon)
Aplica	+	=	op.acc.7	Acceso remoto (remote login)
			op.exp	Explotación
Aplica	=	=	op.exp.1	Inventario de activos
Aplica	=	=	op.exp.2	Configuración de seguridad
	Aplica	=	op.exp.3	Gestión de la configuración
Aplica	=	=	op.exp.4	Mantenimiento
	Aplica	=	op.exp.5	Gestión de cambios
Aplica	=	=	op.exp.6	Protección frente a código dañino
n.a.	Aplica	=	op.exp.7	Gestión de incidencias
n.a.	n.a.	Aplica	op.exp.8	Registro de la actividad de los usuarios
n.a.	Aplica	=	op.exp.9	Registro de la gestión de incidencias
n.a.	n.a.	Aplica	op.exp.10	Protección de los registros de actividad
Aplica	+	=	op.exp.11	Protección de claves criptográficas
			op.ext	Servicios externos
n.a.	Aplica	=	op.ext.1	Contratación y acuerdos de nivel de servicio
n.a.	Aplica	=	op.ext.2	Gestión diaria
n.a.	n.a.	Aplica	op.ext.9	Medios alternativos
			op.cont	Continuidad del servicio
n.a.	Aplica	=	op.cont.1	Análisis de impacto

NIVEL			CÓDIGO	MEDIDA DE SEGURIDAD
BAJO	MEDIO	ALTO		
n.a.	n.a.	Aplica	op.cont.2	Plan de continuidad
n.a.	n.a.	Aplica	op.cont.3	Pruebas periódicas
			op.mon	Monitorización del sistema
n.a.	n.a.	Aplica	op.mon.1	Detección de intrusión
n.a.	n.a.	Aplica	op.mon.2	Sistema de métricas
			mp	Medidas de protección
			mp.if	Protección de las instalaciones e infraestructuras
Aplica	=	=	mp.if.1	Áreas separadas y con control de acceso
Aplica	=	=	mp.if.2	Identificación de las personas
Aplica	=	=	mp.if.3	Acondicionamiento de los locales
Aplica	+	=	mp.if.4	Energía eléctrica
Aplica	=	=	mp.if.5	Protección frente a incendios
n.a.	Aplica	=	mp.if.6	Protección frente a inundaciones
Aplica	=	=	mp.if.7	Registro de entrada y salida de equipamiento
n.a.	n.a.	Aplica	mp.if.9	Instalaciones alternativas
			mp.per	Gestión del personal
n.a.	Aplica	=	mp.per.1	Caracterización del puesto de trabajo
Aplica	=	=	mp.per.2	Deberes y obligaciones
Aplica	=	=	mp.per.3	Concienciación
Aplica	=	=	mp.per.4	Formación
n.a.	n.a.	Aplica	mp.per.9	Personal alternativo
			mp.eq	Protección de los equipos
Aplica	+	=	mp.eq.1	Puesto de trabajo despejado
n.a.	Aplica	+	mp.eq.2	Bloqueo del puesto de trabajo
Aplica	=	+	mp.eq.3	Protección de equipos portátiles
n.a.	Aplica	=	mp.eq.9	Medios alternativos
			mp.com	Protección de las comunicaciones
Aplica	=	+	mp.com.1	Perímetro seguro
n.a.	Aplica	+	mp.com.2	Protección de la confidencialidad
Aplica	+	++	mp.com.3	Protección de la autenticidad y de la integridad
n.a.	n.a.	Aplica	mp.com.4	Segregación de redes
n.a.	n.a.	Aplica	mp.com.9	Medios alternativos
			mp.si	Protección de los soportes de información
Aplica	=	=	mp.si.1	Etiquetado
n.a.	Aplica	+	mp.si.2	Criptografía
Aplica	=	=	mp.si.3	Custodia
Aplica	=	=	mp.si.4	Transporte
n.a.	Aplica	=	mp.si.5	Borrado y destrucción
			mp.sw	Protección de las aplicaciones informáticas (SW)
n.a.	Aplica	=	mp.sw.1	Desarrollo de aplicaciones
Aplica	+	++	mp.sw.2	Aceptación y puesta en servicio
			mp.info	Protección de la información

NIVEL			CÓDIGO	MEDIDA DE SEGURIDAD
BAJO	MEDIO	ALTO		
Aplica	=	=	mp.info.1	Datos de carácter personal
Aplica	+	=	mp.info.2	Calificación de la información
n.a.	n.a.	Aplica	mp.info.3	Cifrado de la información
Aplica	+	++	mp.info.4	Firma electrónica
n.a.	n.a.	Aplica	mp.info.5	Sellos de tiempo
Aplica	=	=	mp.info.6	Limpieza de documentos
n.a.	Aplica	=	mp.info.9	Copias de seguridad (backup)
			mp.s	Protección de los servicios
Aplica	=	=	mp.s.1	Protección del correo electrónico (e-mail)
Aplica	=	=	mp.s.2	Protección de servicios y aplicaciones web
n.a.	Aplica	+	mp.s.8	Protección frente a la denegación de servicio
n.a.	n.a.	Aplica	mp.s.9	Medios alternativos

Tabla 1 – Medidas de Seguridad del ENS

Por último, el tercer anexo del ENS desarrolla el capítulo relativo a la auditoría de las medidas de seguridad del ENS y establece la metodología a seguir para llevar a cabo dicha auditoría.

4.2. Análisis del Esquema Nacional de Seguridad

Una vez conocido el ENS es necesario analizar sus implicaciones, evaluando las consecuencias prácticas que puede tener su cumplimiento.

4.2.1. Ámbito de aplicación

El primero de los aspectos a destacar en relación al ENS es precisamente su ámbito de aplicación. Es un elemento fundamental, sobre todo si tenemos en cuenta que, tomando como referencia el propio nombre de la LAECSP, se podría caer en el error de pensar que dicho ámbito se restringe exclusivamente a las redes de acceso y sistemas front-end de las Administraciones Públicas. Un análisis más detallado del Real Decreto nos revela que sus estipulaciones son aplicables a cualquier medio electrónico que intervenga en la prestación de servicios públicos electrónicos, y por tanto todos los sistemas implicados, incluyendo los de back-end, deben quedar cubiertos por la política de

seguridad. De hecho, uno de los requisitos mínimos de seguridad incluso establece que a toda información en soporte papel que sea origen o consecuencia de la información electrónica considerada también se le deben aplicar las medidas de seguridad que le correspondan. Por tanto, prácticamente se puede concluir que el ámbito real de aplicación del Esquema Nacional de Seguridad es completo, con la excepción de los sistemas que traten información clasificada regulada por la Ley de Secretos Oficiales y aquellos que se puedan excluir expresamente, si es que los hay, por no intervenir en la prestación de servicios electrónicos a los ciudadanos.

4.2.2. Clasificación de la información

El segundo de los aspectos a destacar es que el punto de partida para el establecimiento de las medidas de seguridad es la clasificación de la información. Para ello, considera las 5 dimensiones de la seguridad de la información (confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad) y exige que se clasifique la información en base a ellas. Para conseguirlo, el Esquema Nacional de Seguridad establece 3 niveles (bajo, medio o alto) en función del perjuicio (limitado, grave o muy grave) que pudiera suponer en las funciones de la organización las consecuencias de un incidente de seguridad que afecte a la dimensión considerada. Por tanto, las Administraciones Públicas estarán obligadas al menos a analizar los tipos de información que poseen, normalmente asociados al catálogo de servicios de cada Administración Pública, y a reflexionar acerca de los niveles de seguridad requeridos para cada tipo de información en cada una de sus dimensiones.

4.2.3. Categorización de sistemas

Una vez identificados los activos de información será necesario identificar los medios electrónicos asociados a cada uno de ellos, dado que las medidas de seguridad se aplican sobre estos últimos. Por tanto, será necesario mapear la información con las redes y sistemas asociados, con el fin de determinar la categorización de dichos sistemas. Esta categorización, definida en tres niveles (básico, medio y alto), vendrá dada sencillamente por el máximo nivel que

alcance cualquiera de los activos de información asociados al sistema analizado en cualquiera de sus dimensiones, y dicha categoría constituirá el punto de partida inicial para establecer las medidas de seguridad apropiadas en cada caso.

4.2.4. Identificación de las líneas base de seguridad

Tras haber identificado la categoría de cada uno de los sistemas considerados se aplicarán las medidas de seguridad pertinentes, de acuerdo a lo estipulado en el Esquema Nacional de Seguridad. Para ello, la Administración Pública deberá seleccionar entre las medidas de seguridad indicadas en el Real Decreto las pertinentes para cada sistema, de acuerdo a las dimensiones de seguridad relevantes, sus niveles y la categorización de los sistemas considerados. La relación de medidas seleccionadas deberá quedar formalizada en un documento denominado Declaración de Aplicabilidad, y constituirá la referencia de partida para elaborar el plan de adecuación.

4.2.5. Análisis y gestión de riesgos

Uno de los aspectos que más dudas suscita en torno al ENS es el encaje del análisis y gestión de riesgos, considerado tanto principio básico como requisito mínimo de seguridad, con la aplicación de las líneas base de seguridad, de acuerdo a lo explicado previamente. Su integración puede no ser obvia, sobre todo si tenemos en cuenta que en sí mismas suponen dos estrategias distintas para conseguir un mismo fin, como es el de determinar las medidas de seguridad a aplicar. Sin embargo, la clave está en conseguir que ambas estrategias sean compatibles, de modo que se puedan aprovechar los beneficios de una y otra de forma simultánea.

Bajo un planteamiento “académico”, la idea sería realizar una primera implantación de las medidas de seguridad que constituyen las líneas base de seguridad, con el fin de garantizar un nivel mínimo estandarizado de seguridad, y en ciclos de revisión sucesivos realizar el “ajuste” de dichas medidas de seguridad a través del análisis y gestión de riesgos. No obstante, con un

planteamiento práctico la solución es tan sencilla como utilizar de manera simultánea ambas vías, realizando el análisis de riesgos en paralelo a la identificación de las líneas base de seguridad, con el fin de incorporar las medidas de seguridad resultantes de la gestión de riesgos a la Declaración de Aplicabilidad indicada, de modo que la relación de medidas de seguridad resultante sea el compendio completo de ambas estrategias.

4.2.6. Aplicación de las medidas de seguridad

Una vez desarrollado el plan de adecuación llegará el turno de la implementación de las medidas de seguridad contempladas. Esta es la parte más variable de cualquier adecuación al ENS, ya que en función de la situación de partida y de las medidas concretas recogidas en la Declaración de Aplicabilidad, dicho plan de adecuación probablemente acabe resultando en el desarrollo de un proyecto multidisciplinar de gran duración y con implicaciones en prácticamente todas las áreas de la Administración Pública, dado que las medidas de seguridad a aplicar recogen desde aspectos organizativos y operacionales hasta medidas de protección específicas tanto de carácter tecnológico como de carácter contractual. Por tanto, esta parte de la adecuación al Esquema Nacional de Seguridad va a constituir uno de los puntos más críticos del proyecto, ya que la implicación real y efectiva del personal y la dedicación de los recursos necesarios a la aplicación de las medidas de seguridad definidas va a condicionar completamente el éxito o fracaso de la adecuación en curso.

Con el fin de tratar de asegurar que este factor crítico es resuelto adecuadamente, el propio Real Decreto establece una serie de mecanismos capaces de permitir a la Administración Pública lidiar de forma apropiada con estos problemas:

- Establece la designación específica de responsables de la información y de responsables de los servicios, con el fin de que cada uno de ellos determine los requisitos de seguridad pertinentes en cada caso.
- Requiere la designación de un responsable de seguridad, encargado de determinar las medidas necesarias para satisfacer los requisitos de

seguridad exigidos, con el fin de que exista una figura independiente cuya preocupación específica sea la de velar por el cumplimiento del ENS.

- Exige la determinación de los mecanismos de coordinación y resolución de conflictos necesarios para articular de forma práctica la interacción entre estas figuras.
- Obliga a la creación de una política de seguridad formal y a su aprobación por el órgano superior competente que corresponda, garantizando de ese modo el conocimiento expreso de la misma y de sus implicaciones prácticas.
- Exige que la seguridad comprometa a todos los miembros de la organización y que la política de seguridad identifique a los responsables de velar por su cumplimiento y sea conocida por todos los miembros de la organización administrativa.

En definitiva, el Esquema Nacional de Seguridad trata de asegurar el compromiso personal con la seguridad de todos los integrantes de la Administración Pública comenzando por los representantes de mayor rango, con el objetivo de que la seguridad de la información cuente con el respaldo adecuado y de que sea un factor considerado expresamente de cara a la asignación de recursos.

4.2.7. Articulación de las medidas de seguridad

Más allá de la organización de medidas de seguridad que plantea el ENS, la articulación práctica de las medidas de seguridad se puede desarrollar en función de su forma y ámbito de aplicación, de la siguiente forma:

- Existen una serie de medidas de seguridad cuya aplicación se enmarca en el ámbito de la gestión de la seguridad, relacionadas con la designación de funciones y responsabilidades, la definición de normas de seguridad y la articulación práctica del proceso de seguridad.

- Hay otra serie de medidas de seguridad relacionadas con la gestión del ciclo de vida de los sistemas de información, desde su diseño y planificación iniciales hasta su desarrollo, implantación y mantenimiento.
- Por último, hay otra serie de medidas de seguridad de carácter tecnológico que deben ser implementadas en los sistemas de información, a cada uno de los niveles.

De acuerdo con este planteamiento, la organización de las medidas de seguridad definidas por el ENS se puede articular de la forma que se establece en la tabla que figura a continuación.

CÓDIGO	Gestión Seguridad			Gestión Sistemas					Medidas Técnicas					
	Roles y responsabilidades	Normativa	Proceso	Diseño	Planificación	Desarrollo	Implantación	Mantenimiento	Instalaciones e Infraestructuras	Sistemas y Backup	SW Base	Comunicaciones	Equipamiento de usuario	Aplicaciones
C:org														
GENERAL	X													
C:org.1		X												
C:org.2		X												
C:org.3			X											
C:org.4		X					X							
C:op														
C:op.pl														
C:op.pl.1			X											
C:op.pl.2				X										
C:op.pl.3		X			X									
C:op.pl.4					X									
C:op.pl.5					X									
C:op.acc														
C:op.acc.1		X			X					X	X	X	X	X
C:op.acc.2		X			X									

CÓDIGO	Gestión Seguridad			Gestión Sistemas					Medidas Técnicas					
	Roles y responsabilidades	Normativa	Proceso	Diseño	Planificación	Desarrollo	Implantación	Mantenimiento	Instalaciones e Infraestructuras	Sistemas y Backup	SW Base	Comunicaciones	Equipamiento de usuario	Aplicaciones
C:op.acc.3	X	X												
C:op.acc.4		X						X						
C:op.acc.5										X	X	X	X	X
C:op.acc.6										X	X	X	X	X
C:op.acc.7		X								X	X	X		X
C:op.exp														
C:op.exp.1								X						
C:op.exp.2						X				X	X	X	X	X
C:op.exp.3								X						
C:op.exp.4								X						
C:op.exp.5								X						
C:op.exp.6		X						X		X			X	
C:op.exp.7			X											
C:op.exp.8										X	X	X	X	X
C:op.exp.9			X											
C:op.exp.10										X	X	X	X	X
C:op.exp.11								X		X	X	X		X
C:op.ext														
C:op.ext.1		X			X									
C:op.ext.2		X						X						
C:op.ext.9		X		X										
C:op.cont														
C:op.cont.1			X											
C:op.cont.2				X	X									
C:op.cont.3								X						
C:op.mon														
C:op.mon.1												X		
C:op.mon.2			X											
C:mp														
C:mp.if														
C:mp.if.1									X					

CÓDIGO	Gestión Seguridad			Gestión Sistemas					Medidas Técnicas					
	Roles y responsabilidades	Normativa	Proceso	Diseño	Planificación	Desarrollo	Implantación	Mantenimiento	Instalaciones e Infraestructuras	Sistemas y Backup	SW Base	Comunicaciones	Equipamiento de usuario	Aplicaciones
C:mp.if.2									X					
C:mp.if.3									X					
C:mp.if.4									X					
C:mp.if.5									X					
C:mp.if.6									X					
C:mp.if.7								X						
C:mp.if.9									X					
C:mp.per														
C:mp.per.1	X													
C:mp.per.2	X													
C:mp.per.3			X											
C:mp.per.4			X											
C:mp.per.9	X													
C:mp.eq														
C:mp.eq.1		X												
C:mp.eq.2													X	
C:mp.eq.3		X											X	
C:mp.eq.9													X	
C:mp.com														
C:mp.com.1				X								X		
C:mp.com.2												X		
C:mp.com.3												X		
C:mp.com.4				X								X		
C:mp.com.9												X		
C:mp.si														
C:mp.si.1		X												
C:mp.si.2		X								X			X	
C:mp.si.3		X												
C:mp.si.4		X												
C:mp.si.5		X								X			X	
C:mp.sw														

CÓDIGO	Gestión Seguridad			Gestión Sistemas					Medidas Técnicas					
	Roles y responsabilidades	Normativa	Proceso	Diseño	Planificación	Desarrollo	Implantación	Mantenimiento	Instalaciones e Infraestructuras	Sistemas y Backup	SW Base	Comunicaciones	Equipamiento de usuario	Aplicaciones
C:mp.sw.1					X	X								
C:mp.sw.2						X	X							
C:mp.info														
C:mp.info.1		X												
C:mp.info.2		X	X											
C:mp.info.3		X									X		X	X
C:mp.info.4		X									X		X	X
C:mp.info.5											X			X
C:mp.info.6		X											X	X
C:mp.info.9										X				
C:mp.s														
C:mp.s.1												X		
C:mp.s.2												X		
C:mp.s.8												X		
C:mp.s.9												X		

Tabla 2 – Articulación de las Medidas de Seguridad

4.2.8. Mantenimiento de la Seguridad

El Esquema Nacional de Seguridad no sólo establece las directrices necesarias para implantar las medidas de seguridad, sino que realiza un especial énfasis en tratar de que dichas medidas se mantengan y evolucionen apropiadamente a lo largo del tiempo. Su objetivo es el de garantizar, en última instancia, que las Administraciones Públicas son capaces de mantener a lo largo del tiempo las garantías de seguridad necesarias. Para ello, el Real Decreto establece distintos mecanismos encaminados a lograr estos objetivos:

- Establece como principio básico la necesidad de entender la seguridad como un proceso integral, y no como algo puntual o coyuntural.
- Requiere la reevaluación y actualización periódicas de las medidas de seguridad, con el fin de mantener su eficacia.
- Exige la existencia de un programa de formación y cualificación que garantice que el personal se mantenga formado e informado acerca de la seguridad.
- Requiere la gestión de los incidentes de seguridad que se puedan producir, y establece la posibilidad de hacer uso de los servicios del CCN-CERT como soporte para dicha gestión.
- Exige la mejora continua del proceso de seguridad, que debe ser actualizado y mejorado de forma continua.
- Establece la necesidad de realizar auditorías periódicas de seguridad, con el fin de verificar el cumplimiento del ENS.
- Requiere la realización de informes periódicos sobre el estado de la seguridad, con el fin de que se puedan elaborar perfiles del estado de la seguridad en las Administraciones Públicas.

De este modo, el ENS regula la sistemática a aplicar de cara a garantizar la necesaria adecuación, mantenimiento y mejora de las medidas de seguridad establecidas, definiendo incluso las bases necesarias para su evaluación y seguimiento.

4.3. Dificultades para la aplicación práctica del ENS

Para llevar a cabo un proyecto de adecuación al ENS es necesario considerar algunos aspectos transversales que pueden condicionar el proyecto:

- La existencia de una Política de Seguridad aprobada, cuyo contenido contemple las exigencias del ENS debe ser la prioridad máxima para cualquier organización. Esto se debe a que, con su aprobación, se valida formalmente la estructura de roles y responsabilidades en materia de seguridad de la información y se aprueba la creación del Comité de

Seguridad, dotando de este modo a la Administración Pública de un órgano con la obligación de promover de manera activa la seguridad de la información. De este modo se va a poder garantizar que exista un órgano con la suficiente autoridad y cuya preocupación fundamental deba ser que la adecuación al ENS se vaya desarrollando según lo previsto, y por tanto que la ejecución del Plan de Adecuación correspondiente vaya progresando.

- Existen ciertas tareas contempladas por cualquier proyecto de adecuación al ENS (la propia definición de la estructura organizativa, el desarrollo de las medidas de control de acceso o el despliegue de las medidas de protección relativas al personal) que están relacionadas con la modificación de roles, funciones y responsabilidades del personal. La aplicación práctica de estas medidas de seguridad puede ser muy diversa, y su nivel de formalización también es variable. En función de estos factores su aplicación final puede acabar siendo compleja, puesto que en ciertos casos puede llegar a requerir la modificación de la Relación de Puestos de Trabajo o de las funciones y responsabilidades formalmente asignadas a un Puesto de Trabajo, lo cual puede provocar la aparición de conflictos laborales que dificulten la aplicación de las medidas de seguridad correspondientes.
- Algunas de las medidas de seguridad contempladas por el ENS (las medidas de protección de los equipos, las medidas de protección de los soportes de información o las medidas de protección de la información, principalmente) afectan directamente a los usuarios de los sistemas de información, ya que tienen implicaciones en torno al comportamiento de los usuarios y a la utilización práctica del equipamiento de usuario. Esto supone que la implementación práctica de las medidas de seguridad correspondientes pueda ser compleja, ya que para lograr su aplicación práctica es necesario el establecimiento de directrices de uso que deben ser desplegadas por los responsables de Recursos Humanos y deben contar con la colaboración de los propios usuarios, lo cual puede ralentizar y dificultar su aplicación efectiva, dado el impacto potencial

que estas medidas de seguridad pueden tener en el día a día de la Administración Pública.

- Por último, parte de las medidas de seguridad previstas por el ENS son de carácter eminentemente tecnológico, de modo que pueden conllevar una complejidad muy variable en función de la implementación específica que se decida llevar a cabo, pero que en cualquier caso puede dificultar la aplicación efectiva de las medidas de seguridad a desarrollar.

Considerando todos estos condicionantes transversales que se acaban de indicar, en el siguiente apartado se presenta un posible modelo de aplicación práctica del ENS, planteando una propuesta de implementación que facilite en cierta medida su aplicación práctica, desplegando un modelo de aplicación que permita cumplir con las medidas de seguridad del ENS de manera eficiente y eficaz.

5. Conclusiones

La aparición del Esquema Nacional de Seguridad a principios de 2010 supuso un gran reto para todo el sector público nacional, que tenía la obligación legal de mejorar el nivel de seguridad ofrecido por su infraestructura de administración electrónica en un contexto de crisis económica y creciente conflictividad social que hacia todavía más compleja la ya de por sí difícil labor de adecuarse a las exigencias recogidas por dicho Real Decreto.

A pocos meses de cumplirse el periodo máximo establecido por dicho Real Decreto para que todas las Administraciones Públicas adecuen sus sistemas de información a lo establecido por el ENS, una gran parte de las mismas todavía no ha llevado a cabo los cambios organizativos, normativos, operativos ni tecnológicos necesarios para cumplir con las exigencias del ENS. Considerando dicha situación, y con el objetivo de facilitar a las Administraciones Públicas la ejecución de los citados cambios, a lo largo del presente trabajo se ha desarrollado un análisis de dichas exigencias, de modo que pueda ser utilizado como aclaración para su aplicación por parte de cualquier organismo público.

El análisis del Esquema Nacional de Seguridad desarrollado es un análisis completo, que trata de contemplar todos los ámbitos de aplicabilidad del ENS y la totalidad de las medidas de seguridad contempladas, organizadas con una orientación práctica. De este modo, el análisis realizado facilita el desarrollo, a partir del planteamiento expuesto, de un modelo de aplicación práctica de las medidas de seguridad del ENS.

En definitiva, el análisis del ENS cumple con todos los objetivos específicos planteados, y permite que cualquier Administración Pública pueda utilizarlo como aclaración práctica para su propia adecuación a las exigencias del Esquema Nacional de Seguridad.

6. Bibliografía

A continuación se recogen las principales referencias bibliográficas utilizadas para la elaboración del presente trabajo:

- **LAECSP**: 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

- **ENS**: 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

- **LOPD**: Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal.
  http://www.boe.es/boe/dias/1999/12/14/pdfs/A43088-43099.pdf

- **RDLOPD**: Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de Desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal.
  http://www.boe.es/boe/dias/2008/01/19/pdfs/A04103-04136.pdf

- Mini-site del Esquema Nacional de Seguridad del CCN-CERT.
  https://www.ccn-cert.cni.es/index.php?option=com_wrapper&Itemid=211

- Mini-site del ENS del Portal de Administración Electrónica.
  http://administracionelectronica.gob.es/ctt/verPestanaGeneral.htm?idIniciativa=146

- Portal “Cumplimiento ENS”.
  http://www.cumplimientoens.es/

- Artículo “Segundo cumpleaños del ENS” – Joseba Enjuto
  (Revista SiC Nº 99 – Abril 2012)
  https://revistasic.es/index.php?option=com_content&view=article&id=523&Itemid=564

- Artículo “Entendiendo el Esquema Nacional de Seguridad” – Joseba Enjuto
  http://www.criptored.upm.es/guiateoria/gt_m733b.htm
- Serie de guías CCN-STIC-800 asociadas al ENS:
  https://www.ccn-cert.cni.es/publico/seccion-ens/guias/index.html