

Seminario "El nuevo Esquema Nacional de Seguridad"

30 de septiembre de 2010

Miguel A. Amutio
Ministerio de la Presidencia



- ♦ **Ley 11/2007, art. 42: El Esquema Nacional de Seguridad**
 - tiene por objeto 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.
- ♦ Regulado en el **Real Decreto 3/2010**, de 8 de enero.
- ♦ **Ámbito de aplicación:** todas las AA.PP. (Ley 11/2007, art. 2).



BOLETÍN OFICIAL DEL ESTADO



Núm. 25 Viernes 29 de enero de 2010 Sec. I. Pág. 8089

I. DISPOSICIONES GENERALES

MINISTERIO DE LA PRESIDENCIA

1330 *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.*

Elaboración del ENS

Resultado de un trabajo coordinado por el Ministerio de la Presidencia, con el apoyo del Centro Criptológico Nacional (CCN)

y con la **participación de todas las AA.PP.**,
a través de los órganos colegiados en administración electrónica,
Más las Universidades Públicas a través de la CRUE
+ Opinión de la Industria del sector TIC.

Realizado **a la luz de referentes:**

- **OCDE:** Directrices de seguridad de la información y las redes.
- **Normalización nacional e internacional** en seguridad de TI.
- **Unión Europea:** recomendaciones en materia de seguridad de la información y las redes e identificación y firma electrónica; y actuaciones de ENISA.
- **Actuaciones en otros países:** EE.UU., Reino Unido, Alemania, Francia

- ♦ **Crear las condiciones necesarias de confianza** en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad, **que permita** a los ciudadanos y a las Administraciones públicas, **el ejercicio de derechos y el cumplimiento de deberes a través de estos medios.**
- ♦ **Introducir lenguaje y elementos comunes**
 - Para guiar la actuación de las AA.PP. en materia de seguridad de las tecnologías de la información.
 - Para facilitar la interacción de las AA.PP., así como la comunicación de los requisitos de seguridad de la información a la Industria.

Elementos principales

- ♦ Los **Principios básicos** a considerar en las decisiones en materia de seguridad.
- ♦ **Los Requisitos mínimos** que permitan una protección adecuada de la información.
- ♦ La **Categorización de los sistemas** para la adopción de **medidas de seguridad** proporcionadas a la naturaleza de la información y los servicios a proteger y a los riesgos a los que están expuestos.
- ♦ La **auditoría de la seguridad** que verifique el cumplimiento del Esquema Nacional de Seguridad.
- ♦ La **respuesta a incidentes de seguridad**. Papel de CCN- CERT.
- ♦ La **certificación**, como aspecto a considerar al adquirir los productos de seguridad. Papel del Organismo de Certificación del Esquema Nacional de Evaluación y Certificación de Seguridad de las TIC (el propio CCN).

- ♦ **Condiciones técnicas de notificaciones, comunicaciones-e y firma-e.**
- ♦ **Mecanismos de control:** Cada órgano de la A.P. o Entidad de Derecho Público establecerá sus mecanismos de control para garantizar de forma real y efectiva el cumplimiento del ENS.
- ♦ **Publicación de la conformidad:** “...darán publicidad en las correspondientes sedes electrónicas a las declaraciones de conformidad, y a los distintivos de seguridad de los que sean acreedores, obtenidos respecto al cumplimiento del ENS.”
- ♦ **Comité Sectorial:**
 - Procedimientos necesarios para **conocer regularmente el estado de seguridad de los sistemas de información** a los que se refiere el ENS.
 - Cooperación relacionada con la implantación del ENS.
- ♦ **Formación al personal de las AA.PP.** para garantizar el cumplimiento del ENS.
- ♦ **Papel de INTECO y de organismos análogos:** “...podrá desarrollar proyectos de innovación y programas de investigación dirigidos a la mejor implantación de las medidas de seguridad...”

Todos los órganos superiores de las AA.PP. deberán disponer de su **política de seguridad** en base a los **principios básicos** y aplicando los **requisitos mínimos** para una **protección adecuada de la información.**

Esquema Nacional de Seguridad

Principios básicos

- a) Seguridad integral
- b) Gestión de riesgos
- c) Prevención, reacción y recuperación
- d) Líneas de defensa
- e) Reevaluación periódica
- f) La seguridad como función diferenciada



Requisitos mínimos:

- a) Organización e implantación del proceso de seguridad.
- b) Análisis y gestión de los riesgos.
- c) Gestión de personal.
- d) Profesionalidad.
- e) Autorización y control de los accesos.
- f) Protección de las instalaciones.
- g) Adquisición de productos.
- h) Seguridad por defecto.
- i) Integridad y actualización del sistema.
- j) Protección de la información almacenada y en tránsito.
- k) Prevención ante otros sistemas de información interconectados.
- l) Registro de actividad.
- m) Incidentes de seguridad.
- n) Continuidad de la actividad.
- o) Mejora continua del proceso de seguridad.



Medidas de seguridad

(Protección adecuada de la información)

- a) Marco organizativo.
- b) Marco operacional.
- c) Medidas de protección.

Cumplimiento de los requisitos mínimos

Para dar cumplimiento de los requisitos mínimos, se seleccionarán las medidas de seguridad proporcionadas, atendiendo a:

- ♦ **La categoría del sistema.** Básica, Media y Alta, según valoración de dimensiones de seguridad (Disponibilidad, Autenticidad, Integridad, Confidencialidad, Trazabilidad).
- ♦ Lo dispuesto en la **Ley Orgánica 15/1999**, y normativa de desarrollo.
- ♦ Las **decisiones** que se adopten **para gestionar los riesgos** identificados.

Medidas de seguridad

- ♦ **Marco organizativo:** organización global de la seguridad
- ♦ **Marco operacional:** proteger la operación del sistema como conjunto integral de componentes para un fin.
- ♦ **Medidas de protección:** proteger activos concretos, según su naturaleza y la calidad exigida por su categoría.



- ♦ **Utilización de infraestructuras y servicios comunes** facilitará el cumplimiento de los principios básicos y requisitos mínimos.
- ♦ **CCN elaborará y difundirá las correspondientes guías de seguridad.**

Dimensiones				MEDIDAS DE SEGURIDAD	
Afectadas	B	M	A		
				org	Marco organizativo
categoria	aplica	=	=	org.1	Política de seguridad
categoria	aplica	=	=	org.2	Normativa de seguridad
categoria	aplica	=	=	org.3	Procedimientos de seguridad
categoria	aplica	=	=	org.4	Proceso de autorización
				op	Marco operacional
				op.pl	Planificación
categoria	aplica	+	++	op.pl.1	Análisis de riesgos
categoria	aplica	=	=	op.pl.2	Arquitectura de seguridad
categoria	aplica	=	=	op.pl.3	Adquisición de nuevos componentes
D	n.a.	aplica	=	op.pl.4	Dimensionamiento / Gestión de capacidades
categoria	n.a.	n.a.	aplica	op.pl.5	Componentes certificados
				op.acc	Control de acceso
A T	aplica	=	=	op.acc.1	Identificación
I C A T	aplica	=	=	op.acc.2	Requisitos de acceso
I C A T	n.a.	aplica	=	op.acc.3	Segregación de funciones y tareas
I C A T	aplica	=	=	op.acc.4	Proceso de gestión de derechos de acceso
I C A T	aplica	+	++	op.acc.5	Mecanismo de autenticación
I C A T	aplica	+	++	op.acc.6	Acceso local (local login)
I C A T	aplica	+	=	op.acc.7	Acceso remoto (remote login)
				op.exp	Explotación
categoria	aplica	=	=	op.exp.1	Inventario de activos
categoria	aplica	=	=	op.exp.2	Configuración de seguridad
categoria	n.a.	aplica	=	op.exp.3	Gestión de la configuración



Adecuación al ENS

Los sistemas de las administraciones deberán estar adecuados en el plazo de **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.**

Cabe destacar lo siguiente:

- Establecer **roles, funciones y procedimientos de designación.**
- **Identificación de la información esencial**, de sus responsables y valoración de la misma.
- **Identificación de los servicios** esenciales, de sus responsables y valoración de los mismos.
- **Análisis de riesgos**; evaluación de los riesgos potenciales y residuales.
- **Evaluación del cumplimiento del anexo ii del ENS.**
- **Análisis de las insuficiencias detectadas**: riesgos residuales no aceptables e incumplimientos del anexo ii.
- **Plan de mejora de la seguridad** para la plena adecuación al ENS.

Instrumentos de apoyo a la adecuación



- PRINCIPAL
- SOBRE NOSOTROS
- INCIDENTES
- ACTUALIDAD
- ALERTAS
- HERRAMIENTAS
- CCN-WINDOWS
- SERIES CCN-STIC
- EAR / PILAR 4.4.2
- EAR / PILAR 4.4.3
- EAR / PILAR 5.1
- SISTEMA
- S.A.T.
- ENS
- RECURSOS
- NOTICIAS
- PREFERENCIAS



ccn-cert seguridad tic
capacidad de respuesta ante incidentes de seguridad de la información

NIVEL DE ALERTA
ALTO

CASTELLANO
ENGLISH
CATALÀ
EUSKARA
GALEGO
VALENCIA

ABRIR SESIÓN

Esquema Nacional de Seguridad

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 (que 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 y se fija como objetivo el crear las condiciones de confianza necesarias en el uso de estos medios). 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.

El citado RD fue elaborado después de un proceso coordinado por el Ministerio de la Presidencia con el apoyo del Centro Criptológico Nacional (CCN) en el que participaron 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). También se sometió 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 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 de la Agencia Española de Protección de Datos y del Consejo de Estado.

Guías de Implantación

- Guía 800 - Glosario de Términos y Abreviaturas del Esquema Nacional de Seguridad [\[Descarga\]](#)
Define los diferentes roles establecidos en el Esquema Nacional de Seguridad que tienen ciertas personas en relación con los elementos del sistema de información que hay que proteger.
- Guía 801 - Responsables y Funciones en el Esquema Nacional de Seguridad (BORRADOR) [\[Descarga\]](#)
Recoge los puntos de implantación detallados en el RD 3/2010 que regula el Esquema Nacional de Seguridad
- Guía 802 - Auditoría del Esquema Nacional de Seguridad [\[Descarga\]](#)
Desarrolla las materias necesarias para dar cumplimiento a lo establecido en el artículo 34 y en el Anexo III del RD 3/2010, y por lo tanto, verificar el cumplimiento de los requisitos establecidos por el RD 3/2010 en los capítulos II y III y en los Anexos I y II.
- Guía 803 - Valoración de sistemas en el Esquema Nacional de Seguridad (BORRADOR) [\[Descarga\]](#)
Amplía los criterios definidos en el Esquema Nacional de Seguridad para determinar el nivel requerido en cada dimensión analizando los elementos esenciales (información y servicios), pivotando alrededor de ellos los criterios que el responsable podrá utilizar.
- Guía 804 - Medidas de implantación del Esquema Nacional de Seguridad (BORRADOR) [\[Descarga\]](#)
Recoge las medidas necesarias de implantación para dar cumplimiento a lo desarrollado en el RD 3/2010 que regula el Esquema Nacional de Seguridad.
- Guía 806 - Plan de Adecuación del Esquema Nacional de Seguridad (BORRADOR) [\[Descarga\]](#)
Los sistemas existentes a la entrada en vigor del RD 3/2010, de 8 de enero, deberán adecuarse al Esquema Nacional de Seguridad de forma que permitan el cumplimiento de lo establecido en la disposición final tercera de la Ley 11/2007, de 22 de junio. Esta guía establece unas pautas de carácter general que son aplicables a entidades de distinta naturaleza, dimensión y sensibilidad sin entrar en casuísticas particulares.
- Guía 809 - Declaración de Conformidad del Esquema Nacional de Seguridad (BORRADOR) [\[Descarga\]](#)
La presente guía tiene por objeto dar pautas generales para la aplicación de lo dispuesto en el artículo 41 del Esquema Nacional de Seguridad, sin perjuicio de la particularización de cada organismo.
- [Preguntas Frecuentes sobre el Esquema Nacional de Seguridad](#)



Organismo de certificación
El CCN como Organismo de Certificación

Acreditación de laboratorios
El Documento de Certificación (DC) del Sistema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información (SNETI) se articula en el ámbito de actuación del Centro Criptológico Nacional, según lo dispuesto respectivamente en la Ley 11/2007, de 4 de junio, reguladora del Centro Nacional de Tecnología y el Real Decreto 421/2004, de 17 de marzo, por el que se regula el Centro Criptológico Nacional.

Normaliva
El ámbito de actuación del Organismo de Certificación comprende a las entidades públicas o privadas que quieren obtener el reconocimiento de evaluación de la seguridad de sus tecnologías de la información, y a los creadores, editores o proveedores de productos o sistemas de TI que quieren certificar la seguridad de dichos productos en el marco del Esquema y cuando dichos productos o sistemas sean susceptibles de ser incluidos en el ámbito de actuación del Centro Criptológico Nacional.

Novedades:
El Organismo de Certificación acredita a los laboratorios de ensayos en base al cumplimiento de los requisitos establecidos en el Capítulo VII. Requisitos de acreditación de laboratorios y según el procedimiento incluido en el Capítulo IV. Acreditación de laboratorios de Instrumentos de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información, aprobado en la ORDEN PREC/2740/2007, de 13 de septiembre.

Novedades:
El Organismo de Certificación acredita la seguridad de productos y sistemas en Tecnologías de la Información, según lo establecido en el procedimiento del Capítulo V. Certificación de productos, sistemas y dispositivos, sus utilities, métodos y normas de evaluación de la seguridad finalizada en el Capítulo VI. Certificación de metodologías de ensayos de otros Organismos de Evaluación y Certificación de la seguridad de las tecnologías de la información.

Los certificados "Common Criteria" emitidos por el Organismo de Certificación están reconocidos internadamente por medio de varios países.

Adicionalmente, el Organismo de Certificación está acreditado por la Entidad Nacional de Acreditación, conforme a los estándares recogidos en la Norma UNE-EN 45011:1990 para la prestación de servicios.

[Consulta de última actualización en el SNETI](#)

- ♦ **Base legal** proporcionada por el RD 3/2010 de aplicación a todas las AA.PP.
- ♦ **Cooperación:** elaborado con la **participación de todas las AA.PP.** más opinión recibida del sector TIC, a la luz de referentes principales.
- ♦ **Creación de las condiciones necesarias para la confianza** en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad, que permita el ejercicio de derechos y el cumplimiento de deberes a través de estos medios.
- ♦ **Tratamiento global de la seguridad.**
- ♦ **Aplicación rigurosa del principio de proporcionalidad** para adecuar la protección a la naturaleza de la información, servicios y sistemas y los riesgos a los que están expuestos
- ♦ **Sistema de protección proporcionado a los bienes protegidos** lo que racionaliza la implantación de medidas de seguridad reduciendo la discrecionalidad.
- ♦ Incluye **referencia a medidas de seguridad**; deja abierto cómo implementarlas.

Muchas gracias



Más información:

Esquema Nacional de Seguridad

<http://www.boe.es/boe/dias/2010/01/29/pdfs/BOE-A-2010-1331.pdf>

<http://www.ctt.map.es/web/ens>

<http://www.csaemap.es/csi/pg5e42.htm>

<http://www.epractice.eu/en/cases/ens>

CCN-CERT <https://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 TI <http://www.oc.ccn.cni.es/>

MAGERIT v2, Metodología de análisis y gestión de riesgos

<http://www.csaemap.es/csi/pg5m20.htm>

Herramienta PILAR <https://www.ccn-cert.cni.es>