El Esquema Nacional de Seguridad

22 abril 2010

Miguel A. Amutio
Ministerio de la Presidencia

- Ley 11/2007, art. 42 –> Real Decreto 3/2010, de 8 de enero
- Ámbito de aplicación
- Objetivos del ENS
- Elementos principales
- Política de seguridad
- Principios básicos y requisitos mínimos
- Categorización de los sistemas y Medidas de seguridad
- Auditoría de la seguridad
- Respuesta a incidentes de seguridad
- Certificación de productos de seguridad
- Más cuestiones
- Adecuación al Esquema Nacional de Seguridad
- Instrumentos para el ENS.
- Conclusiones

Ley 11/2007, art. 42 → RD 3/2010

- *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.

- Resultado de un trabajo coordinado por el **Ministerio de la Presidencia,** con el **apoyo del Centro Criptológico Nacional (CCN)** y la **participación de todas las AA.PP.**

+

- **Opinión de:**
  - **La CRUE**
  - **Industria del sector TIC**

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.*

GOBIERNO DE ESPAÑA | MINISTERIO DE LA PRESIDENCIA

Contexto

OCDE

- Directrices de seguridad de la información y de las redes: ... Evaluación del riesgo, Diseño y realización de la seguridad, Gestión de la seguridad, Reevaluación.
- *Implementation Plan for the OECD Guidelines*: "*Government should develop policies that reflect best practices in security management and risk assessment…to create a coherent system of security*."

UNIÓN EUROPEA

- COM(2001) 298 final "Seguridad de las redes y la información…": ... establecimiento de "políticas de seguridad de la organización"
- i2010 [COM(2006) 173 final] Énfasis en eIDM y firma-e

ENISA

- Identificación de buenas prácticas y tendencias tecnológicas y emergentes. Seguimiento de métodos de análisis y gestión de riesgos.
- Apoyo a las actividades de eIDM (i2010).
- Buenas prácticas de CERTs.

NORMALIZACIÓN nacional e internacional en seguridad de TI.

ACTUACIONES EN OTROS PAÍSES: EE.UU., Reino Unido, Alemania, Francia

Ámbito de aplicación

El ámbito de aplicación del **Esquema Nacional de Seguridad** (ENS) es **el establecido en el artículo 2 de la Ley 11/2007**, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos. (1)

(1)

- A la Administración General del Estado, Administraciones de las Comunidades Autónomas y las Entidades que integran la Administración Local, así como las entidades de derecho público vinculadas o dependientes de las mismas
- A los ciudadanos en sus relaciones con las Administraciones Públicas.
- A las relaciones entre las distintas Administraciones Públicas.

Están excluidos del ámbito de aplicación del ENS los sistemas que tratan información clasificada.

Ámbito de aplicación

¿Y las Universidades públicas?

- Las Universidades públicas son administración pública.
- Son organismos autónomos con vinculación (no dependencia) con las Comunidades Autónomas.

Colaboración MPR – CRUE por medio del Grupo de trabajo de Administración electrónica de la sectorial CRUE-TIC.

Objetivos del ENS

- **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 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.

Elementos principales

- 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.
- La **Categorización de los sistemas** para la adopción de **medidas de seguridad** proporcionadas a la naturaleza de la información y de 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**.
- La **certificación**, como aspecto a considerar al adquirir los productos de seguridad.

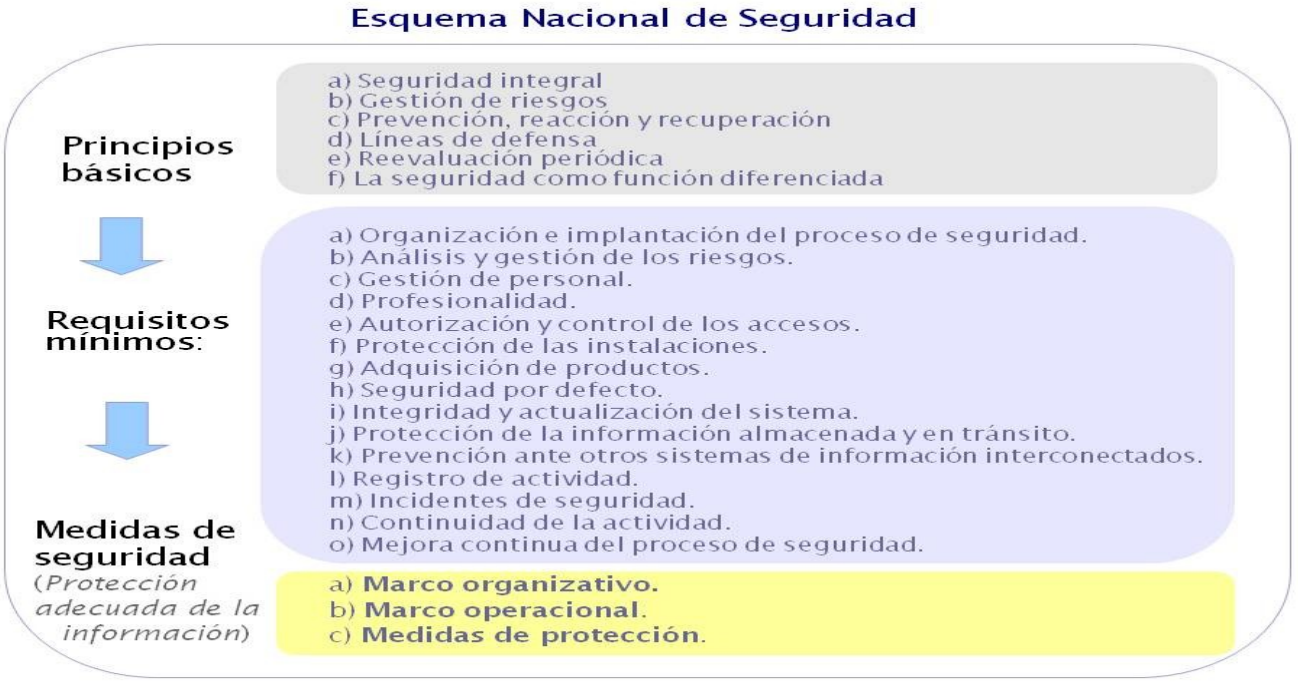
Política de seguridad

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.

Política de seguridad

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.
- **Decisiones** que se adopten para gestionar los **riesgos** identificados.



Principios básicos

En las decisiones en materia de seguridad deberán tenerse en cuenta los siguientes **principios básicos**:

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

Estos principios básicos son fundamentos que deben regir toda acción orientada a asegurar la información y los servicios.

Requisitos mínimos

La política de seguridad se establecerá en base a los principios básicos y se desarrollará aplicando los siguientes **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.

Todos estos requisitos se exigirán en proporción a los riesgos identificados, pudiendo algunos no requerirse en sistemas sin riesgos significativos.

Categorización de los sistemas

- **Categorizar los sistemas es necesario** para modular el equilibrio entre la importancia de los sistemas y el esfuerzo dedicado a su seguridad y satisfacer el principio de proporcionalidad.
- Tres categorías: Básica, Media y Alta.
- **La determinación de la categoría** de un sistema se basa en la valoración del impacto que tendría un incidente con repercusión en la capacidad organizativa para:
  - Alcanzar sus objetivos.
  - Proteger los activos a su cargo.
  - Cumplir sus obligaciones diarias de servicio.
  - Respetar la legalidad vigente.
  - Respetar los derechos de las personas.
- A fin de poder determinar el impacto **se tendrán en cuenta las dimensiones de la seguridad**:
  - Disponibilidad
  - Autenticidad
  - Integridad
  - Confidencialidad
  - Trazabilidad

Categorización de los sistemas

Determinación de la categoría - secuencia de actuaciones:

1. Determinación de las dimensiones de seguridad relevantes.
2. Determinación del nivel correspondiente a cada dimensión de seguridad.
3. Determinación de la categoría del sistema.

- Un sistema puede verse afectado en una o más de sus dimensiones de seguridad.
- Cada dimensión afectada se adscribirá a uno de los niveles: BAJO, MEDIO o ALTO.

  Nivel BAJO: ... perjuicio limitado...
  Nivel MEDIO: ... perjuicio grave...
  Nivel ALTO: ... perjuicio muy grave o catastrófico...

- Determinación de la categoría:
  - ALTA si alguna de las dimensiones alcanza el nivel ALTO.
  - MEDIA si alguna de las dimensiones alcanza el nivel MEDIO, y ninguna otra un nivel superio
  - BÁSICA si alguna de las dimensiones alcanza el nivel BAJO, y ninguna otra un nivel superior

La determinación de la categoría no altera el nivel de las dimensiones de seguridad que no han influido en la determinación de la categoría del mismo.

Medidas de seguridad

Principios básicos -> Requisitos mínimos -> Medidas de seguridad

Selección de las medidas de seguridad apropiadas:

- de acuerdo con las dimensiones de seguridad y sus niveles,
- y, para determinadas medidas de seguridad, de acuerdo con la Categoría.

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

Para facilitar, **cuando en un sistema de información existan sistemas que requieran la aplicación de un nivel de medidas de seguridad diferente** al del sistema principal, **podrán segregarse de este último**, siendo de aplicación en cada caso el nivel de medidas de seguridad correspondiente y siempre que puedan delimitarse la información y los servicios afectados.

Medidas de seguridad

Esquema Nacional de Seguridad

Medidas de seguridad

a) Marco organizativo
- Política de seguridad
- Normativa de seguridad
- Procedimientos de seguridad
- Proceso de autorización

b) Marco operacional
- Planificación
- Control de acceso
- Explotación
- Servicios externos
- Continuidad del servicio
- Monitorización del sistema

c) Medidas de protección
- Protección de las instalaciones e infraestructuras
- Gestión del personal
- Protección de los equipos
- Protección de las comunicaciones
- Protección de los soportes de información
- Protección de las aplicaciones informáticas
- Protección de la información
- Protección de los servicios

+

- La **utilización de infraestructuras y servicios comunes** facilitará el cumplimiento de los principios básicos y requisios comunes en condiciones de mejor eficiencia.
- Para el mejor cumplimiento de lo establecido en el Esquema Nacional de Seguridad **el CCN elaborará y difundirá las correspondientes guías de seguridad**.

GOBIERNO DE ESPAÑA | MINISTERIO DE LA PRESIDENCIA

Medidas de seguridad

Dimensiones				MEDIDAS DE SEGURIDAD	
Afectadas	B	M	A		
				org	**Marco organizativo**
categoría	aplica	=	=	org.1	Política de seguridad
categoría	aplica	=	=	org.2	Normativa de seguridad
categoría	aplica	=	=	org.3	Procedimientos de seguridad
categoría	aplica	=	=	org.4	Proceso de autorización
				op	**Marco operacional**
				op.pl	Planificación
categoría	aplica	+	++	op.pl.1	Análisis de riesgos
categoría	aplica	=	=	op.pl.2	Arquitectura de seguridad
categoría	aplica	=	=	op.pl.3	Adquisición de nuevos componentes
D	n.a.	aplica	=	op.pl.4	Dimensionamiento / Gestión de capacidades
categoría	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 logon)
I C A T	aplica	+	=	op.acc.7	Acceso remoto (remote login)
				op.exp	Explotación
categoría	aplica	=	=	op.exp.1	Inventario de activos
categoría	aplica	=	=	op.exp.2	Configuración de seguridad
categoría	n.a.	aplica	=	op.exp.3	Gestión de la configuración

Dimensiones				MEDIDAS DE SEGURIDAD	
Afectadas	B	M	A		
categoría	aplica	=	=	op.exp.4	Mantenimiento
categoría	n.a.	aplica	=	op.exp.5	Gestión de cambios
categoría	aplica	=	=	op.exp.6	Protección frente a código dañino
categoría	n.a.	aplica	=	op.exp.7	Gestión de incidencias
T	n.a.	n.a.	aplica	op.exp.8	Registro de la actividad de los usuarios
categoría	n.a.	aplica	=	op.exp.9	Registro de la gestión de incidencias
T	n.a.	n.a.	aplica	op.exp.10	Protección de los registros de actividad
categoría	aplica	+	=	op.exp.11	Protección de claves criptográficas
				op.ext	Servicios externos
categoría	n.a.	aplica	=	op.ext.1	Contratación y acuerdos de nivel de servicio
categoría	n.a.	aplica	=	op.ext.2	Gestión diaria
D	n.a.	n.a.	aplica	op.ext.9	Medios alternativos
				op.cont	Continuidad del servicio
D	n.a.	aplica	=	op.cont.1	Análisis de impacto
D	n.a.	n.a.	aplica	op.cont.2	Plan de continuidad
D	n.a.	n.a.	aplica	op.cont.3	Pruebas periódicas
				op.mon	Monitorización del sistema
categoría	n.a.	n.a.	aplica	op.mon.1	Detección de intrusión
categoría	n.a.	n.a.	aplica	op.mon.2	Sistema de métricas
				mp	**Medidas de protección**
				mp.if	Protección de las instalaciones e infraestructuras
categoría	aplica	=	=	mp.if.1	Áreas separadas y con control de acceso
categoría	aplica	=	=	mp.if.2	Identificación de las personas
categoría	aplica	=	=	mp.if.3	Acondicionamiento de los locales
D	aplica	+	=	mp.if.4	Energía eléctrica
D	aplica	=	=	mp.if.5	Protección frente a incendios
D	n.a.	aplica	=	mp.if.6	Protección frente a inundaciones
categoría	aplica	=	=	mp.if.7	Registro de entrada y salida de equipamiento
D	n.a.	n.a.	aplica	mp.if.9	Instalaciones alternativas
				mp.per	Gestión del personal
categoría	n.a.	aplica	=	mp.per.1	Caracterización del puesto de trabajo
categoría	aplica	=	=	mp.per.2	Deberes y obligaciones

Medidas de seguridad

Dimensiones				MEDIDAS DE SEGURIDAD	
Afectadas	B	M	A		
categoría	aplica	=	=	mp.per.3	Concienciación
categoría	aplica	=	=	mp.per.4	Formación
D	n.a.	n.a.	aplica	mp.per.9	Personal alternativo
				mp.eq	Protección de los equipos
categoría	aplica	+	=	mp.eq.1	Puesto de trabajo despejado
A	n.a.	aplica	+	mp.eq.2	Bloqueo de puesto de trabajo
categoría	aplica	=	+	mp.eq.3	Protección de equipos portátiles
D	n.a.	aplica	=	mp.eq.9	Medios alternativos
				mp.com	Protección de las comunicaciones
categoría	aplica	=	+	mp.com.1	Perímetro seguro
C	n.a.	aplica	+	mp.com.2	Protección de la confidencialidad
I A	aplica	+	++	mp.com.3	Protección de la autenticidad y de la integridad
categoría	n.a.	n.a.	aplica	mp.com.4	Segregación de redes
D	n.a.	n.a.	aplica	mp.com.9	Medios alternativos
				mp.si	Protección de los soportes de información
C	aplica	=	=	mp.si.1	Etiquetado
I C	n.a.	aplica	+	mp.si.2	Criptografía
categoría	aplica	=	=	mp.si.3	Custodia
categoría	aplica	=	=	mp.si.4	Transporte
C	n.a.	aplica	=	mp.si.5	Borrado y destrucción
				mp.sw	Protección de las aplicaciones informáticas
categoría	n.a.	aplica	=	mp.sw.1	Desarrollo
categoría	aplica	+	++	mp.sw.2	Aceptación y puesta en servicio
				mp.info	Protección de la información
categoría	aplica	=	=	mp.info.1	Datos de carácter personal
C	aplica	+	=	mp.info.2	Calificación de la información
C	n.a.	n.a.	aplica	mp.info.3	Cifrado
I A	aplica	+	++	mp.info.4	Firma electrónica
T	n.a.	n.a.	aplica	mp.info.5	Sellos de tiempo
C	aplica	=	=	mp.info.6	Limpieza de documentos
D	n.a.	aplica	=	mp.info.9	Copias de seguridad (backup)
				mp.s	Protección de los servicios
categoría	aplica	=	=	mp.s.1	Protección del correo electrónico
categoría	aplica	=	=	mp.s.2	Protección de servicios y aplicaciones web

Dimensiones				MEDIDAS DE SEGURIDAD	
Afectadas	B	M	A		
D	n.a.	aplica	+	mp.s.8	Protección frente a la denegación de servicio
D	n.a.	n.a.	aplica	mp.s.9	Medios alternativos

Auditoría de la seguridad

- **Auditoría de la seguridad,** periódicamente para sistemas de categoría MEDIA o ALTA, que verifique el cumplimiento del ENS.
- El informe de auditoría deberá **dictaminar sobre**
  - el grado de cumplimiento del presente real decreto,
  - identificar sus deficiencias
  - y sugerir las posibles medidas correctoras o complementarias necesarias,
  - así como las recomendaciones que se consideren oportunas.
- Los **informes de auditoría** serán presentados al responsable del sistema y al responsable de seguridad competentes. Estos informes serán analizados por este último que presentará sus conclusiones al responsable del sistema para que adopte las medidas correctoras adecuadas.

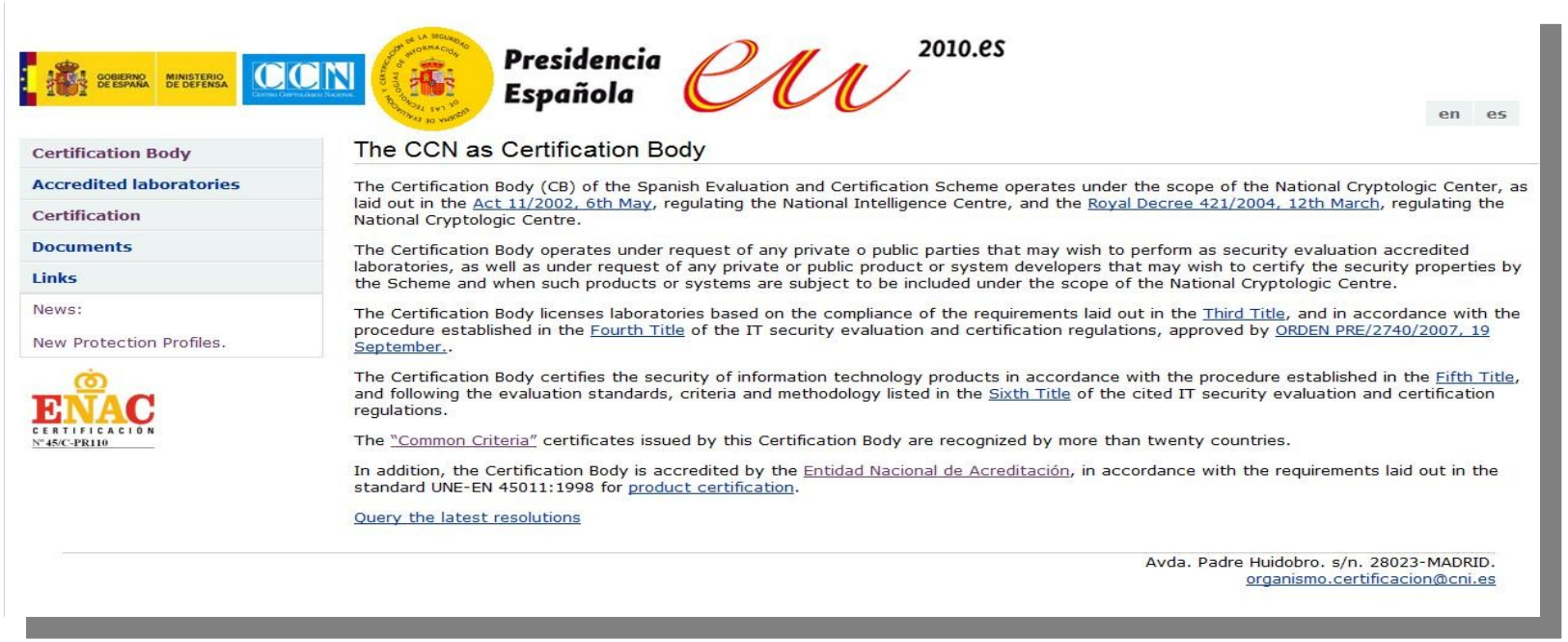
Respuesta a incidentes de seguridad

La **respuesta a incidentes de seguridad** mediante la estructura **CCN-CERT** 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 **servicios de** soporte y coordinación, investigación y divulgación, formación e información.

https://www.ccn-cert.cni.es/

Certificación

La certificación como aspecto **a considerar al adquirir productos de seguridad**, citando al Organismo de Certificación del Esquema Nacional de Evaluación y Certificación de Seguridad de las TIC (el propio Centro Criptológico Nacional).



http://www.oc.ccn.cni.es/index_en.html

Más cuestiones

- **Condiciones técnicas de notificaciones, comunicaciones-e y firma-e.**
- **Mecanismos de control.**
- **Publicación de la conformidad.**
- **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.
- **INTECO:** podrá desarrollar proyectos de innovación y programas de investigación para la mejor implantación del ENS.
- **Adecuación.** Mecanismo escalonado.

Adecuación al ENS

Los sistemas de las administraciones deberán estar adecuados a este Esquema 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).

Instrumentos para facilitar la aplicación del ENS

El reto es **facilitar la aplicación** mediante **orientaciones relativas a cuestiones** tales como:

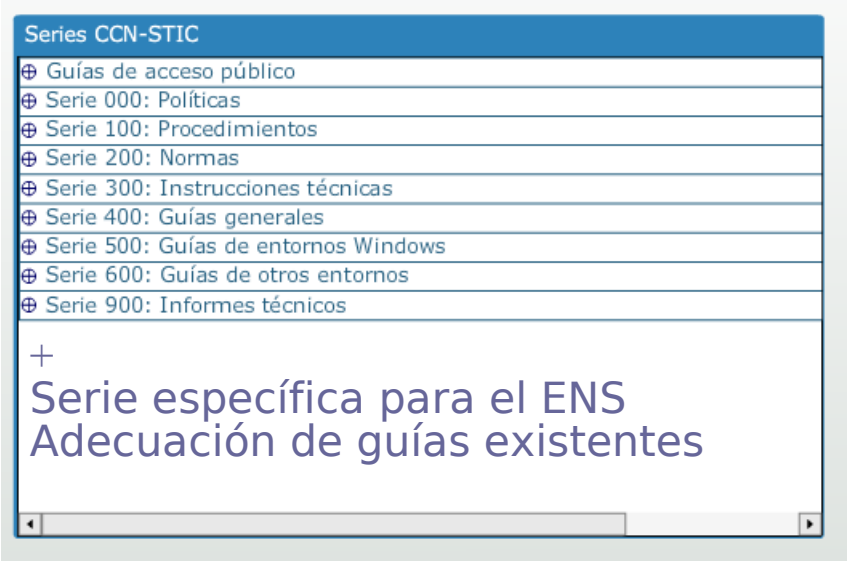
Organización y responsables

- Ámbito de aplicación,
- Análisis y gestión de riesgos,
- Categorización de los sistemas,
- Implantación de las medidas de seguridad,
- Relación con 27001, 27002, RD 1720/2007,
- Auditoría
- ...

Más **instrumentos**:

- Adecuación de PILAR al ENS.

...



https://www.ccn-cert.cni.es/

Conclusiones

- **Base legal** proporcionada por el RD 3/2010 de aplicación a todas las AA.PP.
- **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.
- **Cooperación:** Proceso coordinado por el **Ministerio de la Presidencia** con el apoyo del **Centro Criptológico Nacional (CCN) y participación de todas las AA.PP.** ; más opinión recibida del sector TIC, CRUE, etc.
- **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.
- Incluye **referencia a medidas de seguridad**; deja abierto cómo implementarlas.
- **Tiene presente el estado del arte y referentes principales** en la materia:OCDE, UE, normalización, otros países.

Muchas gracias

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

http://www.ctt.map.es/web/ens
http://www.csae.map.es/csi/pg5e42.htm
http://www.epractice.eu/en/cases/ens
https://www.ccn-cert.cni.es/index.php?lang=en
http://www.oc.ccn.cni.es/certificacion_es.htm