

Mesa redonda sobre **El Esquema Nacional de Seguridad**

Universidad de Girona

26 de mayo de 2010

Miguel A. Amutio
Ministerio de la Presidencia

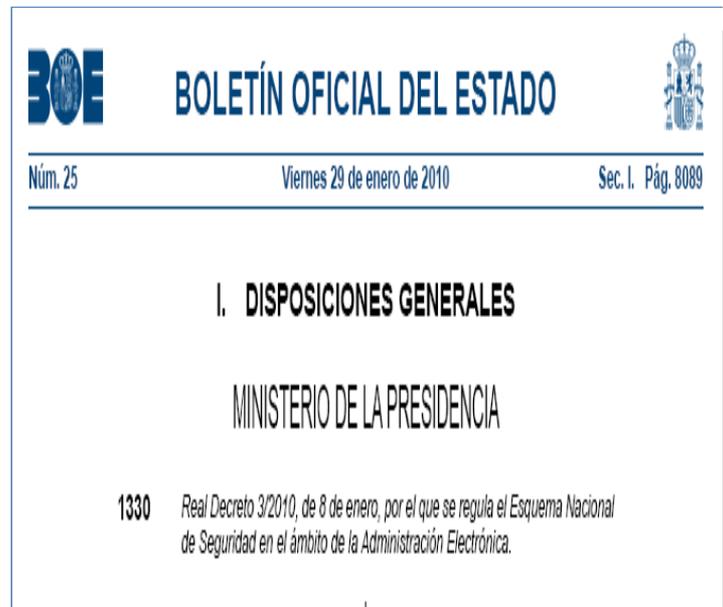


- ♦ Ley 11/2007, art. 42 -> Real Decreto 3/2010, de 8 de enero
- ♦ **Ámbito de aplicación**
- ♦ **Objetivos del ENS**
- ♦ **Elementos principales**
- ♦ **Política de seguridad**
- ♦ **Cumplimiento de los requisitos mínimos**
- ♦ **Categorización de los sistemas y Medidas de seguridad**
- ♦ **Auditoría de la seguridad**
- ♦ **Respuesta a incidentes de seguridad**
- ♦ **Certificación de productos de seguridad**
- ♦ **Más cuestiones**
- ♦ **Adecuación al Esquema Nacional de Seguridad**
- ♦ **Retos**
- ♦ **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.**, incluyendo las **Universidades Públicas** a través de la **CRUE**.
- +
- ♦ **Opinión de Industria del sector TIC**



Participación de los órganos colegiados en materia de adm.-e:

- ▶ **Comisión Permanente del Consejo Superior de Administración Electrónica (CPCSAE)**
 - Grupo de trabajo en la AGE, dependiente de la CSAE.
- ▶ **Comité Sectorial de Administración Electrónica (AGE – CCAA)**
 - Grupo de expertos del ENI del Comité Sectorial de Administración Electrónica
- ▶ **Comisión Nacional de Administración Local (CNAL)**
 - Colaboración con la FEMP
- ▶ **Colaboración MPR - CRUE-TIC.**

Participación a través de informe:

- Ministerio de Política Territorial.
- Ministerio de la Presidencia.
- Agencia Española de Protección de Datos
- Consejo de Estado.

Ampliación de la participación:

- Asociaciones del sector TIC.
- Publicación en el web del CSAE.

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.



Objetivos del ENS

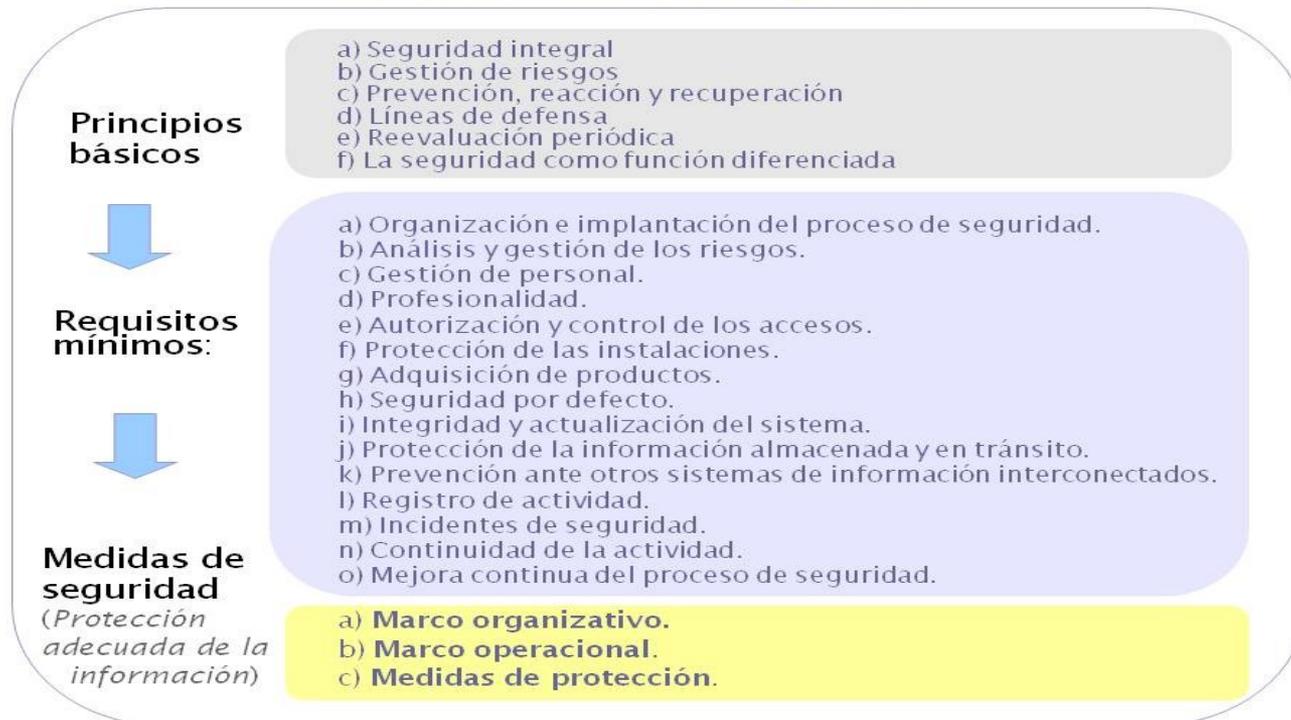
- ♦ **Crear las condiciones necesarias de confianza** en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad, que permita a los ciudadanos y a las Administraciones públicas, el ejercicio de derechos y el cumplimiento de deberes a través de estos medios.
- ♦ **Introducir 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.

- ♦ 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, del sistema 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**.

Esquema Nacional de Seguridad



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

- ♦ **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

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.

Selección de las 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.

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 requisitos 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.**

Medidas 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 logon)
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

Dimensiones				MEDIDAS DE SEGURIDAD	
Afectadas	B	M	A		
categoria	aplica	=	=	op.exp.4	Mantenimiento
categoria	n.a.	aplica	=	op.exp.5	Gestión de cambios
categoria	aplica	=	=	op.exp.6	Protección frente a código dañino
categoria	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
categoria	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
categoria	aplica	+	=	op.exp.11	Protección de claves criptográficas
				op.ext	Servicios externos
categoria	n.a.	aplica	=	op.ext.1	Contratación y acuerdos de nivel de servicio
categoria	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
categoria	n.a.	n.a.	aplica	op.mon.1	Detección de intrusión
categoria	n.a.	n.a.	aplica	op.mon.2	Sistema de métricas
				mp	Medidas de protección
				mp.if	Protección de las instalaciones e infraestructuras
categoria	aplica	=	=	mp.if.1	Áreas separadas y con control de acceso
categoria	aplica	=	=	mp.if.2	Identificación de las personas
categoria	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
categoria	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
categoria	n.a.	aplica	=	mp.per.1	Caracterización del puesto de trabajo
categoria	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,
 - 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.



The screenshot shows the CCN-CERT website with the following sections:

- Navigation Menu:** PRINCIPAL, SOBRE NOSOTROS, INCIDENTES, ACTUALIDAD, ALERTAS, HERRAMIENTAS, RECURSOS, NOTICIAS, PREFERENCIAS.
- Header:** ccn-cert seguridad tic, capacidad de respuesta ante incidentes de seguridad de la información.
- Alert Level:** NIVEL DE ALERTA MEDIO.
- ÚLTIMAS VULNERABILIDADES:**
 - CCN-CERT-1001-05047: Múltiples vulnerabilidades en Kerberos
 - CCN-CERT-1001-05046: Múltiples vulnerabilidades en PowerDNS Recursor
 - CCN-CERT-1001-05045: Múltiples vulnerabilidades en Linux kernel
- ÚLTIMOS INFORMES DE SEGURIDAD:**
 - CCN-CERT IA-03/09 Seguridad en la nube ("Cloud computing")
 - CCN-CERT ID-07/09 Informe de Código Dañino: Botnet Mariposa/Butterfly
 - CCN-CERT IS-23/09 Informe de Actualidad STIC
- SERIES CCN-STIC:**
 - CCN-STIC-001: Seguridad de las TIC en la Administración
 - CCN-STIC-002: Definición de Criptología Nacional
 - CCN-STIC-401: Glosario de términos
- HERRAMIENTA PILAR:** Procedimiento Informático Lógico para el Análisis de Riesgos (última versión)
- CURSOS CCN-STIC:**
 - VI Curso de Gestión STIC del 21 de septiembre al 30 de octubre
 - II Curso STIC - Búsqueda de Evidencias y Control de Integridad del 28 de septiembre al 2 de octubre
 - XXXI Curso de Especialidades Criptológicas (CEC) del 31 de agosto al 4 de diciembre
- NOTICIAS SEGURIDAD:**
 - Los enlaces cortos, víctimas propias a los ataques de 'phishing' - 22/01/2010
 - IPv4 se agota y la llegada de IPv6 se convierte en urgente - 21/01/2010
 - Microsoft lanzará un parche de emergencia para Internet Explorer 6 - 20/01/2010
- COMUNICADOS CCN-CERT:**
 - El CCN, en colaboración con la Xunta de Galicia, presenta en Santiago su Servicio de Respuesta a Incidentes - 30/12/2009
 - Más de trescientas personas provenientes de la AAPP asistieron a la III Jornada STIC organizada por el CCN-CERT - 18/12/2009
 - El CCN-CERT amplía su oferta educativa para el personal de la AAPP con una nueva plataforma de e-learning - 28/10/2009
- Other Features:**
 - CATÁLOGO DE SERVICIOS: descárgate aquí CCN-CERT
 - Curso on-line de Seguridad de la Información
 - SISTEMA MULTIANTIVIRUS: MAV
 - MENCIONES: FIRST, EGC group
 - ABRIR SESIÓN
 - ¿Por qué debería registrarme?
 - ¿Quieres notificar un incidente?

AVISO LEGAL - CONTACTO - MAPA WEB - DECLARACIÓN DE ACCESIBILIDAD
© 2009 Centro Criptológico Nacional - C/Argenta s/n 28023 MADRID

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).




2010.es

en es

<p>Organismo de certificación</p> <p>Acreditación de laboratorios</p> <p>Certificación</p> <p>Documentos</p> <p>Enlaces</p> <p>Novedades:</p> <p>Firma del Acuerdo Europeo SOGIS MRA v3 de Reconocimiento Mutuo de Certificados de Seguridad de Productos TIC.</p> 	<h2>El CCN como Organismo de Certificación</h2> <p>El Organismo de Certificación (OC) del Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información (ENECSTI) se articula en el ámbito de actuación del Centro Criptológico Nacional, según lo dispuesto respectivamente en la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia, y el Real Decreto 421/2004, de 12 de marzo, por el que se regula el Centro Criptológico Nacional.</p> <p>El ámbito de actuación del Organismo de Certificación comprende a las entidades públicas o privadas que quieran ejercer de laboratorios de evaluación de la seguridad de las TI en el marco del Esquema, y a las entidades públicas o privadas fabricantes de productos o sistemas de TI que quieran 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.</p> <p>El Organismo de Certificación acredita a los laboratorios solicitantes en base al cumplimiento de los requisitos establecidos en el Capítulo III. Requisitos de acreditación de laboratorios, y según el procedimiento indicado en el Capítulo IV. Acreditación de laboratorios del Reglamento de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información, aprobado en la ORDEN PRE/2740/2007, de 19 de septiembre..</p> <p>El Organismo de Certificación certifica la seguridad de productos y sistemas de Tecnologías de la información, según lo establecido en el procedimiento del Capítulo V. Certificación de productos y sistemas, y atendiendo a los criterios, métodos y normas de evaluación de la seguridad indicados en el Capítulo VI. Criterios y metodologías de evaluación del citado Reglamento de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información.</p> <p>Los certificados "Common Criteria" emitidos por el Organismo de Certificación están reconocidos internacionalmente por más de veinte países.</p> <p>Adicionalmente, el Organismo de Certificación está acreditado por la Entidad Nacional de Acreditación, conforme a los criterios recogidos en la Norma UNE-EN 45011:1998 para la certificación de productos.</p> <p>Consulta de últimas resoluciones en el BOE</p>
---	---

Avda. Padre Huidobro. s/n. 28023-MADRID.
organismo.certificacion@cni.es

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

- ♦ **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.
- ♦ **Papel de INTECO y de organismos análogos.**
- ♦ **Adecuación.** Mecanismo escalonado.

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.

Retos (I)

Proporcionar orientaciones relativas a cuestiones como:

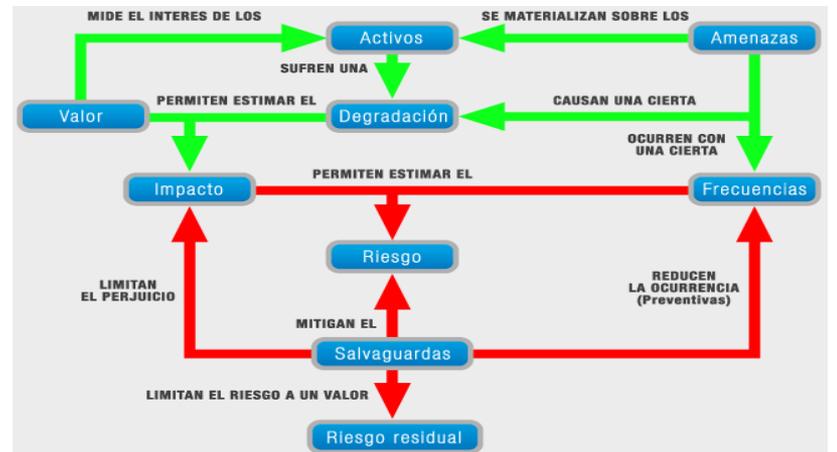
- Organización y responsables
- Ámbito de aplicación
- Análisis y gestión de riesgos,
- Categorización de los sistemas,
- Implantación de las medidas de seguridad,
- Relación con ISO/IEC 27001, ISO/IEC 27002, RD 1720/2007,
- Auditoría
- ...

Más instrumentos:

- Por ejemplo, adecuación de PILAR al ENS.

...

Series CCN-STIC	
+	Guías de acceso público
+	Serie 000: Políticas
+	Serie 100: Procedimientos
+	Serie 200: Normas
+	Serie 300: Instrucciones técnicas
+	Serie 400: Guías generales
+	Serie 500: Guías de entornos Windows
+	Serie 600: Guías de otros entornos
+	Serie 900: Informes técnicos
+ Serie específica para el ENS Adecuación de guías existentes	



Abordar la adecuación (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**).

A destacar lo siguiente:

- Establecer roles, funciones, procedimientos de designación.
- Precisar los criterios para la categorización de los sistemas.
- Identificar la información y los servicios. Identificación de los responsables y valoración.
- Análisis de riesgos y revisión del cumplimiento del Anexo II.
- Elaborar un plan para pleno cumplimiento del ENS.

Conclusiones

- ♦ **Base legal** proporcionada por el RD 3/2010 de aplicación a todas las AA.PP.
- ♦ **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.
- ♦ **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.
- ♦ 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.csaemap.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