



**ens**  
Esquema Nacional de  
Seguridad



Septiembre de 2010



## Presentación

**FORO:** Seminario “El Nuevo Esquema Nacional de Seguridad”

**PONENTE:** Centro Criptológico Nacional

**FECHA:** 30 de septiembre de 2010

- 1. Introducción**
- 2. Marco Legal**
- 3. Guías de desarrollo del ENS**
- 4. PILAR**
- 5. CCN-CERT**
- 6. Conclusiones.**

## 1. Introducción

### ¿Qué es el Esquema Nacional de Seguridad (ENS)?

El Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, regula el citado Esquema previsto en el artículo 42 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos. Su objeto es establecer la política de seguridad en la utilización de medios electrónicos y está constituido por principios básicos y requisitos mínimos que permitan una protección adecuada de la información.

## 1. Introducción

### ¿Es el ENS de obligado cumplimiento para todas las Administraciones Públicas?

El ámbito de aplicación del Esquema Nacional de Seguridad es el establecido en el artículo 2 de la Ley 11/2007:

- 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 regulada por Ley 9/1968, de 5 de abril, de Secretos Oficiales y sus normas de desarrollo.

## 1. Introducción

### ¿Cuál es el impacto del ENS en los sistemas actuales?

Todos los sistemas existentes deben adecuarse al ENS en un plazo de 12 meses desde su aprobación, aunque si hubiera circunstancias que impidieran la plena aplicación, se dispondrá de un plan de adecuación que marque los plazos de ejecución, en ningún caso superior a 48 meses desde la entrada en vigor del esquema.

## 2. Marco Legal



### El CCN actúa según el siguiente marco legal:

Ley 11/2002, 6 de mayo, reguladora del Centro Nacional de Inteligencia (CNI), que incluye al Centro Criptológico Nacional (CCN).



Real Decreto 421/2004, 12 de marzo, que regula y define el ámbito y funciones del CCN.



Orden Ministerio Presidencia PRE/2740/2007, de 19 de septiembre, que regula el Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información



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

### 3. Guías de desarrollo del ENS

El Real Decreto 3/2010 de 8 de Enero de desarrollo del Esquema Nacional de Seguridad fija los principios básicos y requisitos mínimos así como las medidas de protección a implantar en los sistemas de la Administración, y promueve la elaboración y difusión de guías de seguridad de las tecnologías de la información y las comunicaciones por parte de CCN para facilitar un mejor cumplimiento de dichos requisitos mínimos.

La serie de documentos CCN-STIC se elabora para dar cumplimiento a los cometidos del Centro Criptológico Nacional y a lo reflejado en el Esquema Nacional de Seguridad.

### 3. Guías de desarrollo del ENS

## Serie 800

### Glosario de términos y abreviaturas

Versión: 09-08-2010 (borrador)

**Recoge aquellos términos y abreviaturas utilizados en las guías de desarrollo del Esquema Nacional de Seguridad.**

• **CCN-STIC-800**

• CCN-STIC-801

• CCN-STIC-802

• CCN-STIC-803

• CCN-STIC-804

• CCN-STIC-805

• CCN-STIC-806

• CCN-STIC-807

• CCN-STIC-808

• CCN-STIC-809

• CCN-STIC-810

• CCN-STIC-811

• CCN-STIC-812

### 3. Guías de desarrollo del ENS

## Serie 800

### Responsables y funciones

Versión: 20-07-2010 (borrador)

**El objeto de esta guía es crear un marco de referencia que establezca las responsabilidades generales en la gestión de la seguridad de los Sistemas, así como proponer unas figuras o roles de seguridad que las implementen.**

• CCN-STIC-800

• **CCN-STIC-801**

• CCN-STIC-802

• CCN-STIC-803

• CCN-STIC-804

• CCN-STIC-805

• CCN-STIC-806

• CCN-STIC-807

• CCN-STIC-808

• CCN-STIC-809

• CCN-STIC-810

• CCN-STIC-811

• CCN-STIC-812

### 3. Guías de desarrollo del ENS

## Serie 800

### Guía de auditoría

Versión: junio 2010

Esta guía de auditoría del Esquema Nacional de Seguridad se encuadra dentro de lo previsto en el artículo 42 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, y específicamente dentro de los requisitos del artículo 34 (Auditoría de la seguridad), y del Anexo III (Auditoría de la Seguridad) del 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 (RD 3/2010 en adelante).

• CCN-STIC-800

• CCN-STIC-801

• **CCN-STIC-802**

• CCN-STIC-803

• CCN-STIC-804

• CCN-STIC-805

• CCN-STIC-806

• CCN-STIC-807

• CCN-STIC-808

• CCN-STIC-809

• CCN-STIC-810

• CCN-STIC-811

• CCN-STIC-812

### 3. Guías de desarrollo del ENS

## Serie 800

### Valoración de los sistemas

Versión: julio 2010

El Esquema Nacional de Seguridad establece una serie de medidas de protección en su Anexo II que están condicionadas a la valoración del nivel de seguridad en cada dimensión, y a la categoría (artículo 43) del sistema de información de que se trate. A su vez, la categoría del sistema se calcula en función del nivel de seguridad en cada dimensión. Esta guía establece unas pautas de carácter general que son aplicables a entidades de distinta naturaleza, dimensión y sensibilidad sin entrar en casuísticas particulares.

• CCN-STIC-800

• CCN-STIC-801

• CCN-STIC-802

• **CCN-STIC-803**

• CCN-STIC-804

• CCN-STIC-805

• CCN-STIC-806

• CCN-STIC-807

• CCN-STIC-808

• CCN-STIC-809

• CCN-STIC-810

• CCN-STIC-811

• CCN-STIC-812

### 3. Guías de desarrollo del ENS

## Serie 800

### Guía de implantación

Versión: 23-07-2010 (borrador)

El Esquema Nacional de Seguridad establece una serie de medidas de seguridad en su Anexo II que están condicionadas a la valoración del nivel de seguridad en cada dimensión, y a la categoría (artículo 43) del sistema de información de que se trate. A su vez, la categoría del sistema se calcula en función del nivel de seguridad en cada dimensión. Esta guía establece unas pautas de carácter general que son aplicables a entidades de distinta naturaleza, dimensión y sensibilidad sin entrar en casuísticas particulares.

• CCN-STIC-800

• CCN-STIC-801

• CCN-STIC-802

• CCN-STIC-803

• **CCN-STIC-804**

• CCN-STIC-805

• CCN-STIC-806

• CCN-STIC-807

• CCN-STIC-808

• CCN-STIC-809

• CCN-STIC-810

• CCN-STIC-811

• CCN-STIC-812

### 3. Guías de desarrollo del ENS

## Serie 800

### Política de seguridad de la información

Versión: 16-08-2010 (borrador)

**La Política de Seguridad de la Información es un documento de alto nivel que define lo que significa 'seguridad de la información' en una organización. El documento debe estar accesible por todos los miembros de la organización y redactado de forma sencilla, precisa y comprensible.**

- CCN-STIC-800
- CCN-STIC-801
- CCN-STIC-802
- CCN-STIC-803
- CCN-STIC-804
- **CCN-STIC-805**
- CCN-STIC-806

- CCN-STIC-807
- CCN-STIC-808
- CCN-STIC-809
- CCN-STIC-810
- CCN-STIC-811
- CCN-STIC-812

### 3. Guías de desarrollo del ENS

## Serie 800

### Plan de adecuación

Versión: 03-08-2010 (borrador)

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.

- CCN-STIC-800
- CCN-STIC-801
- CCN-STIC-802
- CCN-STIC-803
- CCN-STIC-804
- CCN-STIC-805
- **CCN-STIC-806**

- CCN-STIC-807
- CCN-STIC-808
- CCN-STIC-809
- CCN-STIC-810
- CCN-STIC-811
- CCN-STIC-812

### 3. Guías de desarrollo del ENS

## Serie 800

### Criptología de empleo en el ENS

Versión: XX-XX-XXX (borrador)

La presente guía tiene por objeto especificar las medidas de criptología necesarias a implementar en los diferentes sistemas dependiendo del nivel que tenga asignado.

- CCN-STIC-800
- CCN-STIC-801
- CCN-STIC-802
- CCN-STIC-803
- CCN-STIC-804
- CCN-STIC-805
- CCN-STIC-806

- **CCN-STIC-807**
- CCN-STIC-808
- CCN-STIC-809
- CCN-STIC-810
- CCN-STIC-811
- CCN-STIC-812

### 3. Guías de desarrollo del ENS

## Serie 800

### Verificación de cumplimiento

Versión: XX-XX-XXX (borrador)

**El objeto de esta guía es que sirva tanto de itinerario, como de registro, a aquella persona designada como auditor de los requisitos del Esquema Nacional de Seguridad para un sistema.**

- CCN-STIC-800
- CCN-STIC-801
- CCN-STIC-802
- CCN-STIC-803
- CCN-STIC-804
- CCN-STIC-805
- CCN-STIC-806

- CCN-STIC-807
- **CCN-STIC-808**
- CCN-STIC-809
- CCN-STIC-810
- CCN-STIC-811
- CCN-STIC-812

### 3. Guías de desarrollo del ENS

## Serie 800

### Declaración de conformidad

Versión: 29-07-2010 (borrador)

**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.**

- CCN-STIC-800
- CCN-STIC-801
- CCN-STIC-802
- CCN-STIC-803
- CCN-STIC-804
- CCN-STIC-805
- CCN-STIC-806

- CCN-STIC-807
- CCN-STIC-808
- **CCN-STIC-809**
- CCN-STIC-810
- CCN-STIC-811
- CCN-STIC-812

### 3. Guías de desarrollo del ENS

## Serie 800

### Creación de CERTs

Versión: XX-XX-XXX (borrador)

**Esta Guía pretende ser un instrumento eficaz que facilite una visión global de todas las implicaciones (no sólo tecnológicas) que conlleva la puesta en marcha de estos equipos, tanto en su diseño como en el desarrollo y posterior funcionamiento, especialmente entre las administraciones públicas.**

- CCN-STIC-800
- CCN-STIC-801
- CCN-STIC-802
- CCN-STIC-803
- CCN-STIC-804
- CCN-STIC-805
- CCN-STIC-806

- CCN-STIC-807
- CCN-STIC-808
- CCN-STIC-809
- **CCN-STIC-810**
- CCN-STIC-811
- CCN-STIC-812

### 3. Guías de desarrollo del ENS

## Serie 800

### Interconexión en el ENS

Versión: XX-XX-XXX (borrador)

**En estudio.**

- CCN-STIC-800
- CCN-STIC-801
- CCN-STIC-802
- CCN-STIC-803
- CCN-STIC-804
- CCN-STIC-805
- CCN-STIC-806

- CCN-STIC-807
- CCN-STIC-808
- CCN-STIC-809
- CCN-STIC-810
- **CCN-STIC-811**
- CCN-STIC-812

### 3. Guías de desarrollo del ENS

## Serie 800

### Herramientas de seguridad en el ENS

Versión: XX-XX-XXX (borrador)

**En estudio.**

- CCN-STIC-800
- CCN-STIC-801
- CCN-STIC-802
- CCN-STIC-803
- CCN-STIC-804
- CCN-STIC-805
- CCN-STIC-806

- CCN-STIC-807
- CCN-STIC-808
- CCN-STIC-809
- CCN-STIC-810
- CCN-STIC-811
- **CCN-STIC-812**

## 4. PILAR

- **HERRAMIENTA PILAR.**
  - **Análisis de Riesgos formal con metodología MAGERIT**
  - **Uso libre para la administración**
  - **Perfil del ENS**
  - **Funcionalidades 2010**
- **PILAR-ENS**
  - **Cumplimentar principios básicos y requisitos mínimos**
  - **Apoyo en la realización de las auditorías**

## 5. CCN-CERT



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



NIVEL DE ALERTA  
**ALTO**

- CASTELLANO
- ENGLISH
- CATALA
- EUSKARA
- GALEGO
- VALENCIA

**ABRIR SESIÓN**

- PRINCIPAL
- SOBRE NOSOTROS
- INCIDENTES
- ACTUALIDAD CCN-CERT
- ALERTAS
- HERRAMIENTAS
- RECURSOS
- NOTICIAS
- PREFERENCIAS

### ÚLTIMAS VULNERABILIDADES

- CCN-CERT-1009-05492  
Ejecución remota de código en Windows Media...
- CCN-CERT-1009-05491  
Ejecución remota de código en el procesador de S...
- CCN-CERT-1009-05490  
Ejecución remota de código en Microsoft Windows...

[ver más...](#)

### ÚLTIMOS INFORMES DE SEGURIDAD

- CCN-CERT IA-05-10 Ataques DDoS 2010. Últimas motivaciones y métodos utilizados...
- CCN-CERT ID-07/09 Informe de Código Dañino: Botnet Mari... Este informe analiza el funcionamiento, infección, ejecuci...
- CCN-CERT\_JS-18-10 Informe de Actualidad STIC Plataforma Volatility 1.4; Izeus, el primer troyano bancario para Mac Os X; 2010; réc...

[ver más...](#)

**Servicios S.A.T.**  
CCN-CERT  
Sistema de Alerta Temprana

**ens**  
Esquema Nacional de Seguridad

### 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

[ver más...](#)

### HERRAMIENTA PILAR

Procedimiento Informático Lógico para el Análisis de Riesgos (última versión)

[ver más...](#)

### CURSOS CCN-STIC

- XXII Curso de Especialidades Criptológicas (CEC) del 30 de agosto al 03 de diciembre
- VI Curso de Especialización STIC - Cortafuegos del 13 al 17 de septiembre
- VII Curso de Gestión STIC del 20 de septiembre al 15 de octubre

buscar...

**III Jornada STIC**  
CCN-CERT  
Las AAPP ante las nuevas amenazas

Curso on-line de Seguridad de la Información

SISTEMA MULTIAVIRUS  
**MAV**

MENCIONES

## 5. CCN-CERT

### CAPÍTULO VII

#### Respuesta a incidentes de seguridad

Artículo 36. *Capacidad de respuesta a incidentes de seguridad de la información.*

El Centro Criptológico Nacional (CCN) articulará la respuesta a los incidentes de seguridad en torno a la estructura denominada CCN-CERT (Centro Criptológico Nacional-Computer Emergency Reaction Team), que actuará sin perjuicio de las capacidades de respuesta a incidentes de seguridad que pueda tener cada administración pública y de la función de coordinación a nivel nacional e internacional del CCN.

Artículo 37. *Prestación de servicios de respuesta a incidentes de seguridad a las Administraciones públicas.*

1. De acuerdo con lo previsto en el artículo 36, el CCN-CERT prestará a las Administraciones públicas los siguientes servicios:

## 5. CCN-CERT

### Artículo 37. *Prestación de servicios de respuesta a incidentes de seguridad a las Administraciones públicas.*

1. De acuerdo con lo previsto en el artículo 36, el CCN-CERT prestará a las Administraciones públicas los siguientes servicios:

a) Soporte y coordinación para el **tratamiento de vulnerabilidades y la resolución de incidentes de seguridad** que tengan la Administración General del Estado, las Administraciones de las comunidades autónomas, las entidades que integran la Administración Local y las Entidades de Derecho público con personalidad jurídica propia vinculadas o dependientes de cualquiera de las administraciones indicadas.

El CCN-CERT, a través de su servicio de apoyo técnico y de coordinación, **actuará con la máxima celeridad ante cualquier agresión recibida** en los sistemas de información de las Administraciones públicas. Para el cumplimiento de los fines indicados en los párrafos anteriores se podrán recabar los informes de auditoría de los sistemas afectados.

b) Investigación y divulgación de las mejores prácticas sobre seguridad de la información entre todos los miembros de las Administraciones públicas. Con esta finalidad, las **series de documentos CCN-STIC** (Centro Criptológico Nacional-Seguridad de las Tecnologías de Información y Comunicaciones), elaboradas por el Centro Criptológico Nacional, ofrecerán normas, instrucciones, guías y recomendaciones para aplicar el Esquema Nacional de Seguridad y para garantizar la seguridad de los sistemas de tecnologías de la información en la Administración.

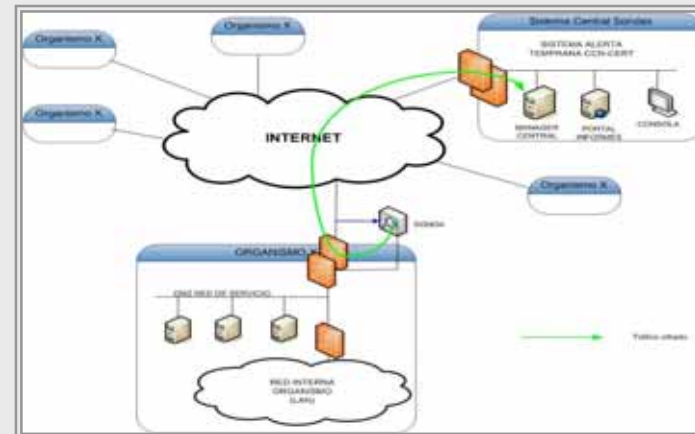
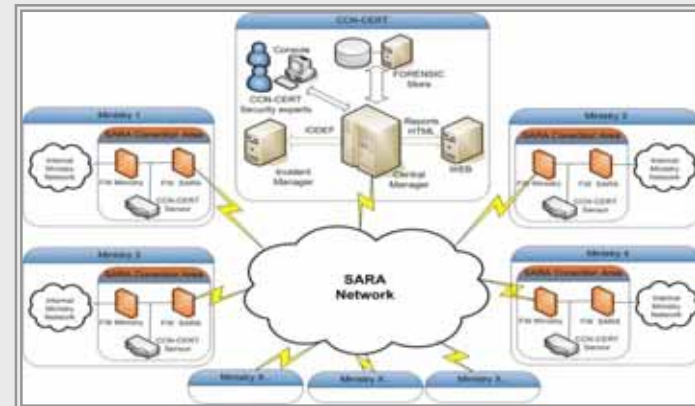
c) **Formación** destinada al personal de la Administración especialista en el campo de la seguridad de las tecnologías de la información, al objeto de facilitar la actualización de conocimientos del personal de la Administración y de lograr la sensibilización y mejora de sus capacidades para la detección y gestión de incidentes.

d) **Información sobre vulnerabilidades, alertas y avisos de nuevas amenazas** a los sistemas de información, recopiladas de diversas fuentes de reconocido prestigio, incluidas las propias.

2. El CCN desarrollará un programa que ofrezca la información, formación, recomendaciones y herramientas necesarias para que las Administraciones públicas puedan desarrollar **sus propias capacidades de respuesta a incidentes de seguridad**, y en el que, aquél, será coordinador a nivel público estatal.

## 5. CCN-CERT. Sistema de Alerta Temprana (S.A.T.)

- **RED SARA:**
  - Servicio para la Intranet Administrativa.
  - Coordinado con M<sup>o</sup> Presidencia.
  - Portal de Informes.
  
- **SONDAS SALIDAS DE INTERNET AAPP:**
  - Servicio por suscripción de los Organismos.
  - Despliegue de sensores.
  - Portal de Informes.
  
- **BENEFICIOS:**
  - Detección de ataques.
  - Estadísticas propias y patrones de ataque.
  - Actualización de Firmas.




F O R M A C I Ó N



# Centro Criptológico Nacional 2010

	Lunes	Martes	Miércoles	Jueves	Viernes	Sábado	Domingo	Lunes	Martes	Miércoles	Jueves	Viernes	Sábado	Domingo	Lunes	Martes	Miércoles	Jueves	Viernes	Sábado	Domingo	Lunes	Martes	Miércoles	Jueves	Viernes	Sábado	Domingo	Lunes	Martes				
<b>ENE</b>				1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
<b>FEB</b>							1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
<b>MAR</b>	VI Curso STIC - Fase de Correspondencia - Defensa																																	
	VII Curso STIC - Fase de Correspondencia																																	
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31			
<b>ABR</b>				1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	
	VI Curso STIC										VI Curso STIC					V Curso Básico STIC Entornos Windows					VII Curso Acreditación STIC Entornos Windows													
	VI Curso STIC										VII Curso STIC					VII Curso STIC																		
<b>MAY</b>				1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	VI Curso STIC										V Curso Básico STIC Entornos Linux					V Curso Básico STIC Base de Datos					V Curso STIC Redes Inalámbricas													
<b>JUN</b>				1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	
	V Curso Básico STIC Infraestructura de Red										III Curso Common Criteria																							
<b>JUL</b>				1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
<b>AGO</b>				1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
<b>SEP</b>				1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	
	VI Curso STIC Cortafuegos										VI Curso STIC Detección de Intrusos					III Curso STIC Búsqueda Evidencias																		
	XXII Curso de Especialidades Criptológicas (correspondencia)																																	
	VII Curso Gestión STIC (Correspondencia)																																	
<b>OCT</b>				1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	
	V Curso STIC Inspecciones de Seguridad										II Jornada de Seguridad en Aplicaciones Web					VII Curso Gestión STIC (Presencial)																		
	VII Curso Gestión STIC (Presencial)																																	
	XXII Curso de Especialidades Criptológicas (correspondencia)																																	
	VII Curso Gestión STIC (Presencial)																																	
<b>NOV</b>				1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	
	XXI CEC (Correspondencia)					XXII CEC					XXII Curso de Especialidades Criptológicas (presencial)					XXII Curso de Especialidades Criptológicas (presencial)					XXII CEC													
<b>DIC</b>				1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	XXII CEC					X Curso Herramienta PILAR																												

## 5. Organismo de Certificación (OC)

- a. Elaborar y difundir normas, instrucciones, guías y recomendaciones para garantizar la seguridad de las TIC en la Administración.
- b. Formar al personal de la Administración especialista en el campo de la seguridad de las TIC.
-  **c. Constituir el organismo de certificación del Esquema Nacional de Evaluación y Certificación de aplicación a productos y sistemas de su ámbito.**
- d. Valorar y acreditar capacidad productos de cifra y Sistemas de las TIC (incluyan medios de cifra) para manejar información de forma segura.
- e. Coordinar la promoción, el desarrollo, la obtención, la adquisición y puesta en explotación y la utilización de la tecnología de seguridad de los Sistemas antes mencionados.
- f. Velar por el cumplimiento normativa relativa a la protección de la información clasificada en su ámbito de competencia.
- g. Establecer las necesarias relaciones y firmar los acuerdos pertinentes con organizaciones similares de otros países, para el desarrollo de las funciones mencionadas.

## 6. Conclusiones

- El Esquema Nacional de Seguridad es un **instrumento al servicio del desarrollo de la administración electrónica**, en cuanto a la creación de condiciones de confianza en el uso de los medios electrónicos por medio de la garantía de seguridad de los sistemas, los datos, las comunicaciones y los servicios electrónicos.
- Está constituido por **principios básicos y requisitos mínimos** que permitan una protección adecuada de la información.
- **Aplica el análisis y gestión de riesgos** para satisfacer principios de proporcionalidad y seguridad.
- **Para la implementación y detalles** se remite a diversos instrumentos, herramientas, servicios e infraestructuras disponibles.

MUCHAS GRACIAS

[ens@ccn-cert.cni.es](mailto:ens@ccn-cert.cni.es)

[organismo.certificacion@cni.es](mailto:organismo.certificacion@cni.es)



The screenshot displays the official website of the Centro Criptológico Nacional (CCN). The main header features the CCN logo and the text 'CENTRO CRIPTOLÓGICO NACIONAL'. Below this, there are navigation tabs for 'Inicio', 'Normas', 'Certificación', 'Actualización', 'Formación', and 'Servicio de Soporte'. The central content area is titled 'CERTIFICACIÓN' and lists various services: 'CERTIFICACIÓN DE SEGURIDAD', 'CERTIFICACIÓN DE SOFTWARE', and 'CERTIFICACIÓN FUNCIONAL'. A sidebar on the left contains links for 'Últimas Noticias', 'Cada día RED', 'Ámbito de actuación', 'Contacto', and 'Organismo de Certificación'. The footer includes the CCN logo, the text 'CCN-CERT', and the address 'C/ Arzobispo Morcillo, 42, 28014 Madrid, España'. The page also features a search bar and a language selector.