



GOBIERNO  
DE ESPAÑA

MINISTERIO  
DE HACIENDA  
Y ADMINISTRACIONES PÚBLICAS

MINISTERIO  
DE INDUSTRIA, ENERGÍA  
Y TURISMO

red.es



Abogacía  
Española  
CONSEJO GENERAL



## ESQUEMA NACIONAL DE SEGURIDAD PARA COLEGIOS PROFESIONALES

**27 de mayo de 2013,**

a las 10:30 horas

Salón de Actos del Consejo General de la Abogacía Española,  
Paseo de Recoletos, 13 – 28004 Madrid

# Adecuación al Esquema Nacional de Seguridad

Madrid, 27 de mayo de 2013

Miguel A. Amutio Gómez

Jefe de Área de Planificación y Explotación

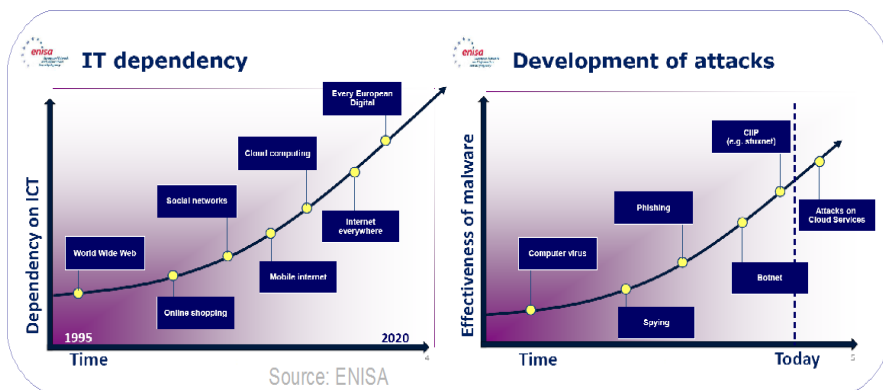
Ministerio de Hacienda y Administraciones Públicas



- 1. Por qué** es necesaria la seguridad de la información y los servicios.
- 2. La seguridad en el marco legal** de la administración electrónica.
- 3. Implantar la seguridad** en la administración electrónica → **adecuarse al Esquema Nacional de Seguridad.**
- 4. Dónde estamos.**
- 5. Retos y conclusiones.**

# Por qué es necesaria la seguridad de información y servicios

- ✓ Los ciudadanos esperan que los servicios se presten en unas condiciones de **confianza y seguridad** equivalentes a las que encuentran cuando se acercan personalmente a las oficinas de las Administración.
- ✓ Buena parte de los sistemas de información de las AA.PP., la información contenida en ellos y los servicios que prestan constituyen **activos nacionales estratégicos**.
- ✓ Los servicios se prestan en un **escenario complejo** que requiere **cooperación**.
- ✓ La información y los servicios están **sometidos a riesgos** provenientes de acciones malintencionadas o ilícitas, errores o fallos y accidentes o desastres.





## **2. La seguridad en el marco legal de la administración electrónica.**



# La seguridad en el marco legal de la Administración Electrónica

La Ley 11/2007 de acceso electrónico de los ciudadanos a los Servicios Públicos **reconoce el derecho de los ciudadanos a relacionarse a través de medios electrónicos con las AA.PP.**



Este reconocimiento implica la **obligación de las AA.PP. de promoción de las condiciones de confianza y seguridad** mediante la aplicación segura de las tecnologías.

Diversos **principios** de la Ley 11/2007 se refieren a la seguridad:

- ✓ El **principio de derecho a la protección de los datos de carácter personal**.
- ✓ El **principio de seguridad** en la implantación y utilización de los medios electrónicos.
- ✓ El **principio de proporcionalidad** → garantías y medidas de seguridad adecuadas a la naturaleza y circunstancias de los trámites y actuaciones.

La seguridad figura también entre los **derechos** de los ciudadanos:

- ✓ **Derecho a la garantía de la seguridad y confidencialidad de los datos** que figuren en los ficheros, sistemas y aplicaciones de las AA.PP.

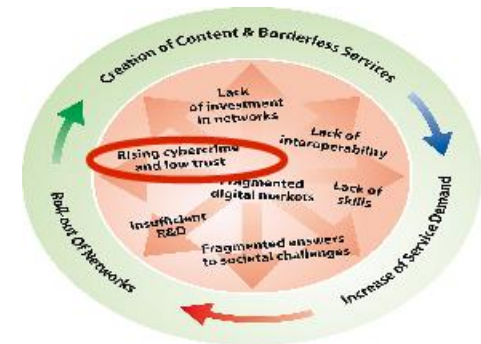
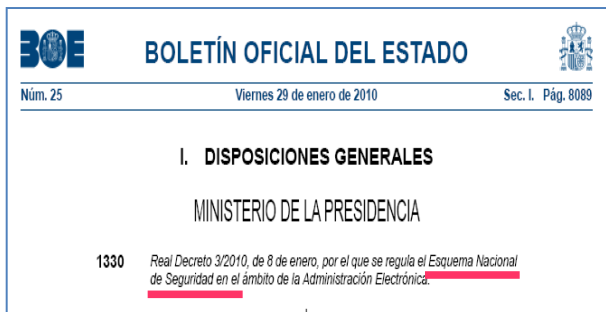


La Ley 11/2007 **crea el Esquema Nacional de Seguridad.**



# El Esquema Nacional de Seguridad

- ✓ **Es un instrumento legal – Real Decreto 3/2010-** que desarrolla lo previsto sobre seguridad en la Ley 11/2007.
- ✓ **Establece la política de seguridad** en los servicios de administración-e.
  - ⤴ Está **constituida por principios básicos y requisitos mínimos** que permitan una **protección adecuada** de la información.
- ✓ **Es de aplicación a todas las AA.PP.**
  - ⤴ Están excluidos los sistemas que manejan la información clasificada.
- ✓ Establece un **mecanismo de adecuación escalonado** (fecha límite 29.01.2014).
- ✓ Resulta de un **esfuerzo colectivo**: AGE, CC.AA., CC.LL.-FEMP, CRUE + Opinión Industria TIC.



Agenda Digital Europea



# 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 AA.PP., **el ejercicio de derechos y el cumplimiento de deberes a través de estos medios.**
- ✓ **Promover la gestión continuada de la seguridad**, al margen de impulsos puntuales, o de su ausencia.
- ✓ **Promover un tratamiento homogéneo de la seguridad** que facilite la cooperación en la prestación de servicios de administración electrónica cuando participan diversas entidades.
- ✓ **Proporcionar 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 y la cooperación de las AA.PP.
  - Para facilitar la comunicación de los requisitos de seguridad de la información a la Industria.
- ✓ **Proporcionar liderazgo en materia de buenas practicas.**
- ✓ **Estimular a la Industria del sector TIC.**



# Elementos principales

- ◆ Los **Principios básicos**, que sirven de guía.
- ◆ Los **Requisitos mínimos**, de obligado cumplimiento.
- ◆ La **Categorización de los sistemas** para la adopción de **medidas de seguridad** proporcionadas.
- ◆ La **auditoría de la seguridad** que verifique el cumplimiento del Esquema Nacional de Seguridad.
- ◆ La **respuesta a incidentes de seguridad**. Papel de CCN- CERT.
- ◆ El uso de **productos certificados**. La certificación, como aspecto a considerar al adquirir los productos de seguridad. Papel del Organismo de Certificación (CCN).
- ◆ La **formación y concienciación**.

## 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

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

**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.



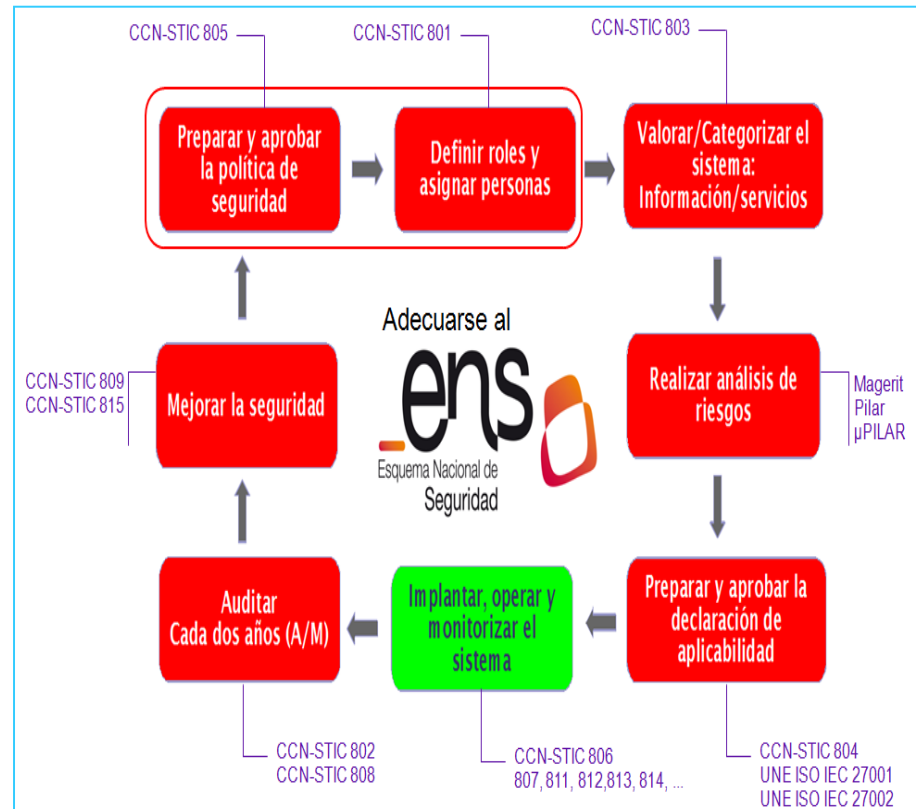
### **3. Implantar la seguridad** en la administración electrónica → **adecuarse al Esquema Nacional de Seguridad.**



# Adecuarse al ENS

## Aspectos principales de la adecuación:

- Se dispone de una **política de seguridad** aprobada (art. 11)
- **Responsables** y asignación de personas. **Responsable de seguridad.** (art. 10)
- Se ha realizado la **categorización** de los sistemas (art. 27)
- **El análisis de riesgos** está actualizado (art. 27)
- Se dispone de una **declaración de aplicabilidad** (anexo II)
- Se dispone de un **plan de adecuación / de mejora** de la seguridad aprobado (d.t)
- Se han implantado las **medidas de seguridad** (Anexo II).
- Se da publicidad a la **conformidad** en la sede electrónica (art. 41)





# Herramientas para adecuarse al ENS

1. **Priorizar**
2. **Usar infraestructuras y servicios comunes**
3. **Usar guías e instrumentos específicos**
4. **Usar la normalización**
5. **Comunicar incidentes de seguridad**
6. **Usar productos certificados**
7. **Preguntar**
8. **Formarse**

<b>Política de seguridad</b> <ul style="list-style-type: none"><li>· Principios básicos</li><li>· Requisitos mínimos</li><li>· Medidas y proporcionalidad</li></ul>	
<b>Guías de seguridad e instrumentos de apoyo</b> <ul style="list-style-type: none"><li>• Guías CCN-STIC</li><li>• Programas de apoyo: PILAR, μPILAR</li><li>• Magerit v2</li></ul>	 
<b>Normalización</b> <ul style="list-style-type: none"><li>• Normalización STIC nacional e internacional (27001, 27002, ...)</li></ul>	
<b>Infraestructuras y servicios comunes</b>	   
<b>Formación</b>	



# Usar infraestructuras y servicios comunes



## Artículo 28. Infraestructuras y servicios comunes.

La utilización de infraestructuras y servicios comunes reconocidos en las Administraciones Públicas facilitará el cumplimiento de los principios básicos y los requisitos mínimos exigidos en el presente real decreto en condiciones de mejor eficiencia. Los supuestos concretos de utilización de estas infraestructuras y servicios comunes serán determinados por cada Administración.

- ◆ **El uso de I&S comunes ofrece oportunidades en seguridad:**
  - ➔ Reducción de perímetro físico y lógico.
  - ➔ Ciertos servicios pasan a 'comunes'.
  
- ◆ **Uso de estructuras virtualizadas y servicios en la nube.** (Véase guía CCN-STIC 823). **Aspectos que requieren especial atención:**
  - ➔ Se delega la función pero no la responsabilidad.
  - ➔ Protección de información, especialmente datos de carácter personal.
  - ➔ Cifrado.
  - ➔ Borrado de datos.
  - ➔ Continuidad del servicio.



# Usar guías e instrumentos

## Guías CCN-STIC publicadas:

- 800 - Glosario de Términos y Abreviaturas del ENS
  - 801 - Responsables y Funciones en el ENS
  - 802 - Auditoría de la seguridad en el ENS
  - 803 - Valoración de sistemas en el ENS
  - 804 - Medidas de implantación del ENS
  - 805 - Política de Seguridad de la Información
  - 806 - Plan de Adecuación del ENS
  - 807 - Criptología de empleo en el ENS
  - 808 - Verificación del cumplimiento de las medidas en el ENS
  - 809 - Declaración de Conformidad del ENS
  - 810 - Creación de un CERT / CSIRT
  - 811 - Interconexión en el ENS
  - 812 - Seguridad en Entornos y Aplicaciones Web
  - 813 - Componentes certificados en el ENS
  - 814 - Seguridad en correo electrónico
  - 815 - Métricas e Indicadores en el ENS
  - 817 - Criterios comunes para la Gestión de Incidentes de Seguridad
  - 818 - Herramientas de Seguridad en el ENS
  - 821 - Ejemplos de Normas de Seguridad
  - 822 - Procedimientos de Seguridad en el ENS
  - 823 – Cloud Computing en el ENS
  - 824 - Informe del Estado de Seguridad
- MAGERIT v3

## Programas de apoyo:

Pilar y µPILAR

## En elaboración:

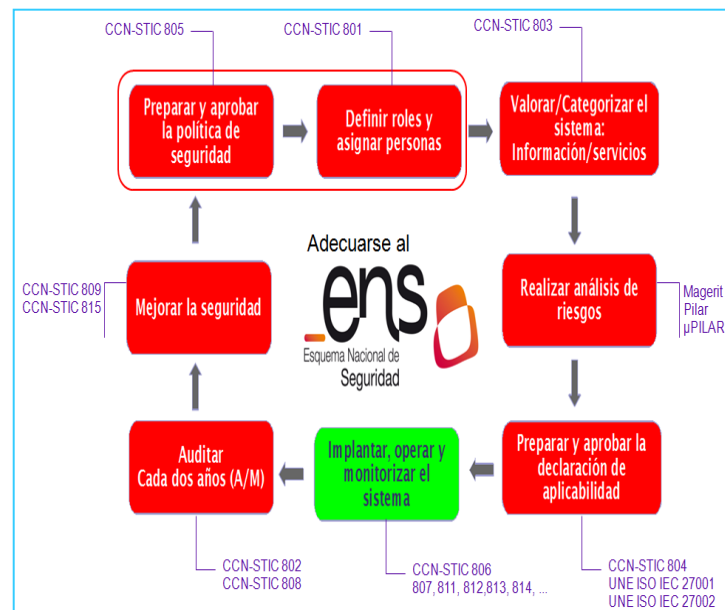
- 819 – Contratación en el ENS
- 820 - Denegación de Servicio

+

Servicios de respuesta ante incidentes CCN-CERT

Formación STIC: presencial / en-línea

Esquema Nacional de Evaluación y Certificación



## ISO/IEC 27001

- ✓ Norma de 'gestión' que contiene los **requisitos de un sistema de gestión de seguridad de la información**, voluntariamente certificable.
- ✓ La certificación de conformidad con 27001 NO es obligatoria en el ENS. Aunque quien se encuentre certificado tiene parte del camino recorrido para lograr su conformidad con el ENS.

## ISO/IEC 27002

- ✓ Muchas de las medidas indicadas en el Anexo II del ENS coinciden con controles de 27002.
- ✓ El ENS añade un sistema de protección proporcionado a la información y servicios a proteger para racionalizar la implantación de medidas y reducir la discrecionalidad.
- ✓ El ENS contempla aspectos de especial interés para la protección de la información y los servicios de administración electrónica (p.ej., aquellos relativos a firma-e) no recogidos en 27002.



# Comunicar los incidentes de seguridad

The screenshot shows the CCN-CERT website interface. At the top, there's a navigation menu with options like 'PRINCIPAL', 'SOBRE NOSOTROS', 'INCIDENTES', 'ACTUALIDAD', 'ALERTAS', 'HERRAMIENTAS', 'RECURSOS', 'NOTICIAS', and 'PREFERENCIAS'. The main content area is divided into several sections: 'ÚLTIMAS VULNERABILIDADES' (listing issues like Moodle and OfficeConnect), 'ÚLTIMOS INFORMES DE SEGURIDAD' (listing reports on DDoS attacks, botnets, and trojans), 'SERIES CCN-STIC' (listing various STIC series), 'HERRAMIENTA PILAR' (a logic analysis tool), 'CURSOS CCN-STIC' (listing specialized courses), 'NOTICIAS SEGURIDAD' (listing security news), 'COMUNICADOS CCN-CERT' (listing press releases), and '¿Quieres notificar un incidente?' (a form to report incidents). There are also logos for 'Servicios S.A.T.', 'ens', and 'III Jornada STIC CCN-CERT'.

**CCN-CERT:** Centro de alerta y respuesta de incidentes de seguridad y ayuda a las AA.PP. a responder de forma más rápida y eficiente ante las amenazas de seguridad que afecten a sus sistemas de información.

✓ **Comunidad: AA.PP. de España**

✓ **Reconocimiento internacional: 2007, EGC (2008)**

✓ **Presta servicios de:**

- **resolución de incidentes,**
- **divulgación de buenas prácticas,**
- **formación**
- **e información de amenazas y alertas.**

✓ **Sondas en Red SARA e Internet.**





GOBIERNO  
DE ESPAÑA

MINISTERIO  
DE HACIENDA  
Y ADMINISTRACIONES PÚBLICAS

# Usar productos certificados



Organismo de certificación

Relación de productos certificados

- ✓ El ENS reconoce la contribución de los **productos evaluados y certificados** para el cumplimiento de los requisitos mínimos de manera proporcionada.
- ✓ Relación con el **Organismo de Certificación** (el propio CCN).
- ✓ La certificación es un aspecto a **considerar** al adquirir productos de seguridad.
- ✓ En función del nivel, se contempla el uso preferentemente de productos certificados.
- ✓ **Modelo de cláusula** para los pliegos de prescripciones técnicas.

[http://www.oc.ccn.cni.es/index\\_en.html](http://www.oc.ccn.cni.es/index_en.html)



# Preguntar

- Escucha y resolución de dudas de manera continuada.
- Hay una **base de conocimiento sobre cuestiones de interés común.**
- Destacan las preguntas sobre:
  - ✓ El ámbito de aplicación del ENS.
  - ✓ Relación entre ENS y LOPD/RD 1720/2007
  - ✓ Elaboración de la política de seguridad.
  - ✓ Organización y roles singulares en el ENS.
  - ✓ Valoración y categorización de sistemas.
  - ✓ Aplicación de medidas concretas.
  - ✓ El papel del análisis de riesgos.
  - ✓ La adquisición de productos de seguridad.



## Esquema Nacional de Seguridad – Preguntas Frecuentes

1. Cuestiones Generales .....	2
2. Ámbito de aplicación, alcance e implantación del ENS.....	4
3. Ley Orgánica de Protección de Datos de Carácter Personal y Esquema Nacional de Seguridad .....	14
4. El equipo humano de la seguridad de la información.....	15
5. Plan de Adecuación al ENS .....	21
6. Las Guías STIC del CCN.....	24
7. La categorización de los sistemas .....	25
8. El análisis de riesgos y la gestión de riesgos .....	26
9. La auditoría de la seguridad .....	28
10. Certificaciones.....	29
11. Medidas de seguridad.....	30
12. El ENS y la normalización voluntaria relativa a sistemas de gestión de seguridad de la información.....	31



# Formarse



## Cursos on-line de Seguridad de la Información



Aviso  
CCN-CERT

En este momento está usando el acceso para i

Cursos > Esquema Nacional de Seguridad (público) > SCORMs > Esquema Nacional Seguridad (público)

Salir

Esquema Nacional de Seguridad

ADJUNTOS



Menú

- Inicio al Esquema Nacional de Seguridad
- Instrucciones de navegación
- Objetivos del curso
- Unidad 1: La Administración Electrónica y la Seguridad de la Información
- Unidad 2: Introducción al Esquema Nacional de Seguridad
- Unidad 3: Los Requisitos Mínimos de Seguridad de Información
- Unidad 4: Infraestructura y Herramientas de Seguridad
- Unidad 5: Auditorías de Seguridad y Respuesta a Incidentes
- Unidad 6: Órganos y organismos de Referencia
- Unidad 7: Categorización de Sistemas y Medidas de Seguridad
- Unidad 8: Ejercicio Práctico
- Unidad 9: Las Guías CCN-STIC del ENS
- Información Complementaria
- Evaluación Final



siguiente

### 2ª Convocatoria de los Cursos CCN-STIC del primer semestre de 2012

El Equipo de Respuesta ante Incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN-CERT, le comunica que está abierta la segunda convocatoria de los Cursos de Seguridad de las Tecnologías de la Información y Comunicaciones, CCN-STIC 2012, para el primer semestre del año. El plazo de presentación de solicitudes será de quince días naturales, durante 24 horas, contados a partir del día siguiente al de la publicación de la resolución 1834 del Boletín Oficial del Estado del 7 de febrero de 2012.

Estas acciones formativas, y según la Resolución de 27 de enero de 2012 del Instituto Nacional de Administración Pública (INAP), se desarrollan en colaboración con el Centro Criptológico Nacional y están estructurados en dos categorías diferentes:

#### \*\* Cursos Básicos de Seguridad \*\*

VII Curso Básico STIC - Infraestructura de Red

Fechas: del 09 al 13 de abril

VII Curso Básico STIC - Base de Datos

Fechas: del 16 al 20 de abril

#### \*\* Cursos de Especialización en Seguridad \*\*

IX Curso Acreditación STIC - Entornos Windows

Fechas: del 26 al 30 de marzo

V Curso STIC - Búsqueda de Evidencias

Fechas: del 07 al 11 de mayo

VII Curso STIC - Inspecciones de Seguridad

Fechas: del 21 al 25 de mayo

III Curso STIC - Seguridad en Aplicaciones Web

Fechas: del 11 al 15 de junio

Los cursos se realizarán en las instalaciones que el Instituto Nacional de Administración Pública (INAP) tiene

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

URL: <http://administracionelectronica.gob.es/>



GOBIERNO  
DE ESPAÑA

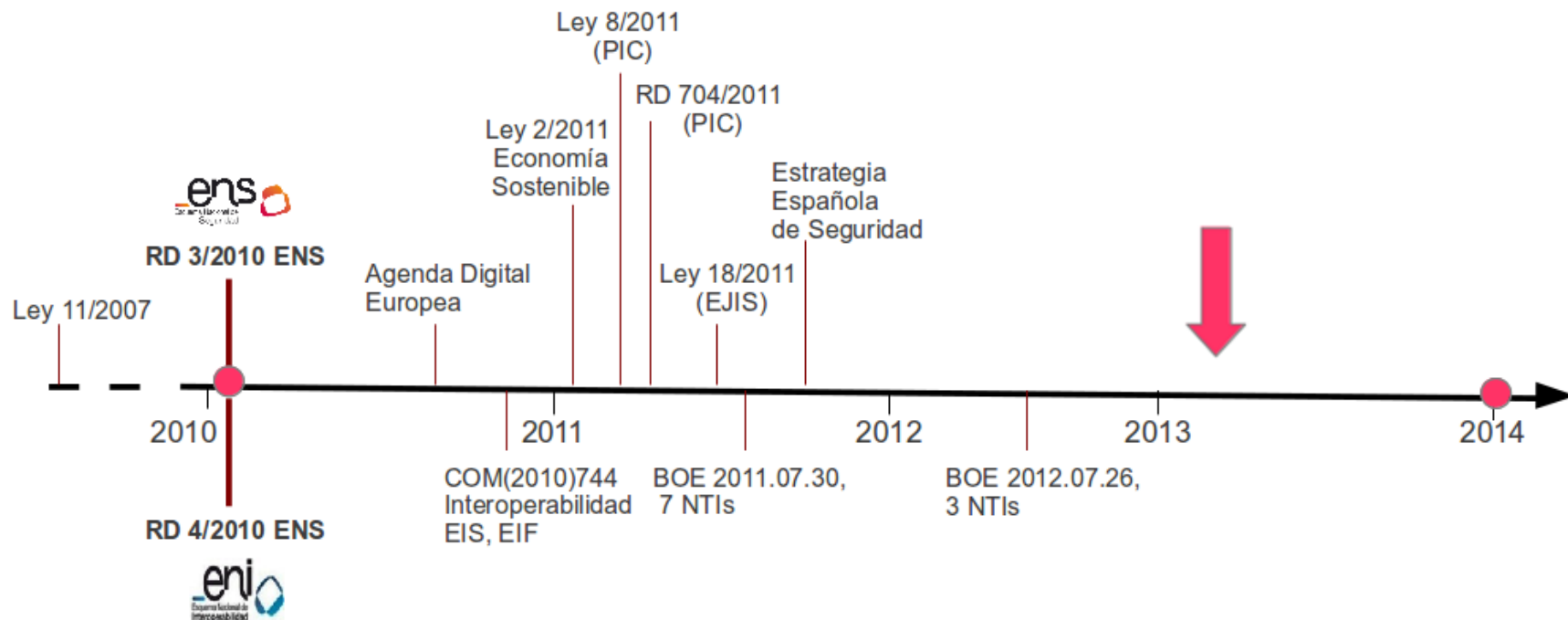
MINISTERIO  
DE HACIENDA  
Y ADMINISTRACIONES PÚBLICAS

## 4. Dónde estamos.



# Dónde estamos

A menos de un año del fin del plazo de adecuación



## ◆ **ENS:**

- Seguimiento en las AA.PP.:
- Acuerdos de la Comisión Permanente del Consejo Superior de Administración Electrónica y del Comité de Seguridad de la información de las AA.PP.
- Febrero (solo AGE), mayo, septiembre y diciembre de 2013.





# Seguimiento del progreso de la adecuación Autoservicio, ¿cómo estoy en relación con los demás?

**[gen.5] Declaración de Aplicabilidad**

**i**

- 1 - no se ha calculado el conjunto de medidas de aplicación
- 2 - se ha iniciado el proceso de determinación de las medidas que son de aplicación
- 3 - existe una estimación informal del conjunto de medidas
- 4 - se ha preparado una declaración completa y está pendiente de aprobación
- 5 - se ha aprobado formalmente la declaración

**Aceptar**

## Avance del Plan de Adecuación al ENS (v21 - 25.2.2013)

Abrir Guardar Guardar como ... Salir

Responsable: responsable

Organismo: organismo

2012 2013 2014

controles		ay...	dat...	ene	feb	mar	abr	may	jun	jul	ago	sep	oct	nov	dic
Progreso															
[gen] Asuntos generales		?	...		1,8										
[gen.1] Responsable de la Seguridad (nombramiento)		?	...		2										
[gen.2] Responsable del Sistema (nombramiento)		?	...		2										
[gen.3] Categorización del sistema (Anexo I)		?	...		2										
[gen.4] Análisis de riesgos (op.pl. 1)		?	...		4										
[gen.5] Declaración de Aplicabilidad		?	...		1										
[gen.6] Plan de Adecuación		?	...		1										
[gen.7] Publicidad de la conformidad en la sede electrónica		?	...		1										
[gen.8] Progreso del Plan de Adecuación		?	...		1										
[a2] Anexo II		?	...		3,3										

**[gen.5] Declaración de Aplicabilidad**

**i**

	1	2	3	4	5	mediana	org
feb 2013	8	8	10	11	6	3,0	1

**Aceptar**

## Obligación de conocer regularmente el estado de la seguridad en las AA.PP. :

Artículo 35. Informe del estado de la seguridad.

El Comité Sectorial de Administración Electrónica articulará los procedimientos necesarios para conocer regularmente el estado de las principales variables de la seguridad en los sistemas de información a los que se refiere el presente real decreto, de forma que permita elaborar un perfil general del estado de la seguridad en las Administraciones públicas.

### **Acción: Informe del estado de la seguridad.**

- Primer trimestre de 2013.
- Ámbitos: AGE y CC.AA.

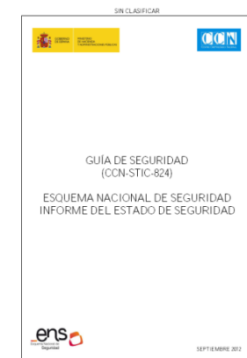
Destinatarios:

- La entidad propietaria del sistema de información.
- El informe anual de estado de seguridad de las AA.PP.

Se persigue conocimiento:

- De las medidas adoptadas.
- Esfuerzo dedicado a seguridad TIC (euros, personas y tiempo).

*Contraste con los datos de seguimiento del progreso de adecuación.*







GOBIERNO  
DE ESPAÑA

MINISTERIO  
DE HACIENDA  
Y ADMINISTRACIONES PÚBLICAS

## **5. Retos y conclusiones.**

# Lo que viene: La seguridad en planes, estrategias, directivas

## ♦ **Proyecto de Estrategia Española de Ciberseguridad:**

Pilar: la seguridad de información y servicios manejados por AA.PP.

- Asegurar la **plena implantación del Esquema Nacional de Seguridad**.
- Fortalecer las capacidades de respuesta a incidentes del **CCN-CERT**.
- **Reforzar el uso de Red SARA como infraestructura común y segura** de las AA.PP. potenciando su uso, sus capacidades de seguridad y el desarrollo de nuevos servicios horizontales.
- **Optimizar el modelo de interconexión de las AA.PP.** con las redes públicas de datos maximizando su eficacia, disponibilidad y seguridad.

## ♦ **Propuesta de Directiva de seguridad de la información y las redes.** Las AA.PP. deberán:

- Adoptar **medidas organizativas y técnicas para gestionar los riesgos**.
- Adoptar **medidas para prevenir y minimizar incidentes** que afecten a sus redes y sistemas de información y **asegurar la continuidad** de los servicios soportados por dichas redes y sistemas.



# Evolución del ENS

**Eje**  
**Administración General del Estado**

**Plan Racionaliz@**

**RETO R5. Avanzar en la consecución de una Administración sin papeles.**

**MEDIDA – R5.M3: Desarrollar el Esquema Nacional de Seguridad.**

**OBJETIVOS**

- Proporcionar normas e instrumentos que faciliten la seguridad en el ámbito de la administración electrónica.
- Apoyar la implantación del Esquema Nacional de Seguridad.
- Alinear el Esquema Nacional de Seguridad con la evolución de las actuaciones en materia de seguridad en el ámbito internacional.

**ACTIVIDADES PREVISTAS**

- **Como letar la serie de guías de seguridad** previstas en el artículo 29 del Real Decreto 3/2010 (Colección de guías CCN-STIC).
- **Actualizar el Esquema Nacional de Seguridad** a la luz de la experiencia de aplicación del mismo, de la evolución de los riesgos, de los sistemas de protección y de los estándares internacionales sobre seguridad de las tecnologías de la información.
- **Articular procedimientos para conocer regularmente el estado de seguridad en las Administraciones Públicas** (RD 3/2010, art. 35).
- **Alinear el Esquema Nacional de Seguridad con las actuaciones en materia de seguridad en el ámbito internacional** (OCDE – Grupo de seguridad de la información y privacidad, Arreglo de reconocimiento mutuo de los certificados de los Criterios Comunes, etc.)
- **Constituir el Comité de Seguridad de la Información de las Administraciones Públicas**, dependiente del Comité Sectorial de Administración Electrónica. (RD 3/2010, d.o. 3)
- **Apoyar la implantación de la Estrategia Española de Ciberseguridad.**

**RESULTADOS**

- Desarrollo completo del Esquema Nacional de Seguridad.

**BENEFICIOS ESPERADOS**

- Mejorar la seguridad de los servicios de Administración electrónica ofrecidos a los ciudadanos y garantizarles su derecho a relacionarse electrónicamente con las Administraciones públicas.

**INDICADORES**

- Disponibilidad del conjunto completo de guías de seguridad previstas en el artículo 29 del Real Decreto 3/2010, junto con otros instrumentos para la aplicación del Esquema Nacional de Seguridad.
- Conocimiento del estado de las principales variables de seguridad en los sistemas de información de las Administraciones Públicas que sustentan los servicios de administración electrónica.

**PLAZO**

- Año 2015.

- Escucha, análisis del escenario cambiante, retroalimentación.
- Mejor articulación de la participación de los órganos colegiados con competencias en materia de administración-e y de los procedimientos para la **recogida de la información que permita elaborar un perfil general del estado de la seguridad en las AA.PP.** (art. 35).
- Anexo II: Ajustes en diversas medidas. Introducir **modificaciones puntuales** en algunas medidas:
  - ➔ Arquitectura de seguridad [op.pl.2]
  - ➔ Mecanismo de autenticación [op.acc.5]
  - ➔ Registro de la actividad de los usuarios [op.exp.8]
  - ➔ Detección de intrusión [op.mon.1]
  - ➔ Borrado y destrucción [mp.si.5]
  - ➔ Firma electrónica [mp.info.4]
  - ➔ Copias de seguridad (backup) [mp.info.9]
  - ➔ ...

## Conclusiones:

- ✓ **El ENS es un instrumento legal de aplicación a todas las AA.PP.**
- ✓ **Persigue la creación de condiciones de seguridad** para la realización del derecho de los ciudadanos a relacionarse por medios electrónicos con las AA.PP.
- ✓ **Impulsa la gestión continuada y el tratamiento global de la seguridad.**
- ✓ **Las medidas de seguridad se han seleccionado atendiendo a necesidades de las AA.PP.**

## Retos próximos:

- ✓ **Adecuarse en condiciones de limitación de recursos humanos y económicos.**
- ✓ **Continuar el esfuerzo de desarrollo de guías y de otros instrumentos de apoyo a la adecuación al ENS.**
- ✓ **Conocer regularmente el estado de seguridad en las AA.PP.**





# Muchas gracias

- **Portal CCN-CERT – ENS:**

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

- **Portal de la Administración Electrónica - ENS:**

<http://administracionelectronica.gob.es>

- **Preguntas frecuentes:**

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

- **Espacio virtual del ENS:**

<http://circa.administracionelectronica.gob.es/circabc>

- **Contacto para preguntas, dudas: [ens@ccn-cert.cni.es](mailto:ens@ccn-cert.cni.es)**