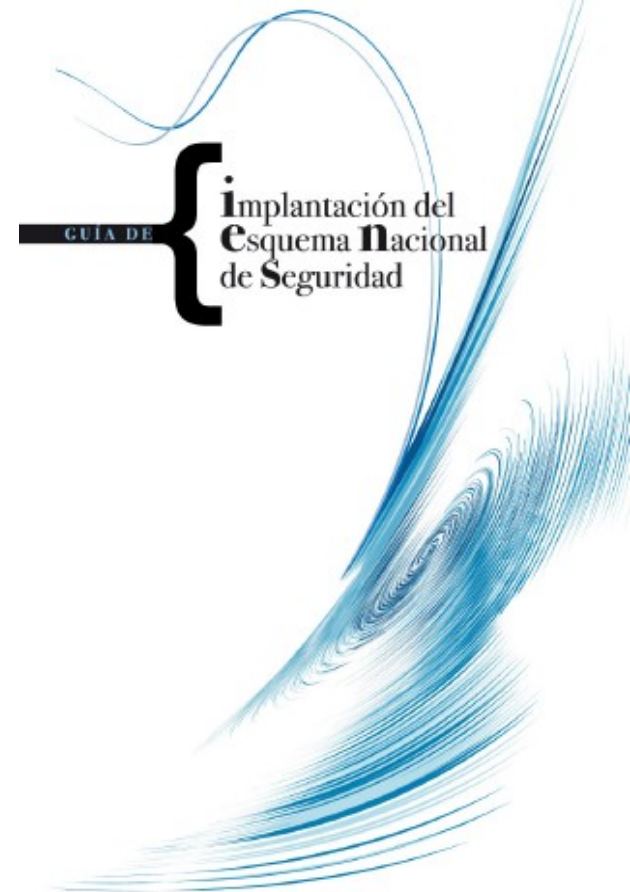


“Jornada de difusión del ENS”

Esquema Nacional de Seguridad

2 de junio de 2011

Miguel A. Amutio Gómez
Ministerio de Política Territorial
y Administración Pública



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.

♦ Tiene por objeto:

- ➔ establecer la **política de seguridad** en la utilización de medios electrónicos,
- ➔ está **constituido por principios básicos y requisitos mínimos** que permitan una **protección adecuada** de la información.

♦ Regulado por el RD 3/2010 que desarrolla la Ley 11/2007, art. 42.2

♦ Ámbito de aplicación: todas las AA.PP. (Ley 11/2007, art. 2).

- ➔ Están excluidos los sistemas que manejan la información clasificada.
- ➔ También las actividades que desarrollen las Administraciones en régimen de derecho privado y las actividades que no sean la gestión de sus competencias.

♦ Adecuación:

- Los sistemas existentes en los plazos establecidos → **límite 29.01.2014**
- Los nuevos sistemas aplicarán lo establecido desde su concepción.

Elaboración y Objetivos

Elaborado con la **participación de todas las AA.PP.** (AGE, CC.AA., CC.LL. a través de la FEMP y CRUE) mediante los órganos colegiados competentes en administración electrónica + **Opinión de la Industria del sector TIC.**

Tiene en cuenta: directrices y recomendaciones de la OCDE, de la UE, normalización nacional e internacional y actuaciones en otros países.

Objetivos:

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

♦ **Introducir lenguaje y elementos comunes**

- Para guiar la actuación de las AA.PP. en materia de seguridad de las tecnologías de la información.
- Para facilitar la interacción de las AA.PP.
- Para **facilitar la comunicación de los requisitos de seguridad de la información a la Industria.**

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.
- ♦ La **certificación**, como aspecto a considerar al adquirir los productos de seguridad. Papel del Organismo de Certificación (CCN).

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.

Adecuación al ENS

Artículo 27. Cumplimiento de requisitos mínimos.

1. Para dar cumplimiento a los requisitos mínimos establecidos en el presente real decreto, las Administraciones públicas aplicarán las medidas de seguridad indicadas en el Anexo II, teniendo en cuenta:

- a) Los activos que constituyen el sistema.
- b) La categoría del sistema, según lo previsto en el artículo 43.
- c) Las decisiones que se adopten para gestionar los riesgos identificados.

2. Cuando un sistema al que afecte el presente real decreto maneje datos de carácter personal le será de aplicación lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, y normativa de desarrollo, sin perjuicio de los requisitos establecidos en el Esquema Nacional de Seguridad.

3. Las medidas a las que se refieren los apartados 1 y 2 tendrán la condición de mínimos exigibles, y podrán ser ampliados por causa de la concurrencia indicada o del prudente arbitrio del responsable de la seguridad del sistema, habida cuenta del estado de la tecnología, la naturaleza de los servicios prestados y la información manejada, y los riesgos a que están expuestos.



-
- ```

graph TD
 A[Preparar y aprobar la política de seguridad] --> B[Definir roles y asignar personas]
 B --> C[Valorar/Categorizar el sistema: Información/servicios]
 C --> D[Realizar análisis de riesgos]
 D --> E[Preparar y aprobar la declaración de aplicabilidad]
 E --> F[Implantar, operar y monitorizar el sistema]
 F --> G[Auditar Cada dos años (A/M)]
 G --> H[Mejorar la seguridad]
 H --> A
 F --> C

```
- El diagrama de flujo ilustra el ciclo de vida de la gestión de la seguridad de la información, con los siguientes pasos:
- Preparar y aprobar la política de seguridad
  - Definir roles y asignar personas
  - Valorar/Categorizar el sistema: Información/servicios
  - Realizar análisis de riesgos
  - Preparar y aprobar la declaración de aplicabilidad
  - Implantar, operar y monitorizar el sistema
  - Auditar Cada dos años (A/M)
  - Mejorar la seguridad
- Las flechas indican la secuencia de los pasos, con una flecha de retroalimentación que conecta "Mejorar la seguridad" con "Preparar y aprobar la política de seguridad".

# Ámbito de aplicación

## Artículo 3. Ámbito de aplicación.

El ámbito de aplicación del presente real decreto será el establecido en el artículo 2 de la Ley 11/2007, de 22 de junio.

Están excluidos del ámbito de aplicación indicado en el párrafo anterior los sistemas que tratan información clasificada regulada por Ley 9/1968, de 5 de abril, de Secretos Oficiales y normas de desarrollo.

- ♦ **Determinar sistemas dentro** del ámbito de aplicación del ENS.
- ♦ **Determinar la información y servicios propios** frente a externos:
  - El responsable de la información o servicio puede ser externo.
  - Los **requisitos de seguridad** los marca cada responsable.
- ♦ Decisiones sobre el tratamiento conjunto o singular de los diversos elementos.



- ♦ Sedes electrónicas.
- ♦ Registros electrónicos.
- ♦ S.I. accesibles electrónicamente por los ciudadanos.
- ♦ S.I. para el ejercicio de derechos.
- ♦ S.I. para el cumplimiento de deberes.
- ♦ S.I. para recabar información y estado del procedimiento administrativo



- ♦ Sistemas que tratan información clasificada,
- ♦ Actividades que se desarrollen en régimen de derecho privado
- ♦ Sistemas no relacionados con:
  - el ejercicio de derechos por medios electrónicos
  - el cumplimiento de deberes por medios electrónicos
  - el acceso por medios-e de ciudadanos a infor. y procedimiento adm.



# Organización de la seguridad



Ilustración 1 – Responsables

| nivel           | opción A                              | opción B                      |
|-----------------|---------------------------------------|-------------------------------|
| 1 - gobierno    | comité de seguridad corporativa       |                               |
|                 | comité de seguridad de la información | responsable de la información |
|                 |                                       | responsable del servicio      |
| 2 - ejecutivo   | responsable de la seguridad           |                               |
| 3 - operaciones | responsable del sistema               |                               |

Véase CCN-STIC 801 – ROLES Y FUNCIONES

- ➔ **responsable de la seguridad**  $\neq$  **responsable del sistema**
- ➔ La determinación de quién es responsable de qué debe adecuarse a las particularidades de cada organización y es difícil establecer una regla única para toda la Administración.
- ➔ Se señalan responsabilidades; en algunos sitios serán más formales (se limita a firmar) y en otros serán más operacionales (se involucra activamente)
- ➔ Ejemplo:

**ORDEN COMUNICADA SOBRE CREACIÓN DEL COMITÉ DE SEGURIDAD DE LA INFORMACIÓN DEL MINISTERIO DE CIENCIA E INNOVACIÓN EN LA UTILIZACIÓN DE MEDIOS ELECTRÓNICOS, PARA LA PROTECCIÓN DE DICHA INFORMACIÓN.**



# Política de seguridad

## Artículo 11. Requisitos mínimos de seguridad.

1. ~~No~~ Todos los órganos superiores de las Administraciones públicas deberán disponer formalmente de su política de seguridad, que será aprobada por el titular del órgano superior correspondiente. Esta política de seguridad, se establecerá en base a los principios básicos indicados y se desarrollará aplicando los siguientes requisitos mínimos:

### Secciones típicas de una Política de S.I.:

1. Misión u objetivos del organismo
2. Marco normativo
3. Organización de seguridad
  - Definición de comités y roles unipersonales
  - Funciones
  - Responsabilidades
  - Mecanismos de coordinación
  - Procedimientos de designación de personas
4. Concienciación y formación
5. Postura para la gestión de riesgos
  - Plan de análisis
  - Criterios de evaluación de riesgos
  - Directrices de tratamiento
  - Proceso de aceptación del riesgo residual
6. Proceso de revisión de la política de seguridad

### *Ejemplos:*

- **Ministerio de Industria, Turismo y Comercio**  
(Orden ITC/657/2011, de 11 de marzo)
- **Junta de Andalucía** (Decreto 1/2011, de 11 de enero)

Véase **CCN-STIC-805 POLÍTICA DE SEGURIDAD**

# Categorización

Se definen tres categorías:

- BÁSICA
- MEDIA
- ALTA



- a) **Un sistema de información será de categoría ALTA** si alguna de sus dimensiones de seguridad alcanza el nivel ALTO.
- b) **Un sistema de información será de categoría MEDIA** si alguna de sus dimensiones de seguridad alcanza el nivel MEDIO, y ninguna alcanza un nivel superior.
- c) **Un sistema de información será de categoría BÁSICA** si alguna de sus dimensiones de seguridad alcanza el nivel BAJO, y ninguna alcanza un nivel superior.

La determinación de la categoría de un sistema no implicará que se altere el nivel de las dimensiones de seguridad que no han influido en la determinación de la categoría del mismo.

**Categorizar los sistemas es necesario para modular el equilibrio entre la importancia de la información manejada y de los servicios prestados, y el esfuerzo dedicado a su seguridad, para satisfacer el principio de proporcionalidad.**

## ♦ Valoración de la información y de los sistemas → Homogeneidad.

|                                                                       |           |
|-----------------------------------------------------------------------|-----------|
| <b>2. INFORMACIÓN</b>                                                 | <b>5</b>  |
| 2.1. IDENTIFICACIÓN                                                   | 5         |
| 2.2. VALORACIÓN                                                       | 6         |
| 2.2.1. Criterios generales para valorar la confidencialidad necesaria | 7         |
| 2.2.2. Criterios generales para valorar la integridad necesaria       | 8         |
| 2.2.3. Criterios generales para valorar la autenticidad necesaria     | 9         |
| 2.2.4. Criterios generales para valorar la trazabilidad necesaria     | 10        |
| 2.2.5. Criterios generales para valorar la disponibilidad necesaria   | 10        |
| <b>3. SERVICIOS</b>                                                   | <b>12</b> |
| 3.1. IDENTIFICACIÓN                                                   | 12        |
| 3.2. VALORACIÓN                                                       | 13        |
| 3.2.1. Criterios generales para valorar la disponibilidad necesaria   | 13        |
| 3.2.2. Criterios generales para valorar la autenticidad necesaria     | 15        |
| 3.2.3. Criterios generales para valorar la trazabilidad necesaria     | 16        |
| 3.2.4. Criterios generales para valorar la confidencialidad necesaria | 17        |
| 3.2.5. Criterios generales para valorar la integridad necesaria       | 18        |

# Gestión de riesgos

## 12. GESTIÓN DE LOS RIESGOS

115. La gestión de los riesgos son tareas que deben realizarse de manera continua sobre los sistemas de información y orientar todas las demás actividades, de acuerdo a los principios (b) “Gestión de riesgos” y (e) “Reevaluación periódica”:
- o ver Artículo 6 del ENS, “Gestión de la seguridad basada en los riesgos”
  - o ver Artículo 9 del ENS, “Reevaluación periódica”
116. La forma de realizar el análisis de riesgos se detalla en el Anexo II, [op.pl.1] “Análisis de riesgos”, estableciendo una proporcionalidad entre el nivel de detalle del análisis y la categoría del sistema de información.
117. Véase el Anexo A: Tareas, donde se muestran escenarios posibles de asignación de tareas relativas a la gestión de riesgos.
118. El Responsable de la Información es el propietario de los riesgos sobre la información.
119. El Responsable del Servicio es el propietario de los riesgos sobre los servicios.
120. El propietario de un riesgo debe ser informado de los riesgos que afectan a su propiedad y del riesgo residual al que está sometida. Cuando un sistema de información entra en operación, los riesgos residuales deben haber sido aceptados formalmente por su correspondiente propietario.

122. La responsabilidad de monitorizar un riesgo recae en su propietario, sin perjuicio de que la función puede ser delegada en el día a día, retomando el control de la situación cuando hay que tomar medidas para atajar un riesgo que se ha salido de los márgenes tolerables.

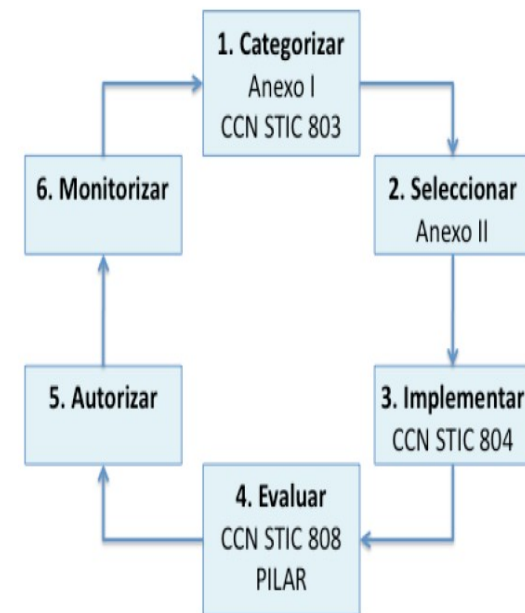


Ilustración 4 - Proceso de Gestión de Riesgos

Véase **CCN-STIC 801 – ROLES y FUNCIONES**

- Papel de la gestión de riesgos en el ENS.
- Herramientas para realizarlo de forma ágil (PILAR / μPILAR).

▪ The only mandatory requirement under the FISMA security standards and guidance is the application of the NIST Risk Management Framework—everything else is negotiable.

# Declaración de aplicabilidad

## 3.7. DECLARACIÓN DE APLICABILIDAD DE LAS MEDIDAS DEL ANEXO II DEL ENS

22. Vistas las exigencias del Anexo II del ENS y las exigencias derivadas de los datos de carácter personal, el Responsable de Seguridad elaborará una relación de las medidas que son de aplicación al sistema (o a cada sub-sistema, si se ha recurrido a una fragmentación como se describe en la sección anterior).
23. Habitualmente se recurrirá a las medidas detalladas en el Anexo II, enriquecidas o matizadas por características determinadas del sistema o exigencias derivadas del tratamiento de datos de carácter personal.
24. Cuando una medida requerida por el Anexo II en función de la valoración del sistema no vaya a considerarse aplicable, esta no-aplicabilidad debe estar motivada.
25. Cuando se recurra a medidas alternativas, se indicará el motivo, así como las medidas que sustituye.
26. Las medidas se complementarán con aquellas que sean pertinentes a la vista del análisis de riesgos realizado. Téngase en cuenta que tanto el ENS como la reglamentación de protección de datos de carácter personal, establecen una serie de medidas mínimas que deben ampliarse cuando sea prudente hacerlo.

Véase **CCN-STIC-806 PLAN DE ADECUACIÓN**

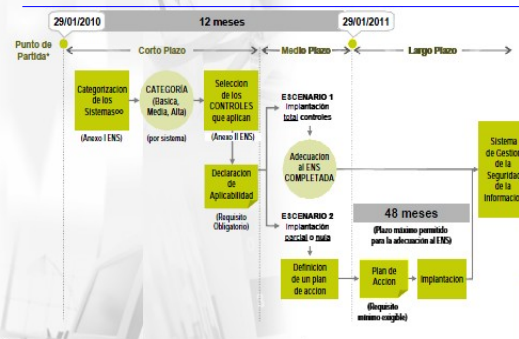
### Esquema Nacional de Seguridad

¿Qué viene después?



Disponer de la Declaración de Aplicabilidad **no es más que el primer paso** para la adecuación al ENS.

#### La Hoja de Ruta para la Adecuación al ENS



» Propios o que se proporcionan a través de un proveedor de servicios contratado: custodia legal, sellado de tiempo, validación (VA), firma electrónica, certificados, etc.

#### Los pasos siguientes:

1. Comparar la situación real de la Seguridad con lo que exige la Declaración
2. Identificar las debilidades y carencias existentes
3. Analizar qué es necesario para corregirlas
4. Agruparlo todo en PROYECTOS
5. Elaborar un PLAN DE ACCIÓN

Artículo 41. Publicación de conformidad.

Los órganos y Entidades de Derecho Público darán publicidad en las correspondientes sedes electrónicas a las declaraciones de conformidad, y a los distintivos de seguridad de los que sean acreedores, obtenidos respecto al cumplimiento del Esquema Nacional de Seguridad.

CCN-STIC-809

SIN CLASIFICAR

Declaración de Conformidad del Esquema Nacional de Seguridad

ÍNDICE

1. INTRODUCCIÓN.....4

2. CONSIDERACIONES CONJUNTAS DE ADECUACIÓN Y CONFORMIDAD.....4

3. DECLARACIÓN DE CONFORMIDAD.....4

3.1. CONTENIDO.....4

3.2. IDENTIFICACIÓN DEL DECLARANTE.....5

3.3. OBJETO DE LA DECLARACIÓN.....5

3.4. BASE Y FINALIDAD DE LA DECLARACIÓN DE CONFORMIDAD.....5

3.5. LUGAR, FECHA Y FIRMA DE LA DECLARACIÓN.....6

4. MECANISMO DE CONTROL.....6

5. DISTINTIVO DE SEGURIDAD.....6

6. MODELO DE DECLARACIÓN DE CONFORMIDAD.....6

6. MODELO DE DECLARACIÓN DE CONFORMIDAD.

22. El modelo recomendado para efectuar la declaración de conformidad es el siguiente:

“DECLARACIÓN DE CONFORMIDAD CON EL ESQUEMA NACIONAL DE SEGURIDAD

Nombre del declarante:.....

(identificación del órgano o entidad de derecho público que la formula)

- Manifestación expresa de que el sistema cumple lo establecido en el ENS.
- No existe, de momento, una certificación 'oficial' de adecuación.
- Oferta del mercado:** se va incluyendo la adecuación al ENS en ofertas de servicios de auditoría y de cumplimiento normativo.
- Ejemplos:
  - Secretaría de Estado de la Seguridad Social.
  - Universidad Pablo de Olavide, de Sevilla.



# Guías y herramientas

## Artículo 29. Guías de seguridad.

Para el mejor cumplimiento de lo establecido en el Esquema Nacional de Seguridad, el Centro Criptológico Nacional, en el ejercicio de sus competencias, elaborará y difundirá las correspondientes guías de seguridad de las tecnologías de la información y las comunicaciones.

### Guías de seguridad



- 801 – Roles y funciones
- 802 – Guía de auditoría
- 803 – Valoración de los sistemas
- 804 – Guía de implantación
- 805 – Política de seguridad
- 806 – plan de adecuación
- 807 – Uso de criptografía
- 808 – Guía de inspección de cumplimiento
- 809 – Declaración de conformidad
- 810 – Guía de creación de CERTs
- ...
- Metodología de análisis y gestión de riesgos Magerit v2

### Programas de ayuda

#### CERT

#### Alerta temprana

#### Productos certificados

#### Formación

- Análisis y gestión de riesgos PILAR / μPILAR
- Servicios CCN-CERT
- SAT Red SARA
- Esquema Nacional de Evaluación y Certificación
- Cursos STIC

+ **Proporcionados por la Industria:** ej. Guía de implantación del ENS de AMETIC.

# Muchas gracias



## Esquema Nacional de Seguridad

<http://administracionelectronica.gob.es/es/ctt/ens> , <https://www.ccn-cert.cni.es/>

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

**Series CCN-STIC** <http://www.ccn-cert.cni.es>

## Esquema Nacional de Evaluación y Certificación de la Seguridad de las TI

<http://www.oc.ccn.cni.es/>

## MAGERIT v2, Metodología de análisis y gestión de riesgos

<http://administracionelectronica.gob.es/es/ctt/magerit>

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

<http://administracionelectronica.gob.es/es/ctt/pilar>

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

