GOBIERNO DE ESPAÑA
MINISTERIO DE POLÍTICA TERRITORIAL Y ADMINISTRACIÓN PÚBLICA

AMETIC

"Jornada de difusión del ENS"

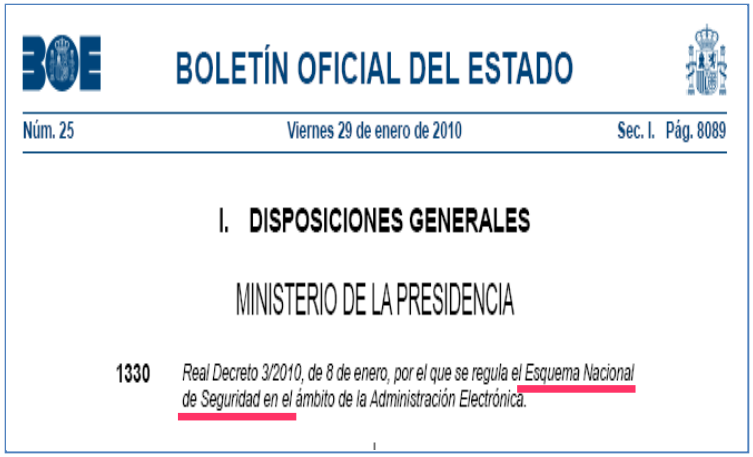
Esquema Nacional de Seguridad

27 de abril de 2011

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

GOBIERNO DE ESPAÑA
MINISTERIO DE POLÍTICA TERRITORIAL Y ADMINISTRACIÓN PÚBLICA

ens Esquema Nacional de Seguridad


BOLETÍN OFICIAL DEL ESTADO
Núm. 25 Viernes 29 de enero de 2010 Sec. I. Pág. 8089

I. DISPOSICIONES GENERALES

MINISTERIO DE LA PRESIDENCIA

1330 *Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.*

- **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.

GOBIERNO DE ESPAÑA
MINISTERIO DE POLÍTICA TERRITORIAL Y ADMINISTRACIÓN PÚBLICA

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**.

Teniendo en cuenta: recomendaciones de la UE, directrices de la OCDE, actuaciones en otros países y normalización.

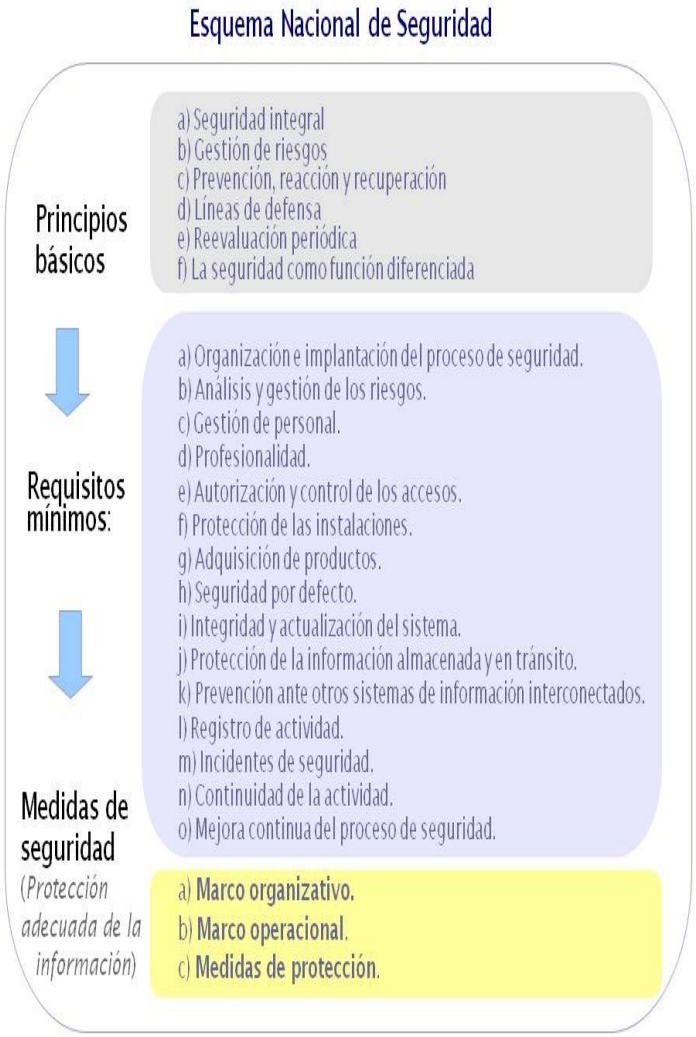
Objetivos:

- **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).



GOBIERNO DE ESPAÑA
MINISTERIO DE POLÍTICA TERRITORIAL Y ADMINISTRACIÓN PÚBLICA

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. Los 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.

GOBIERNO DE ESPAÑA
MINISTERIO DE POLÍTICA TERRITORIAL Y ADMINISTRACIÓN PÚBLICA

Algunas cuestiones sobre la adecuación al ENS

- ¿Cuál es el **ámbito de aplicación** del ENS?
- ¿Cómo se **organiza la seguridad**?
- ¿Qué contiene la **política de seguridad** y cuál es el instrumento adecuado para su aplicación?
- ¿Por qué es importante la **categorización** de los sistemas?
- ¿Cuál es el papel de la **gestión de los riesgos**?
- ¿Qué es la **declaración de aplicabilidad**?
- ¿Cómo se **publica la conformidad**?
- ¿Hay **guías y herramientas** para la adecuación al ENS?

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 ≠ 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.

GOBIERNO DE ESPAÑA
MINISTERIO DE POLÍTICA TERRITORIAL Y ADMINISTRACIÓN PÚBLICA

Política de seguridad

Artículo 11. Requisitos mínimos de seguridad.

1. 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

Cuestión:

- Tipo idóneo de instrumento y publicidad

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

GOBIERNO DE ESPAÑA
MINISTERIO DE POLÍTICA TERRITORIAL Y ADMINISTRACIÓN PÚBLICA

Política de seguridad
Ejemplos: Junta de Andalucía, MITYC

5575 *Orden ITC/657/2011, de 11 de marzo, por la que se aprueba la política de seguridad de la información en el ámbito de la administración electrónica del Ministerio de Industria, Turismo y Comercio.*

1. Objeto y ámbito de aplicación
2. Misión del Departamento
3. Marco normativo
4. Estructura organizativa de la Política de SI
5. El Comité para la Gestión y Coordinación de SI
6. El Responsable de Seguridad
7. Equipo de Seguridad
8. El Responsable de la Información
9. El Responsable del Servicio
10. Resolución de conflictos
11. Gestión de riesgos
12. Desarrollo normativo
13. Protección de datos de carácter personal
14. Formación y concienciación
15. Actualización permanente y revisiones periód.

DECRETO 1/2011, de 11 de enero, por el que se establece la política de seguridad de las tecnologías de la información y comunicaciones en la Administración de la Junta de Andalucía.

1. Objeto
2. Definiciones y estándares
3. Ámbito de aplicación
4. Objetivos de la política de seguridad de las TIC
5. Principios de la política de seguridad TIC
6. Responsabilidad general
7. Comité de seguridad TIC de la J. de Andalucía
8. Responsable de la Coordinación en Seguridad TIC de la Junta de Andalucía
9. Grupo de Personas Expertas en Seguridad TIC de la Junta de Andalucía
10. Comités de Seguridad TIC de las Entidades
11. Responsable de seguridad TIC
12. Gestión de la seguridad TIC en la Administración de la Junta de Andalucía

Anexo I Glosario de términos

Anexo II Estándares

GOBIERNO DE ESPAÑA
MINISTERIO DE POLÍTICA TERRITORIAL Y ADMINISTRACIÓN PÚBLICA

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 los sistemas y el esfuerzo dedicado a su seguridad y satisfacer el principio de proporcionalidad.

- **Valoración de la información y de los sistemas** → Homogeneidad.

Véase **CCN-STIC 803 – VALORACIÓN DE LOS SISTEMAS**

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":
    - ver Artículo 6 del ENS, "Gestión de la seguridad basada en los riesgos"
    - 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.

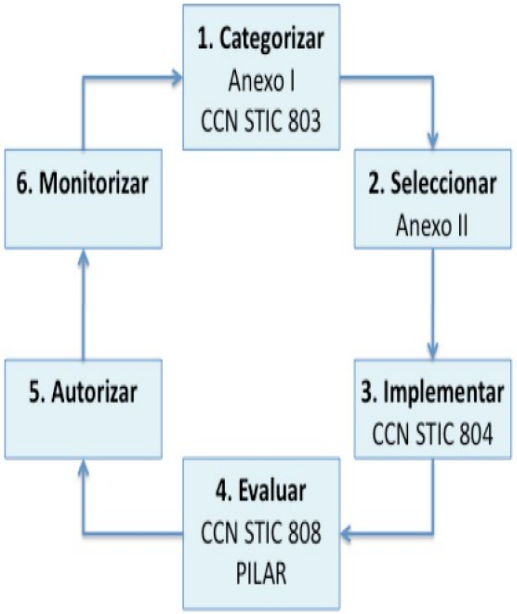


Ilustración 4 - Proceso de Gestión de Riesgos

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.

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

GOBIERNO DE ESPAÑA
MINISTERIO DE POLÍTICA TERRITORIAL Y ADMINISTRACIÓN PÚBLICA

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).

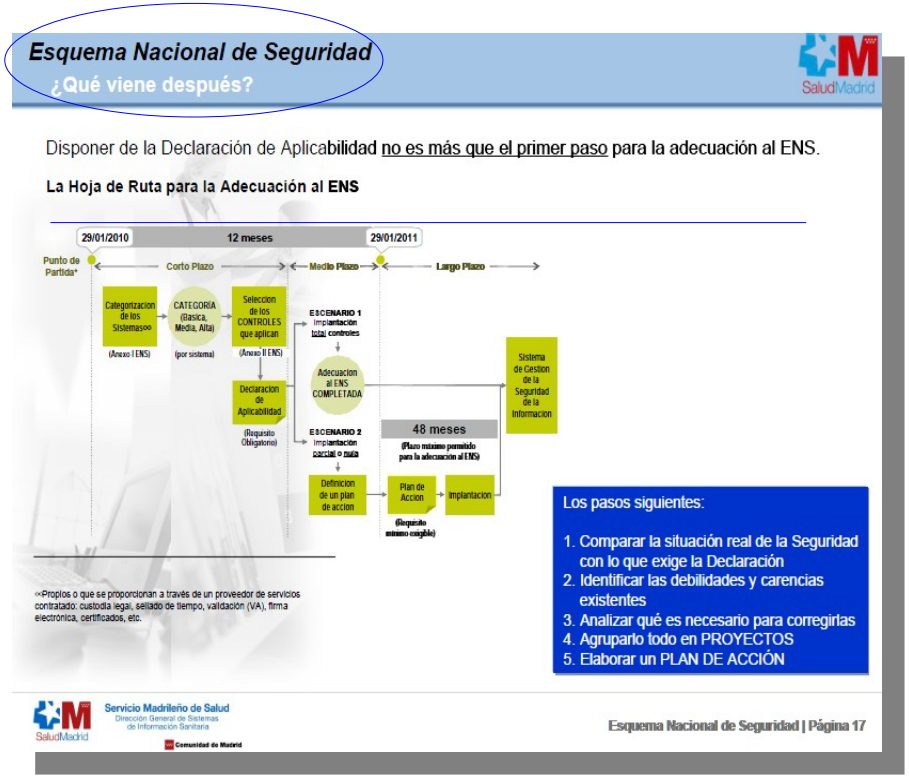
23. Habitualmente se recurrirá a las medidas detalladas en el Anexo II, enriquecidas o matizadas por características determinadas del sistema o exigencias derivadas del tratamiento de datos de carácter personal.

24. Cuando una medida requerida por el Anexo II en función de la valoración del sistema no vaya se consideré 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**



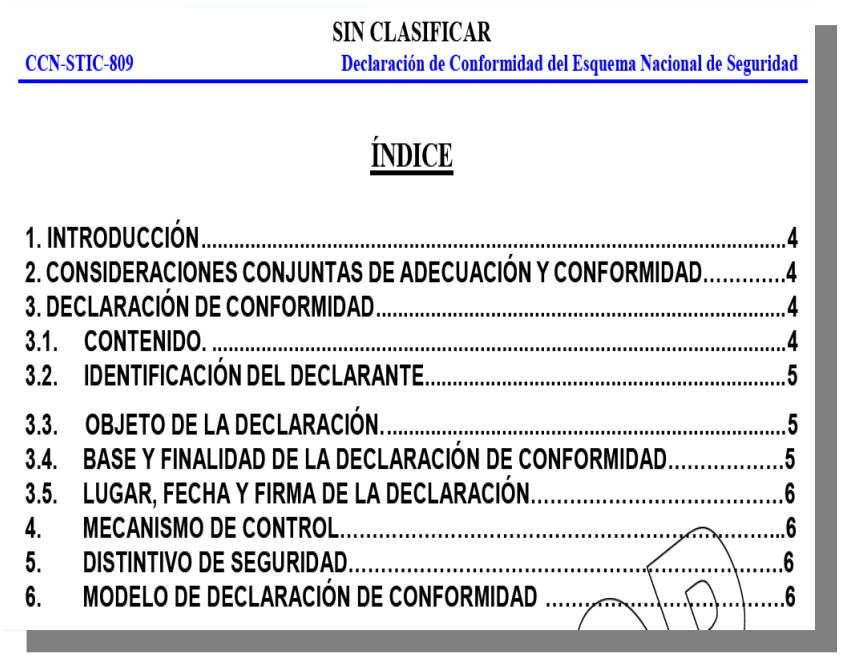
http://www.steria.es/documents/File/Eventos%202010/ENS%20MADRID/ENSCM1.pdf

GOBIERNO DE ESPAÑA
MINISTERIO DE POLÍTICA TERRITORIAL Y ADMINISTRACIÓN PÚBLICA

Publicación de conformidad

Artículo 41. Publicación de conformidad.

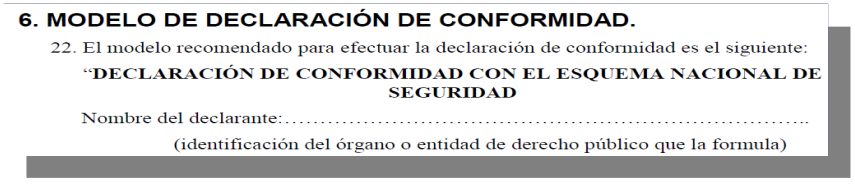
Los órganos y Entidades de Derecho Público darán publicidad en las correspondientes sedes electrónicas a las declaraciones de conformidad, y a los distintivos de seguridad de los que sean acreedores, obtenidos respecto al cumplimiento del Esquema Nacional de Seguridad.



SIN CLASIFICAR

CCN-STIC-809 Declaración de Conformidad del Esquema Nacional de Seguridad

ÍNDICE



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.

Véase **CCN-STIC-809 DECLARACIÓN DE CONFORMIDAD CON EL ENS**

GOBIERNO DE ESPAÑA
MINISTERIO DE POLÍTICA TERRITORIAL Y ADMINISTRACIÓN PÚBLICA

Publicación de conformidad
Ejemplos de declaraciones

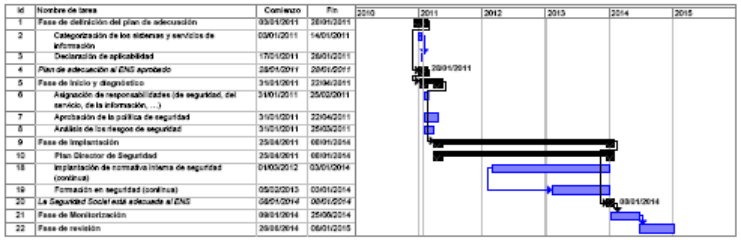
GOBIERNO DE ESPAÑA
MINISTERIO DE TRABAJO E INMIGRACIÓN
SECRETARÍA DE ESTADO DE LA SEGURIDAD SOCIAL

Declaración de conformidad con el Esquema Nacional de Seguridad

De acuerdo al capítulo VIII, artículo 41 del RD 3/2010 "Esquema Nacional de Seguridad", la Seguridad Social comunica que:

- Los sistemas de información que forman parte y dan soporte a su Sede Electrónica han sido analizados conforme a las exigencias recogidas en el Esquema Nacional de Seguridad.
- Como resultado de este análisis se ha aprobado un Plan de Adecuación al Esquema, dentro de los plazos legalmente establecidos y que prevé la adaptación completa de estos sistemas en Enero de 2014.
- Entre tanto, los sistemas de información han sido protegidos adecuadamente y están siendo sometidos de forma continua a revisiones de seguridad y sus subsiguientes actuaciones con el fin de mantenerlos en todo momento con un nivel de seguridad adecuado.
- Que la Seguridad Social se someterá a las auditorías periódicas para garantizar el cumplimiento del objetivo anterior con el paso del tiempo.

El Plan de Adecuación tiene la siguiente planificación general:



Id	Nombre de tarea	Comienzo	Fin
1	Fase de definición del plan de adecuación	03/01/2011	28/04/2011
2	Categorización de los sistemas y servicios de información	03/01/2011	14/01/2011
3	Declaración de aplicabilidad	17/01/2011	28/01/2011
4	Plan de adecuación al ENS aprobado	28/01/2011	28/01/2011
5	Fase de Inicio y diagnóstico	31/01/2011	22/04/2011
6	Asignación de responsabilidades (de seguridad, del servicio, de la información, ...)	31/01/2011	25/02/2011
7	Aprobación de la política de seguridad	31/01/2011	22/04/2011
8	Análisis de los riesgos de seguridad	31/01/2011	25/03/2011
9	Fase de Implantación	25/04/2011	08/01/2014
10	Plan Director de Seguridad	25/04/2011	08/01/2014
18	Implantación de normativa interna de seguridad (continua)	01/03/2012	03/01/2014
19	Formación en seguridad (continua)	05/02/2013	03/01/2014
20	La Seguridad Social está adecuada al ENS	08/01/2014	08/01/2014
21	Fase de Monitorización	09/01/2014	25/06/2014
22	Fase de revisión	26/06/2014	06/01/2015

Esta información publicada en la Sede se irá actualizando conforme avance el proyecto o bien haya cambios sustanciales que deban ser notificados.

Fuente: https://sede.seg-social.gob.es/Sede_1/InformacionLegal/index.htm#documentoPDF

Universidad Pablo de Olavide, de Sevilla

Declaración de conformidad con el Esquema Nacional de Seguridad, de la Universidad Pablo de Olavide, de Sevilla.

De acuerdo al capítulo VIII, artículo 41 del RD 3/2010 "Esquema Nacional de Seguridad", la Universidad Pablo de Olavide, de Sevilla comunica que:

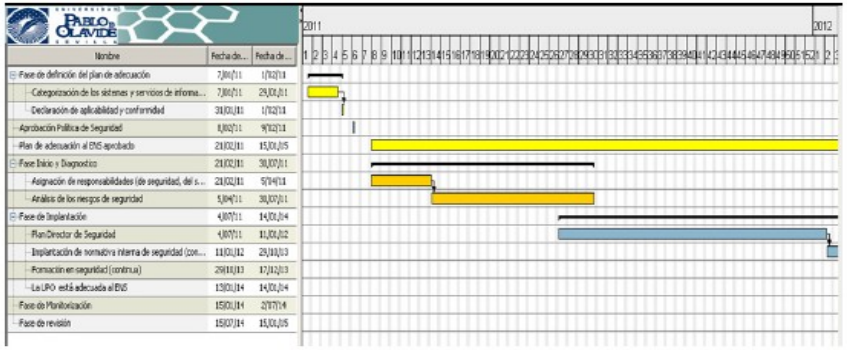
1) Los sistemas de información y registro electrónico que forman parte y dan soporte a su Portal de Administración Electrónica, futura Sede Electrónica, así como el acceso electrónico de los ciudadanos a los mismos y a los servicios que proporcionan han sido analizados conforme a las exigencias recogidas en el Esquema Nacional de Seguridad.

2) Como resultado de este análisis se ha aprobado el Plan de Adecuación al Esquema, dentro de los plazos legalmente establecidos y que prevé la adaptación completa de los sistemas en Enero de 2014.

3) Entre tanto, los sistemas de información han sido protegidos adecuadamente y están siendo sometidos de forma continua a revisiones de seguridad y control para garantizar el cumplimiento del ENS y sus subsiguientes actuaciones con el fin de mantenerlos en todo momento con un nivel de seguridad adecuado.

4) Que la Universidad Pablo de Olavide, de Sevilla someterá a auditorías periódicas los sistemas de información y registro electrónico que conforman su futura Sede Electrónica para garantizar el cumplimiento del objetivo anterior con el paso del tiempo.

El Plan de Adecuación tiene la siguiente planificación general:



Nombre	Fecha de...	Fecha de...
Fase de definición del plan de adecuación	7/01/11	1/02/11
Categorización de los sistemas y servicios de informa...	7/01/11	28/01/11
Declaración de aplicabilidad y conformidad	31/01/11	1/02/11
Aprobación Política de Seguridad	8/02/11	9/02/11
Plan de adecuación al ENS aprobado	21/02/11	15/01/15
Fase Inicio y Diagnostico	21/02/11	30/07/11
Asignación de responsabilidades (de seguridad, del s...	21/02/11	5/04/11
Análisis de los riesgos de seguridad	5/04/11	30/07/11
Fase de Implantación	4/07/11	14/01/14
Plan Director de Seguridad	4/07/11	11/01/12
Implantación de normativa interna de seguridad (con...	11/01/12	29/10/13
Formación en seguridad (continua)	29/10/13	17/12/13
La UPO está adecuada al ENS	13/01/14	14/01/14
Fase de Monitorización	15/01/14	2/07/14
Fase de revisión	15/07/14	15/01/15

Esta información publicada en el Portal de Administración Electrónica se irá actualizando conforme avance el proyecto o bien haya cambios sustanciales que deban ser notificados.

Aprobado por la Comisión de Seguridad de TIC de la Universidad Pablo de Olavide, el 31 de Enero de 2011.

Fuente: www.upo.es/ae/ficheros/UPO_declaracion_conformidad_ENS.pdf

GOBIERNO DE ESPAÑA
MINISTERIO DE POLÍTICA TERRITORIAL Y ADMINISTRACIÓN PÚBLICA

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

- Análisis y gestión de riesgos PILAR / µPILAR

CERT

- Servicios CCN-CERT

Alerta temprana

- SAT Red SARA

Productos certificados

- Esquema Nacional de Evaluación y Certificación

Formación

- Cursos STIC

GOBIERNO DE ESPAÑA
MINISTERIO DE POLÍTICA TERRITORIAL Y ADMINISTRACIÓN PÚBLICA

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