GOBIERNO DE ESPAÑA
MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS

X Foro de Seguridad de RedIRIS

ESQUEMA NACIONAL DE SEGURIDAD

"ENS. Estado de situación y retos próximos"

6 de marzo de 2012

Miguel A. Amutio Gómez
Jefe de Área de Planificación y Explotación
Ministerio de Hacienda y Administraciones Públicas

GOBIERNO DE ESPAÑA
MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS

Esquema Nacional de Seguridad

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

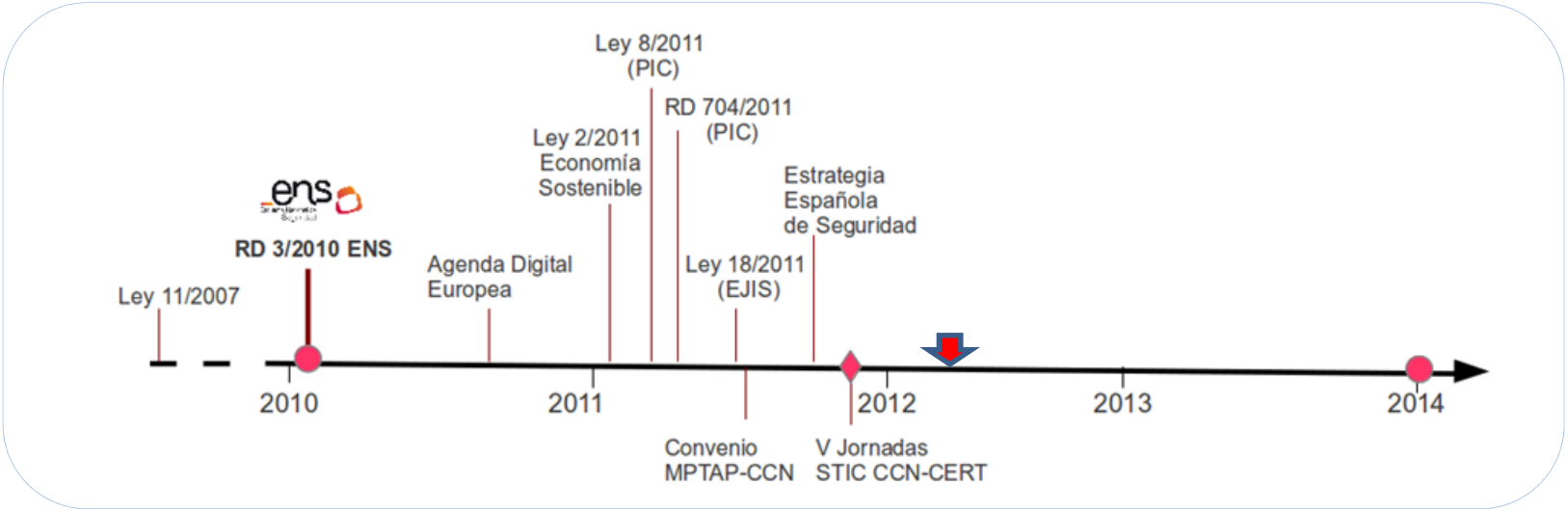
Objetivos:

✓ **Crear la confianza que permita** a ciudadanos y AA.PP., **el ejercicio de derechos y el cumplimiento de deberes a través de estos medios**.

✓ **Introducir lenguaje y elementos comunes: Para guiar** y facilitar la interacción de las AA.PP. y para **facilitar la comunicación de requisitos de seguridad a la Industria.**

Dónde estamos

- **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.
- En los procedimientos **crece la proporción del soporte electrónico frente al papel**; y, cada vez más, ya no hay papel.
- **La información y los servicios están sometidos a riegos** provenientes de acciones malintencionadas o ilícitas, errores o fallos y accidentes o desastres.



Abordar la adecuación

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:

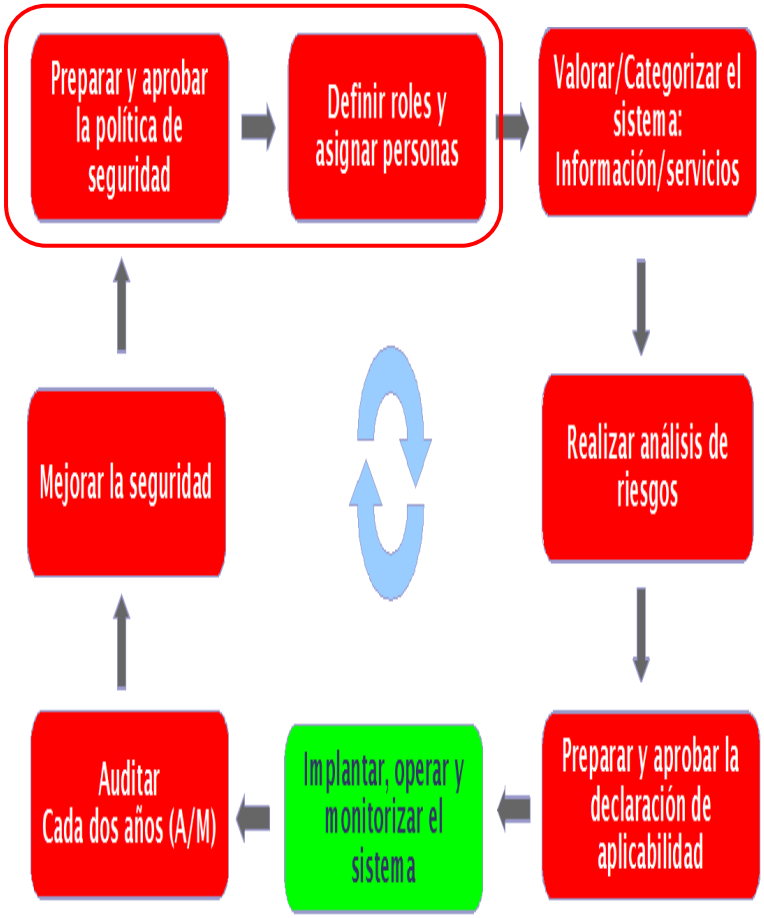
a) Los activos que constituyen el sistema.

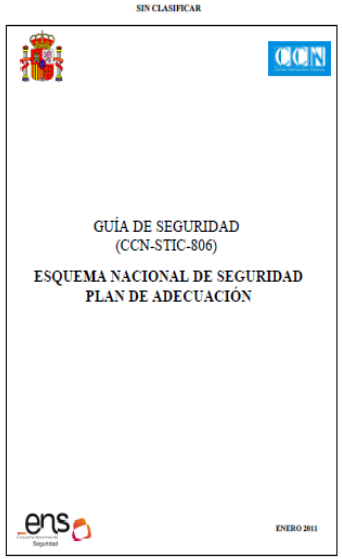
b) La categoría del sistema, según lo previsto en el artículo 43.

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.




SIN CLASIFICAR

GUÍA DE SEGURIDAD
(CCN-STIC-806)

ESQUEMA NACIONAL DE SEGURIDAD
PLAN DE ADECUACIÓN

ENERO 2011

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:


SIN CLASIFICAR

GUÍA DE SEGURIDAD
(CCN-STIC-805)

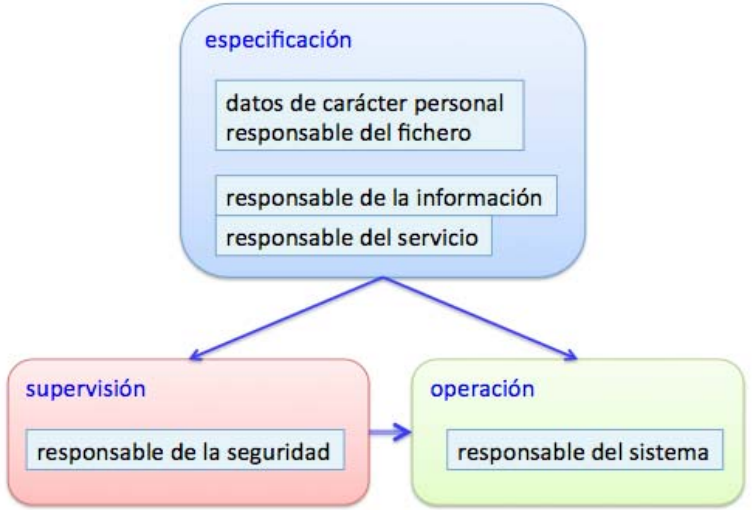
ESQUEMA NACIONAL DE SEGURIDAD
POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

SEPTIEMBRE 2011

3. CONTENIDO.....
- 3.1. MISIÓN DEL ORGANISMO.....
- 3.2. MARCO NORMATIVO.....
- 3.3. ORGANIZACIÓN DE LA SEGURIDAD.....
- 3.4. CONCIENCIACIÓN Y FORMACIÓN .....
- 3.5. GESTIÓN DE RIESGOS .....
- 3.6. PROCESO DE APROBACIÓN Y REVISIÓN.

Atención a:

- ✓ Los roles en el ENS.
- ✓ Ubicación adecuada en la organización.
- ✓ La segregación de funciones.



Categorizar los sistemas

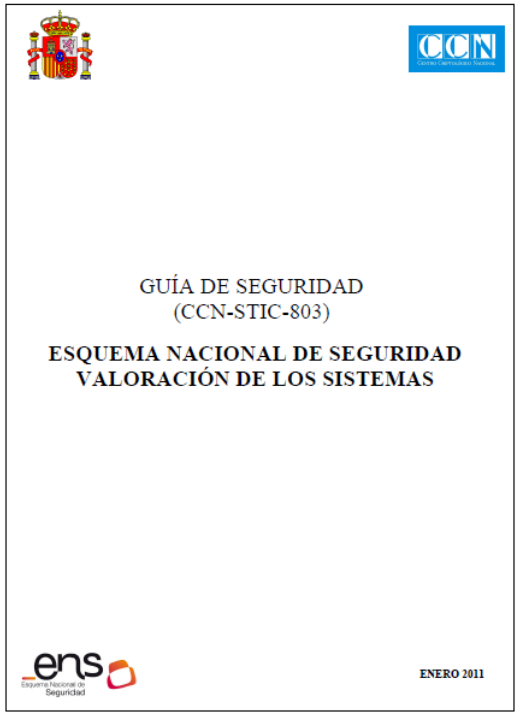
✓ Categorizar los sistemas es necesario para modular el equilibrio entre la importancia de los sistemas y el esfuerzo dedicado a su seguridad y satisfacer el principio de proporcionalidad.

✓ La determinación de la categoría de un sistema se basa en la valoración del impacto que tendría un incidente con repercusión en la capacidad organizativa para:

- Alcanzar sus objetivos.
- Proteger los activos a su cargo.
- Cumplir sus obligaciones diarias de servicio.
- Respetar la legalidad vigente.
- Respetar los derechos de las personas.

✓ A fin de poder determinar el impacto se tendrán en cuenta las dimensiones de la seguridad:

- Disponibilidad
- Autenticidad
- Integridad
- Confidencialidad
- Trazabilidad



Medidas de seguridad

Dimensiones				MEDIDAS DE SEGURIDAD	
Afectadas	B	M	A		
				org	**Marco organizativo**
categoría	aplica	=	=	org.1	Política de seguridad
categoría	aplica	=	=	org.2	Normativa de seguridad
categoría	aplica	=	=	org.3	Procedimientos de seguridad
categoría	aplica	=	=	org.4	Proceso de autorización
				op	**Marco operacional**
				op.pl	Planificación
categoría	aplica	+	++	op.pl.1	Análisis de riesgos
categoría	aplica	=	=	op.pl.2	Arquitectura de seguridad
categoría	aplica	=	=	op.pl.3	Adquisición de nuevos componentes
D	n.a.	aplica	=	op.pl.4	Dimensionamiento / Gestión de capacidades
categoría	n.a.	n.a.	aplica	op.pl.5	Componentes certificados
				op.acc	Control de acceso
A T	aplica	=	=	op.acc.1	Identificación
I C A T	aplica	=	=	op.acc.2	Requisitos de acceso
I C A T	n.a.	aplica	=	op.acc.3	Segregación de funciones y tareas
I C A T	aplica	=	=	op.acc.4	Proceso de gestión de derechos de acceso
I C A T	aplica	+	++	op.acc.5	Mecanismo de autenticación
I C A T	aplica	+	++	op.acc.6	Acceso local (local logon)
I C A T	aplica	+	=	op.acc.7	Acceso remoto (remote login)
				op.exp	Explotación
categoría	aplica	=	=	op.exp.1	Inventario de activos
categoría	aplica	=	=	op.exp.2	Configuración de seguridad
categoría	n.a.	aplica	=	op.exp.3	Gestión de la configuración

Dimensiones				MEDIDAS DE SEGURIDAD	
Afectadas	B	M	A		
categoría	aplica	=	=	op.exp.4	Mantenimiento
categoría	n.a.	aplica	=	op.exp.5	Gestión de cambios
categoría	aplica	=	=	op.exp.6	Protección frente a código dañino
categoría	n.a.	aplica	=	op.exp.7	Gestión de incidencias
T	n.a.	n.a.	aplica	op.exp.8	Registro de la actividad de los usuarios
categoría	n.a.	aplica	=	op.exp.9	Registro de la gestión de incidencias
T	n.a.	n.a.	aplica	op.exp.10	Protección de los registros de actividad
categoría	aplica	+	=	op.exp.11	Protección de claves criptográficas
				op.ext	Servicios externos
categoría	n.a.	aplica	=	op.ext.1	Contratación y acuerdos de nivel de servicio
categoría	n.a.	aplica	=	op.ext.2	Gestión diaria
D	n.a.	n.a.	aplica	op.ext.9	Medios alternativos
				op.cont	Continuidad del servicio
D	n.a.	aplica	=	op.cont.1	Análisis de impacto
D	n.a.	n.a.	aplica	op.cont.2	Plan de continuidad
D	n.a.	n.a.	aplica	op.cont.3	Pruebas periódicas
				op.mon	Monitorización del sistema
categoría	n.a.	n.a.	aplica	op.mon.1	Detección de intrusión
categoría	n.a.	n.a.	aplica	op.mon.2	Sistema de métricas
				mp	**Medidas de protección**
				mp.if	Protección de las instalaciones e infraestructuras
categoría	aplica	=	=	mp.if.1	Áreas separadas y con control de acceso
categoría	aplica	=	=	mp.if.2	Identificación de las personas
categoría	aplica	=	=	mp.if.3	Acondicionamiento de los locales
D	aplica	+	=	mp.if.4	Energía eléctrica
D	aplica	=	=	mp.if.5	Protección frente a incendios
D	n.a.	aplica	=	mp.if.6	Protección frente a inundaciones
categoría	aplica	=	=	mp.if.7	Registro de entrada y salida de equipamiento
D	n.a.	n.a.	aplica	mp.if.9	Instalaciones alternativas
				mp.per	Gestión del personal
categoría	n.a.	aplica	=	mp.per.1	Caracterización del puesto de trabajo
categoría	aplica	=	=	mp.per.2	Deberes y obligaciones

Dimensiones				MEDIDAS DE SEGURIDAD	
Afectadas	B	M	A		
D	n.a.	aplica	=	mp.s.8	Protección frente a la denegación de servicio
D	n.a.	n.a.	aplica	mp.s.9	Medios alternativos

- ✓ Incorporar el cumplimiento del ENS en los pliegos de prescripciones técnicas de las contrataciones.
- ✓ Cláusula tipo para los pliegos.

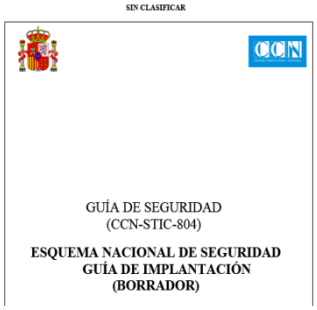
GOBIERNO DE ESPAÑA
MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS

Cumplimiento del ENS. Auditoría de la seguridad


SIN CLASIFICAR

GUÍA DE SEGURIDAD
(CCN-STIC-802)

ESQUEMA NACIONAL DE SEGURIDAD
GUÍA DE AUDITORÍA


SIN CLASIFICAR

GUÍA DE SEGURIDAD
(CCN-STIC-804)

ESQUEMA NACIONAL DE SEGURIDAD
GUÍA DE IMPLANTACIÓN
(BORRADOR)


SIN CLASIFICAR

GUÍA DE SEGURIDAD
(CCN-STIC-808)

VERIFICACIÓN DEL CUMPLIMIENTO DE LAS MEDIDAS EN EL ENS

SEPTIEMBRE 2011

Artículo 34. Auditoría de la seguridad.

1. Los sistemas de información a los que se refiere el presente real decreto serán objeto de una auditoría regular ordinaria, al menos cada dos años, que verifique el cumplimiento de los requerimientos del presente Esquema Nacional de Seguridad.

- ✓ **Política de seguridad (805) + Roles, funciones y procedimientos de designación (801).**
- ✓ **Categorización de los sistemas (803)**. Identificación y valoración de información manejada y servicios prestados.
- ✓ **Análisis de riesgos (Magerit / PILAR).** Valoración de las medidas de seguridad presentes.
- ✓ **Plan de adecuación (806).** Análisis de insuficiencias detectadas; incumplimientos del anexo II y riesgos no asumibles; plazos estimados de ejecución.
- ✓ **Documentación de la seguridad.**

Instrumentos: 801, 802, 804, 805, 806, 808, PILAR/µPILAR – Perfil ENS

NIVEL DE MADUREZ		DESCRIPCIÓN DEL NIVEL
Nivel	%	
L0	0	Inexistente. Esta salvaguarda no existe en este momento.
L1	10	Inicial/ad hoc. Se hace cuando se considera adecuado, pero no está establecido.
L2	50	Reproducible, pero intuitivo. Se realiza, pero no está formalizado documentalmente.
L3	90	Proceso definido. Se realiza y está definido documentalmente (procedimientos).
L4	95	Gestionado y medible. Se están gestionando y son susceptibles de ser medidas.
L5	100	Optimizado. La medida está definida, medida y se aplica proceso de mejora y optimización.

Cumplimiento del ENS. Publicación de la 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.

- ✓ **Manifestación expresa de que el sistema cumple lo establecido en el ENS.**
- ✓ No se observan, por el momento, referencias a la conformidad con el ENS en la sección de declarativas de las sedes electrónicas.
- ✓ 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.

Conocer el estado de seguridad

El ENS establece la obligación de conocer regularmente el estado de la seguridad:

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.

Así mismo se contempla el establecimiento de un sistema de medición:

4.6.2 Sistema de métricas [op.mon.2].

dimensiones	todas		
categoría	básica	media	alta
	no aplica	no aplica	aplica

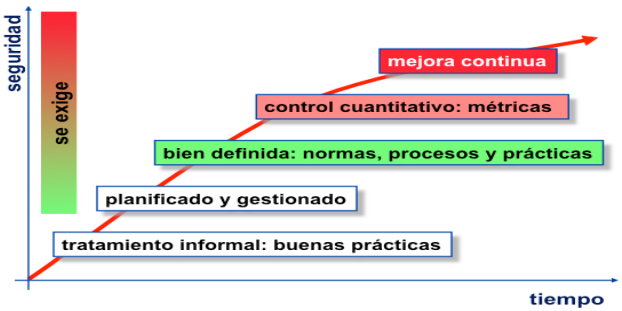
Categoría ALTA

Se establecerá un conjunto de indicadores que mida el desempeño real del sistema en materia de seguridad, en los siguientes aspectos:

a) Grado de implantación de las medidas de seguridad.

b) Eficacia y eficiencia de las medidas de seguridad.

c) Impacto de los incidentes de seguridad.



Fuente: trabajo en curso sobre la guía CCN-STIC 815

De interés para conocer:

- ✓ La evolución de la implantación del ENS.
- ✓ El estado de seguridad general de la Administración.
- ✓ El estado de seguridad de un organismo concreto.

GOBIERNO DE ESPAÑA
MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS

Guías e instrumentos

Esfuerzo realizado para proporcionar guías e instrumentos de apoyo:

Guías CCN-STIC publicadas:

- 800 - Glosario de Términos y Abreviaturas del ENS.
- 801 - Responsables y Funciones en el ENS.
- 802 - Auditoría del 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 - Guía de Creación de un CERT/CSIRT.
- 812 - Seguridad en Entornos y Aplicaciones Web.
- 813 - Componentes certificados.
- 814 - Seguridad en correo electrónico.
- 815 - Indicadores y Métricas en el ENS.

En desarrollo:

- 816 - Seguridad en Redes Inalámbricas en el ENS.
- 817 - Criterios Comunes para la Gestión de Incidentes de Seguridad en el ENS.
- 818 - Herramientas de seguridad.
- MAGERIT v3

Próximamente:

- 819 – Requisitos de seguridad en redes privadas virtuales en el ENS.
- 820 – Requisitos de seguridad de cloud computing en el ENS
- 821 – Seguridad en DNS en el ámbito del ENS.

Programas de apoyo:

- PILAR y µPILAR

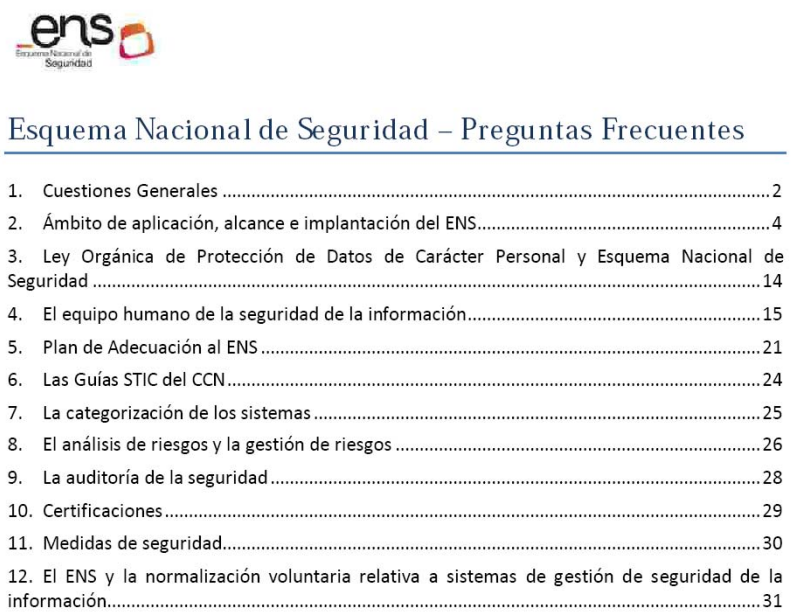
Servicios de respuesta a incidentes de seguridad CCN-CERT

+ Esquema Nacional de Evaluación y Certificación

Convenio de colaboración
GOBIERNO DE ESPAÑA
MINISTERIO DE POLITICA TERRITORIAL Y ADMINISTRACIÓN PÚBLICA
CNI - CCN
centro nacional de inteligencia · centro criptológico nacional
INAP
INSTITUTO NACIONAL DE ADMINISTRACIÓN PÚBLICA

Orientación

- Escucha y resolución de dudas de manera continuada.
- Construcción de 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.



ens
Esquema Nacional 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

URL: https://www.ccn-cert.cni.es
URL: http://administracionelectronica.gob.es/

GOBIERNO DE ESPAÑA
MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS

Formación en línea y presencial

CCN-CERT

Cursos on-line de Seguridad de la Información

CCN-CERT

Aviso CCN-CERT

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 resolucion **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

Convenio de colaboración

GOBIERNO DE ESPAÑA — MINISTERIO DE POLITICA TERRITORIAL Y ADMINISTRACIÓN PUBLICA

CNI-CCN centro nacional de inteligencia · centro criptológico nacional

INAP INSTITUTO NACIONAL DE ADMINISTRACIÓN PÚBLICA

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

Colaboración de la Industria con las AA.PP.

- ✓ Ayudar a conocer y analizar la **situación de partida**.
- ✓ Elaborar el **plan de adecuación**.
- ✓ Asesorar sobre ciertos aspectos:
  - **Alcance** (información y servicios incluidos).
  - **Organización de la seguridad**.
  - Elaboración de **política de seguridad**.
  - Preparación de **declaración de conformidad**.
- ✓ **Valorar los sistemas,** para su categorización.
- ✓ Analizar **los riesgos.**
- ✓ Elaborar la **declaración de aplicabilidad.**
- ✓ **Implantar** las medidas de seguridad.
- ✓ Aplicar **guías y herramientas** para adecuación.
- ✓ **Auditar** la conformidad con el ENS.
- ✓ Elaborar la **declaración de conformidad con ENS**.

ENS, 27001 y 27002

- **ENS, RD 3/2010**
  - **Es una norma jurídica**, al servicio de la realización de derechos de los ciudadanos y de aplicación obligatoria a todas las AA.PP.
  - **Trata la 'protección' de la información y los servicios** y exige la gestión continuada de la seguridad, para lo cual cabe aplicar un sistema de gestión de seguridad de la información.
- **ISO/IEC 27001**
  - **Es una 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 contra 27001 tiene parte del camino recorrido para lograr su conformidad con el ENS.
- **ISO/IEC 27002**
  - Aunque muchas de las medidas indicadas en el anexo II del ENS coinciden con controles de 27002, **el ENS es más preciso y establece un sistema de protección proporcionado a la información y servicios a proteger** para racionalizar la implantación de medidas y reducir la discrecionalidad.
  - 27002 carece de esta proporcionalidad, quedando a la mejor opinión del auditor que certifica la conformidad con 27001.
  - **El ENS contempla diversos aspectos de especial interés para la** protección de la información y los servicios de **administración electrónica** (por ejemplo, aquellos relativos a la firma electrónica) no recogidos en 27002.

GOBIERNO DE ESPAÑA
MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS

ENS, 27001 y 27002

Política de seguridad
- Principios básicos
- Requisitos mínimos
- Medidas y proporcionalidad

ens Esquema Nacional de Seguridad

Guías de seguridad e instrumentos de apoyo

- Guías CCN-STIC
- Programas de apoyo: PILAR, µPILAR
- Magerit v2

CCN Centro Criptológico Nacional

Convenio de colaboración CNI-CCN INAP

Normalización

- Normalización STIC nacional e internacional (27001, 27002, ...)

Infraestructuras y servicios comunes

CCN-CERT Centro Criptológico Nacional

@firma

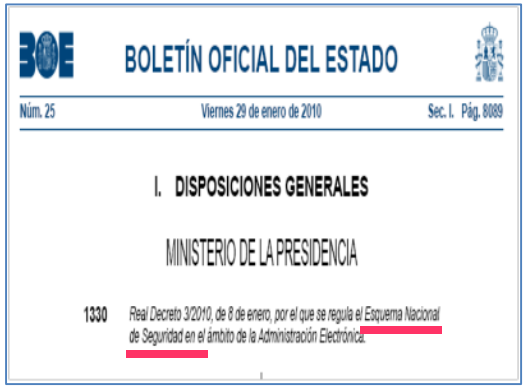
...

Formación

Convenio de colaboración CNI-CCN INAP

GOBIERNO DE ESPAÑA
MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS

Para saber más sobre seguridad y administración electrónica


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.*

http://www.boe.es/boe/dias/2010/01


Estrategia Española de Seguridad

Una responsabilidad de todos

GOBIERNO DE ESPAÑA
MADRID 2011

www.lamoncloa.gob.es/NR
/.../EstrategiaEspanolaDeSeguridad.pdf


Country Reports May 11

Spain Country Report

http://www.epractice.eu/en/factsheets/

http://www.enisa.europa.eu/act/sr/files/
country-reports/?searchterm=country%20reports

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

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

http://administracionelectronica.gob.es

GOBIERNO DE ESPAÑA
MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS

Muchas gracias

X Foro de Seguridad de RedIRIS

- **Portal CCN-CERT – ENS:**

https://www.ccn-cert.cni.es/index.php?option=com_content&view=article&id=2420&Itemid=211&lang=es

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

http://administracionelectronica.gob.es

- **Preguntas frecuentes:**

https://www.ccn-cert.cni.es/index.php?option=com_content&view=article&id=2855&Itemid=211&lang=es

http://administracionelectronica.gob.es

- **Espacio virtual del ENS:**

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

- **Contacto para preguntas, dudas: ens@ccn-cert.cni.es**