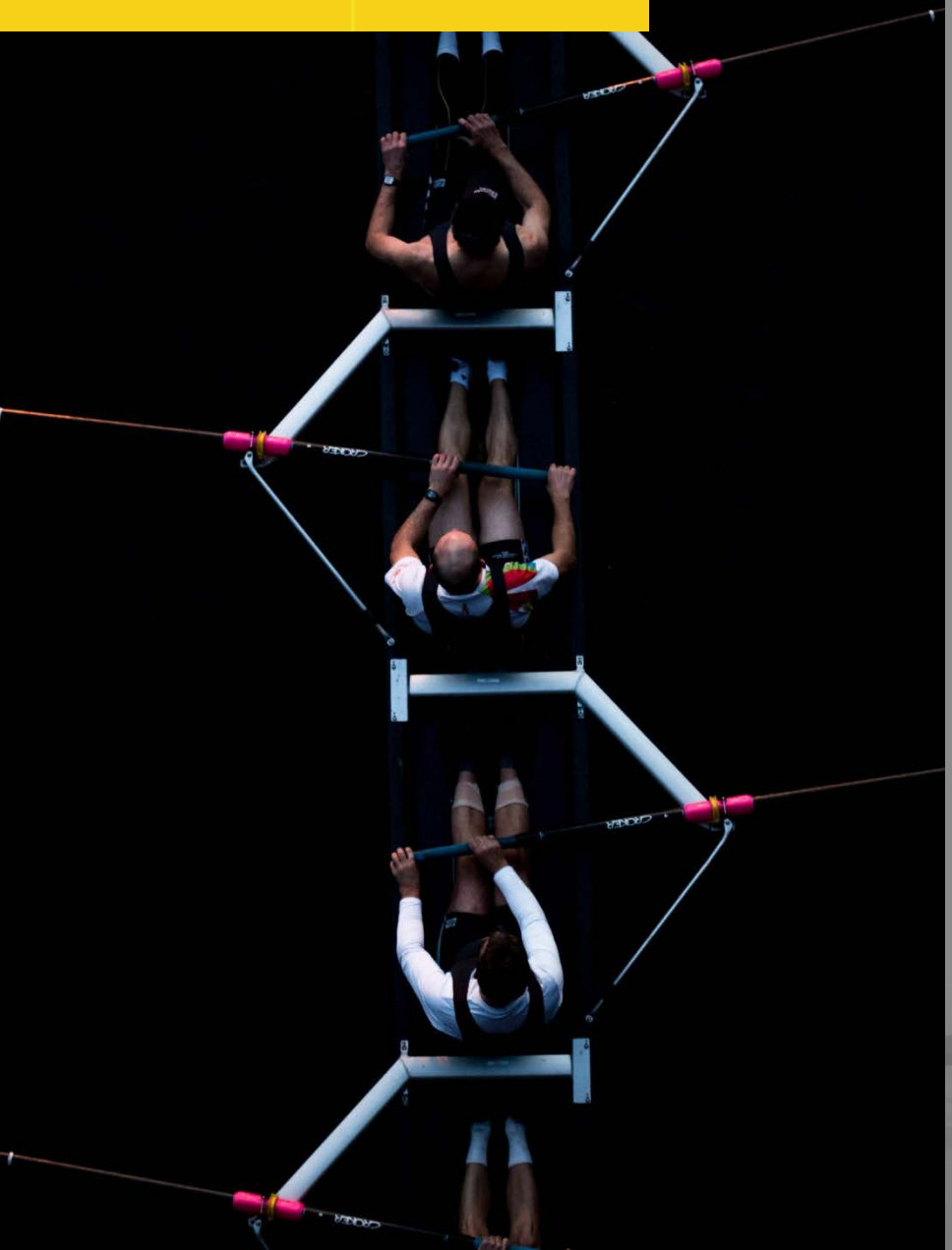
GOBIERNO DE ESPAÑA
MINISTERIO DE HACIENDA Y FUNCIÓN PÚBLICA

FEMP
FEDERACION ESPAÑOLA DE MUNICIPIOS Y PROVINCIAS



GUÍA ESTRATÉGICA PARA EL CUMPLIMIENTO DEL ESQUEMA NACIONAL DE SEGURIDAD (ENS) POR LAS ADMINISTRACIONES LOCALES. Cuaderno de Recomendaciones

Estado de situación, evolución y desarrollo del ENS

Madrid 31 de enero de 2018

Miguel A. Perchín de Torres
Secretaría General de Administración Digital

Contenidos

1. ¿Por qué es necesaria la seguridad de la información y los servicios?
2. Implantar la seguridad en el Sector Público: el Esquema Nacional de Seguridad
3. Conformidad con el ENS
4. Retos y conclusiones

1. Por qué es necesaria la seguridad de la información y los servicios

Por qué es necesaria la seguridad de información y servicios

- ✓ **Los ciudadanos esperan que los servicios se presten en condiciones de confianza y seguridad** equivalentes a las que encuentran cuando se acercan personalmente a las oficinas de la Administración.
- ✓ Buena parte de la información y los servicios manejados por las AA.PP. **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.
- ✓ **Los servicios 24 x 7 -> requieren seguridad 24 x 7.**

Incremento notable de incidentes

La Capacidad de Respuesta de Ciberincidentes del Centro Criptológico Nacional (CCN-CERT) gestionó en el año **2016** un total de **20.940 ciberincidentes, detectados principalmente en el sector público y** en empresas consideradas de interés estratégico para España, lo que supone **un 14,5% más que en 2015**.

De ellos, el 3,6% fueron considerados como muy altos o críticos, en función del grado de peligrosidad determinado por el tipo de amenaza, origen del atacante, perfil de la víctima, número o tipología de los sistemas afectados, impacto, inclusión o no en una campaña de mayor calado, etc.

2. Implantar la seguridad en el Sector Público: el Esquema Nacional de Seguridad

Ley 39/2015

13. Derechos de las personas

h) A la **protección de datos** de carácter personal, y en particular a la **seguridad y confidencialidad de los datos** que figuren **en los ficheros, sistemas y aplicaciones** de las Administraciones Públicas.

Ley 40/2015

La **seguridad**, principio de actuación

Artículo 3. Principios generales

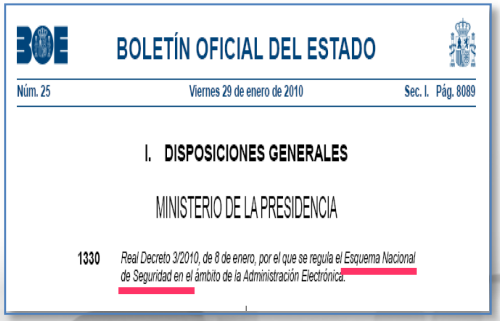
2. Las Administraciones Públicas se relacionarán entre sí y con sus órganos, organismos públicos y entidades vinculados o dependientes a través de medios electrónicos, **que aseguren la interoperabilidad y seguridad** de los sistemas y soluciones adoptadas por cada una de ellas, **garantizarán la protección de los datos de carácter personal**, y facilitarán preferentemente la prestación conjunta de servicios a los interesados.

Artículo 156. Esquema Nacional de Interoperabilidad y Esquema Nacional de Seguridad

2. **El Esquema Nacional de Seguridad** tiene por objeto establecer la política de seguridad en la utilización de medios electrónicos **en el ámbito de la presente Ley**, y está constituido por los principios básicos y requisitos mínimos que garanticen adecuadamente la seguridad de la información tratada.

El Esquema Nacional de Seguridad

- ✓ **Instrumento legal – Real Decreto 3/2010**
- ✓ **Establece la política de seguridad** en la utilización de medios electrónicos.
- ✓ **De aplicación al Sector Público.**
- ✓ Resulta de un **esfuerzo colectivo**: AGE, CC.AA., CC.LL.-FEMP, EJIS (Justicia), CRUE + Opinión Industria TIC.
- ✓ **Actualizado** (RD 951/2015, BOE de 4.11.2015).


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.

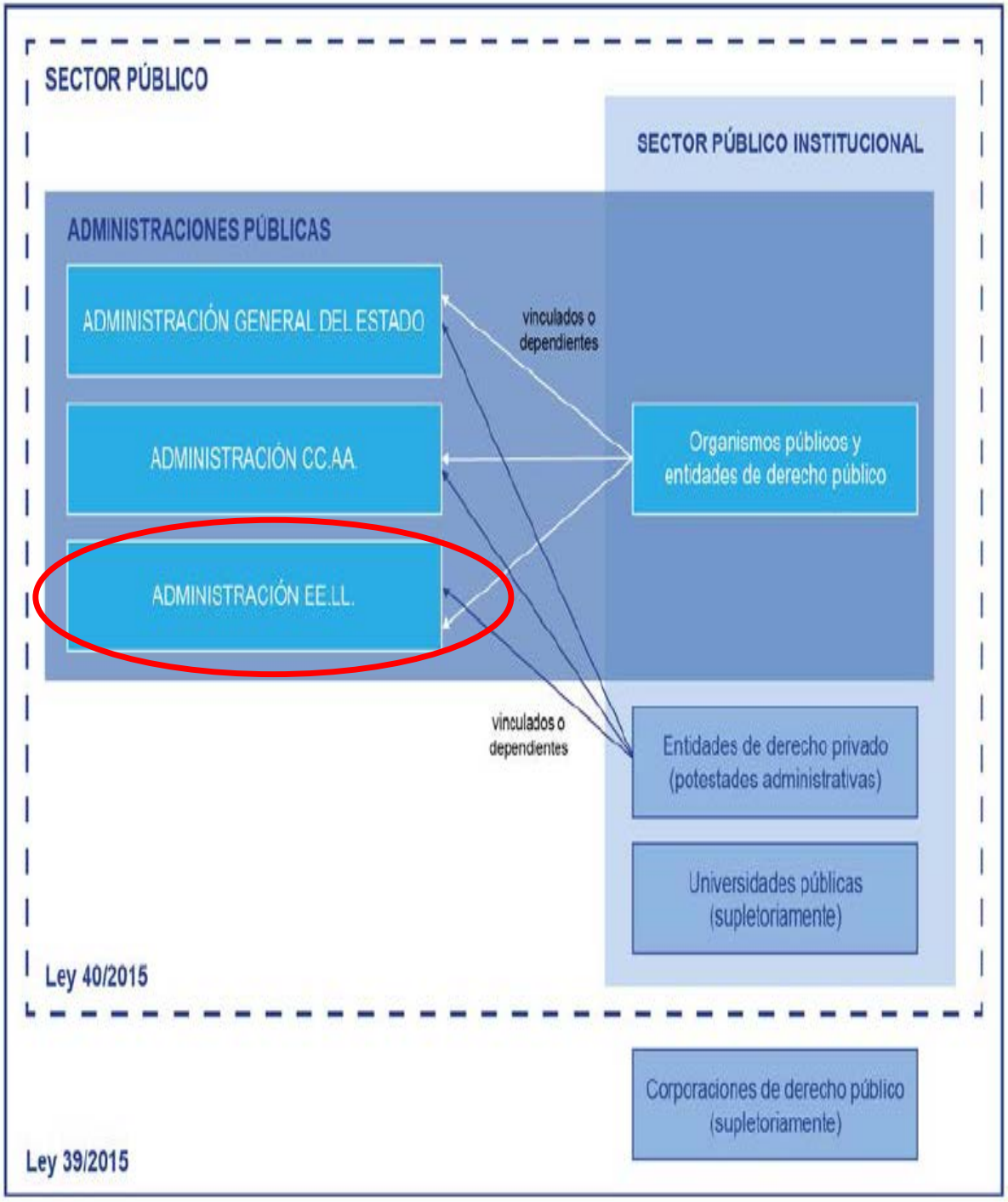

BOLETÍN OFICIAL DEL ESTADO
Núm. 264 Miércoles 4 de noviembre de 2015 Sec. I. Pág. 104246

I. DISPOSICIONES GENERALES

MINISTERIO DE LA PRESIDENCIA

11881 Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

ens
Esquema Nacional de Seguridad



GOBIERNO DE ESPAÑA
MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS

CCN

GUÍA DE SEGURIDAD
(CCN-STIC-830)

ÁMBITO DE APLICACIÓN DEL ESQUEMA NACIONAL DE SEGURIDAD

ens Esquema Nacional de Seguridad

SEPTIEMBRE 2016

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 la prevención detección y corrección**.

- ✓ **Promover un tratamiento homogéneo de la seguridad** que facilite la cooperación en la prestación de servicios de administración electrónica cuando participan diversas entidades mediante **lenguaje y elementos comunes**, adecuados al quehacer de la Administración.

  - **Para guiar la actuación de las entidades del Sector Público en materia de seguridad** de las tecnologías de la información.
  - **Para facilitar la interacción** y la cooperación .
  - Para **facilitar la comunicación de los requisitos de seguridad de la información a la Industria**.

- ✓ **Proporcionar liderazgo en materia de buenas practicas.**

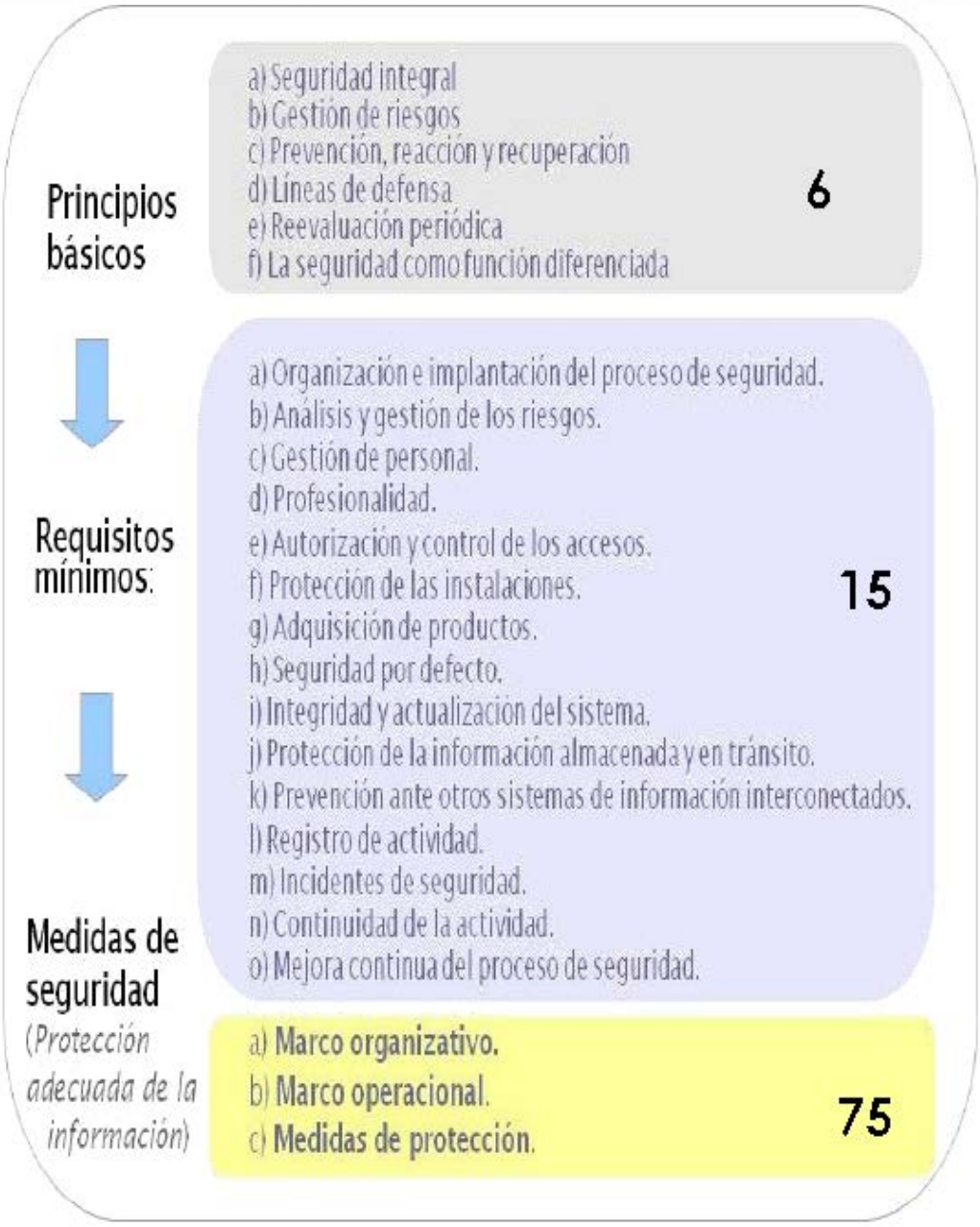
Artículo 5. ***La seguridad como un proceso integral.***

1. La seguridad se entenderá como un proceso integral constituido por **todos los elementos técnicos, humanos, materiales y organizativos, relacionados con el sistema**. La aplicación del Esquema Nacional de Seguridad estará presidida por este principio, que excluye cualquier actuación puntual o tratamiento coyuntural.

2. Se prestará la **máxima atención a la concienciación de las personas que intervienen en el proceso y a sus responsables jerárquicos**, **para que, ni la ignorancia, ni la falta de organización y coordinación, ni instrucciones inadecuadas, sean fuentes de riesgo para la seguridad**.

7 elementos principales

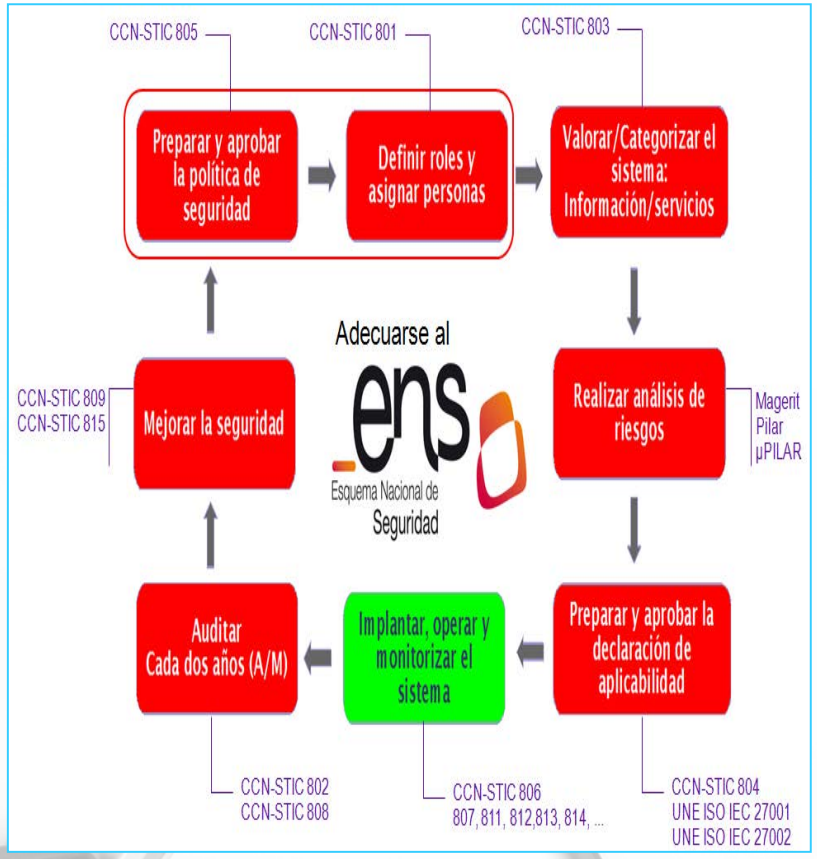
1. Los **Principios básicos,** que sirven de guía.
2. **Los Requisitos mínimos,** de obligado cumplimiento.
3. La **Categorización de los sistemas** para la adopción de **medidas de seguridad** proporcionadas.
4. La **auditoría de la seguridad** que verifique el cumplimiento del ENS.
5. La **respuesta a incidentes de seguridad**. Papel de CCN- CERT.
6. El uso de **productos certificados**. Papel del Organismo de Certificación (OC-CCN).
7. La **formación y concienciación**.



Adecuarse al ENS: 8 acciones principales

Aspectos principales de la adecuación:

- Elaborar y aprobar la **política de seguridad** (art. 11)
- **Definir roles** y asignar personas. **Responsable de seguridad**. (art. 10)
- **Categorizar** los sistemas (art. 27)
- **Analizar los riesgos** está actualizado (art. 27)
- Seleccionar y elaborar la **declaración de aplicabilidad;** e implantar las **medidas de seguridad**. (Anexo II)
- **Auditar la seguridad** (art. 34)
- Publicar la **conformidad** en la sede electrónica (art. 41)
- **Informar del estado de la seguridad** (art. 35)



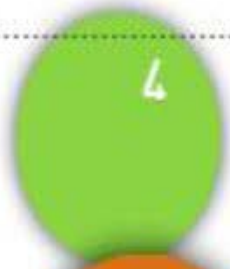
ESQUEMA NACIONAL DE SEGURIDAD

75 MEDIDAS DE SEGURIDAD

ens
Esquema Nacional de Seguridad

MARCO ORGANIZATIVO

El marco organizativo está constituido por un conjunto de medidas relacionadas con la organización global de la seguridad



- POLÍTICA DE SEGURIDAD
- NORMATIVA DE SEGURIDAD
- PROCEDIMIENTOS DE SEGURIDAD
- PROCESO DE AUTORIZACIÓN

MARCO OPERACIONAL

El marco operacional está constituido por las medidas a tomar para proteger la operación del sistema como conjunto integral de componentes para un fin

- PLANIFICACIÓN
- CONTROL DE ACCESO
- EXPLOTACIÓN
- SERVICIOS EXTERNOS
- CONTINUIDAD DEL SERVICIO
- MONITORIZACIÓN DEL SISTEMA

MEDIDAS DE PROTECCIÓN

Las medidas de protección, se centrarán en proteger activos concretos, según su naturaleza, con el nivel requerido en cada dimensión de seguridad.

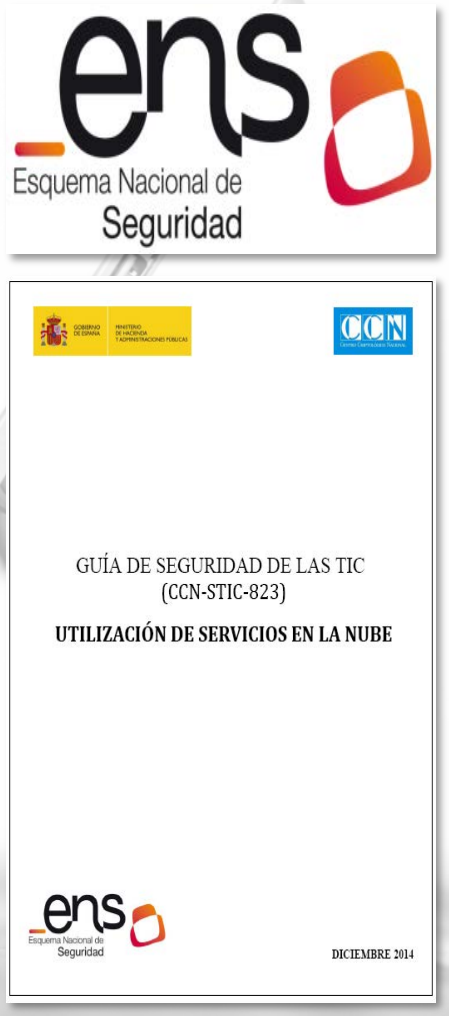
- INSTALACIONES E INFRAESTRUCTURAS
- GESTIÓN DEL PERSONAL
- PROTECCIÓN DE LOS EQUIPOS
- PROTECCIÓN DE LAS COMUNICACIONES
- PROTECCIÓN SOPORTES DE INFORMACIÓN
- PROTECCIÓN APLICACIONES INFORMÁTICAS
- PROTECCIÓN DE LA INFORMACION
- PROTECCIÓN DE LOS SERVICIOS

Infraestructuras y servicios comunes.
Oportunidades en seguridad

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.

- ✓ **Reducción del perímetro físico**: se reduce la carga en medidas de protección de las instalaciones e infraestructuras *[mp.if]* para las entidades usuarias.
- ✓ **Reducción del perímetro lógico**: se reduce la carga para las entidades usuarias en medidas tales como: explotación *[mp.exp],* protección de las aplicaciones informáticas *[mp.sw],* protección de los servicios *[mp.s]* y monitorización del sistema *[op.mon].*
- ✓ **Gestión de incidentes**: se reduce la carga de gestión de incidentes *[op.exp7].*
- ✓ **Mejor elasticidad**: para hacer frente a picos de actividad o ataques de denegación de servicio *[mp.s.8].*
- ✓ **Mejor conformidad con estándares**: para mejor recuperación, integración, interoperabilidad, portabilidad, integración con herramientas de seguridad *(medidas varias de tipo [op]).*



Instrucciones técnicas de seguridad

Disposición adicional cuarta. *Desarrollo del Esquema Nacional de Seguridad.*

1. Sin perjuicio de las propuestas que pueda acordar el Comité Sectorial de Administración Electrónica según lo establecido en el artículo 29, apartado 2, se desarrollarán las siguientes instrucciones técnicas de seguridad que serán de obligado cumplimiento por parte de las Administraciones públicas:

a) Informe del estado de la seguridad.
b) Notificación de incidentes de seguridad.
c) Auditoría de la seguridad.
d) Conformidad con el Esquema Nacional de Seguridad.
e) Adquisición de productos de seguridad.
f) Criptología de empleo en el Esquema Nacional de Seguridad.
g) Interconexión en el Esquema Nacional de Seguridad.
h) Requisitos de seguridad en entornos externalizados.

2. La aprobación de estas instrucciones se realizará de acuerdo con el procedimiento establecido en el citado artículo 29 apartados 2 y 3.

Estrategias

Estrategia TIC AGE

Leyes 39 y 40/2015

Racionaliza y Comparte

Identidad y firma electrónica

Interoperabilidad

Archivo electrónico

Seguridad

- Esquema Nacional de Seguridad - ENS
- Instrucciones Técnicas
- Métodos, instrumentos y normas
- Políticas de Seguridad de la Información
- Evaluación y certificación
- Normalización en

Instrucciones Técnicas de Seguridad

Valorar Escuchar Imprimir PDF

El Real Decreto 3/2010, recogido en el artículo 156 de la Ley 40/2015, establece las instrucciones técnicas de seguridad, esenciales para lograr una adecuada, homogénea y coherente implantación de los requisitos y medidas recogidos en el Esquema Nacional de Seguridad.

- Informe del Estado de la Seguridad
- Conformidad con el Esquema Nacional de Seguridad

Informe del Estado de la Seguridad

- Resolución de 7 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de Informe del Estado de la Seguridad
- Guía CCN-STIC 815 Indicadores y métricas en el ENS
- Guía CCN-STIC 824 Informe del Estado de Seguridad
- Guía CCN-STIC 844 Manual de Usuario de INES / Anexo
- Herramienta INES (Informe Nacional del Estado de Seguridad)

Conformidad con el Esquema Nacional de Seguridad

- Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad
- Conformidad con el Esquema Nacional de Seguridad
- Guía CCN-STIC 809 Declaración y Certificación de Conformidad con el ENS

Próximamente…

INSTRUCCIÓN TÉCNICA DE SEGURIDAD SOBRE NOTIFICACIÓN DE INCIDENTES DE SEGURIDAD.

I. Objeto.
II. Ámbito de aplicación.
III. Criterios de determinación del nivel de impacto.
IV. Notificación obligatoria de los incidentes con nivel de impacto Alto, Muy alto y Crítico.
V. Evidencias a entregar en el caso de incidentes nivel Alto, Muy alto y Crítico.
VI. Obligación de remisión de estadísticas de incidentes.
VII. Notificación de impactos recibidos.
VIII. Desarrollo de herramientas automatizadas para facilitar las notificaciones.
IX. Régimen legal de las notificaciones y comunicación de información.
X. Disposición Adicional.

(Sometidos a cambios)

El Esquema Nacional de Seguridad recoge las medidas que debe aplicar el sector público para cumplir con los requisitos del RGPD en este ámbito

El CCN-CERT y la AEPD establecen un mecanismo de colaboración para ofrecer a las Administraciones Públicas una referencia de cumplimiento normativo en materia de protección de datos y seguridad.

- La herramienta PILAR para Administraciones Públicas incluye desde hoy un módulo para facilitar el cumplimiento
- El Reglamento General de Protección de Datos (RGPD), que establece nuevos requisitos, será aplicable el 25 de mayo de 2018

(Madrid, 12 de diciembre de 2017). El CCN-CERT y la Agencia Española de Protección de Datos (AEPD) han establecido un mecanismo de colaboración con el objetivo de ofrecer a las Administraciones Públicas una referencia de cumplimiento normativo en materia de protección de datos y seguridad ante la próxima entrada en vigor del Reglamento General de Protección de Datos (RGPD) el 25 de mayo de 2018.

El Esquema Nacional de Seguridad y el RGPD establecen la obligación de que las Administraciones Públicas realicen análisis de riesgos para determinar el posible impacto de los tratamientos de datos sobre los derechos y libertades de las personas y las medidas de seguridad aplicables.

En este sentido, la AEPD ha publicado un documento en el que pone de manifiesto que esas medidas de seguridad –en el caso de las AAPP– estarán marcadas por los criterios establecidos en el Esquema Nacional de Seguridad. El Proyecto de Ley Orgánica de Protección de Datos, actualmente en fase de tramitación, lo recoge de la misma forma en su disposición adicional primera.

Fruto de la colaboración, el CCN-CERT y la AEPD han trabajado de forma conjunta para ofrecer una herramienta a las Administraciones Públicas que les permita evaluar de manera sistemática y objetiva los posibles riesgos en materia de protección de datos y de seguridad de la información. Así, la herramienta PILAR incluye desde hoy un módulo de cumplimiento que permite a las AAPP verificar los requisitos establecidos en el RGPD, facilitando la gestión normativa tanto del Reglamento como del Esquema Nacional de Seguridad.

La obligatoriedad de contar con un registro de actividades de tratamiento, designar un Delegado de Protección de Datos o notificar las quiebras de seguridad en caso de producirse son algunos de los aspectos recogidos en este nuevo módulo.

3. Conformidad con el ENS

Auditoría, informe y conformidad

Auditoría de la seguridad
(art. 34; A.III / CCN 802, 804, 808)

Informe del Estado de la seguridad (INES)
(art. 35 / CCN-STIC 815, 824)

Conformidad con el
(art. 41 / CCN-STIC 809)

ens Esquema Nacional de Seguridad

BOLETÍN OFICIAL DEL ESTADO
Núm. 265 Miércoles 2 de noviembre de 2016 Sec. III. Pág. 76363

INSTRUCCIÓN TÉCNICA DE SEGURIDAD DE INFORME DEL ESTADO DE LA SEGURIDAD

ÍNDICE

SIN CLASIFICAR

GOBIERNO DE ESPAÑA · MINISTERIO DE HACIENDA Y ADMINISTRACIONES PUBLICAS · CCN Centro Criptológico Nacional

GUÍA DE SEGURIDAD
(CCN-STIC-824)

ESQUEMA NACIONAL DE SEGURIDAD
INFORME NACIONAL DEL ESTADO DE SEGURIDAD

ens Esquema Nacional de Seguridad

Octubre de 2016

BOLETÍN OFICIAL DEL ESTADO
Núm. 265 Miércoles 2 de noviembre de 2016 Sec. III. Pág. 76365

INSTRUCCIÓN TÉCNICA DE SEGURIDAD DE CONFORMIDAD CON EL ESQUEMA NACIONAL DE SEGURIDAD

ÍNDICE

Conformidad con el ENS

Entidades del Sector 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.**

Según **la categoría del sistema** se distingue entre:

- **Declaración de Conformidad**: de aplicación a sistemas de información de categoría Básica.
- **Certificación de Conformidad**: de aplicación obligatoria a sistemas de información de categoría Media o Alta y voluntaria en el caso de sistemas de información de categoría Básica.

Prestadores de servicios o soluciones: mismos procedimientos y documentos.

Entidades de certificación: Acreditación por ENAC **conforme a** UNE-EN ISO/IEC 17065:2012, para la certificación de sistemas del ámbito de aplicación del **ENS**.


Logotipo de la Entidad Certificadora con marca de certificación acreditada

CERTIFICACIÓN DE CONFORMIDAD CON EL ens Esquema Nacional de Seguridad Categoría MEDIA RD 3/2010

CERTIFICADO DE CONFORMIDAD CON EL ESQUEMA NACIONAL DE SEGURIDAD

"<<Entidad Certificadora>>" certifica que los sistemas de información reseñados, todos ellos de categoría <<señalar categoría máxima aplicable (BÁSICA, MEDIA o ALTA)>> y los servicios que se relacionan, de

<< Entidad [pública o privada], dirección postal>>,

han sido auditados y encontrados conforme con las exigencias del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración, según se indica en el correspondiente Informe de Auditoría de <<fecha>> para:

<<enumerar los sistemas de información y los servicios objeto de la certificación>>.

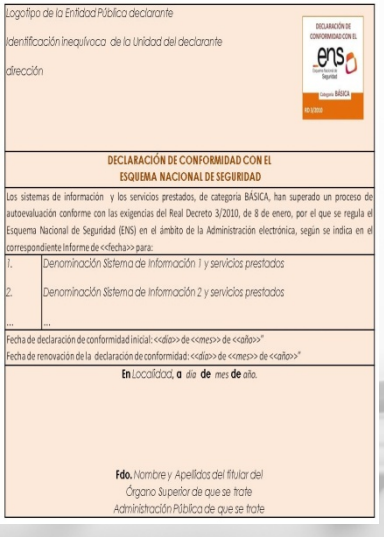
Fecha de certificación de conformidad inicial: <<día>> de <<mes>> de <<año>>.
Fecha de renovación de la certificación de conformidad: <<día>> de <<mes>> de <<año>>.

Número de certificado: <<número de certificado>>

Fecha<<Localidad (la que corresponda)>>, <<día>> de <<mes>> de <<año>>".
Firma: <<Nombre y Apellidos del responsable competente de la Entidad Certificadora>>.

Firma del responsable de la Entidad Certificadora:

Nombre completo /razón social de la Entidad Certificadora y pág. web.
Dirección postal / electrónica.
Código Postal. Provincia. País.


Logotipo de la Entidad Pública declarante

Identificación inequívoca de la Unidad del declarante

dirección

DECLARACIÓN DE CONFORMIDAD CON EL ESQUEMA NACIONAL DE SEGURIDAD

Los sistemas de información y los servicios prestados, de categoría BÁSICA, han superado un proceso de autoevaluación conforme con las exigencias del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad (ENS) en el ámbito de la Administración electrónica, según se indica en el correspondiente Informe de <<fecha>> para:

1.	Denominación Sistema de información 1 y servicios prestados
2.	Denominación Sistema de información 2 y servicios prestados
...	...

Fecha de declaración de conformidad inicial: <<día>> de <<mes>> de <<año>>"
Fecha de renovación de la declaración de conformidad: <<día>> de <<mes>> de <<año>>"

En Localidad, a día de mes de año.

Fdo. Nombre y Apellidos del titular del Órgano Superior de que se trate
Administración Pública de que se trate

¿Cuáles son los requisitos para **operadores del Sector Privado**?

Prestadores de servicios o soluciones a AA.PP.
a quienes resulte exigible el cumplimiento del ENS.

Mismos procedimientos que para la Administración:

Sistemas de información de **categoría BÁSICA** → DECLARACIÓN DE CONFORMIDAD CON EL ens Esquema Nacional de Seguridad — Categoría BÁSICA — RD 3/2010

Sistemas de información de **categorías MEDIA o ALTA** → CERTIFICACIÓN DE CONFORMIDAD CON EL ens Esquema Nacional de Seguridad — Categoría ALTA — RD 3/2010

Las entidades de la Administración usuarias **podrán solicitar los Informes de Autoevaluación o Auditoría** correspondientes.

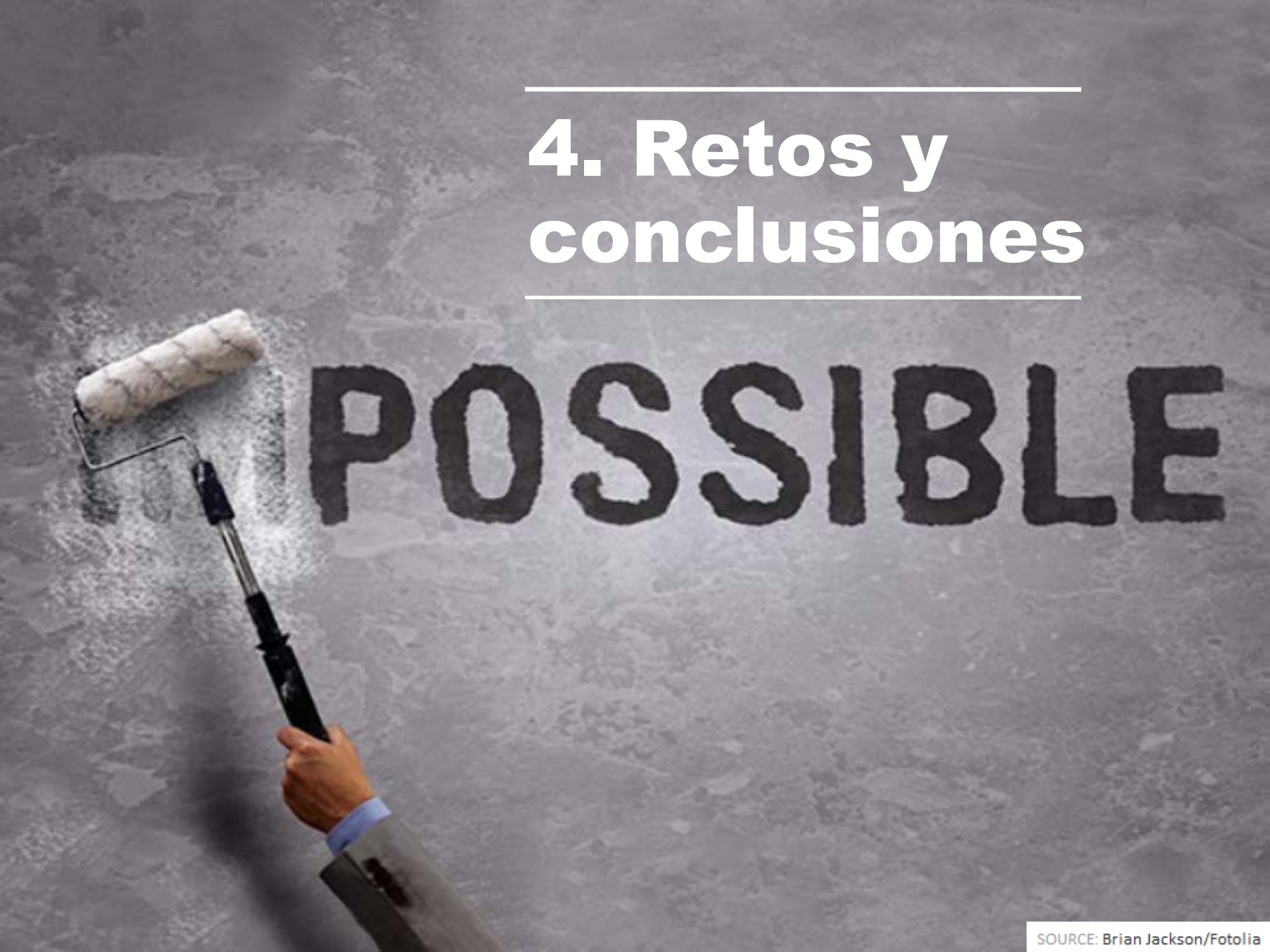
Próximamente…

INSTRUCCIÓN TÉCNICA DE SEGURIDAD DE AUDITORÍA DE LA SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN

Índice

(Sometido a cambios)

4. Retos y conclusiones



SOURCE: Brian Jackson/Fotolia

Conclusiones

- ✓ La **plena aplicación de las leyes 39/2015 y 40/2015** requiere la **protección de la información y los servicios** (en el contexto de la transformación digital).
- ✓ La seguridad de la información y de los servicios **requiere la implicación todos** los elementos técnicos, humanos, materiales y organizativos.
- ✓ **El ENS**, de aplicación al Sector Público, persigue la creación de condiciones de seguridad, **impulsa la gestión continuada y el tratamiento homogéneo de la seguridad**, adaptado al quehacer de la Administración, proporcionando el adecuado respaldo legal.
- ✓ **Auditorías independientes** como base de la aportación de datos al informe de la seguridad y posterior certificación de la conformidad.
- ✓ **Uso de los servicios y plataformas ofrecidos por la Administración**.

Retos

- ✓ **Presupuesto para seguridad proporcionado a la realidad de la transformación digital.**
- ✓ **Avanzar en ciberseguridad de las entidades del Sector Público, mejorando apoyo a las entidades con menos recursos humanos y técnicos.**
- ✓ **Mejorar la seguridad del conjunto y reducir el esfuerzo individual** por parte de las entidades del Sector Público Estatal.
- ✓ **Mejorar la adecuación -> Conformidad con el ENS.**

Esfuerzo colectivo

✓ El RD 3/2010, ITS, Guías CCN-STIC (Serie 800), seguimiento, herramientas, servicios…

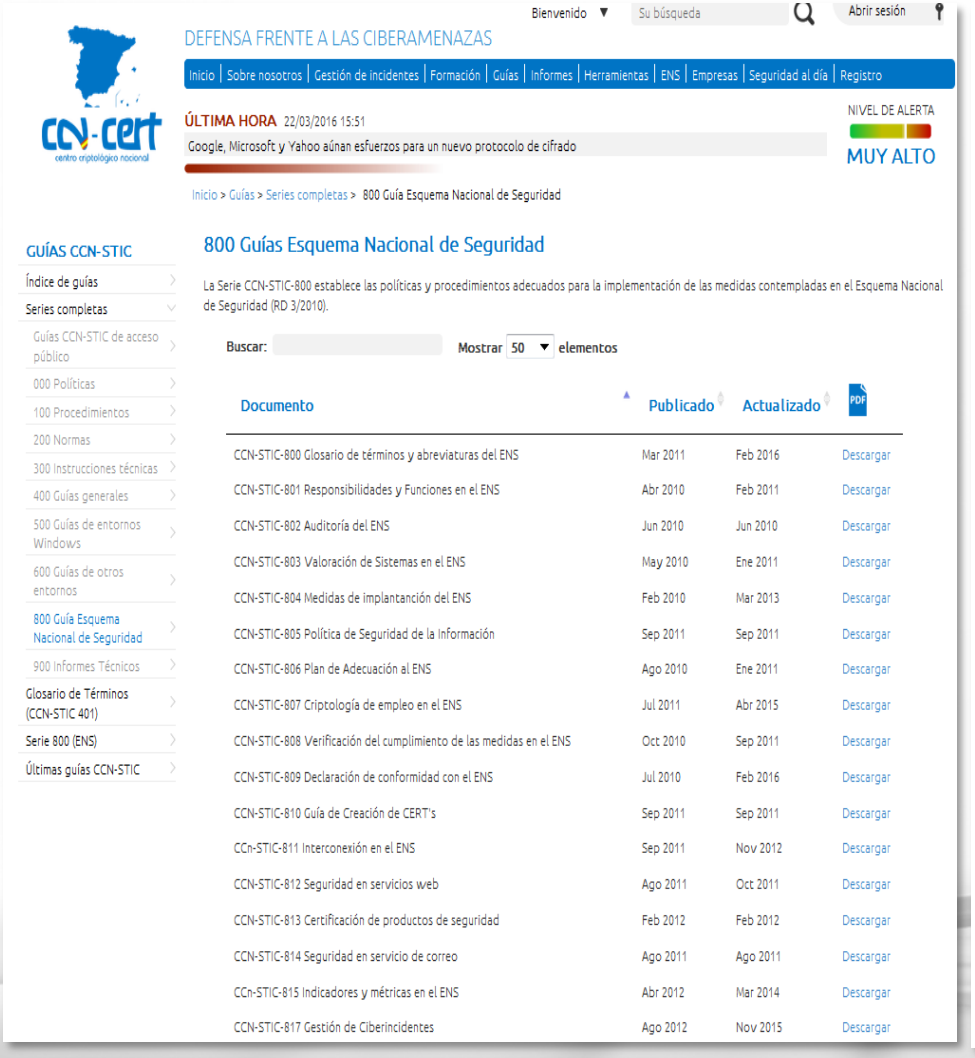
Pero sobre todo:

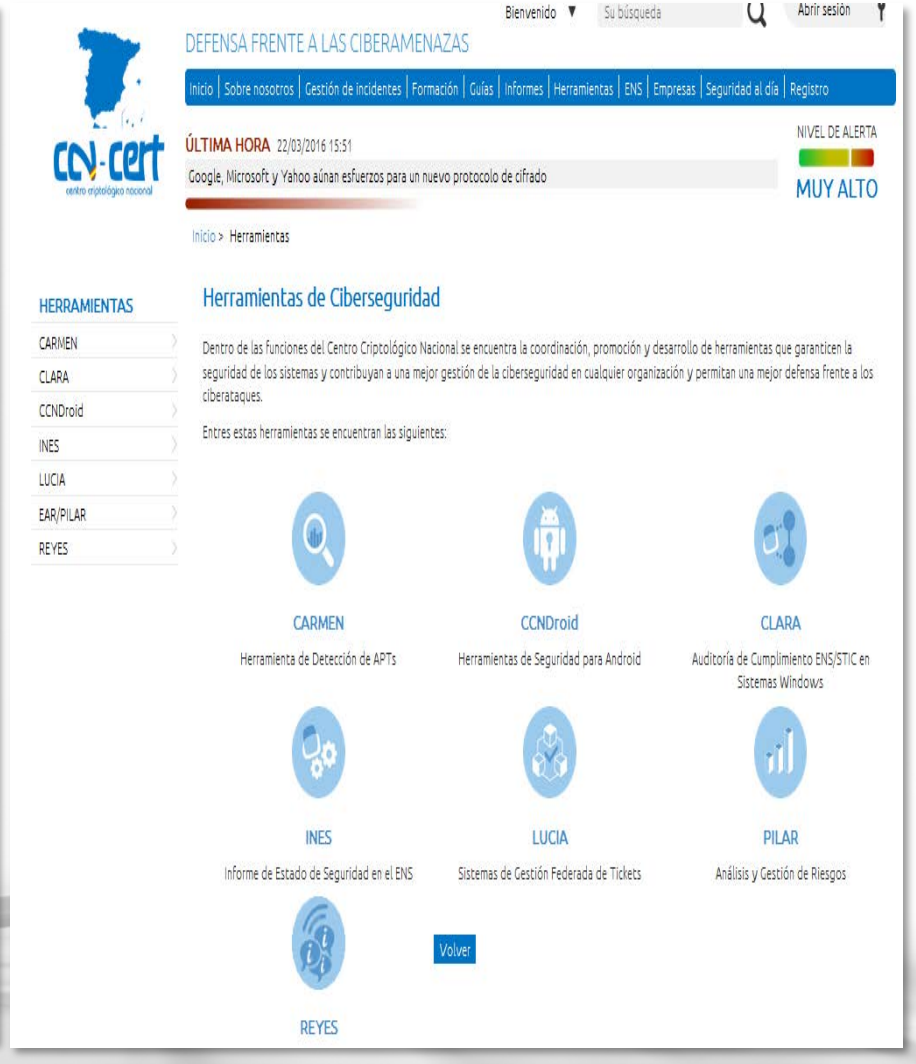
✓ Esfuerzo colectivo del **Sector Público**, **coordinado por MINHAFP-SGAD y CNI-CCN**.

✓ **+ Industria** sector seguridad TIC.

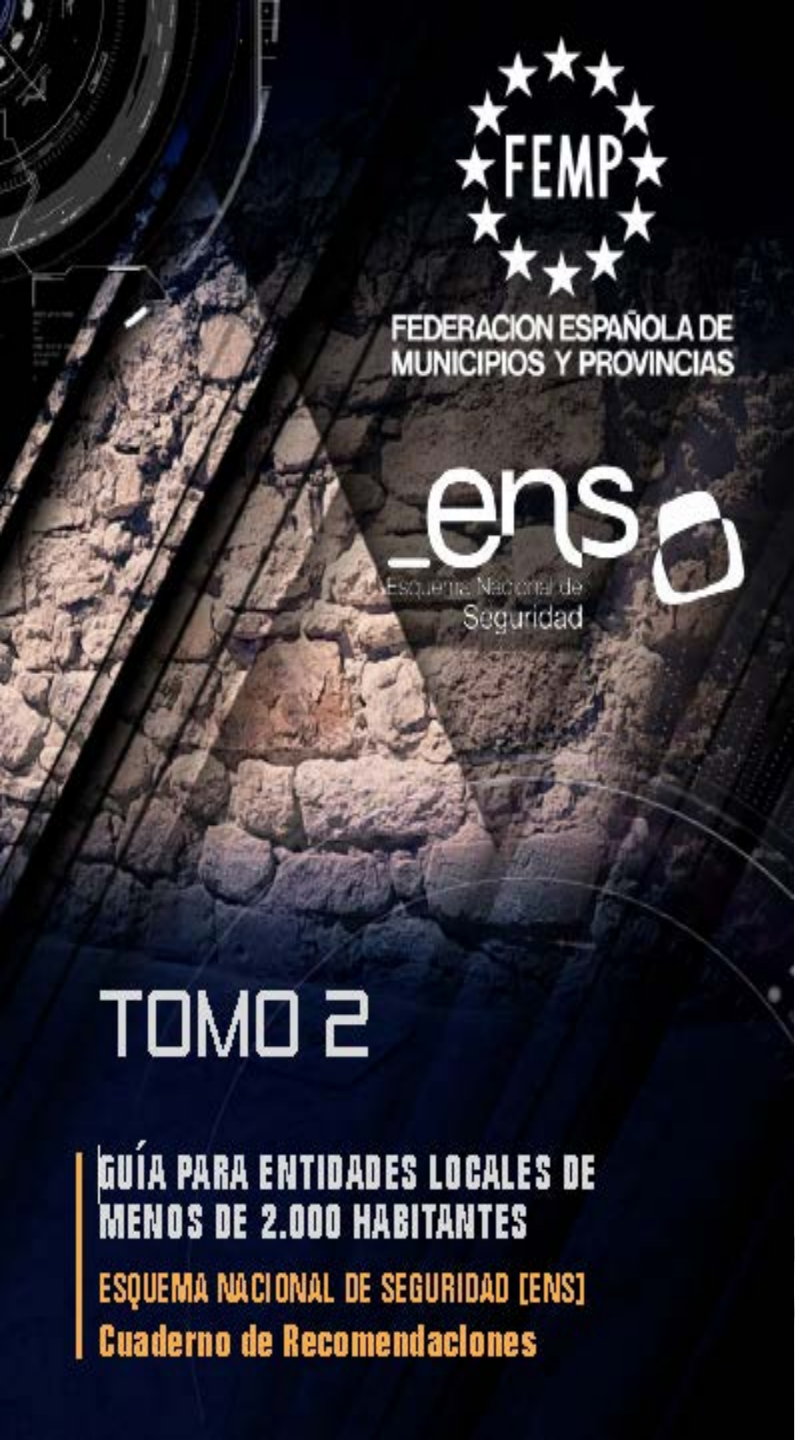
✓ **Convencimiento común:** gestión continuada de la seguridad, con un tratamiento homogéneo y adaptado al quehacer del Sector Público.

Guías y herramientas





ÍNDICE



ÍNDICE

Muchas gracias

- ✓ **Correos electrónicos**
  - ens@ccn-cert.cni.es
  - ines@ccn-cert.cni.es
  - ens.minhap@correo.gob.es
  - ccn@cni.es
  - sondas@ccn-cert.cni.es
  - redsara@ccn-cert.cni.es
  - organismo.certificacion@cni.es
- ✓ **Páginas Web:**
  - http://administracionelectronica.gob.es
  - www.ccn-cert.cni.es
  - www.ccn.cni.es
  - www.oc.ccn.cni.es