



GOBIERNO
DE ESPAÑA

MINISTERIO
DE HACIENDA
Y FUNCIÓN PÚBLICA



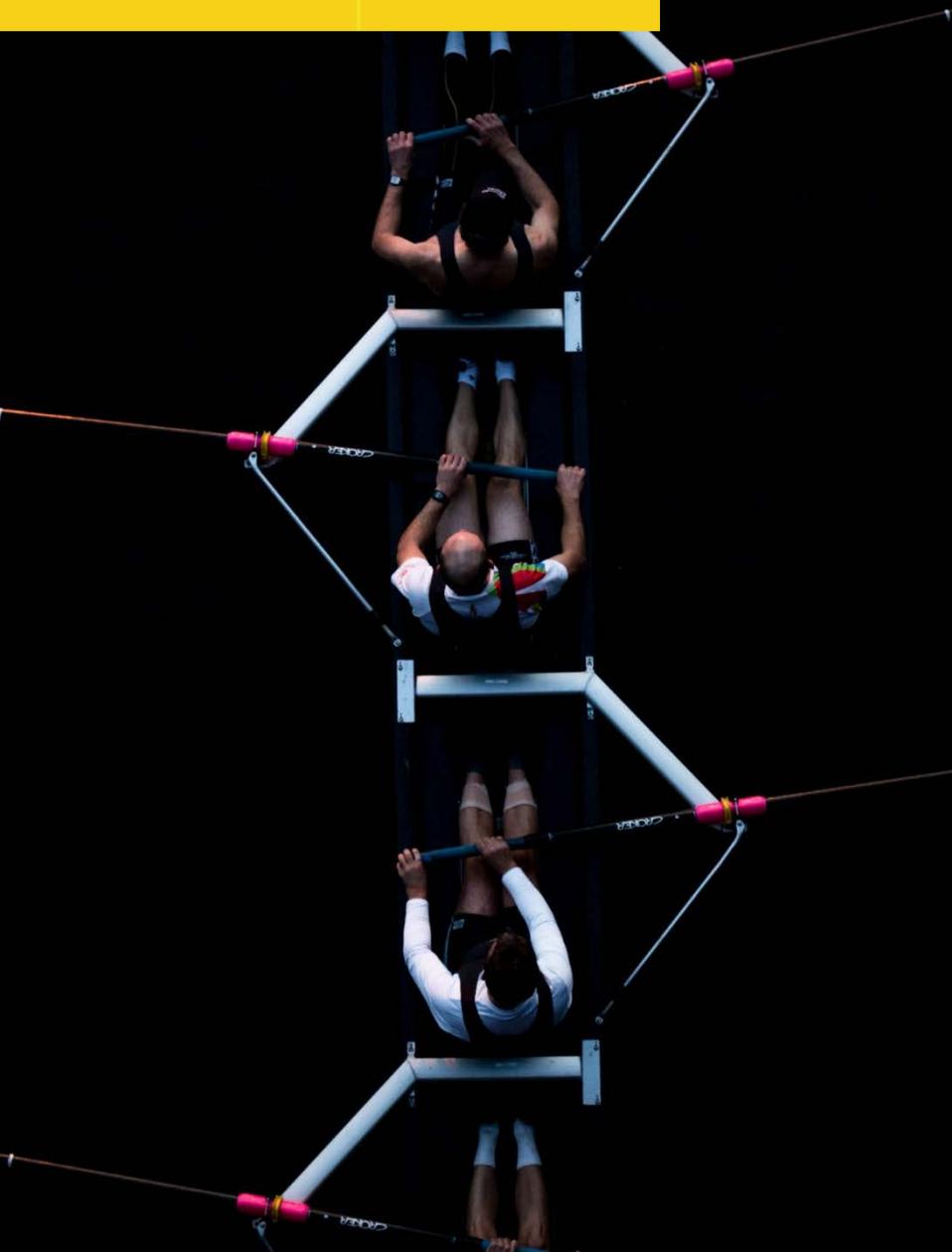
FEDERACION ESPAÑOLA DE
MUNICIPIOS Y PROVINCIAS

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

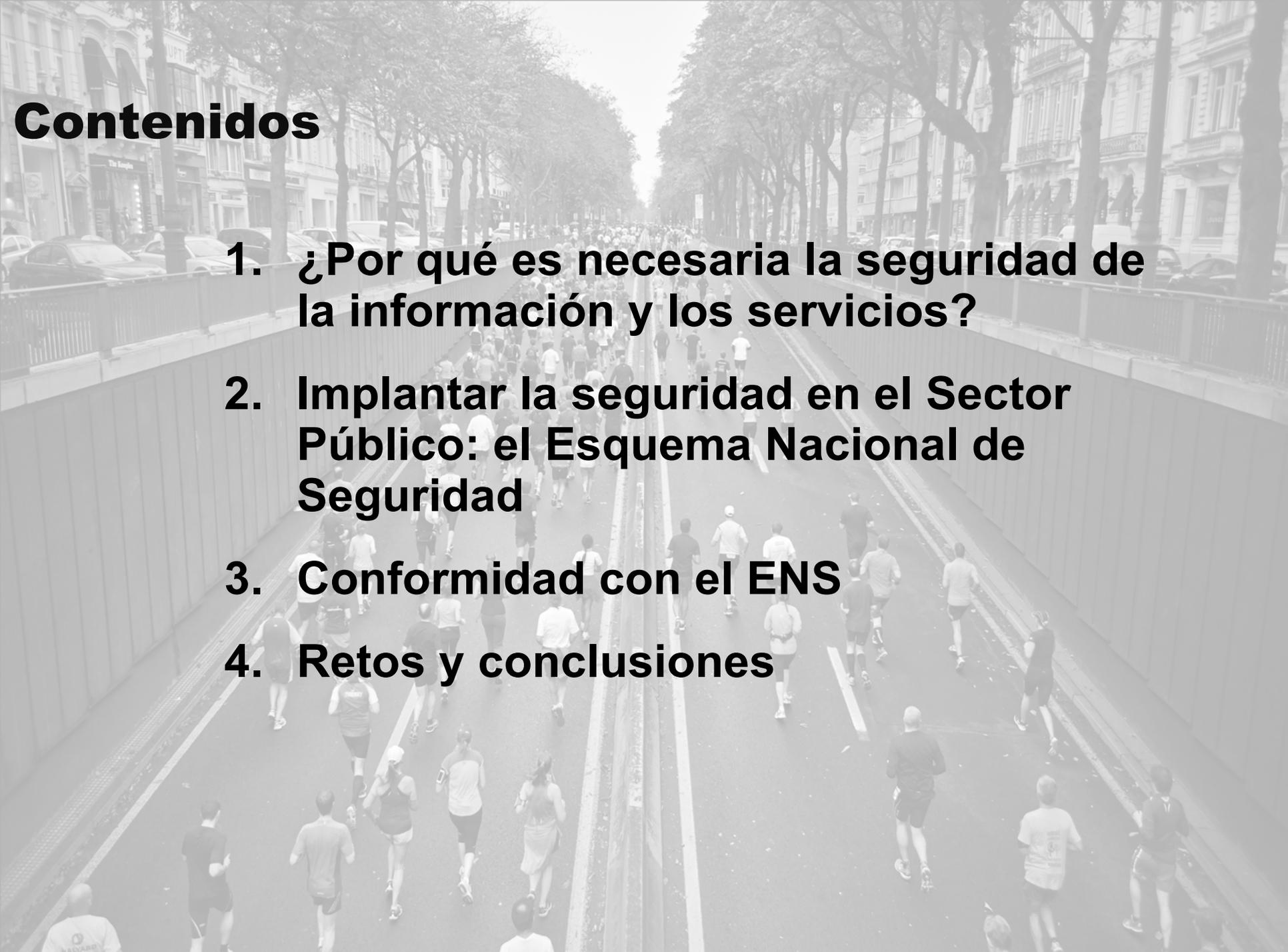
Estado de situación, evolución y desarrollo del ENS

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**

A person stands on a sandy beach with their arms raised, looking out at the ocean. A large, powerful wave is breaking in the background, creating a massive wall of white foam. The sky is overcast with grey clouds. The overall scene is dramatic and emphasizes the scale of the natural world compared to the human figure.

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.



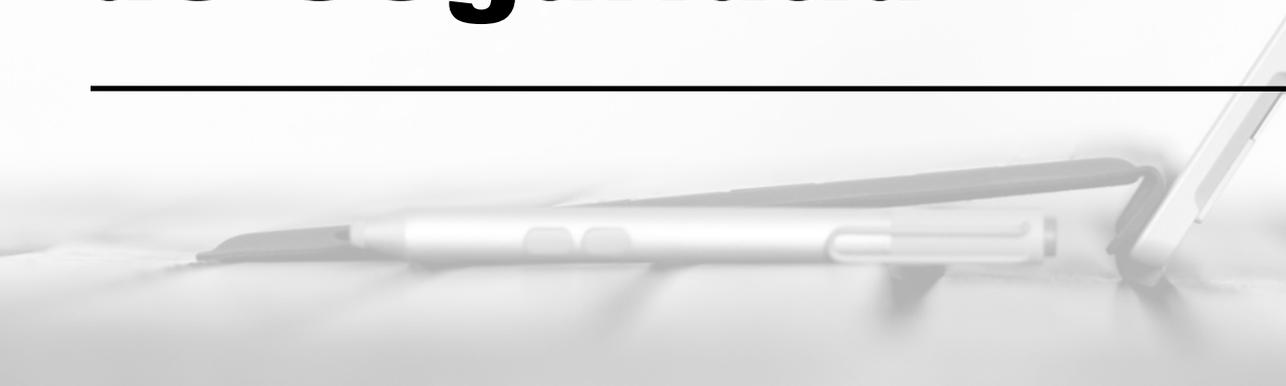
Incremento notable de incidentes



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.

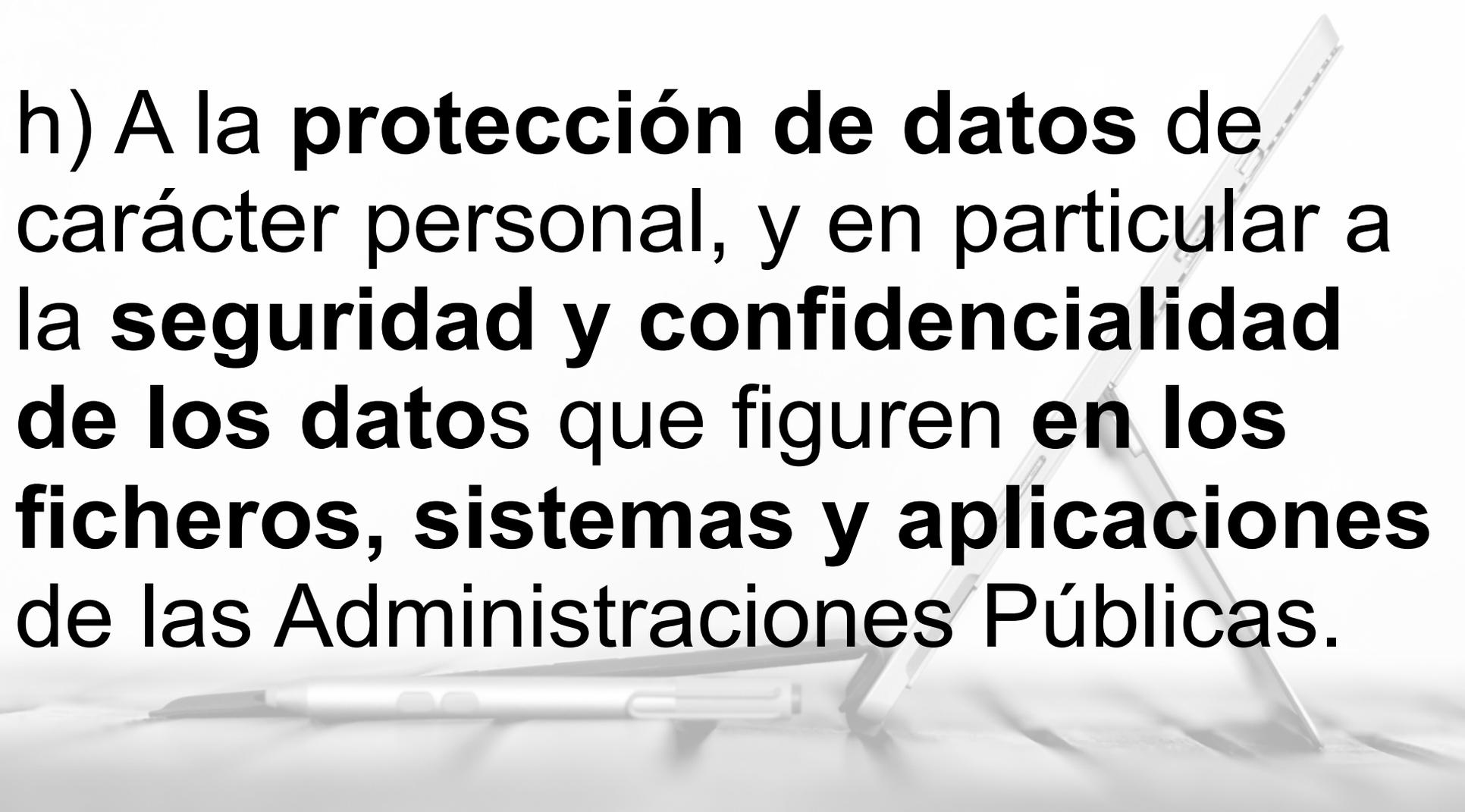
2. Implantar la seguridad en el Sector Público: el Esquema Nacional de Seguridad



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).



SECTOR PÚBLICO

SECTOR PÚBLICO INSTITUCIONAL

ADMINISTRACIONES PÚBLICAS

ADMINISTRACIÓN GENERAL DEL ESTADO

ADMINISTRACIÓN CC.AA.

ADMINISTRACIÓN EE.LL.

Organismos públicos y entidades de derecho público

vinculados o dependientes

Entidades de derecho privado (potestades administrativas)

Universidades públicas (supletoriamente)

Corporaciones de derecho público (supletoriamente)

Ley 40/2015

Ley 39/2015

GUÍA DE SEGURIDAD
(CCN-STIC-830)

ÁMBITO DE APLICACIÓN DEL
ESQUEMA NACIONAL DE SEGURIDAD

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**.

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

6



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.

15



Medidas de seguridad

(Protección adecuada de la información)

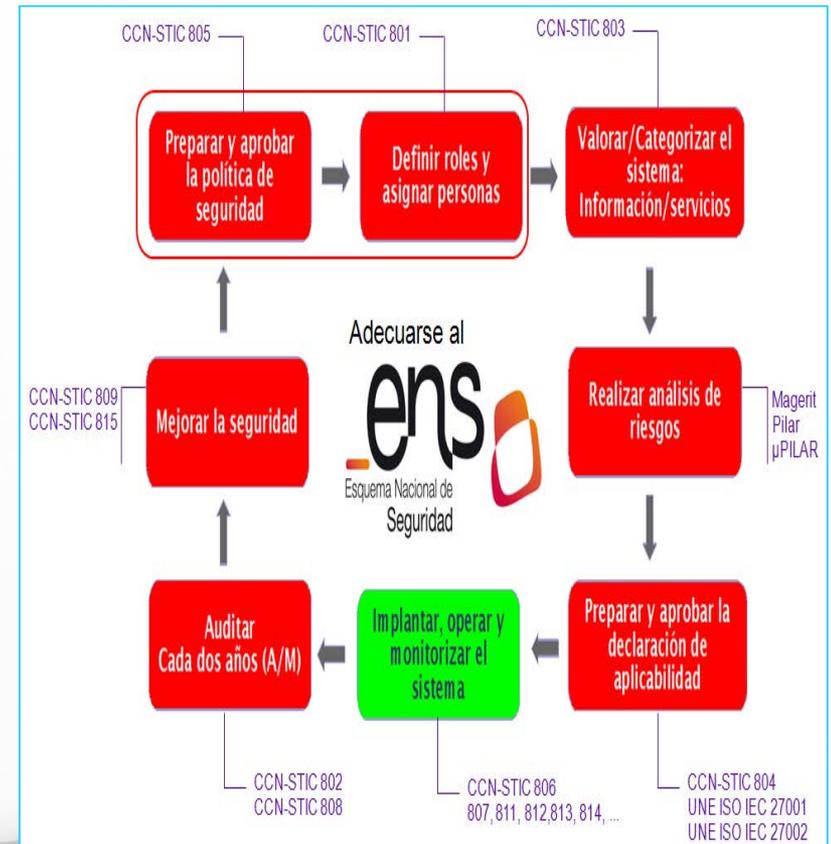
- a) Marco organizativo.
- b) Marco operacional.
- c) Medidas de protección.

75

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



MARCO ORGANIZATIVO

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

4

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

31

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.

40

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

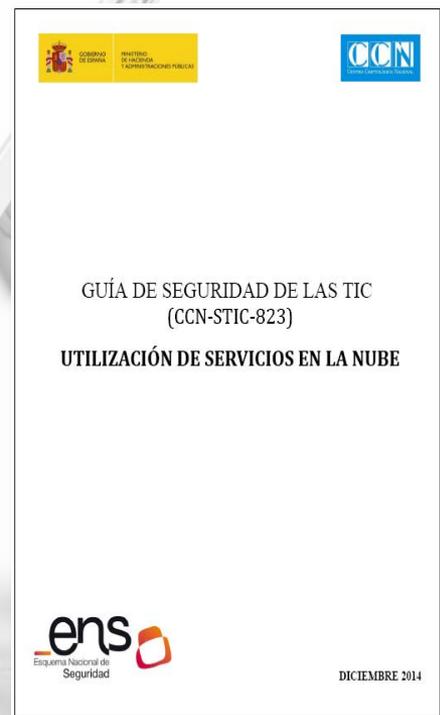
Infraestructuras y servicios comunes.

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.



[Actualidad](#)[Estrategias](#)[Soluciones - CTT](#)[Observatorio - OBSAE](#)[Documen](#)Estás en: [Inicio](#) > [Estrategias](#) > [Seguridad](#) > [Instrucciones Técnicas](#)**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.

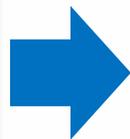
La obligatoriedad de contar con un registro de actividades de tratamiento, designar un Delegado de Protección de Datos o notificar las quebras de seguridad en caso de producirse son algunos de los aspectos recogidos en este nuevo módulo.



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)



INSTRUCCIÓN TÉCNICA DE SEGURIDAD DE INFORME DEL ESTADO DE LA SEGURIDAD

ÍNDICE

- I. Objeto.
- II. Ámbito de aplicación.
- III. Recopilación y comunicación de datos.
- IV. Tratamiento de datos.

SIN CLASIFICAR



GUÍA DE SEGURIDAD
(CCN-STIC-824)

**ESQUEMA NACIONAL DE SEGURIDAD
INFORME NACIONAL DEL ESTADO DE
SEGURIDAD**

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

ÍNDICE

- I. Objeto.
- II. Ámbito de aplicación.
- III. **Procedimientos** de determinación de la conformidad.
- IV. **Declaración de Conformidad** con el Esquema Nacional de Seguridad de sistemas de categoría BÁSICA y su publicidad.
- V. **Certificación de Conformidad** con el Esquema Nacional de Seguridad de sistemas de categoría MEDIA o ALTA y su publicidad.
- VI. **Requisitos de las entidades certificadoras.**
- VII. **Soluciones y servicios prestados por el sector privado.**
- Anexo I. Contenido de la Declaración de Conformidad con el Esquema Nacional de Seguridad.
- Anexo II. Distintivo de Declaración de Conformidad con el Esquema Nacional de Seguridad.
- Anexo III. Contenido de la Certificación de Conformidad con el Esquema Nacional de Seguridad.
- Anexo IV. Distintivo de Certificación de Conformidad con el Esquema Nacional de Seguridad.

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 marco de certificación correspondiente

CERTIFICACIÓN DE CONFORMIDAD CON EL ENS Esquema Nacional de Seguridad

CERTIFICADO DE CONFORMIDAD CON EL ESQUEMA NACIONAL DE SEGURIDAD

<<Entidad Certificadora>> certifica que los sistemas de información reseñados, todos ellos de categoría <<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 electrónica, 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: <<dd>> de <<mes>> de <<año>>.
Fecha de renovación de la certificación de conformidad: <<dd>> de <<mes>> de <<año>>.

Número de certificado: <<número de certificación>>

Fecha <<localidad (a que corresponda)>>, <<dd>> 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 página web.
Dirección postal, electrónica.
Código Postal, Provincia, País.

Logotipo de la Entidad Pública declarante

Identificación inequívoca de la Unidad del declarante

dirección

CERTIFICACIÓN DE CONFORMIDAD CON EL ENS Esquema Nacional de Seguridad

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: <<dd>> de <<mes>> de <<año>>
Fecha de renovación de la declaración de conformidad: <<dd>> de <<mes>> de <<año>>

En Localidad, a 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**



Sistemas de información de categorías **MEDIA o ALTA**



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

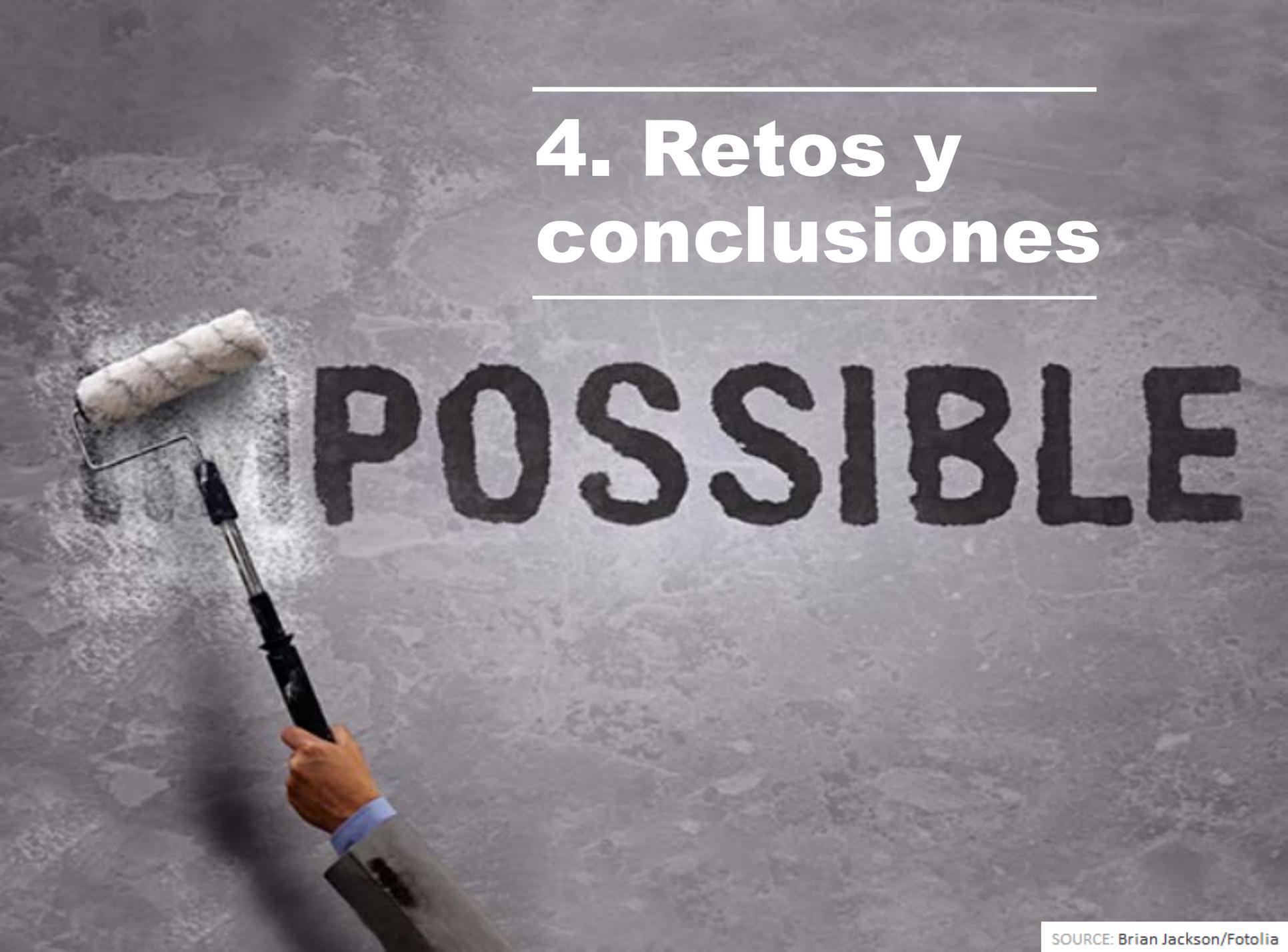
Próximamente...

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

Índice

- I. Objeto.
- II. Ámbito de aplicación.
- III. Propósito de la Auditoría de la Seguridad, obligatoriedad y normativa reguladora.
- IV. Definición del alcance y objetivo de la Auditoría de la Seguridad.
- V. Ejecución de la Auditoría de la Seguridad.
- VI. El Informe de Auditoría.
- VII. Entidades Auditoras del Sector Público.
- VIII. Disposición adicional. Datos personales

4. Retos y conclusiones

A hand in a suit sleeve is using a paint roller to paint the word "POSSIBLE" in large, bold, black letters on a grey wall. The roller is positioned at the start of the word, and the hand is holding the handle. The background is a textured grey wall.

POSSIBLE

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

Bienvenido ▾ Su búsqueda 🔍 Abrir sesión 👤

DEFENSA FRENTE A LAS CIBERAMENAZAS

Inicio | Sobre nosotros | Gestión de incidentes | Formación | Guías | Informes | Herramientas | ENS | Empresas | Seguridad al día | Registro

ÚLTIMA HORA 22/03/2016 15:51 NIVEL DE ALERTA MUY ALTO

Google, Microsoft y Yahoo añan esfuerzos para un nuevo protocolo de cifrado

Inicio > Guías > Series completas > 800 Guía Esquema Nacional de Seguridad

GUÍAS CCN-STIC

Índice de guías >

Series completas ▾

- Guías CCN-STIC de acceso público >
- 000 Políticas >
- 100 Procedimientos >
- 200 Normas >
- 300 Instrucciones técnicas >
- 400 Guías generales >
- 500 Guías de entornos Windows >
- 600 Guías de otros entornos >
- 800 Guía Esquema Nacional de Seguridad >**
- 900 Informes Técnicos >

Glosario de Términos (CCN-STIC 401) >

Serie 800 (ENS) >

Últimas guías CCN-STIC >

Buscar: Mostrar elementos

Documento	Publicado	Actualizado	PDF
CCN-STIC-800 Glosario de términos y abreviaturas del ENS	Mar 2011	Feb 2016	Descargar
CCN-STIC-801 Responsabilidades y Funciones en el ENS	Abr 2010	Feb 2011	Descargar
CCN-STIC-802 Auditoría del ENS	Jun 2010	Jun 2010	Descargar
CCN-STIC-803 Valoración de Sistemas en el ENS	May 2010	Ene 2011	Descargar
CCN-STIC-804 Medidas de implantación del ENS	Feb 2010	Mar 2013	Descargar
CCN-STIC-805 Política de Seguridad de la Información	Sep 2011	Sep 2011	Descargar
CCN-STIC-806 Plan de Adecuación al ENS	Ago 2010	Ene 2011	Descargar
CCN-STIC-807 Criptología de empleo en el ENS	Jul 2011	Abr 2015	Descargar
CCN-STIC-808 Verificación del cumplimiento de las medidas en el ENS	Oct 2010	Sep 2011	Descargar
CCN-STIC-809 Declaración de conformidad con el ENS	Jul 2010	Feb 2016	Descargar
CCN-STIC-810 Guía de Creación de CERT's	Sep 2011	Sep 2011	Descargar
CCN-STIC-811 Interconexión en el ENS	Sep 2011	Nov 2012	Descargar
CCN-STIC-812 Seguridad en servicios web	Ago 2011	Oct 2011	Descargar
CCN-STIC-813 Certificación de productos de seguridad	Feb 2012	Feb 2012	Descargar
CCN-STIC-814 Seguridad en servicio de correo	Ago 2011	Ago 2011	Descargar
CCN-STIC-815 Indicadores y métricas en el ENS	Abr 2012	Mar 2014	Descargar
CCN-STIC-817 Gestión de Ciberincidentes	Ago 2012	Nov 2015	Descargar

Bienvenido ▾ Su búsqueda 🔍 Abrir sesión 👤

DEFENSA FRENTE A LAS CIBERAMENAZAS

Inicio | Sobre nosotros | Gestión de incidentes | Formación | Guías | Informes | Herramientas | ENS | Empresas | Seguridad al día | Registro

ÚLTIMA HORA 22/03/2016 15:51 NIVEL DE ALERTA MUY ALTO

Google, Microsoft y Yahoo añan esfuerzos para un nuevo protocolo de cifrado

Inicio > Herramientas

HERRAMIENTAS

- CARMEN >
- CLARA >
- CCNDroid >
- INES >
- LUCIA >
- EAR/PILAR >
- REYES >**

Herramientas de Ciberseguridad

Dentro de las funciones del Centro Criptológico Nacional se encuentra la coordinación, promoción y desarrollo de herramientas que garanticen la seguridad de los sistemas y contribuyan a una mejor gestión de la ciberseguridad en cualquier organización y permitan una mejor defensa frente a los ciberataques.

Entre estas herramientas se encuentran las siguientes:

- CARMEN**
Herramienta de Detección de APTs
- CCNDroid**
Herramientas de Seguridad para Android
- CLARA**
Auditoría de Cumplimiento ENS/STIC en Sistemas Windows
- INES**
Informe de Estado de Seguridad en el ENS
- LUCIA**
Sistemas de Gestión Federada de Tickets
- PILAR**
Análisis y Gestión de Riesgos
- REYES**

Volver



FEDERACION ESPAÑOLA DE
MUNICIPIOS Y PROVINCIAS

_ens
Esquema Nacional de
Seguridad

TOMO 1

**GUÍA ESTRATÉGICA EN SEGURIDAD
PARA ENTIDADES LOCALES**

ESQUEMA NACIONAL DE SEGURIDAD [ENS]

Cuaderno de Recomendaciones

ÍNDICE

Introducción	8
1. Objetivo y alcance	10
1.1 Objetivos	11
1.1.1 Elementos del Esquema Nacional de Seguridad	12
1.1.2 Adecuación al Esquema Nacional de Seguridad	12
1.2 Alcance	14
2. Definición y Marco Legal	15
2.1 La seguridad de la información en el marco de la Administración electrónica	17
2.2 El marco legal de la Ley 11/2007 a las Leyes 39/2015 y 40/2015	17
2.3 Consecuencias del derecho a la "relación electrónica"	19
2.4 La Seguridad en las Leyes 39/2015 y 40/2015	20
2.5 ¿Qué es el Esquema Nacional de Seguridad? Un enfoque legal	23
2.6 Las Instrucciones Técnicas de Seguridad del ENS	25
2.7 Ámbito de aplicación del ENS	25
2.8 La conexión entre el ENS y el Reglamento General de Protección de Datos	32
2.9 Principales roles	35
2.9.1 Las responsabilidades en la seguridad de la información	35
2.9.2 Responsable de la Información	36
2.9.3 Responsable del Servicio	36
2.9.4 Responsable de Seguridad	37
2.9.5 Otros actores	38
2.9.6 La distribución en niveles de las responsabilidades	40
2.9.7 El Comité de Seguridad de la Información	42
2.9.8 Nominamientos	44
2.9.9 Asignación de tareas y determinación de responsabilidades	45
2.9.10 Competencias de las Diputaciones Provinciales	45
3. Diagrama General por fases	46
3.1 FASES1 Definición de las Fases Principales	47
3.1.1 FASE G11 Desarrollo de un Plan de Adecuación ENS	48
3.1.2 FASE G21 Implementación del Plan de Adecuación	64
3.1.3 FASE G31 Conformidad con el ENS	74
3.1.4 FASE G41 Puesta en marcha del sistema de mejora continua	76
4. Sistemas de medición	78
4.1 Métricas e Indicadores	79
4.2 Medición de la seguridad	81
4.2.1 Datos	83
4.2.2 Medidas	83
4.2.3 Métricas	84
4.2.4 Indicadores	84
4.2.5 Tipos de métricas e indicadores	86
4.2.6 Explotación	88



FEDERACION ESPAÑOLA DE
MUNICIPIOS Y PROVINCIAS

_ens
Esquema Nacional de
Seguridad

TOMO 2

**GUÍA PARA ENTIDADES LOCALES DE
MENOS DE 2.000 HABITANTES**

**ESQUEMA NACIONAL DE SEGURIDAD [ENS]
Cuaderno de Recomendaciones**

TOMO II GUÍA PARA ENTIDADES LOCALES DE MENOS DE 2.000 HABITANTES

ÍNDICE

Introducción	7
1. El Sistema de Información Local	9
2. Ayuntamiento tipo	12
2.1 Equipamiento.....	13
2.1.1 Equipamiento Físico	13
2.1.2 Software instalado localmente.....	13
2.1.3 Software en la nube o en modo servicio (SaaS).....	14
2.2 Recursos Humanos.....	14
2.3 Servicios prestados.....	15
3. Ámbito de aplicación	16
4. Figura del Responsable de Seguridad	18
5. Medidas de seguridad.....	20
5.1 Identificación de Personas con Acceso a los Sistemas de Información y Firma de acuerdos de Confidencialidad	21
5.2 Inventario de Activos y Servicios.....	21
5.3 Aplicación de medidas de seguridad	21
A.1 Seguridad Física en las Instalaciones	22
A.2 Seguridad de Red LAN	23
A.3 Seguridad de la conexión al Internet	24
A.4 Seguridad en los equipos.....	26
A.5 Gestión de soportes y documentos.....	28
A.6 Cifrado de datos	30
A.7 Uso del Correo Electrónico	30
A.8 Firma electrónica y certificados	31
5.4 Formación y Concienciación	31
6. Notificación de incidentes de Seguridad	32
7. Evaluación y mejora continua	32

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



Screenshot of the PAE portal administration electrónica website. The page shows a navigation menu with 'Estrategias' selected, and a main content area titled 'Seguridad'. The content includes a section for 'Esquema Nacional de Seguridad - ENS' and 'Métodos, Instrumentos y normas'. The ENS section describes its purpose: 'Su finalidad es crear las condiciones necesarias para la confianza en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones, y los servicios electrónicos.' The 'Métodos, Instrumentos y normas' section mentions 'Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, Guías CCN-STIC para la seguridad de los sistemas de la Administración Pública. CCN-CERT.'

Screenshot of the DEFENSA FRENTE A LAS CIBERAMENAZAS website. The page features a header with the CCN-CERT logo and navigation links. A prominent section titled 'ÚLTIMA HORA' indicates 'Publicadas las ponencias de la V Jornada SAT del CCN-CERT' on 14/05/2015 at 19:08. A sidebar on the right shows a 'NIVEL DE ALERTA' indicator set to 'MUY ALTO' and a menu with options like 'Guías (Serie 800)', 'CLARA', 'INES', 'Programas de Apoyo', 'Adecuación', 'Documentación', 'FAQ', 'Más información', and 'Contacto'. The main content area lists 'ENS' with sub-links for 'Guías (Serie 800)', 'CLARA', 'INES', 'Programas de Apoyo', 'Adecuación', 'Documentación', 'FAQ', 'Más información', and 'Contacto'. The ENS logo is displayed as 'Esquema Nacional de Seguridad'. At the bottom, a paragraph explains the Real Decreto 3/2010, de 8 de enero (BOE de 29 de enero), which regulates the ENS in the context of electronic administration.