Cumplimiento normativo: Protección de Datos, ENS e Instrucciones Técnicas de Seguridad

DR. CARLOS GALÁN

Profesor UC3M
Presidente ATL

Carlos Galán es Doctor en Informática, Abogado especialista en Derecho de las Tecnologías de la Información, *Certified Information Security Manager* (CISM) por ISACA y Consultor/Formador Homologado de la EOI.

Autor de una decena de libros relacionados con las Tecnologías de la Información, su Derecho y sus aplicaciones, ha escrito asimismo una multiplicidad de artículos y comentarios en prensa y publicaciones especializadas.
Ha desarrollado parte de su carrera profesional en el Grupo Telefónica, ocupando diversos cargos y desarrollando importantes proyectos nacionales e internacionales.

Ha sido Vocal Asesor y Director de la Oficina de Modernización del Ministerio del Interior, donde, entre otras actividades, diseñó en Plan de Modernización de los Cuerpos y Fuerzas de Seguridad del Estado y presidido la Comisión de Informática y Comunicaciones de la Seguridad de los Juegos Olímpicos de Barcelona ’92.

Ha sido profesor de la Facultad de Informática de la Universidad Politécnica de Madrid, de la Escuela Técnica Superior de Ingenieros Industriales de la UNED, de la licenciatura de Administración y Dirección de Empresas de la Universidad Complutense de Madrid y del Instituto de Postgrado de la Universidad Pontificia de Comillas. Ha sido Director General de la Agencia de Certificación Electrónica ACE (primera Autoridad de Certificación de España), Vicepresidente de la Asociación de Entidades de Confianza Digital AECODI, Director General de Desarrollo y Tecnología de la Fundación General de la Universidad de Málaga y Presidente del Comité de Nuevas Tecnologías de Hispajuris, la mayor red de despachos de abogados de España.

En el terreno académico, en su calidad de especialista en Administración Electrónica, Seguridad y Firma Electrónica, ha sido profesor de *Calidad, Seguridad y Protección de la Información*, de la Ingeniería de Informática de la Universidad Pontificia de Salamanca. Actualmente es miembro del Área de Derecho Administrativo de la Universidad Carlos III de Madrid, institución en la que imparte *Derecho de las TIC* en el Grado de Derecho de la Facultad de Ciencias Sociales y Jurídicas, y *Aspectos Legales de la Ingeniería Informática,* en el Máster de *Derecho de las Telecomunicaciones y Tecnologías de la Información,* actividades que compagina con la escritura de monografías y artículos y el dictado de conferencias y cursos donde es ponente habitual en las materias relativas al Derecho de las Tecnologías de la Información y las Comunicaciones, la Administración Electrónica, Firma Electrónica, Certificación Digital y Seguridad IT.

Carlos Galán ha sido asesor parlamentario en la redacción de la Ley 59/2003, de firma electrónica y, en la actualidad, es colaborador del Ministerio de Hacienda y Administraciones Públicas -dónde es miembro del Grupo de Expertos del Plan de Acción de Administración Electrónica 213-2015- y del Centro Criptológico Nacional –del Centro Nacional de Inteligencia-, donde es colaborador permanente en materias relativas a Seguridad IT, Esquema Nacional de Seguridad, habiendo formado parte del equipo redactor de la Estrategia de Ciberseguridad Nacional.

Además de la presidencia de la Agencia de Tecnología Legal, es vicepresidente de la Comisión de Contratación Electrónica de la Asociación Nacional de Empresas de Internet, miembro del Observatorio Notarial para la Sociedad de la Información y miembro del Observatorio de la Mesa de la Justicia del Ilustre Colegio de Abogados de Madrid.

Contenido

- La conformidad legal
- Protección de Datos
- Esquema Nacional de Seguridad
- El camino hacia la conformidad legal

La necesaria conformidad legal

- ✓ **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.**
- ✓ **¿Responsabilidad patrimonial?**

Conformidad legal y SEGURIDAD

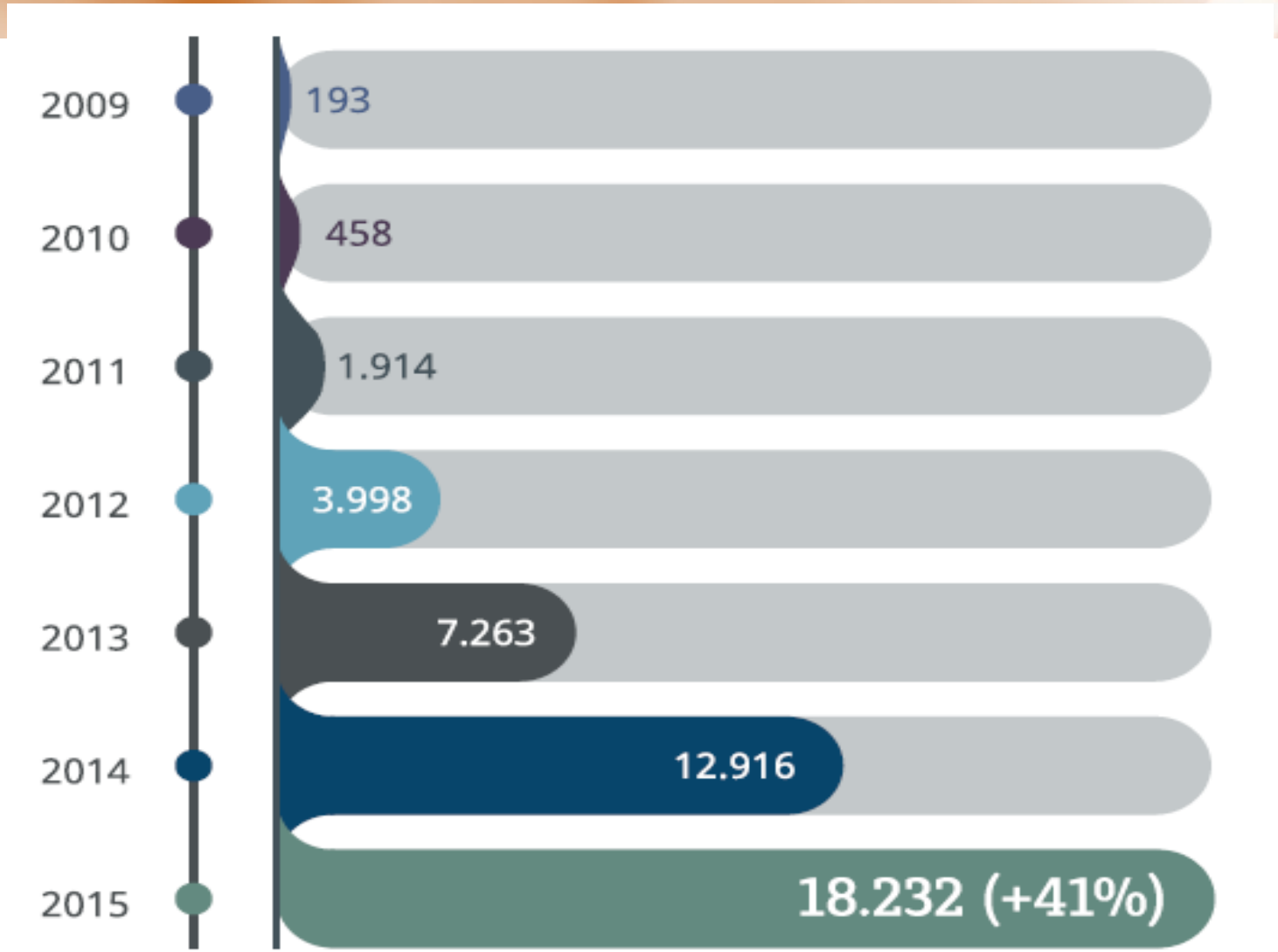
SEGURIDAD DE LA INFORMACIÓN

RD 3/2010, Esquema Nacional de Seguridad
Instrucciones Técnicas de Seguridad

PROTECCIÓN DE DATOS

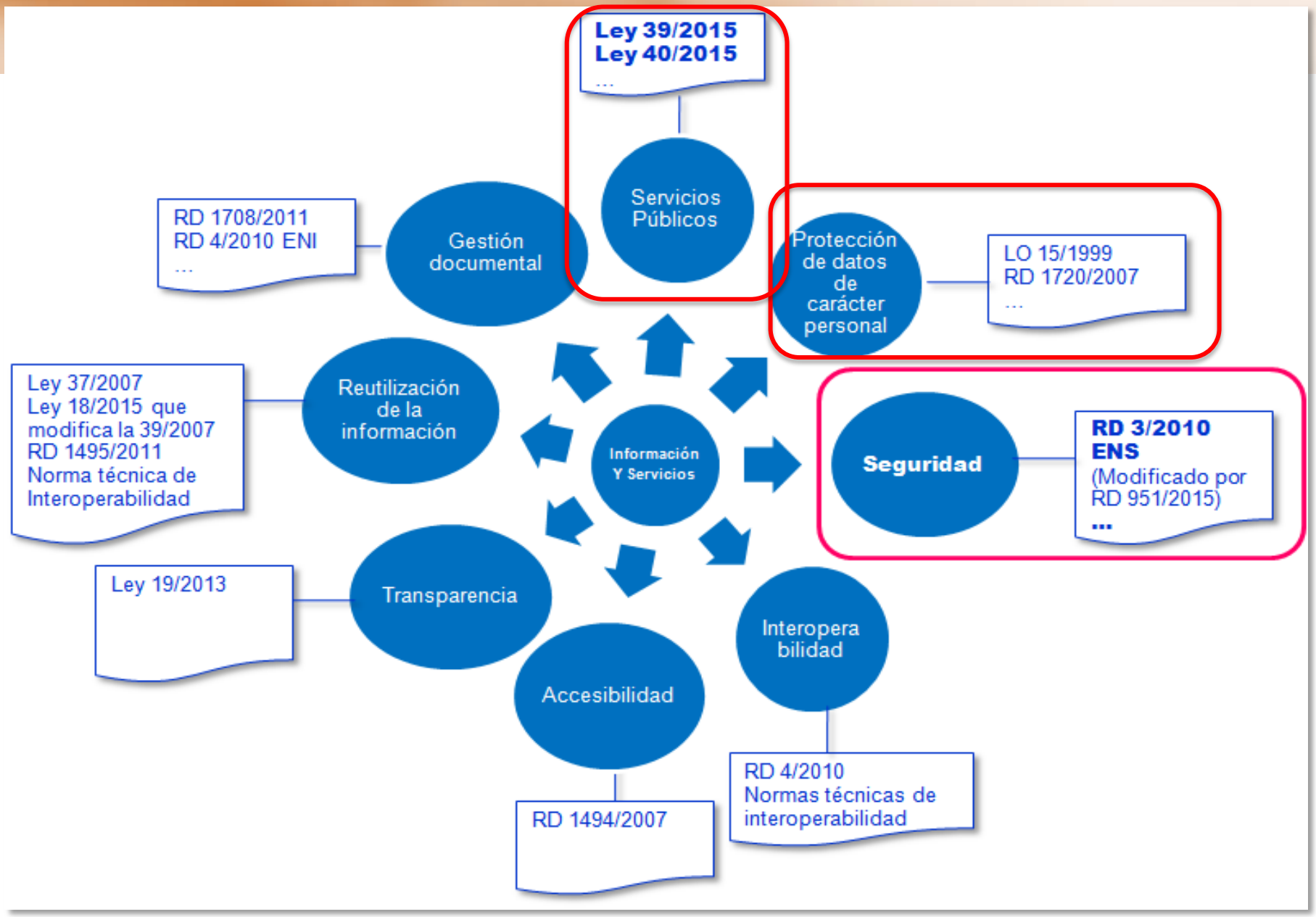
Ley Orgánica 15/1999, LOPD
RD 1720/2007, RDLOPD
Reglamento (UE) 2016/679 General de Protección de Datos

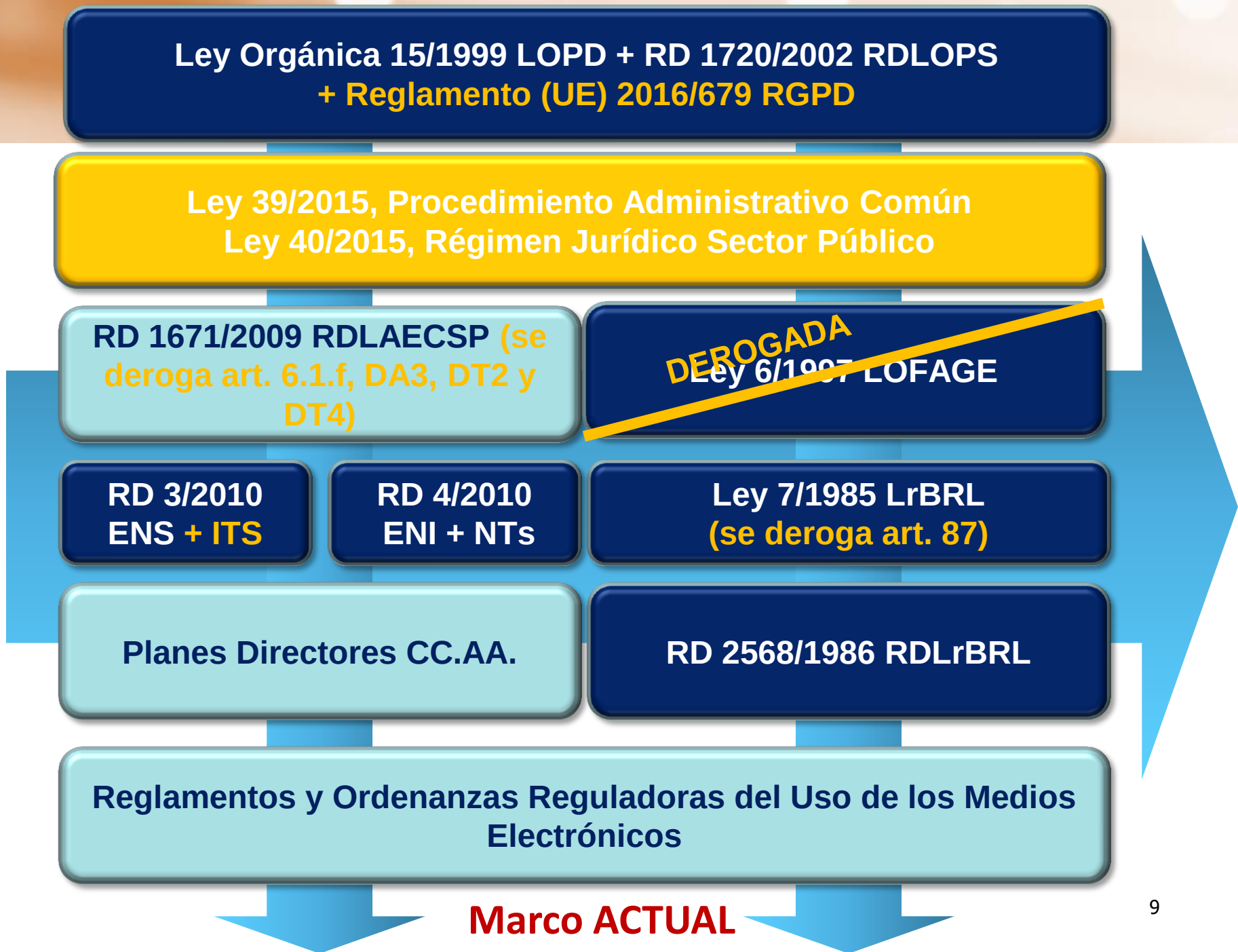
Incremento notable de incidentes



Evolución de los Incidentes gestionados por el CCN-CERT

El medio electrónico como medio habitual





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.

Los **actos administrativos se producirán por escrito** a **través de medios electrónicos**, a menos que su naturaleza exija otra forma más adecuada de expresión y constancia. (art. 36)

Las AA.PP. emitirán los **documentos administrativos por escrito, a través de medios electrónicos**, a menos que su naturaleza exija otra forma más adecuada…(art. 26)

Los **expedientes tendrán formato electrónico**… (art. 70)

Cada Administración deberá mantener un archivo electrónico único de los documentos electrónicos que correspondan a procedimientos finalizados…(art. 17)

[Ley 39/2015]

Ley 40/2015

3. Principios generales y 156. Esquema …

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.*

1. El Esquema Nacional de Interoperabilidad comprende el conjunto de criterios y recomendaciones en materia de seguridad, conservación y normalización de la información, de los formatos y de las aplicaciones que deberán ser tenidos en cuenta por las Administraciones Públicas para la toma de decisiones tecnológicas que garanticen la interoperabilidad.

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.

- + Referencias específicas:
  - **Ley 39/2015**: archivo electrónico, validez y eficacia de las copias de documentos y adhesión de CCAA y EELL a las plataformas y registros e la AGE.

¿Qué tenemos que hacer en los Ayuntamientos?

Asegurar la:

- **Conformidad en materia de PROTECCIÓN DE DATOS**
- **Conformidad en materia de SEGURIDAD DE LA INFORMACIÓN : ESQUEMA NACIONAL DE SEGURIDAD (ENS)**

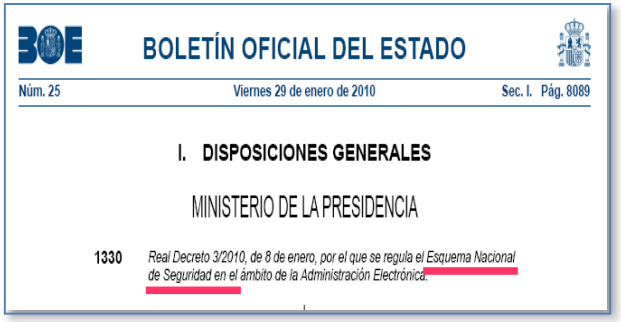
Protección de Datos

Conformidad en materia de PROTECCIÓN DE DATOS:

- Identificar Ficheros/Tratamientos.
- Determinar la tipología del tratamiento (Básica/Media/Alta)
- Notificar AEPD Ficheros/Tratamientos.
- Adoptar las medidas de Seguridad (Básico/Medio/Alto).
- Ir trabajando en las adaptaciones necesarias para dar cumplimiento al Reglamento (UE) 2016/679 RGPD.

El Esquema Nacional de Seguridad (ENS)

- ✓ **Es un instrumento legal – Real Decreto 3/2010-** que desarrolla lo previsto sobre seguridad en la Ley 11/2007.
- ✓ **Establece la política de seguridad** en los servicios de administración-e.
  - Está **constituida por principios básicos** y **requisitos mínimos** que permitan una **protección adecuada** de la información.
- ✓ **Es de aplicación a todas las AA.PP.**
  - Están excluidos los sistemas que manejan la información clasificada.
- ✓ Resulta de un **esfuerzo colectivo**: AGE, CC.AA., CC.LL.-FEMP, CRUE + Opinión Industria TIC.
- ✓ **Actualizado,** (Real Decreto 951/2015).



BOLETÍN OFICIAL DEL ESTADO

Núm. 25 Viernes 29 de enero de 2010 Sec. I. Pág. 8089

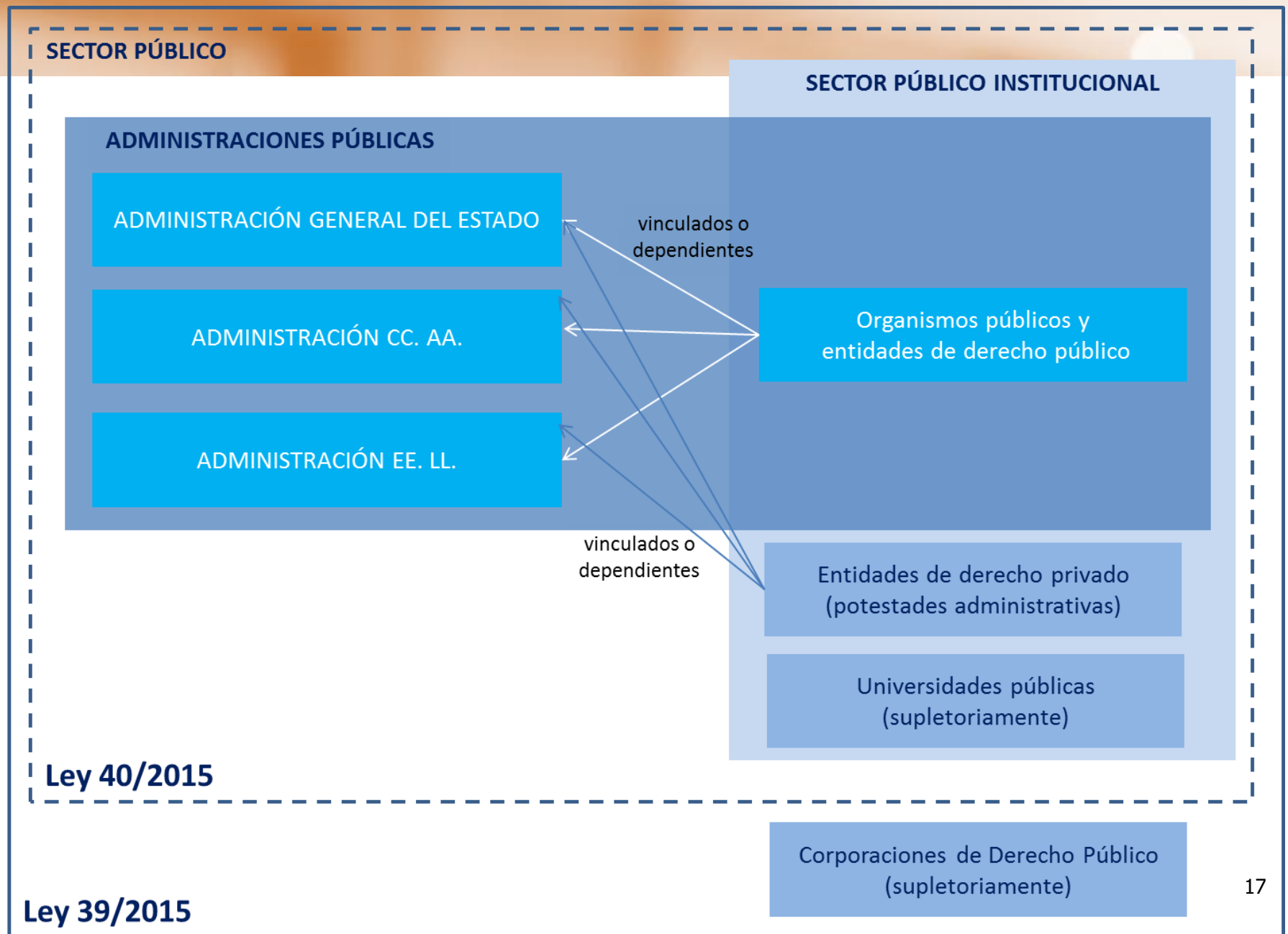
I. DISPOSICIONES GENERALES

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.*

ens Esquema Nacional de Seguridad

Ámbito subjetivo de aplicación



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.

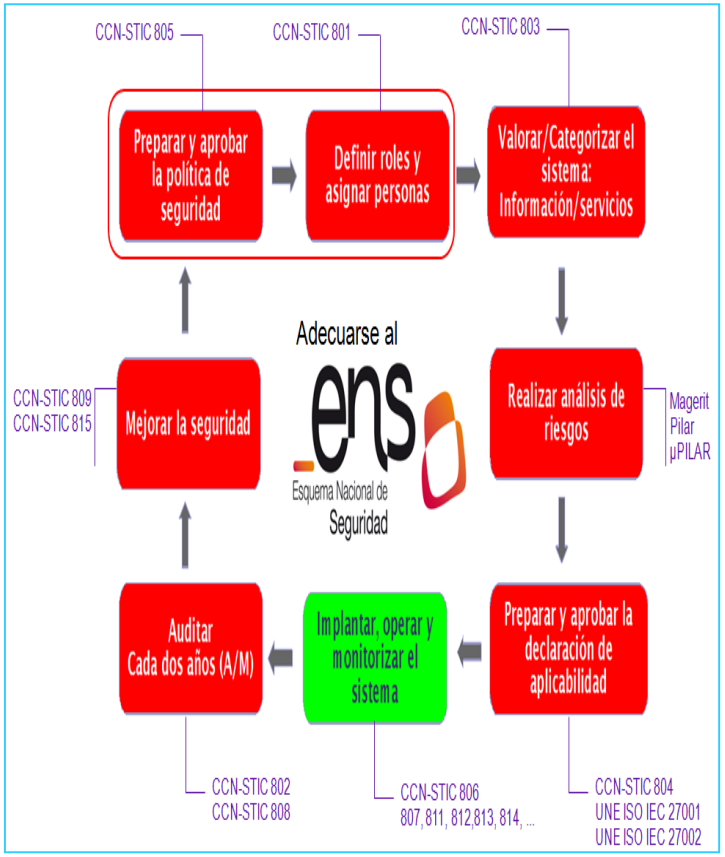
- ✓ **Proporcionar lenguaje y elementos comunes**:
  - **Para guiar la actuación de las AA.PP. en materia de seguridad** de las tecnologías de la información.
  - **Para facilitar la interacción** y la cooperación de las AA.PP.
  - Para **facilitar la comunicación de los requisitos de seguridad de la información a la Industria.**

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

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)



Actualizando el ENS

- ✓ **RD 3/2010 revisado a la luz de**:
  - la experiencia adquirida,
  - los comentarios recibidos por vías formales e informales,
  - la evolución de la tecnología y las ciberamenazas,
  - el contexto regulatorio europeo.
- ✓ **Alineado con el Reglamento (UE) Nº 910/2014 de identidad electrónica y servicios de confianza**.
- ✓ **Consensuado** en las AA.PP. (3 años de trabajo).
- ✓ **Visto por la Industria**.
- ✓ Real decreto de modificación **aprobado en Consejo de Ministros de 23 de octubre** de 2015.

Instrucciones Técnicas de Seguridad

- ✓ Artículo afectado: 29
- ✓ Para **armonizar el modo común de actuar** en relación con ciertas cuestiones.
- ✓ Para su elaboración se aplicarán los procedimientos consolidados en el ámbito de la Interoperabilidad.
- ✓ Se contemplan las siguientes:
  - **Informe del estado de la seguridad.**
  - **Notificación de incidentes de seguridad.**
  - **Auditoría de la seguridad.**
  - **Conformidad con el Esquema Nacional de Seguridad.**
  - **Adquisición de productos de seguridad.**
  - **Criptología de empleo en el Esquema Nacional de Seguridad.**
  - **Interconexión en el Esquema Nacional de Seguridad.**
  - **Requisitos de seguridad en entornos externalizados.**

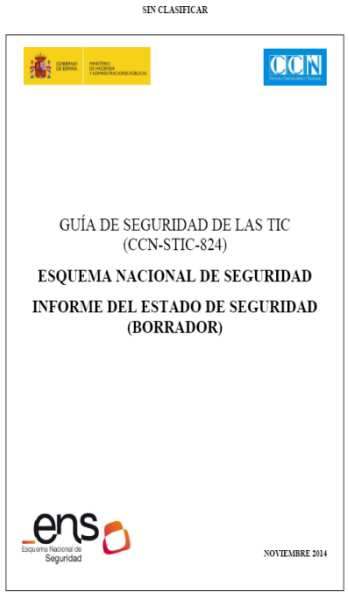
Evaluar el estado de la seguridad

El ENS exige **evaluar regularmente el estado de seguridad**:

«El Comité Sectorial de Administración Electrónica recogerá la información relacionada con 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.
El Centro Criptológico Nacional articulará los procedimientos necesarios para la recogida y consolidación de la información, así como los aspectos metodológicos para su tratamiento y explotación, a través de los correspondientes grupos de trabajo que se constituyan al efecto en el Comité Sectorial de Administración Electrónica y en la Comisión de Estrategia TIC para la Administración General del Estado. »

(*) Actualizado

También, la **medición de la seguridad**: **4.6.2 Sistema de métricas [op.mon.2]**



La herramienta 'INES' facilita la recogida y consolidación de información para el *Informe del Estado de la Seguridad* (RD 3/2010, art. 35 y línea de acción 2 de Estrategia de Ciberseguridad Nacional).

</inés>
Informe del Estado de la Seguridad en el ENS.

Informe 2016. Participación

- Administración General del Estado (AGE)
- Comunidades Autónomas (CC.AA.)
- Universidades (UNIV)
- Ayuntamientos de más de 30.000 habitantes y diputaciones

2015

	total	datos > 33%		baja	media	alta
AGE	94	90	96%	12	49	29
CCAA	34	30	88%	2	11	17
UNIV	45	43	96%	5	35	3
EELL	182	149	82%	9	105	35

Total: 355 organismos

Informe 2016. Resultados

	AGE	CCAA	UNI	EELL
[org] Marco organizativo	59	68	49	40
[op] Marco operacional	50	60	50	50
[op.pl] Planificación	50	50	38.5	30
[op.acc] Control de acceso	71	70	54.5	70
[op.exp] Explotación	60	60	50	50
[op.ext] Servicios externos	50	60	48	20
[op.cont] Continuidad del servicio	10	37	10	0
[op.mon] Monitorización del sistema	40	60	20	10
[mp] Medidas de protección	64.5	66	50	50
[mp.if] Protección de las instalaciones e infraestructuras	85	90	77.5	50
[mp.per] Gestión del personal	50	50	30	21
[mp.eq] Protección de los equipos	60	50	33	50
[mp.com] Protección de las comunicaciones	75	80	75	60
[mp.si] Protección de los soportes de información	50	50	50	35
[mp.sw] Protección de las aplicaciones informáticas	52	70	50	46
[mp.info] Protección de la información	60	55	50	50
[mp.s] Protección de los servicios	70	75	50	60

Informe 2016. Resultados

AGE	CCAA	UNIV	EELL	
80	80	67	71	[op.exp.1] Inventario de activos
88	90	88	70	[mp.if.1] Áreas separadas y con control de acceso
54	59	50	40	[op.pl.2] Arquitectura de seguridad
70	75	50	50	[op.acc.7] Acceso remoto (remote login)
80	85	80	90	[mp.com.1] Perímetro seguro
60	60	50	51	[op.exp.2] Configuración de seguridad
80	80	72.5	80	[op.exp.6] Protección frente a código dañino
90	90	90	90	[mp.info.9] Copias de seguridad (backup)
64	52	50	50	[op.exp.4] Mantenimiento
50	61	50	40	[op.exp.5] Gestión de cambios
53.5	70	50	50	[op.exp.7] Gestión de incidentes
50	50	49	38	[op.exp.8] Registro de la actividad de los usuarios
50	65	40	38.5	[org.2] Normativa de seguridad
50	48.5	25	24	[mp.per.3] Concienciación
67	75	50	70	[mp.s.2] Protección de servicios y aplicaciones web
60	50	30	50	[mp.eq.3] Protección de equipos portátiles
44	46.5	28	12	[mp.per.4] Formación
24	20	30	10	[mp.si.2] Criptografía
80	80	80	80	[mp.s.1] Protección del correo electrónico (e-mail)

Puntos de mejora urgente:

- registro de la actividad de los usuarios .... VIGILANCIA DÉBIL
- concienciación y formación, especialmente en UNIV y EELL
- gestión de cambios y mantenimiento
- Protección equipos portátiles /Criptografía.

Informe 2016. Principales conclusiones

La **valoración principal que cabe realizarse es la siguiente:**

Con carácter general, **el nivel de cumplimiento global del Esquema Nacional de Seguridad es BAJO, situándose en el 50% por lo que es necesario un esfuerzo en los próximos años para cumplir los requisitos especificados en el mismo.**

A la luz de esta situación, se considera que se deben **impulsar las acciones que aceleren la implantación del ENS en los diferentes organismos.**

26

Informe 2016. Principales conclusiones

Es muy pobre la **gestión de cambios, mantenimiento, configuración y gestión de la configuración**.

Es mejorable el proceso de **gestión de incidentes**.

Es muy baja la implantación de **medidas de continuidad del servicio**.

Es mejorable la **concienciación y formación** del personal.

Es muy bajo el **empleo de criptografía** para proteger los soportes de información.

27

Informe 2016. Principales conclusiones

AGE - Administración General del Estado.

Es baja la formación del personal.

Es mejorable el proceso de gestión de incidentes.

CC.AA. - Comunidades Autónomas.

Es baja la formación del personal.

Es mejorable del proceso de autorización.

EE.LL. - Entidades Locales

Es muy baja la monitorización de la actividad del sistema.

Es muy baja la formación y la concienciación del personal.

UNIV - Universidades

Es muy baja la monitorización de la actividad del sistema.

Es muy baja la formación y la concienciación del personal.

Es muy baja la protección de equipos portátiles.

Son débiles los procesos de autorización.

28

Informe 2016. Principales recomendaciones

Promover la conformidad con el ENS. En particular, fomentar la certificación de la conformidad a través de la realización de auditorías independientes, de acuerdo con lo previsto en el artículo 41 y en la guía CCN-STIC-809.

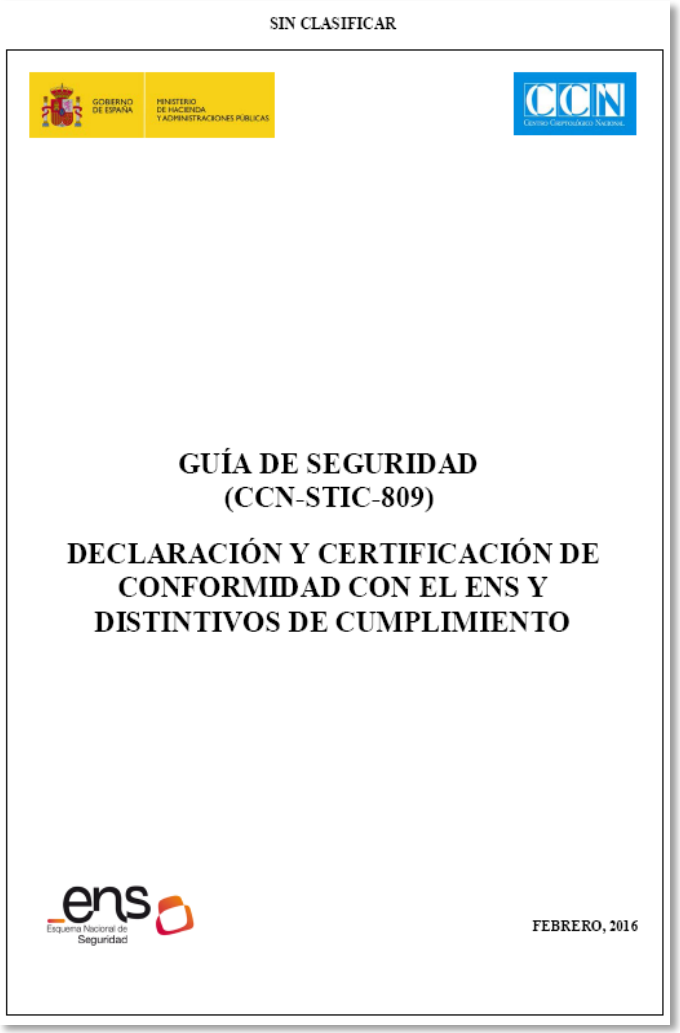
Promover que los datos que se aporten al Informe se sustenten mediante una auditoría para sistemas de categorías MEDIA y ALTA y una autoevaluación para sistemas de categoría BÁSICA.

Ampliar el alcance del Informe a un mayor número de entidades de la Administración Local.

Reforzar las capacidades de detección y mejorar la defensa de los sistemas clasificados según se recoge en la Estrategia de Ciberseguridad Nacional con la aprobación de los recursos extraordinarios que se reflejan en los planes derivados aprobados en julio de 2015.

29

La conformidad con el ENS, ¿cuál es el procedimiento?



SIN CLASIFICAR

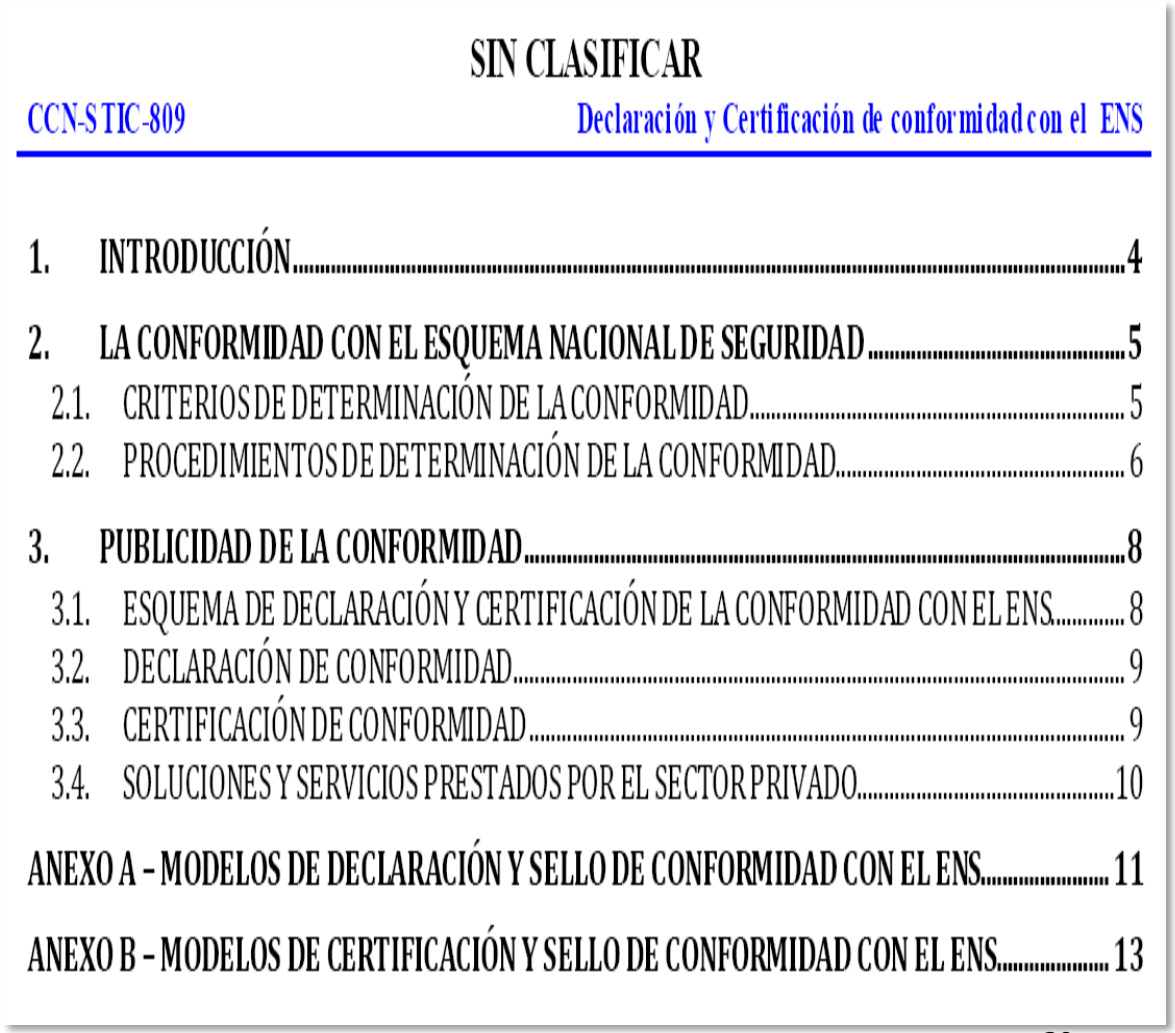
GOBIERNO DE ESPAÑA · MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS · CCN Centro Criptológico Nacional

GUÍA DE SEGURIDAD
(CCN-STIC-809)

DECLARACIÓN Y CERTIFICACIÓN DE CONFORMIDAD CON EL ENS Y DISTINTIVOS DE CUMPLIMIENTO

ens Esquema Nacional de Seguridad

FEBRERO, 2016



SIN CLASIFICAR

CCN-STIC-809 Declaración y Certificación de conformidad con el ENS

1. INTRODUCCIÓN 4

2. LA CONFORMIDAD CON EL ESQUEMA NACIONAL DE SEGURIDAD 5
   2.1. CRITERIOS DE DETERMINACIÓN DE LA CONFORMIDAD 5
   2.2. PROCEDIMIENTOS DE DETERMINACIÓN DE LA CONFORMIDAD 6

3. PUBLICIDAD DE LA CONFORMIDAD 8
   3.1. ESQUEMA DE DECLARACIÓN Y CERTIFICACIÓN DE LA CONFORMIDAD CON EL ENS 8
   3.2. DECLARACIÓN DE CONFORMIDAD 9
   3.3. CERTIFICACIÓN DE CONFORMIDAD 9
   3.4. SOLUCIONES Y SERVICIOS PRESTADOS POR EL SECTOR PRIVADO 10

ANEXO A - MODELOS DE DECLARACIÓN Y SELLO DE CONFORMIDAD CON EL ENS 11

ANEXO B - MODELOS DE CERTIFICACIÓN Y SELLO DE CONFORMIDAD CON EL ENS 13

¿Cuáles son los requisitos para **entidades públicas**?

Sistemas de información de categoría BÁSICA

- Realizar **Autoevaluación**
- Elaborar el documento de autoevaluación
- Exhibir una **Declaración de Conformidad**

¿Cuáles son los requisitos para **entidades públicas?**

Sistemas de información de categoría BÁSICA

Declaración de Conformidad, podrá representarse:

- ✓ Mediante **Sello o Distintivo de Declaración de Conformidad**
- ✓ Generado por la **entidad bajo cuya responsabilidad esté el sistema**
- ✓ Con **uso condicionado a la Declaración de Conformidad** con el ENS.

DECLARACIÓN DE CONFORMIDAD

CON EL RD 3/2010, DE 8 DE ENERO, POR EL QUE SE REGULA EL ESQUEMA NACIONAL DE SEGURIDAD EN EL ÁMBITO DE LA ADMINISTRACIÓN ELECTRÓNICA

(ENS)

DECLARACIÓN DE CONFORMIDAD CON EL ens Esquema Nacional de Seguridad Categoría BÁSICA aaaa / mm / dd

Logotipo de la Entidad Pública declarante	*Identificación inequívoca del declarante, incluyendo la denominación legal que aprueba la estructura orgánica a la que está adscrito.*

Los sistemas de información reseñados seguidamente, todos ellos de categoría BÁSICA, y conforme a lo dispuesto en el Anexo III del RD 3/2010, han superado un proceso de autoevaluación realizado en las fechas que se indican:

1.	*aaaa/mm/dd*	*Denominación Sistema de Información 1 y servicios prestados*
2.	*aaaa/mm/dd*	*Denominación Sistema de Información 2 y servicios prestados*
…	…	…

Dicho proceso de autoevaluación garantiza que los sistemas referenciados cumplen las medidas de seguridad impuestas por el RD 3/2010, para sistemas de categoría BÁSICA.

En *Localidad*, **a** ___ **de** _____ **de 20**__

Fdo. *Nombre y Apellidos del titular del*

Órgano Superior de que se trate

Administración Pública de que se trate

Evidencias de

Firma electrónica [personal / para actuación administrativa automatizada]

del declarante

Nota: Los textos señalados en *letra cursiva* deben ser adaptados a cada caso.

¿Cuáles son los requisitos para **entidades públicas**?

Sistemas de información de categorías MEDIA o ALTA

- Realizar **Auditoría formal**
- Elaborar Informe de auditoría
- Exhibir una **Certificación de Conformidad**
  (Voluntaria para categoría Básica)

¿Cuáles son los requisitos para **entidades públicas**?

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

Certificación de Conformidad, podrá representarse:

- ✓ Mediante un **Sello o Distintivo de Certificación de Conformidad**
- ✓ **Expedido por una entidad** certificadora
- ✓ **Con uso condicionado a la posesión del Certificado de Conformidad** con el ENS.


Logotipo de la Entidad Certificadora

CERTIFICACIÓN DE CONFORMIDAD CON EL ens Esquema Nacional de Seguridad
Categoría [BÁSICA/MEDIA/ALTA]
aaaa / mm / dd
Número del certificado: _____

Certificación

Concedida a

Entidad(1)

Población

Dirección postal

Entidad Certificadora **certifica que el Sistema de Información** ***Denominación del Sistema de Información*****, de categoría _____ (2), ha sido auditado y encontrado 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.**

Los servicios prestados por el antedicho Sistema de Información son: _____

Declaración de aplicabilidad: versión ___, fecha: ___ de _____ de 201_

Fecha de certificación inicial: ___ de _____ de 201_
Fecha de expiración: ____ de _____ de 201_ (3).

Para cualquier aclaración sobre el alcance del presente certificado y la aplicación de los requisitos del ENS, pueden ponerse en contacto con la *Entidad Certificadora*.

Número del Certificado: _____
Fecha: ___ de _____ de 201_
Firma *del responsable de la Entidad Certificadora:*

Nombre completo /razón social de la Entidad Certificadora y pág. web.
Dirección postal / electrónica.
Oficina de emisión (en su caso).
Código Postal. Provincia. País.

(1) Pudiendo ser de naturaleza jurídica pública o privada.
(2) BÁSICA/MEDIA/ALTA
(3) Máximo de 2 años.

¿Cuáles son los requisitos para operadores del **sector privado**?

Prestadores de servicios o soluciones a las entidades públicas, a los que 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

¿Cuáles son los requisitos para entidades de **auditoría y certificación**?

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

✓ **Las Entidades de Certificación que no posean la acreditación**, **podrán iniciar sus actividades de certificación de forma transitoria, disponiendo de 12 meses** para obtener la acreditación.

✓ **El CCN mantendrá en su sede electrónica una relación actualizada de las Entidades de Certificación, acreditadas o en vías de acreditación**, para expedir Certificaciones de Conformidad con el ENS.

✓ **Exentas aquellas entidades de las AA.PP. cuyas competencias se correspondan con el desarrollo de auditorías** de sistemas de información y así conste en su normativa de creación.

El camino hacia la conformidad legal

Revisión, presentación y publicación de la Ordenanza de Administración Electrónica

Formación general en AE a empleados públicos

Formación general en AE a cargos políticos

Desarrollo de la Ordenanza

- Modelo de Gestión de Documentos Electrónicos
  - Política de Gestión de Documentos Electrónicos
- Archivo Electrónico Único
- Repertorio Genérico de Procedimien-tos
  - Detalle de Procedimien tos escogidos
- Actuación Administrati-va Automatiza-da
- Política de Identifica-ción y Firma Electrónica
- Puestos de asistencia al ciudadano
- Registro Electrónico de Apoderamie ntos
- Adecuación al ENS
  - Política de Seguridad de la Información
- Adecuación a la LOPD
- Sede Electrónica
- Registro Electrónico General
- Sistema de Notificacio-nes (Plataforma)
- Tablón Electrónico de Anuncios o Edictos

Formación específica en la materia concreta

TIEMPO

Desarrollos Departamentales

- Órganos Colegiados
- Contratac. Electrónica
- Gestión Tributaria
- Contabilidad
- Gestión Policial
- RR.HH.
- Patrimonio e Inventario
- Etc.

Muchas GRACIAS

cgalan@atl.es

Informe 2016. Nivel de madurez

Nivel de Madurez		Descripción del nivel
Nivel	**%**	
L0	0	***Inexistente***. La medida no se está aplicando.
L1	10	***Inicial / ad hoc***. Se hace algo, de vez en cuando.
L2	50	***Reproducible, pero intuitivo***. Se realiza, pero no está sistematizado ni documentado.
L3	90	***Proceso definido***. Se realiza sistemáticamente y los procedimientos están escritos.
L4	95	***Gestionado y medible.*** Se hace un seguimiento de su desempeño.
L5	100	***Optimizado***. Se aplica un proceso de mejora continua.

categoría del sistema	nivel mínimo de madurez requerido
BÁSICA	L2 – reproducible, pero intuitivo (50%)
MEDIA	L3 – proceso definido (90%)
ALTA	L4 – gestionado y medible (95%)

Informe 2016. Resultados

2015

AGE	CCAA	UNIV	EELL	
5	5	5	3	Se dispone de una política de seguridad aprobada
5	5	5	3	El responsable de la seguridad es independiente del responsable del sistema
3	3	2	2	El análisis de riesgos está actualizado al último año
4	3.5	2	3	Se dispone de una declaración de aplicabilidad
3	3.5	3	3	Se dispone de un plan de adecuación aprobado
1	1	1	1	Se dispone de una certificación de cumplimiento actualizada al último año