Funcionamiento del Sector Público: Ley 40/2015 y ENS

Dr. Carlos Galán (cgalan@atl.es)
Agencia de Tecnología Legal – Universidad Carlos III de Madrid

Diciembre, 2015

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 participando en 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, 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.

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-, en Administración Electrónica y Ciberseguridad, colaborando asimismo con varias organizaciones públicas y privadas. Es Presidente de la Agencia de Tecnología Legal, 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

1. **Ley 40/2015: Distribución de conceptos jurídico-electrónicos más significativos.**
2. **ENS:**
   - **¿Por qué es necesaria la seguridad de la información y los servicios?**
   - **Implantar la ciberseguridad en las AA.PP.: el Esquema Nacional de Seguridad (ENS).**
   - **Estado de situación: ¿Dónde estamos?**
   - **Retos y conclusiones.**

1. Ley 40/2015: Distribución de conceptos jurídico-electrónicos más significativos.

Artículo 2. Ámbito Subjetivo

1. La presente Ley se aplica al sector público que comprende:
a) La **Administración General del Estado**.
b) Las **Administraciones de las Comunidades Autónomas**.
c) Las **Entidades que integran la Administración Local**.
d) El sector público institucional.

2. El **sector público institucional** se integra por:
a) Cualesquiera organismos públicos y entidades de derecho público vinculados o dependientes de las Administraciones Públicas.
b) Las entidades de derecho privado vinculadas o dependientes de las Administraciones Públicas que quedarán sujetas a lo dispuesto en las normas de esta Ley que específicamente se refieran a las mismas, en particular a los principios previstos en el artículo 3, y en todo caso, cuando ejerzan potestades administrativas.
c) Las Universidades públicas que se regirán por su normativa específica y supletoriamente por las previsiones de la presente Ley.

3. Tienen la consideración de **Administraciones Públicas** la Administración General del Estado, las Administraciones de las Comunidades Autónomas, las Entidades que integran la Administración Local, así como los organismos públicos y entidades de derecho público previstos en la letra a) del apartado 2.

Funcionamiento del Sector Púbico: Ley 40/2015 y ENS

Concepto	Ley 39/2015 - LPAC	Ley 40/2015 - LRJSP
Representación	(5) Comparecencia electrónica / registro electrónico de apoderamientos / Representación de los interesados (6) Registro electrónico de apoderamientos (General / Particulares)	
Identificación (para verificar la identidad de los interesados en el procedimiento administrativo)	(De los INTERESADOS en el procedimiento) (9) Usando un registro previo: (certificados cualificados de firma electrónica y sello electrónico + claves concertadas + otros sistemas validados por las AA.PP.	(De las AA.PP.) * (40.1) Usando sello electrónico (basado en certificado cualificado: NIF+denominación+identidad -titular) + relación de sellos usados / facilitando verificación
Actuación administrativa automatizada		* (41.1) acto realizado íntegramente por una AP usando medios electrónicos (en un procedimiento administrativo / sin intervención de empleado público). (41.2) órganos competentes para: • Especificar, programar, mantener… • Considerado responsable a efectos de impugnación.

Funcionamiento del Sector Púbico: Ley 40/2015 y ENS

Concepto	Ley 39/2015 - LPAC	Ley 40/2015 - LRJSP
Firma [electrónica] (para acreditar la autenticidad de la expresión de su voluntad y consentimiento)	**(Admitidos por las AA.PP.)** (10.1.a) Firma electrónica cualificada (y avanzada, basada en certificados cualificados) de persona física + persona jurídica + entes sin personalidad. (10.1.b) Sello electrónico cualificado (y avanzado, basado en certificados cualificados) (10.1.c) Otros sistemas validados por las AA.PP.	**(Para la actuación administrativa automatizada)** * (42.a) Sello electrónico de AP, órgano, organismo público o entidad de DP (basado en cert. cualif.) (42.b) CSV vinculado a AP, órgano, organismo público o entidad de DP (en las condiciones establecidas + mecanismo de comprobación). **(Del personal de las AA.PP.)** * (43.1) Del titular del órgano o del empleado público. (43.2) Cada AP determinará los sistemas de firma de su personal. • Identificando titular + Admón. • [Indicando sólo el NIP]
Interoperabilidad firma electrónica		* (45.1) Las AA.PP. determinarán trámites e informes que incluirán firma electrónica (cualificada o avanzada). (45.2) Si se usan otros sistemas de FE se podrá superponer un sello electrónico.

Funcionamiento del Sector Púbico: Ley 40/2015 y ENS

Concepto	Ley 39/2015 - LPAC	Ley 40/2015 - LRJSP
Transmisiones de datos entre AA.PP.		(155.1) Facilitar el acceso de otras AA.PP. a los datos que obren en su poder. (155.2) Limitación → a la tramitación y resolución de los procedimientos de su competencia. (155.3) Interconexión de redes AGE-CCAA-EELL → SARA
Asistencia (por funcionario)	(12) funcionarios habilitados.	
Derechos de las personas: • A comunicarse con las AA.PP.	• (13.a) Punto de Acceso Gral. Electrónico.	
Derecho (y obligación) a la relación electrónica con las AA.PP.	(14.1) Personas físicas: voluntario. (14.2) Personas jurídicas + entidades sin personalidad + p.f. colegiadas + representantes + funcionarios: obligatorio.	
Registro	(16.1) Existencia de un Registro Electrónico Gral. en cada Administración.	

Funcionamiento del Sector Púbico: Ley 40/2015 y ENS

Archivo	**(17) Archivo Electrónico Único en cada Administración (de procs. finalizados).**	***(46.1) Todos los documentos utilizados en actuaciones administrativas se almacenarán por medios electrónicos.** **(46.2) Si afectan a derechos o intereses de los particulares → formato que asegure la identidad + integridad.** **(46.3) soportes → medidas de seguridad → ENS. Identificación de usuarios + control de accesos.**
Documento público administrativo	(26.1) Los válidamente emitidos por órganos de las AA.PP. Uso "por defecto" del medio electrónico. (26.2) Validez: información + formato + identificación + referencia temporal + metadatos firma electrónica aplicable.	
Copias realizadas por las AA.PP.	(27.1) Cada AA.PP. determinará órganos con competencias. Mediante funcionario habilitado o Actuación Administrativa Automatizada. (27.2) Copia auténtica: la realizada por órgano competente (identificado) y su contenido. (27.3.a) de doc. electrónico: incluir metadatos. (27.3.b) de doc. papel: digitalizar + metadatos. (27.3.c) en papel: incluir código.	

Funcionamiento del Sector Púbico: Ley 40/2015 y ENS

Concepto	Ley 39/2015 - LPAC	Ley 40/2015 - LRJSP
Forma (de los actos administrativos)	(36) Los a.a. se producirán por escrito a través de medios electrónicos.	
Notificaciones (condiciones generales de las…)	(41) Por medios electrónicos (y siempre que el interesado resulte obligado por esta vía).	
Notificaciones (validez)	(41.b) constancia de: envío o puesta a disposición + recepción o acceso + fechas y horas + contenido íntegro + identidad del remitente y destinatario. Reglamentariamente → en ciertos procedimientos para ciertos colectivos de personas físicas. (41.6) Los avisos de notificaciones → a través de dispositivo electrónico o dirección de email.	
Notificaciones (práctica)	(43) Por Comparecencia en la sede electrónica / a través de Dirección Electrónica Habilitada Única. Si NO acceso en 10 días → rechazada. Podrá accederse a través del Punto de Acceso General Electrónico.	

Funcionamiento del Sector Púbico: Ley 40/2015 y ENS

Concepto	Ley 39/2015 - LPAC	Ley 40/2015 - LRJSP
Expediente Administrativo	(70.1) Conjunto ordenado de documentos antecedentes de la resolución administrativa. (70.2) Tendrán formato electrónico + índice. Teniendo en cuenta el ENI.	
Procedimientos competencia de cada Administración	(21) Relación de procedimientos en página web.	
Órganos colegiados (convocatoria y sesiones)		* (17.1) De forma presencial o a distancia. A distancia asegurando: identidad miembros + contenido manifestaciones + momento + interactividad + disponibilidad de medios. (válidos → email / audioconferecias / videoconferencias). (17.3) Convocatorias: Por medios electrónicos / incluyendo orden del día y documentación / condiciones de celebración / sistema de conexión / lugares disponibles.
Actas (de las sesiones de los órganos colegiados)		* (18.1) Grabación de la sesión + certificación (autenticidad e integridad) del Secretario + documentos electrónicos usados (+garantía de conservación) → Acta. (18.2) Remisión Acta por medios electrónicos. + conformidad o disconformidad.

Funcionamiento del Sector Púbico: Ley 40/2015 y ENS

Concepto	Ley 39/2015 - LPAC	Ley 40/2015 - LRJSP
Sede electrónica		* (38.1) dirección electrónica accesible a los ciudadanos. (38.2) responsabilidad de su titular (integridad + veracidad + actualización información y servicios) (38.3) Cada Administración → condiciones de creación. Principios → transparencia + publicidad + responsabilidad + calidad + seguridad + disponibilidad + accesibilidad + neutralidad + interoperabilidad. • Identificación del órgano titular de la sede → certificados cualificados de autenticación de sitio web. (38.4) Comunicaciones seguras.
Portal de Internet		* (39) Punto de acceso electrónico: • el titular es una A.P. • permite el acceso a través de Internet a la información publicada. + [sede electrónica].
Esquema Nacional de Interoperabilidad y Esquema Nacional de Seguridad		* (156.1) ENI: criterios y recomendaciones (seguridad, conservación y normalización) sobre información, formatos y aplicaciones. (156.2) ENS: Principios básicos y requisitos mínimos de seguridad información tratada [servicios prestados].

Concepto	Ley 39/2015 - LPAC	Ley 40/2015 - LRJSP
Reutilización de sistemas y aplicaciones de propiedad de la Administración		* (157.1) Las AA.PP. pondrán a disposición (si poseen dchos. prop. intelectual) (157.2) Podrán declararse de fuentes abiertas. (157.3) Consulta previa al directorio general de aplicaciones de la AGE → obligadas a su uso , salvo razones justificadas de eficiencia (art. 7 LO 2/2012 EPSF).
Transferencia de tecnología entre Administraciones		* (158.1) Las AA.PP. mantendrán directorios actualizados de aplicaciones para su libre reutilización (interoperables con el directorio de la AGE). (158.2) La AGE mantendrá un directorio general de aplicaciones para su reutilización.

2. ENS:

- ## ¿Por qué es necesaria la seguridad de la información y los servicios?

¿Por qué?

- ✓ **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.**
- ✓ **Como así exigen las Leyes 39/2015 y 40/2015.**

El medio electrónico como medio habitual

BOLETÍN OFICIAL DEL ESTADO

Viernes 2 de octubre de 2015

I. DISPOSICIONES GENERALES

JEFATURA DEL ESTADO

10566 *Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.*

BOLETÍN OFICIAL DEL ESTADO

Viernes 2 de octubre de 2015 Sec. I.

I. DISPOSICIONES GENERALES

JEFATURA DEL ESTADO

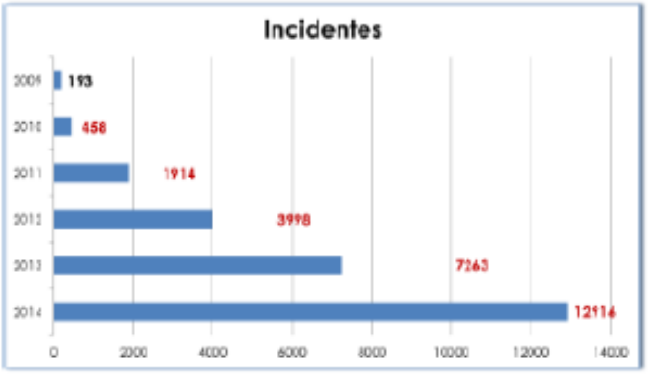
10565 *Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.*

PLAN DE TRANSFORMACIÓN DIGITAL DE LA ADMINISTRACIÓN GENERAL DEL ESTADO Y SUS ORGANISMOS PÚBLICOS

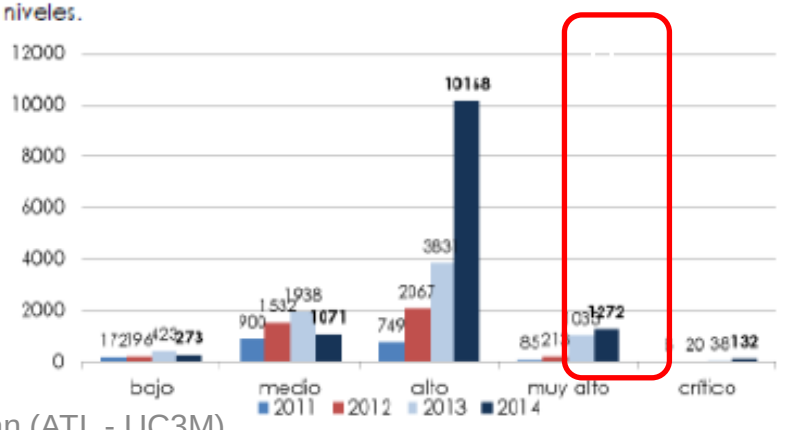
(ESTRATEGIA TIC)
2015 - 2020

Incremento notable de incidentes

Como puede observarse, en 2014 ha crecido significativamente el número de incidentes gestionados.



La Guía CCN-STIC 817 Gestión de Ciberincidentes, tipifica los incidentes de seguridad, atendiendo a su peligrosidad, en cinco niveles: Bajo, Medio, Alto, Muy Alto y Crítico. La figura siguiente muestra la distribución de los incidentes de los últimos años en estos niveles.



Contexto y referentes

OCDE

- Digital Security Risk Management for Economic and Social Prosperity. Recommendation and Companion Doc.

UNIÓN EUROPEA

- Agenda Digital para Europa.
- Estrategia de ciberseguridad de la Unión Europea.
- **Reglamento de identidad electrónica y servicios de confianza (eIDAS)**
- Otros proyectos en curso: de Directiva NIS, de Reglamento de protección de datos de carácter personal.

ENISA

- Identificación de buenas prácticas y tendencias **tecnológicas y emergentes.**

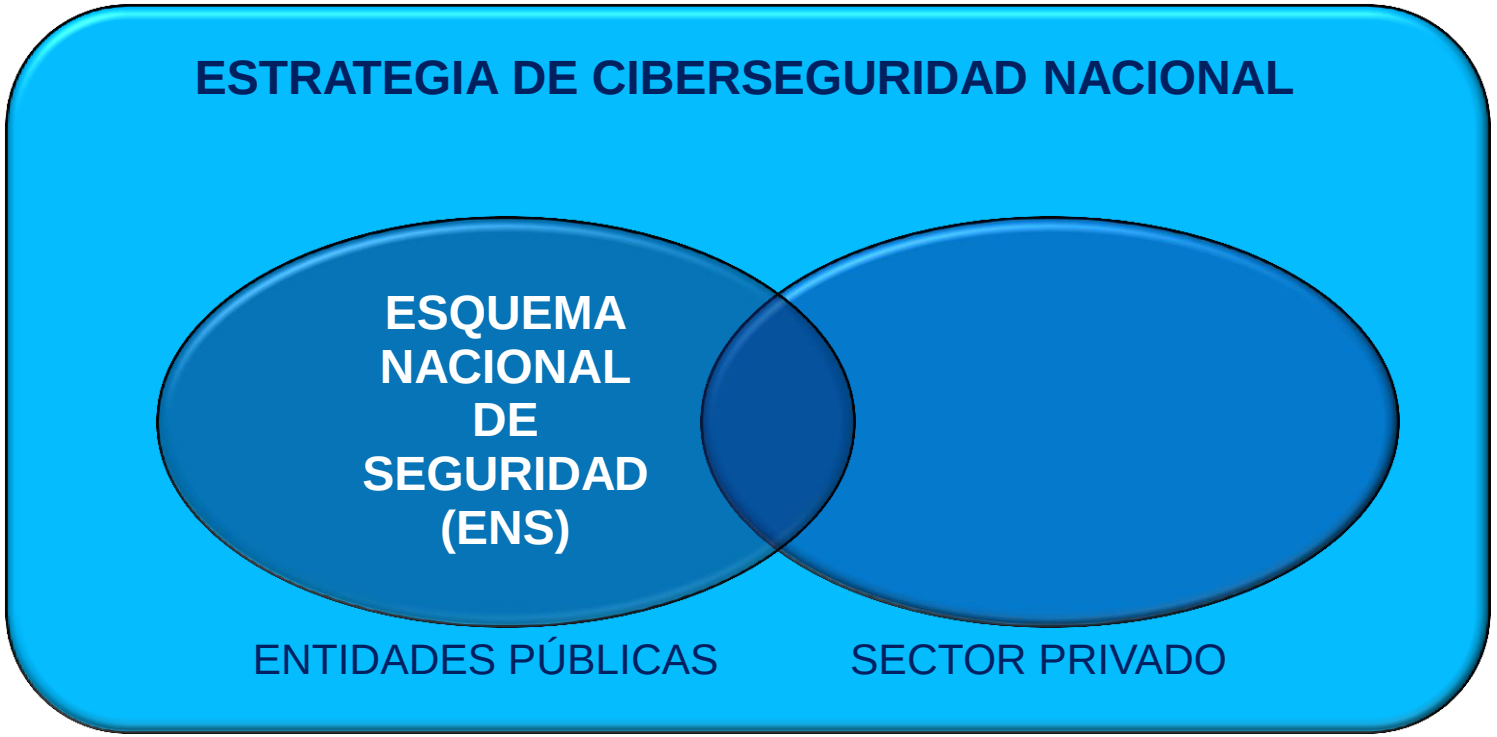
NORMALIZACIÓN en seguridad de TI.

ACTUACIONES EN OTROS PAÍSES:

- EE.UU.: *Federal Information Security Management Act* (FISMA).
- Otros: Reino Unido, Alemania, Francia
- Estrategias nacionales de ciberseguridad

Agenda Digital Europea

Contexto


ESTRATEGIA DE CIBERSEGURIDAD NACIONAL
ESQUEMA NACIONAL DE SEGURIDAD (ENS)
ENTIDADES PÚBLICAS
SECTOR PRIVADO

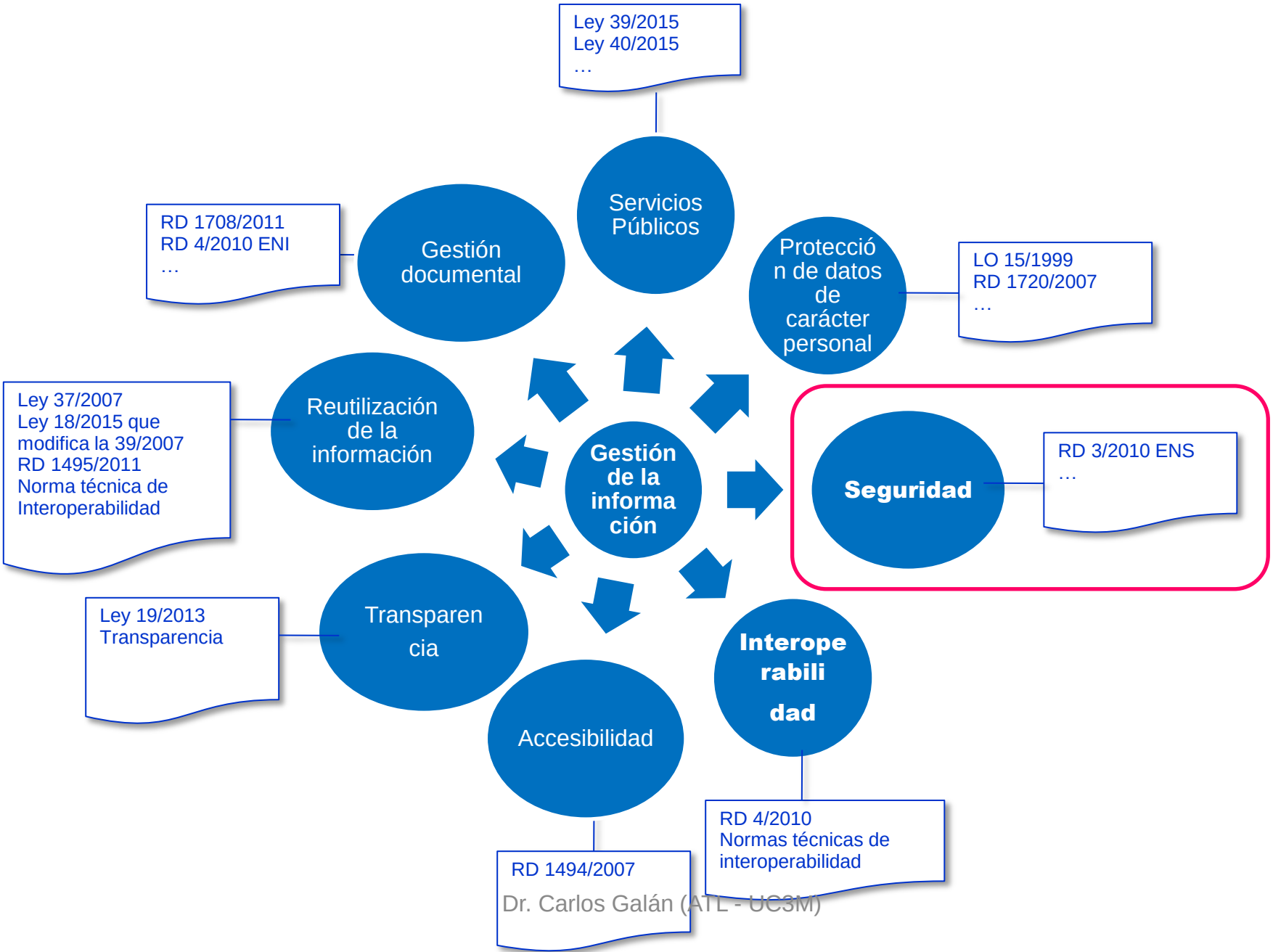
¿Qué es la seguridad de la información?

Es la capacidad de las redes o de los sistemas de información **para resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o malintencionadas que comprometan** la disponibilidad, autenticidad, integridad y confidencialidad de **los datos** almacenados o transmitidos y de **los servicios** que dichas redes y sistemas ofrecen o hacen accesibles.

SEGURIDAD TECNOLÓGICA Y JURÍDICA

Implantar la seguridad en las AA.PP.: el Esquema Nacional de Seguridad

Funcionamiento del Sector Púbico: Ley 40/2015 y ENS



Ley 40/2015 y ciberseguridad pública

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.

El Esquema Nacional de Seguridad

✓ **Es un instrumento legal – Real Decreto 3/2010-** que desarrolla lo previsto sobre seguridad en la Ley 11/2007 (Ley 40/2015).

✓ **Establece la política de seguridad** en los servicios de administración-e.

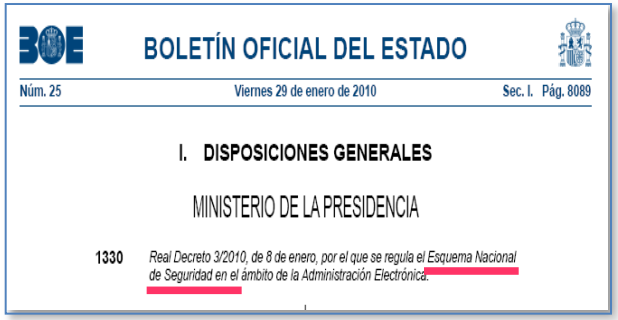
- Está **constituida por principios básicos** y **requisitos mínimos** que permitan una **protección adecuada** de la información.

✓ **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.

✓ **Actualización → Publicado RD 951/2015, Modificación ENS.**



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

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.**

7 elementos principales

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

Actualizando el ENS

- ✓ **RD 3/2010 revisado a la luz de**:
  - la ECSN,
  - a 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 951/2015 modificación ENS.**

Evolución del ENS. Grandes cuestiones tratadas

A la luz de la experiencia y del *feedback* recibido se han tratado las siguientes grandes cuestiones:

- ✓ ¿Cómo avanzar en la **armonización del modo común de actuar** en ciertas cuestiones?
- ✓ ¿Cómo **conocer periódicamente el estado de la seguridad** en las AA.PP. de forma *fácil* para todos?
- ✓ ¿Cómo **reforzar la capacidad de respuesta** frente a los incidentes de seguridad?
- ✓ **¿Qué medidas de seguridad deben mejorarse?**

Aspectos principales de la actualización (I/II)

- ✓ Se enfatiza que la política de seguridad **articule la gestión continuada de la seguridad** (art.11).
- ✓ Se introduce la noción de **profesionales cualificados** (art.15).
- ✓ **En la adquisición de productos certificados** se introduce la **noción de la proporcionalidad** a la categoría del sistema y nivel de seguridad determinados y a los riesgos (art. 18).
- ✓ Se refuerza la **gestión de incidentes** (art. 24)
- ✓ La relación de medidas seleccionadas del anexo II se formalizará en un documento denominado **Declaración de Aplicabilidad**, firmado por el responsable de seguridad (art. 27).
- ✓ Las medidas de seguridad referenciadas en el anexo II podrán ser reemplazadas por otras **compensatorias** siempre y cuando se justifique documentalmente que protegen igual o mejor el riesgo sobre los activos (art. 27).

Aspectos principales de la actualización (II/II)

- ✓ Se introducen la figura de las **instrucciones técnicas de seguridad** para señalar el modo común de actuar (art. 29) en ciertas cuestiones.
- ✓ Se mejoran los mecanismos para obtener un **conocimiento regular del estado de la seguridad** en las AA.PP. (art. 35).
- ✓ Se introduce la **notificación de incidentes de seguridad** (art. 36).
- ✓ Se precisan los **elementos necesarios para la investigación de incidentes de seguridad** (art. 37).
- ✓ **Se mejora la eficacia de ciertas medidas** de seguridad (anexo II): apartados 3.4, 4.1.2, 4.1.5, 4.2.1, 4.2.5, 4.3.3, 4.3.7, 4.3.8, 4.3.9, 4.3.11, 4.4.2, 4.6.1, 4.6.2, 5.2.3, 5.3.3, 5.4.2, 5.4.3, 5.5.2, 5.5.5, 5.6.1, 5.7.4, 5.7.5, 5.7.7 y 5.8.2
- ✓ Se mejora el anexo III de **auditoría de la seguridad**.
- ✓ Se revisa la **clausula de adquisición de productos** de seguridad (anexo V).
- ✓ Se introducen diversas **mejoras editoriales**.

Estado de situación: ¿Dónde estamos?

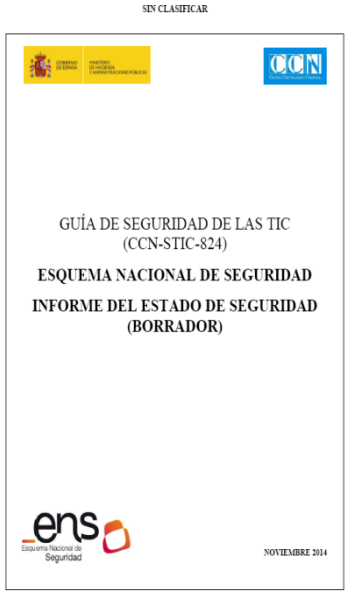
Evaluar el estado de la seguridad

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]**


SIN CLASIFICAR

GUÍA DE SEGURIDAD DE LAS TIC
(CCN-STIC-824)

ESQUEMA NACIONAL DE SEGURIDAD

INFORME DEL ESTADO DE SEGURIDAD
(BORRADOR)

ens Esquema Nacional de Seguridad

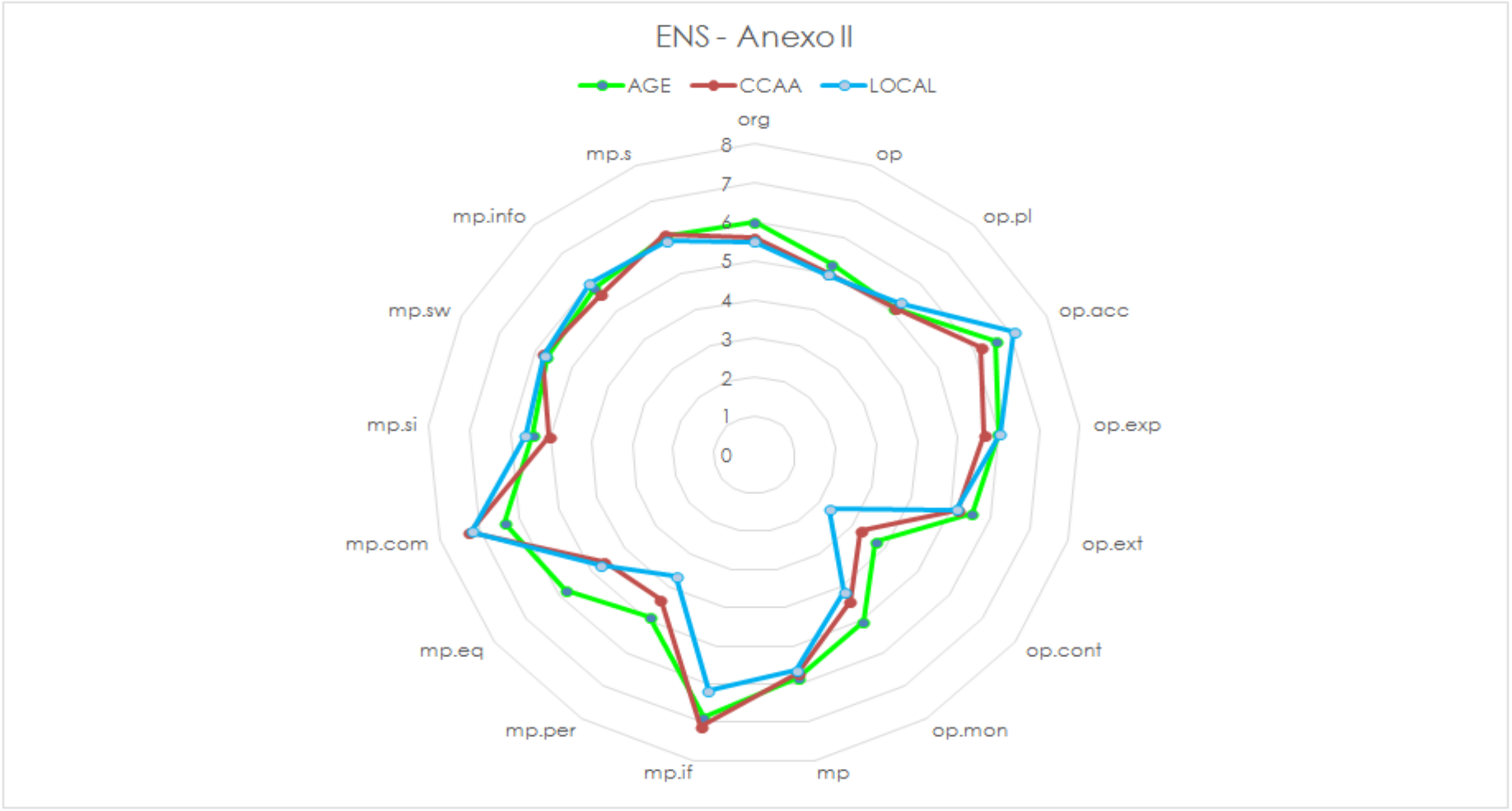
NOVIEMBRE 2014

La herramienta '<inés>' 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.

Fecha tope para cumplimentar INES: 18.12.2015

Situación. Fuente: INES



¿Qué podemos hacer? *Urgencias*

Es esencial que haya:

- ✓ un **plan de adecuación**;
- ✓ un **responsable de seguridad** nombrado;
- ✓ una **categorización** de los sistemas;
- ✓ que se realice el **análisis de riesgos**.

Recomendaciones:

- ✓ Abordar aspectos de gobernanza y documentación:
  - **Proceso de autorización** y **Arquitectura de seguridad**.
- ✓ Aplicar guías CCN-STIC: **Configuración de seguridad** y **Protección de aplicaciones web**.
- ✓ Impulsar:
  - [op.exp.2] **Configuración de seguridad.**
  - [op.exp.3] **Gestión de la configuración.**
  - [op.exp.4] **Mantenimiento** y [op.exp.5] **Gestión de cambios.**
  - [op.exp.8] **Registro de la actividad de los usuarios.**
  - [op.mon.1] **Detección de intrusión** y [op.mon.2] **Sistema de métricas.**
  - [mp.per.3] **Concienciación** y [mp.per.4] **Formación.**

Los servicios comunes reducen la carga para las entidades usuarias en estas medidas.

✓ Servicios comunes
✓ Servicios de seguridad gestionada prestados de forma centralizada.

- # Retos y conclusiones

Garantizar que los Sistemas que utilizan las AA.PP. poseen el adecuado nivel de ciberseguridad y resiliencia

ESTRATEGIA DE CIBERSEGURIDAD NACIONAL

LÍNEA DE ACCIÓN 2

Seguridad de los Sistemas de Información y Telecomunicaciones que soportan las Administraciones Públicas

Asegurar la plena implantación del ENS y articular los procedimientos necesarios para **conocer regularmente el estado** de las principales variables de seguridad de los sistemas afectados.

Ampliar y mejorar las capacidades del CERT de las AA.PP.-CCN-CERT- y particularmente de sus Sistemas de Detección y de Alerta Temprana.

Reforzar las estructuras de seguridad y la capacidad de vigilancia de los Sistemas de Información, en particular los que manejan información clasificada.

Optimizar el modelo de interconexión de los organismos de las AA.PP. españolas a las redes públicas de voz y datos, maximizando su eficacia, disponibilidad y seguridad.

Reforzar la implantación y seguridad de la infraestructura común y segura en la Administración Pública española (**Red SARA**), potenciando su uso y sus capacidades de seguridad y resiliencia.

Desarrollar nuevos servicios horizontales seguros, de acuerdo con directrices de la DTIC de la AGE, organismo responsable de la coordinación, dirección y racionalización del uso de las TIC en la AGE.

Incrementar las actividades nacionales para el desarrollo y evaluación de productos, servicios y sistemas a fin de obtener su certificación apoyando específicamente aquellas que sustenten necesidades de interés nacional.

Potenciar la creación, difusión y aplicación de las Mejores Prácticas en materia de Ciberseguridad en el ámbito de las AA.PP.

Conclusiones

- ✓ La **transformación digital** de la Administración requiere la **protección de la información y los servicios**.
- ✓ **El ENS**, de aplicación a todas las AA.PP., 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.
- ✓ **Retos**:
  - ✓ **Avanzar en ciberseguridad de las AA.PP.**
  - ✓ **Mejorar la seguridad del conjunto y reducir el esfuerzo individual**.
  - ✓ **Mejorar la adecuación**

Muchas gracias

cgalan@atl.es

Primera declaración de servicios compartidos

1. **Servicio unificado de telecomunicaciones**
2. **Servicio de seguridad gestionada**
3. Servicio de alojamiento de infraestructuras TIC
4. Servicio de nube híbrida (Nube SARA)
5. Servicio de correo electrónico unificado
6. Servicio multicanal de atención al ciudadano
7. Servicio de gestión del registro
8. Servicio de gestión de notificaciones
9. Servicio de gestión de nómina
10. Servicio integrado de gestión de personal
11. Servicio común de gestión económico-presupuestaria
12. Servicio común de generación y validación de firmas electrónicas
13. Servicio de gestión de expediente y documento electrónico
14. Servicio de gestión de archivo electrónico

Fuente: http://administracionelectronica.gob.es/pae_Home/dms/pae_Home/documentos/Estrategias/Estrategia_TIC/20151002-Declaracion-servicios-compartidos.pdf

Sección 3ª. Órganos colegiados de las distintas administraciones públicas

Artículo 17. Convocatorias y sesiones

1. Todos los órganos colegiados se podrán constituir, convocar, celebrar sus sesiones, adoptar acuerdos y remitir actas tanto **de forma presencial como a distancia**, salvo que su reglamento interno recoja expresa y excepcionalmente lo contrario.

En las sesiones que celebren los órganos colegiados a distancia, sus miembros podrán encontrarse en distintos lugares siempre y cuando se asegure por m**edios electrónicos,** considerándose también tales los telefónicos, y audiovisuales, **la identidad de los miembros o personas que los suplan, el contenido de sus manifestaciones, el momento en que éstas se producen, así como la interactividad e intercomunicación entre ellos en tiempo real y la disponibilidad de los medios durante la sesión. Entre otros, se considerarán incluidos entre los medios electrónicos válidos, el correo electrónico, las audioconferencias y las videoconferencias.**

2. Para la válida constitución del órgano, a efectos de la celebración de sesiones, deliberaciones y toma de acuerdos, se requerirá la asistencia, presencial o a distancia, del Presidente y Secretario o en su caso, de quienes les suplan, y la de la mitad, al menos, de sus miembros.

Cuando se trate de los órganos colegiados a que se refiere el artículo 15.2, el Presidente podrá considerar válidamente constituido el órgano, a efectos de celebración de sesión, si asisten los representantes de las Administraciones Públicas y de las organizaciones representativas de intereses sociales miembros del órgano a los que se haya atribuido la condición de portavoces.

Cuando estuvieran reunidos, de manera presencial o a distancia, el Secretario y todos los miembros del órgano colegiado, o en su caso las personas que les suplan, éstos podrán constituirse válidamente como órgano colegiado para la celebración de sesiones, deliberaciones y adopción de acuerdos sin necesidad de convocatoria previa cuando así lo decidan todos sus miembros.

3. Los órganos colegiados podrán establecer el régimen propio de convocatorias, si éste no está previsto por sus normas de funcionamiento. Tal régimen podrá prever una segunda convocatoria y especificar para ésta el número de miembros necesarios para constituir válidamente el órgano.

Salvo que no resulte posible, **las convocatorias serán remitidas a los miembros del órgano colegiado a través de medios electrónicos, haciendo constar en la misma el orden del día junto con la documentación necesaria para su deliberación cuando sea posible, las condiciones en las que se va a celebrar la sesión, el sistema de conexión y, en su caso, los lugares en que estén disponibles los medios técnicos necesarios para asistir y participar en la reunión.**

4. No podrá ser objeto de deliberación o acuerdo ningún asunto que no figure incluido en el orden del día, salvo que asistan todos los miembros del órgano colegiado y sea declarada la urgencia del asunto por el voto favorable de la mayoría.

5. Los acuerdos serán adoptados por mayoría de votos. Cuando se asista a distancia, **los acuerdos se entenderán adoptados en el lugar donde tenga la sede el órgano colegiado y, en su defecto, donde esté ubicada la presidencia.**

6. Cuando los miembros del órgano voten en contra o se abstengan, quedarán exentos de la responsabilidad que, en su caso, pueda derivarse de los acuerdos.

7. Quienes acrediten la titularidad de un interés legítimo podrán dirigirse al Secretario de un órgano colegiado para que les sea expedida certificación de sus acuerdos. La **certificación será expedida por medios electrónicos**, salvo que el interesado manifieste expresamente lo contrario y no tenga obligación de relacionarse con las Administraciones por esta vía.

Artículo 18. Actas

1. De cada sesión que celebre el órgano colegiado se levantará acta por el Secretario, que especificará necesariamente los asistentes, el orden del día de la reunión, las circunstancias del lugar y tiempo en que se ha celebrado, los puntos principales de las deliberaciones, así como el contenido de los acuerdos adoptados.
Podrán grabarse las sesiones que celebre el órgano colegiado. El fichero resultante de la grabación, junto con la certificación expedida por el Secretario de la autenticidad e integridad del mismo, y cuantos documentos en soporte electrónico se utilizasen como documentos de la sesión, podrán acompañar al acta de las sesiones, sin necesidad de hacer constar en ella los puntos principales de las deliberaciones.

2. El acta de cada sesión podrá aprobarse en la misma reunión o en la inmediata siguiente. El Secretario elaborará el acta con el visto bueno del Presidente y lo remitirá a través de medios electrónicos, a los miembros del órgano colegiado, quienes podrán manifestar por los mismos medios su conformidad o reparos al texto, a efectos de su aprobación, considerándose, en caso afirmativo, aprobada en la misma reunión. Cuando se hubiese optado por la grabación de las sesiones celebradas o por la utilización de documentos en soporte electrónico, **deberán conservarse de forma que se garantice la integridad y autenticidad de los ficheros electrónicos correspondientes y el acceso a los mismos por parte de los miembros del órgano colegiado.**

CAPÍTULO V. Funcionamiento electrónico del sector público

Artículo 38. La sede electrónica

1. La sede electrónica es aquella **dirección electrónica, disponible para los ciudadanos a través de redes de telecomunicaciones**, cuya titularidad corresponde a una Administración Pública, o bien a una o varios organismos públicos o entidades de Derecho Público en el ejercicio de sus competencias.

2. El establecimiento de una sede electrónica conlleva la **responsabilidad del titular** respecto de la integridad, veracidad y actualización de la información y los servicios a los que pueda accederse a través de la misma.

3. **Cada Administración Pública determinará las condiciones e instrumentos de creación de las sedes electrónicas**, con sujeción a los principios de transparencia, publicidad, responsabilidad, calidad, seguridad, disponibilidad, accesibilidad, neutralidad e interoperabilidad. En todo caso deberá **garantizarse la identificación del órgano titular de la sede**, así como los medios disponibles para la formulación de sugerencias y quejas.

…

…

4. Las sedes electrónicas dispondrán de sistemas que permitan el **establecimiento de comunicaciones seguras** siempre que sean necesarias.

5. La publicación en las sedes electrónicas de informaciones, servicios y transacciones respetará los principios de accesibilidad y uso de acuerdo con las normas establecidas al respecto, estándares abiertos y, en su caso, aquellos otros que sean de uso generalizado por los ciudadanos.

6. Las sedes electrónicas utilizarán, para identificarse y garantizar una comunicación segura con las mismas, **certificados reconocidos o cualificados de autenticación de sitio web o medio equivalente.**

Artículo 39. Portal de internet

Se entiende por portal de internet el **punto de acceso electrónico cuya titularidad corresponda a una Administración Pública**, organismo público o entidad de Derecho Público que permite el acceso a través de internet a la información publicada y, en su caso, a la sede electrónica correspondiente.

Artículo 40. Sistemas de identificación de las Administraciones Públicas

1. Las Administraciones Públicas podrán identificarse mediante el uso de un **sello electrónico basado en un certificado electrónico reconocido o cualificado** que reúna los requisitos exigidos por la legislación de firma electrónica. Estos certificados electrónicos **incluirán el número de identificación fiscal y la denominación correspondiente, así como, en su caso, la identidad de la persona titular** en el caso de los sellos electrónicos de órganos administrativos. La relación de sellos electrónicos utilizados por cada Administración Pública, incluyendo las características de los certificados electrónicos y los prestadores que los expiden, deberá ser pública y accesible por medios electrónicos. Además, cada Administración Pública adoptará las medidas adecuadas para **facilitar la verificación de sus sellos electrónicos**.

2. Se entenderá identificada la Administración Pública respecto de la información que se publique como propia en su portal de internet.

Artículo 41. Actuación administrativa automatizada

1. Se entiende por actuación administrativa automatizada, **cualquier acto o actuación realizada íntegramente a través de medios electrónicos por una Administración Pública en el marco de un procedimiento administrativo y en la que no haya intervenido de forma directa un empleado público.**

2. En caso de actuación administrativa automatizada deberá establecerse previamente el **órgano u órganos competentes**, según los casos, para la definición de las **especificaciones, programación, mantenimiento, supervisión y control de calidad** y, en su caso, auditoría del sistema de información y de su código fuente. Asimismo, se indicará el órgano que debe ser **considerado responsable a efectos de impugnación**.

Artículo 42. Sistemas de firma para la actuación administrativa automatizada

En el ejercicio de la competencia en la actuación administrativa automatizada, cada Administración Pública podrá determinar los supuestos de utilización de los siguientes sistemas de firma electrónica:

a) **Sello electrónico** de Administración Pública, órgano, organismo público o entidad de derecho público, basado en certificado electrónico reconocido o cualificado que reúna los requisitos exigidos por la legislación de firma electrónica.

b) **Código seguro de verificación** vinculado a la Administración Pública, órgano, organismo público o entidad de Derecho Público, en los términos y condiciones establecidos, permitiéndose en todo caso la comprobación de la integridad del documento mediante el acceso a la sede electrónica correspondiente.

Artículo 43. Firma electrónica del personal al servicio de las Administraciones Públicas

1. Sin perjuicio de lo previsto en los artículos 38, 41 y 42, la actuación de una Administración Pública, órgano, organismo público o entidad de derecho público, cuando utilice medios electrónicos, se realizará mediante **firma electrónica del titular del órgano o empleado público.**

2. Cada Administración Pública determinará los sistemas de firma electrónica que debe utilizar su personal, los cuales podrán **identificar de forma conjunta al titular del puesto de trabajo o cargo y a la Administración u órgano** en la que presta sus servicios. Por razones de seguridad pública los sistemas de firma electrónica podrán referirse sólo el **número de identificación profesional** del empleado público.

Artículo 44. Intercambio electrónico de datos en entornos cerrados de comunicación

1. Los documentos electrónicos transmitidos en entornos cerrados de comunicaciones establecidos entre Administraciones Públicas, órganos, organismos públicos y entidades de derecho público, serán **considerados válidos a efectos de autenticación e identificación de los emisores y receptores en las condiciones establecidas en este artículo.**

2. Cuando los participantes en las comunicaciones pertenezcan **a una misma Administración Pública**, ésta determinará las condiciones y garantías por las que se regirá que, al menos, comprenderá la **relación de emisores y receptores autorizados y la naturaleza de los datos a intercambiar.**

3. Cuando los participantes pertenezcan a **distintas Administraciones**, las condiciones y garantías citadas en el apartado anterior se establecerán **mediante convenio** suscrito entre aquellas.

4. En todo caso **deberá garantizarse la seguridad** del entorno cerrado de comunicaciones y la **protección de los datos** que se transmitan.

Artículo 45. Aseguramiento e interoperabilidad de la firma electrónica

1. **Las Administraciones Públicas podrán determinar los trámites e informes que incluyan firma electrónica reconocida o cualificada y avanzada** basada en certificados electrónicos reconocidos o cualificados de firma electrónica.

2. Con el fin de favorecer la interoperabilidad y posibilitar la verificación automática de la firma electrónica de los documentos electrónicos, cuando una Administración utilice **sistemas de firma electrónica distintos de aquellos basados en certificado electrónico reconocido o cualificado**, para remitir o poner a disposición de otros órganos, organismos públicos, entidades de Derecho Público o Administraciones la documentación firmada electrónicamente, **podrá superponer un sello electrónico basado en un certificado electrónico reconocido o cualificado.**

Artículo 46. Archivo electrónico de documentos

1. **Todos los documentos utilizados en las actuaciones administrativas se almacenarán por medios electrónicos, salvo cuando no sea posible**.

2. Los documentos electrónicos que contengan actos administrativos que afecten a derechos o intereses de los particulares deberán conservarse en soportes de esta naturaleza, ya sea en el mismo formato a partir del que se originó el documento o en otro cualquiera que **asegure la identidad e integridad de la información** necesaria para reproducirlo. Se asegurará en todo caso la posibilidad de trasladar los datos a otros formatos y soportes que garanticen el acceso desde diferentes aplicaciones.

3. Los medios o soportes en que se almacenen documentos, deberán contar con **medidas de seguridad**, de acuerdo con lo previsto en el **Esquema Nacional de Seguridad**, que garanticen la integridad, autenticidad, confidencialidad, calidad, protección y conservación de los documentos almacenados. En particular, asegurarán la **identificación de los usuarios y el control de accesos**, el cumplimiento de las garantías previstas en la legislación de protección de datos, así como la recuperación y conservación a largo plazo de los documentos electrónicos producidos por las Administraciones Públicas que así lo requieran, de acuerdo con las especificaciones sobre el ciclo de vida de los servicios y sistemas utilizados.

CAPÍTULO IV. Relaciones electrónicas entre las Administraciones

Artículo 155. Transmisiones de datos entre Administraciones Públicas

1. De conformidad con lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y su normativa de desarrollo, **cada Administración deberá facilitar el acceso de las restantes Administraciones Públicas a los datos relativos a los interesados que obren en su poder**, especificando las condiciones, protocolos y criterios funcionales o técnicos necesarios para acceder a dichos datos con las máximas garantías de seguridad, integridad y disponibilidad.

2. La disponibilidad de tales datos estará limitada estrictamente a aquellos que son requeridos a los interesados por las restantes Administraciones **para la tramitación y resolución de los procedimientos y actuaciones de su competencia**, de acuerdo con la normativa reguladora de los mismos.

3. La Administración General del Estado, las Administraciones Autonómicas y las Entidades Locales, adoptarán las medidas necesarias e incorporarán en sus respectivos ámbitos las tecnologías precisas para posibilitar la **interconexión de sus redes** con el fin de crear una red de comunicaciones que interconecte los sistemas de información de las Administraciones Públicas y permita el intercambio de información y servicios entre las mismas, así como la interconexión con las redes de las **instituciones de la Unión Europea** y de otros Estados Miembros.

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**.

Artículo 157. Reutilización de sistemas y aplicaciones de propiedad de la Administración

1. **Las Administraciones pondrán a disposición de cualquiera de ellas que lo solicite las aplicaciones, desarrolladas por sus servicios o que hayan sido objeto de contratación y de cuyos derechos de propiedad intelectual sean titulares**, salvo que la información a la que estén asociadas sea objeto de especial protección por una norma. Las Administraciones cedentes y cesionarias podrán acordar la repercusión del coste de adquisición o fabricación de las aplicaciones cedidas.

2. Las aplicaciones a las que se refiere el apartado anterior podrán ser **declaradas como de fuentes abiertas**, cuando de ello se derive una mayor transparencia en el funcionamiento de la Administración Pública o se fomente con ello la incorporación de los ciudadanos a la Sociedad de la información.

…

…

3. Las Administraciones Públicas, **con carácter previo a la adquisición**, desarrollo o al mantenimiento a lo largo de todo el ciclo de vida de una aplicación, tanto si se realiza con medios propios o por la contratación de los servicios correspondientes, **deberán consultar en el directorio general de aplicaciones**, dependiente de la Administración General del Estado, si existen soluciones disponibles para su reutilización, que puedan satisfacer total o parcialmente las necesidades, mejoras o actualizaciones que se pretenden cubrir, y siempre que los requisitos tecnológicos de interoperabilidad y seguridad así lo permitan.

En este directorio constarán tanto las aplicaciones disponibles de la Administración General del Estado como las disponibles en los directorios integrados de aplicaciones del resto de Administraciones.

En el caso de existir una solución disponible para su reutilización total o parcial, **las Administraciones Públicas estarán obligadas a su uso, salvo que la decisión de no reutilizarla se justifique en términos de eficiencia conforme al artículo 7 de la Ley Orgánica 2/2012, de 27 de abril, de Estabilidad Presupuestaria y Sostenibilidad Financiera.**

Artículo 158. Transferencia de tecnología entre Administraciones

1. Las Administraciones Públicas mantendrán **directorios actualizados de aplicaciones para su libre reutilización**, de conformidad con lo dispuesto en el Esquema Nacional de Interoperabilidad. Estos directorios deberán ser plenamente interoperables con el directorio general de la Administración General del Estado, de modo que se garantice su compatibilidad informática e interconexión.

2. **La Administración General del Estado, mantendrá un directorio general de aplicaciones para su reutilización**, prestará apoyo para la libre reutilización de aplicaciones e impulsará el desarrollo de aplicaciones, formatos y estándares comunes en el marco de los esquemas nacionales de interoperabilidad y seguridad.

Disposición derogatoria única. Derogación normativa

Quedan derogadas cuantas disposiciones de igual o inferior rango se opongan, contradigan o resulten incompatibles con lo dispuesto en la presente Ley y, en especial:
a) El artículo 87 de la Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local.
b) El artículo 110 del texto refundido de las disposiciones legales vigentes en materia de Régimen Local aprobado por el Real Decreto Legislativo 781/1986, de 18 de abril.
c) Ley 6/1997, de 14 de abril, de Organización y Funcionamiento de la Administración General del Estado.
d) Los artículos 44, 45 y 46 de la Ley 50/2002, de 26 de diciembre, de Fundaciones.
e) Ley 28/2006, de 18 de julio, de Agencias estatales para la mejora de los servicios públicos.
f) Los artículos 12, 13, 14 y 15 y disposición adicional sexta de la Ley 15/2014, de 16 de septiembre, de racionalización del Sector Público y otras medidas de reforma administrativa.
g) El artículo 6.1.f), la disposición adicional tercera, la disposición transitoria segunda y la disposición transitoria cuarta del Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos.
h) Los artículos 37, 38, 39 y 40 del Decreto de 17 de junio de 1955 por el que se aprueba el Reglamento de Servicios de las Corporaciones locales.
Hasta que, de acuerdo con lo previsto en la disposición adicional cuarta, concluya el plazo de adaptación de las agencias existentes en el sector público estatal, se mantendrá en vigor la Ley 28/2006, de 18 de julio.