GOBIERNO DE ESPAÑA
MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS

CEOE
CONFEDERACIÓN ESPAÑOLA DE ORGANIZACIONES EMPRESARIALES

AMETIC

ens Esquema Nacional de Seguridad V2

Esquema Nacional de Seguridad v2: Mejorando la mejora de la Seguridad de la Administración

11 de noviembre de 2015, 10:00-12:00

Sala JDN-Hemiciclo CEOE - Diego de León, 50 - 28006 Madrid

Principales novedades en el ENS

Miguel A. Amutio Gómez
Subdirector Adjunto de Coordinación de Unidades TIC
Dirección de Tecnologías de la Información y las Comunicaciones

1. Actualización del ENS, ¿qué novedades hay?

Foto: Austin Schmid

El medio electrónico como medio habitual

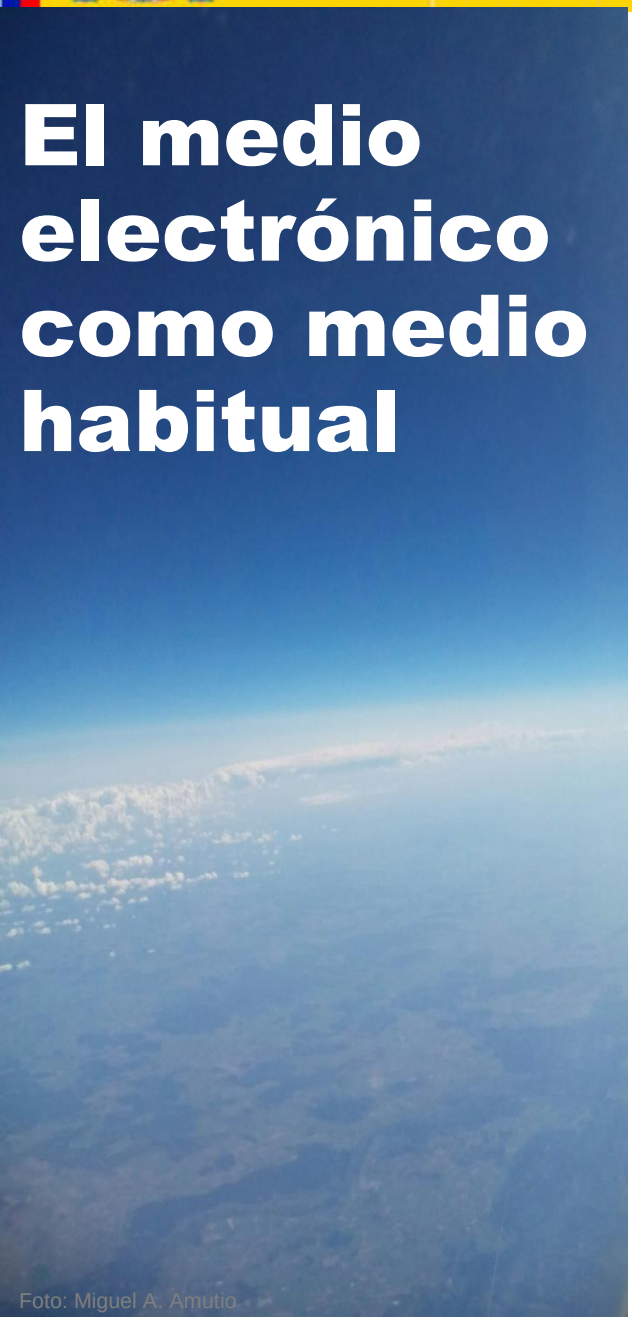


Foto: Miguel A. Amutio

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.*

Ley 40/2015 y seguridad

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 en la 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.

Estrategia TIC

Objetivo Estratégico V

Estrategia corporativa de seguridad y usabilidad

Línea de acción 9

Garantizar la seguridad de los sistemas de información de la AGE y sus organismos públicos

El Esquema Nacional de Seguridad introduce los elementos necesarios para generar confianza en el uso de los medios electrónicos para que los ciudadanos puedan relacionarse con la Administración digitalmente con plena garantía y seguridad.

Para ello, dispone un conjunto de medidas a aplicar en las redes y sistemas de información de los que es titular la Administración. El ENS se enfoca fundamentalmente en todos aquellos sistemas que dan soporte a un servicio público dirigido al ciudadano o empresa. Es necesario ampliar ese enfoque, e iniciar ciclos de mejora continua en la protección de todos los sistemas de información.

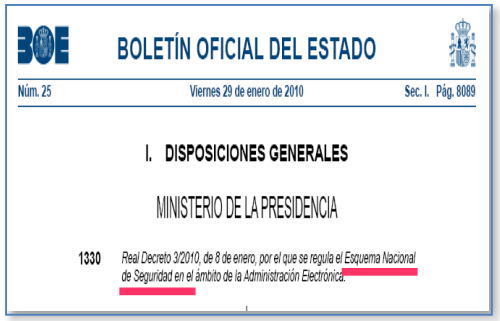
Además, es necesario tener en cuenta el equilibrio entre seguridad y usabilidad, así como avanzar en aumentar la disponibilidad de los sistemas y publicarlos.

Esta línea está directamente relacionada con el objetivo 1 de la Estrategia Nacional de Ciberseguridad, como contribución a la misma.

- Ampliación del alcance del ENS a todos los Sistemas de Información de las AA.PP. españolas, al objeto de ampliar los beneficios derivados de su implantación y facilitar su plena implantación según lo previsto en la Estrategia de Ciberseguridad Nacional.
- Informar sobre la disponibilidad de los servicios y para aquellos servicios más críticos indicar el porcentaje máximo de indisponibilidad.
- Crear un entorno que confiera al ciudadano seguridad al hacer uso de los servicios públicos digitales.
- Desarrollar una Política de Seguridad Común a toda la AGE y sus organismos públicos.
- Implantar una plataforma común de seguridad gestionada que permita garantizar unos niveles mínimos y aceptables de seguridad para todos los organismos.

Esquema Nacional de Seguridad

- ✓ **Instrumento legal – Real Decreto 3/2010**
- ✓ **Establece la política de seguridad** en los servicios de administración-e:
  - **Principios básicos** y **requisitos mínimos** que permitan una **protección adecuada** de la información.
- ✓ **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 (BOE de 4.11.2015).


BOLETÍN OFICIAL DEL ESTADO
Núm. 25 Viernes 29 de enero de 2010 Sec. I. Pág. 8089

I. DISPOSICIONES GENERALES

MINISTERIO DE LA PRESIDENCIA

1330 Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.


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

I. DISPOSICIONES GENERALES

MINISTERIO DE LA PRESIDENCIA

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

ens Esquema Nacional de Seguridad

Política de seguridad y gestión continuada

Artículo 11. Requisitos mínimos de seguridad.(*)

Todos los órganos superiores de las Administraciones públicas **deberán disponer formalmente de su política de seguridad que articule la gestión continuada de la seguridad**, que será aprobada por el titular del órgano superior correspondiente.

(*) Actualizado

Aspectos principales de la actualización (I/III)

- ✓ 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/III)

- ✓ 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 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**.

Aspectos principales de la actualización (III/III)

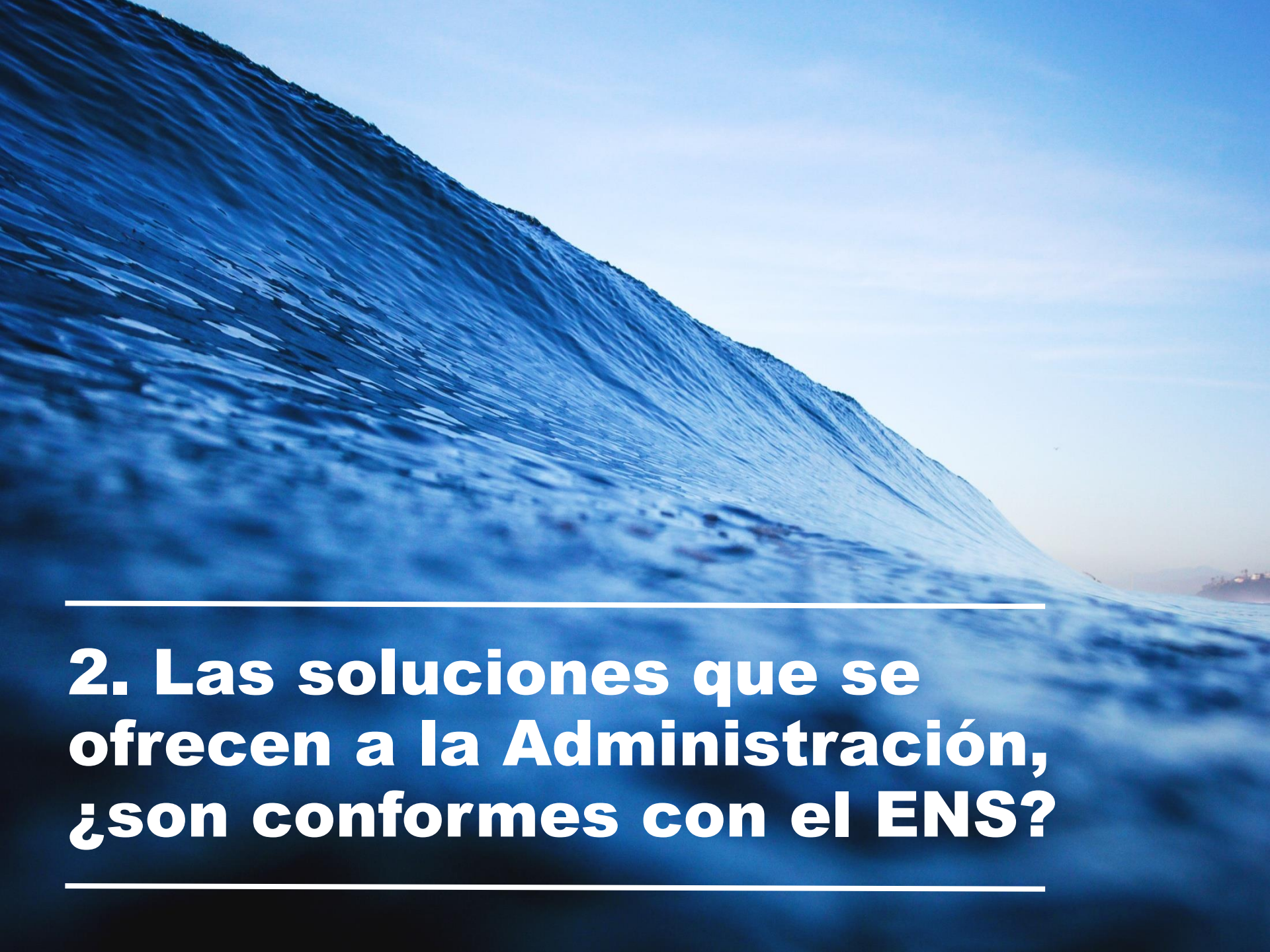
- ✓ **Se mejoran ciertas medidas** de seguridad (anexo II). Principalmente:
  - 3.4 Proceso de autorización [org.4]
  - 4.1.2. Arquitectura de seguridad [op.pl.2]
  - 4.1.5 Componentes certificados [op.pl.5] + medidas relacionadas
  - 4.2.1. Identificación [op.acc.1]
  - 4.2.5. Mecanismo de autenticación [op.acc.5]
  - 4.3.7. Gestión de incidentes [op.exp.7]
  - 4.3.8. Registro de la actividad de los usuarios [op.exp.8]
  - 4.3.9. Registro de la gestión de incidentes [op.exp.9]
  - 4.6.1. Detección de intrusión [op.mon.1]
  - 4.6.2. Sistema de métricas [op.mon.2]
  - 5.4.3. Protección de la autenticidad y de la integridad [mp.com.3]
  - 5.5.5. Borrado y destrucción [mp.si.5]
  - 5.6.1. Desarrollo de aplicaciones [mp.sw.1]
  - 5.7.4. Firma electrónica [mp.info.4]
  - 5.7.7. Copias de seguridad [mp.info.9]

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

Contribución de AMETIC a la actualización

Los comentarios de **AMETIC** han ayudado a mejorar:

- ✓ Artículo **15 Profesionalidad**.
- ✓ Artículo **24 Gestión de incidentes**.
- ✓ Artículo **39 Ciclo de vida**
- ✓ 5.6.1 **Desarrollo seguro [mp.sw.1]**
- ✓ 4.3.7 **Gestión de incidentes [op.exp.7]**



2. Las soluciones que se ofrecen a la Administración, ¿son conformes con el ENS?

Las soluciones que se ofrecen a la Administración,

¿son conformes con el ENS?

Conformidad con el ENS

Art. 41: ... 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 ENS.

Demanda

- ✓ **Órganos y Entidades** de Derecho Público.
- ✓ **Proveedores** de soluciones y tecnología.
- ✓ Prestadores de **servicios de auditoría y certificación**.

Capacidades

Hay quien sabe:

- ✓ Auditar y certificar.
- ✓ Acreditar la competencia técnica.

Pautas

- ✓ Verificación cumplimiento y **publicación** de **conformidad**.
- ✓ También de soluciones y tecnología.
- ✓ **Auditoría y certificación**.

27001 como soporte al cumplimiento del ENS

ens Esquema Nacional de Seguridad

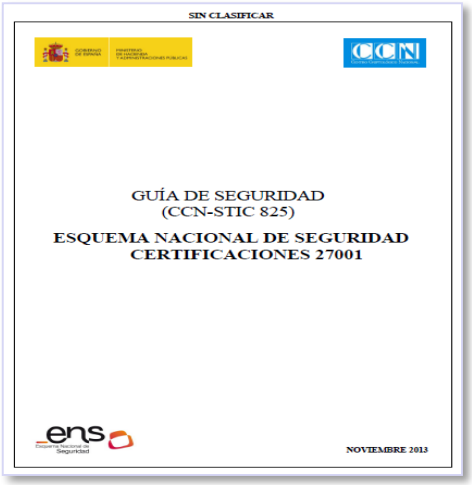
✓ Requiere la **protección de información y servicios**, proporcionada para racionalizar la implantación de las medidas.

✓ Contempla **aspectos de interés la Administración**.

✓ **Exige la gestión continuada de la seguridad.**

norma española
UNE-ISO/IEC 27001

✓ **Proporciona los requisitos para la construcción** (y posterior certificación, en su caso) **de un SGSI** (sistema de gestión de seguridad de la información).


SIN CLASIFICAR

GUÍA DE SEGURIDAD
(CCN-STIC 825)
ESQUEMA NACIONAL DE SEGURIDAD
CERTIFICACIONES 27001

NOVIEMBRE 2013

✓ CCN-STIC 825 **explica la aplicación de 27001 como soporte de cumplimiento del ENS**.

✓ Ayuda a determinar:

- **qué controles del Anexo A** de 27001, desarrollados en la 27002, **son necesarios** para cumplimiento de cada medida del Anexo II del ENS
- y, en su caso, **qué elementos adicionales son requeridos**.

27001 como soporte al cumplimiento del ENS

Aspectos de interés de la Administración

✓ La Administración requiere tratar las **5 dimensiones**:

- ✓Disponibilidad
- ✓**Autenticidad**
- ✓Integridad
- ✓Confidencialidad
- ✓**Trazabilidad**

✓ **Ciertas medidas de seguridad son de especial interés** en el quehacer de la Administración, por ejemplo:

op.acc	Control de acceso	
op.acc.1	Identificación	1
op.acc.2	Requisitos de acceso	1
op.acc.3	Segregación de funciones y tareas	0
op.acc.4	Proceso de gestión de derechos de acceso	1
op.acc.5	Mecanismo de autenticación	3
op.acc.6	Acceso local (local logon)	1
op.acc.7	Acceso remoto (remote login)	1

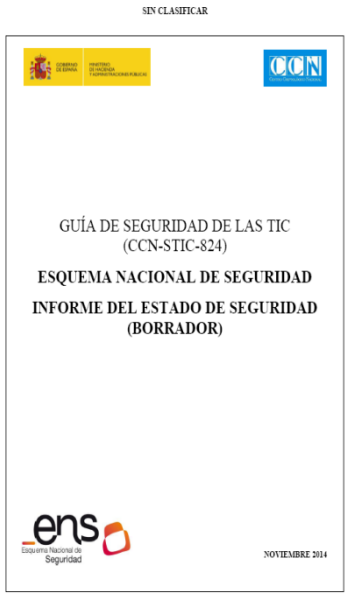
✓ **CCN-STIC 825 orienta en el esfuerzo adicional para completar** lo requerido por el ENS:

nivel	comentario
0	cubierto siempre conviene validar que se contemplan los detalles específicos del ENS
1	probablemente cubierto hay que verificar que se cubren todos y cada uno de los aspectos contemplados en el ENS para los niveles de seguridad requeridos por el sistema y la categoría del mismo; pero cabe esperar que el esfuerzo adicional sea marginal
2	probablemente se necesite completar hay que verificar que se cubren todos y cada uno de los aspectos contemplados en el ENS para los niveles de seguridad requeridos por el sistema y la categoría del mismo; pero cabe esperar que el esfuerzo adicional sea significativo
3	no cubierto son aspectos que no se cubren en los controles de la norma 27002 ni en los requisitos de la norma 27001, por lo que deberán ser objeto de una auditoría específica

Evaluar el estado de la seguridad

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

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 ' 

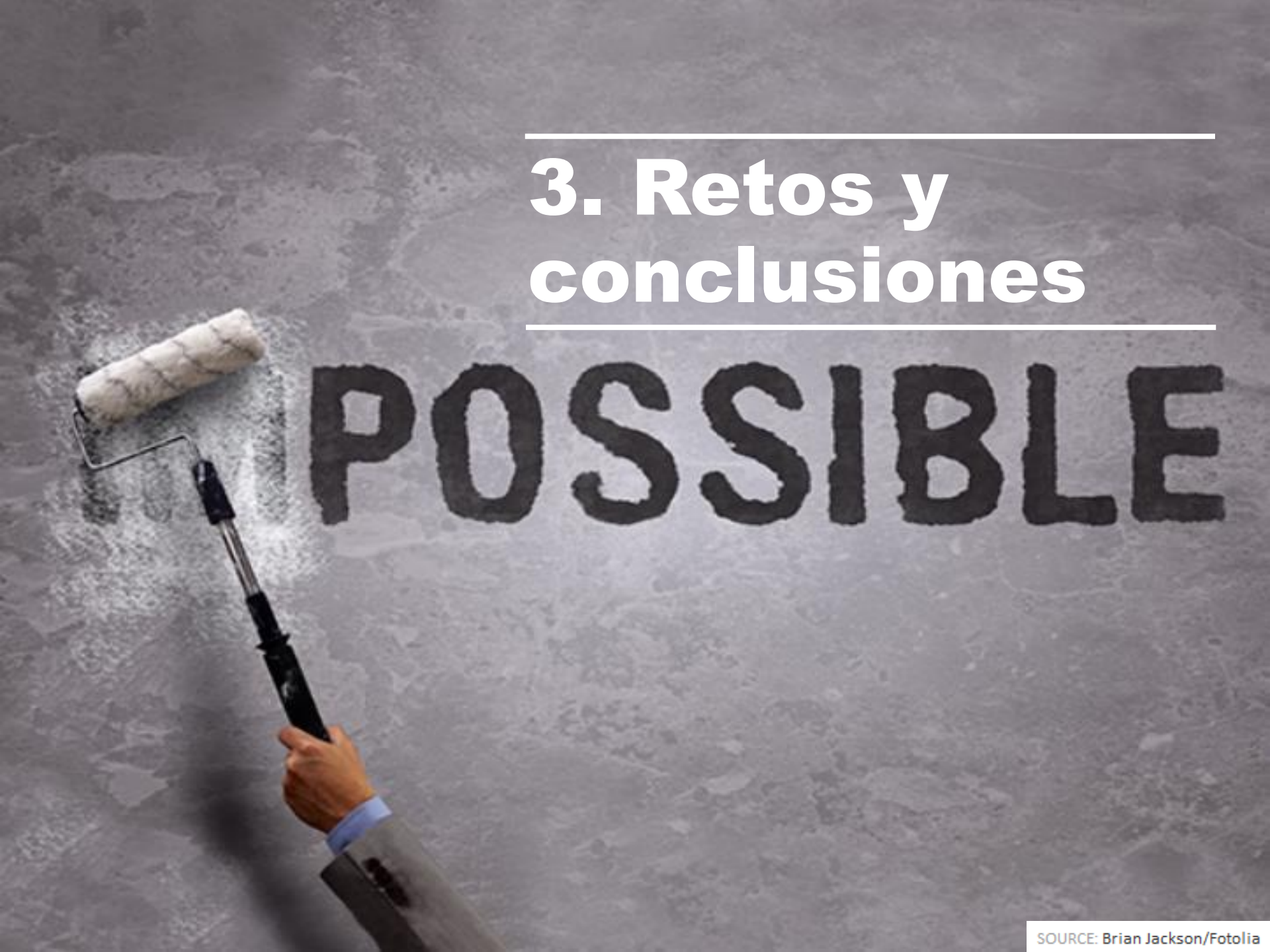
' facilita la recogida y consolidación de información** para el *Informe del Estado de la Seguridad* (RD 3/2010, art. 35 y línea de acción 2 de Estrategia de Ciberseguridad Nacional).

Informe del Estado de la Seguridad en el ENS.

1) Registro portal CCN-CERT
2) Acceso a INES
   - ines@ccn-cert.cni.es

18.12.2015 Fin plazo recogida de datos

3. Retos y conclusiones



SOURCE: Brian Jackson/Fotolia

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.

Retos y conclusiones

- ✓ La **evolución hacia la administración digital** requiere la **protección de la información y los servicios**.
- ✓ **El ENS**, de aplicación a todas las AA.PP., **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**:
    - De las AA.PP.
    - De los proveedores de soluciones y tecnología
    - De los prestadores de servicios de auditoría y certificación.

ens Esquema Nacional de Seguridad

Esfuerzo colectivo

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

Pero sobre todo:

- ✓ Esfuerzo colectivo de **todas las AA.PP.** (AGE, CC.AA., EE.LL. (FEMP), Universidades (CRUE), ámbito de Justicia (EJIS), **coordinado por MINHAP y CCN**.
- ✓ **+ Industria** sector seguridad TIC.
- ✓ **Convencimiento común:** gestión continuada de la seguridad, con un tratamiento homogéneo y adaptado al quehacer de la Administración.

Guías CCN-STIC publicadas en https://www.ccn-cert.cni.es :

800 - Glosario de Términos y Abreviaturas del ENS
801 - Responsables y Funciones en el ENS
802 - Auditoría de la seguridad en el ENS
803 - Valoración de sistemas en el ENS
804 - Medidas de implantación del ENS
805 - Política de Seguridad de la Información
806 - Plan de Adecuación del ENS
807 - Criptología de empleo en el ENS
808 - Verificación del cumplimiento de las medidas en el ENS
809 - Declaración de Conformidad del ENS
810 - Creación de un CERT / CSIRT
811 - Interconexión en el ENS
812 - Seguridad en Entornos y Aplicaciones Web
813 - Componentes certificados en el ENS
814 - Seguridad en correo electrónico
815 - Métricas e Indicadores en el ENS
817 - Gestión de Ciberincidentes
818 - Herramientas de Seguridad en el ENS
820 - Protección contra Denegación de Servicio
821 - Ejemplos de Normas de Seguridad
822 - Procedimientos de Seguridad en el ENS
823 – Cloud Computing en el ENS
824 - Informe del Estado de Seguridad
825 – ENS & 27001
827 - Gestión y uso de dispositivos móviles
844 - Manual de usuario de INES
850A - Implantación del ENS en Windows 7 (cliente en dominio)
850B - Implementación del ENS en Windows 7 (cliente independiente)
851A - Implementación del ENS en Windows Server 2008 R (controlador de dominio y servidor miembro)
851B - Implementación del ENS en Windows Server 2008 R2 (servidor Independiente)
859 - Recolección y consolidación de eventos con Windows Server 2008 R2
860 - Seguridad en el Servicio Outlook Web App (OWA) de MS Exchange Server 2010
869 - Implementación de AppLocker en el ENS
870A - Implementación del ENS en Windows Server 2012 R2 (controlador de dominio y servidor miembro)
870B - Implementación del ENS en Windows Server 2012 R2 (servidor independiente)
MAGERIT v3 – Metodología de análisis y gestión de riesgos de los sistemas de información

Herramientas de ciberseguridad: Pilar , INÉS, CLARA, LUCÍA, CARMEN, …

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