CCN-CERT
centro criptológico nacional

X JORNADAS STIC CCN-CERT

2006 2016

DIEZ AÑOS FORTALECIENDO LA CIBERSEGURIDAD NACIONAL

Auditorías conjuntas ENS/LOPD en el MEYSS

CCN
Centro Criptológico Nacional

AELSI

Auditorías ENS y LOPD de Sistemas de Información

- Carlos Gómez Plaza, María José Lucas y Guillermo Mora
- Unidad de Calidad, Seguridad y Auditoría (SGTIC-MEYSS)
- sgtic-csa@meyss.es

Índice

1. Problemas a resolver
2. Objetivos de AELSI
3. Descripción de AELSI:
    - Los destinatarios y el modo de trabajo
    - Cuestionario 1
    - Cuestionario 2
4. De Excel a aplicación WEB
5. Los resultados a obtener

1. Problemas a resolver

- Ley Orgánica de Protección de Datos / Nuevo Reglamento Europeo.
- Esquema Nacional de Seguridad.
- Política de Seguridad del MEYSS.

2. Objetivos de AELSI

- Garantizar el cumplimiento del ENS y de la LOPD.
- Facilitar la realización de la auditoría bienal, a los responsables de los SI del ministerio.
- Impulsar el trabajo de mejora continua de los SI.
- Obtener resultados en un tiempo razonable con los recursos disponibles.

3. Descripción de AELSI

- Destinatarios:
  - 3 Roles de gestión
  - 4 Roles en unidades de soporte
  - Máximo de 141 medidas

- Modo de trabajo:
  - Fase 1 definir la Unidad
  - Fase 2 describir las medidas de seguridad
  - Fase 3 Resultados

Roles	Áreas	Número de preguntas
Unidad Responsable del S.I	Gestión	10
	Operativo	49
	Puesto de trabajo	9
		68

Roles	Áreas	Número de preguntas
Responsable Técnico SGTIC*	Sistemas	34
	Comunicaciones	14
	Aplicaciones	13
	Microinformática	12
		73

3. Descripción de AELSI – Fase 1

- El Responsable de la Unidad define los Sistemas de Información y ficheros con datos personales
- Con esos datos se genera el segundo cuestionario ajustado a sus requerimientos de seguridad.

Unidad XXXXX

Cuestionario 1 de Sistemas de Información y ficheros LOPD

Cumplimente las casillas azules cuando corresponda.

Toda la información incluida en estos documentos tiene carácter interno, de uso exclusivo de la Unidad

Unidad Responsable:	
Responsable de los S.I. de la Unidad:	
Ámbito del S.I.:	

Niveles de seguridad ENS del Sistema de Información (Ponga Sistemas de Información en todas las casillas necesarias).

	ENS						
Sistema de Información	Autenticidad	Confidencialidad	Integridad:	Disponibilidad	Trazabilidad	Principales elementos del S.I. (si se puede distinguir más de uno):	Descripción del Sistema de información.
Sistema de Información 1							
Sistema de Información 2							
Sistema de Información 3							

Niveles de seguridad de los ficheros afectados por la LOPD (Ponga "si" en todas las casillas necesarias).

Ficheros	Automatizado	No automatizado	Descripción del fichero.	Enlace al registro AEPD:
Fichero LOPD 1				
Fichero LOPD 2				
Fichero LOPD 3				
Fichero LOPD 4				

3. Descripción de AELSI – Fase 2

- Cada persona recibirá el cuestionario asociado a su rol.
- Definir el nivel de madurez (L0 a L5) de la medida, los procedimientos de trabajo y las evidencias de su ejecución.

Cuestionario 2 de evaluación / auditoría de los Sistemas de Información

Todas las medidas son obligatorias en alguno de sus Sistemas de Información o Ficheros LOPD, y se evalúan cada dos años como máximo
Cumplimente las casillas azules con una de las opciones que se indican junto con las evidencias y observaciones.

Rellenar este bloque **solo** en el caso de que la medida de seguridad aplicada en el SI o el Fichero indicado abajo, sea diferente a la indicada en el formulario principal (en azul). Si no se indica nada aquí abajo, se considera que la medida en azul se aplica a todos los SI y a todos los ficheros LOPD.

Responsable		Código	Medida de seguridad a verificar	Respuesta	Evidencias propuestas o equivalentes	Adjuntar Documento	Observaciones	SISTEMAS DE INFORMACIÓN EVALUADOS	FICHEROS LOPD EVALUADOS
					Documentos, procedimientos, informes…	Hechos, listados, fotografías, copias de pantalla…		Sistema de Información 1	Fichero LOPD 1
Resp. del S.I.	Gestión	P1	El Departamento dispone de su propia Política de Seguridad publicada en la sede electrónica y que cumple todos los requisitos de la legislación vigente. Nuestra Unidad, como parte del mismo, se encuentra bajo su paraguas.	L0 No se hace nada de este apartado o bien la medida no está completamente desplegada. No tenemos documentación.					
Resp. del S.I.	Gestión	P2	El responsable del S.I. vela por que todos los elementos que conforman el S.I. y el propio S.I. están categorizados tanto respecto a los datos que manejan (LOPD) como respecto al impacto que sobre la Organización tendría un incidente de seguridad (Esquema Nacional de Seguridad), indicándose siempre el correspondiente nivel de seguridad desde los dos puntos de vista	NO APLICA			Cuando se selecciona como respuesta "No aplica", hay que incluir obligatoriamente los motivos en el campo "Observaciones".		

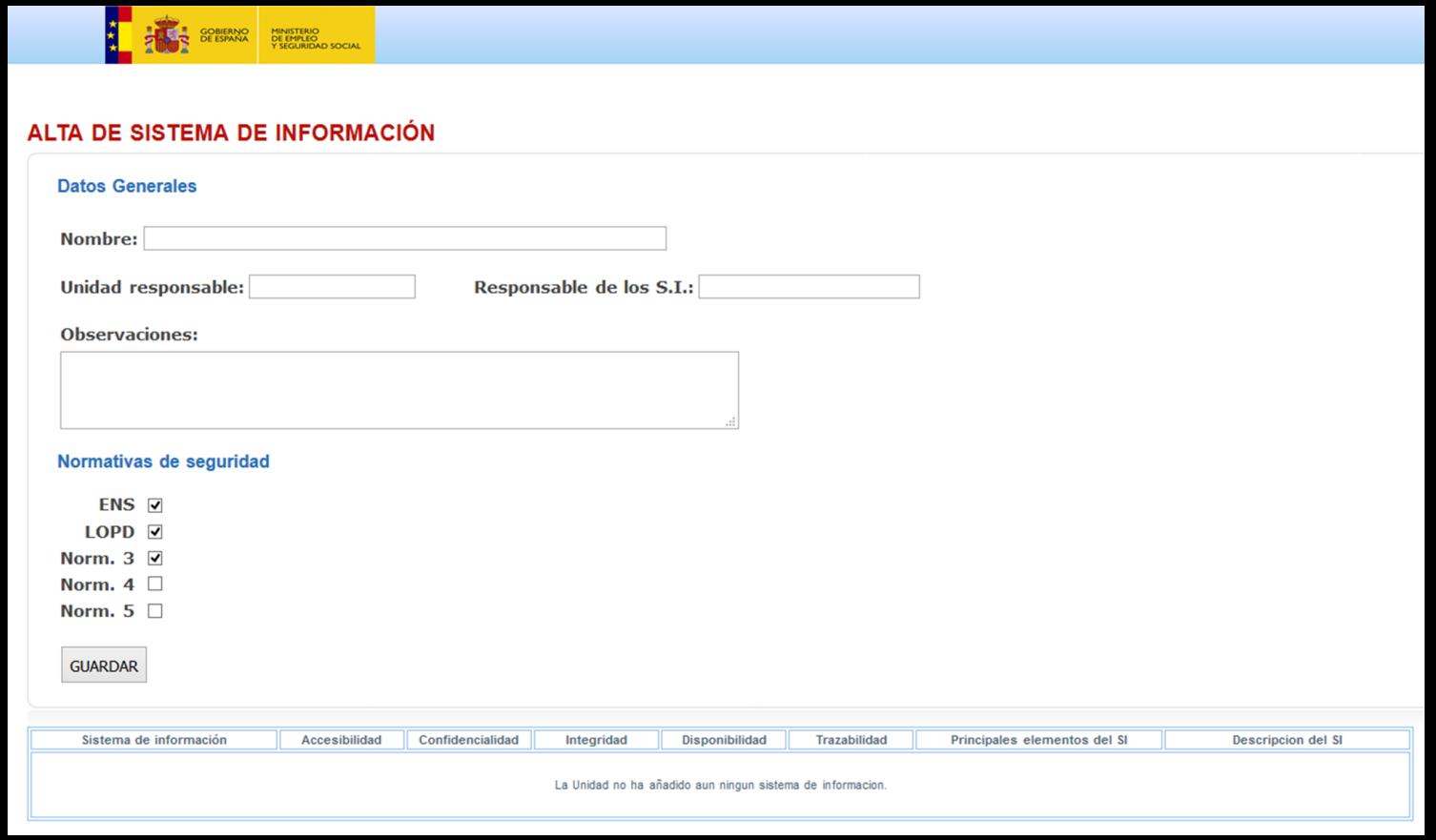
3. Descripción de AELSI – Fase 3

- Tras el análisis de los datos recabados, el sistema permite obtener con menos esfuerzo que una auditoría convencional:

1. La auditoría de cumplimiento exigida por el ENS y la LOPD.
2. El documento de seguridad requerido por la LOPD.
3. Las declaraciones de aplicabilidad ENS.
4. Cuadro de indicadores básico para hacer recomendaciones e iniciar procesos de mejora.

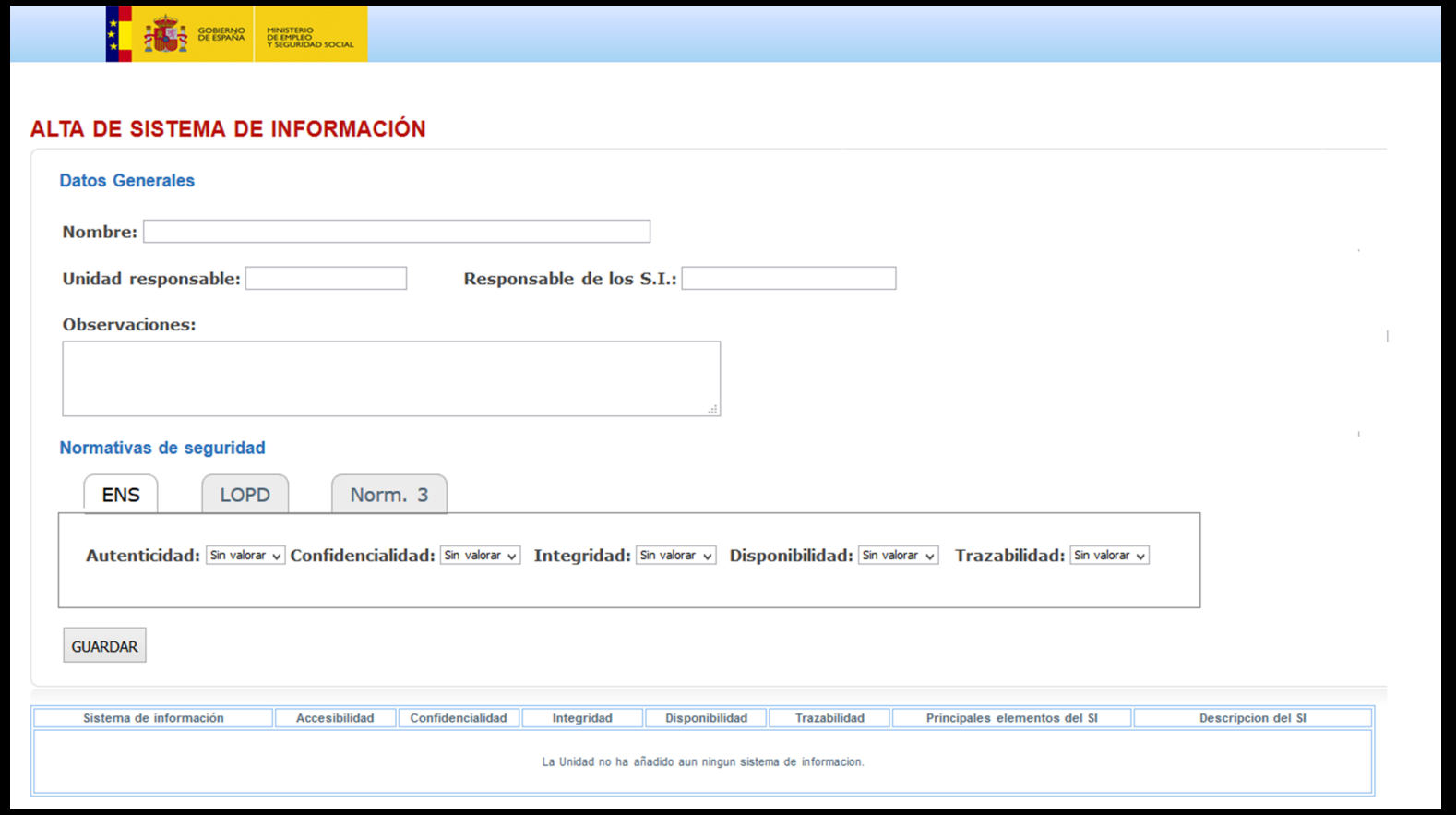
3. Descripción de AELSI – Web (1)

- Una forma más fácil de hacer auditorías y gestionarlas. Definición de un S.I.



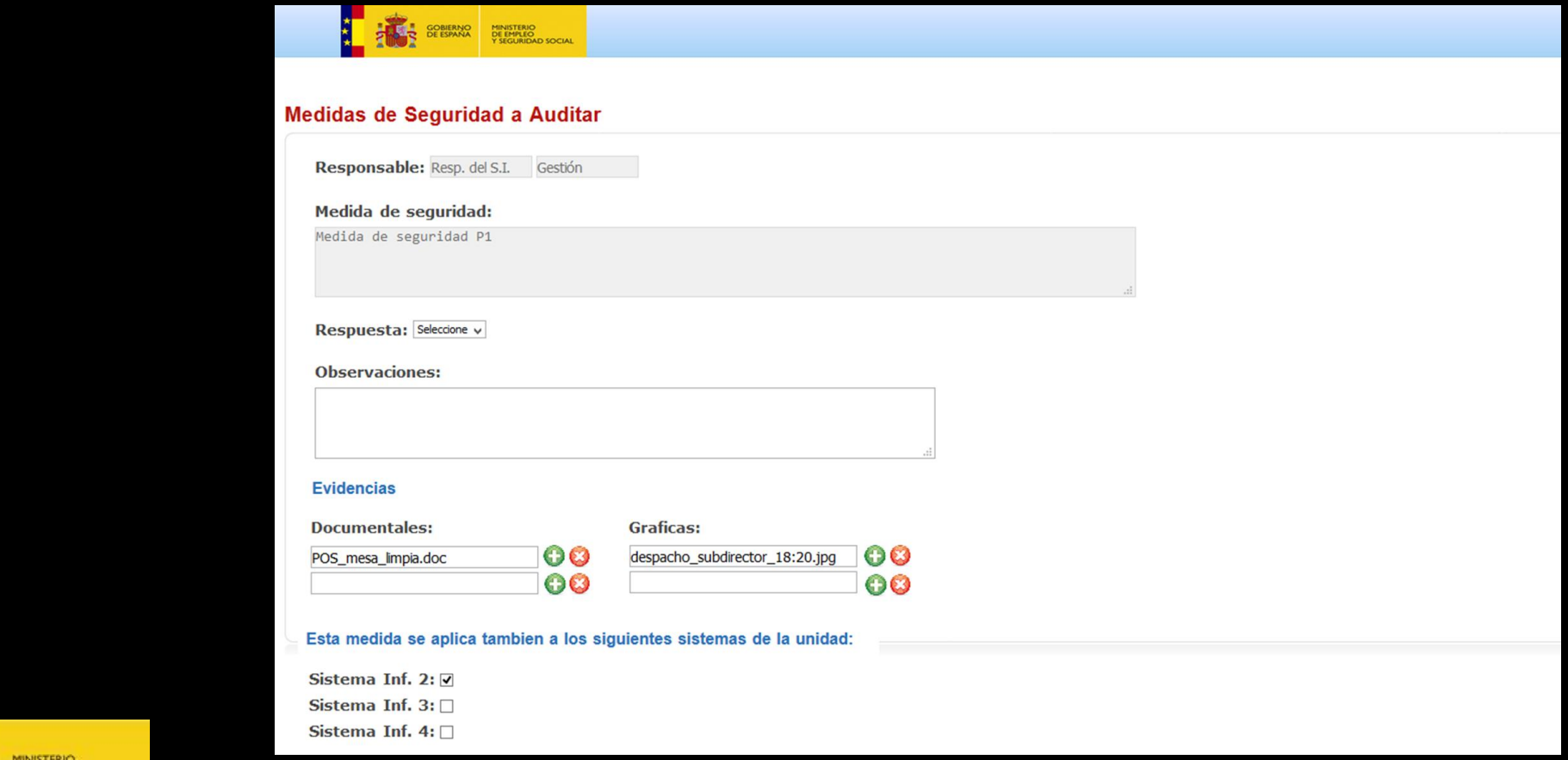
3. Descripción de AELSI – Web (2)

- Una forma más fácil de hacer auditorías y gestionarlas. Definición de un S.I.



3. Descripción de AELSI – Web (3)

- Una forma más fácil de hacer auditorías y gestionarlas. Definición de un S.I.



4. De Excel a aplicación WEB

- Aplicación más amigable:
  - Interacción de usuario ágil, amigable, comprensible.
  - En cualquier dispositivo: ordenador, portátil, tableta.
  - Cuadro de mando e indicadores: por unidad, tiempos, etc.
  - Generación de informes y certificados (cumplimiento normativo, auditoría, autoevaluación, ….).
- Proceso masivo de autoevaluación del resto de SSII ENS junto con sus ficheros con datos personales.

5. Resultados obtenidos hasta ahora

- 5 auditorías de los SSII ENS categoría media y LOPD nivel medio/alto de 4 Subdirecciones Generales.
- Buena disposición general a la realización de la auditoría.
- Niveles de madurez sobreestimados por aquellos que responden a los cuestionarios.

Muchas gracias por su atención

sgtic-csa@meyss.es