



Auditorías conjuntas ENS/LOPD en el MEYSS

DIEZ AÑOS FORTALECIENDO LA
CIBERSEGURIDAD 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).							
Sistema de Información	ENS					Principales elementos del S.I. (si se puede distinguir más de uno):	Descripción del Sistema de información.
	Autenticidad	Confidencialidad	Integridad:	Disponibilidad	Trazabilidad		
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.

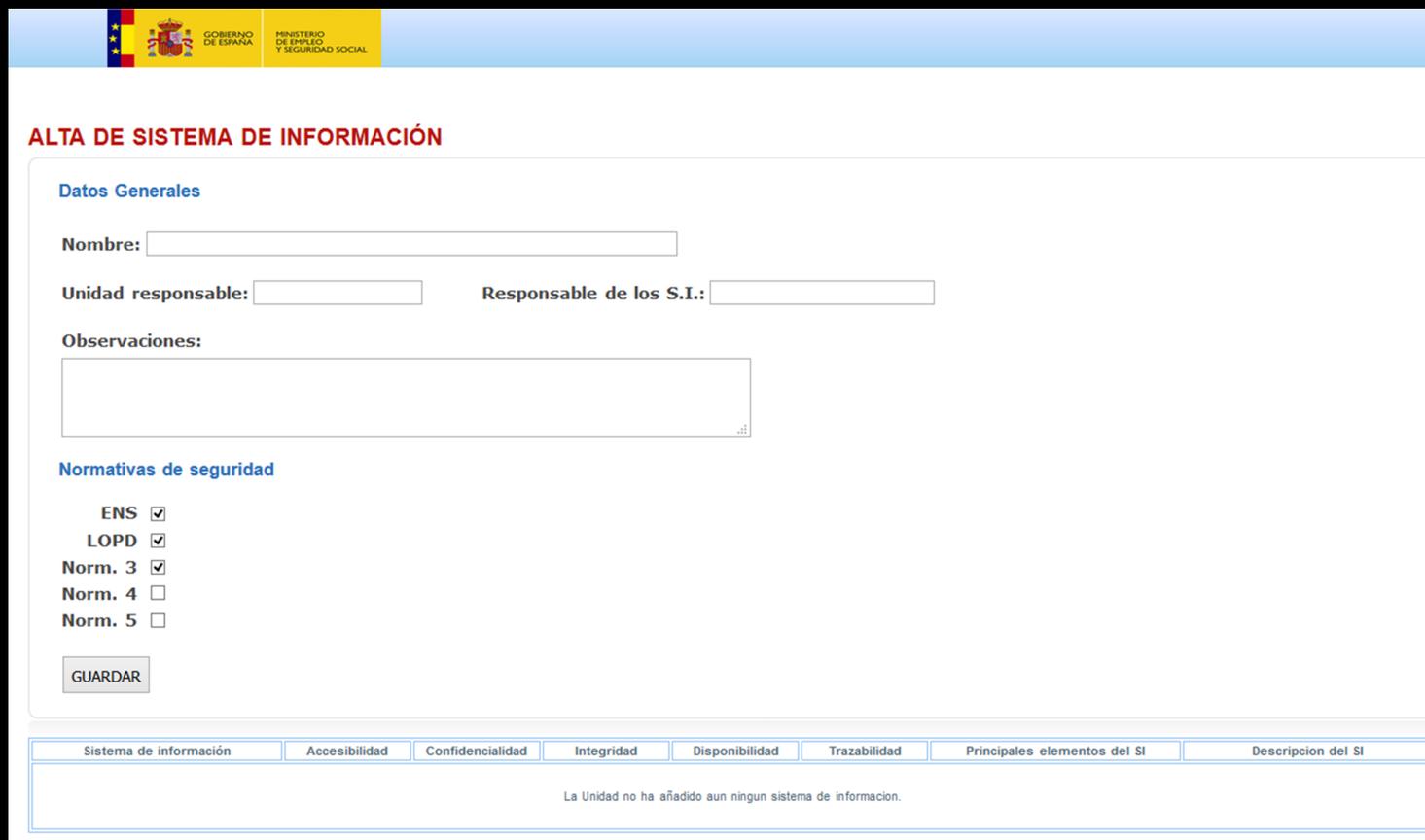
<p align="center">Cuestionario 2 de evaluación / auditoría de los Sistemas de Información</p> <p align="center">Todas las medidas son obligatorias en alguno de sus Sistemas de Información o Ficheros LOPD, y se evalúan cada dos años como máximo Cumplimente las casillas azules con una de las opciones que se indican junto con las evidencias y observaciones.</p>							<p>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.</p>	
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.



The screenshot shows the 'ALTA DE SISTEMA DE INFORMACIÓN' (System Registration) page. At the top, there are logos for the Spanish Government and the Ministry of Employment and Social Security. The main content area is titled 'ALTA DE SISTEMA DE INFORMACIÓN' and contains a form with the following sections:

- Datos Generales:** Includes input fields for 'Nombre:', 'Unidad responsable:', and 'Responsable de los S.I.:'. There is also a large text area for 'Observaciones:'.
- Normativas de seguridad:** A list of security norms with checkboxes:
 - ENS
 - LOPD
 - Norm. 3
 - Norm. 4
 - Norm. 5
- A 'GUARDAR' (Save) button is located below the security norms section.

At the bottom of the form, there is a navigation bar with tabs for: 'Sistema de información', 'Accesibilidad', 'Confidencialidad', 'Integridad', 'Disponibilidad', 'Trazabilidad', 'Principales elementos del SI', and 'Descripcion del SI'. Below the navigation bar, a message states: 'La Unidad no ha añadido aun ningun sistema de informacion.'

3. Descripción de AELSI – Web (2)

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

GOBIERNO DE ESPAÑA
MINISTERIO DE EMPLEO Y SEGURIDAD SOCIAL

ALTA DE SISTEMA DE INFORMACIÓN

Datos Generales

Nombre:

Unidad responsable: Responsable de los S.I.:

Observaciones:

Normativas de seguridad

ENS LOPD Norm. 3

Autenticidad: Confidencialidad: Integridad: Disponibilidad: Trazabilidad:

GUARDAR

Sistema de información	Accesibilidad	Confidencialidad	Integridad	Disponibilidad	Trazabilidad	Principales elementos del SI	Descripcion del SI
La Unidad no ha añadido aun ningun sistema de informacion.							

3. Descripción de AELSI – Web (3)

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

The screenshot displays the 'Medidas de Seguridad a Auditar' section of the AELSI web application. The interface includes the following elements:

- Header:** Logos for the Spanish Government (GOBIERNO DE ESPAÑA) and the Ministry of Employment and Social Security (MINISTERIO DE EMPLEO Y SEGURIDAD SOCIAL).
- Title:** 'Medidas de Seguridad a Auditar'.
- Responsible:** A dropdown menu with 'Resp. del S.I.' and 'Gestión' as options.
- Medida de seguridad:** A text area containing 'Medida de seguridad P1'.
- Respuesta:** A dropdown menu with 'Seleccione' as the current selection.
- Observaciones:** A large empty text area for notes.
- Evidencias:** A section with two columns:
 - Documentales:** A list of document names with '+' and '-' icons. The first entry is 'POS_mesa_limpia.doc'.
 - Graficas:** A list of graphic names with '+' and '-' icons. The first entry is 'despacho_subdirector_18:20.jpg'.
- Esta medida se aplica tambien a los siguientes sistemas de la unidad:** A section with three checkboxes:
 - Sistema Inf. 2:
 - Sistema Inf. 3:
 - Sistema Inf. 4:

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