NUEVOS INSTRUMENTOS PARA AUDITAR EL ENS

MEYSS

08 febrero 2017

GOBIERNO DE ESPAÑA
MINISTERIO DE EMPLEO Y SEGURIDAD SOCIAL

AELSI
Auditorías ENS 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

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

2.- OBJETIVOS DE LA APLICACIÓN (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, para involucrarlos en la gestión de la seguridad y de la protección de datos.
- Impulsar el trabajo de mejora continua de los SI
- Nuevos objetivos
- Obtener resultados en un tiempo razonable con los recursos disponibles.

3. DESCRIPCIÓN

- Destinatarios:
  - 141/154 preguntas.
  - 3 Roles posibles para responder en el cliente (responsable del SI)
  - 4 Roles en unidades de soporte
- Modo de trabajo:
  - 2 cuestionarios
  - 1.Cuestión, 2. respuesta con elección, 3. Se adjuntan evidencias

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

* En el caso de que la propia Unidad realice tareas no contempladas por la SGTIC, deberá incorporarlo en observaciones.

3.- CUESTIONARIO 1

- Cumplimentado por el Responsable del Sistema de Información.
- Necesario para generar el Cuestionario 2 ajustado a los SSII y ficheros LOPD de su Responsable

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.- CUESTIONARIO 2

- Cumplimentado por el Responsable del SI junto con su equipo según los roles que desempeñan.
- Se solicita su nivel de madurez (de L0 a L5), procedimientos de trabajo y 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 Politica 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 y,cuando esto es posible, el nivel global del S.I.. e implanta las medidas de seguridad correspondientes.	NO APLICA			Cuando se selecciona como respuesta "No aplica", hay que incluir obligatoriamente los motivos en el campo "Observaciones".		
Resp. del S.I.	Gestión	P5	La Unidad tiene contratos o acuerdos con terceros para ciertos servicios que no tienen que ver con el tratamiento de datos (por ejemplo limpieza de los locales) que incluyen una cláusula de confidencialidad respecto de los datos que pudieran conocer al desarrollar el servicio y cláusula de no acceso a los datos.	L4 Se hace siempre, está documentado y se miden los resultados. Se generan indicadores del cumplimiento.					

4.- LOS RESULTADOS QUE SE OBTIENEN

- El sistema permite obtener con menos esfuerzo que una auditoría convencional:

1. La auditoría de cumplimiento exigida por el ENS y la LOPD.
2. La documentación de seguridad requerida por la LOPD.
3. Las declaraciones de aplicabilidad ENS pertinentes.
4. Comparación del cumplimiento legal con los objetivos de la organización.
5. Cuadro de indicadores básico para hacer recomendaciones e iniciar procesos de mejora.

4.- RESULTADOS OBTENIDOS

- 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.

5.- DE EXCEL A APLICACIÓN WEB

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

Muchas gracias por su atención

sgtic-csa@meyss.es