GOBIERNO DE ESPAÑA
MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS

CCN
CENTRO CRIPTOLÓGICO NACIONAL

ESQUEMA NACIONAL DE SEGURIDAD

INSTRUCCIONES PARA SEGUIMIENTO DEL PROGRESO DE IMPLANTACIÓN

ens
Esquema Nacional de Seguridad

ENERO 2013

ÍNDICE

1. INTRODUCCIÓN

1. El Esquema Nacional de Seguridad, en su Disposición Transitoria sobre Adecuación de los Sistema, dice que:

   1. Los sistemas existentes a la entrada en vigor del presente real decreto se adecuarán al Esquema Nacional de Seguridad de forma que permitan el cumplimiento de lo establecido en la disposición final tercera de la Ley 11/2007, de 22 de junio. Los nuevos sistemas aplicarán lo establecido en el presente real decreto desde su concepción.
   2. Si a los doce meses de la entrada en vigor del Esquema Nacional de Seguridad hubiera circunstancias que impidan la plena aplicación de lo exigido en el mismo, se dispondrá de un plan de adecuación que marque los plazos de ejecución los cuales, en ningún caso, serán superiores a 48 meses desde la entrada en vigor. El plan indicado en el párrafo anterior será elaborado con la antelación suficiente y aprobado por los órganos superiores competentes.

2. Este documento proporciona orientación para cumplimentar un cuestionario que facilite el seguimiento mensual del progreso de la adecuación al Esquema Nacional de Seguridad (ENS).
3. Dicho cuestionario se cumplimenta a través de una aplicación que se encuentra disponible en:

- Para ejecutar en HTML: https://www.ccn-cert.cni.es/publico/herramientas/ens.html
- Para ejecutar en windows: https://www.ccn-cert.cni.es/publico/herramientas/ens-windows.exe
- para ejecutar en cualquier sistema operativo: https://www.ccn-cert.cni.es/publico/herramientas/ENS2_signed.jar

2. PASOS

4. Cada mes:

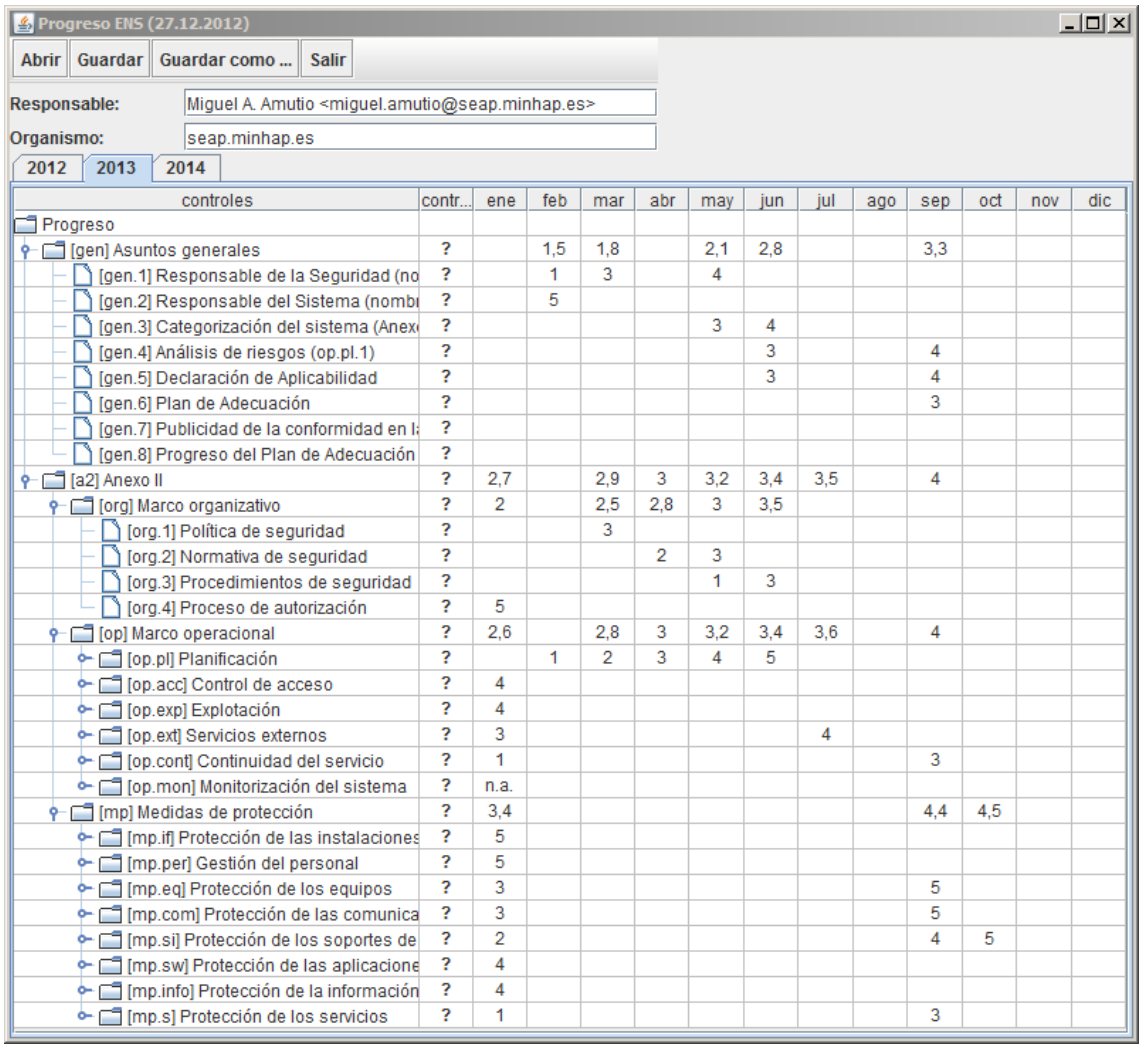
- Abra la aplicación
- Rellene la columna del mes actual
- Cierre guardando los datos en un fichero
- Envíe el fichero a la dirección de correo electrónico ens.minhap@correo.gob.es

5. Todas las preguntas se responden con un dato en la escala 1-5, donde

   1 = no hay nada hecho al respecto
   5 = tarea completada
   n.a. = no aplica.

6. Las preguntas están agrupadas jerárquicamente, y en las agrupaciones se toma como valor el valor medio de las valoraciones de los componentes del agregado.

3. INTERFAZ



controles	contr...	ene	feb	mar	abr	may	jun	jul	ago	sep	oct	nov	dic
Progreso													
[gen] Asuntos generales	?		1,5	1,8		2,1	2,8			3,3			
[gen.1] Responsable de la Seguridad (no	?		1	3		4							
[gen.2] Responsable del Sistema (nombi	?		5										
[gen.3] Categorización del sistema (Anex	?					3	4						
[gen.4] Análisis de riesgos (op.pl.1)	?						3			4			
[gen.5] Declaración de Aplicabilidad	?						3			4			
[gen.6] Plan de Adecuación	?									3			
[gen.7] Publicidad de la conformidad en l	?												
[gen.8] Progreso del Plan de Adecuación	?												
[a2] Anexo II	?	2,7		2,9	3	3,2	3,4	3,5		4			
[org] Marco organizativo	?	2		2,5	2,8	3	3,5						
[org.1] Política de seguridad	?			3									
[org.2] Normativa de seguridad	?				2	3							
[org.3] Procedimientos de seguridad	?					1	3						
[org.4] Proceso de autorización	?	5											
[op] Marco operacional	?	2,6		2,8	3	3,2	3,4	3,6		4			
[op.pl] Planificación	?		1	2	3	4	5						
[op.acc] Control de acceso	?	4											
[op.exp] Explotación	?	4											
[op.ext] Servicios externos	?	3						4					
[op.cont] Continuidad del servicio	?	1								3			
[op.mon] Monitorización del sistema	?	n.a.											
[mp] Medidas de protección	?	3,4								4,4	4,5		
[mp.if] Protección de las instalaciones	?	5											
[mp.per] Gestión del personal	?	5											
[mp.eq] Protección de los equipos	?	3								5			
[mp.com] Protección de las comunica	?	3								5			
[mp.si] Protección de los soportes de	?	2								4	5		
[mp.sw] Protección de las aplicacione	?	4											
[mp.info] Protección de la información	?	4											
[mp.s] Protección de los servicios	?	1								3			

Abrir	para cargar los datos de un fichero XML; sirve para retomar datos de un reporte anterior
Guardar	para grabar los datos en el fichero XML
Guardar como …	para grabar los datos en un nuevo fichero XML
Salir	guardar y terminar
Responsable	nombre del responsable de la seguridad
Organismo	identificación del organismo; normalmente basta reflejar el dominio de la dirección email del organismo

4. PREGUNTAS DE CARÁCTER GENERAL

Nombramiento del responsable de la seguridad Ver art. 10.	1. no se han definido las funciones 2. hay una definición informal de las funciones 3. hay una definición consensuada de las funciones, pero no están aprobadas ni se ha nombrado a la persona 4. hay una definición formal de las funciones y hay una persona actuando como tal aunque sin nombramiento formal 5. las funciones están aprobadas formalmente y hay una persona nombrada para ejercerlas
Nombramiento del responsable del sistema Ver art. 10.	
Categorización del sistema Arts. 43 y 44. Anexo I.	1. no se han definido los criterios de valoración 2. existe una definición informal de los criterios y se ha aplicado de forma voluntarista 3. hay una definición consensuada de los criterios y se ha aplicado a una fracción importante de los sistemas 4. hay una definición formal de los criterios y se ha aplicado sistemáticamente a todos los sistemas 5. los criterios están aprobados formalmente y la categorización de los sistemas está aprobada por el órgano competente según política
Análisis de riesgos Arts. 6 y 13. Anexo II – [op.pl.1]	1. no se ha iniciado el análisis de riesgos de los sistemas 2. se ha iniciado el análisis pero aún es informal 3. se ha realizado el análisis pero no se han evaluado los resultados 4. se ha realizado el análisis y presentado los resultados para aprobación 5. se han aprobado las conclusiones del análisis de riesgos
Declaración de aplicabilidad Anexo II Selección de medidas de seguridad	1. no se ha calculado el conjunto de medidas de aplicación 2. se ha iniciado el proceso de determinación de las medidas que son de aplicación 3. existe una estimación informal del conjunto de medidas 4. se ha preparado una declaración completa y está pendiente de aprobación 5. se ha aprobado formalmente la declaración

Plan de adecuación Disposición transitoria única. Adecuación de sistemas.	1. no existe un plan de adecuación 2. se ha iniciado la preparación de un plan de adecuación 3. existe un borrador muy completo que cubre todas las tareas a ejecutar 4. existe una propuesta formal de plan de adecuación, pendiente de aprobación y dotación económica 5. el plan de adecuación está aprobado y dotado de recursos para su ejecución
Publicidad de la conformidad en la sede electrónica Artículo 41	1. No se ha publicado 5. Se ha publicado en la sede electrónica la declaración de conformidad y distintivo de seguridad

Progreso del plan de adecuación Disposición transitoria única. Adecuación de sistemas.	1. no se ha iniciado la ejecución del plan 2. el plan avanza pero con un retraso superior al 50% 3. el plan avanza pero con un retraso entre el 30% y el 50% 4. el plan avanza pero con un retraso entre el 10% y el 30% 5. el plan avanza con una desviación menor del 10% respecto del plan previsto La desviación se medirá en términos de esfuerzo (horas-hombre) $\frac{\text{planificado} - \text{ejecutado}}{\text{esfuerzo total}}$

5. ANEXO II

5.1. [org] Marco organizativo

[org.1] Política de seguridad Ver artículos 1 y 11.	1. no existe 2. se ha empezado a elaborar 3. existe un acuerdo informal consensuado sobre el contenido de la política 4. está elaborada pero pendiente de aprobar 5. está aprobada formalmente y publicada
[org.2] Normativa de seguridad Ver art. 14.3.	1. hay menos de un 10% de normas elaboradas sobre el total previsto 2. hay alrededor de 1/3 de normas elaboradas 3. hay alrededor de 1/2 de normas elaboradas 4. hay alrededor de 2/3 de normas elaboradas 5. hay más de un 90% de normas elaboradas, aprobadas y publicadas

[org.3] Procedimiento de seguridad POS – Procedimientos Operativos de Seguridad	1. menos de un 10% de las actividades rutinarias está procedimentado 2. hay alrededor de 1/3 de las actividades rutinarias está procedimentado formalmente 3. hay alrededor de 1/2 de las actividades rutinarias está procedimentado formalmente 4. hay alrededor de 2/3 de las actividades rutinarias está procedimentado formalmente 5. hay más de un 90% de las actividades rutinarias está procedimentado formalmente
[org.4] Proceso de autorización	porcentaje de cumplimiento de lo exigido en el Anexo II para la categoría del sistema

5.2. [op] Marco operacional

[op.pl] Planificación	porcentaje de cumplimiento de lo exigido en el Anexo II para la categoría del sistema
[op.acc] Control de acceso	
[op.exp] Explotación	
[op.ext] Servicios externos	
[op.cont] Continuidad del servicio	
[op.mon] Monitorización del sistema	

5.3. [mp] Medidas de protección

[mp.if] Protección de las instalaciones e infraestructuras	porcentaje de cumplimiento de lo exigido en el Anexo II para la categoría del sistema
[mp.per] Gestión del personal	
[mp.eq] Protección de los equipos	
[mp.com] Protección de las comunicaciones	
[mp.si] Protección de los soportes de información	
[mp.sw] Protección de las aplicaciones informáticas	
[mp.info] Protección de la información	
[mp.s] Protección de los servicios	

5.4. Porcentaje de cumplimiento

nivel	porcentaje
1	< 10%
2	10% - 40%
3	40% - 60%
4	60% - 90%
5	> 90%