

Edita:



© Centro Criptológico Nacional, 2019

NIPO: 083-19-171-X

Fecha de Edición: junio de 2019

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

PRÓLOGO

El uso masivo de las tecnologías de la información y las telecomunicaciones (TIC), en todos los ámbitos de la sociedad, ha creado un nuevo espacio, el ciberespacio, donde se producirán conflictos y agresiones, y donde existen ciberamenazas que atentarán contra la seguridad nacional, el estado de derecho, la prosperidad económica, el estado de bienestar y el normal funcionamiento de la sociedad y de las administraciones públicas.

La Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia (CNI), encomienda al Centro Nacional de Inteligencia el ejercicio de las funciones relativas a la seguridad de las tecnologías de la información en su artículo 4.e), y de protección de la información clasificada en su artículo 4.f), a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional (CCN) en su artículo 9.2.f).

Partiendo del conocimiento y la experiencia del CNI sobre amenazas y vulnerabilidades en materia de riesgos emergentes, el Centro realiza, a través de su Centro Criptológico Nacional, regulado por el Real Decreto 421/2004, de 12 de marzo, diversas actividades directamente relacionadas con la seguridad de las TIC, orientadas a la formación de personal experto, a la aplicación de políticas y procedimientos de seguridad, y al empleo de tecnologías de seguridad adecuadas.

El 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, en adelante), al que se refiere el apartado segundo del artículo 156 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, establece la política de seguridad en la utilización de medios electrónicos que permita una protección adecuada de la información.

Precisamente el Real Decreto 3/2010 de 8 de Enero, actualizado por el Real Decreto 951/2015, de 23 de octubre, fija los principios básicos y requisitos mínimos así como las medidas de protección a implantar en los sistemas de la Administración, y promueve la elaboración y difusión de guías de seguridad de las tecnologías de la información y las comunicaciones (STIC) por parte de CCN para facilitar un mejor cumplimiento de dichos requisitos mínimos.

En definitiva, la serie de documentos CCN-STIC se elabora para dar cumplimiento a los cometidos del Centro Criptológico Nacional y a lo reflejado en el Esquema Nacional de Seguridad, conscientes de la importancia que tiene el establecimiento de un marco de referencia en esta materia que sirva de apoyo para que el personal de la Administración lleve a cabo su difícil, y en ocasiones, ingrata tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

Junio de 2019

A handwritten signature in blue ink, appearing to read 'Felix Sanz Roldan', with a horizontal line underneath.

Félix Sanz Roldán
Secretario de Estado
Director del Centro Criptológico Nacional

ÍNDICE

FIGURAS	4
1. INTRODUCCIÓN	6
2. OBJETO	6
3. ALCANCE.....	6
4. REQUISITOS GENERALES	6
5. MICRO PILAR. HERRAMIENTA PARA EL ANÁLISIS DE RIESGOS.....	7
5.1. INTRODUCCIÓN	7
5.2. LA HERRAMIENTA PILAR	7
5.3. ANÁLISIS DE RIESGOS CON MICRO PILAR	8
5.3.1. INICIO DE LA APLICACIÓN.....	8
5.3.2. DESCRIPCIÓN DEL PROYECTO.....	10
5.3.3. ACTIVOS Y VALORACIÓN	11
5.3.4. ESQUEMA NACIONAL DE SEGURIDAD.....	15
5.3.5. REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS.....	20
5.3.6. RIESGOS	21
5.3.7. GESTIONAR RIESGOS CON ENS.....	22
5.3.8. GESTIONAR RIESGOS CON RGPD.....	23
5.3.9. INFORMES.....	24
5.3.10. FINALIZAR Y SALIR.....	35
6. PLAN DE TRATAMIENTO DE RIESGOS	36
7. ANEXO A. REFERENCIAS	36

FIGURAS

Figura 1 Icono de PILAR	9
Figura 2 Ejecutable de PILAR	9
Figura 3 Ventanas iniciales de PILAR	9
Figura 4 Opciones iniciales	9
Figura 5 Opción "Guardar"	10
Figura 6 Buscar, Seleccionar y Abrir fichero PILAR.....	11
Figura 7 Activos predefinidos	11
Figura 8 Ventana con los activos seleccionados (I)	13
Figura 9 Ventana con los activos seleccionados (y II)	13
Figura 10 Clases de Activos de la infraestructura	14
Figura 11 Servicios "somos clientes de..."	14
Figura 12 Ventana inicial del ENS	15
Figura 13 Columna "dudas"	16
Figura 14 Ventana "comentario"	16
Figura 15 Documentar [objetivo]	17
Figura 16 Valorar medida/pregunta.....	19
Figura 17 Opción guardar como fichero CSV.....	19
Figura 18 Medidas de protección adicionales.....	20

Figura 19 Pantalla de valoración del RGPD	20
Figura 20 Top 10 resumen (riesgo).....	21
Figura 21 Gestionar riesgos con ENS	22
Figura 22 Sugerencias de mejora para ENS	23
Figura 23 Informes.....	24
Figura 24 Seleccionar situación del análisis	24
Figura 25 Informe de Análisis de riesgos	25
Figura 26 Índice del documento de Análisis de Riesgos.....	25
Figura 27 Informe de Declaración de Aplicabilidad	26
Figura 28 Índice del documento de Declaración de Aplicabilidad	27
Figura 29 Seleccionar situación de la valoración.....	27
Figura 30 Informe de Valoración ENS.....	28
Figura 31 Índice del documento de Valoración ENS	28
Figura 32 Informe de Cumplimiento del ENS	29
Figura 33 Índice del documento de Cumplimiento ENS.....	30
Figura 34 Informe de Cumplimiento del RGPD	31
Figura 35 Índice del documento Declaración RGPD.....	32
Figura 36 Seleccionar objetivo	33
Figura 37 Informe de Recomendaciones.....	33
Figura 38 Índice del documento Recomendaciones	33
Figura 39 Seleccionar ámbito	34
Figura 40 Contenido Informe Inés.....	35
Figura 41 Salvar y salir de Pilar	35

1. INTRODUCCIÓN

1. La necesidad, por parte de las Entidades Locales, de cumplir con las normativas y reglamentos (ENS y RGPD) en materia de Seguridad de la Información y la Protección de Datos de Carácter Personal, han motivado que el CCN aborde el desarrollo de guías y herramientas que ayuden a las Entidades Locales a la consecución de dicho cumplimiento.
2. Con el fin de facilitar este cumplimiento normativo y reglamentario, en esta guía se plantea el uso de la herramienta micro PILAR para realizar el Análisis de Riesgos, pieza clave para conseguirlo.
3. La funcionalidad ofrecida por la herramienta micro Pilar permite la elaboración de informes de diverso tipo que pueden ayudar al definición y desarrollo de las tareas por realizar en las Entidades Locales para su cumplimiento con el ENS y el RGPD, incluso para la presentación del preceptivo Informe INES en la sede electrónica del CCN.

2. OBJETO

4. El objeto de este documento de “Guía para el Análisis de Riesgos con PILAR del ENS y RGPD para Entidades Locales” es desarrollar el proceso de Análisis y Gestión de Riesgos utilizando la herramienta Micro PILAR paso a paso, de manera que sirva de ayuda guiada para las personas responsables de realizar este análisis de riesgos en una Entidad Local para el cumplimiento del Esquema Nacional de Seguridad (ENS) y el Reglamento General de Protección de Datos (RGPD).

3. ALCANCE

5. Esta guía permite realizar el Análisis de Riesgos en base al Esquema Nacional de Seguridad (ENS) y al Reglamento General de Protección de Datos (RGPD) para Entidades Locales de manera independiente a su localización geográfica o tamaño.

4. REQUISITOS GENERALES

6. Debe disponer de la herramienta micro PILAR en versión 7.3 o superior instalada y con la licencia adecuada para su funcionamiento.
7. Debe disponer de un inventario de los servicios, datos, tratamientos de datos de carácter personal e infraestructura tecnológica actualizado de la institución.

5. MICRO PILAR. HERRAMIENTA PARA EL ANÁLISIS DE RIESGOS

5.1. Introducción

8. PILAR es una herramienta que implementa la metodología MAGERIT de análisis y gestión de riesgos, desarrollada por el Centro Criptológico Nacional (CCN) y de amplia utilización en la administración pública española.
9. Se puede descargar del Portal del CCN-CERT en: <https://www.ccn-cert.cni.es/herramientas-de-ciberseguridad/ear-pilar.html>
10. O bien desde: <http://www.ar-tools.com/es/index.html>
11. Los organismos de la administración pública española pueden solicitar una licencia libre de cargos al Centro Criptológico Nacional; para ello, debe dirigir la solicitud a la dirección de correo electrónico del Centro Criptológico Nacional: ccn@cni.es.
12. Para conocer el estado de seguridad de un sistema, se necesita modelarlo, identificando y valorando sus activos, e identificando y valorando las amenazas sobre dichos activos. Así, podemos estimar el riesgo a que el sistema está sujeto.
13. El riesgo se puede mitigar por medio de las salvaguardas o contramedidas desplegadas para proteger el sistema. Es inusual que las salvaguardas reduzcan el riesgo a cero; es más frecuente que siga existiendo un riesgo residual que la organización o bien pueda aceptar, o bien intente reducir más, estableciendo un plan de seguridad orientado a llevar el riesgo a niveles aceptables.
14. El análisis de riesgos proporciona información para las actividades de tratamiento de los riesgos. Estas actividades se ejercen una vez y otra vez, incorporando nuevos activos, nuevas amenazas, nuevas vulnerabilidades, y nuevas salvaguardas.
15. PILAR es un conjunto de herramientas que permite realizar un análisis de riesgos, sobre las diversas dimensiones de seguridad (confidencialidad, integridad, disponibilidad, autenticidad, trazabilidad y protección de datos)

5.2. La herramienta PILAR

16. Micro PILAR (en adelante PILAR) conjuga los activos de un sistema con las amenazas posibles, calcula los riesgos y permite incorporar medidas para reducir el riesgo a valores residuales aceptables. Esto permite fundamentar la confianza en el sistema.
17. Las organizaciones públicas dependen de forma creciente de las tecnologías de la información y comunicaciones (TIC) para la consecución de sus objetivos de servicio. La razón de ser de PILAR está directamente relacionada con la generalización del uso de los medios electrónicos, informáticos y telemáticos, que supone unos beneficios evidentes para los usuarios; pero también da lugar a ciertos riesgos que deben minimizarse con medidas de seguridad que generen confianza en el uso de tales medios.
18. Los objetivos perseguidos son:

- Realizar el análisis de riesgos según la metodología Magerit.
 - Diseño del plan de mejora de la seguridad.
19. PILAR consiste en una aplicación informática que compila los activos del sistema, sus relaciones de interdependencia y su valor para la organización. Conocido el sistema, permite introducir las amenazas posibles en los aspectos de disponibilidad, integridad, confidencialidad, autenticidad, trazabilidad y protección de datos, para derivar los riesgos potenciales sobre el sistema.
20. Una vez conocidos los riesgos, se pueden determinar una serie de medidas y estimar el riesgo residual. El tratamiento del riesgo es un proceso continuo y recurrente en el que el sistema de protección se va mejorando regularmente para afrontar nuevos riesgos y aumentar la confianza que el sistema merece para los responsables y los usuarios.
21. Los resultados que se obtienen con el uso de esta herramienta son los siguientes:
- Obtener el Análisis de Riesgos para el Esquema Nacional de Seguridad y el Reglamento General de Protección de Datos.
 - Obtener la Declaración de Aplicabilidad del ENS para los sistemas de información.
 - Obtener la valoración del sistema (o sistemas) en base al ENS.
 - Obtener el grado de cumplimiento respecto al ENS.
 - Obtener el grado de cumplimiento respecto al RGPD.
 - Obtener recomendaciones para la mejora del grado de cumplimiento al ENS y el RGPD.
 - Obtener el Informe Inés para enviarlo al CCN.
22. Las ventajas que aportan la utilización de la herramienta:
- Conocer los riesgos a fin de poder tratarlos.
 - Conocer el grado de cumplimiento de diferentes perfiles de seguridad: protección de datos de carácter personal siguiendo el Reglamento de la UE y Esquema Nacional de Seguridad.
 - Implementar la metodología Magerit.

5.3. Análisis de riesgos con Micro PILAR

5.3.1. Inicio de la aplicación

23. Una vez instalada la herramienta PILAR, iniciamos la ejecución de PILAR, bien a través del icono del escritorio:



Figura 1 Icono de PILAR

24. O bien desde el ejecutable situado en el directorio principal de la instalación de PILAR:

Nombre	Fecha de modifica...	Tipo	Tamaño
ens	14/02/2019 8:35	Carpeta de archivos	
exs_ens	14/02/2019 8:35	Carpeta de archivos	
help_micro_es	14/02/2019 8:34	Carpeta de archivos	
info_es	14/02/2019 8:35	Carpeta de archivos	
lics	14/02/2019 8:36	Carpeta de archivos	
micro_eell	15/02/2019 17:13	Carpeta de archivos	
rd1720	14/02/2019 8:35	Carpeta de archivos	
util	14/02/2019 8:34	Carpeta de archivos	
hgr.gif	11/02/2019 9:37	Archivo GIF	1 KB
LICENSE_es.html	11/02/2019 9:38	Documento HTML	5 KB
MICRO_eell.car	18/02/2019 8:40	Archivo CAR	3 KB
pilar.ico	11/02/2019 9:37	Archivo ICO	4 KB
pilarmicro.exe	13/02/2019 21:16	Aplicación	2.519 KB
README_Micro_es.txt	11/02/2019 9:37	Documento de tex...	1 KB
unins000.dat	14/02/2019 8:35	Archivo DAT	129 KB
unins000.exe	14/02/2019 8:34	Aplicación	1.179 KB

Figura 2 Ejecutable de PILAR

25. En ambos casos aparecerán las ventanas iniciales de PILAR:

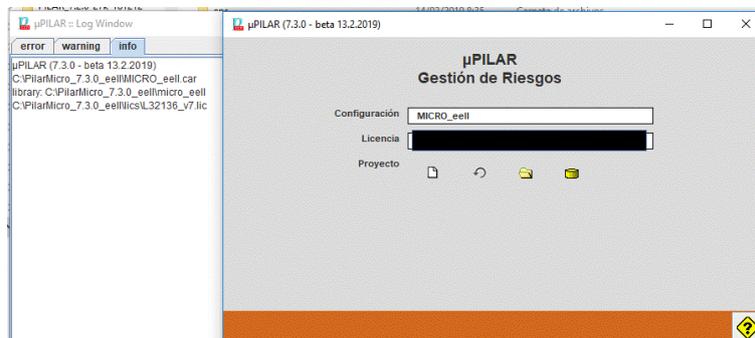


Figura 3 Ventanas iniciales de PILAR

26. Al ser la primera vez que ejecutamos PILAR se debe crear el fichero PILAR. Si ya lo creó previamente entonces puede utilizar la opción “recientes” o “abrir” cargar el fichero PILAR creado anteriormente para continuar con el Análisis de Riesgos. Esto se realiza desde la opción del menú “Proyecto”:

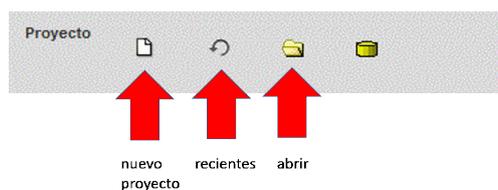


Figura 4 Opciones iniciales

27. Supongamos que es la primera vez que utiliza la herramienta PILAR y quiere iniciar el Análisis y Gestión de Riesgos (en adelante AGR) de su organismo.
28. Seleccionamos la opción de nuevo proyecto.

5.3.2. Descripción del proyecto

29. Aparecerá la ventana para la descripción del proyecto y sus características principales.
30. Se recomienda completar la información descriptiva del proyecto y sus principales características con el fin de documentar adecuadamente su ejecución:
31. Utilice la opción “Guardar” para guardar el fichero PILAR:

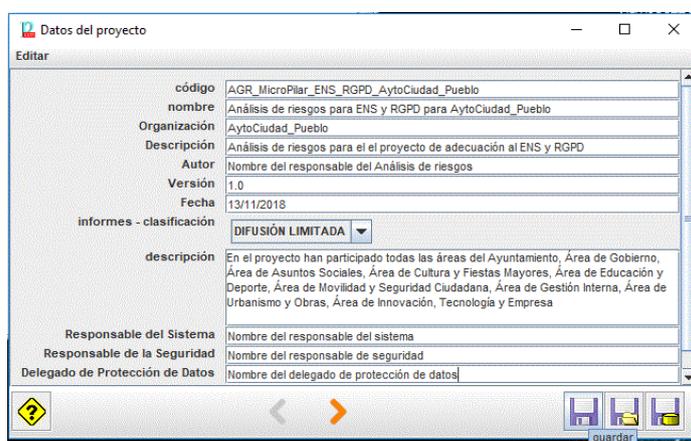


Figura 5 Opción “Guardar”

32. Aparece una ventana de selección. Pulse el botón “fichero”
33. Aparece una pantalla para guardar ficheros. Si es necesario cree una nueva carpeta, entre en ella y guarde el nuevo fichero PILAR con un nombre significativo, por ejemplo, AGR_MicroPilar_ENS_RGPD_NombreEntidadLocal.
34. Aparece una ventana donde permite guardar con una clave de protección el nuevo fichero:
 - Si no quiere guardarlo con contraseña, deje los campos en blanco y pulse el botón  para guardar o bien  para cancelar.
 - Volverá a la ventana de información del proyecto, pulse  para continuar.
 - Si quiere abrir un fichero PILAR previamente existente seleccione la opción “abrir...” del menú inicial. Aparece una ventana para buscar (1), seleccionar (2) y abrir (3) el fichero PILAR (con extensión “.mgr”):

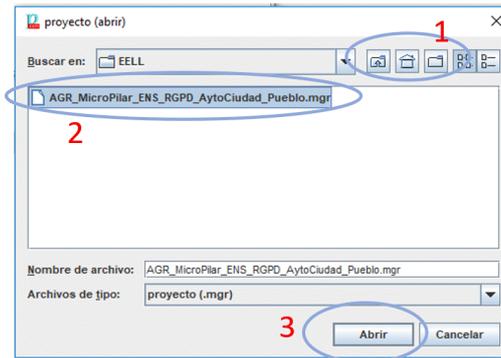


Figura 6 Buscar, Seleccionar y Abrir fichero PILAR

- PILAR procede a la carga del fichero. Se muestra una ventana de información sobre los diferentes componentes de PILAR cargados y se debe pulsar en el botón “Aceptar” para terminar la carga del fichero de PILAR:
- También por este camino llega a la ventana de información del proyecto, pulse  para continuar.

5.3.3. Activos y valoración

35. A continuación, se muestra la pantalla de “Activos”, en la que se aparecen los activos predefinidos¹:

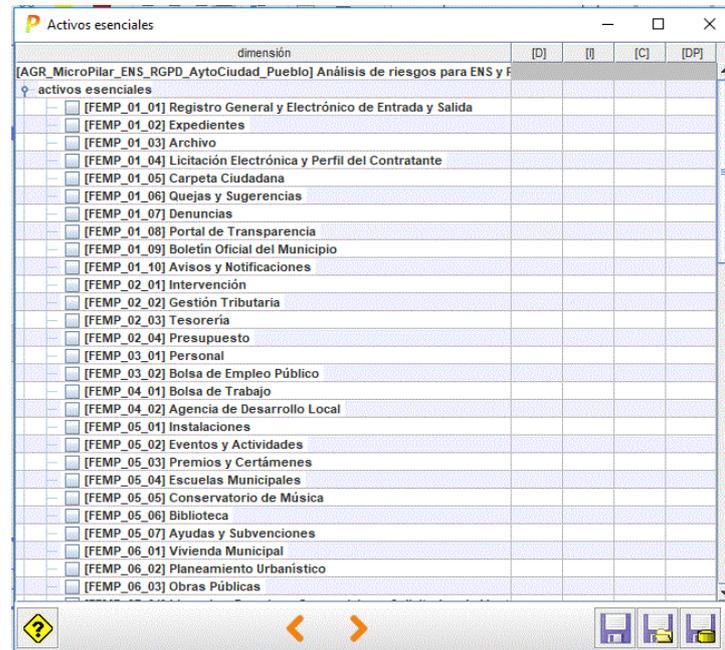
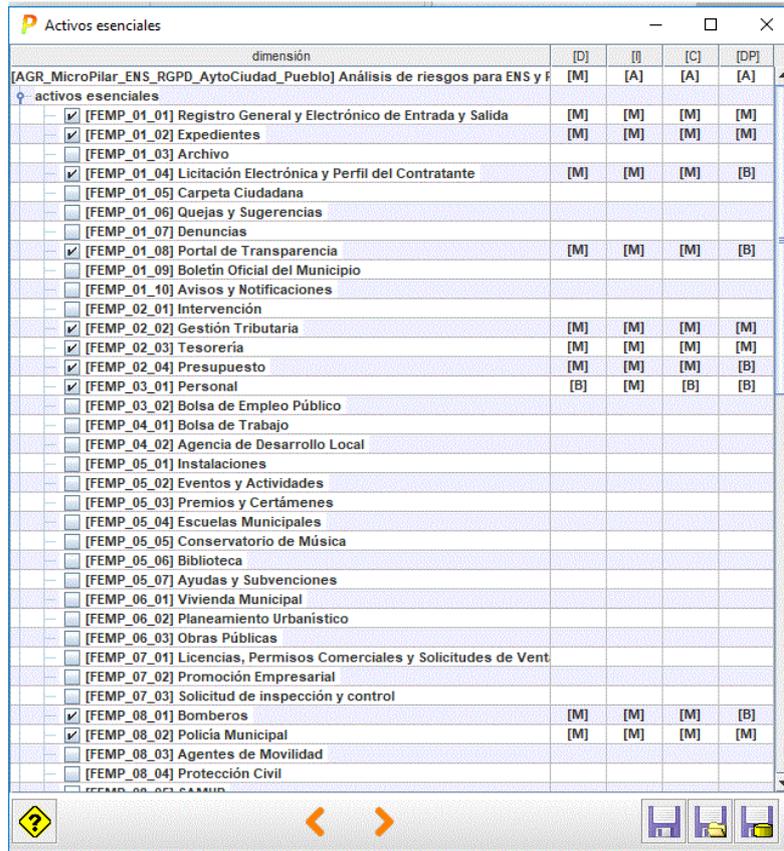


Figura 7 Activos predefinidos

36. Estos activos predefinidos tratan de reflejar el común denominador de los activos presentes en cualquier Entidad Local.

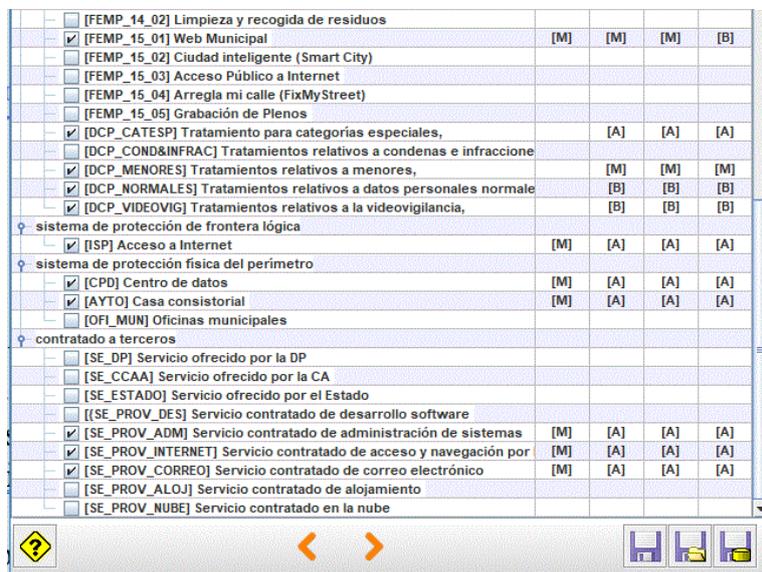
¹ Ver guía Anexo II Entidades Locales de la guía 803 - Valoración de los sistemas

37. Los “Activos esenciales” son aquellos activos que representan las actividades principales (servicios y datos) que ofrece la Entidad Local a los ciudadanos.
38. Los activos “sistema de protección física del perímetro” corresponden a los activos tecnológicos firewalls o cortafuegos que disponga la institución y que protegen la conexión al exterior, típicamente Internet.
39. Los activos “sistema de protección física del perímetro” se refiere a los activos físicos que sirven de ubicación y protección de la infraestructura tecnológica, como son los edificios en los que se localizan.
40. Los activos “contratado a terceros” son aquellos activos tanto físicos como lógicos que son suministrados por un tercero, ejemplos típicos son aplicaciones que pertenecen y están ubicadas en otro organismo como puede ser una Diputación Provincial y que son utilizados por la Entidad Local, o bien, un servicio de mantenimiento de microinformática que está contratado con una empresa privada mediante licitación.
41. Con la ayuda de la Guía Anexo II Entidades Locales de la guía 803 - Valoración de los sistemas, revise cada uno de ellos para comprobar en qué grado se ajustan a sus características.
42. Seleccione cada uno de los activos que conforman de manera más aproximada las características de su Entidad Local. Para ello, marque el recuadro al lado del nombre del activo que quiere seleccionar.
43. La ventana de activos quedará como se muestra en las dos siguientes figuras:



dimensión	[D]	[I]	[C]	[DP]
[AGR_MicroPilar_ENS_RGPD_AytoCiudad_Pueblo] Análisis de riesgos para ENS y F	[M]	[A]	[A]	[A]
activos esenciales				
<input checked="" type="checkbox"/> [FEMP_01_01] Registro General y Electrónico de Entrada y Salida	[M]	[M]	[M]	[M]
<input checked="" type="checkbox"/> [FEMP_01_02] Expedientes	[M]	[M]	[M]	[M]
<input type="checkbox"/> [FEMP_01_03] Archivo				
<input checked="" type="checkbox"/> [FEMP_01_04] Licitación Electrónica y Perfil del Contratante	[M]	[M]	[M]	[B]
<input type="checkbox"/> [FEMP_01_05] Carpeta Ciudadana				
<input type="checkbox"/> [FEMP_01_06] Quejas y Sugerencias				
<input type="checkbox"/> [FEMP_01_07] Denuncias				
<input checked="" type="checkbox"/> [FEMP_01_08] Portal de Transparencia	[M]	[M]	[M]	[B]
<input type="checkbox"/> [FEMP_01_09] Boletín Oficial del Municipio				
<input type="checkbox"/> [FEMP_01_10] Avisos y Notificaciones				
<input type="checkbox"/> [FEMP_02_01] Intervención				
<input checked="" type="checkbox"/> [FEMP_02_02] Gestión Tributaria	[M]	[M]	[M]	[M]
<input checked="" type="checkbox"/> [FEMP_02_03] Tesorería	[M]	[M]	[M]	[M]
<input checked="" type="checkbox"/> [FEMP_02_04] Presupuesto	[M]	[M]	[M]	[B]
<input checked="" type="checkbox"/> [FEMP_03_01] Personal	[B]	[M]	[B]	[B]
<input type="checkbox"/> [FEMP_03_02] Bolsa de Empleo Público				
<input type="checkbox"/> [FEMP_04_01] Bolsa de Trabajo				
<input type="checkbox"/> [FEMP_04_02] Agencia de Desarrollo Local				
<input type="checkbox"/> [FEMP_05_01] Instalaciones				
<input type="checkbox"/> [FEMP_05_02] Eventos y Actividades				
<input type="checkbox"/> [FEMP_05_03] Premios y Certámenes				
<input type="checkbox"/> [FEMP_05_04] Escuelas Municipales				
<input type="checkbox"/> [FEMP_05_05] Conservatorio de Música				
<input type="checkbox"/> [FEMP_05_06] Biblioteca				
<input type="checkbox"/> [FEMP_05_07] Ayudas y Subvenciones				
<input type="checkbox"/> [FEMP_06_01] Vivienda Municipal				
<input type="checkbox"/> [FEMP_06_02] Planeamiento Urbanístico				
<input type="checkbox"/> [FEMP_06_03] Obras Públicas				
<input type="checkbox"/> [FEMP_07_01] Licencias, Permisos Comerciales y Solicitudes de Vent				
<input type="checkbox"/> [FEMP_07_02] Promoción Empresarial				
<input type="checkbox"/> [FEMP_07_03] Solicitud de inspección y control				
<input checked="" type="checkbox"/> [FEMP_08_01] Bomberos	[M]	[M]	[M]	[B]
<input checked="" type="checkbox"/> [FEMP_08_02] Policía Municipal	[M]	[M]	[M]	[M]
<input type="checkbox"/> [FEMP_08_03] Agentes de Movilidad				
<input type="checkbox"/> [FEMP_08_04] Protección Civil				

Figura 8 Ventana con los activos seleccionados (I)



<input type="checkbox"/> [FEMP_14_02] Limpieza y recogida de residuos				
<input checked="" type="checkbox"/> [FEMP_15_01] Web Municipal	[M]	[M]	[M]	[B]
<input type="checkbox"/> [FEMP_15_02] Ciudad inteligente (Smart City)				
<input type="checkbox"/> [FEMP_15_03] Acceso Público a Internet				
<input type="checkbox"/> [FEMP_15_04] Arregla mi calle (FixMyStreet)				
<input type="checkbox"/> [FEMP_15_05] Grabación de Plenos				
<input checked="" type="checkbox"/> [DCP_CATESP] Tratamiento para categorías especiales,		[A]	[A]	[A]
<input type="checkbox"/> [DCP_COND&INFRAC] Tratamientos relativos a condenas e infracciones				
<input checked="" type="checkbox"/> [DCP_MENORES] Tratamientos relativos a menores,		[M]	[M]	[M]
<input checked="" type="checkbox"/> [DCP_NORMALES] Tratamientos relativos a datos personales normales		[B]	[B]	[B]
<input checked="" type="checkbox"/> [DCP_VIDEOVIG] Tratamientos relativos a la videovigilancia,		[B]	[B]	[B]
sistema de protección de frontera lógica				
<input checked="" type="checkbox"/> [ISP] Acceso a Internet	[M]	[A]	[A]	[A]
sistema de protección física del perímetro				
<input checked="" type="checkbox"/> [CPD] Centro de datos	[M]	[A]	[A]	[A]
<input checked="" type="checkbox"/> [AYTO] Casa consistorial	[M]	[A]	[A]	[A]
<input type="checkbox"/> [OFL_MUN] Oficinas municipales				
contratado a terceros				
<input type="checkbox"/> [SE_DP] Servicio ofrecido por la DP				
<input type="checkbox"/> [SE_CCAA] Servicio ofrecido por la CA				
<input type="checkbox"/> [SE_ESTADO] Servicio ofrecido por el Estado				
<input type="checkbox"/> [SE_PROV_DES] Servicio contratado de desarrollo software				
<input checked="" type="checkbox"/> [SE_PROV_ADM] Servicio contratado de administración de sistemas	[M]	[A]	[A]	[A]
<input checked="" type="checkbox"/> [SE_PROV_INTERNET] Servicio contratado de acceso y navegación por	[M]	[A]	[A]	[A]
<input checked="" type="checkbox"/> [SE_PROV_CORREO] Servicio contratado de correo electrónico	[M]	[A]	[A]	[A]
<input type="checkbox"/> [SE_PROV_ALOJ] Servicio contratado de alojamiento				
<input type="checkbox"/> [SE_PROV_NUBE] Servicio contratado en la nube				

Figura 9 Ventana con los activos seleccionados (y II)

44. Los activos están pre-valorados en sus dimensiones de Disponibilidad [D], Integridad [I], Confidencialidad [C] y Protección de Datos [DP]². Estos valores no se pueden modificar. Estos valores se configuran en el fichero Excel ubicado en [UNIDAD]:\PilarMicro_7.3.0_eell\micro_eell\assets.xlsx.

² Ver guía Anexo II Entidades Locales de la guía 803 - Valoración de los sistemas

45. Si ha realizado cambios pulse el botón “guardar”  antes de avanzar  o de retroceder .
46. Si avanzamos, se pasa a la pantalla en la que se describe las clases de activos que conforman nuestra infraestructura técnica, de seguridad, instalaciones, personas, etc.:

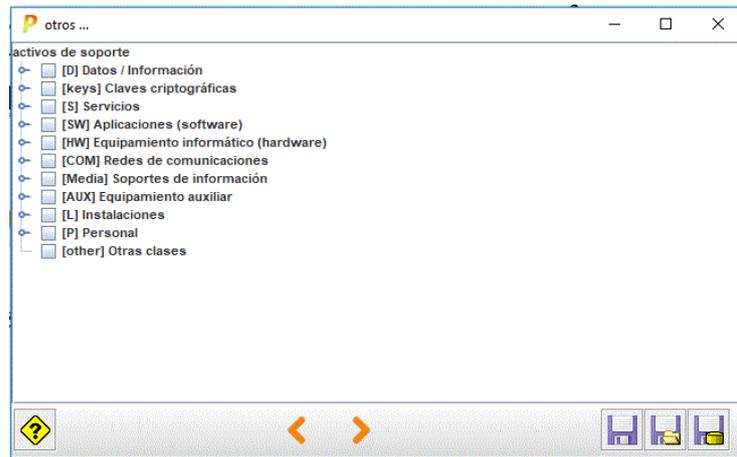


Figura 10 Clases de Activos de la infraestructura

47. Despliegue todo el árbol de activos.
48. Marque aquellas clases de activos según disponga de ellos en su infraestructura.
49. Siguiendo con el ejemplo, se dispone de dos servicios que los suministran proveedores externos, [SE_PROV_INTERNET] y [SE_PROV_CORREO]. Por tanto, debemos comprobar que las clases de activos correspondientes están marcadas y que las correspondientes a servicios similares que se prestarán de forma interna no lo están.



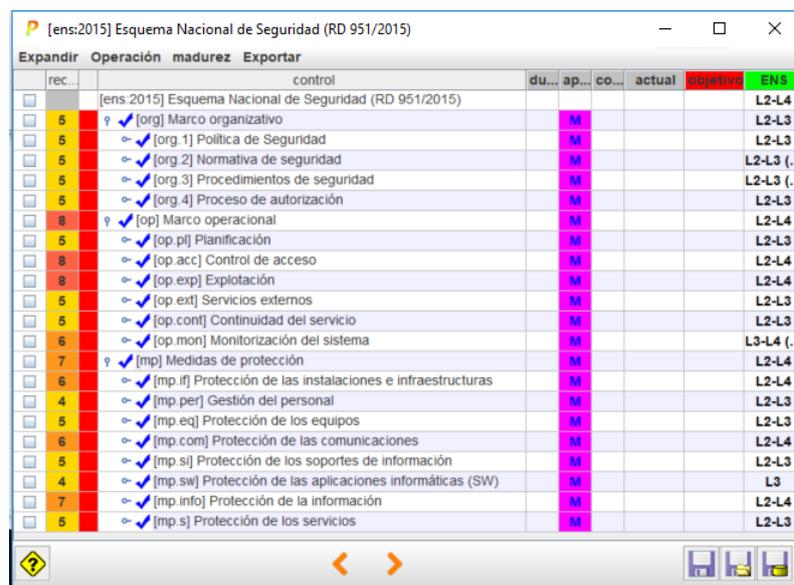
Figura 11 Servicios "somos clientes de..."

50. En nuestro ejemplo, somos clientes de correo electrónico y navegación web pero no se dispone de teletrabajo. Por tanto, se dejan marcados los dos primeros y se desmarca el correspondiente a teletrabajo.
51. Consecuentemente, los correspondientes a los Servicios “proporcionados por nosotros”, no deben estar desmarcar los correspondientes a [www] y [email].
52. Así mismo, vamos a comprobar si entre las “[SW] Aplicaciones” se encuentra alguna que tampoco deba estar marcada:
53. Siguiendo con nuestro ejemplo están [email_client] y [email_server].

54. En el caso de [email_client], si está instalado un software para correo electrónico en los equipos de usuario (PC, portátil, Tablet, móvil), como por ejemplo Outlook de Microsoft, debe marcarse. Si, por el contrario, el usuario utiliza el correo electrónico conectándose a una aplicación Web, como OWA, Gmail o similar, entonces no se debe marcar. Supongamos este segundo caso, en consecuencia no debe estar marcado el [email_client].
55. En el caso del [email_server], debe estar desmarcado, ya que es un servicio que ofrece un tercero.
56. De igual forma que se ha realizado en este ejemplo, revise todas las Clases de activo que se muestran.
57. Si ha realizado cambios pulse el botón “guardar”  antes de avanzar  o de retroceder .

5.3.4. Esquema Nacional de Seguridad

58. A continuación se muestra la pantalla del ENS:



rec.	Operación	madurez	Exportar	du...	ap...	co...	actual	objetivo	ENS
	[ens:2015] Esquema Nacional de Seguridad (RD 951/2015)								L2-L4
5	✓ [org] Marco organizativo				M				L2-L3
5	✓ [org.1] Política de Seguridad				M				L2-L3
5	✓ [org.2] Normativa de seguridad				M				L2-L3 (...)
5	✓ [org.3] Procedimientos de seguridad				M				L2-L3 (...)
5	✓ [org.4] Proceso de autorización				M				L2-L3
8	✓ [op] Marco operacional				M				L2-L4
5	✓ [op.pl] Planificación				M				L2-L3
8	✓ [op.acc] Control de acceso				M				L2-L4
8	✓ [op.exp] Explotación				M				L2-L4
5	✓ [op.ext] Servicios externos				M				L2-L3
5	✓ [op.cont] Continuidad del servicio				M				L2-L3
6	✓ [op.mon] Monitorización del sistema				M				L3-L4 (...)
7	✓ [mp] Medidas de protección				M				L2-L4
6	✓ [mp.if] Protección de las instalaciones e infraestructuras				M				L2-L4
4	✓ [mp.per] Gestión del personal				M				L2-L3
5	✓ [mp.eq] Protección de los equipos				M				L2-L3
6	✓ [mp.com] Protección de las comunicaciones				M				L2-L4
5	✓ [mp.si] Protección de los soportes de información				M				L2-L3
4	✓ [mp.sw] Protección de las aplicaciones informáticas (SW)				M				L3
7	✓ [mp.info] Protección de la información				M				L2-L4
5	✓ [mp.s] Protección de los servicios				M				L2-L3

Figura 12 Ventana inicial del ENS

59. Utilice la opción Expandir → preguntas para que se muestren las medidas de seguridad y un conjunto de preguntas que le servirán para valorar con más precisión dichas medidas. Las “preguntas” se corresponden con los requisitos específicos que aparecen en el Anexo II del ENS para cada uno de los controles de seguridad.
60. Las diferentes columnas que aparecen permiten valorar y documentar las medidas del ENS.

61. La columna “dudas” indica si existe alguna duda sobre la valoración o bien falta información sobre una medida de seguridad concreta:

control	dudas
[ens:2015] Esquema Nacional de Seguridad (RD 951/2015)	
☑ [org] Marco organizativo	
☑ [org.1] Política de Seguridad	¿...?
☑ [org.2] Normativa de seguridad	
☑ [org.3] Procedimientos de seguridad	
☑ [org.4] Proceso de autorización	¿...?
☑ [org] Marco operacional	

Figura 13 Columna “dudas”

62. La columna “aplica” permite indicar si el control o salvaguarda aplica o no a nuestra organización. Pinche en ese campo y el valor pasa de “M” o en blanco a “n.a.”

63. En nuestro ejemplo, al tratarse de sistemas valorados como de categoría Media, podemos considerar que las medidas aplicables a sistemas valorados de categoría Alta no son aplicables. Marquemos la celda correspondiente a columna “aplica” de las medidas para sistemas de categoría Alta para que pase a “n.a”.

64. La no aplicabilidad de alguna medida puede venir dado por varios motivos:

- Porque en el sistema de información concreto no tiene sentido ese control, por no utilizarse o por otra razón
- Porque, en función de la categoría del sistema y, en base a lo establecido en el Anexo II del ENS, puede no ser de aplicación de cara al cumplimiento. No obstante, aunque no fuera aplicable de cara al cumplimiento, sí que podría serlo para mitigar riesgos. Si al obtener los valores de riesgo hubiera alguno demasiado elevado y que se pudiera mitigar con esa medida, sería preciso tenerla en consideración.

65. Revisemos la aplicabilidad de todas las medidas del ENS.

66. Utilice la columna “comentario” para documentar la valoración y las acciones correspondientes a la medida/pregunta correspondiente.

67. Al pinchar en la celda de comentario correspondiente, aparece la siguiente ventana:

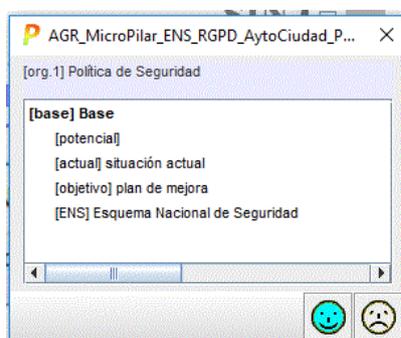


Figura 14 Ventana “comentario”

68. Se recomienda documentar al menos la situación actual [actual] y el plan de mejora [objetivo]:
69. Selecciones [actual] y documente la situación actual de esta medida/pregunta.
70. Salga salvando los cambios pulsando el icono: 😊. Si no quiere salvar los cambios o bien no ha realizado cambios, pulse el icono: 😞.
71. De igual forma actúe para la situación [objetivo].
72. Estos comentarios enriquecen el análisis realizado y permitirán determinar las acciones de mejora a realizar por la Entidad Local para cumplir con el ENS. Estas acciones son las piezas básicas que permitirán construir el Plan de Tratamiento de Riesgos (ver apartado 6 PLAN DE TRATAMIENTO DE RIESGOS).
73. Puede utilizar una nomenclatura que le permita reunir las acciones de mejora por tipo (proyecto) que luego conformarán el Plan de Tratamiento, por ejemplo, las acciones de documentación (generar política, normativas, procedimientos, instructivos, etc.) denominarlas como “DOC”, las de tipo organizativo (designación de responsables, Comités, relaciones con otros organismos, etc.) como “ORG”, las de tipo formativo, difusión y concienciación como “FOR” o las de tipo técnico (compra de herramientas software, equipamiento, consultoría, etc.) como “TEC”.

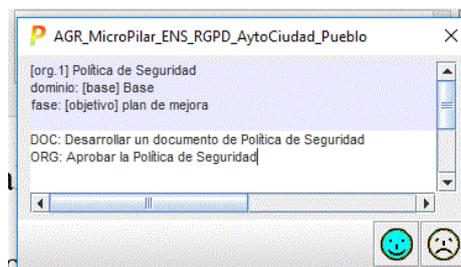


Figura 15 Documentar [objetivo]

74. Salga salvando los cambios pulsando el icono: 😊. Si no quiere salvar los cambios o bien no ha realizado cambios, pulse el icono: 😞.
75. En la columna “comentario” viene señalada la celda correspondiente a la medida/pregunta documentada.
76. Ahora toca el turno de valorar la medida de seguridad o pregunta. Para ello se utilizan los valores correspondientes a la madurez según la escala CMM, con valores que van desde L0 a L5. En la siguiente tabla se muestra la descripción de cada nivel y los porcentajes numéricos en los que se traducen:

Nivel	Descripción	% madurez
L0	Inexistente. Esta medida no está siendo aplicada en este momento. Por ejemplo, se trata de “hacer backup”. No se hacen backups	L0
L1	Inicial / ad hoc.	L1

Nivel	Descripción	% madurez
	<p>Cuando la organización no proporciona un entorno estable. El éxito o fracaso del proceso depende de la competencia y buena voluntad de las personas. Pese a una naturaleza caótica, es más que no tener nada; pero es difícil prever la reacción ante una situación de emergencia.</p> <p>Por ejemplo, seguimos con los backups. Se hace backup cuando el técnico se acuerda.</p>	
L2	<p>Repetible, pero intuitivo.</p> <p>Cuando existe un mínimo de planificación que, acompañada de la buena voluntad de las personas proporciona una pauta a seguir cuando se repiten las mismas circunstancias. Es impredecible el resultado si se dan circunstancias nuevas.</p> <p>Por ejemplo, seguimos con los backups. Se hacen todas las semanas, pero si el técnico está de vacaciones no se hacen.</p>	L2
L3	<p>Proceso definido.</p> <p>Se dispone un catálogo de procesos que se mantiene actualizado. Estos procesos garantizan la consistencia de las actuaciones entre las diferentes partes de la organización, que adaptan sus procesos particulares al proceso general.</p> <p>Una diferencia importante entre el nivel 2 y el nivel 3 es la coordinación entre departamentos y proyectos, coordinación que no existe en el nivel 2, y que se gestiona en el nivel 3.</p> <p>Por ejemplo, seguimos con los backups. Existe un procedimiento documentado de backups que es conocido por todos los técnicos y si falta el encargado de los backups, otro técnico, con la ayuda del procedimiento, los realiza.</p>	L3
L4	<p>Gestionado y medible.</p> <p>Cuando se dispone de un sistema de medidas y métricas para conocer el desempeño (eficacia y eficiencia) de los procesos. La Dirección es capaz de establecer objetivos cualitativos a alcanzar y dispone de medios para valorar si se han alcanzado los objetivos y en qué medida.</p> <p>Por ejemplo, seguimos con los backups. Se revisan los logs, se hacen pruebas de restauración, se hacen mediciones de tiempos de backup para ajustar las ventanas de copia.</p>	L4
L5	<p>Optimizado.</p> <p>En este nivel la organización es capaz de mejorar el desempeño de los sistemas a base de una mejora continua de los procesos basada en los resultados de las medidas e indicadores.</p> <p>Por ejemplo, seguimos con el ejemplo de los backups. Se revisan las mediciones, los resultados de prueba, el propio procedimiento, para determinar aspectos de mejora que se documentan, planifican, implementan y se evalúan.</p>	L5

Tabla 1 Niveles de madurez

77. La guía CCN-STIC 804 establece unos niveles de madurez mínimos para cada una de las medidas aplicables del ENS en función de la categoría del sistema, que son las que a continuación se indican.

VALOR DEL SISTEMA EN DIMENSIÓN DE SEGURIDAD SIGNIFICATIVA PARA LA MEDIDA DE SEGURIDAD	CATEGORÍA DEL SISTEMA	NIVEL DE MADUREZ MÍNIMO DE LA MEDIDA DE SEGURIDAD
BAJO	BÁSICA	L2 - Repetible, pero intuitivo
MEDIO	MEDIA	L3 - Proceso definido
ALTO	ALTA	L4 - Gestionado y medible

Tabla 2 Niveles de madurez mínimos

78. Por lo tanto, cuando los niveles reales estén por debajo de estos valores recomendados (insuficiencias), habrá que implementar acciones para la mejora a la adecuación al ENS y del riesgo. En los apartados siguientes se presentan los valores de riesgo asociado a estos niveles actuales y los niveles a los que se propone llegar en cada una de las medidas, así como las acciones para alcanzar dichos porcentajes (organizadas en un Plan de tratamiento de riesgos).
79. Para realizar la valoración se pincha con el botón derecho sobre la celda correspondiente de la medida/pregunta tanto de la columna “actual” como en la “objetivo”:

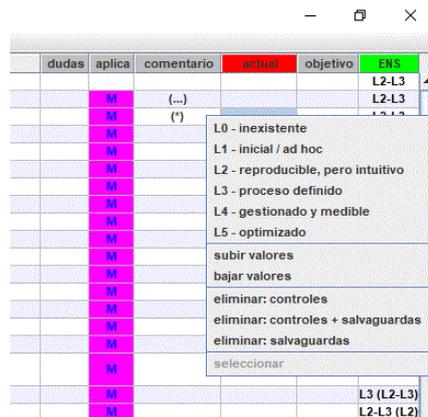


Figura 16 Valorar medida/pregunta

80. No olvide que en “objetivo” se debe describir la acción que haría falta para cumplir el requisito en cuestión para el nivel de madurez que se está poniendo como objetivo. Así, por ejemplo, si se está tendiendo a L3 la acción deberá contemplar documentar y difundir, si es un documento. Y si es L4, la acción deberá incluir revisiones periódicas y medición de indicadores de funcionamiento.
81. Esta información completada para el ENS se puede además guardar en un fichero de tipo CSV con la opción “Exportar” del menú superior de la pantalla:

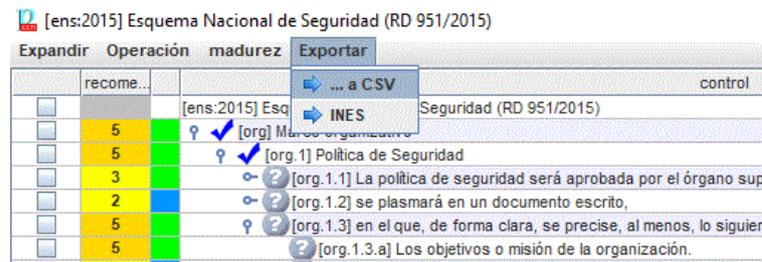


Figura 17 Opción guardar como fichero CSV

82. Aparecerá una ventana de manejo de ficheros en el que le propondrá “controls_ens_2015.csv” como nombre para el fichero de valoración de medidas y preguntas. Este fichero puede abrirlo con Excel o su programa de hoja de cálculo disponible

83. Una vez valorados y documentados cada una de las medidas/preguntas que apliquen, pulse el botón “guardar”  antes de avanzar  o de retroceder .
84. A continuación se pasa a una pantalla con medidas de seguridad adicionales que pueden aplicarse para nuestro entorno:

rec...	control	dud...	apli...	com...	actual	objetivo	ENS
	[ens+:2015] ENS: Medidas de seguridad adicionales						L3-L4 (L2-L4)
5	[ENS+.1] Servicios potencialmente peligrosos		✓				L3 (L2-L3)
4	[ENS+.2] Máquinas virtuales		✓				L3 (L2-L3)
7	[ENS+.3] Redes WiFi		✓				L4 (L3-L4)
4	[ENS+.4] Protección del perímetro lógico (interconexión)		✓				L3

Figura 18 Medidas de protección adicionales

85. Se actúa de igual forma que se ha realizado para las medidas del ENS descritas anteriormente.

5.3.5. Reglamento General de Protección de Datos

86. A continuación, se avanza hacia la pantalla correspondiente a la valoración del RGPD:

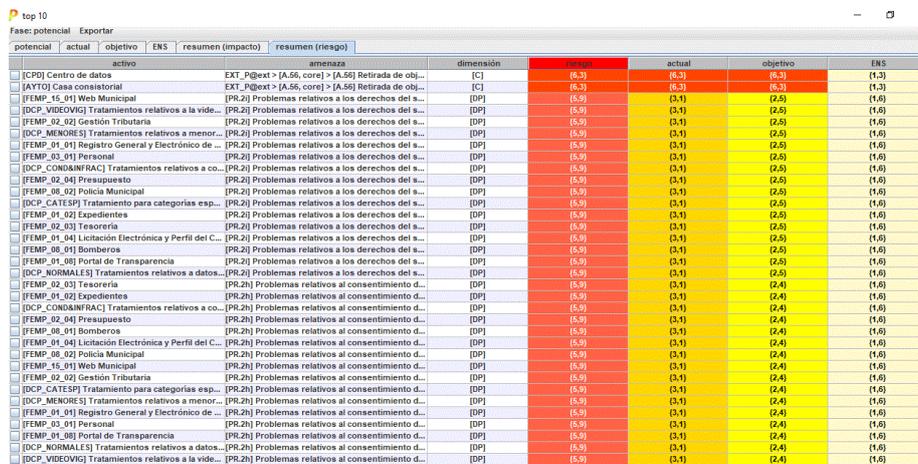
rec.	Operación	madurez	Exportar	control	du...	ap...	co...	actual	objetivo	ENS
5	[A6] Artículo 6 - Licitud del tratamiento					✓				L3
5	[A7] Artículo 7 - Condiciones para el consentimiento					✓				L3
5	[A8] Artículo 8 - Condiciones aplicables al consentimiento del niño en relación con los servicios de la sociedad de la información					✓				L3
5	[A9] Artículo 9 - Tratamiento de categorías especiales de datos personales					✓				L3
5	[A10] Artículo 10 - Tratamiento de datos personales relativos a condenas e infracciones penales					✓				L3
5	[A11] Artículo 11 - Tratamiento que no requiere identificación					✓				L3
5	[A12] Artículo 12 - Transparencia de la información, comunicación y modalidades de ejercicio de los derechos del interesado					✓				L3
5	[A13] Artículo 13 - Información que deberá facilitarse cuando los datos personales se obtengan del interesado					✓				L3
5	[A14] Artículo 14 - Información que deberá facilitarse cuando los datos personales no se hayan obtenido del interesado					✓				L3
5	[A15] Artículo 15 - Derecho de acceso del interesado					✓				L3
5	[A16] Artículo 16 - Derecho de rectificación					✓				L3
5	[A17] Artículo 17 - Derecho de supresión («el derecho al olvido»)					✓				L3
5	[A18] Artículo 18 - Derecho a la limitación del tratamiento					✓				L3
5	[A19] Artículo 19 - Obligación de notificación relativa a la rectificación o supresión de datos personales o la limitación del tratamiento					✓				L3
5	[A20] Artículo 20 - Derecho a la portabilidad de los datos					✓				L3
5	[A21] Artículo 21 - Derecho de oposición					✓				L3
5	[A22] Artículo 22 - Decisiones individuales automatizadas, incluida la elaboración de perfiles					✓				L3
5	[A24] Artículo 24 - Responsabilidad del responsable del tratamiento					✓				L3
5	[A25] Artículo 25 - Protección de datos desde el diseño y por defecto					✓				L3
5	[A26] Artículo 26 - Corresponsables del tratamiento					✓				L3
5	[A28] Artículo 28 - Encargado del tratamiento					✓				L3

Figura 19 Pantalla de valoración del RGPD

87. Utilice la opción “Expandir”, “preguntas” para que se muestren las medidas de seguridad y un conjunto de preguntas que le servirán para valorar con más precisión dichas medidas.
88. De igual forma a como se realizó la valoración para el ENS, se realiza para este caso del RGPD.
89. Recuerde utilizar las columnas “duda”, “aplica”, “comentarios” “actual” y “objetivo” como lo hizo en el caso del ENS.
90. También puede exportar esta valoración a un fichero CSV (controls_GDPR_2016.csv) como se realiza para el ENS.
91. Una vez valorados y documentados cada uno de los artículos/preguntas que apliquen, pulse el botón “guardar”  antes de avanzar  o de retroceder .

5.3.6. Riesgos

92. En la siguiente pantalla aparecen los valores correspondientes a las 10 amenazas más significativas (“Top 10”) con las pestañas “potencial”, “actual”, “objetivo”, “ENS”, “resumen (impacto)” y “resumen (riesgo)”:



potencial	actual	objetivo	ENS	resumen (impacto)	resumen (riesgo)																																																																																																																																																																																																																																																					
					<table border="1"> <thead> <tr> <th>activo</th> <th>amenaza</th> <th>dimensión</th> <th>riesgo</th> <th>actual</th> <th>objetivo</th> <th>ENS</th> </tr> </thead> <tbody> <tr> <td>[CPD] Centro de datos</td> <td>EXT_P@ext > [A.56, core] > [A.56] Retirada de obj...</td> <td>[C]</td> <td>(6,3)</td> <td>(6,3)</td> <td>(6,3)</td> <td>(1,3)</td> </tr> <tr> <td>[AYT0] Casa consistorial</td> <td>EXT_P@ext > [A.56, core] > [A.56] Retirada de obj...</td> <td>[C]</td> <td>(6,3)</td> <td>(6,3)</td> <td>(6,3)</td> <td>(1,3)</td> </tr> <tr> <td>[FEMP_15_01] Web Municipal</td> <td>[PR.2] Problemas relativos a los derechos del s...</td> <td>[DP]</td> <td>(5,9)</td> <td>(3,1)</td> <td>(2,6)</td> <td>(1,6)</td> </tr> <tr> <td>[DCP_VIDEOVIG] Tratamientos relativos a la vide...</td> <td>[PR.2] Problemas relativos a los derechos del s...</td> <td>[DP]</td> <td>(5,9)</td> <td>(3,1)</td> <td>(2,6)</td> <td>(1,6)</td> </tr> <tr> <td>[FEMP_02_02] Gestión Tributaria</td> <td>[PR.2] Problemas relativos a los derechos del s...</td> <td>[DP]</td> <td>(5,9)</td> <td>(3,1)</td> <td>(2,6)</td> <td>(1,6)</td> </tr> <tr> <td>[DCP_MENORES] Tratamientos relativos a menor...</td> <td>[PR.2] Problemas relativos a los derechos del s...</td> <td>[DP]</td> <td>(5,9)</td> <td>(3,1)</td> <td>(2,6)</td> <td>(1,6)</td> </tr> <tr> <td>[FEMP_01_01] Registro General y Electrónico de...</td> <td>[PR.2] Problemas relativos a los derechos del s...</td> <td>[DP]</td> <td>(5,9)</td> <td>(3,1)</td> <td>(2,6)</td> <td>(1,6)</td> </tr> <tr> <td>[FEMP_03_01] Personal</td> <td>[PR.2] Problemas relativos a los derechos del s...</td> <td>[DP]</td> <td>(5,9)</td> <td>(3,1)</td> <td>(2,6)</td> <td>(1,6)</td> </tr> <tr> <td>[DCP_CONDANFIRAC] Tratamientos relativos a co...</td> <td>[PR.2] Problemas relativos a los derechos del s...</td> <td>[DP]</td> <td>(5,9)</td> <td>(3,1)</td> <td>(2,6)</td> <td>(1,6)</td> </tr> <tr> <td>[FEMP_02_04] Presupuesto</td> <td>[PR.2] Problemas relativos a los derechos del s...</td> <td>[DP]</td> <td>(5,9)</td> <td>(3,1)</td> <td>(2,6)</td> <td>(1,6)</td> </tr> <tr> <td>[FEMP_06_02] Policía Municipal</td> <td>[PR.2] Problemas relativos a los derechos del s...</td> <td>[DP]</td> <td>(5,9)</td> <td>(3,1)</td> <td>(2,6)</td> <td>(1,6)</td> </tr> <tr> <td>[DCP_CATESP] Tratamiento para categorías esp...</td> <td>[PR.2] Problemas relativos a los derechos del s...</td> <td>[DP]</td> <td>(5,9)</td> <td>(3,1)</td> <td>(2,6)</td> <td>(1,6)</td> </tr> <tr> <td>[FEMP_01_02] Expedientes</td> <td>[PR.2] Problemas relativos a los derechos del s...</td> <td>[DP]</td> <td>(5,9)</td> <td>(3,1)</td> <td>(2,6)</td> <td>(1,6)</td> </tr> <tr> <td>[FEMP_02_03] Tesorería</td> <td>[PR.2] Problemas relativos a los derechos del s...</td> <td>[DP]</td> <td>(5,9)</td> <td>(3,1)</td> <td>(2,6)</td> <td>(1,6)</td> </tr> <tr> <td>[FEMP_01_04] Licitación Electrónica y Perfil del C...</td> <td>[PR.2] Problemas relativos a los derechos del s...</td> <td>[DP]</td> <td>(5,9)</td> <td>(3,1)</td> <td>(2,6)</td> <td>(1,6)</td> </tr> <tr> <td>[FEMP_06_01] Bomberos</td> <td>[PR.2] Problemas relativos a los derechos del s...</td> <td>[DP]</td> <td>(5,9)</td> <td>(3,1)</td> <td>(2,6)</td> <td>(1,6)</td> </tr> <tr> <td>[FEMP_01_03] Portal de Transparencia</td> <td>[PR.2] Problemas relativos a los derechos del s...</td> <td>[DP]</td> <td>(5,9)</td> <td>(3,1)</td> <td>(2,6)</td> <td>(1,6)</td> </tr> <tr> <td>[DCP_NORMALES] Tratamientos relativos a datos...</td> <td>[PR.2] Problemas relativos a los derechos del s...</td> <td>[DP]</td> <td>(5,9)</td> <td>(3,1)</td> <td>(2,6)</td> <td>(1,6)</td> </tr> <tr> <td>[FEMP_02_03] Tesorería</td> <td>[PR.2] Problemas relativos al consentimiento d...</td> <td>[DP]</td> <td>(5,9)</td> <td>(3,1)</td> <td>(2,4)</td> <td>(1,6)</td> </tr> <tr> <td>[FEMP_01_02] Expedientes</td> <td>[PR.2] Problemas relativos al consentimiento d...</td> <td>[DP]</td> <td>(5,9)</td> <td>(3,1)</td> <td>(2,4)</td> <td>(1,6)</td> </tr> <tr> <td>[DCP_CONDANFIRAC] Tratamientos relativos a co...</td> <td>[PR.2] Problemas relativos al consentimiento d...</td> <td>[DP]</td> <td>(5,9)</td> <td>(3,1)</td> <td>(2,4)</td> <td>(1,6)</td> </tr> <tr> <td>[FEMP_02_04] Presupuesto</td> <td>[PR.2] Problemas relativos al consentimiento d...</td> <td>[DP]</td> <td>(5,9)</td> <td>(3,1)</td> <td>(2,4)</td> <td>(1,6)</td> </tr> <tr> <td>[FEMP_06_01] Bomberos</td> <td>[PR.2] Problemas relativos al consentimiento d...</td> <td>[DP]</td> <td>(5,9)</td> <td>(3,1)</td> <td>(2,4)</td> <td>(1,6)</td> </tr> <tr> <td>[FEMP_01_03] Portal de Transparencia</td> <td>[PR.2] Problemas relativos al consentimiento d...</td> <td>[DP]</td> <td>(5,9)</td> <td>(3,1)</td> <td>(2,4)</td> <td>(1,6)</td> </tr> <tr> <td>[FEMP_06_02] Policía Municipal</td> <td>[PR.2] Problemas relativos al consentimiento d...</td> <td>[DP]</td> <td>(5,9)</td> <td>(3,1)</td> <td>(2,4)</td> <td>(1,6)</td> </tr> <tr> <td>[FEMP_16_01] Web Municipal</td> <td>[PR.2] Problemas relativos al consentimiento d...</td> <td>[DP]</td> <td>(5,9)</td> <td>(3,1)</td> <td>(2,4)</td> <td>(1,6)</td> </tr> <tr> <td>[FEMP_02_02] Gestión Tributaria</td> <td>[PR.2] Problemas relativos al consentimiento d...</td> <td>[DP]</td> <td>(5,9)</td> <td>(3,1)</td> <td>(2,4)</td> <td>(1,6)</td> </tr> <tr> <td>[DCP_CATESP] Tratamiento para categorías esp...</td> <td>[PR.2] Problemas relativos al consentimiento d...</td> <td>[DP]</td> <td>(5,9)</td> <td>(3,1)</td> <td>(2,4)</td> <td>(1,6)</td> </tr> <tr> <td>[DCP_MENORES] Tratamientos relativos a menor...</td> <td>[PR.2] Problemas relativos al consentimiento d...</td> <td>[DP]</td> <td>(5,9)</td> <td>(3,1)</td> <td>(2,4)</td> <td>(1,6)</td> </tr> <tr> <td>[FEMP_01_01] Registro General y Electrónico de...</td> <td>[PR.2] Problemas relativos al consentimiento d...</td> <td>[DP]</td> <td>(5,9)</td> <td>(3,1)</td> <td>(2,4)</td> <td>(1,6)</td> </tr> <tr> <td>[FEMP_03_01] Personal</td> <td>[PR.2] Problemas relativos al consentimiento d...</td> <td>[DP]</td> <td>(5,9)</td> <td>(3,1)</td> <td>(2,4)</td> <td>(1,6)</td> </tr> <tr> <td>[FEMP_01_03] Portal de Transparencia</td> <td>[PR.2] Problemas relativos al consentimiento d...</td> <td>[DP]</td> <td>(5,9)</td> <td>(3,1)</td> <td>(2,4)</td> <td>(1,6)</td> </tr> <tr> <td>[DCP_NORMALES] Tratamientos relativos a datos...</td> <td>[PR.2] Problemas relativos al consentimiento d...</td> <td>[DP]</td> <td>(5,9)</td> <td>(3,1)</td> <td>(2,4)</td> <td>(1,6)</td> </tr> <tr> <td>[DCP_VIDEOVIG] Tratamientos relativos a la vide...</td> <td>[PR.2] Problemas relativos al consentimiento d...</td> <td>[DP]</td> <td>(5,9)</td> <td>(3,1)</td> <td>(2,4)</td> <td>(1,6)</td> </tr> </tbody> </table>	activo	amenaza	dimensión	riesgo	actual	objetivo	ENS	[CPD] Centro de datos	EXT_P@ext > [A.56, core] > [A.56] Retirada de obj...	[C]	(6,3)	(6,3)	(6,3)	(1,3)	[AYT0] Casa consistorial	EXT_P@ext > [A.56, core] > [A.56] Retirada de obj...	[C]	(6,3)	(6,3)	(6,3)	(1,3)	[FEMP_15_01] Web Municipal	[PR.2] Problemas relativos a los derechos del s...	[DP]	(5,9)	(3,1)	(2,6)	(1,6)	[DCP_VIDEOVIG] Tratamientos relativos a la vide...	[PR.2] Problemas relativos a los derechos del s...	[DP]	(5,9)	(3,1)	(2,6)	(1,6)	[FEMP_02_02] Gestión Tributaria	[PR.2] Problemas relativos a los derechos del s...	[DP]	(5,9)	(3,1)	(2,6)	(1,6)	[DCP_MENORES] Tratamientos relativos a menor...	[PR.2] Problemas relativos a los derechos del s...	[DP]	(5,9)	(3,1)	(2,6)	(1,6)	[FEMP_01_01] Registro General y Electrónico de...	[PR.2] Problemas relativos a los derechos del s...	[DP]	(5,9)	(3,1)	(2,6)	(1,6)	[FEMP_03_01] Personal	[PR.2] Problemas relativos a los derechos del s...	[DP]	(5,9)	(3,1)	(2,6)	(1,6)	[DCP_CONDANFIRAC] Tratamientos relativos a co...	[PR.2] Problemas relativos a los derechos del s...	[DP]	(5,9)	(3,1)	(2,6)	(1,6)	[FEMP_02_04] Presupuesto	[PR.2] Problemas relativos a los derechos del s...	[DP]	(5,9)	(3,1)	(2,6)	(1,6)	[FEMP_06_02] Policía Municipal	[PR.2] Problemas relativos a los derechos del s...	[DP]	(5,9)	(3,1)	(2,6)	(1,6)	[DCP_CATESP] Tratamiento para categorías esp...	[PR.2] Problemas relativos a los derechos del s...	[DP]	(5,9)	(3,1)	(2,6)	(1,6)	[FEMP_01_02] Expedientes	[PR.2] Problemas relativos a los derechos del s...	[DP]	(5,9)	(3,1)	(2,6)	(1,6)	[FEMP_02_03] Tesorería	[PR.2] Problemas relativos a los derechos del s...	[DP]	(5,9)	(3,1)	(2,6)	(1,6)	[FEMP_01_04] Licitación Electrónica y Perfil del C...	[PR.2] Problemas relativos a los derechos del s...	[DP]	(5,9)	(3,1)	(2,6)	(1,6)	[FEMP_06_01] Bomberos	[PR.2] Problemas relativos a los derechos del s...	[DP]	(5,9)	(3,1)	(2,6)	(1,6)	[FEMP_01_03] Portal de Transparencia	[PR.2] Problemas relativos a los derechos del s...	[DP]	(5,9)	(3,1)	(2,6)	(1,6)	[DCP_NORMALES] Tratamientos relativos a datos...	[PR.2] Problemas relativos a los derechos del s...	[DP]	(5,9)	(3,1)	(2,6)	(1,6)	[FEMP_02_03] Tesorería	[PR.2] Problemas relativos al consentimiento d...	[DP]	(5,9)	(3,1)	(2,4)	(1,6)	[FEMP_01_02] Expedientes	[PR.2] Problemas relativos al consentimiento d...	[DP]	(5,9)	(3,1)	(2,4)	(1,6)	[DCP_CONDANFIRAC] Tratamientos relativos a co...	[PR.2] Problemas relativos al consentimiento d...	[DP]	(5,9)	(3,1)	(2,4)	(1,6)	[FEMP_02_04] Presupuesto	[PR.2] Problemas relativos al consentimiento d...	[DP]	(5,9)	(3,1)	(2,4)	(1,6)	[FEMP_06_01] Bomberos	[PR.2] Problemas relativos al consentimiento d...	[DP]	(5,9)	(3,1)	(2,4)	(1,6)	[FEMP_01_03] Portal de Transparencia	[PR.2] Problemas relativos al consentimiento d...	[DP]	(5,9)	(3,1)	(2,4)	(1,6)	[FEMP_06_02] Policía Municipal	[PR.2] Problemas relativos al consentimiento d...	[DP]	(5,9)	(3,1)	(2,4)	(1,6)	[FEMP_16_01] Web Municipal	[PR.2] Problemas relativos al consentimiento d...	[DP]	(5,9)	(3,1)	(2,4)	(1,6)	[FEMP_02_02] Gestión Tributaria	[PR.2] Problemas relativos al consentimiento d...	[DP]	(5,9)	(3,1)	(2,4)	(1,6)	[DCP_CATESP] Tratamiento para categorías esp...	[PR.2] Problemas relativos al consentimiento d...	[DP]	(5,9)	(3,1)	(2,4)	(1,6)	[DCP_MENORES] Tratamientos relativos a menor...	[PR.2] Problemas relativos al consentimiento d...	[DP]	(5,9)	(3,1)	(2,4)	(1,6)	[FEMP_01_01] Registro General y Electrónico de...	[PR.2] Problemas relativos al consentimiento d...	[DP]	(5,9)	(3,1)	(2,4)	(1,6)	[FEMP_03_01] Personal	[PR.2] Problemas relativos al consentimiento d...	[DP]	(5,9)	(3,1)	(2,4)	(1,6)	[FEMP_01_03] Portal de Transparencia	[PR.2] Problemas relativos al consentimiento d...	[DP]	(5,9)	(3,1)	(2,4)	(1,6)	[DCP_NORMALES] Tratamientos relativos a datos...	[PR.2] Problemas relativos al consentimiento d...	[DP]	(5,9)	(3,1)	(2,4)	(1,6)	[DCP_VIDEOVIG] Tratamientos relativos a la vide...	[PR.2] Problemas relativos al consentimiento d...	[DP]	(5,9)	(3,1)	(2,4)	(1,6)
activo	amenaza	dimensión	riesgo	actual	objetivo	ENS																																																																																																																																																																																																																																																				
[CPD] Centro de datos	EXT_P@ext > [A.56, core] > [A.56] Retirada de obj...	[C]	(6,3)	(6,3)	(6,3)	(1,3)																																																																																																																																																																																																																																																				
[AYT0] Casa consistorial	EXT_P@ext > [A.56, core] > [A.56] Retirada de obj...	[C]	(6,3)	(6,3)	(6,3)	(1,3)																																																																																																																																																																																																																																																				
[FEMP_15_01] Web Municipal	[PR.2] Problemas relativos a los derechos del s...	[DP]	(5,9)	(3,1)	(2,6)	(1,6)																																																																																																																																																																																																																																																				
[DCP_VIDEOVIG] Tratamientos relativos a la vide...	[PR.2] Problemas relativos a los derechos del s...	[DP]	(5,9)	(3,1)	(2,6)	(1,6)																																																																																																																																																																																																																																																				
[FEMP_02_02] Gestión Tributaria	[PR.2] Problemas relativos a los derechos del s...	[DP]	(5,9)	(3,1)	(2,6)	(1,6)																																																																																																																																																																																																																																																				
[DCP_MENORES] Tratamientos relativos a menor...	[PR.2] Problemas relativos a los derechos del s...	[DP]	(5,9)	(3,1)	(2,6)	(1,6)																																																																																																																																																																																																																																																				
[FEMP_01_01] Registro General y Electrónico de...	[PR.2] Problemas relativos a los derechos del s...	[DP]	(5,9)	(3,1)	(2,6)	(1,6)																																																																																																																																																																																																																																																				
[FEMP_03_01] Personal	[PR.2] Problemas relativos a los derechos del s...	[DP]	(5,9)	(3,1)	(2,6)	(1,6)																																																																																																																																																																																																																																																				
[DCP_CONDANFIRAC] Tratamientos relativos a co...	[PR.2] Problemas relativos a los derechos del s...	[DP]	(5,9)	(3,1)	(2,6)	(1,6)																																																																																																																																																																																																																																																				
[FEMP_02_04] Presupuesto	[PR.2] Problemas relativos a los derechos del s...	[DP]	(5,9)	(3,1)	(2,6)	(1,6)																																																																																																																																																																																																																																																				
[FEMP_06_02] Policía Municipal	[PR.2] Problemas relativos a los derechos del s...	[DP]	(5,9)	(3,1)	(2,6)	(1,6)																																																																																																																																																																																																																																																				
[DCP_CATESP] Tratamiento para categorías esp...	[PR.2] Problemas relativos a los derechos del s...	[DP]	(5,9)	(3,1)	(2,6)	(1,6)																																																																																																																																																																																																																																																				
[FEMP_01_02] Expedientes	[PR.2] Problemas relativos a los derechos del s...	[DP]	(5,9)	(3,1)	(2,6)	(1,6)																																																																																																																																																																																																																																																				
[FEMP_02_03] Tesorería	[PR.2] Problemas relativos a los derechos del s...	[DP]	(5,9)	(3,1)	(2,6)	(1,6)																																																																																																																																																																																																																																																				
[FEMP_01_04] Licitación Electrónica y Perfil del C...	[PR.2] Problemas relativos a los derechos del s...	[DP]	(5,9)	(3,1)	(2,6)	(1,6)																																																																																																																																																																																																																																																				
[FEMP_06_01] Bomberos	[PR.2] Problemas relativos a los derechos del s...	[DP]	(5,9)	(3,1)	(2,6)	(1,6)																																																																																																																																																																																																																																																				
[FEMP_01_03] Portal de Transparencia	[PR.2] Problemas relativos a los derechos del s...	[DP]	(5,9)	(3,1)	(2,6)	(1,6)																																																																																																																																																																																																																																																				
[DCP_NORMALES] Tratamientos relativos a datos...	[PR.2] Problemas relativos a los derechos del s...	[DP]	(5,9)	(3,1)	(2,6)	(1,6)																																																																																																																																																																																																																																																				
[FEMP_02_03] Tesorería	[PR.2] Problemas relativos al consentimiento d...	[DP]	(5,9)	(3,1)	(2,4)	(1,6)																																																																																																																																																																																																																																																				
[FEMP_01_02] Expedientes	[PR.2] Problemas relativos al consentimiento d...	[DP]	(5,9)	(3,1)	(2,4)	(1,6)																																																																																																																																																																																																																																																				
[DCP_CONDANFIRAC] Tratamientos relativos a co...	[PR.2] Problemas relativos al consentimiento d...	[DP]	(5,9)	(3,1)	(2,4)	(1,6)																																																																																																																																																																																																																																																				
[FEMP_02_04] Presupuesto	[PR.2] Problemas relativos al consentimiento d...	[DP]	(5,9)	(3,1)	(2,4)	(1,6)																																																																																																																																																																																																																																																				
[FEMP_06_01] Bomberos	[PR.2] Problemas relativos al consentimiento d...	[DP]	(5,9)	(3,1)	(2,4)	(1,6)																																																																																																																																																																																																																																																				
[FEMP_01_03] Portal de Transparencia	[PR.2] Problemas relativos al consentimiento d...	[DP]	(5,9)	(3,1)	(2,4)	(1,6)																																																																																																																																																																																																																																																				
[FEMP_06_02] Policía Municipal	[PR.2] Problemas relativos al consentimiento d...	[DP]	(5,9)	(3,1)	(2,4)	(1,6)																																																																																																																																																																																																																																																				
[FEMP_16_01] Web Municipal	[PR.2] Problemas relativos al consentimiento d...	[DP]	(5,9)	(3,1)	(2,4)	(1,6)																																																																																																																																																																																																																																																				
[FEMP_02_02] Gestión Tributaria	[PR.2] Problemas relativos al consentimiento d...	[DP]	(5,9)	(3,1)	(2,4)	(1,6)																																																																																																																																																																																																																																																				
[DCP_CATESP] Tratamiento para categorías esp...	[PR.2] Problemas relativos al consentimiento d...	[DP]	(5,9)	(3,1)	(2,4)	(1,6)																																																																																																																																																																																																																																																				
[DCP_MENORES] Tratamientos relativos a menor...	[PR.2] Problemas relativos al consentimiento d...	[DP]	(5,9)	(3,1)	(2,4)	(1,6)																																																																																																																																																																																																																																																				
[FEMP_01_01] Registro General y Electrónico de...	[PR.2] Problemas relativos al consentimiento d...	[DP]	(5,9)	(3,1)	(2,4)	(1,6)																																																																																																																																																																																																																																																				
[FEMP_03_01] Personal	[PR.2] Problemas relativos al consentimiento d...	[DP]	(5,9)	(3,1)	(2,4)	(1,6)																																																																																																																																																																																																																																																				
[FEMP_01_03] Portal de Transparencia	[PR.2] Problemas relativos al consentimiento d...	[DP]	(5,9)	(3,1)	(2,4)	(1,6)																																																																																																																																																																																																																																																				
[DCP_NORMALES] Tratamientos relativos a datos...	[PR.2] Problemas relativos al consentimiento d...	[DP]	(5,9)	(3,1)	(2,4)	(1,6)																																																																																																																																																																																																																																																				
[DCP_VIDEOVIG] Tratamientos relativos a la vide...	[PR.2] Problemas relativos al consentimiento d...	[DP]	(5,9)	(3,1)	(2,4)	(1,6)																																																																																																																																																																																																																																																				

Figura 20 Top 10 resumen (riesgo)

93. De nuevo pueden guardarse cada una de ellas en un fichero CSV, aunque la pestaña “resumen (riesgo)” es con la que se debe trabajar
94. Se recomienda darle un nombre significativo para diferenciar cada caso. Por ejemplo “top_10_ResumenRiesgos.csv” o similar.
95. Revise los valores de riesgo que aparecen en las diferentes tablas. Sobre todo, los que aparecen en “resumen(riesgos)”. Si los valores observados en “objetivo” son superiores a los valores de riesgo que se consideren aceptables se deben aplicar más acciones que permitan reducir estos valores “objetivo” de riesgo.

- 96. Si los valores de los riesgos “objetivo” son adecuados o aceptables, entonces estamos en condiciones de obtener los informes de cumplimiento respecto a los estándares evaluados.
- 97. Para avanzar pulse una vez  para pasar a Informe.
- 98. Si los valores de los riesgos “objetivo” no son adecuados o aceptables, Pilar ofrece sugerencias para mejorar los riesgos.
- 99. Para gestionar los riesgos, debemos volver a la pantalla de los controles del ENS y a la pantalla del RGPD.
- 100. Para ello, debemos pulsar  hasta volver a la pantalla del ENS o la pantalla del RGPD.

5.3.7. Gestionar Riesgos con ENS

- 101. En la pantalla del ENS, en el menú situado en la parte superior de la pantalla, seleccionar “Operación → sugiere”.



Figura 21 Gestionar riesgos con ENS

- 102. Aparece la pantalla del ENS dividida en dos partes. En la superior aparecen las medidas del ENS y en la inferior, aquellas medidas que pueden mejorarse para disminuir los riesgos resultantes. Estas medidas aparecen ordenadas de mayor a menor relevancia.

- 110. Se accede a las sugerencias que ofrece Pilar desde la opción de menú “Operación → sugiere”.
- 111. Actuamos de igual forma que en el caso del ENS. Revisamos las sugerencias y completamos los campos “comentarios” (“actual” y “objetivo”) y la madurez de los campos “actual” y “objetivo”.
- 112. Comprobamos como varían los riesgos hasta que alcanzan los valores adecuados.
- 113. Si se alcanzan los valores adecuados o aceptables, puede avanzar hasta la pantalla de informes.

114. Pulse el botón “guardar”  antes de avanzar  o de retroceder .

5.3.9. Informes

115. A continuación se avanza hacia la pantalla correspondiente a los Informes



Figura 23 Informes

5.3.9.1. Análisis de Riesgos

116. Al seleccionar “Análisis de Riesgos” aparece una ventana de gestión de ficheros:

- Elijamos un nombre significativo para el documento de “Informe de Análisis de Riesgos” para nuestro caso.
- Al pulsar en  aparece una ventana para seleccionar fase o situación de la que queremos el informe de análisis de riesgos

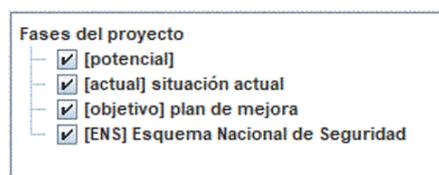
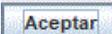


Figura 24 Seleccionar situación del análisis

- Se recomienda seleccionar [actual] y [objetivo]
- Al pulsar en  aparece una ventana de información sobre la creación del documento de Análisis de riesgos que debemos confirmar pulsando de nuevo en el botón de  de dicha ventana.

- En el directorio seleccionado y con el nombre asignado se encontrará el informe de riesgo que tiene el aspecto que se muestra en la siguiente figura.

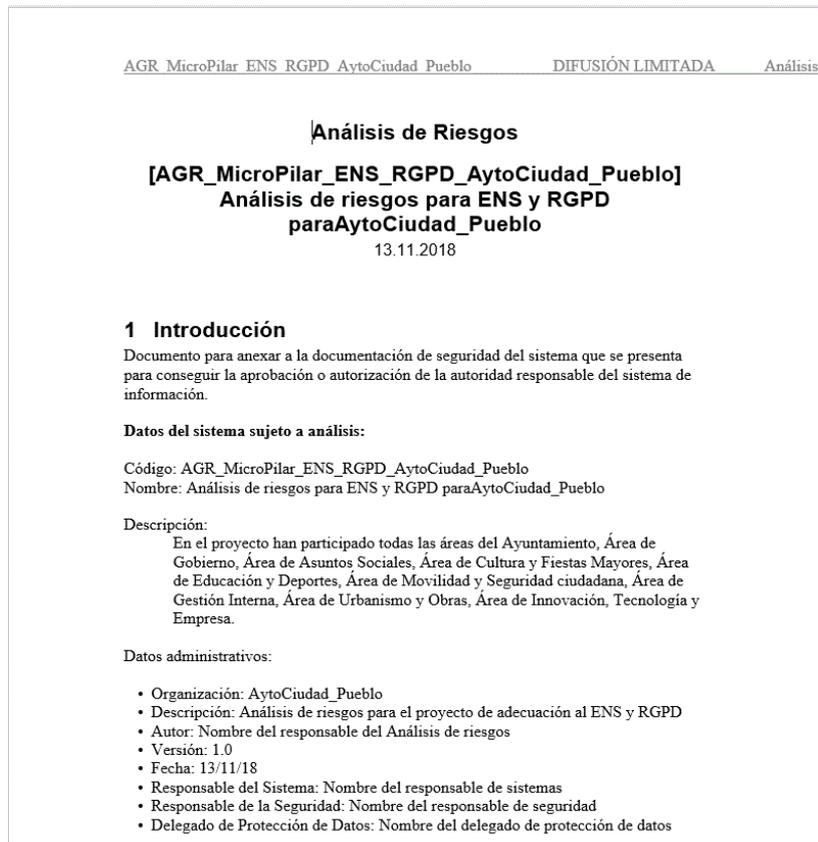


Figura 25 Informe de Análisis de riesgos

- El contenido de este informe es el siguiente:

1. Introducción

1.1. Dimensiones de valoración

2. Dominios de seguridad

2.1. Agravantes y atenuantes

2.2. Valoración de los activos

2.3. Valoración de los dominios

3. Riesgo acumulado

4. Riesgo repercutido

5. Activos

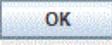
Figura 26 Índice del documento de Análisis de Riesgos

- Regresamos a la ventana de “Informes”.

5.3.9.2. Declaración de Aplicabilidad ENS – Anexo II (2015)

117. Seleccionemos ahora “Declaración de Aplicabilidad ENS – Anexo II (2015)”

118. Como en el caso anterior, aparece una ventana de gestión de ficheros para guardar el informe correspondiente.

119. Elijamos un nombre significativo para el documento de “Declaración de Aplicabilidad” para nuestro caso.
120. Al pulsar en  aparece una ventana de información sobre la creación del documento de declaración de aplicabilidad que debemos confirmar pulsando en el botón de  de dicha ventana.
121. En el directorio seleccionado y con el nombre asignado se encontrará el informe de declaración de aplicabilidad ENS que tiene el aspecto que se muestra en la siguiente figura.

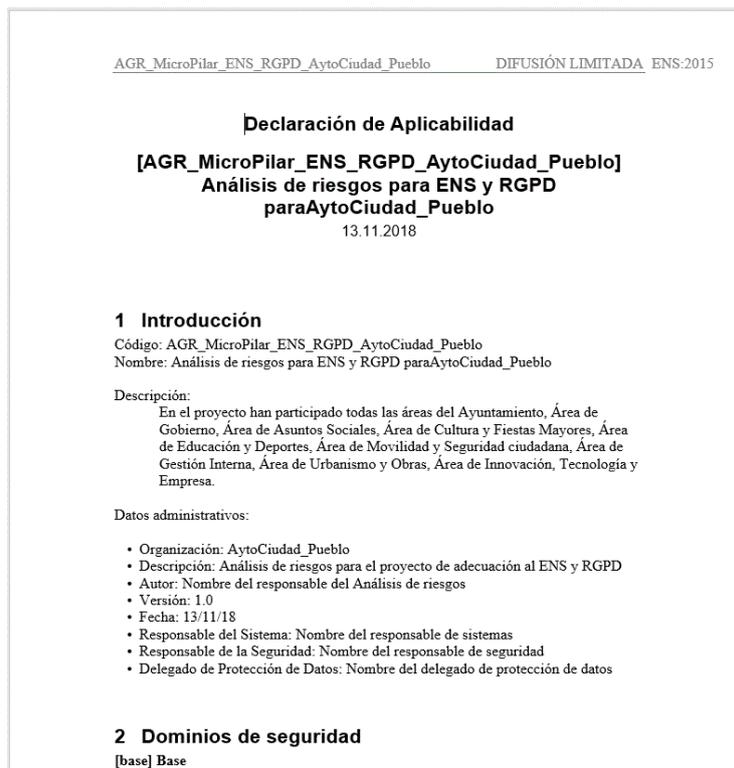


Figura 27 Informe de Declaración de Aplicabilidad

122. El contenido de este informe es el siguiente:

1. Introducción
2. Dominios de seguridad
3. Valoración de los activos
4. Medidas de Seguridad (Anexo II del ENS)
 - 4.1. [org] Marco organizativo
 - 4.2. [op] Marco operacional
 - 4.2.1. [op.pl] Planificación
 - 4.2.2. [op.acc] Control de acceso
 - 4.2.3. [op.exp] Explotación
 - 4.2.4. [op.ext] Servicios externos
 - 4.2.5. [op.cont] Continuidad del servicio
 - 4.2.6. [op.mon] Monitorización del sistema
 - 4.3. [mp] Medidas de protección
 - 4.3.1. [mp.if] Protección de las instalaciones e infraestructuras
 - 4.3.2. [mp.per] Gestión del personal
 - 4.3.3. [mp.eq] Protección de los equipos
 - 4.3.4. [mp.com] Protección de las comunicaciones
 - 4.3.5. [mp.si] Protección de los soportes de información
 - 4.3.6. [mp.sw] Protección de las aplicaciones informáticas (SW)
 - 4.3.7. [mp.info] Protección de la información
 - 4.3.8. [mp.s] Protección de los servicios

Figura 28 Índice del documento de Declaración de Aplicabilidad

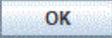
123.Regresamos a la ventana de “Informes”.

5.3.9.3. Valoración del ENS – Anexo II (2015)

124.Seleccionamos ahora “Valoración del ENS – Anexo II (2015)”

125.Como en el caso anterior, aparece una ventana de gestión de ficheros para guardar el informe correspondiente.

126.Elijamos un nombre significativo para el documento de “Valoración ENS” para nuestro caso.

127.Al pulsar en  aparece una ventana de información sobre la creación del documento de declaración de aplicabilidad que debemos confirmar pulsando en el botón de  de dicha ventana.

128.Al pulsar en  aparece una ventana para seleccionar fase o situación de la que queremos el informe Valoración ENS

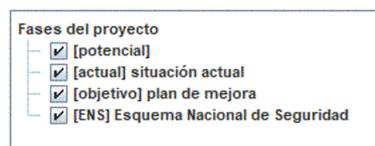


Figura 29 Seleccionar situación de la valoración

129.Se recomienda seleccionar [actual].

130. En el directorio seleccionado y con el nombre asignado se encontrará el informe de Valoración ENS que tiene el aspecto que se muestra en la siguiente figura.

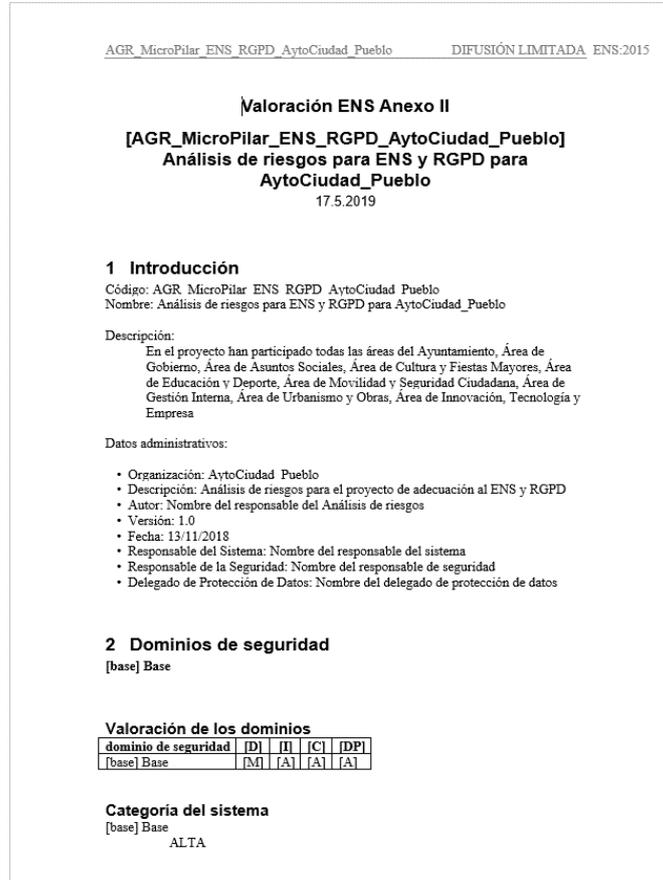


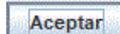
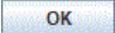
Figura 30 Informe de Valoración ENS

131. El contenido de este informe es el siguiente:

- 1 Introducción**
- 2 Dominios de seguridad**
- 3 Medidas de Seguridad (Anexo II del ENS)**
 - 3.1 **[ora] Marco organizativo**
 - 3.2 **[op] Marco operacional**
 - 3.3 **[op.pl] Planificación**
 - 3.3.1 **[op.acc] Control de acceso**
 - 3.3.2 **[op.exp] Explotación**
 - 3.3.3 **[op.ext] Servicios externos**
 - 3.3.4 **[op.cont] Continuidad del servicio**
 - 3.3.5 **[op.mon] Monitorización del sistema**
 - 3.4 **[mp] Medidas de protección**
 - 3.4.1 **[mp.if] Protección de las instalaciones e infraestructuras**
 - 3.4.2 **[mp.per] Gestión del personal**
 - 3.4.3 **[mp.eq] Protección de los equipos**
 - 3.4.4 **[mp.com] Protección de las comunicaciones**
 - 3.4.5 **[mp.si] Protección de los soportes de información**
 - 3.4.6 **[mp.sw] Protección de las aplicaciones informáticas (SW)**
 - 3.4.7 **[mp.info] Protección de la información**
 - 3.4.8 **[mp.s] Protección de los servicios**

Figura 31 Índice del documento de Valoración ENS

5.3.9.4. Cumplimiento del ENS – Anexo II (2015)

132. Seleccionemos ahora “Cumplimiento del ENS – Anexo II (2015)”
133. Como en el caso anterior, aparece una ventana de gestión de ficheros.
134. Elijamos un nombre significativo para el documento de “Informe de Cumplimiento del ENS” para nuestro caso.
135. Al pulsar en  aparece una ventana para seleccionar fase o situación de la que queremos el informe de cumplimiento ENS.
136. Se recomienda seleccionar [actual] como en anteriores informes.
137. Al pulsar en  aparece una ventana de información sobre la creación del documento de cumplimiento ENS que debemos confirmar pulsando de nuevo en el botón de  de dicha ventana.
138. En el directorio seleccionado y con el nombre asignado se encontrará el informe de cumplimiento del ENS que tiene el aspecto que se muestra en la siguiente figura.

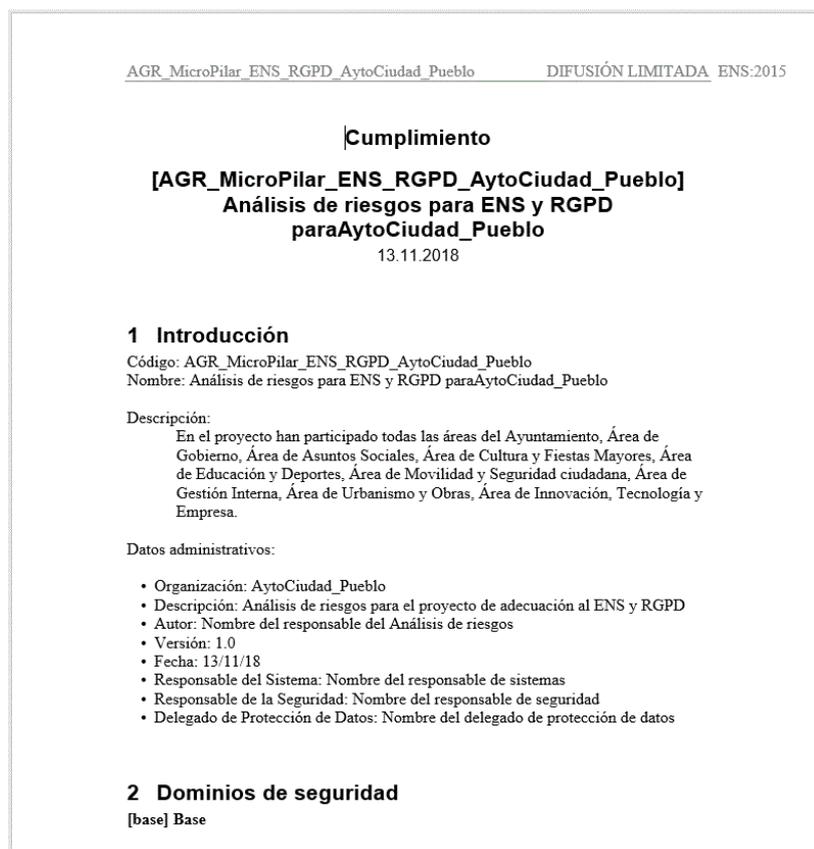


Figura 32 Informe de Cumplimiento del ENS

139. El contenido de este informe es el siguiente:

1	Introducción
2	Dominios de seguridad
3	Medidas de Seguridad (Anexo II del ENS)
3.1	[org] Marco organizativo
3.2	[op] Marco operacional
3.2.1	[op.pl] Planificación
3.2.2	[op.aco] Control de acceso
3.2.3	[op.exp] Explotación
3.2.4	[op.ext] Servicios externos
3.2.5	[op.cont] Continuidad del servicio
3.2.6	[op.mon] Monitorización del sistema
3.3	[mp] Medidas de protección
3.3.1	[mp.if] Protección de las instalaciones e infraestructuras
3.3.2	[mp.per] Gestión del personal
3.3.3	[mp.eq] Protección de los equipos
3.3.4	[mp.com] Protección de las comunicaciones
3.3.5	[mp.si] Protección de los soportes de información
3.3.6	[mp.sw] Protección de las aplicaciones informáticas (S/I)
3.3.7	[mp.info] Protección de la información
3.3.8	[mp.s] Protección de los servicios

Figura 33 Índice del documento de Cumplimiento ENS

140.Regresamos a la ventana de “Informes”.

5.3.9.5. Cumplimiento Reglamento (UE) 2016/679

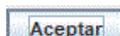
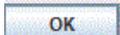
141.Seleccionemos ahora “Cumplimiento Reglamento (UE) 2016/679”

142.Como en el caso anterior, aparece una ventana de gestión de ficheros.

143.Elijamos un nombre significativo para el documento de “Informe de Cumplimiento del Reglamento (UE)” para nuestro caso.

144.Al pulsar en  aparece una ventana para seleccionar fase o situación de la que queremos el informe de cumplimiento RGPD

145.Se recomienda seleccionar [actual] como en informes anteriores.

146.Al pulsar en  aparece una ventana de información sobre la creación del documento de cumplimiento RGPD que debemos confirmar pulsando de nuevo en el botón de  de dicha ventana.

147.En el directorio seleccionado y con el nombre asignado se encontrará el informe de cumplimiento del RGPD que tiene el aspecto que se muestra en la siguiente figura.

AGR_MicroPilar_ENS_RGPD_AytoCiudad_Pueblo

DIFUSIÓN LIMITADA GDPR:2016

Cumplimiento

REGLAMENTO (UE) 2016/679

[AGR_MicroPilar_ENS_RGPD_AytoCiudad_Pueblo] Análisis de riesgos para ENS y RGPD paraAytoCiudad_Pueblo

13.11.2018

1 Introducción

Código: AGR_MicroPilar_ENS_RGPD_AytoCiudad_Pueblo

Nombre: Análisis de riesgos para ENS y RGPD paraAytoCiudad_Pueblo

Descripción:

En el proyecto han participado todas las áreas del Ayuntamiento, Área de Gobierno, Área de Asuntos Sociales, Área de Cultura y Fiestas Mayores, Área de Educación y Deportes, Área de Movilidad y Seguridad ciudadana, Área de Gestión Interna, Área de Urbanismo y Obras, Área de Innovación, Tecnología y Empresa.

Datos administrativos:

- Organización: AytoCiudad_Pueblo
- Descripción: Análisis de riesgos para el proyecto de adecuación al ENS y RGPD
- Autor: Nombre del responsable del Análisis de riesgos
- Versión: 1.0
- Fecha: 13/11/18
- Responsable del Sistema: Nombre del responsable de sistemas
- Responsable de la Seguridad: Nombre del responsable de seguridad
- Delegado de Protección de Datos: Nombre del delegado de protección de datos

2 Dominios de seguridad

Figura 34 Informe de Cumplimiento del RGPD

148.El contenido de este informe es el siguiente:

1	Introducción
2	Dominios de seguridad
2.1	Valoración de los dominios
2.2	Valoración de los activos
3	Reglamento
3.1	Artículo 5 - Principios relativos al tratamiento
3.2	Artículo 6 - Licitud del tratamiento
3.3	Artículo 7 - Condiciones para el consentimiento
3.4	Artículo 8 - Condiciones aplicables al consentimiento del niño en relación con los servicios de la sociedad de la información
3.5	Artículo 9 - Tratamiento de categorías especiales de datos personales
3.6	Artículo 10 - Tratamiento de datos personales relativos a condenas e infracciones penales
3.7	Artículo 11 - Tratamiento que no requiere identificación
3.8	Artículo 12 - Transparencia de la información, comunicación y modalidades de ejercicio de los derechos del interesado
3.9	Artículo 13 - Información que deberá facilitarse cuando los datos personales se obtengan del interesado
3.10	Artículo 14 - Información que deberá facilitarse cuando los datos personales no se hayan obtenido del interesado
3.11	Artículo 15 - Derecho de acceso del interesado
3.12	Artículo 16 - Derecho de rectificación
3.13	Artículo 17 - Derecho de supresión («el derecho al olvido»)
3.14	Artículo 18 - Derecho a la limitación del tratamiento
3.15	Artículo 19 - Obligación de notificación relativa a la rectificación o supresión de datos personales o la limitación del tratamiento
3.16	Artículo 20 - Derecho a la portabilidad de los datos
3.17	Artículo 21 - Derecho de oposición
3.18	Artículo 22 - Decisiones individuales automatizadas, incluida la elaboración de perfiles
3.19	Artículo 24 - Responsabilidad del responsable del tratamiento
3.20	Artículo 25 - Protección de datos desde el diseño y por defecto
3.21	Artículo 26 - Corresponsables del tratamiento
3.22	Artículo 28 - Encargado del tratamiento
3.23	Artículo 29 - Tratamiento bajo la autoridad del responsable o del encargado del tratamiento
3.24	Artículo 30 - Registro de las actividades de tratamiento
3.25	Artículo 31 - Cooperación con la autoridad de control
3.26	Artículo 32 - Seguridad del tratamiento
3.27	Artículo 33 - Notificación de una violación de la seguridad de los datos personales a la autoridad de control
3.28	Artículo 34 - Comunicación de una violación de la seguridad de los datos personales al interesado
3.29	Artículo 35 - Evaluación de impacto relativa a la protección de datos
3.30	Artículo 36 - Consulta previa
3.31	Artículo 37 - Designación del delegado de protección de datos
3.32	Artículo 38 - Posición del delegado de protección de datos
3.33	Artículo 39 - Funciones del delegado de protección de datos
3.34	Artículo 45 - Transferencias basadas en una decisión de adecuación
3.35	Artículo 46 - Transferencias mediante garantías adecuadas
3.36	Artículo 47 - Normas corporativas vinculantes
3.37	Artículo 48 - Transferencias o comunicaciones no autorizadas por el Derecho de la Unión
3.38	Artículo 49 - Excepciones para situaciones específicas

Figura 35 Índice del documento Declaración RGPD

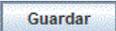
149.Regresamos a la ventana de “Informes”.

5.3.9.6. Recomendaciones

150.Seleccionamos ahora “Recomendaciones”

151.Como en casos anteriores, aparece una ventana de gestión de ficheros para guardar el informe correspondiente.

152.Elijamos un nombre significativo para el documento de Recomendaciones para nuestro caso.

153.Al pulsar en  aparece una ventana para seleccionar la fase o situación de la que queremos el informe de recomendaciones. En este caso, sólo se puede seleccionar una de ellas

154.Se recomienda seleccionar [actual], ya que se trata de mejorar el cumplimiento y riesgos de la situación actual e incorporar esas recomendaciones al plan de mejora.

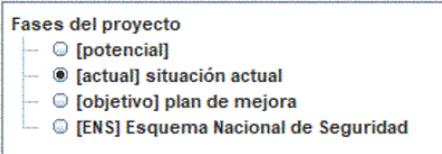
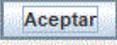
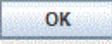


Figura 36 Seleccionar objetivo

155. Al pulsar en  aparece una ventana de información sobre la creación del documento de recomendaciones que debemos confirmar pulsando de nuevo en el botón de  de dicha ventana.

156. En el directorio seleccionado y con el nombre asignado se encontrará el informe de recomendaciones que tiene el aspecto que se muestra en la siguiente figura.

AGR_MicroPilar_ENS_RGPD_AytoCiudad_Pueblo DIFUSIÓN LIMITADA Recomendaciones

Recomendaciones

[AGR_MicroPilar_ENS_RGPD_AytoCiudad_Pueblo] Análisis de riesgos para ENS y RGPD para AytoCiudad_Pueblo

12.12.2018

1 Introducción

Código: AGR_MicroPilar_ENS_RGPD_AytoCiudad_Pueblo
Nombre: Análisis de riesgos para ENS y RGPD para AytoCiudad_Pueblo

Descripción:
En el proyecto han participado todas las áreas del Ayuntamiento, Área de Gobierno, Área de Asuntos Sociales, Área de Cultura y Fiestas Mayores, Área de Educación y Deporte, Área de Movilidad y Seguridad Ciudadana, Área de Gestión Interna, Área de Urbanismo y Obras, Área de Innovación, Tecnología y Empresa

Datos administrativos:

- Organización: AytoCiudad_Pueblo
- Descripción: Análisis de Riesgos para el proyecto de adecuación al ENS y RGPD
- Autor: Nombre del responsable del Análisis de riesgos
- Versión: 1.0
- Fecha: 13/11/18
- Responsable del Sistema: Nombre del responsable de sistemas
- Responsable de la Seguridad: Nombre del responsable de seguridad
- Delegado de Protección de Datos: Nombre del delegado de protección de datos

2 Dominios de seguridad

[base] Base

Valoración de los dominios

dominio de seguridad	[D]	[I]	[C]	[DP]
[base] Base	[M]	[M]	[M]	[M]

Categoría del sistema

[base] Base
MEDIA

12.12.2018
DIFUSIÓN LIMITADA
1 (of 5)

Figura 37 Informe de Recomendaciones

157. El contenido de este informe es el siguiente:

- 1 Introducción
- 2 Dominios de seguridad
- 3 Medidas de seguridad: Anexo II del ENS
- 4 Riesgos legales (RGPD)

Figura 38 Índice del documento Recomendaciones

158. Regresamos a la ventana de “Informes”.

5.3.9.7. INÉS Informe Anual

159. Seleccionemos ahora “INÉS Informe Anual”

160. Como en el caso anterior, aparece una ventana de gestión de ficheros.

161. Elijamos un nombre significativo para el documento de “Informe INÉS” para nuestro caso.

162. Al pulsar en aparece una ventana para seleccionar fase o situación de la que queremos el informe de análisis de riesgos

163. Se recomienda seleccionar [actual]:

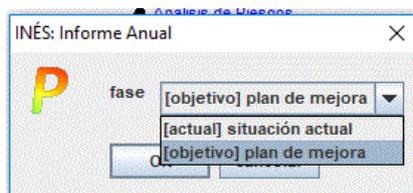


Figura 39 Seleccionar ámbito

- Al pulsar en aparece una ventana de información sobre la creación del documento de Informe Inés que debemos confirmar pulsando de nuevo en el botón de de dicha ventana.
- En el directorio seleccionado y con el nombre asignado se encontrará el informe Inés que tiene el aspecto que se muestra en la siguiente figura.

```

<?xml version="1.0" encoding="UTF-8"?>
- <metrics id="ens">
- <asset code="01" type="is">
  <name>Sede Electrónica</name>
  <value level="M" dimension="D"/>
  <value level="M" dimension="I"/>
  <value level="M" dimension="C"/>
</asset>
- <asset code="02" type="is">
  <name>Economía, Hacienda y Personal</name>
  <value level="M" dimension="D"/>
  <value level="M" dimension="I"/>
  <value level="M" dimension="C"/>
</asset>
- <asset code="03" type="is">
  <name>Contratación y Empleo</name>
  <value level="M" dimension="D"/>
  <value level="M" dimension="I"/>
  <value level="M" dimension="C"/>
</asset>
- <asset code="04" type="is">
  <name>Cultura, Ocio, Educación y Deporte</name>
  <value level="M" dimension="D"/>
  <value level="M" dimension="I"/>
  <value level="M" dimension="C"/>
</asset>
- <asset code="05" type="is">
  <name>Urbanismo</name>
  <value level="M" dimension="D"/>
  <value level="M" dimension="I"/>
  <value level="M" dimension="C"/>
</asset>
- <asset code="06" type="is">
  <name>Consumo y Comercio</name>
  <value level="M" dimension="D"/>
  <value level="M" dimension="I"/>
  <value level="M" dimension="C"/>
</asset>
- <asset code="07" type="is">
  <name>Seguridad</name>
  <value level="M" dimension="D"/>
  <value level="M" dimension="I"/>
  <value level="M" dimension="C"/>
</asset>
- <asset code="08" type="is">
  <name>Salud</name>
  <value level="M" dimension="D"/>
  <value level="M" dimension="I"/>
  <value level="M" dimension="C"/>
</asset>
- <asset code="09" type="is">
  <name>Servicios Sociales</name>
  <value level="M" dimension="D"/>
  <value level="M" dimension="I"/>
  <value level="M" dimension="C"/>
</asset>
- <asset code="10" type="is">
  <name>Medio Ambiente</name>
  <value level="M" dimension="D"/>
  <value level="M" dimension="I"/>
  <value level="B" dimension="C"/>
</asset>
- <asset code="DCP_CATESP" type="it">

```

Figura 40 Contenido Informe Inés

5.3.10. Finalizar y salir

164. Una vez obtenido y salvado todo el trabajo, se puede abandonar la aplicación.

Para ello debe cerrarse pulsando en la  de la esquina superior derecha

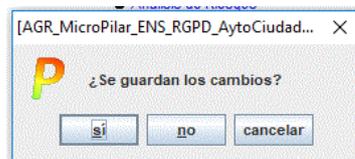


Figura 41 Salvar y salir de Pilar

165. Pulse  para cerrar salvando todas las actividades realizadas. Esto es importante para evitar cualquier pérdida de información y trabajos realizados.

6. PLAN DE TRATAMIENTO DE RIESGOS

166. En este apartado sólo se mostrarán las ayudas que puede ofrecer la información incorporada en la herramienta PILAR para realizar el Análisis de riesgos, en el desarrollo del Plan de Tratamiento de riesgos.
167. Como se indicaba en los apartados 5.3.4 Esquema Nacional de Seguridad y 5.3.5 Reglamento General de Protección de Datos, utilice los comentarios que introdujo a la hora de valorar las medidas/preguntas y artículos/preguntas para definir las acciones que conformarán el Plan de Tratamiento. Estos comentarios (acciones a realizar) se pueden obtener como se indica para el ENS en el punto 82 y para el RGPD en el punto 89.
168. Si ha empleado una nomenclatura específica para documentar las acciones de mejora, ahora puede sacar provecho de ello.
169. Reúna todas las acciones designadas bajo cada uno de los tipos utilizados (“DOC”, “ORG”, “FOR”, “TEC”, ...). Organice las acciones dentro de cada tipo (proyecto), en grupos afines (subproyectos). Por ejemplo, todos los documentos referentes a control de acceso lógico reunirlos en un subproyecto “DOC-1”, los referentes a documentación de las operaciones “DOC-2”, y así en todos los casos hasta completar todas las acciones definidas.
170. Con esta distribución de proyectos, subproyectos y acciones podrá evaluar el resto de información para completar el Plan de Tratamiento:
- Valoración estimativa de cada una de las acciones o conjunto de acciones en recursos internos y coste e inversión externos.
 - Plazo de ejecución y fechas estimativas (calendarización) de cada una de las acciones o conjunto de acciones,
 - Responsables de la ejecución de cada una de las acciones o conjunto de acciones,
 - Los controles (ENS, RGPD) que se mejoran total o parcialmente cada una de las acciones.

7. ANEXO A. REFERENCIAS

CCN-STIC-803 Valoración de sistemas en el Esquema Nacional de Seguridad

CCN-STIC-803. ANEXO II: Valoración de los sistemas en EE.LL.

CCN-STIC-804. ENS. Guía de implantación