TRABAJO FINAL DE MÁSTER

Desarrollo de una guía de controles ciberseguridad para la protección integral en Administraciónes Locales. Adaptación al Esquema Nacional de Seguridad.

José María Botí Hernández

Trabajo Final de Máster: Máster Interuniversitario de Seguridad en las Tecnologías de Información y de las Comunicaciones

Director: Jorge Chinea López
Instituto Nacional de Ciberseguridad (INCIBE)

Fecha: Diciembre 2018

Índice

1. Introducción:

1.1 Contexto y justificación del Trabajo

La ciberseguridad es el área de las tecnologías de la información y las comunicaciones enfocada en la protección de la infraestructura computacional, de la información y de la comunicación de esta.

Debido a que vivimos en la denominada “sociedad de la información” donde las organizaciones públicas y privadas, las personas, las infraestructuras, y multitud de dispositivos estamos interconectados a través de Internet es necesario adoptar medidas de seguridad para proteger la disponibilidad, integridad y confidencialidad de la información. Para conseguir este objetivo en organizaciones públicas y privadas, es necesario adaptar una política de seguridad que nos ayude a mitigar y evitar, en la medida de lo posible, los crecientes riesgos y amenazas.

Por todo ello, y debido al carácter estratégico de la ciberseguridad, en España, se crea el 28 de octubre de 2014 el Instituto Nacional de Ciberseguridad de España (INCIBE). Este instituto es una sociedad dependiente del Ministerio de Economía y Empresa a través de la Secretaría de Estado para el Avance Digital y consolidada como entidad de referencia para el desarrollo de la ciberseguridad y de la confianza digital de ciudadanos, red académica y de investigación, profesionales, empresas y especialmente para sectores estratégicos. INCIBE lidera diferentes actuaciones para la ciberseguridad a nivel nacional e internacional, y entre otras actuaciones, promueve la creación de una serie de guías de controles de ciberseguridad en formato checklist para ayudar al cumplimiento de la política de seguridad en pequeñas y medianas empresas (PYMEs)[1].

Partiendo del éxito de estas guías de controles de ciberseguridad, este Trabajo Fin de Máster pretende realizar una guía de controles de ciberseguridad en formato checklist aplicada a entidades locales, que ayude a las mismas a cumplir sus políticas de seguridad, especialmente las 75 medidas de seguridad recogidas en el Esquema Nacional de Seguridad, regulado por el Real Decreto 3/2010, de 8 de enero, y de obligado cumplimiento en todas las Administraciones Públicas.[2]

El Esquema Nacional de Seguridad (ENS) persigue fundamentar la confianza en que los sistemas de información prestarán sus servicios y custodiarán la información de acuerdo con sus especificaciones funcionales, sin interrupciones o modificaciones fuera de control, y sin que la información pueda llegar al conocimiento de personas no autorizadas. Actualmente existen diversas guías estratégicas del Centro Criptológico Nacional[3] y de la Federación Española de Municipios y Provincias[4], así como herramientas de gestión de riesgos como PILAR[5] o de análisis de características de seguridad

como CLARA[6] que ayudan a preparar a las entidades locales al cumplimiento de las medidas de seguridad recogidas en el ENS, pero para administraciones locales de tamaño pequeño-mediano donde los recursos económicos y de personal técnico de las tecnologías de la información y las comunicaciones son escasos, es muy complejo realizar un seguimiento completo de estas guías.

Por todo ello, este trabajo pretende ser un punto de partida para que una administración local conozca el estado de cumplimiento de su política de seguridad y comenzar la adecuación a dicho Esquema Nacional de Seguridad.

1.2 Objetivos del Trabajo

El objetivo principal del presente trabajo es crear una guía de controles de ciberseguridad para administraciones locales en formato checklist[1] que de forma rápida, directa y realista, permita evaluar el resultado, y realice una comparación del mismo con los requisitos de seguridad de obligado cumplimiento en el Esquema Nacional de Seguridad.

De esta manera, cualquier administración local que aplique dichas guía de controles podrá comenzar la adecuación al ENS de forma rápida y clara, pues conocerá perfectamente su punto de partida y donde debe llegar. Para obtener este objetivo se debe:

- Entender el concepto de riesgo de seguridad en el ámbito de las administraciones públicas y analizar los tipos de amenazas más frecuentes.

- Analizar y entender las medidas de seguridad recogidas en el ENS[2] y que se dividen en: marco organizativo, marco operacional y medidas de protección centradas en activos concretos.

- Comprender el concepto de gestión de riesgos y aplicarlo mediante herramienta PILAR[5] a administraciones locales, pues las competencias de estas están claramente definidas en la Ley 7/1985, de 2 de abril, reguladora de las Bases del Régimen Local[7], y debido a que estas competencias son comunes y parecidas a todas las entidades locales, la aplicación de la gestión de riesgos es bastante uniforme en todas ellas.

- Estudiar y preparar la gestión de los incidentes de seguridad que puedan tener las administraciones locales y que incluye un sistema de detección y reacción frente a código dañino y un registro de los incidentes de seguridad que se produzcan, así como las acciones de tratamiento seguidas.

- Diseñar y elaborar la guía de controles de ciberseguridad para administraciones locales en formato checklist, de forma análoga a las ya realizadas por INCIBE para PYMES[1].

- Exponer las conclusiones del trabajo realizado y acciones futuras que se puedan desprender del presente trabajo.

1.3 Enfoque y metodología

En enfoque y método de seguido para alcanzar los objetivos del presente Trabajo Fin de Máster vienen definidos por las siguientes etapas:

1. **Plan de trabajo**
   El plan de trabajo es el elemento clave que describe detalladamente el problema que se pretende resolver, el trabajo concreto que se llevará a cabo, los objetivos que se quieren alcanzar y la descomposición del trabajo en tareas y metas temporales. Finalmente se enumeran los entregables.

2. **Análisis de las guías de controles de ciberseguridad INCIBE**
   Se estudian en detalle las guías de controles de ciberseguridad editadas en INCIBE a disposición de PYMEs[1], tanto desde el punto de vista técnico, como de estilo, para adecuar el resultado de este Trabajo Fin de Máster a dicho estilo.

3. **Análisis de los riesgos de ciberseguridad más comunes**
   En esta etapa se explica el concepto de riesgo de ciberseguridad y se estudian los riesgos más comunes a cualquier organización pública o privada

4. **Análisis de los riesgos de ciberseguridad y amenazas en administraciones locales**
   Partiendo de la fase anterior, se estudian con detalle los riesgos de ciberseguridad y amenazas más usuales que afectan a administraciones locales, teniendo en cuenta que dichas entidades proporcionan unos servicios parecidos a sus ciudadanos y otras administraciones públicas.

5. **Estudio de las medidas de seguridad del Esquema Nacional de Seguridad**
   En esta fase se analizarán las medidas de seguridad recogidas en el Esquema Nacional de Seguridad[2] y que se dividen en: marco organizativo, marco operacional y medidas de protección centradas en activos concretos. Así mismo en esta etapa se estudiarán otras implicaciones en las administraciones locales que derivan de la adecuación a dicho Esquema.

6. **Analisis de la gestión de riesgos mediante herramienta PILAR**
   Se estudia en PILAR[5], como herramienta EAR (Entorno de Análisis de Riesgos) que siguiendo metodología Magerit[8] (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información) ha sido desarrollada parcialmente por el Centro Criptológico Nacional. En concreto se estudiará la versión µPILAR[5], versión sencilla para PYMES y Administración Local. Una vez estudiada, se realizará un análisis de riesgos común para cualquier Administración Local.

7. **Gestión de los incidentes de ciberseguridad en Administraciones Locales**
   La gestión de los ciberincidentes es una parte muy importante de la ciberseguridad, y por ello, partiendo de la guía de Seguridad de las TIC CCN-STIC 817[3] se realizará un breve análisis de cómo gestionar incidentes de ciberseguridad en Administraciones Locales.

8. **Diseño y elaboración de la guía de controles de ciberseguridad en formato checklist**
   En esta tarea se realiza el diseño y elaboración de la guía de controles de ciberseguridad en formato checklist de forma análoga a las guías ya existentes realizadas por INCIBE para PYMEs. Se trata de una de las fases más importantes de este documento, pues es la aplicación práctica de todas las etapas anteriores.

9. **Conclusiones y trabajo futuro**
   Finalmente, se presentan las conclusiones del trabajo y se identifican las líneas derivadas de este trabajo para estudios futuros, que por su extensión o volumen de trabajo de investigación, no han podido ser tratadas en profundidad.

1.4 Riesgos preliminares

A continuación se identifican los principales riesgos que se han detectado en la primera fase de este trabajo y que pueden afectar a la correcta realización de este trabajo y/o a la planificación temporal del mismo. Para cada riesgo se valora la probabilidad e impacto de la materialización del mismo y se proponen posibles acciones mitigadoras para controlar el mismo.

1. **Sobredimensionamiento del trabajo**

   Inicialmente es el riesgo más preocupante, debido a que se pretende abarcar un ámbito muy grande para la dedicación teórica y calendario previsto.

   Probabilidad / Impacto (1-5): 4 / 5

   Posibles acciones mitigadoras a realizar: simplificar en la medida de lo posible el estudio de las medidas de seguridad y análisis de riesgos del Esquema Nacional de Seguridad; elaboración de una guía de controles de seguridad parcial, dejando para otros trabajos de investigación el resto de guías de controles parciales definidas.

2. **Resultado obtenido demasiado complejo**

   La guía de controles de ciberseguridad en formato checklist obtenida es demasiado compleja para una aplicación sencilla y limitada en el tiempo.

   Probabilidad / Impacto (1-5): 4 / 3

   Posibles acciones mitigadoras a realizar: simplificar en lo posible los controles de ciberseguridad, y si es necesario obviar parcialmente la adaptación al Esquema Nacional de Seguridad[2]; elaboración de una guía de controles de seguridad parcial, dejando para otros trabajos de investigación el resto de guías de controles parciales definidas.

3. **Falta de información**

   Alguno de los temas de estudio o alguna herramienta no está suficientemente documentado.

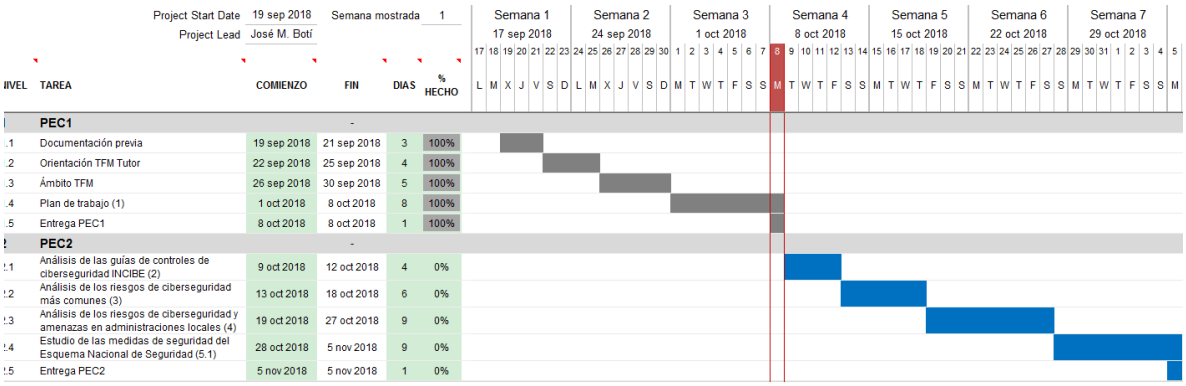
   Probabilidad / Impacto (1-5): 2 / 3

   Posibles acciones mitigadoras a realizar: búsqueda de documentación alternativa como puede ser la legislación europea, incluido el Reglamento General de Protección de Datos[9], herramientas EAR alternativas a PILAR[5], estudio de otras metodologías, casos prácticos, etc.

1.5 Planificación del Trabajo

NIVEL	TAREA	COMIENZO	FIN	DIAS	% HECHO
1	**PEC1**		-		
1.1	Documentación previa	19 sep 2018	21 sep 2018	3	100%
1.2	Orientación TFM Tutor	22 sep 2018	25 sep 2018	4	100%
1.3	Ámbito TFM	26 sep 2018	30 sep 2018	5	100%
1.4	Plan de trabajo (1)	1 oct 2018	8 oct 2018	8	100%
1.5	Entrega PEC1	8 oct 2018	8 oct 2018	1	100%
2	**PEC2**		-		
2.1	Análisis de las guías de controles de ciberseguridad INCIBE (2)	9 oct 2018	12 oct 2018	4	0%
2.2	Análisis de los riesgos de ciberseguridad más comunes (3)	13 oct 2018	18 oct 2018	6	0%
2.3	Análisis de los riesgos de ciberseguridad y amenazas en administraciones locales (4)	19 oct 2018	27 oct 2018	9	0%
2.4	Estudio de las medidas de seguridad del Esquema Nacional de Seguridad (5.1)	28 oct 2018	5 nov 2018	9	0%
2.5	Entrega PEC2	5 nov 2018	5 nov 2018	1	0%
3	**PEC3**		-		
3.1	Continuación estudio de las medidas de seguridad del Esquema Nacional de Seguridad (5.2)	6 nov 2018	11 nov 2018	6	0%
3.2	Analisis de la gestión de riesgos mediante herramienta PILAR (6)	12 nov 2018	25 nov 2018	14	0%
3.3	7. Gestión de los incidentes de ciberseguridad en Administraciones Locales (7)	26 nov 2018	3 dic 2018	8	0%
3.4	Entrega PEC3	3 dic 2018	3 dic 2018	1	0%
4	**PEC4**		-		
4.1	Diseño y elaboración de la guía de controles de ciberseguridad en formato checklist (8)	4 dic 2018	17 dic 2018	14	0%
4.2	Conclusiones y trabajo futuro (9)	18 dic 2018	20 dic 2018	3	0%
4.3	Finalización redaccion memoria	21 dic 2018	28 dic 2018	8	0%
4.4	Repaso memoria y guía	28 dic 2018	31 dic 2018	4	0%
4.5	Entrega PEC4	31 dic 2018	31 dic 2018	1	0%
5	**Presentación Video**		-		
5.1	Preparación video	1 ene 2019	7 ene 2019	7	0%
5.2	Entrega video	7 ene 2019	7 ene 2019	1	0%
6	**Defensa TFM**		-		
6.1	Preparación defensa	8 ene 2019	17 ene 2019	10	0%
6.2	Defensa TFM	18 ene 2019	18 ene 2019	1	0%

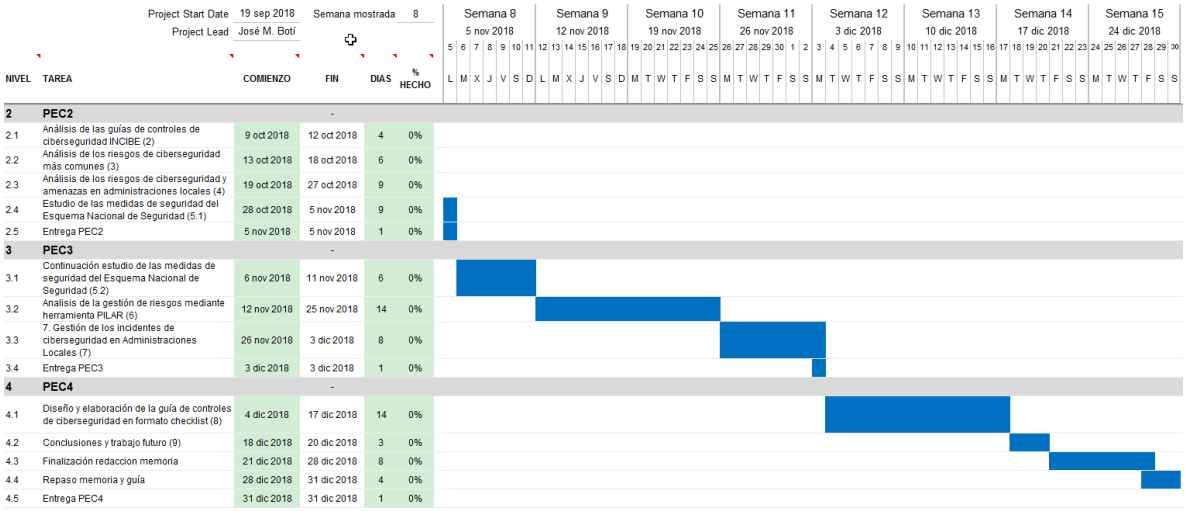
Semana 1-7



Project Start Date 19 sep 2018 | Semana mostrada 1 | Project Lead José M. Botí

NIVEL	TAREA	COMIENZO	FIN	DIAS	% HECHO
	PEC1		-		
.1	Documentación previa	19 sep 2018	21 sep 2018	3	100%
.2	Orientación TFM Tutor	22 sep 2018	25 sep 2018	4	100%
.3	Ámbito TFM	26 sep 2018	30 sep 2018	5	100%
.4	Plan de trabajo (1)	1 oct 2018	8 oct 2018	8	100%
.5	Entrega PEC1	8 oct 2018	8 oct 2018	1	100%
!	**PEC2**		-		
!.1	Análisis de las guías de controles de ciberseguridad INCIBE (2)	9 oct 2018	12 oct 2018	4	0%
!.2	Análisis de los riesgos de ciberseguridad más comunes (3)	13 oct 2018	18 oct 2018	6	0%
!.3	Análisis de los riesgos de ciberseguridad y amenazas en administraciones locales (4)	19 oct 2018	27 oct 2018	9	0%
!.4	Estudio de las medidas de seguridad del Esquema Nacional de Seguridad (5.1)	28 oct 2018	5 nov 2018	9	0%
!.5	Entrega PEC2	5 nov 2018	5 nov 2018	1	0%

Semana 8-15



Project Start Date 19 sep 2018 | Semana mostrada 8 | Project Lead José M. Botí

NIVEL	TAREA	COMIENZO	FIN	DIAS	% HECHO
2	**PEC2**		-		
2.1	Análisis de las guías de controles de ciberseguridad INCIBE (2)	9 oct 2018	12 oct 2018	4	0%
2.2	Análisis de los riesgos de ciberseguridad más comunes (3)	13 oct 2018	18 oct 2018	6	0%
2.3	Análisis de los riesgos de ciberseguridad y amenazas en administraciones locales (4)	19 oct 2018	27 oct 2018	9	0%
2.4	Estudio de las medidas de seguridad del Esquema Nacional de Seguridad (5.1)	28 oct 2018	5 nov 2018	9	0%
2.5	Entrega PEC2	5 nov 2018	5 nov 2018	1	0%
3	**PEC3**		-		
3.1	Continuación estudio de las medidas de seguridad del Esquema Nacional de Seguridad (5.2)	6 nov 2018	11 nov 2018	6	0%
3.2	Análisis de la gestión de riesgos mediante herramienta PILAR (6)	12 nov 2018	25 nov 2018	14	0%
3.3	7. Gestión de los incidentes de ciberseguridad en Administraciones Locales (7)	26 nov 2018	3 dic 2018	8	0%
3.4	Entrega PEC3	3 dic 2018	3 dic 2018	1	0%
4	**PEC4**		-		
4.1	Diseño y elaboración de la guía de controles de ciberseguridad en formato checklist (8)	4 dic 2018	17 dic 2018	14	0%
4.2	Conclusiones y trabajo futuro (9)	18 dic 2018	20 dic 2018	3	0%
4.3	Finalización redaccion memoria	21 dic 2018	28 dic 2018	8	0%
4.4	Repaso memoria y guía	28 dic 2018	31 dic 2018	4	0%
4.5	Entrega PEC4	31 dic 2018	31 dic 2018	1	0%

Semana 16-18

Project Start Date 19 sep 2018 | Semana mostrada 16 | Project Lead José M. Botí

NIVEL	TAREA	COMIENZO	FIN	DIAS	% HECHO
4	**PEC4**		-		
4.1	Diseño y elaboración de la guía de controles de ciberseguridad en formato checklist (8)	4 dic 2018	17 dic 2018	14	0%
4.2	Conclusiones y trabajo futuro (9)	18 dic 2018	20 dic 2018	3	0%
4.3	Finalización redaccion memoria	21 dic 2018	28 dic 2018	8	0%
4.4	Repaso memoria y guía	28 dic 2018	31 dic 2018	4	0%
4.5	Entrega PEC4	31 dic 2018	31 dic 2018	1	0%
5	**Presentación Video**		-		
5.1	Preparación video	1 ene 2019	7 ene 2019	7	0%
5.2	Entrega video	7 ene 2019	7 ene 2019	1	0%
6	**Defensa TFM**		-		
6.1	Preparación defensa	8 ene 2019	17 ene 2019	10	0%
6.2	Defensa TFM	18 ene 2019	18 ene 2019	1	0%

1.6 Breve sumario de productos obtenidos

El Trabajo Final de Máster se divide en los siguientes entregables parciales, que formarán parte del resultado final del proyecto:

- PEC1: Se traba del plan de trabajo, que enmarca y define la realización del proyecto, su ámbito y la previsión temporal de su ejecución.

- PEC2: Se trata de una entrega parcial de los resultados del análisis teórico. Incluye un análisis de amenazas de ciberseguridad, la descripción de los activos de un sistema de información, las dimensiones de valoración de los mismos y las amenazas sobre dichos activos.

- PEC3: Se trata de una entrega parcial de los resultados del análisis de gestión de riesgos en una entidad local según ENS[2] usando µPILAR[5]. Debido a la complejidad del trabajo, se finaliza en la PEC4.

- PEC4: Se finaliza y compila todo el trabajo anterior para generar la memoria final del proyecto que sintetice el trabajo realizado, y se completa con las conclusiones, glosario, bibliografía y anexos.

    - Dentro de esta PEC4 ademas se incluye la guía de controles de ciberseguridad para la protección integral en Administraciones Locales según el ENS, tal y como era objetivo de este Trabajo Final de Máster.

- PEC5: Se trata de una presentación resumen con la voz en off del autor, describiendo el trabajo realizado.

2. Amenazas de ciberseguridad

2.1 Definición y contexto

La información ha sido históricamente un activo estratégico de poder, y por tanto la seguridad de la información una pieza fundamental en cualquier organización que haya necesitado resguardar y proteger su información. Con el paso del tiempo el campo de la seguridad de la información ha crecido y evolucionando declarándose tres principios o propiedades fundamentales:

- **Confidencialidad:** propiedad que impide la divulgación de la información a personas, entidades o procesos no autorizados; sólo los autorizados pueden acceder a la información.

- **Integridad**: principio que asegura que la información no ha sido modificada sin autorización, y por tanto salvaguarda la exactitud, precisión y completitud de la misma. Dentro de esta propiedad multitud de autores incluyen la autentificación, es decir, la identificación del generador de la identificación de formo unívoca.

- **Disponibilidad:** propiedad que asegura que un usuario, entidad o proceso autorizado tenga acceso a la información cuando lo requiera.

Durante siglos la seguridad de la información ha estado incluida dentro de los sistemas de información tradicionales donde la información se guardaba de forma oral o escrita en papiro, pergamino, papel, etc. Debido a la irrupción de las tecnologías de la información y las comunicaciones, dichos sistemas de información se han transformado en sistemas de información informatizados donde la información ha sido introducida, procesada y almacenada en medios informáticos, y actualmente en la era de las comunicaciones transmitida por medios telemáticos.

Este cambio de paradigma ha llevado al nacimiento de la ciberseguridad o seguridad informática que es el área de las tecnologías de la información y las comunicaciones enfocada en la protección de la infraestructura computacional, de la información y de la comunicación de esta.

Una vez que los sistemas de la información se han informatizado casi en su totalidad, y además dichos sistemas de información se han interconectado a través de redes de comunicaciones para que su acceso sea más fácil y rápido, las amenazas de seguridad han aumentado exponencialmente, y por tanto los riesgos de seguridad.

Se entiende por amenaza de seguridad a la violación en potencia que existe a partir de unas circunstancias, capacidad, acción o evento que pueda llegar a causar una infracción de seguridad en el sistema de información informatizado (en adelante por simplicidad, sistema de información).

Las infracciones de seguridad se cometen sobre los activos del sistema, es decir, aquello que tiene algún valor para la organización: datos, servicios, personal, hardware, instalaciones…y se pueden catalogar a partir de los principios básicos antes mencionados; infracción en la confidencialidad de la información, en su integridad o en la disponibilidad de la misma. Dentro de estas amenazas de seguridad se encuentran los famosos ciberataques o ataques informáticos, pero no se debe olvidar que también existen amenazas por incidentes no deliberados o fortuitos, como puede ser una catástrofe natural o un desabastecimiento de energía.

Para que una amenaza de seguridad ocurra, esta debe explotar una vulnerabilidad de la seguridad del sistema de información, es decir, no puede darse un problema de seguridad si no existe un fallo o debilidad en el diseño, implementación, operación o gestión del sistema que pueda ser explotado con el fin de violar la seguridad del mismo, por lo que es muy importante reducir al mínimo posible las vulnerabilidades del sistema.

Una parte importante de la ciberseguridad es evaluar el riesgo asociado a un sistema o servicio concreto, que suele ser directamente proporcional a la existencia de vulnerabilidades y amenazas de seguridad, aunque también viene determinado por la criticidad o gravedad de la vulnerabilidad. El riesgo es una expectativa de pérdida expresada como la probabilidad de que una amenaza explote una vulnerabilidad particular con resultados especialmente perjudiciales. En este punto es importante señalar que debido a la creciente complejidad de sistemas y cantidad de servicios ofertados por dichos sistemas de información resulta imposible en la práctica disponer de un sistema totalmente libre de vulnerabilidades y amenazas, siendo parte fundamental de la seguridad de la información mitigar en lo posible dichos riesgos mediante la adopción de mejoras en los sistemas y contramedidas.

En este capítulo, se van a analizar las amenazas de seguridad informáticos más comunes, focalizando dichas amenazas en administraciones públicas, más concretamente en entidades locales.

2.2 Activos de un sistema de información

El primer paso antes de estudiar las amenazas de un sistema de información, es inventariar y clasificar los activos del sistema que pueden sufrir dichas amenazas. La tipificación de los activos es tanto una información documental como un criterio de reconocimiento de amenazas potenciales y contramedidas adecuadas.

Existen multitud de clasificaciones de activos, desde la más simple que sólo distingue entre infraestructura, servicios y datos hasta clasificaciones más complejas. En este trabajo, al ser un desarrollo de una guía de controles ciberseguridad para la protección integral de Administraciones Locales y adaptación al Esquema Nacional de Seguridad se ha decidido el uso de la clasificación de activos sugerida por MAGERIT 3.0 específicamente publicado para las Administraciones Públicas por el Gobierno de España[8]. La Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de la Administraciones (MAGERIT) cubre la fase de Análisis y Gestión de Riesgos de la Seguridad de un Sistema de Seguridad de la Información y es una metodología basada en la Norma UNE 71504:2008 y que permite cumplir la ISO 27001, una norma internacional que permite el aseguramiento, la confidencialidad e integridad de los datos y de la información, así como de los sistemas que lo procesan.

MAGERIT 3.0 clasifica los tipos de activos en:

- **[essential] Activos esenciales:** datos y servicios esenciales para la supervivencia de la Organización y aquellos datos sometidos a normativa específica de control de acceso y distribución por tener un alto grado de confidencialidad. Dentro de estos activos MAGERIT hace mención especial a los datos de carácter personal pues establecen una serie de obligaciones legales específicas.

- **[arch] Arquitectura del sistema:** elementos que permiten estructurar el sistema, definir su arquitectura interna y sus interconexiones con otros sistemas. Especialmente relevante son los puntos de acceso al servicio donde los requisitos de seguridad del usuario se convierten en obligaciones del prestatario, mientras que los incidentes de seguridad en el proveedor repercuten en el usuario.

- **[D] Datos/información:** la información es un activo que está almacenado en equipos o soportes de información, en forma de archivos o bases de datos normalmente y puede ser transferido por medios telemáticos y/o de copia de datos. Así mismo se incluyen datos de configuración, código fuente, control de acceso, credenciales, registros de actividad, etc.

- **[K] Claves criptográficas:** la criptografía se usa para proteger la información o autenticar a las partes, las claves criptográficas son esenciales para dicha criptografía. En estos activos se incluyen las claves de cifra, firma, las claves de cifrado de comunicaciones, de soporte de la información y los certificados de clave pública.

- **[S] Servicios:** los prestados por el sistema de información. Dentro de los mismos pueden ser de varios tipos: anónimos, públicos, a usuarios externos autenticados, a usuarios internos de la organización, servicios de directorios, de infraestructura de clave pública, de acceso remoto, www, email…

- **[SW] Software:** en este apartado se incluyen las aplicaciones informáticas que gestionan, analizan y transforman los datos permitiendo la explotación de la información para la prestación de servicios. No se incluyen códigos fuente o programas que sean datos de interés comercial, que deben ir incluidos en el epígrafe datos/información. Se subdivide en aplicaciones de desarrollo propio, a medida o estándar, donde están incluidos los sistemas operativos, hipervisores, aplicaciones ofimáticas, navegadores, clientes ftp, email, servidor de ficheros, sistemas gestores de bases de datos, etc.

- **[HW] Hardware:** equipamiento informático, periféricos y equipos de comunicaciones. Dentro del equipamiento informático destacan los grandes equipos (pocos, costosos y de difícil reemplazo), los equipos medios (requerimientos estándar, reemplazo no dificultoso), los equipos personales (muchos, económicos y reemplazables fácilmente), los equipos móviles (portátiles, táblets y smartphone), los de respaldo (preparados para reemplazar inmediatamente equipos en producción) e incluso los equipos virtuales.

- **[COM] Redes de comunicaciones:** medios de transporte de datos, tanto instalaciones dedicadas, como servicios de comunicaciones contratos a terceros: redes telefónicas, LAN, MAN, WAN, puntos a punto, WiFi, radio, satélite, etc.

- **[Media] Soportes de información:** dispositivos físicos que permiten almacenar información de forma duradera en el tiempo. Se pueden divivir en soportes electrónicos (discos, discos virtuales, almacenamiento en red, usb, cintas…) o en no electrónicos como el material impreso.

- **[AUX] Equipamiento auxiliar:** equipos que sirven de soporte a los sistemas de información que no están directamente relacionados con los datos tales como fuentes de alimentación, generadores eléctricos, sistemas de alimentación ininterrumpida, equipos de climatización, cableado, robots de cintas o discos, equipos de destrucción de soportes de información, mobiliario, armarios o cajas de seguridad.

- **[L] Instalaciones:** lugares donde se albergan los sistemas de información y las comunicaciones incluyendo plataformas móviles e instalaciones de respaldo.

- **[P] Personal:** todas las personas relacionadas con los sistemas de información, incluyendo usuarios, operadores, administradores, desarrolladores, subcontratas y proveedores.

Esta clasificación no es exhaustiva, y puede ir cambiando durante la vida del sistema de información. Actualmente algunos autores incluyen dentro de esta clasificación los activos en la nube (pública o privada), como activos que sin ser propiedad de la organización, dan un servicio o albergan datos de esta y que tiene unas amenazas distintas a otros activos que estén albergados en instalaciones propias.

Es importante reseñar que un activo concreto puede pertenecer a más de uno de los tipos vistos, siendo el caso más claro de esto, una base de datos personales que por definición es un activo esencial y que a su vez es un dato.

Por último mencionar que no todos los activos de nuestra organización son físicos y por tanto clasificables bajo estos criterios, sino que según existen activos intangibles que es discutible que sean recursos propiamente dichos del sistema de información, pero que deben ser tenidos en cuenta:

- Credibilidad, reputación o buena imagen.

- Know-how: Habilidades o conocimientos acumulados en los procesos de la organización.

- Independencia de criterio o actuación.

- Integridad física e intimidad de las personas.

2.3 Dimensiones de valoración

Las dimensiones se utilizan para valorar las consecuencias de una materialización de una amenaza que recibe un activo. Parten de las propiedades de los sistemas de información vistas anteriormente (confidencialidad, integridad y disponibilidad), pero MAGERIT 3.0[8] lo completa con dos dimensiones más; autenticidad (que ya se ha visto que puede tratarse dentro de la propiedad de integridad); y trazabilidad que viene derivada de la necesidad legal de tener constancia fehaciente del uso del acceso a los datos.

En términos MAGERIT 3.0 tenemos las siguientes dimensiones:

- **[D] Disponibilidad:** propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren.

- **[I] Integridad:** propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada

- **[C] Confidencialidad:** propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados.

- **[A] Autenticidad:** propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la procedencia de los datos.

- **[T] Trazabilidad:** propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad.

2.4 Amenazas sobre los activos

El catálogo de tipos de amenazas posibles sobre los activos del sistema de información es muy amplio y variado, existiendo múltiples formas de clasificación dependiendo de autores y normas usadas.

Como en puntos anteriores, en este trabajo se ha tomado como referencia MAGERIT 3.0[8] y su catálogo de amenazas. En cada tipo de amenazas se incluye una tabla resumen con identificador, descripción amenaza, origen de la misma, la dimensión y activos afectados según documentación MAGERIT 3.0[8]:

- **[N] Desastres naturales:** sucesos de carácter ambiental que ocurren sin intervención directa de los seres humanos. Afectan a la disponibilidad del sistema. Los más usuales son los de fuego y daños por agua, pero también se incluyen los derivados todo tipo de catástrofes naturales.

	Origen amenaza			Dimensión afectada					Activos afectados											
Amenazas desastres naturales	Natural	Humano accidental	Humano deliberado	D	I	C	A	T	essential	Arch	D	K	S	SW	HW	COM	Media	AUX	L	P
[N.1] Fuego																				
[N.2] Daños por agua																				
N.3 Otras catástrofes																				

- **[I] De origen industrial:** a diferencia de los anteriores, se producen derivados de la actividad humana. Afectan a la disponibilidad del sistema. Este tipo de amenazas pueden darse de forma accidental o intencional. De nuevo se tienen las amenazas por fuego, daños por agua y todo tipo de desastres industriales (explosiones, derrumbes,etc). Además se han de tener en cuenta las amenazas por contaminación mecánica, electromagnética, averías del hardware, cortes de suministro eléctrico, condiciones inadecuadas de temperatura o humedad, fallos de los servicios de telecomunicaciones, interrupción de servicios o suministros esenciales, degradación de los soportes de almacenamiento. También de origen industrial, pero de diferente dimensión se tienen las emanaciones electromagnéticas, que pueden afectar a la confidencialidad mediante la emisión vía radio de datos internos, de forma deliberada o accidental.

	Origen amenaza			Dimensión afectada					Activos afectados											
Amenazas de origen industrial	Entorno Ind.	Humano accidental	Humano deliberado	D	I	C	A	T	essential	Arch	D	K	S	SW	HW	COM	Media	AUX	L	P
[I.1] Fuego																				
[I.2] Daños por agua																				
[I.*] Desastres industriales																				
[I.3] Contaminación mecánica																				
[I.4] Contaminación electromagnética																				
[I.5] Avería de origen físico o lógico																				
[I.6] Corte suministro eléctrico																				
[I.7] Condiciones inadecaudas de temperatura o humedad																				
[I.8] Fallo de servicios de comunicaciones																				
[I.9] Interrupción de otros servicios y suministros esenciales																				
[I.10] Degradación soportes almacenamiento de la información																				
[I.11] Emanaciones electromagnéticas																				

- [**E] Errores y fallos no intencionados:** se producen derivados de la actividad de las personas de forma accidental y pueden afectar tanto a la disponibilidad, como a la integridad, la confidencialidad y la trazabilidad. En esta categoría se clasifican errores de los usuarios y administradores, de monitorización y configuración, deficiencias estructurales de la organización, difusión de software dañino, errores de (re-)encamientamiento de mensajes, de secuencia en el orden de los mensajes transmitidos, alteración accidental de información, destrucción de información, fugas de información, vulnerabilidades del software, errores de mantenimiento/actualización del software y del hardware, caída por agotamiento de recursos, pérdida de equipos e indisponibilidad del personal (por cualquier causa, incluidas catástrofes).

	Origen amenaza			Dimensión afectada					Activos afectados											
Amenazas debidas a errores y fallos no intencionados	Natural/Ind.	Humano accidental	Humano deliberado	D	I	C	A	T	essential	Arch	D	K	S	SW	HW	COM	Media	AUX	L	P
[E.1] Errores de los usuarios																				
[E.2] Errores del administrador																				
[E.3] Errores de monitorización (log)																				
[E.4] Errores de configuración																				
[E.7] Deficiencias en la organización*/**																				
[E.8] Difusión de software dañino																				
[E.9] Errores de (re-) encaminamiento																				
[E.10] Errores de secuencia																				
[E.15] Alteración accidental de la información																				
[E.18] Destrucción de información																				
[E.19] Fugas de información																				
[E.20] Vulnerabilidades de los programas (software)																				
[E.21] Errores de mantenimiento / actualización de programas (software)																				
[E.23] Errores de mantenimiento / actualización de equipos (hardware)																				
[E.24] Caída del sistema por agotamiento de recursos																				
[E.25] Pérdida de equipos																				
[E.28] Indisponibilidad del personal																				

* Esta amenaza está declarada obsoleta según MAGERIT 3.0[8].

** Se observa que la numeración no es consecutiva. Esto es debido a que se quieren relacionar estas amenazas con las amenazas de ataques intencionados y por ello su numeración se entremezcla. Por ejemplo, tenemos la amenaza por error E.03 (errores de monitorización) que coincide numérica con la amenaza por ataque A.03 (manipulación de los registros de actividad).

- **[A] Ataques intencionados:** en este caso, derivados de la actividad intencionada de las personas, y pueden afectar a todas las dimensiones. En este categoría se clasifican amenazas de origen humano y deliberado tales como manipulación de los registros de actividad, manipulación de la configuración, suplantación de la identidad, abuso de privilegios de acceso o uso no previsto. Estas dos últimas amenazas consisten en que un usuario pueda abusar de su nivel de privilegios para realizar tareas que no le incumben o son de competencia, o bien, en el caso del uso no previsto el uso de los recursos para fínes no previstos de carácter personal. Otras amenazas en esta categoría son la difusión de software dañino, errores de (re-)encamientamiento de mensajes, de secuencia en el orden de los mensajes transmitidos, acceso no autorizado, análisis de tráfico, repudio (de origen, recepción o entrega), interceptación de información, modificación deliberada de la información, destrucción de información, divulgación de información, manipulación de programas o equipos, denegación de servicio, robo, ataque destructivo, ocupación enemiga, indisponibilidad del personal, extorsión o ingeniería social, basada en el abuso de la buena fé de las personas para que realicen actividades que beneficien al atacante.

	Origen amenaza			Dimensión afectada					Activos afectados											
Amenazas por ataques intencionados	Natural/Ind.	Humano accidental	Humano deliberado	D	I	C	A	T	essential	Arch	D	K	S	SW	HW	COM	Media	AUX	L	P
[A.3] Manipulación de los registros de actividad (log)																				
[A.4] Manipulación de la configuración																				
[A.5] Suplantación de la identidad del usuario																				
[A.6] Abuso de privilegios de acceso																				
[A.7] Uso no previsto																				
[A.8] Difusión de software dañino																				
[A.9] (Re-)encaminamiento de mensajes																				
[A.10] Alteración de secuencia																				
[A.11] Acceso no autorizado																				
[A.12] Análisis de tráfico																				
[A.13] Repudio																				
[A.14] Interceptación de información (escucha)																				
[A.15] Modificación deliberada de la información																				
[A.18] Destrucción de información																				
[A.19] Divulgación de información																				
[A.22] Manipulación de programas																				
[A.23] Manipulación de los equipos																				
[A.24] Denegación de servicio																				
[A.25] Robo																				
[A.26] Ataque destructivo																				
[A.27] Ocupación enemiga																				
[A.28] Indisponibilidad del personal																				
[A.29] Extorsión																				
[A.30] Ingeniería social (picaresca)																				

Adicionalmente a esta clasificación de amenazas propuesta, MAGERIT 3.0[8] incluye una gramática tipo XML que permite describir nuevos tipos de amenazas y actualizar las existentes de forma periódica.

De las amenazas, las dimensiones y activos afectados se pueden obtener, entre muchas otras, las siguientes conclusiones:

1. MAGERIT 3.0 no utiliza la dimensión Autenticidad en su catálogo de amenazas, por entender que se encuentran dentro de la dimensión Integridad.

2. MAGERIT 3.0 no incluye en su catálogo de amenazas los activos de arquitectura del sistema ni esenciales como activos afectados en ninguna de sus amenazas. Se entiende que en el caso de la arquitectura del sistema por su dificultad para encuadrar este activo como afectado por alguna amenaza, pero en el caso de los activos esenciales, en mi opinión y teniendo en cuenta que las Administraciones Públicas trabajan con multitud de datos de carácter personal, cada vez que un activo de tipo dato se ve afectado por una amenaza, también se ve afecto un activo esencial. Se debe tener en cuenta que en las Administraciones Públicas se trabaja con muchos datos encuadrados en los niveles medio y altos de Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, que, hasta su derogación, sigue conviviendo con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos

3. MAGERIT 3.0 ha declarado obsoleta la amenaza [E.7] Deficiencias en la organización. Peso a ello, en este trabajo se decide mantenerla en el catálogo de amenazas, puesto que en el posterior análisis de riesgos puede convertirse en un riesgo muy importante en una Administración Pública de tamaño pequeño como son las Entidades Locales de menos de 20.000 habitantes. En virtud de lo dispuesto en el Esquema Nacional de Seguridad se recogen multitud de actores principales como el Responsable de Información, el Responsable del Servicio, el Responsable de Seguridad y el Responsable del Sistema que se deben definir correctamente para poder realizar de forma exitosa la adecuación y correcto cumplimiento del ENS[2]. En muchos casos, la escasez de personal al servicio de estas Administraciones Públicas puede llevar a que una sola persona deba asumir varios roles.

4. Dada la cantidad de tipos de amenazas catalogados, un objetivo prioritario del análisis de riesgos en este trabajo debe ser que el número de amenazas analizadas no escale exponencialmente para poder obtener una guía de políticas de seguridad con un checklist con un número de controles asumible.
   Estudiando las guías de políticas de seguridad de INCIBE[1] se ha comprobado que suelen contener alrededor de 10 controles, no superando en ningún caso los 15 controles como ocurre en el checklist de la guía referida al Cumplimiento Legal. Debido a esto, es necesario simplificar al máximo los controles de la guía resultante, y para ello se deberá simplificar en lo posible el análisis de riesgos que se realice con la herramienta PILAR[5] en el próximo PEC3.

3. Análisis de gestión de riesgos en una entidad local según ENS

3.1 Definición y contexto

Como hemos visto anteriormente evaluar el riesgo asociado a un sistema o servicio concreto es una parte muy importante de la ciberseguridad. El riesgo es una expectativa de pérdida expresada como la probabilidad de que una amenaza explote una vulnerabilidad particular con resultados especialmente perjudiciales. Por tanto, analizar los riesgos es identificar los riesgos potenciales y residuales en un sistema de información. Se denomina riesgo a la incertidumbre sobre lo que puede pasar, teniendo en cuenta posibilidades positivas o negativas.

En este punto es importante señalar que debido a la creciente complejidad de sistemas y cantidad de servicios ofertados por dichos sistemas de información resulta imposible en la práctica disponer de un sistema totalmente libre de vulnerabilidades y amenazas, siendo parte fundamental de la seguridad de la información mitigar en lo posible dichos riesgos mediante la adopción de mejoras en los sistemas y contramedidas.

Para ayudar a realizar esta mitigación en todas las Administraciones Públicas el Gobierno de España publicó el Real Decreto 3/2010, de 8 de enero, Esquema Nacional de Seguridad[2], que tiene tiene por objeto determinar la política de seguridad en la utilización de medios electrónicos en su ámbito de aplicación y estará constituido por los principios básicos y requisitos mínimos que permitan una protección adecuada de la información. Posteriormente, la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, recoge el Esquema Nacional de Seguridad en su artículo 156 apartado 2 en similares términos.

En 2015 se publicó la modificación del Esquema Nacional de Seguridad a través del Real Decreto 951/2015, de 23 de octubre[2], en respuesta a la evolución del entorno regulatorio, en especial de la Unión Europea, de las tecnologías de la información y de la experiencia de la implantación del Esquema.

Para realizar el análisis de riesgos según el Esquema Nacional de Seguridad es necesario el uso de una herramienta EAR (Entorno de Análisis de Riesgos) que siguiendo metodología Magerit[8] (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información). El Centro Criptológico Nacional proporciona a las Administraciones Públicas la herramienta PILAR, en su versión completa, y en sus versión simplificada PILAR BASIC y µPILAR, esta última pensada para PYMES y Entidades Locales[5].

3.2 Introducción al Esquema Nacional de Seguridad (ENS)

El Esquema Nacional de Seguridad (ENS)[2], regulado por el Real Decreto 3/2010 , de 8 de enero, determina la política de seguridad que se ha de aplicar en la utilización de los medios electrónicos, y es de aplicación obligatoria en todas las Administraciones Públicas, debiendo por tanto todas ellas realizar la adecuación de sus Sistemas de Información al mismo. El ENS está constituido por los principios básicos y requisitos mínimos para una protección adecuada de la información.

El ENS recoge 75 medidas de seguridad clasificadas según sigue:

- **Marco organizativo:** constituido por 4 medidas relacionadas con la organización global de la seguridad. Las medidas son política de seguridad, normativa de seguridad, procedimientos de seguridad y proceso de autorización.

- **Marco operaciones:** 31 medidas a tomar para proteger la operación del sistema como conjunto integral de componentes para un fin. Se incluyen medidas de planificación, control de acceso, explotación, servicios externos, continuidad del servicio y monitorización del sistema.

- **Medidas de protección**: 41 medidas centradas en la protección de activos concretos, según su naturaleza, con el nivel requerido en cada dimensión de seguridad. Se incluyen medidas respecto a las instalaciones e infraestructuras, gestión del personal, y protección de: equipos, comunicaciones, soportes de información, aplicaciones informáticos, información y servicios.

Y persigue los siguientes objetivos:

- Crear las condiciones necesarias de confianza en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de la información y los servicios electrónicos, que permita a los ciudadanos y a las Administraciones Públicas, el ejercicio de derechos y el cumplimiento de deberes a través de estos medios.

- Establecer la política de seguridad en la utilización de medios electrónicos en el ámbito de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas) y la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, constituyendo los principios básicos y los requisitos mínimos para una protección adecuada de la información.

- Introducir los elementos comunes que han de guiar la actuación de las Administraciones públicas en materia de seguridad de las tecnologías de la información.

- Aportar un lenguaje común para facilitar la interacción de las Administraciones públicas, así como la comunicación de los requisitos de seguridad de la información a la Industria.

- Aportar un tratamiento homogéneo de la seguridad que facilite la cooperación en la prestación de servicios de administración electrónica cuando participan diversas entidades.

- Facilitar un tratamiento continuado de la seguridad.

En el Esquema Nacional de Seguridad[2] se concibe la seguridad como una actividad integral, en la que no caben actuaciones puntuales o tratamientos coyunturales, debido a que la debilidad de un sistema la determina su punto más frágil y, a menudo, este punto es la coordinación entre medidas individualmente adecuadas pero deficientemente ensambladas.

La adecuación ordenada al Esquema Nacional de Seguridad[2] requiere el tratamiento de una serie de cuestiones, cubiertas todas ellas por las guías del Centro Criptológico Nacional de la serie CCN-STIC 800[3] correspondientes al ENS. Para realizar la adecuación se requiere:

- Preparar y aprobar la política de seguridad, incluyendo la definición de roles y la asignación de responsabilidades. Guía CCN-STIC 805[3].

- Categorizar los sistemas atendiendo a la valoración de la información manejada y de los servicios prestados. Guía CCN-STIC 803[3].

- Realizar el análisis de riesgos, incluyendo la valoración de las medidas de seguridad existentes. Mediante uso de MAGERIT[8] y PILAR[5].

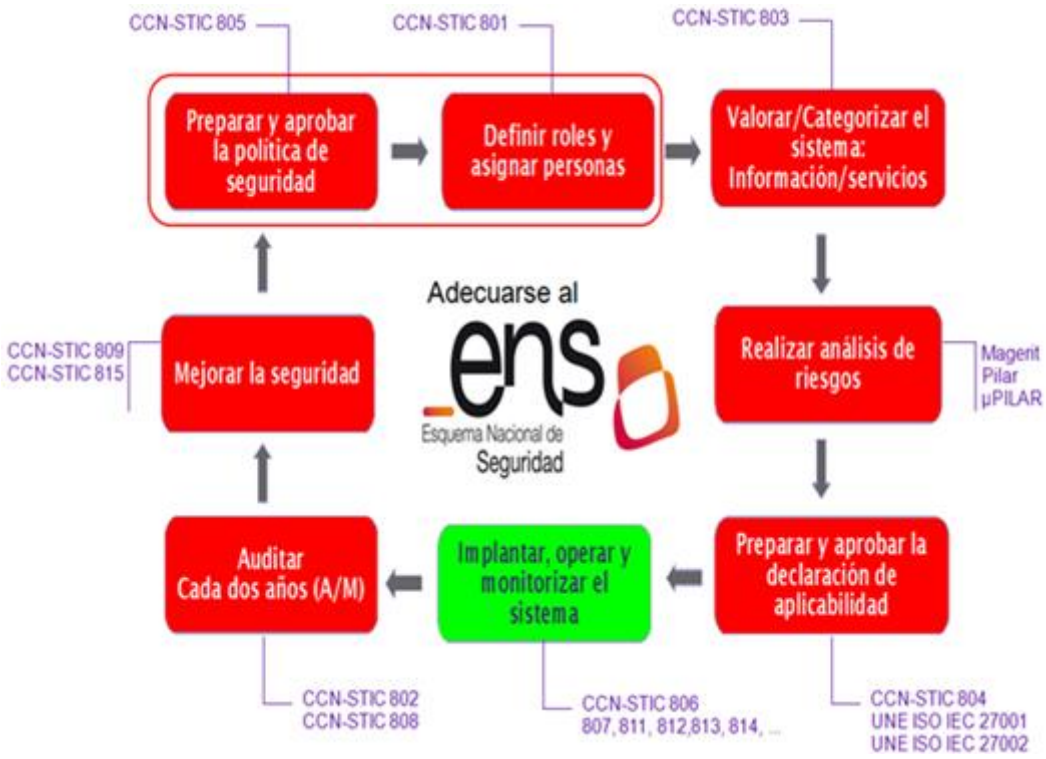
- Preparar y aprobar la Declaración de aplicabilidad de las medidas del Anexo II del ENS. Guía CCN-STIC 804[3]

- Elaborar un plan de adecuación para la mejora de la seguridad, sobre la base de las insuficiencias detectadas, incluyendo plazos estimados de ejecución. Guía CCN-STIC 806[3]

- Implantar operar y monitorizar las medidas de seguridad a través de la gestión continuada de la seguridad correspondiente. Serie completa guías CCN-STIC.

- Auditar la seguridad. Guías CCN-STIC 802 y 808. [3]
- Informar sobre el estado de la seguridad. Guía CCN-STIC 815 y CCNS-STIC 824[3].

FIGURA ADECUACIÓN ENS Y GUÍAS CCN-STIC:



3.3 Análisis de gestión de riesgos mediante µPILAR[5]

3.3.1 La herramienta µPILAR

Debido a que el análisis de riesgos requiere la aplicación de una metodología sistemática que nos permita:

- Identificar el valor que hay que proteger
- Identificar los elementos del sistema que soportan ese valor; es decir, aquellos donde los ataques pueden causar daño.
- Establecer medidas de seguridad para protegernos contra los ataques.
- Estimar indicadores de la posición de riesgo para ayudar a los que tienen que tomar decisiones

El Centro Criptológico Nacional proporciona a las Administraciones Públicas la herramienta PILAR[5], en su versión completa, y en su versión simplificada µPILAR pensada para PYMES y Entidades Locales, que nos permiten realizar el análisis de riesgos en nuestra Entidad Local según el Esquema Nacional de Seguridad, mediante el uso de una herramienta EAR (Entorno de Análisis de Riesgos) que sigue metodología Magerit[3].

µPILAR intenta simplificar en la medida de lo posible la gran complejidad de la realización de un análisis de riesgos y adecuación al ENS[2], mediante la creación de un proyecto que incluye diversas fases y pantallas:

- Introducción de datos del proyecto.
- Activos esenciales y los criterios de valoración que se aplican a los mismos en las dimensiones de valoración MAGERIT: disponibilidad, confidencialidad, autenticidad, integridad y trazabilidad así como una dimensión de valor de vidas humanas y patrimonio corporativo. Desde 2018 y para mayor compatibilidad con el Reglamento General de Protección de Datos de la Unión Europea también añade la dimensión DP: privacidad, consecuencias legales de una violación sobre datos personales.
- Selección del resto de activos no esenciales.
- Identificación de factores agravantes o atenuantes del riesgo según la preselección de µPILAR que pueden suponer una vulnerabilidad.

- Cumplimiento del perfil de seguridad, siendo los perfiles a elegir en la versión 7.2 de µPILAR: ENS:2015, GPDR:2016 y 29151:2017.

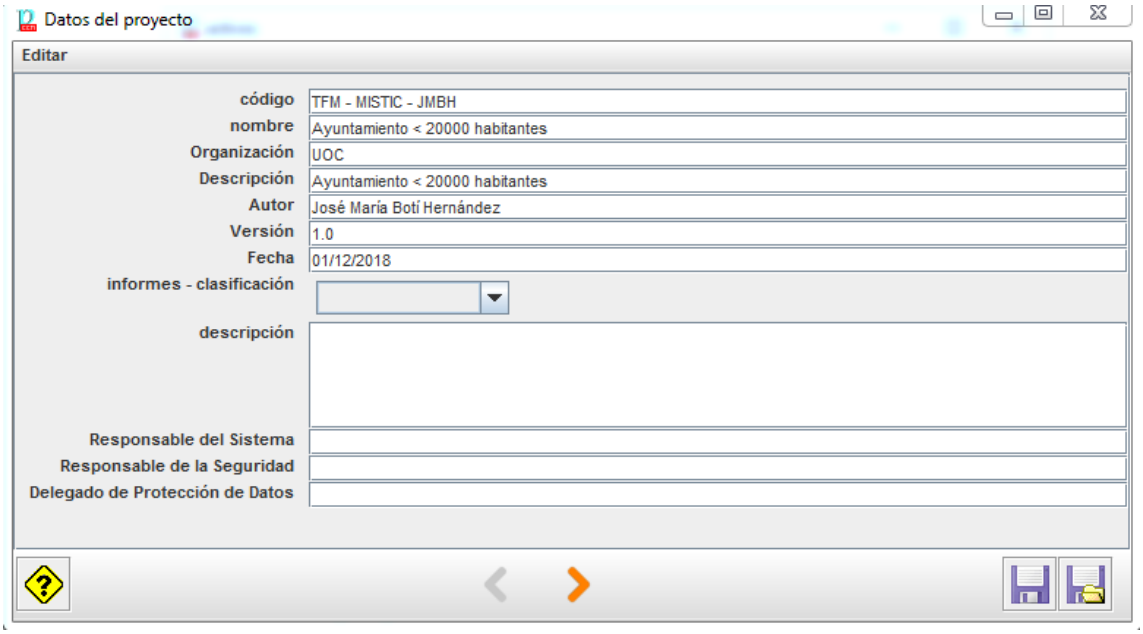
- Visualización de los riesgos derivados del análisis, divididos en riesgo potencia, actual (según la valoración de lo introducido en pantallas anteriores), y objetivo (el que debemos llegar para total cumplimiento ENS).

- Visualización de los mayores riesgos en cada fase, así como un resumen del impacto y el riesgo.

- Informes con resultados finales para exportar en formato RTF.

- Visualización de salvaguardas que pueden aplicarse para limitar el riesgo residual resultante.

Para el uso de cualquier versión de PILAR es necesaria la adquisición de una licencia comercial, excepto las Administraciones Públicas que pueden solicitarla de manera gratuita en el Centro Criptológico Nacional.



3.3.2 Activos esenciales y criterios de valoración

La selección de los activos esenciales y la valoración o nivel de seguridad requerido en todas las dimensiones, es una pieza fundamental del análisis de riesgos. Para una entidad local, el número de activos esenciales puede ser muy grande, y hacer crecer exponencialmente el trabajo de valoración, lo que puede traer como consecuencia un sobredimensionamiento del trabajo y la obtención de un resultado muy complejo y difícil de aplicar tras un largo desarrollo del análisis de riesgos.

En µPILAR[5] el formato de selección de activos esenciales es fijo, requieren un código, y se dividen en cuatro categorías:

- **Activos de información y servicios:** en esta categoría se incluyen todos los activos esenciales de tipo información y servicios, teniendo en cuenta que puede ser útil combinar información y servicios en un único activo.

- **Sistema de protección de frontera lógica:** donde se encuentran las interconexiones con otras redes.

- **Sistema de protección física del perímetro:** activos que se deben proteger de forma física mediante un control de acceso.

- **Servicios contratados a una tercera parte:** servicios subcontratados a terceros.

Comenzando con los activos de información y servicios, se tiene que según el Anexo II: Valoración de los sistemas en Entidades Locales de la Guía CCN-STIC 803, la Federación Española de Municipios y Provincias (FEMP)[4] recoge 49 tipos de información diferentes en una entidad local, que van desde el Registro General hasta los datos de las grabaciones de plenos y actos municipales. Así mismo, en dicho Anexo II se recogen hasta 60 servicios pertenecientes a 15 áreas diferentes, lo que nos llevaría a recoger al menos 109 activos esenciales que deberíamos valorar.

A modo de ejemplo, sólo el subsistema “Servicios Sociales” propuesto por el CCN y la FEMP, explotaría en cinco activos, dos de tipo información: Ayuda a Domicilio-Teleasistencia, y Servicios Sociales; y tres servicios: Asistencia a Domicilio-Teleasistencia, Atención a Colectivos Vulnerables y Violencia de Género. A mayor abundamiento, este subsistema es fácil que pueda aumentar si incluimos más servicios como el Punto de Atención Temprana para niños con dificultades psicomotrices que incluiría dos activos más (información y servicio), u otros servicios como el Centro de Día para personas mayores, etc…sumando, al menos, cuatro activos esenciales más

Dado que cada activo hay que valorarlo en todas sus dimensiones, es fundamental para el desarrollo de una guía de controles abordable para Entidades Locales pequeñas y medianas la agrupación del mayor número de activos esenciales, dejando sólo unos pocos muy representativos que nos sirvan como inicio del proceso de mejora de nuestra ciberseguridad mediante una protección integral y adaptación al ENS[2]. Así mismo, y en beneficio de esta simplificación, la mayor parte de activos se han elegido de tipo información y servicio, obteniéndose finalmente:

- **[Exp] Expedientes/Documentos Ayuntamiento:** Activo de tipo información que incluye expedientes, documentos y datos vitales del Ayuntamiento de cualquier procedimiento, iniciados a instancia de parte o de oficio. Se exceptuan los expedientes de: Personal, Padrón de Habitantes, Datos Contables-Económicos-Financieros, Gestión Tributaria, Servicios Sociales y Seguridad Ciudadana (Policia Local). Por simplificación se incluye el Archivo Único Electrónico según Ley 39/2015.

- **[RGE/RGS] Registro General de Entrada y Salida:** Activo de tipo información que incluye datos y documentos del registro general de entrada y salida.

- **[Personal] Datos y servicios personal:** Activo de tipo información y servicio que integra datos de expedientes de personal, servicio de nóminas, etc.

- **[Intervención] Datos y servicios contables, económicos, financieros y presupuestarios**: Activo de tipo información y servicio que incluye expedientes de intervención y tesorería, así como servicios de contabilidad, facturación, pago, etc.

- **[Tributaria] Datos y servicios de gestión tributaria y recaudación:** Activo de tipo información y servicio que incluye datos y servicios de gestión tributaria y recaudación. Así mismo se incluyen datos de padrones gestionados por el Ayuntamiento: Vados, terrazas, mercados, etc.

- **[PMH] Padrón de Habitantes:** Activo de tipo información y servicio que integra datos y servicios de Padrón Municipal, incluyendo altas, bajas, modificaciones de empadronamientos, emisión de volantes y certificados, etc.

- **[ServSociales] Datos y servicios expedientes Servicios Sociales:** Activo de tipo información y servicio que incluye expedientes de Servicios Sociales. Así mismo dispone de información sensible sobre personas de colectivos vulnerables como menores, tercera edad, movilidad reducida, inmigrantes, personas sin hogar, sin recursos,

drogodependientes, etc. En este caso, dependiendo de la Entidad Local, se puede encontrar externalizado como servicio de las Comunidades Autónomas, aunque en este TFM no se suponga así.

- **[SegCiudadana] Datos y servicios Seguridad Ciudadana**: Activo de tipo información y servicio, que incluye datos, expedientes y servicios usados por la Policía Local en sus tareas de Seguridad Ciudadana y Policía Administrativa. Se incluye video vigilancia de espacios públicos, edificios municipales, base de datos de delitos, vehículos, infracciones de movilidad, etc.

- **[Gestor] Gestor expedientes municipal.** Activo de tipo servicio. Gestor expedientes municipal que permite mediante procesos BPMN acceder a los datos, redactar documentos, realizar firma electrónica, acceder y relacionar datos Registro General Entrada/Salida con expedientes, mandar a archivo, notificar, etc. Se incluye expresamente el acceso al Registro de Entrada, servicio de Registro presencial mediante asiento registral y digitalización de documentación según Esquema Nacional de Interoperabilidad.

- **[Sede electrónica] Tramitación telemática.** Activo de tipo servicio. Se incluye la sede electrónica según Leyes 39 y 40/2015 por tanto incluye: registro telemático, servicio de notificaciones, de verificación de código seguro, carpeta ciudadana, etc. En muchas Entidades Locales pequeñas, al igual que el gestor de expedientes municipales se puede encontrar externalizado en terceros públicos como diputaciones o privados. En este TFM se incluye como servicio propio albergado en nuestro Centro de Proceso de Datos, al igual que el gestor de expedientes municipal.

A estos activos esenciales de tipo información y servicio se han añadido los que considero mínimo imprescindibles:

- **[Firewall] Firewall UTM con DMZ:** De tipo sistema de protección de frontera lógica. Proporciona una barrera perimetral y incluye servicios UTM: antivirus, antispyware, antispam, firewall de red, prevención y detección de intrusiones, filtrado de contenido y prevención de fugas. Se debe configurar una zona desmilitarizada para sede electrónica y otros servicios web.

- **[oficinas] Edificios municipales**: De tipo sistema de protección física de perímetro. Edificios municipales donde se puede acceder al Sistema de Información a través de ordenadores corporativos.

- **[cpd] Centro de Proceso de Datos: De tipo sistema de protección física de perímetro.** Espacio físico cerrado y con acceso restringido donde se encuentran albergados servidores, cabinas de almacenamiento de información y elementos de comunicaciones centrales.

- **[web] Webs corporativas:** Activo contrato a tercero. Web municipal, de turismo y otros servicios que lo requieran. Se puede transformar en un activo de tipo servicio en caso de que lo soporte directamente la Entidad Local.

- **[inet] Conexión a Internet:** Activo contrato a tercero.

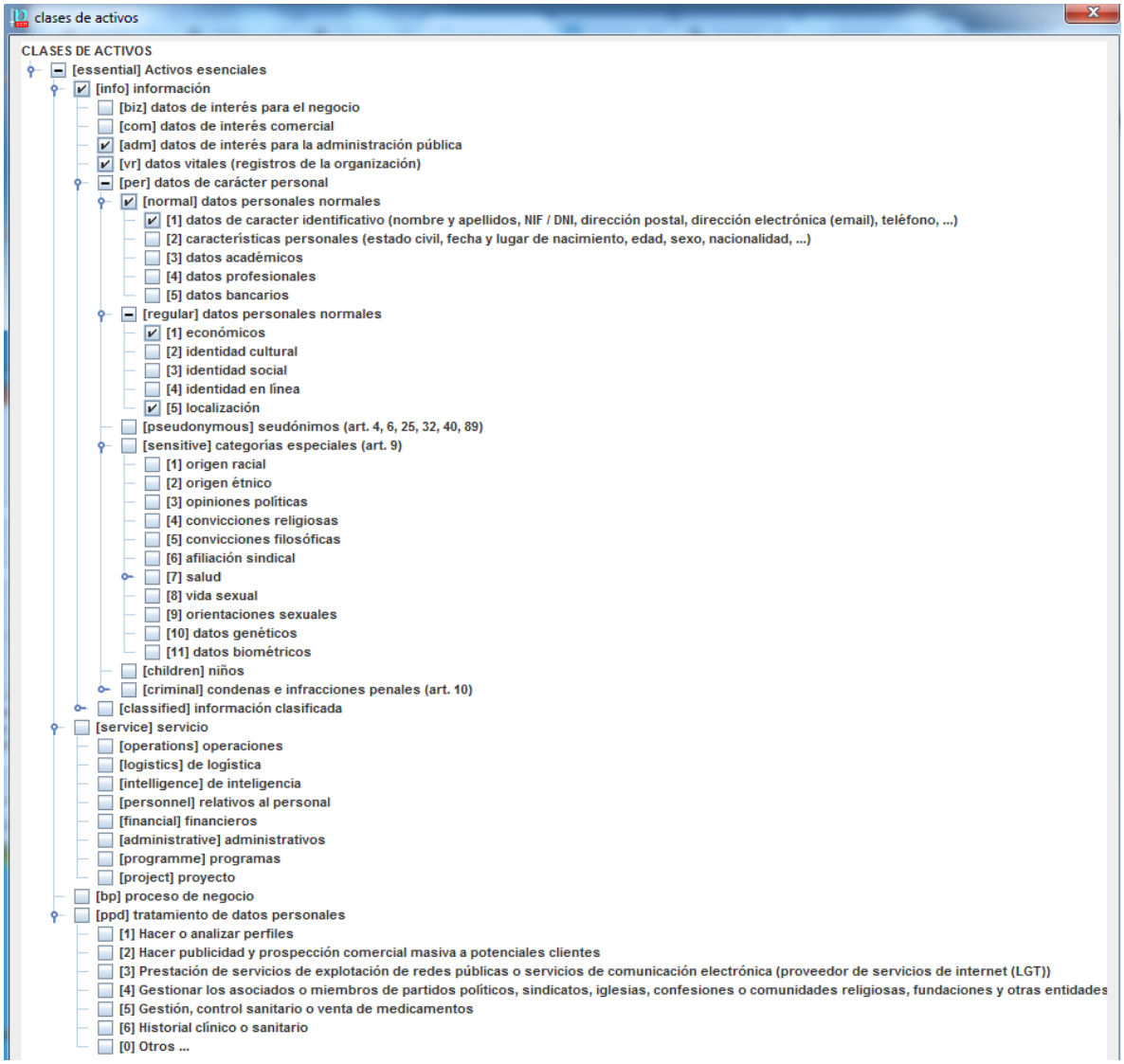
- **[email] Correo electrónico**: Activo contrato a tercero. Se puede transformar en un activo de tipo servicio en caso de que lo soporte directamente la Entidad Local.

Los activos esenciales de personal se han excluido expresamente por razones de simplicidad. En este caso, las Entidades Locales trabajan de forma muy dispar, con funcionarios, funcionarios interinos, personal laboral fijo, personal laboral interino, servicios de personal externalizados, etc, donde además la formación de dicho personal es muy variable, por lo que resulta muy complejo poder realizar un supuesto de Entidad Local. Cada Entidad debe consultar a la Secretaría General y al departamento de Personal como abordar este tipo de activo.

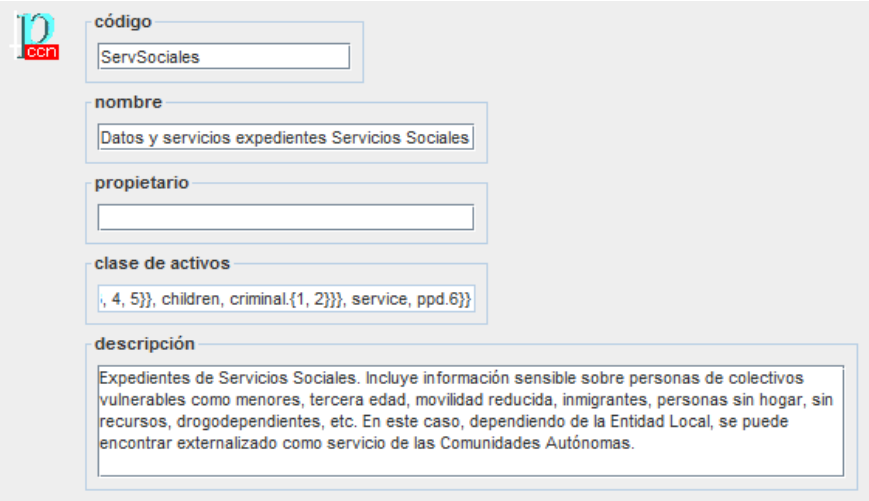
Una vez definidos los activos esenciales de tipo información y/o servicio, se deben clasificar de forma exhaustiva y realizar la valoración de los mismos en todas las dimensiones: disponibilidad, integridad, confidencialidad, autenticidad, trazabilidad y datos personales. La dimensión de valoración de vidas humanas y/o patrimonio corporativo no se va a evaluar en este TFM, pues el mismo CCN[3] no realiza dicha valoración para Entidades Locales. La valoración de los activos de sistema de protección de frontera lógica, física del perímetro y contratados a terceros se realiza de forma automática por µPILAR, y sólo nos permite no aplicar la valoración del riesgo en una dimensión concreta.

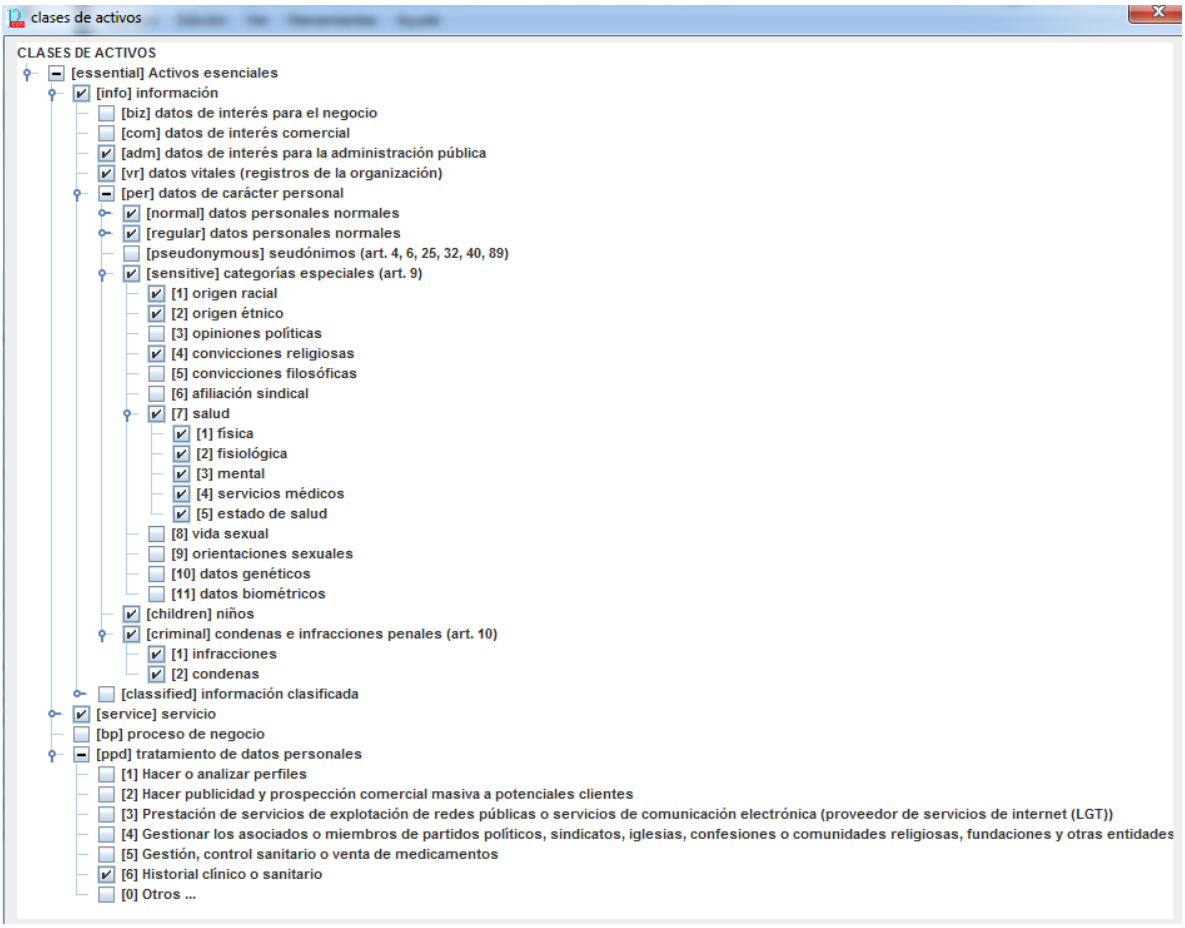
Como ejemplos de la clasificación exhaustiva del tipo de activo esencial de información y/o servicio, se ofrecen dos ejemplos significativos mediante captura de pantalla:

EJEMPLO 1: **[Exp] Expedientes/Documentos Ayuntamiento:**



EJEMPLO 2: **[ServSociales] Datos y servicios expedientes Servicios Sociales:**





Para realizar la valoración de los activos esenciales de tipo información y/o servicio se aplican una serie de criterios que ofrece µPILAR clasificados en distintos grupos de criterios de valoración: integridad, información personal, obligaciones legales, seguridad, intereses económicos, interrupción del servicio, orden público, administración y gestión, pérdida de confianza, persecución de delitos, confidencialidad, disponibilidad de la información, disponibilidad del servicio, trazabilidad de la información, trazabilidad del servicio e información clasificada. Todas las agrupaciones se dividen en criterios altos, medios, bajos y sin valorar, lo que da lugar a que cada dimensión tenga un riesgo asociado, alto, medio, bajo o sin valorar.

Para la aplicación de los criterios de valoración de cada dimensión en este TFM se han tomado cinco decisiones que pueden ser discutidas y revisables.

1. La dimensión de disponibilidad en los activos esenciales de tipo sólo información no se valora, puesto que se incluye dentro de la valoración de la disponibilidad del servicio. Si el servicio no está disponible, la información tampoco, y si la información no está disponible, el servicio asociado tampoco. Para la toma de esta decisión se toma como punto de partida ejemplos de valoración de sistemas en Entidades Locales del CCN.

2. Las dimensiones de integridad y confidencialidad en los activos esenciales de tipo sólo servicio no se valoran, dado que son dimensiones que por simplicidad se asume que sólo afectan a la información no al servicio que la ofrece y/o manipula. Para la toma de esta decisión se toma como punto de partida ejemplo del CCN.

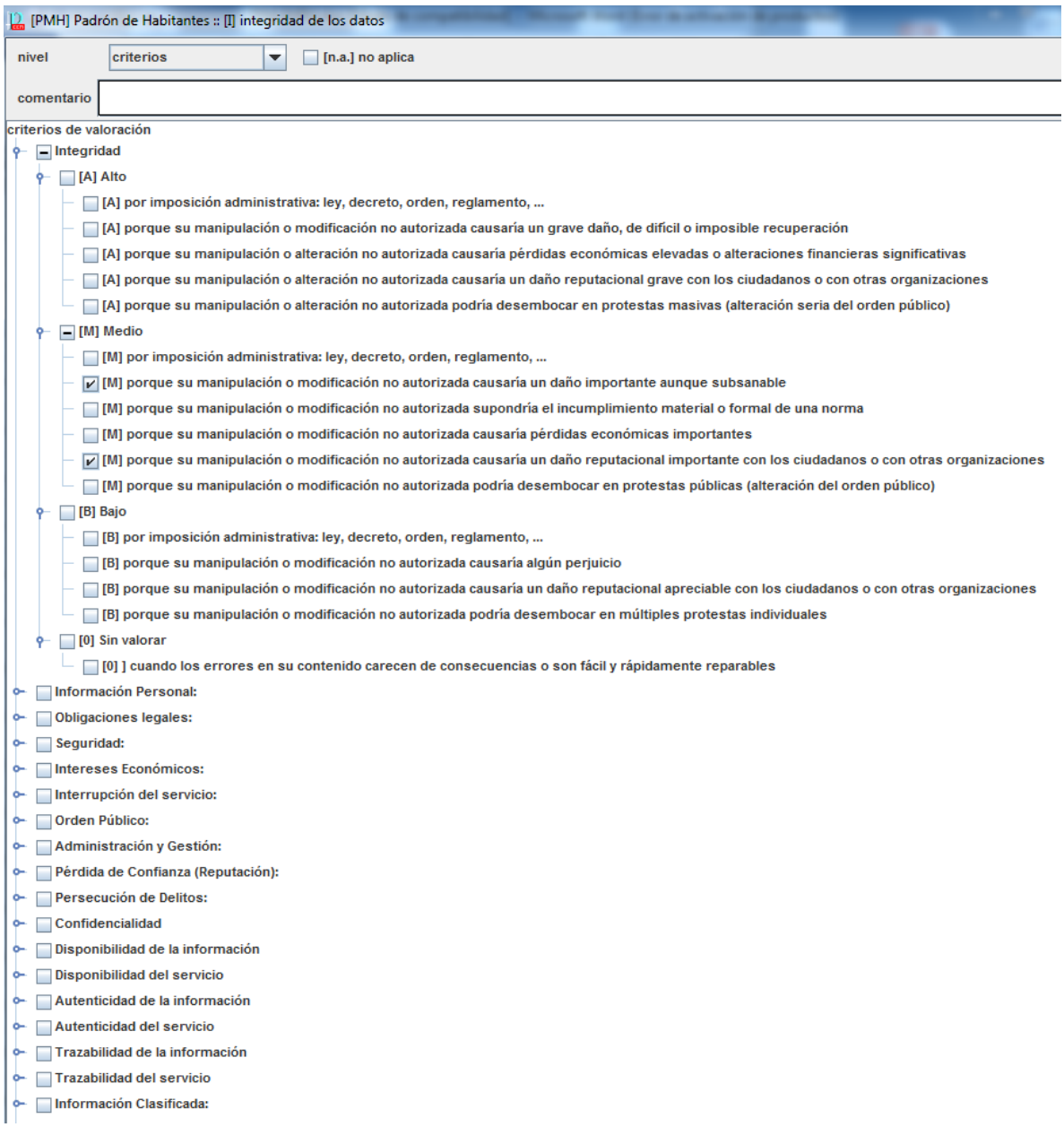
3. Las dimensiones de autenticidad y trazabilidad se valoran en todos los activos esenciales, incluyendo los de sólo servicio puesto que este autor entiende que es importante valorar la autenticidad de un servicio, y la trazabilidad de lo que cada usuario realiza sobre este servicio. Esto es contrario a lo que el CCN muestra en sus ejemplos, pero este autor considera que la Trazabilidad o Autenticidad en un servicio de Sede Electrónica es muy importante, ya que en un momento dado es necesario saber que ha hecho y visualizado un usuario concreto, o es necesario Autenticar al servicio y/o al usuario.

4. Como ya se ha comentado anteriormente la dimensión de valor de vidas humanas o patrimonio no se valora, por no considerarse necesario y derivar en más complejidad innecesaria.

5. La aplicación de los criterios de valoración respecto a los datos personales, se han aplicado exclusivamente en la dimensión [DP] de datos personales en los activos de tipo información o información y servicio. Por simplicidad, claridad, y evitar desproporcionalidad en las medidas resultantes no se aplican criterios de datos personales en el resto de dimensiones.

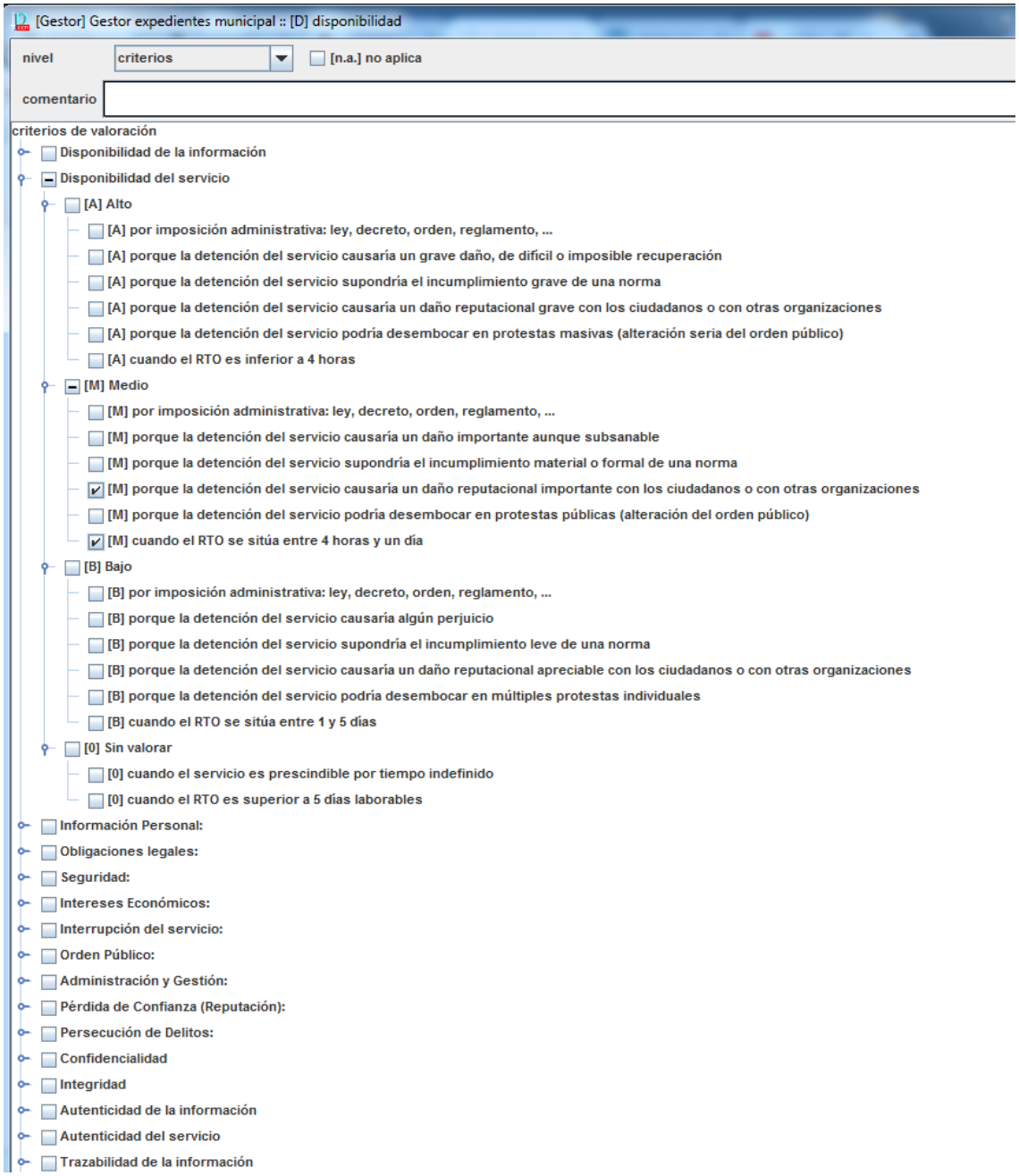
Se ofrecen tres ejemplos explicados y significativos mediante captura de pantalla de valoración de una dimensión de un activo esencial concreto:

EJEMPLO 1: **[PMH] Padrón de Habitantes - [I] Integridad:**



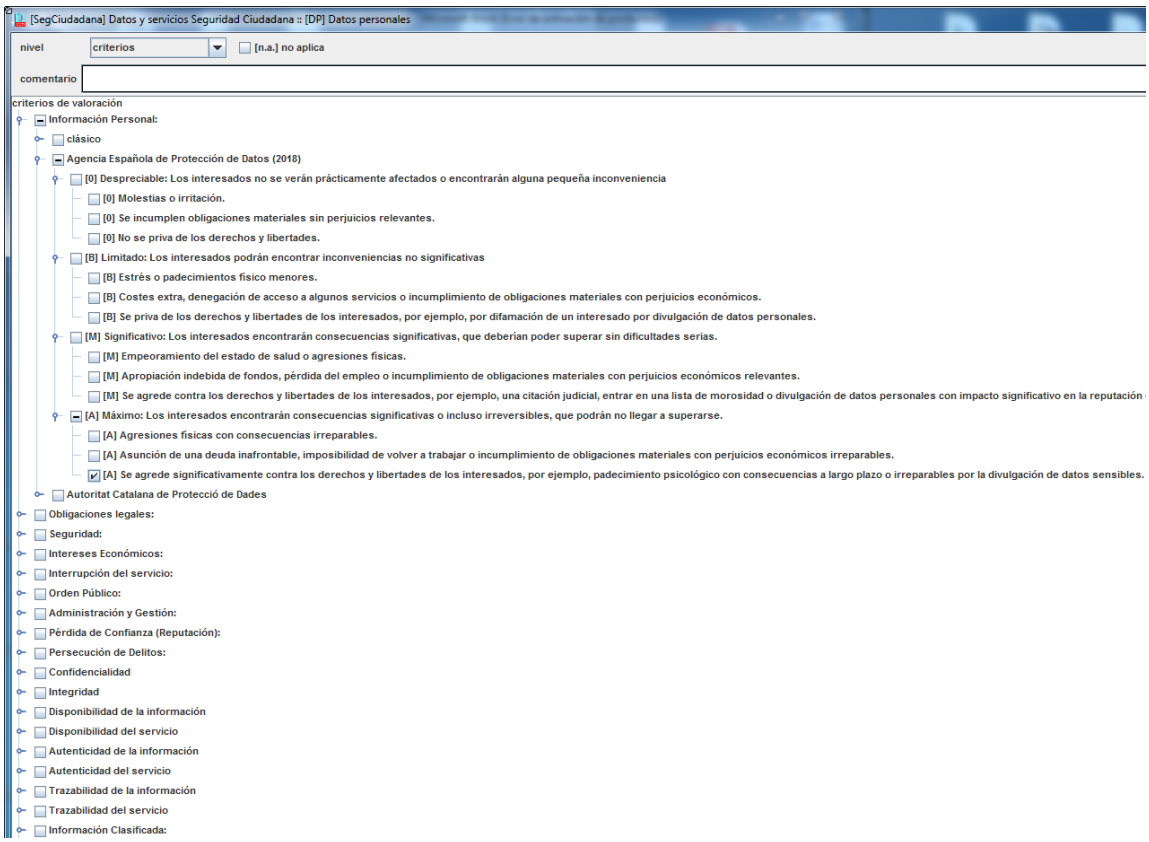
De todos los criterios de valoración, nos centramos en la integridad de los datos, y se han seleccionado dos criterios de grado medio, puesto que se ha considerado que una alteración de los datos de forma no autorizada podría causar un daño importante aunque subsanable a los ciudadanos, y además un daño reputacional para la Entidad Local importante.

EJEMPLO 2: **[Gestor] Gestor expedientes municipal - [D] Disponilidad:**



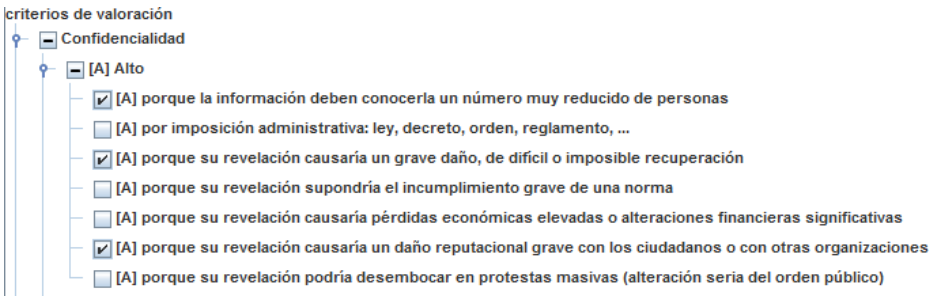
De todos los criterios de valoración, nos centramos en la disponibilidad del servicio, y se han seleccionado dos criterios de grado medio, puesto que se ha considerado que al ser un servicio muy importante del Ayuntamiento que da acceso a multitud de expedientes y su documentación la detención puede suponer un daño reputaciones importante e incluso que procedimientos administrativos con plazos sean seriamente afectados. Es importante valorar la disponibilidad de forma cuantitativa respecto al tiempo máximo admisible que puede no estar disponible el servicio, y se ha estimado que no puede ser en ningún caso mayor de un día, si bien se puede admitir que sea de más de cuatro horas, lo que da lugar a la aplicación de un criterio de grado medio.

EJEMPLO 3: **[SegCiudadana] Datos y servicios Seguridad Ciudadana - [DP] Datos Personales:**

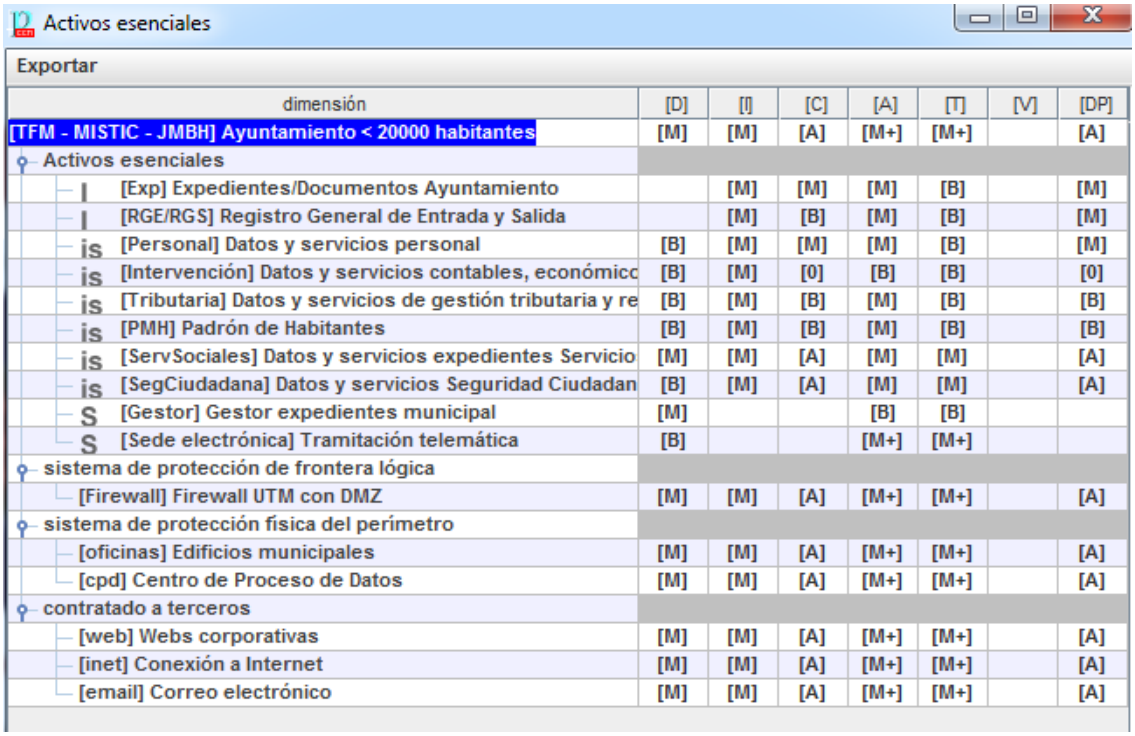


En este caso, y tal y como se ha valorado anteriormente, nos centramos en los criterios de valoración de información personal, y más concretamente en los de la Agencia Española de Protección de Datos de 2018. Una vez revisados todos los criterios, este autor entiende que una fuga o alteración de información como la que incluye Seguridad Ciudadana de penas y restricciones de libertad, puede agredir significativamente contra los derechos y libertades de un interesado, incluyendo daños irreparables en su reputación por la divulgación de estos datos sensibles.

De esta manera, se obtiene una valoración alta del riesgo en esta dimensión, al igual que en dimensión Confidencialidad para este activo como describe la siguiente captura:



Una vez realizadas todas las valoraciones, y que podemos encontrar en los informes finales de µPILAR que se encuentran como anexos a este documento, tenemos la siguiente valoración resumida en la siguiente captura de pantalla, donde en la primera fila vemos el resultado global de una Entidad Local de menos de 20000 habitantes:


Activos esenciales

Exportar

dimensión	[D]	[I]	[C]	[A]	[T]	[V]	[DP]
[TFM - MISTIC - JMBH] Ayuntamiento < 20000 habitantes	[M]	[M]	[A]	[M+]	[M+]		[A]
Activos esenciales							
[Exp] Expedientes/Documentos Ayuntamiento		[M]	[M]	[M]	[B]		[M]
[RGE/RGS] Registro General de Entrada y Salida		[M]	[B]	[M]	[B]		[M]
[Personal] Datos y servicios personal	[B]	[M]	[M]	[M]	[B]		[M]
[Intervención] Datos y servicios contables, económicc	[B]	[M]	[0]	[B]	[B]		[0]
[Tributaria] Datos y servicios de gestión tributaria y re	[B]	[M]	[B]	[M]	[B]		[B]
[PMH] Padrón de Habitantes	[B]	[M]	[B]	[M]	[B]		[B]
[ServSociales] Datos y servicios expedientes Servicio	[M]	[M]	[A]	[M]	[M]		[A]
[SegCiudadana] Datos y servicios Seguridad Ciudadan	[B]	[M]	[A]	[M]	[M]		[A]
[Gestor] Gestor expedientes municipal	[M]			[B]	[B]		
[Sede electrónica] Tramitación telemática	[B]			[M+]	[M+]		
sistema de protección de frontera lógica							
[Firewall] Firewall UTM con DMZ	[M]	[M]	[A]	[M+]	[M+]		[A]
sistema de protección física del perímetro							
[oficinas] Edificios municipales	[M]	[M]	[A]	[M+]	[M+]		[A]
[cpd] Centro de Proceso de Datos	[M]	[M]	[A]	[M+]	[M+]		[A]
contratado a terceros							
[web] Webs corporativas	[M]	[M]	[A]	[M+]	[M+]		[A]
[inet] Conexión a Internet	[M]	[M]	[A]	[M+]	[M+]		[A]
[email] Correo electrónico	[M]	[M]	[A]	[M+]	[M+]		[A]

3.3.3 Activos no esenciales

En la siguiente pantalla del proyecto, µPILAR[5], nos pide los activos no esenciales de nuestro Sistema de Información, y para ello nos ofrece una lista desplegable de los mismos, clasificados tal y como vimos en la sección 2.2 de este TFM.

En concreto, para una Entidad Local tipo de menos de 20000 habitantes se han elegido los siguientes activos no esenciales:

[D] Datos / Información:

- [D.files] ficheros de datos
- [D.e-files] ficheros cifrados
- [D.backup] copias de respaldo
- [D.conf] datos de configuración
- [D.int] datos de gestión interna
- [D.password] credenciales (ej. contraseñas)
- [D.acl] datos de control de acceso
- [D.log] registro de actividad (log)
- [D.multimedia] multimedia
- [D.source] código fuente
- [D.exe] código ejecutable
- [keys] Claves criptográficas
- [keys.info.encrypt] claves de cifra
- [keys.info.sign] claves de firma
- [keys.com.channel] claves de cifrado del canal
- [keys.com.authentication] claves de autenticación
- [keys.x509] certificados de clave pública

[S] Servicios:

- [S.prov.pub] al público en general (sin relación contractual)
- [S.prov.int] interno (usuarios y medios de la propia organización)
- [S.prov.www] world wide web
- [S.prov.file] almacenamiento de ficheros
- [S.prov.print] servicio de impresión
- [S.prov.pki.ra] autoridad de registro

[SW] Aplicaciones (software):

- [SW.prp] desarrollo propio (in house)
- [SW.sub] desarrollo a medida (subcontratado)
- [SW.std.browser] navegador web
- [SW.std.www] servidor de presentación
- [SW.std.app] servidor de aplicaciones
- [SW.std.email_client] cliente de correo electrónico
- [SW.std.email_server] servidor de correo electrónico
- [SW.std.directory] servidor de directorio
- [SW.std.file] servidor de ficheros
- [SW.std.dbms] sistema de gestión de bases de datos
- [SW.std.office] ofimática
- [SW.std.os] sistema operativo
- [SW.std.os.windows] windows

- [SW.std.os.linux] linux
- [SW.std.hypervisor] hypervisor (gestor de la máquina virtual)
- [SW.std.backup] servidor de backup
- [SW.sec.av] anti virus
- [SW.sec.ids] IDS / IPS (deteción / prevención de intrusion)
- [SW.sec.dlp] prevención de pérdida de datos
- [SW.sec.traf] análisis de tráfico
- [SW.sec.hp] honey pot

[HW] Equipamiento informático (hardware):
- [HW.mid] equipos medios
- [HW.pc] informática personal
- [HW.mobile] informática móvil
- [HW.vhost] equipos virtuales (máquinas virtuales)
- [HW.backup] equipamiento de respaldo
- [HW.data] que almacena datos
- [HW.network.switch] conmutador
- [HW.network.router] encaminador
- [HW.network.wap] punto de acceso wireless

[COM] Redes de comunicaciones:
- [COM.ADSL] ADSL
- [COM.wifi] WiFi
- [COM.LAN] red local
- [COM.VLAN] LAN virtual
- [COM.vpn] canal cifrado (red privada virtual)
- [COM.backup] comunicaciones de respaldo

[Media] Soportes de información:
- [Media.electronic.disk] discos
- [Media.electronic.vdisk] discos virtuales
- [Media.electronic.san] almacenamiento en red

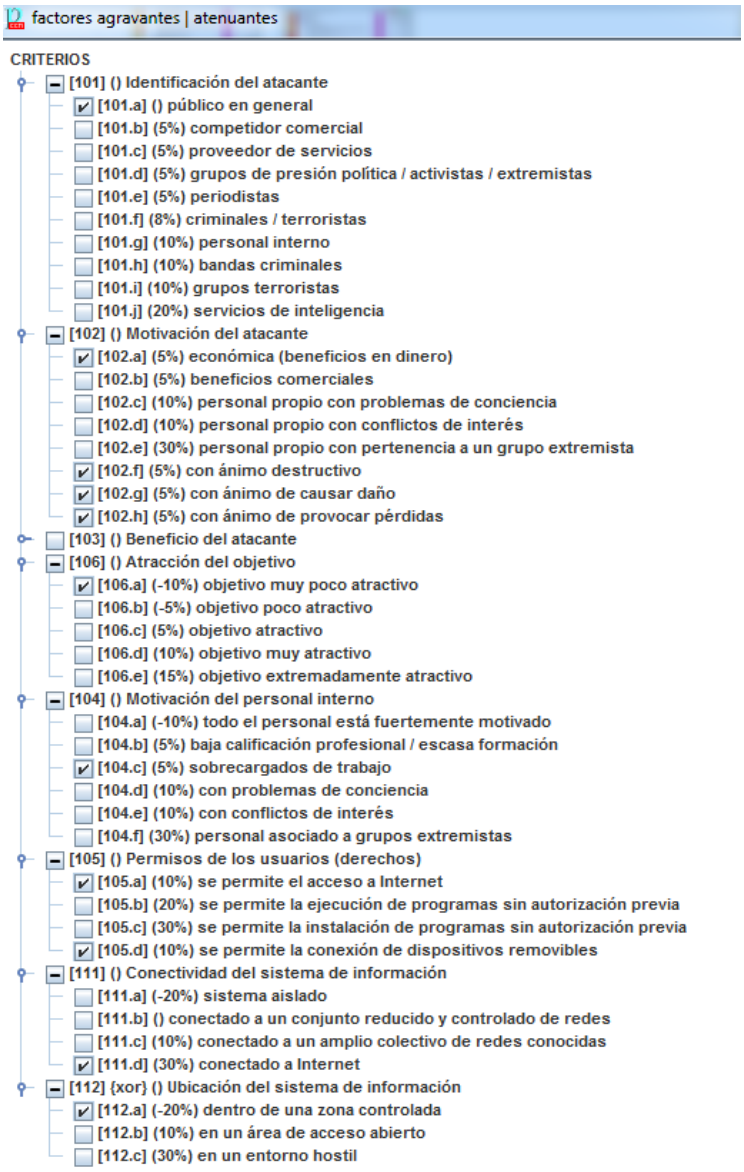
[AUX] Equipamiento auxiliar:
- [AUX.ups] sai - sistemas de alimentación ininterrumpida
- [AUX.cabling] cableado de datos

[L] Instalaciones:
- [L.local] cuarto

[P] Personal:
- [P.ui] usuarios internos
- [P.op] operadores
- [P.adm] administradores de sistemas
- [P.com] administradores de comunicaciones
- [P.dba] administradores de BBDD
- [P.sec] administradores de seguridad
- [P.prov] proveedores

3.3.4 Factores agravantes o atenuantes del riesgo

Para el análisis del riesgo µPILAR[5] dispone de factores agravantes o atenuantes que pueden afectar a nuestra entidad. En este caso de entre todos los propuestos, se ha realizado la siguiente selección, tal y como podemos ver en la siguiente captura:



Para justificar la selección de estos factores se tiene que:

- Respecto a la identificación del atacante, no hay ninguna corrección puesto que una Entidad Local de menos de 20000 habitantes difícilmente va a ser un objetivo directo de periodistas, grupos de presión, terroristas, etc. Por tanto se identifica al atacante como: [101.a] público en general.

- La motivación del atacante en este caso si puede ser múltiple, principalmente con ánimo de causar daño, provocar pérdidas, ánimo destructivo o simplemente como ha ocurrido en los dos últimos años motivación económica mediante ransomware de encriptación que deja inaccesibles los datos, y hay que realizar un pago en bitcoins para obtener la clave de cifrado. Por tanto tenemos: [102.a] económica (beneficios en dinero), [102.f] con ánimo destructivo, [102.g] con ánimo de causar daño y [102.h] con ánimo de provocar pérdidas

- Respecto a los beneficios del atacante, este autor entiende que no existe un interés moderado, muy interesado o extremadamente interesado, sino que muchas veces es un interés derivado del azar en la selección del objetivo.

- La valoración como atracción del objetivo deriva en un atenuante del 10%, puesto que nuevamente se considera que el objetivo es muy poco atractivo, pues no es llamativo para ciberdelincuentes, terroristas, servicios de inteligencia, etc. Por tanto el objetivo se atenúa como: [106.a] objetivo muy poco atractivo

- La motivación del personal interno es muy discutible, y puede variar según la Entidad Local, en este caso, y debido a todos los recientes cambios normativos respecto a Transparencia, Facturación Electrónica, Ley de Contratación, Ley de Sostenibilidad Presupuestaria, etc, el personal, en la mayoría de Entidad Locales va sobrecargado y por tanto se selecciona el agravante: [104.c] sobrecargados de trabajo

- Respecto a los permisos de los usuarios, esto depende del Departamento Informático de la Entidad Local, que dependiendo del tamaño en muchos casos no existe. Se seleccionan dos agravantes: [105.a] se permite el acceso a Internet y [105.d] se permite la conexión de dispositivos removibles, descartando la ejecución e instalación de programas sin autorización previa.

- Hoy día la conectividad del sistema de información es un agravante muy importante, puesto que es muy difícil encontrar sistemas aislados. En concreto, y como mínimo una Entidad Local está conectada a internet, y en muchos casos a otras redes como la red SARA. Por tanto se selecciona el agravante: [111.d] conectado a Internet

- El último grupo de agravantes o atenuantes se refiere a la ubicación del sistema de información, y también puede ser bastante debatido dependiendo la administración que representemos. En este caso el criterio aplicado es que se encuentra dentro de una zona controlada y no hay acceso abierto a los ciudadanos, por lo que se transforma en un atenuante: [112.a] dentro de una zona controlada

3.3.5 Controles ENS

El ENS[2] recoge 75 medidas de seguridad clasificadas en tres marcos, tal y como hemos expuesto en el punto 3.2 de introducción al ENS, y estas medidas se ven directamente reflejadas en los controles mostrados por µPILAR en la pantalla de perfil de seguridad. Estos controles se presentan en una tabla con filas y columnas, donde cada una de las filas define un control que tiene una serie de características, destacando:

- **Recomendación:** presenta un nivel de recomendación calcula por µPILAR[5] teniendo en cuenta los activos del sistema y su valoración.

- **Control:** Descripción de los controles que componen el perfil en forma de árbol jerárquico. Cuando terminan los controles formales, µPILAR sigue desplegando las salvaguardas asociadas a ellos, o preguntas específicas.

- **Aplicación:** Se usa para indicar que un control o salvaguarda no es de aplicación (n.a.). Lo más normal es que todos los controles y salvaguardas sean aplicables, aunque en nuestro caso no se aplican los controles de gestión del personal por las razones previamente mencionadas, al igual que algunas preguntas referentes a controles muy específicos como los de transporte físico de los soportes de sistema de información.

- **Grado de cumplimiento actual:** Presenta el grado de cumplimiento de los controles en forma de porcentaje o nivel de madurez. Se obtienen mediante la cumplimentación de las preguntas referente a cada control. En este trabajo se ha decidido el uso de los niveles de madurez según los niveles indicados por la guía CCN-STIC 804[2]:

    - **L0 – Inexistente:** Esta medida no está siendo aplicada en este momento.
    - **L1 – Inicial/ad hoc:** 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 su naturaleza caótica, es más que no tener nada; pero es difícil prever la reacción ante una situación de emergencia.
    - **L2 – Repetible, pero intuitivo:** 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.
    - **L3 – Proceso definido:** 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.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.

- **L4 - Gestionado y medible**: 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.
- **L5 – Optimizado:** 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.

- **Grado de cumplimiento objetivo:** Como norma general el Esquema Nacional de Seguridad requiere un nivel de madurez en las medidas en proporción al nivel de dimensiones afectadas o de la categoría de la misma, concretamente como mínimo exige:

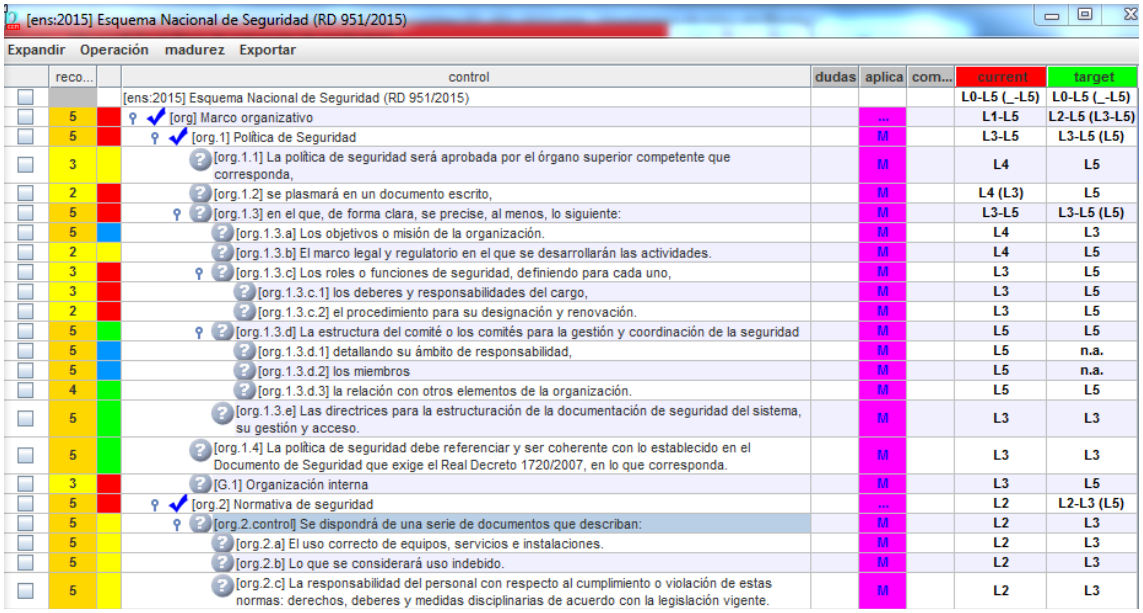
  - Nivel bajo exige un nivel de madurez L2.
  - Nivel medio exige un nivel de madurez L3.
  - Nivel alto exige un nivel de madurez L4.

Es clave señalar que en una Entidad Local de menos de 20000 habitantes, donde el Servicio de Informática es de una o dos personas, si es que existe, es muy difícil superar un grado de cumplimiento L3, siendo en muchos casos alcanzable únicamente un grado de madurez L2. Debido a esto, es altamente complicado que una Entidad Local de este tipo cumpla el Esquema Nacional de Seguridad en su totalidad, pues como hemos visto hay diversos activos esenciales que requieren nivel alto en sus dimensiones de confidencialidad y protección de datos.

Una vez realizado el amplísimo trabajo de responder de forma coherente a las diversas cuestiones que conlleva cada uno de los 75 controles del Esquema Nacional de Seguridad se ha obtenido una tabla con 564 filas y que se adjunta como archivo .csv adjunto por razones de espacio, aunque al ser un resultado directo se debería incluir dentro de este apartado.

A modo de ejemplo, y de forma no exhaustiva se presentan diversas capturas de pantalla, que pueden ayudar a entender la dimensión del trabajo realizado, y como la aplicación del Esquema Nacional de Seguridad ayuda a realizar una reflexión metódica de toda la seguridad de una Entidad Local.

EJEMPLO 1: **Controles y preguntas sobre el marco organizativo:**

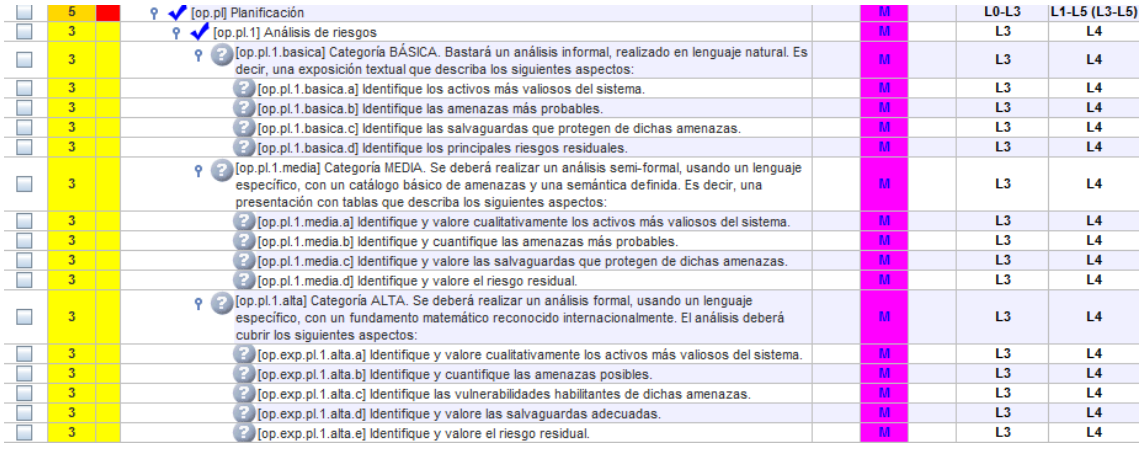

[ens:2015] Esquema Nacional de Seguridad (RD 951/2015)

Expandir Operación madurez Exportar

reco...		control	dudas	aplica	com...	current	target
		[ens:2015] Esquema Nacional de Seguridad (RD 951/2015)				L0-L5 (_-L5)	L0-L5 (_-L5)
5		[org] Marco organizativo		...		L1-L5	L2-L5 (L3-L5)
5		[org.1] Política de Seguridad		M		L3-L5	L3-L5 (L5)
3		[org.1.1] La política de seguridad será aprobada por el órgano superior competente que corresponda,		M		L4	L5
2		[org.1.2] se plasmará en un documento escrito,		M		L4 (L3)	L5
5		[org.1.3] en el que, de forma clara, se precise, al menos, lo siguiente:		M		L3-L5	L3-L5 (L5)
5		[org.1.3.a] Los objetivos o misión de la organización.		M		L4	L3
2		[org.1.3.b] El marco legal y regulatorio en el que se desarrollarán las actividades.		M		L4	L5
3		[org.1.3.c] Los roles o funciones de seguridad, definiendo para cada uno,		M		L3	L5
3		[org.1.3.c.1] los deberes y responsabilidades del cargo,		M		L3	L5
2		[org.1.3.c.2] el procedimiento para su designación y renovación.		M		L3	L5
5		[org.1.3.d] La estructura del comité o los comités para la gestión y coordinación de la seguridad		M		L5	L5
5		[org.1.3.d.1] detallando su ámbito de responsabilidad,		M		L5	n.a.
5		[org.1.3.d.2] los miembros		M		L5	n.a.
4		[org.1.3.d.3] la relación con otros elementos de la organización.		M		L5	L5
5		[org.1.3.e] Las directrices para la estructuración de la documentación de seguridad del sistema, su gestión y acceso.		M		L3	L3
5		[org.1.4] La política de seguridad debe referenciar y ser coherente con lo establecido en el Documento de Seguridad que exige el Real Decreto 1720/2007, en lo que corresponda.		M		L3	L3
3		[G.1] Organización interna		M		L3	L5
5		[org.2] Normativa de seguridad		...		L2	L2-L3 (L5)
5		[org.2.control] Se dispondrá de una serie de documentos que describan:		M		L2	L3
5		[org.2.a] El uso correcto de equipos, servicios e instalaciones.		M		L2	L3
5		[org.2.b] Lo que se considerará uso indebido.		M		L2	L3
5		[org.2.c] La responsabilidad del personal con respecto al cumplimiento o violación de estas normas: derechos, deberes y medidas disciplinarias de acuerdo con la legislación vigente.		M		L2	L3

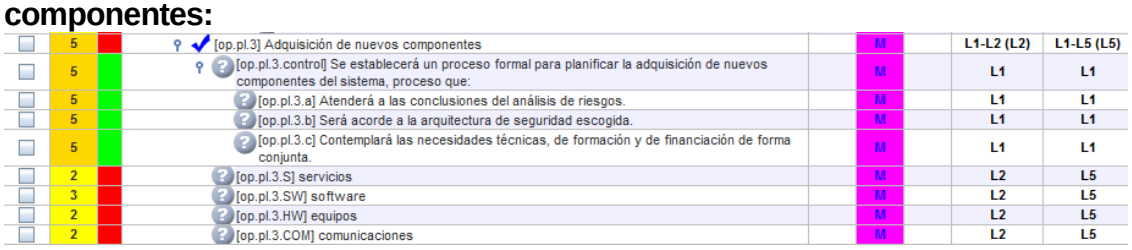
Como vemos, nos marca numerosas preguntas y controles en rojo, puesto que en nuestro análisis se ha demostrado que la situación actual es insuficiente para cumplir completamente el ENS.

EJEMPLO 2: **Controles y preguntas sobre análisis de riesgos en la planificación:**



5	[op.pl] Planificación		M		L0-L3	L1-L5 (L3-L5)
3	[op.pl.1] Análisis de riesgos		M		L3	L4
3	[op.pl.1.basica] Categoría BÁSICA. Bastará un análisis informal, realizado en lenguaje natural. Es decir, una exposición textual que describa los siguientes aspectos:		M		L3	L4
3	[op.pl.1.basica.a] Identifique los activos más valiosos del sistema.		M		L3	L4
3	[op.pl.1.basica.b] Identifique las amenazas más probables.		M		L3	L4
3	[op.pl.1.basica.c] Identifique las salvaguardas que protegen de dichas amenazas.		M		L3	L4
3	[op.pl.1.basica.d] Identifique los principales riesgos residuales.		M		L3	L4
3	[op.pl.1.media] Categoría MEDIA. Se deberá realizar un análisis semi-formal, usando un lenguaje específico, con un catálogo básico de amenazas y una semántica definida. Es decir, una presentación con tablas que describa los siguientes aspectos:		M		L3	L4
3	[op.pl.1.media.a] Identifique y valore cualitativamente los activos más valiosos del sistema.		M		L3	L4
3	[op.pl.1.media.b] Identifique y cuantifique las amenazas más probables.		M		L3	L4
3	[op.pl.1.media.c] Identifique y valore las salvaguardas que protegen de dichas amenazas.		M		L3	L4
3	[op.pl.1.media.d] Identifique y valore el riesgo residual.		M		L3	L4
3	[op.pl.1.alta] Categoría ALTA. Se deberá realizar un análisis formal, usando un lenguaje específico, con un fundamento matemático reconocido internacionalmente. El análisis deberá cubrir los siguientes aspectos:		M		L3	L4
3	[op.exp.pl.1.alta.a] Identifique y valore cualitativamente los activos más valiosos del sistema.		M		L3	L4
3	[op.exp.pl.1.alta.b] Identifique y cuantifique las amenazas posibles.		M		L3	L4
3	[op.exp.pl.1.alta.c] Identifique las vulnerabilidades habilitantes de dichas amenazas.		M		L3	L4
3	[op.exp.pl.1.alta.d] Identifique y valore las salvaguardas adecuadas.		M		L3	L4
3	[op.exp.pl.1.alta.e] Identifique y valore el riesgo residual.		M		L3	L4

EJEMPLO 3: **Controles y preguntas la planificación de adquisición de nuevos componentes:**



5	[op.pl.3] Adquisición de nuevos componentes		M		L1-L2 (L2)	L1-L5 (L5)
5	[op.pl.3.control] Se establecerá un proceso formal para planificar la adquisición de nuevos componentes del sistema, proceso que:		M		L1	L1
5	[op.pl.3.a] Atenderá a las conclusiones del análisis de riesgos.		M		L1	L1
5	[op.pl.3.b] Será acorde a la arquitectura de seguridad escogida.		M		L1	L1
5	[op.pl.3.c] Contemplará las necesidades técnicas, de formación y de financiación de forma conjunta.		M		L1	L1
2	[op.pl.3.S] servicios		M		L2	L5
3	[op.pl.3.SW] software		M		L2	L5
2	[op.pl.3.HW] equipos		M		L2	L5
2	[op.pl.3.COM] comunicaciones		M		L2	L5

EJEMPLO 4: **Controles y preguntas la monitorización del sistema:**

	6		[op.mon] Monitorización del sistema		M		L2-L3 (L3)	L3-L5 (L5)
	6		[op.mon.1] Detección de intrusión		M		L3	L5
	6		[op.mon.1.control] Categoría MEDIA. Se dispondrán de herramientas de detección o de prevención de intrusión.		M		L3	L5
	5		[op.mon.2] Sistema de métricas		M		L2	L3
	5		[op.mon.2.control.B] Categoría BÁSICA. Se recopilarán los datos necesarios atendiendo a la categoría del sistema para conocer el grado de implantación de las medidas de seguridad que apliquen de las detalladas en el Anexo II y, en su caso, para proveer el informe anual requerido por el artículo 35.		M		L2	L3
	5		[op.mon.2.control.M] Categoría MEDIA: Además, se recopilarán datos para valorar el sistema de gestión de incidentes, permitiendo conocer:		M		L2	L3
	5		[op.mon.2.control.M.a] Número de incidentes de seguridad tratados.		M		L2	L3
	5		[op.mon.2.control.M.b] Tiempo empleado para cerrar el 50% de los incidentes.		M		L2	L3
	5		[op.mon.2.control.M.c] Tiempo empleado para cerrar el 90% de los incidentes.		M		L2	L3
	5		[op.mon.2.control.A] Categoría ALTA: Se recopilarán datos para conocer la eficiencia del sistema de seguridad TIC: Recursos consumidos: horas y presupuesto.		M		L2	L3

EJEMPLO 5: **Controles y preguntas sobre la protección de las aplicaciones informáticas:**

	5		[mp.sw] Protección de las aplicaciones informáticas (SW)		M		L1-L5	L5
	5		[mp.sw.1] Desarrollo de aplicaciones		M		L1-L5	L5
	5		[mp.sw.1.a] El desarrollo de aplicaciones se realizará sobre un sistema diferente y separado del de producción, no debiendo existir herramientas o datos de desarrollo en el entorno de producción.		M		L3	L5
	4		[mp.sw.1.b] Se aplicará una metodología de desarrollo reconocida que:		M		L1-L3	L5
	4		[mp.sw.1.b.1] Tome en consideración los aspectos de seguridad a lo largo de todo el ciclo de vida.		M		L3	L5
	4		[mp.sw.1.b.2] Trate específicamente los datos usados en pruebas.		M		L1	L5
	4		[mp.sw.1.b.3] Permita la inspección del código fuente.		M		L1	L5
	4		[mp.sw.1.c] Los siguientes elementos serán parte integral del diseño del sistema:		M		L3	L5
	4		[mp.sw.1.c.1] Los mecanismos de identificación y autenticación.		M		L3	L5
	4		[mp.sw.1.c.2] Los mecanismos de protección de la información tratada.		M		L3	L5
	4		[mp.sw.1.c.3] La generación y tratamiento de pistas de auditoría.		M		L3	L5
	4		[mp.sw.1.d] Las pruebas anteriores a la implantación o modificación de los sistemas de información no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente.		M		L5	L5
	5		[mp.sw.2] Aceptación y puesta en servicio		M		L1-L5	L5
	4		[mp.sw.2.basica] Categoría BÁSICA. Antes de pasar a producción se comprobará el correcto funcionamiento de la aplicación.		M		L2-L5 (L1-L5)	L5
	4		[mp.sw.2.basica.a] Se comprobará que:		M		L2-L3 (L1-L3)	L5
	4		[mp.sw.2.basica.a.1] Se cumplen los criterios de aceptación en materia de seguridad.		M		L3	L5
	4		[mp.sw.2.basica.a.2] No se deteriora la seguridad de otros componentes del servicio.		M		L2 (L1)	L5
	4		[mp.sw.2.basica.b] Las pruebas se realizarán en un entorno aislado (pre-producción).		M		L3	L5
	4		[mp.sw.2.basica.c] Las pruebas de aceptación no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente.		M		L5	L5
	3		[mp.sw.2.media] Categoría MEDIA. Se realizarán las siguientes inspecciones previas a la entrada en servicio:		M		L2-L3	L5
	3		[mp.sw.2.media.a] Análisis de vulnerabilidades.		M		L3	L5
			[mp.sw.2.media.b] Pruebas de penetración.		M		L2	L5
	5		[mp.sw.2.alta] Categoría ALTA. Se realizarán las siguientes inspecciones previas a la entrada en servicio:		M		L1	L5
	4		[mp.sw.2.alta.a] Análisis de coherencia en la integración en los procesos.		M		L1	L5
	5		[mp.sw.2.alta.b] Se considerará la oportunidad de realizar una auditoría de código fuente.		M		L1	L5

EJEMPLO 6: **Protección frente a la denegación de servicio:**

	5		[mp.s.8] Protección frente a la denegación de servicio		M		L1-L2	L5
	5		[mp.s.8.medio] Nivel MEDIO. Se establecerán medidas preventivas y reactivas frente a ataques de denegación de servicio (DOS Denial of Service). Para ello:		M		L2	L5
	5		[mp.s.8.medio.a] Se planificará y dotará al sistema de capacidad suficiente para atender a la carga prevista con holgura.		M		L2	L5
	4		[mp.s.8.medio.b] Se desplegarán tecnologías para prevenir los ataques conocidos.		M		L2	L5
	4		[mp.s.8.alto] Nivel ALTO				L1-L2	L5
	2		[mp.s.8.alto.a] Se establecerá un sistema de detección de ataques de denegación de servicio.				L2	L5
	3		[mp.s.8.alto.b] Se establecerán procedimientos de reacción a los ataques, incluyendo la comunicación con el proveedor de comunicaciones.				L1	L5
	4		[mp.s.8.alto.c] Se impedirá el lanzamiento de ataques desde las propias instalaciones perjudicando a terceros.				L1	L5

Finalmente se incluyen dos capturas de pantalla, una como resumen de todos los controles y su nivel de madurez actual y objetivo, donde de nuevo se puede apreciar como los controles marcados en rojo.

RESUMEN DE CONTROLES:

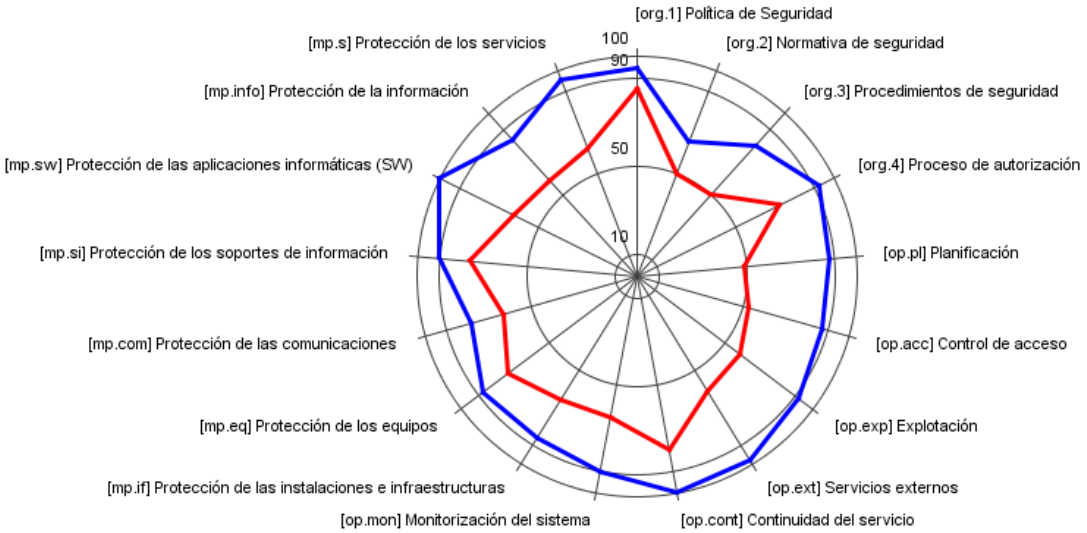
[ens:2015] Esquema Nacional de Seguridad (RD 951/2015)

Expandir Operación madurez Exportar

reco...	control	dudas	aplica	com...	current	target
	[ens:2015] Esquema Nacional de Seguridad (RD 951/2015)				L0-L5 (_-L5)	L0-L5 (_-L5)
5	[org] Marco organizativo		...		L1-L5	L2-L5 (L3-L5)
5	[org.1] Política de Seguridad		M		L3-L5	L3-L5 (L5)
5	[org.2] Normativa de seguridad		...		L2	L2-L3 (L5)
5	[org.3] Procedimientos de seguridad		...		L2	L3
3	[org.4] Proceso de autorización		M		L1-L4	L3-L5
8	[op] Marco operacional		...		L0-L3 (_-L5)	L0-L5 (_-L5)
5	[op.pl] Planificación		M		L0-L3	L1-L5 (L3-L5)
8	[op.acc] Control de acceso		...		L0-L3 (_-L4)	L0-L5 (_-L5)
8	[op.exp] Explotación		...		L0-L3 (L0-L5)	L3-L5 (L1-L5)
5	[op.ext] Servicios externos		M		L0-L3	L4-L5
5	[op.cont] Continuidad del servicio		M		L3	L5
6	[op.mon] Monitorización del sistema		M		L2-L3 (L3)	L3-L5 (L5)
7	[mp] Medidas de protección		...		L0-L5 (_-L5)	L0-L5 (_-L5)
6	[mp.if] Protección de las instalaciones e infraestructuras		M		L1-L3	L3-L5
	[mp.per] Gestión del personal		n.a.			
5	[mp.eq] Protección de los equipos		M		L0-L5	L0-L5
6	[mp.com] Protección de las comunicaciones		M		L0-L5 (_-L4)	L0-L5 (_-L5)
4	[mp.si] Protección de los soportes de información		...		L2-L3	L4 (L3-L4)
5	[mp.sw] Protección de las aplicaciones informáticas (SW)		M		L1-L5	L5
7	[mp.info] Protección de la información		...		L0-L5	L0-L5 (L1-L5)
5	[mp.s] Protección de los servicios		M		L1-L3	L4-L5

Así mismo se muestra un gráfico que la herramienta puede mostrar con los principales controles y el grado de cumplimiento actual de los mismos –línea roja-, y el grado objetivo según ESN – línea azul. En este caso se puede ver como la Entidad Local no parte de cero en la mayoría de controles, sino que el grado de madurez es insuficiente.

RESUMEN GRÁFICO DE CONTROLES:



3.3.6 Resultado del análisis de riesgos según ENS[2]

El resultado del análisis de riesgos es ofrecido por µPILAR[5] con tres clasificaciones distintas:

- **Potencial**: presenta el riesgo potencial; es decir, el riesgo si no hubiera salvaguardas, es decir, si no se hubieran realizado tareas previas.

- **Current:** riesgo residual a fecha de hoy, cuando se aplican las salvaguardas o preguntas del ENS con la madurez declarada en la fase 'current'.

- **Target:** riesgo residual objetivo del ENS, cuando se aplican las salvaguardas o preguntas del ENS con la madurez declarada en la fase 'target'.

Y en cada una de estas clasificaciones distintas se atiende a todos las dimensiones incluidas en MAGERIT 3.0, quedando el resultado de la siguiente manera:

RIESGOS POTENCIALES ACTIVOS ESENCIALES:

potencial | current | target

activo	[D]	[I]	[C]	[A]	[T]
ACTIVOS	{4,2}	{4,7}	{6,4}	{5,3}	{5,1}
[Exp] Expedientes/Documentos Ayuntamiento		{4,7}	{4,7}	{4,7}	{2,7}
[RGE/RGS] Registro General de Entrada y Salida		{4,7}	{2,9}	{4,7}	{2,7}
[Personal] Datos y servicios personal	{2,4}	{4,7}	{4,7}	{4,7}	{2,7}
[Intervención] Datos y servicios contables, económicos, financieros	{2,4}	{4,7}	{2,3}	{2,9}	{2,7}
[Tributaria] Datos y servicios de gestión tributaria y recaudación	{2,4}	{4,7}	{2,9}	{4,7}	{2,7}
[PMH] Padrón de Habitantes	{2,4}	{4,7}	{2,9}	{4,7}	{2,7}
[ServSociales] Datos y servicios expedientes Servicios Sociales	{4,2}	{4,7}	{6,4}	{4,7}	{4,5}
[SegCiudadana] Datos y servicios Seguridad Ciudadana	{2,4}	{4,7}	{6,4}	{4,7}	{4,5}
[Gestor] Gestor expedientes municipal	{4,2}			{2,9}	{2,7}
[Sede electrónica] Tramitación telemática	{2,4}			{5,3}	{5,1}

RIESGOS ACTUALES ACTIVOS ESENCIALES:

potencial | current | target

activo	[D]	[I]	[C]	[A]	[T]
ACTIVOS	{2,0}	{2,4}	{4,4}	{3,0}	{2,9}
[Exp] Expedientes/Documentos Ayuntamiento		{2,4}	{2,6}	{2,4}	{0,90}
[RGE/RGS] Registro General de Entrada y Salida		{2,4}	{0,97}	{2,4}	{0,90}
[Personal] Datos y servicios personal	{0,85}	{2,4}	{2,6}	{2,4}	{0,90}
[Intervención] Datos y servicios contables, económicos, financieros	{0,85}	{2,4}	{0,85}	{0,93}	{0,90}
[Tributaria] Datos y servicios de gestión tributaria y recaudación	{0,85}	{2,4}	{0,97}	{2,4}	{0,90}
[PMH] Padrón de Habitantes	{0,85}	{2,4}	{0,97}	{2,4}	{0,90}
[ServSociales] Datos y servicios expedientes Servicios Sociales	{2,0}	{2,4}	{4,4}	{2,4}	{2,3}
[SegCiudadana] Datos y servicios Seguridad Ciudadana	{0,85}	{2,4}	{4,4}	{2,4}	{2,3}
[Gestor] Gestor expedientes municipal	{2,0}			{0,93}	{0,90}
[Sede electrónica] Tramitación telemática	{0,85}			{3,0}	{2,9}

RIESGOS OBJETIVOS ACTIVOS ESENCIALES SEGÚN ENS:

potencial | current | target

activo	[D]	[I]	[C]	[A]	[T]
ACTIVOS	{0,64}	{0,90}	{2,3}	{1,1}	{1,1}
[Exp] Expedientes/Documentos Ayuntamiento		{0,90}	{0,90}	{0,90}	{0,54}
[RGE/RGS] Registro General de Entrada y Salida		{0,90}	{0,55}	{0,90}	{0,54}
[Personal] Datos y servicios personal	{0,29}	{0,90}	{0,90}	{0,90}	{0,54}
[Intervención] Datos y servicios contables, económicos, financieros	{0,29}	{0,90}	{0,43}	{0,55}	{0,54}
[Tributaria] Datos y servicios de gestión tributaria y recaudación	{0,29}	{0,90}	{0,55}	{0,90}	{0,54}
[PMH] Padrón de Habitantes	{0,29}	{0,90}	{0,55}	{0,90}	{0,54}
[ServSociales] Datos y servicios expedientes Servicios Sociales	{0,64}	{0,90}	{2,3}	{0,90}	{0,89}
[SegCiudadana] Datos y servicios Seguridad Ciudadana	{0,29}	{0,90}	{2,3}	{0,90}	{0,89}
[Gestor] Gestor expedientes municipal	{0,64}			{0,55}	{0,54}
[Sede electrónica] Tramitación telemática	{0,29}			{1,1}	{1,1}

Además la herramienta nos ofrece todos los riesgos no esenciales clasificados de la misma manera. Se incluyen en el archivo .csv adjunto correspondiente, pero como ejemplo se muestra una captura de pantalla:

potencial | current | target | resumen (impacto) | resumen (riesgo)

activo	amenaza	dimensión	riesgo	current	target
[D.backup] copias de respaldo	[A.11] Acceso no autorizado	[C]	{6,4}	{4,4}	{1,7}
[D.e-files] ficheros cifrados	[A.11] Acceso no autorizado	[C]	{6,4}	{4,4}	{1,7}
[D.source] código fuente	[A.11] Acceso no autorizado	[C]	{6,4}	{4,4}	{1,7}
[D.exe] código ejecutable	[A.11] Acceso no autorizado	[C]	{6,4}	{4,4}	{1,7}
[D.multimedia] multimedia	[A.11] Acceso no autorizado	[C]	{6,4}	{4,4}	{1,7}
[D.files] ficheros de datos	[A.11] Acceso no autorizado	[C]	{6,4}	{4,4}	{1,7}
[keys.com.channel] claves de cifrado del c...	[A.11] Acceso no autorizado	[C]	{6,4}	{4,1}	{1,6}
[keys.com.authentication] claves de auten...	[A.11] Acceso no autorizado	[C]	{6,4}	{4,1}	{1,6}
[keys.info.encrypt] claves de cifra	[A.11] Acceso no autorizado	[C]	{6,4}	{4,1}	{1,6}
[D.conf] datos de configuración	[A.5] Suplantación de la identidad	[A]	{6,1}	{4,2}	{2,3}
[D.int] datos de gestión interna	[A.5] Suplantación de la identidad	[A]	{6,1}	{4,2}	{2,3}
[keys.com.authentication] claves de auten...	[A.5] Suplantación de la identidad	[A]	{6,1}	{4,0}	{1,8}
[keys.info.encrypt] claves de cifra	[A.5] Suplantación de la identidad	[A]	{6,1}	{4,0}	{1,8}
[keys.com.channel] claves de cifrado del c...	[A.5] Suplantación de la identidad	[A]	{6,1}	{4,0}	{1,8}
[P.dba] administradores de BBDD	EXT_P@ext > [A.5, core] > [A.30] Ingeniería ...	[C]	{5,9}	{3,9}	{0,99}
[P.sec] administradores de seguridad	EXT_P@ext > [A.5, core] > [A.29] Extorsión	[C]	{5,9}	{3,9}	{0,99}
[P.dba] administradores de BBDD	EXT_P@ext > [A.5, core] > [A.29] Extorsión	[C]	{5,9}	{3,9}	{0,99}
[P.adm] administradores de sistemas	EXT_P@ext > [A.5, core] > [A.30] Ingeniería ...	[C]	{5,9}	{3,9}	{0,99}
[P.sec] administradores de seguridad	EXT_P@ext > [A.5, core] > [A.30] Ingeniería ...	[C]	{5,9}	{3,9}	{0,99}
[P.adm] administradores de sistemas	EXT_P@ext > [A.5, core] > [A.29] Extorsión	[C]	{5,9}	{3,9}	{0,99}
[SW.sec.av] anti virus	EXT_L@ext > [A.11, core] > [A.8] Difusión d...	[C]	{5,9}	{3,6}	{0,97}
[SW.sec.hp] honey pot	EXT_L@ext > [A.11, core] > [A.8] Difusión d...	[C]	{5,9}	{3,6}	{0,97}
[SW.sec.traf] análisis de tráfico	EXT_L@ext > [A.11, core] > [A.8] Difusión d...	[C]	{5,9}	{3,6}	{0,97}
[SW.sec.ids] IDS / IPS (detección / prevenció...	EXT_L@ext > [A.11, core] > [A.8] Difusión d...	[C]	{5,9}	{3,6}	{0,97}
[SW.sec.dlp] prevención de pérdida de dat...	EXT_L@ext > [A.11, core] > [A.8] Difusión d...	[C]	{5,9}	{3,6}	{0,97}
[SW.sub] desarrollo a medida (subcontrat...	EXT_L@ext > [A.11, core] > [A.8] Difusión d...	[C]	{5,9}	{3,6}	{0,97}
[SW.prp] desarrollo propio (in house)	EXT_L@ext > [A.11, core] > [A.8] Difusión d...	[C]	{5,9}	{3,6}	{0,97}
[SW.std.www] servidor de presentación	EXT_L@ext > [A.11, core] > [A.8] Difusión d...	[C]	{5,9}	{3,6}	{0,97}
[SW.std.directory] servidor de directorio	EXT_L@ext > [A.11, core] > [A.8] Difusión d...	[C]	{5,9}	{3,6}	{0,97}
[SW.std.backup] servidor de backup	EXT_L@ext > [A.11, core] > [A.8] Difusión d...	[C]	{5,9}	{3,6}	{0,97}
[SW.std.os.windows] windows	EXT_L@ext > [A.11, core] > [A.8] Difusión d...	[C]	{5,9}	{3,6}	{0,97}
[SW.std.os.linux] linux	EXT_L@ext > [A.11, core] > [A.8] Difusión d...	[C]	{5,9}	{3,6}	{0,97}
[SW.std.browser] navegador web	EXT_L@ext > [A.11, core] > [A.8] Difusión d...	[C]	{5,9}	{3,6}	{0,97}
[SW.std.app] servidor de aplicaciones	EXT_L@ext > [A.11, core] > [A.8] Difusión d...	[C]	{5,9}	{3,6}	{0,97}
[SW.std.dbms] sistema de gestión de bas...	EXT_L@ext > [A.11, core] > [A.8] Difusión d...	[C]	{5,9}	{3,6}	{0,97}
[SW.std.os] sistema operativo	EXT_L@ext > [A.11, core] > [A.8] Difusión d...	[C]	{5,9}	{3,6}	{0,97}
[SW.std.file] servidor de ficheros	EXT_L@ext > [A.11, core] > [A.8] Difusión d...	[C]	{5,9}	{3,6}	{0,97}
[SW.std.office] ofimática	EXT_L@ext > [A.11, core] > [A.8] Difusión d...	[C]	{5,9}	{3,6}	{0,97}
[SW.std.hypervisor] hypervisor (gestor de...	EXT_L@ext > [A.11, core] > [A.8] Difusión d...	[C]	{5,9}	{3,6}	{0,97}
[SW.std.email_client] cliente de correo ele...	EXT_L@ext > [A.11, core] > [A.8] Difusión d...	[C]	{5,9}	{3,6}	{0,97}
[SW.std.email_server] servidor de correo ...	EXT_L@ext > [A.11, core] > [A.8] Difusión d...	[C]	{5,9}	{3,6}	{0,97}

3.3.7 Informes y salvaguardas según ENS[2]

µPILAR[5] permite exportar a documento RTF tres tipos de informes que se incluyen como anexos:

- **Análisis de riesgos.**
- **Declaración de aplicabilidad ENS – Anexo II**
- **Cumplimiento del ENS – Anexo II**

Finalmente la herramienta nos muestra una serie de sugerencias en forma de salvaguardas que debemos repasar y aplicar. Estas salvaguardas pueden ser en los aspectos de Gestión (G), Técnicos (T), Seguridad Física (F) y de Personal (P) y cada una de ellas puede mostrarse en cuatro colores: gris: peso bajo, verde: importante, amarillo: muy importante y rojo: crítica.

Así mismo cada una de la salvaguardas puede ser de distintos tipos de protección: Prevención (PR), Disuasion (DR), Eliminación (EL), Minimización del impacto (IM), Corrección (CR), Recuperación (RC), Administrativo (AD), Concienciación (AW), Detección (DC), Monitorización (MN), Normativa (std), Procedimiento (proc) y Certificación (cert). Se incluyen todas las salvaguardas como fichero .csv adjunto.

Como ejemplo podemos ver esta captura de pantalla:

aspe...	tdp	reco...	salvaguarda	dudas	aplica	com...	surr...	target
			SALVAGUARDAS					
G	EL	8	[IA] Identificación y autenticación				L0-L3	L3-L4
G	std	3	[IA.1] Se dispone de normativa de identificación y autenticación				L2	L3
G	proc	3	[IA.2] Se dispone de procedimientos para las tareas de identificación y autenticación				L2	L3
G	EL	5	[IA.3] Identificación de los usuarios				L2-L3	L3-L4
G	EL	5	[IA.3.1] Cada usuario recibe un identificador exclusivo (no compartido)				L3	L4
G	EL	3	[IA.3.2] La identificación del usuario no indica ni su función ni su nivel de privilegios				L2	L3
T	EL	3	[IA.3.3] Las cuentas de invitados están sometidas a un control estricto				L2	L3
G	EL	5	[IA.4] Gestión de la identificación y autenticación de usuario				L2-L3	L3-L4
G	EL	5	[IA.5] Cuentas especiales (administración)				L0-L2	L3-L4
T	EL	6	[IA.6] Canal seguro de autenticación				L3	L3
G	PR	8	[IA.7] {xor} Factores de autenticación que se requieren:				L3	L3
T	EL	7	[AC] Control de acceso lógico		...		_-L5	_-L5
T	PR	5	[AC.1] Gestión de privilegios				L2-L5	L4-L5
T	EL	5	[AC.2] Imposición del control de acceso				_-L5	_-L5
T	PR	4	[AC.2.1] Acceso sin identificación					
T	PR	4	[AC.2.2] Acceso restringido				L2	L3
T	PR	3	[AC.2.3] Se restringe el uso de las utilidades del sistema				L3	L5
T	PR	5	[AC.2.4] Se restringe el acceso a la configuración del sistema				L3	L5
T	PR	4	[AC.2.5] Se restringe el acceso a la configuración de seguridad del sistema				L1	L4
T	DC	4	[AC.2.6] Se controla el trabajo fuera del horario normal				L1-L5	L5
T	EL	5	[AC.2.7] {xor} Modelo de control de acceso				L1	L4
T	EL	5	[AC.2.8] Conexión en terminales (logon)				L0-L3	L3-L4
T	PR	3	[AC.2.9] Se limita el tiempo de conexión				L0	L3
T	PR	4	[AC.2.a] Se limita el número de sesiones concurrentes de un usuario				L3	L5
T	PR	5	[AC.2.b] Equipo informático de usuario desatendido				L1-L5	L5
T	EL	5	[AC.2.c] Los terminales se desconectan automáticamente				L0	L3
T	IM	7	[H.ST] Segregación de tareas		...		L0-L2	L5
T	PR	7	[H.ST.1] Se separan las responsabilidades de administración y operación				L0	L5
T	EL	5	[H.ST.2] Todos los procesos críticos requieren al menos 2 personas				L2	L5
T	IM	5	[H.ST.3] Se definen roles con autorización exclusiva para realizar tareas		...		L2	L5
T	IM	5	[H.ST.4] Se controla la efectividad de la estructura de segregación		...		L0-L2	L5
T	MN	4	[H.ST.4.1] Se registran todas las operaciones				L2	L5
T	DC		[H.ST.4.2] Se monitorizan todas las operaciones		n.a.		n.a.	n.a.
T	EL	3	[H.ST.4.3] Se impide que alguien pueda autorizarse a sí mismo				L0	L5
T	EL		[H.ST.4.4] Se impide que los operadores puedan modificar datos de operación		n.a.		n.a.	n.a.
T	EL		[H.ST.4.5] Se impide que los operadores puedan realizar transacciones		n.a.		n.a.	n.a.
T	PR	3	[H.ST.4.6] Se designa personal específico para la realización de transferencias de fondos				L2	L5
T	EL		[H.ST.4.7] Los desarrolladores no pueden pasar aplicaciones a producción		n.a.		n.a.	n.a.
T	EL		[H.ST.4.8] Los desarrolladores no pueden configurar aplicaciones en producción		n.a.		n.a.	n.a.
T	EL		[H.ST.4.9] Los operadores ni desarrollan ni pueden modificar los desarrollos		n.a.		n.a.	n.a.
T	EL		[H.ST.4.a] Los usuarios ni desarrollan ni pueden modificar los desarrollos		n.a.		n.a.	n.a.

4. Guía de controles de ciberseguridad en formato checklist para Administraciones Locales

4.1 Antecedentes

Ante el incesante aumento de los ataques de ciberseguridad, las Administraciones Públicas deben determinar su nivel de seguridad actual y establecer el nivel que ha de conseguir para protegerlos sistemas y la información corporativos.

Por este motivo, el Esquema Nacional de Seguridad (ENS), regulado por el Real Decreto 3/2010, de 8 de enero, determina la política de seguridad que se ha de aplicar en la utilización de los medios electrónicos, y es de aplicación obligatoria en todas las Administraciones Públicas, debiendo por tanto todas ellas realizar la adecuación de sus Sistemas de Información al mismo. El ENS está constituido por los principios básicos y requisitos mínimos para una protección adecuada de la información.

4.2 Objetivos

- Crear las condiciones necesarias de confianza en el uso de los medios electrónicos que permitan a los ciudadanos y a las Administraciones Públicas, el ejercicio de derechos y el cumplimiento de deberes a través de estos medios.

- Introducir los elementos y metodologías comunes que han de guiar la actuación de las Administraciones públicas en materia de seguridad de las tecnologías de la información.

4.3 Checklist

A continuación se incluyen una serie de controles para revisar el cumplimiento de las políticas de seguridad en una Administración Local. Una vez elaborada la política de seguridad y definidas las responsabilidad y funciones, para Administraciones Locales de menos de 20.000 habitantes se puede partir de todo el trabajo realizado en este TFM que sería puesto a disposición de dichas Administraciones.

Los controles podrán tener el siguiente alcance:

- Procesos (PRO): aplica a la dirección o al personal de gestión
- Tecnología (TEC): aplica al personal técnico especializado.

ALCANCE	CONTROL	
PRO	**Elaboración de una política de seguridad** Has elaborado la política según la Guía CCN-STIC 805 que propone un modelo a seguir.	☐
PRO	**Definición de responsabilidad y funciones** Has definido las responsabilidad y roles para lo que te has podido ayudar de la Guía CCN-STIC 801 que proporciona información sobre las responsabilidad de los diferentes roles.	☐
PRO/TEC	**Identificación de activos** Tienes identificados los activos más relevantes, especialmente los activos esenciales de información y servicios.	☐
TEC	**Valoración del riesgo de los activos** Realizas la valoración del riesgo de cada activo esencial en todas las dimensiones MAGERIT 3.0 mediante la herramienta µPILAR o similar.	☐
TEC	**Selección de factores agravantes o atenuantes** Has seleccionado los factores agravantes o atenuantes que se aplican en tu Administración Local mediante la herramienta µPILAR o similar.	☐
TEC	**Cumplimentación de los controles del ENS** Has respondido a todas las preguntas de los controles que verifican el grado de madurez de tu organización respecto al ENS mediante herramienta µPILAR o similar.	☐
PRO/TEC	**Revisión de informes y salvaguardas** Has revisado los informes obtenidos como resultado del análisis de riesgos realizado, y aplicado en la medida de los posible las salvaguardas indicadas por µPILAR o similar.	☐
TEC	**Realización de auditorías periódicas** Realizas auditorías de tus sistemas de información, obligadas o no por el ENS cada _____.	☐
PRO/TEC	Análisis del resultado de la auditoría Analizas los resultados de la auditoría en busca de debilidades a corregir y obtención de un plan de mejora	☐

Revisado por:_____ Fecha:_____

5. Conclusiones

En un mundo cada vez más globalizado y conectado las Administraciones Públicas están obligadas a crear las condiciones necesarias de confianza en el uso de los medios electrónicos que permitan a los ciudadanos el ejercicio de derechos y el cumplimiento de deberes a través de estos medios.

En este escenario, la ciberseguridad es uno de los grandes retos de cualquier organización, y para ello las Administraciones Públicas deben realizar una protección integral de sus Sistemas de Información y Comunicaciones, y para ello cuentan con una legislación específica, el Esquema Nacional de Seguridad (ENS), regulado por el Real Decreto 3/2010 , de 8 de enero, que determina la política de seguridad que se ha de aplicar en la utilización de los medios electrónicos, y es de aplicación obligatoria en todas las Administraciones Públicas.

La aplicación de esta regulación es compleja en cualquier Administración, pero más compleja aún en Administraciones Locales pequeñas y medianas de menos de 50.000 habitantes pues los Servicios de Informática y Comunicaciones (TIC) están compuestos por muy poco personal y con una sobrecarga importante de trabajo debido a la adaptación de todas las Administraciones Públicas a las normativas vigentes, que como no puede ser de otra manera, están suponiendo una modernización de las Administraciones lideradas por, entre otros, el personal TIC. En el caso de Administraciones Locales de menos de 20.000 habitantes muchas de ellas ni siquiera disponen de este servicio TIC , o si lo disponen está compuesto de una o dos personas, siendo asistidas por las diputaciones, de manera más o menos afortunada.

El presente trabajo pretende cubrir la necesidad de mejorar la ciberseguridad y realizar una adaptación al ENS de manera concisa y efectiva, facilitando una guía de controles de ciberseguridad en formato checklist para Administraciones Locales que nos permite verificar nuestro nivel de ciberseguridad y el cumplimiento ENS de una Administración Local. Así mismo, y lo que es más importante, este trabajo incluye un estudio detallado de activos esenciales mínimos de los que dispone una Administración Local, y un ejemplo de análisis de valoración de riesgos en la herramienta EAR µPILAR.

Una vez concluido el trabajo, y tal y como se preveía inicialmente el riesgo de sobredimensionamiento ha sido grande, y ha supuesto no poder estudiar la gestión de los incidentes de ciberseguridad en Administraciones Locales, dejando este estudio para trabajos futuros, si bien, gracias al trabajo de simplificación de activos se ha logrado el objetivo inicial del mismo.

Así mismo, se deja para trabajos futuros realizar un plan de auditorías de ciberseguridad y mejora continua de la misma, donde se incluya qué, cómo y quién debe auditarse, y que tras su estudio por los responsables pertinentes, se realice una mejora continua de la ciberseguridad.

Finalmente, introducir como reflexión final, que si bien el abordaje de una adaptación al Esquema Nacional de Seguridad es una tarea bastante compleja y que requiere tiempo que normalmente no se dispone en los servicios TIC de Administraciones Locales de tamaño pequeño y medio, es muy importante para los responsables de seguridad de la información la realización de este, pues ayuda a reflexionar de una manera global sobre la seguridad de nuestra organización y el grado de madurez de las medidas que se toman, pues habría que intentar disponer de un sistema de medidas y métricas para conocer el desempeño en términos de eficacia y eficiencia de los procesos que atañen a la ciberseguridad.

6. Bibliografía

[1] Guías política de seguridad para la PYME de INCIBE
https://www.incibe.es/protege-tu-empresa/herramientas/politicas

[2] 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.
https://www.boe.es/buscar/act.php?id=BOE-A-2010-1330

[3] Guías Esquema Nacional de Seguridad CCN-STIC serie 800
https://www.ccn-cert.cni.es/guias/guias-series-ccn-stic/800-guia-esquema-nacional-de-seguridad.html

[4] Web Federación Española de Municipios y Provincias.
Sección adaptación Esquema Nacional de Seguridad

[5] Web Centro Criptológico Nacional CCN-CERT. Sección PILAR
https://www.ccn-cert.cni.es/soluciones-seguridad/ear-pilar.html

[6] Web Centro Criptológico Nacional CCN-CERT. Sección CLARA
https://www.ccn-cert.cni.es/soluciones-seguridad/clara.html

[7] Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local
https://www.boe.es/buscar/act.php?id=BOE-A-1985-5392

[8] MAGERIT versión 3. Libro I: Método, Libro II: Catálogo de Elementos, Libro III: Guía de Técnicas. Editan los libros Ministerio de Hacienda y Administraciones Públicas
https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.XCpJpVVKiUk

[9] Reglamento UE 2016/679, de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personalesy a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)
https://www.boe.es/doue/2016/119/L00001-00088.pdf

7. Anexos

7.1 Documento Análisis de Riesgos obtenido en µPILAR

1 Introducción

Documento para anexar a la documentación de seguridad del sistema que se presenta para conseguir la aprobación o autorización de la autoridad responsable del sistema de información.

Datos del sistema sujeto a análisis:

Código: TFM - MISTIC - JMBH
Nombre: Ayuntamiento < 20000 habitantes

Descripción:

Datos administrativos:

- Descripción: Ayuntamiento < 20000 habitantes
- propietario: Juan García Iturriaga
- Organización: UOC
- Versión: 1.0
- Fecha: 01/12/2018
- Autor: José María Botí Hernández

1.1 Dimensiones de valoración
- [D] disponibilidad
- [I] integridad de los datos
- [C] confidencialidad de los datos
- [A] autenticidad de los usuarios y de la información
- [T] trazabilidad del servicio y de los datos
- [V] Valor (ej. vidas humanas, patromonio corporativo, etc.)
- [DP] Datos personales

2 Dominios de seguridad

dominios de seguridad
- [base] red corporativa

2.1 Agravantes y atenuantes
[base] red corporativa
- [101] Identificación del atacante
- [101.a] público en general
- [102] Motivación del atacante
- [102.a] económica (beneficios en dinero)
- [102.f] con ánimo destructivo
- [102.g] con ánimo de causar daño
- [102.h] con ánimo de provocar pérdidas
- [106] Atracción del objetivo
- [106.a] objetivo muy poco atractivo

- [104] Motivación del personal interno
- [104.c] sobrecargados de trabajo
- [105] Permisos de los usuarios (derechos)
- [105.a] se permite el acceso a Internet
- [105.d] se permite la conexión de dispositivos removibles
- [111] Conectividad del sistema de información
- [111.d] conectado a Internet
- [112] {xor} Ubicación del sistema de información
- [112.a] dentro de una zona controlada

2.2 Valoración de los activos
capa: [essential] Activos esenciales

activo	[D]	[I]	[C]	[A]	[T]	[V]	[DP]
[Exp] Expedientes/Documentos Ayuntamiento		[M](1)	[M](2)	[M](3)	[B](4)		[M](5)
[RGE/RGS] Registro General de Entrada y Salida		[M](1)	[B](6)	[M](3)	[B](7)		[M](8)
[Personal] Datos y servicios personal	[B](9)	[M](10)	[M](11)	[M](12)	[B](13)		[M](8)
[Intervención] Datos y servicios contables, económicos, financieros y presupuestarios	[B](14)	[M](1)	[0](15)	[B](16)	[B](17)		[0](18)
[Tributaria] Datos y servicios de gestión tributaria y recaudación	[B](19)	[M](1)	[B](20)	[M](21)	[B](17)		[B](22)
[PMH] Padrón de Habitantes	[B](9)	[M](1)	[B](20)	[M](21)	[B](23)		[B](22)
[ServSociales] Datos y servicios expedientes Servicios Sociales	[M](24)	[M](1)	[A](25)	[M](26)	[M](27)		[A](28)
[SegCiudadana] Datos y servicios Seguridad Ciudadana	[B](29)	[M](1)	[A](30)	[M](21)	[M](31)		[A](28)
[Gestor] Gestor expedientes municipal	[M](32)			[B](33)	[B](4)		
[Sede electrónica] Tramitación telemática	[B](34)			[M+](35)	[M+](36)		

(1) [M] porque su manipulación o modificación no autorizada causaría un daño importante aunque subsanable
[M] porque su manipulación o modificación no autorizada causaría un daño reputacional importante con los ciudadanos o con otras organizaciones

(2) [M] porque la información deben conocerla sólo quienes lo necesiten para su trabajo, con autorización explícita
[M] porque su revelación causaría un daño reputacional importante con los ciudadanos o con otras organizaciones

(3) [M] porque la falsedad en su origen o en su destinatario causaría un daño importante aunque subsanable
[M] porque la falsedad en su origen o en su destinatario causaría un daño reputacional importante con los ciudadanos o con otras organizaciones

(4) [B] porque la incapacidad para rastrear un acceso al servicio dificultaría la capacidad de subsanar errores
[B] porque la incapacidad para rastrear un acceso al servicio dificultaría la capacidad para perseguir delitos

(5) [B] Se priva de los derechos y libertades de los interesados, por ejemplo, por difamación de un interesado por divulgación de datos personales.
[M] Se agrede contra los derechos y libertades de los interesados, por ejemplo, una citación judicial, entrar en una lista de morosidad o divulgación de datos personales con impacto significativo en la reputación del interesado.

(6) [B] porque la información no deben conocerla personas ajenas a la organización

(7) [B] porque la incapacidad para rastrear un acceso a la información dificultaría la capacidad de subsanar errores
[B] porque la incapacidad para rastrear un acceso a la información dificultaría la capacidad para perseguir delitos
(8) [M] Se agrede contra los derechos y libertades de los interesados, por ejemplo, una citación judicial, entrar en una lista de morosidad o divulgación de datos personales con impacto significativo en la reputación del interesado.
(9) [B] porque la indisponibilidad de la información causaría algún perjuicio
[B] cuando el RTO se sitúa entre 1 y 5 días
[B] porque la detención del servicio causaría algún perjuicio
[B] cuando el RTO se sitúa entre 1 y 5 días
(10) [M] porque su manipulación o modificación no autorizada causaría un daño importante aunque subsanable
(11) [M] porque la información deben conocerla sólo quienes lo necesiten para su trabajo, con autorización explícita
[M] porque su revelación causaría un daño importante aunque subsanable
(12) [M] porque la falsedad en su origen o en su destinatario causaría un daño importante aunque subsanable
(13) [B] Bajo
(14) [B] porque la indisponibilidad de la información causaría algún perjuicio
[B] cuando el RTO se sitúa entre 1 y 5 días
[B] Bajo
[B] porque la detención del servicio causaría algún perjuicio
[B] porque la detención del servicio causaría un daño reputacional apreciable con los ciudadanos o con otras organizaciones
[B] cuando el RTO se sitúa entre 1 y 5 días
(15) [0] Sin valorar
[0] información de carácter público, accesible por cualquier persona
(16) [B] porque la falsedad en su origen o en su destinatario causaría algún perjuicio
[B] porque la falsedad en su origen o en su destinatario causaría algún perjuicio
[B] porque la falsedad en su origen o en su destinatario causaría un daño reputacional apreciable con los ciudadanos o con otras organizaciones
(17) [B] porque la incapacidad para rastrear un acceso a la información dificultaría la capacidad de subsanar errores
[B] porque la incapacidad para rastrear un acceso al servicio dificultaría la capacidad de subsanar errores
(18) [0] Se incumplen obligaciones materiales sin perjuicios relevantes.
(19) [B] porque la indisponibilidad de la información causaría algún perjuicio
[B] porque la indisponibilidad de la información causaría un daño reputacional apreciable con los ciudadanos o con otras organizaciones
[B] cuando el RTO se sitúa entre 1 y 5 días
(20) [B] porque su revelación causaría algún perjuicio
[B] porque su revelación causaría un daño reputacional apreciable con los ciudadanos o con otras organizaciones
(21) [M] porque la falsedad en su origen o en su destinatario causaría un daño importante aunque subsanable
[M] porque la falsedad en su origen o en su destinatario causaría un daño reputacional importante con los ciudadanos o con otras organizaciones
[M] porque la falsedad en su origen o en su destinatario causaría un daño importante aunque subsanable
[M] porque la falsedad en su origen o en su destinatario causaría un daño reputacional importante con los ciudadanos o con otras organizaciones
(22) [B] Costes extra, denegación de acceso a algunos servicios o incumplimiento de obligaciones materiales con perjuicios económicos.
[B] Se priva de los derechos y libertades de los interesados, por ejemplo, por difamación de un interesado por divulgación de datos personales.
(23) [0] cuando no se pueden producir errores de importancia, o son fácilmente reparables por otros medios

[B] porque la incapacidad para rastrear un acceso al servicio dificultaría la capacidad de subsanar errores

(24) [M] porque la indisponibilidad de la información causaría un daño importante aunque subsanable
[M] porque la indisponibilidad de la información podría desembocar en protestas públicas (alteración del orden público)
[M] porque la detención del servicio causaría un daño importante aunque subsanable
[M] porque la detención del servicio podría desembocar en protestas públicas (alteración del orden público)
[B] cuando el RTO se sitúa entre 1 y 5 días

(25) [A] porque su revelación causaría un grave daño, de difícil o imposible recuperación
[A] porque su revelación causaría un daño reputacional grave con los ciudadanos o con otras organizaciones
[M] porque la información deben conocerla sólo quienes lo necesiten para su trabajo, con autorización explícita

(26) [M] porque la falsedad en su origen o en su destinatario causaría un daño importante aunque subsanable
[M] porque la falsedad en su origen o en su destinatario causaría un daño importante aunque subsanable

(27) [B] porque la incapacidad para rastrear un acceso a la información dificultaría la capacidad para perseguir delitos
[M] porque la incapacidad para rastrear un acceso al servicio dificultaría notablemente la capacidad para perseguir delitos

(28) [A] Se agrede significativamente contra los derechos y libertades de los interesados, por ejemplo, padecimiento psicológico con consecuencias a largo plazo o irreparables por la divulgación de datos sensibles.

(29) [B] porque la indisponibilidad de la información causaría algún perjuicio
[B] porque la indisponibilidad de la información causaría un daño reputacional apreciable con los ciudadanos o con otras organizaciones
[B] cuando el RTO se sitúa entre 1 y 5 días
[B] porque la detención del servicio causaría algún perjuicio
[B] porque la detención del servicio causaría un daño reputacional apreciable con los ciudadanos o con otras organizaciones
[B] cuando el RTO se sitúa entre 1 y 5 días

(30) [A] porque la información deben conocerla un número muy reducido de personas
[A] porque su revelación causaría un grave daño, de difícil o imposible recuperación
[A] porque su revelación causaría un daño reputacional grave con los ciudadanos o con otras organizaciones

(31) [M] porque la incapacidad para rastrear un acceso a la información dificultaría notablemente la capacidad para perseguir delitos
[M] porque la incapacidad para rastrear un acceso al servicio impediría o dificultaría notablemente la capacidad de subsanar un error importante

(32) [M] porque la detención del servicio causaría un daño reputacional importante con los ciudadanos o con otras organizaciones
[M] cuando el RTO se sitúa entre 4 horas y un día

(33) [B] porque la falsedad en su origen o en su destinatario causaría algún perjuicio

(34) [M] porque la detención del servicio supondría el incumplimiento material o formal de una norma
[M] porque la detención del servicio causaría un daño reputacional importante con los ciudadanos o con otras organizaciones

(35) [M] porque la falsedad en su origen o en su destinatario causaría un daño importante aunque subsanable
[M] porque la falsedad en su origen o en su destinatario causaría un daño reputacional importante con los ciudadanos o con otras organizaciones
[M+] probablemente sea causa de incumplimiento de una ley o regulación

(36) [M] porque la incapacidad para rastrear un acceso al servicio impediría o dificultaría notablemente la capacidad de subsanar un error importante
[M] porque la incapacidad para rastrear un acceso al servicio dificultaría notablemente la capacidad para perseguir delitos
[M] porque la incapacidad para rastrear un acceso al servicio facilitaría la comisiÛn de delitos
[M+] probablemente sea causa de incumplimiento de una ley o regulación

2.3 Valoración de los dominios

dominio de seguridad	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**	**[V]**	**[DP]**
[base] red corporativa	[M]	[M]	[A]	[M+]	[M+]		[A]

3 Riesgo acumulado

Se presentan los principales riesgos en cada dominio de seguridad del sistema en las diferentes fases de trabajo.

amenaza
presenta la amenaza dentro del catálogo de PILAR. Una amenaza aparece cuando algún activo del sistema está expuesto a ella

D – dimensión
se muestra la dimensión (o dimensiones) de seguridad a las que afecta la amenaza

I – impacto
se muestra el máximo impacto causado por esta amenaza en algún activo del sistema

R – riesgo
se muestra el máximo riesgo al que está expuesto el sistema por causa de esta amenaza

[potencial]
[base] red corporativa

amenaza	D	I	R
[A.11] Acceso no autorizado	C	[A-]	{6,4}
[A.5] Suplantación de la identidad	A	[A]	{6,1}
[A.22] Manipulación de programas	C	[A]	{5,9}
[A.8] Difusión de software dañino	C	[A]	{5,9}

[current] situación actual
[base] red corporativa

amenaza	D	I	R
[A.11] Acceso no autorizado	C	[M]	{4,4}
[A.5] Suplantación de la identidad	A	[M+]	{4,2}
[A.22] Manipulación de programas	C	[M+]	{4,0}

[target] situación objetivo
[base] red corporativa

amenaza	D	I	R

[A.5] Suplantación de la identidad	C, A	[B+]	{2,3}
[A.11] Acceso no autorizado	C	[0]	{1,7}

4 Riesgo repercutido

Se presentan los máximos riesgos a los que están expuestos los activos esenciales del sistema en cada fase de trabajo.

activo
: presenta el activo esencial que está en riesgo; es decir, sobre el que repercute indirectamente la amenaza

amenaza
: presenta la amenaza dentro del catálogo de PILAR.

D – dimensión
: se muestra la dimensión (o dimensiones) de seguridad a las que afecta la amenaza

I – impacto
: se muestra el máximo impacto causado por esta amenaza sobre el activo esencial

R – riesgo
: se muestra el máximo riesgo al que está expuesto el activo esencial por causa de esta amenaza

[potencial]
[base] red corporativa

activo	amenaza	D	I	R
[ServSociales] Datos y servicios expedientes Servicios Sociales	[A.11] Acceso no autorizado	C	[A]	{6,4}
[SegCiudadana] Datos y servicios Seguridad Ciudadana	[A.11] Acceso no autorizado	C	[A]	{6,4}
[ServSociales] Datos y servicios expedientes Servicios Sociales	[A.5] Suplantación de la identidad	C	[A]	{6,1}
[SegCiudadana] Datos y servicios Seguridad Ciudadana	[A.5] Suplantación de la identidad	C	[A]	{6,1}
[ServSociales] Datos y servicios expedientes Servicios Sociales	[A.22] Manipulación de programas	C	[A]	{5,9}
[ServSociales] Datos y servicios expedientes Servicios Sociales	[A.8] Difusión de software dañino	C	[A]	{5,9}
[ServSociales] Datos y servicios expedientes Servicios Sociales	[A.29] Extorsión	C	[A]	{5,9}
[ServSociales] Datos y servicios expedientes Servicios Sociales	[A.30] Ingeniería social (picaresca)	C	[A]	{5,9}
[SegCiudadana] Datos y servicios Seguridad Ciudadana	[A.22] Manipulación de programas	C	[A]	{5,9}
[SegCiudadana] Datos y servicios Seguridad Ciudadana	[A.8] Difusión de software dañino	C	[A]	{5,9}
[SegCiudadana] Datos y servicios Seguridad Ciudadana	[A.29] Extorsión	C	[A]	{5,9}
[SegCiudadana] Datos y servicios Seguridad Ciudadana	[A.30] Ingeniería social (picaresca)	C	[A]	{5,9}
[ServSociales] Datos y servicios expedientes Servicios Sociales	[A.19] Revelación de información	C	[A-]	{5,6}
[ServSociales] Datos y servicios expedientes Servicios Sociales	[A.6] Abuso de privilegios de acceso	C	[A]	{5,6}
[SegCiudadana] Datos y servicios Seguridad	[A.19] Revelación de	C	[A-	{5,6}

Ciudadana	información		]	
[SegCiudadana] Datos y servicios Seguridad Ciudadana	[A.6] Abuso de privilegios de acceso	C	[A]	{5,6}
[ServSociales] Datos y servicios expedientes Servicios Sociales	[A.7] Uso no previsto	C	[A]	{5,3}
[SegCiudadana] Datos y servicios Seguridad Ciudadana	[A.7] Uso no previsto	C	[A]	{5,3}
[Sede electrónica] Tramitación telemática	[A.11] Acceso no autorizado	A	[M]	{5,3}
[ServSociales] Datos y servicios expedientes Servicios Sociales	[E.25] Pérdida de equipos	C	[A]	{5,2}
[SegCiudadana] Datos y servicios Seguridad Ciudadana	[E.25] Pérdida de equipos	C	[A]	{5,2}

[current] situación actual
[base] red corporativa

activo	amenaza	D	I	R
[ServSociales] Datos y servicios expedientes Servicios Sociales	[A.11] Acceso no autorizado	C	[M]	{4,4}
[SegCiudadana] Datos y servicios Seguridad Ciudadana	[A.11] Acceso no autorizado	C	[M]	{4,4}
[ServSociales] Datos y servicios expedientes Servicios Sociales	[A.5] Suplantación de la identidad	C	[M+]	{4,2}
[SegCiudadana] Datos y servicios Seguridad Ciudadana	[A.5] Suplantación de la identidad	C	[M+]	{4,2}
[ServSociales] Datos y servicios expedientes Servicios Sociales	[A.22] Manipulación de programas	C	[M+]	{4,0}
[SegCiudadana] Datos y servicios Seguridad Ciudadana	[A.22] Manipulación de programas	C	[M+]	{4,0}
[ServSociales] Datos y servicios expedientes Servicios Sociales	[A.29] Extorsión	C	[M+]	{3,9}
[ServSociales] Datos y servicios expedientes Servicios Sociales	[A.30] Ingeniería social (picaresca)	C	[M+]	{3,9}
[SegCiudadana] Datos y servicios Seguridad Ciudadana	[A.29] Extorsión	C	[M+]	{3,9}
[SegCiudadana] Datos y servicios Seguridad Ciudadana	[A.30] Ingeniería social (picaresca)	C	[M+]	{3,9}
[ServSociales] Datos y servicios expedientes Servicios Sociales	[A.6] Abuso de privilegios de acceso	C	[M]	{3,8}
[SegCiudadana] Datos y servicios Seguridad Ciudadana	[A.6] Abuso de privilegios de acceso	C	[M]	{3,8}
[ServSociales] Datos y servicios expedientes Servicios Sociales	[A.8] Difusión de software dañino	C	[M]	{3,6}
[SegCiudadana] Datos y servicios Seguridad Ciudadana	[A.8] Difusión de software dañino	C	[M]	{3,6}

[target] situación objetivo
[base] red corporativa

activo	amenaza	D	I	R
[ServSociales] Datos y servicios expedientes Servicios Sociales	[A.5] Suplantación de la identidad	C	[B+]	{2,3}
[SegCiudadana] Datos y servicios Seguridad Ciudadana	[A.5] Suplantación de la identidad	C	[B+]	{2,3}

5 Activos

Relación de activos identificados en el sistema de información.

dominio de seguridad: [base] red corporativa

- Activos esenciales
  - [essential] Activos esenciales
    - [Exp] Expedientes/Documentos Ayuntamiento
    - [RGE/RGS] Registro General de Entrada y Salida
    - [Personal] Datos y servicios personal
    - [Intervención] Datos y servicios contables, económicos, financieros y presupuestarios
    - [Tributaria] Datos y servicios de gestión tributaria y recaudación
    - [PMH] Padrón de Habitantes
    - [ServSociales] Datos y servicios expedientes Servicios Sociales
    - [SegCiudadana] Datos y servicios Seguridad Ciudadana
    - [Gestor] Gestor expedientes municipal
    - [Sede electrónica] Tramitación telemática
- activos
  - [arch.ip] sistema de protección de frontera lógica
    - [Firewall] Firewall UTM con DMZ
  - [arch.pps] sistema de protección física del perímetro
    - [oficinas] Edificios municipales
    - [cpd] Centro de Proceso de Datos
  - [S.3rd] contratado a terceros
    - [web] Webs corporativas
    - [inet] Conexión a Internet
    - [email] Correo electrónico
  - [D] Datos / Información
    - [D.files] ficheros de datos
    - [D.e-files] ficheros cifrados
    - [D.backup] copias de respaldo
    - [D.conf] datos de configuración
    - [D.int] datos de gestión interna
    - [D.password] credenciales (ej. contraseñas)
    - [D.acl] datos de control de acceso
    - [D.log] registro de actividad (log)
    - [D.multimedia] multimedia
    - [D.source] código fuente
    - [D.exe] código ejecutable
  - [keys] Claves criptográficas
    - [keys.info.encrypt] claves de cifra
    - [keys.info.sign] claves de firma
    - [keys.com.channel] claves de cifrado del canal
    - [keys.com.authentication] claves de autenticación
    - [keys.x509] certificados de clave pública
  - [S] Servicios
    - [S] Servicios
    - [S.prov.pub] al público en general (sin relación contractual)
    - [S.prov.int] interno (usuarios y medios de la propia organización)
    - [S.prov.www] world wide web
    - [S.prov.file] almacenamiento de ficheros
    - [S.prov.print] servicio de impresión
    - [S.prov.pki.ra] autoridad de registro
  - [SW] Aplicaciones (software)
    - [SW.prp] desarrollo propio (in house)
    - [SW.sub] desarrollo a medida (subcontratado)
    - [SW.std.browser] navegador web
    - [SW.std.www] servidor de presentación

  - [SW.std.app] servidor de aplicaciones
  - [SW.std.email_client] cliente de correo electrónico
  - [SW.std.email_server] servidor de correo electrónico
  - [SW.std.directory] servidor de directorio
  - [SW.std.file] servidor de ficheros
  - [SW.std.dbms] sistema de gestión de bases de datos
  - [SW.std.office] ofimática
  - [SW.std.os] sistema operativo
  - [SW.std.os.windows] windows
  - [SW.std.os.linux] linux
  - [SW.std.hypervisor] hypervisor (gestor de la máquina virtual)
  - [SW.std.backup] servidor de backup
  - [SW.sec.av] anti virus
  - [SW.sec.ids] IDS / IPS (deteción / prevención de intrusion)
  - [SW.sec.dlp] prevención de pérdida de datos
  - [SW.sec.traf] análisis de tráfico
  - [SW.sec.hp] honey pot
- [HW] Equipamiento informático (hardware)
  - [HW] Equipamiento informático (hardware)
  - [HW.mid] equipos medios
  - [HW.pc] informática personal
  - [HW.mobile] informática móvil
  - [HW.vhost] equipos virtuales (máquinas virtuales)
  - [HW.backup] equipamiento de respaldo
  - [HW.data] que almacena datos
  - [HW.network.switch] conmutador
  - [HW.network.router] encaminador
  - [HW.network.wap] punto de acceso wireless
- [COM] Redes de comunicaciones
  - [COM.ADSL] ADSL
  - [COM.wifi] WiFi
  - [COM.LAN] red local
  - [COM.VLAN] LAN virtual
  - [COM.vpn] canal cifrado (red privada virtual)
  - [COM.backup] comunicaciones de respaldo
- [Media] Soportes de información
  - [Media.electronic.disk] discos
  - [Media.electronic.vdisk] discos virtuales
  - [Media.electronic.san] almacenamiento en red
- [AUX] Equipamiento auxiliar
  - [AUX.ups] sai - sistemas de alimentación ininterrumpida
  - [AUX.cabling] cableado de datos
- [L] Instalaciones
  - [L.local] cuarto
- [P] Personal
  - [P.ui] usuarios internos
  - [P.op] operadores
  - [P.adm] administradores de sistemas
  - [P.com] administradores de comunicaciones
  - [P.dba] administradores de BBDD
  - [P.sec] administradores de seguridad
  - [P.prov] proveedores

7.2 Documento Declaración de Aplicabilidad obtenido en µPILAR

1. Introducción

Código: TFM - MISTIC - JMBH
Nombre: Ayuntamiento < 20000 habitantes

Descripción:

Datos administrativos:

- Descripción: Ayuntamiento < 20000 habitantes
- propietario: Juan García Iturriaga
- Organización: UOC
- Versión: 1.0
- Fecha: 01/12/2018
- Autor: José María Botí Hernández

2. Dominios de seguridad

[base] red corporativa

3. Valoración de los activos

capa: [essential] Activos esenciales

Activos esenciales

activo	[D]	[I]	[C]	[A]	[T]	[V]	[DP]
[Exp] Expedientes/Documentos Ayuntamiento		[M](1)	[M](2)	[M](3)	[B](4)		[M](5)
[RGE/RGS] Registro General de Entrada y Salida		[M](1)	[B](6)	[M](3)	[B](7)		[M](8)
[Personal] Datos y servicios personal	[B](9)	[M](10)	[M](11)	[M](12)	[B](13)		[M](8)
[Intervención] Datos y servicios contables, económicos, financieros y presupuestarios	[B](14)	[M](1)	[0](15)	[B](16)	[B](17)		[0](18)
[Tributaria] Datos y servicios de gestión tributaria y recaudación	[B](19)	[M](1)	[B](20)	[M](21)	[B](17)		[B](22)
[PMH] Padrón de Habitantes	[B](9)	[M](1)	[B](20)	[M](21)	[B](23)		[B](22)
[ServSociales] Datos y servicios expedientes Servicios Sociales	[M](24)	[M](1)	[A](25)	[M](26)	[M](27)		[A](28)
[SegCiudadana] Datos y servicios Seguridad Ciudadana	[B](29)	[M](1)	[A](30)	[M](21)	[M](31)		[A](28)
[Gestor] Gestor expedientes municipal	[M](32)			[B](33)	[B](4)		
[Sede electrónica] Tramitación telemática	[B](34)			[M+](35)	[M+](36)		

(1) [M] porque su manipulación o modificación no autorizada causaría un daño importante aunque subsanable

[M] porque su manipulación o modificación no autorizada causaría un daño reputacional importante con los ciudadanos o con otras organizaciones

(2) [M] porque la información deben conocerla sólo quienes lo necesiten para su trabajo, con autorización explícita
[M] porque su revelación causaría un daño reputacional importante con los ciudadanos o con otras organizaciones

(3) [M] porque la falsedad en su origen o en su destinatario causaría un daño importante aunque subsanable
[M] porque la falsedad en su origen o en su destinatario causaría un daño reputacional importante con los ciudadanos o con otras organizaciones

(4) [B] porque la incapacidad para rastrear un acceso al servicio dificultaría la capacidad de subsanar errores
[B] porque la incapacidad para rastrear un acceso al servicio dificultaría la capacidad para perseguir delitos

(5) [B] Se priva de los derechos y libertades de los interesados, por ejemplo, por difamación de un interesado por divulgación de datos personales.
[M] Se agrede contra los derechos y libertades de los interesados, por ejemplo, una citación judicial, entrar en una lista de morosidad o divulgación de datos personales con impacto significativo en la reputación del interesado.

(6) [B] porque la información no deben conocerla personas ajenas a la organización

(7) [B] porque la incapacidad para rastrear un acceso a la información dificultaría la capacidad de subsanar errores
[B] porque la incapacidad para rastrear un acceso a la información dificultaría la capacidad para perseguir delitos

(8) [M] Se agrede contra los derechos y libertades de los interesados, por ejemplo, una citación judicial, entrar en una lista de morosidad o divulgación de datos personales con impacto significativo en la reputación del interesado.

(9) [B] porque la indisponibilidad de la información causaría algún perjuicio
[B] cuando el RTO se sitúa entre 1 y 5 días
[B] porque la detención del servicio causaría algún perjuicio
[B] cuando el RTO se sitúa entre 1 y 5 días

(10) [M] porque su manipulación o modificación no autorizada causaría un daño importante aunque subsanable

(11) [M] porque la información deben conocerla sólo quienes lo necesiten para su trabajo, con autorización explícita
[M] porque su revelación causaría un daño importante aunque subsanable

(12) [M] porque la falsedad en su origen o en su destinatario causaría un daño importante aunque subsanable

(13) [B] Bajo

(14) [B] porque la indisponibilidad de la información causaría algún perjuicio
[B] cuando el RTO se sitúa entre 1 y 5 días
[B] Bajo
[B] porque la detención del servicio causaría algún perjuicio
[B] porque la detención del servicio causaría un daño reputacional apreciable con los ciudadanos o con otras organizaciones
[B] cuando el RTO se sitúa entre 1 y 5 días

(15) [0] Sin valorar
[0] información de carácter público, accesible por cualquier persona

(16) [B] porque la falsedad en su origen o en su destinatario causaría algún perjuicio
[B] porque la falsedad en su origen o en su destinatario causaría algún perjuicio
[B] porque la falsedad en su origen o en su destinatario causaría un daño reputacional apreciable con los ciudadanos o con otras organizaciones

(17) [B] porque la incapacidad para rastrear un acceso a la información dificultaría la capacidad de subsanar errores
[B] porque la incapacidad para rastrear un acceso al servicio dificultaría la capacidad de subsanar errores

(18) [0] Se incumplen obligaciones materiales sin perjuicios relevantes.

(19) [B] porque la indisponibilidad de la información causaría algún perjuicio
[B] porque la indisponibilidad de la información causaría un daño reputacional apreciable con los ciudadanos o con otras organizaciones
[B] cuando el RTO se sitúa entre 1 y 5 días

(20) [B] porque su revelación causaría algún perjuicio
[B] porque su revelación causaría un daño reputacional apreciable con los ciudadanos o con otras organizaciones

(21) [M] porque la falsedad en su origen o en su destinatario causaría un daño importante aunque subsanable
[M] porque la falsedad en su origen o en su destinatario causaría un daño reputacional importante con los ciudadanos o con otras organizaciones
[M] porque la falsedad en su origen o en su destinatario causaría un daño importante aunque subsanable
[M] porque la falsedad en su origen o en su destinatario causaría un daño reputacional importante con los ciudadanos o con otras organizaciones

(22) [B] Costes extra, denegación de acceso a algunos servicios o incumplimiento de obligaciones materiales con perjuicios económicos.
[B] Se priva de los derechos y libertades de los interesados, por ejemplo, por difamación de un interesado por divulgación de datos personales.

(23) [0] cuando no se pueden producir errores de importancia, o son fácilmente reparables por otros medios
[B] porque la incapacidad para rastrear un acceso al servicio dificultaría la capacidad de subsanar errores

(24) [M] porque la indisponibilidad de la información causaría un daño importante aunque subsanable
[M] porque la indisponibilidad de la información podría desembocar en protestas públicas (alteración del orden público)
[M] porque la detención del servicio causaría un daño importante aunque subsanable
[M] porque la detención del servicio podría desembocar en protestas públicas (alteración del orden público)
[B] cuando el RTO se sitúa entre 1 y 5 días

(25) [A] porque su revelación causaría un grave daño, de difícil o imposible recuperación
[A] porque su revelación causaría un daño reputacional grave con los ciudadanos o con otras organizaciones
[M] porque la información deben conocerla sólo quienes lo necesiten para su trabajo, con autorización explícita

(26) [M] porque la falsedad en su origen o en su destinatario causaría un daño importante aunque subsanable
[M] porque la falsedad en su origen o en su destinatario causaría un daño importante aunque subsanable

(27) [B] porque la incapacidad para rastrear un acceso a la información dificultaría la capacidad para perseguir delitos
[M] porque la incapacidad para rastrear un acceso al servicio dificultaría notablemente la capacidad para perseguir delitos

(28) [A] Se agrede significativamente contra los derechos y libertades de los interesados, por ejemplo, padecimiento psicológico con consecuencias a largo plazo o irreparables por la divulgación de datos sensibles.

(29) [B] porque la indisponibilidad de la información causaría algún perjuicio
[B] porque la indisponibilidad de la información causaría un daño reputacional apreciable con los ciudadanos o con otras organizaciones
[B] cuando el RTO se sitúa entre 1 y 5 días
[B] porque la detención del servicio causaría algún perjuicio
[B] porque la detención del servicio causaría un daño reputacional apreciable con los ciudadanos o con otras organizaciones
[B] cuando el RTO se sitúa entre 1 y 5 días

(30) [A] porque la información deben conocerla un número muy reducido de personas
[A] porque su revelación causaría un grave daño, de difícil o imposible recuperación
[A] porque su revelación causaría un daño reputacional grave con los ciudadanos o con otras organizaciones

(31) [M] porque la incapacidad para rastrear un acceso a la información dificultaría notablemente la capacidad para perseguir delitos
[M] porque la incapacidad para rastrear un acceso al servicio impediría o dificultaría notablemente la capacidad de subsanar un error importante

(32) [M] porque la detención del servicio causaría un daño reputacional importante con los ciudadanos o con otras organizaciones
[M] cuando el RTO se sitúa entre 4 horas y un día

(33) [B] porque la falsedad en su origen o en su destinatario causaría algún perjuicio

(34) [M] porque la detención del servicio supondría el incumplimiento material o formal de una norma
[M] porque la detención del servicio causaría un daño reputacional importante con los ciudadanos o con otras organizaciones

(35) [M] porque la falsedad en su origen o en su destinatario causaría un daño importante aunque subsanable
[M] porque la falsedad en su origen o en su destinatario causaría un daño reputacional importante con los ciudadanos o con otras organizaciones
[M+] probablemente sea causa de incumplimiento de una ley o regulación

(36) [M] porque la incapacidad para rastrear un acceso al servicio impediría o dificultaría notablemente la capacidad de subsanar un error importante
[M] porque la incapacidad para rastrear un acceso al servicio dificultaría notablemente la capacidad para perseguir delitos
[M] porque la incapacidad para rastrear un acceso al servicio facilitaría la comisiÛn de delitos
[M+] probablemente sea causa de incumplimiento de una ley o regulación

Categoría del sistema
[base] red corporativa
ALTA

4. Medidas de Seguridad (Anexo II del ENS)

[org] Marco organizativo

dominio de seguridad: [base] red corporativa

control	aplica
[org] Marco organizativo	M
[org.1] Política de Seguridad	M
[org.2] Normativa de seguridad	M
[org.3] Procedimientos de seguridad	M
[org.4] Proceso de autorización	M

[op] Marco operacional

[op.pl] Planificación

dominio de seguridad: [base] red corporativa

control	aplica
[op] Marco operacional	M
[op.pl] Planificación	M
[op.pl.1] Análisis de riesgos	M
[op.pl.2] Arquitectura de seguridad	M
[op.pl.3] Adquisición de nuevos componentes	M
[op.pl.4] Dimensionamiento / Gestión de capacidades	M
[op.pl.5] Componentes certificados	M

[op.acc] Control de acceso

dominio de seguridad: [base] red corporativa

control	aplica
[op] Marco operacional	M
[op.acc] Control de acceso	M
[op.acc.1] Identificación	M
[op.acc.2] Requisitos de acceso	M
[op.acc.3] Segregación de funciones y tareas	M
[op.acc.4] Proceso de gestión de derechos de acceso	M
[op.acc.5] Mecanismo de autenticación	M
[op.acc.6] Acceso local (local logon)	M
[op.acc.7] Acceso remoto (remote login)	M

[op.exp] Explotación
dominio de seguridad: [base] red corporativa

control	aplica
[op] Marco operacional	M
[op.exp] Explotación	M
[op.exp.1] Inventario de activos	M
[op.exp.2] Configuración de seguridad	M
[op.exp.3] Gestión de la configuración	M
[op.exp.4] Mantenimiento	M
[op.exp.5] Gestión de cambios	M
[op.exp.6] Protección frente a código dañino	M
[op.exp.7] Gestión de incidentes	M
[op.exp.8] Registro de la actividad de los usuarios	M
[op.exp.9] Registro de la gestión de incidentes	M
[op.exp.10] Protección de los registros de actividad	sí
[op.exp.11] Protección de claves criptográficas	M

[op.ext] Servicios externos
dominio de seguridad: [base] red corporativa

control	aplica
[op] Marco operacional	M
[op.ext] Servicios externos	M
[op.ext.1] Contratación y acuerdos de nivel de servicio	M
[op.ext.2] Gestión diaria	M
[op.ext.9] Medios alternativos	sí

[op.cont] Continuidad del servicio
dominio de seguridad: [base] red corporativa

control	aplica
[op] Marco operacional	M
[op.cont] Continuidad del servicio	M
[op.cont.1] Análisis de impacto	M
[op.cont.2] Plan de continuidad	sí
[op.cont.3] Pruebas periódicas	sí

[op.mon] Montorización del sistema
dominio de seguridad: [base] red corporativa

control	aplica
[op] Marco operacional	M

[op.mon] Monitorización del sistema	M
[op.mon.1] Detección de intrusión	M
[op.mon.2] Sistema de métricas	M

[mp] Medidas de protección

[mp.if] Protección de las instalaciones e infraestructuras
dominio de seguridad: [base] red corporativa

control	aplica
[mp] Medidas de protección	M
[mp.if] Protección de las instalaciones e infraestructuras	M
[mp.if.1] Áreas separadas y con control de acceso	M
[mp.if.2] Identificación de las personas	M
[mp.if.3] Acondicionamiento de los locales	M
[mp.if.4] Energía eléctrica	M
[mp.if.5] Protección frente a incendios	M
[mp.if.6] Protección frente a inundaciones	M
[mp.if.7] Registro de entrada y salida de equipamiento	M
[mp.if.9] Instalaciones alternativas	sí

[mp.per] Gestión del personal
dominio de seguridad: [base] red corporativa

control	aplica
[mp] Medidas de protección	M
[mp.per] Gestión del personal	M /n.a.
[mp.per.1] Caracterización del puesto de trabajo	M /n.a.
[mp.per.2] Deberes y obligaciones	M /n.a.
[mp.per.3] Concienciación	M /n.a.
[mp.per.4] Formación	M /n.a.
[mp.per.9] Personal alternativo	n.a.

[mp.eq] Protección de los equipos
dominio de seguridad: [base] red corporativa

control	aplica
[mp] Medidas de protección	M
[mp.if] Protección de las instalaciones e infraestructuras	M
[mp.if.1] Áreas separadas y con control de acceso	M
[mp.if.2] Identificación de las personas	M
[mp.if.3] Acondicionamiento de los locales	M
[mp.if.4] Energía eléctrica	M
[mp.if.5] Protección frente a incendios	M
[mp.if.6] Protección frente a inundaciones	M
[mp.if.7] Registro de entrada y salida de equipamiento	M

[mp.if.9] Instalaciones alternativas	sí

[mp.com] Protección de las comunicaciones
dominio de seguridad: [base] red corporativa

control	aplica
[mp] Medidas de protección	M
[mp.com] Protección de las comunicaciones	M
[mp.com.1] Perímetro seguro	M
[mp.com.2] Protección de la confidencialidad	M
[mp.com.3] Protección de la autenticidad y de la integridad	M
[mp.com.4] Segregación de redes	M
[mp.com.9] Medios alternativos	sí

[mp.si] Protección de los soportes de información
dominio de seguridad: [base] red corporativa

control	aplica
[mp] Medidas de protección	M
[mp.si] Protección de los soportes de información	M
[mp.si.1] Etiquetado	M
[mp.si.2] Criptografía	M
[mp.si.3] Custodia	M
[mp.si.4] Transporte	M /n.a.
[mp.si.5] Borrado y destrucción	M

[mp.sw] Protección de las aplicaciones informáticas (SW)
dominio de seguridad: [base] red corporativa

control	aplica
[mp] Medidas de protección	M
[mp.sw] Protección de las aplicaciones informáticas (SW)	M
[mp.sw.1] Desarrollo de aplicaciones	M
[mp.sw.2] Aceptación y puesta en servicio	M

[mp.info] Protección de la información
dominio de seguridad: [base] red corporativa

control	aplica
[mp] Medidas de protección	M
[mp.info] Protección de la información	M
[mp.info.1] Datos de carácter personal	M
[mp.info.2] Calificación de la información	M

[mp.info.3] Cifrado de la información	M
[mp.info.4] Firma electrónica	M
[mp.info.5] Sellos de tiempo	sí
[mp.info.6] Limpieza de documentos	M
[mp.info.9] Copias de seguridad (backup)	M

[mp.s] Protección de los servicios

dominio de seguridad: [base] red corporativa

control	**aplica**
[mp] Medidas de protección	M
[mp.s] Protección de los servicios	M
[mp.s.1] Protección del correo electrónico (e-mail)	sí
[mp.s.2] Protección de servicios y aplicaciones web	M
[mp.s.8] Protección frente a la denegación de servicio	M
[mp.s.9] Medios alternativos	sí

7.3 Documento Cumplimiento ENS en µPILAR

1 Introducción

Código: TFM - MISTIC - JMBH
Nombre: Ayuntamiento < 20000 habitantes

Descripción:

Datos administrativos:

- Descripción: Ayuntamiento < 20000 habitantes
- propietario: Juan García Iturriaga
- Organización: UOC
- Versión: 1.0
- Fecha: 01/12/2018
- Autor: José María Botí Hernández

2 Dominios de seguridad

[base] red corporativa

Valoración de los dominios

dominio de seguridad	[D]	[I]	[C]	[A]	[T]	[V]	[DP]
[base] red corporativa	[M]	[M]	[A]	[M+]	[M+]		[A]

Categoría del sistema
[base] red corporativa
ALTA

3 Medidas de Seguridad (Anexo II del ENS)

3.1 [org] Marco organizativo

fase: [current] situación actual

control	base	
[org] Marco organizativo	96%	
[org.1] Política de Seguridad	100%	
[org.2] Normativa de seguridad	77%	<
[org.3] Procedimientos de seguridad	62%	<
[org.4] Proceso de autorización	100%	

fase: [target] situación objetivo

control	base	
[org] Marco organizativo	100%	
[org.1] Política de Seguridad	100%	
[org.2] Normativa de seguridad	100%	
[org.3] Procedimientos de seguridad	100%	
[org.4] Proceso de autorización	100%	

3.2 [op] Marco operacional

fase: [current] situación actual

control	base	
[op] Marco operacional	81%	<
[op.pl] Planificación	69%	<
[op.acc] Control de acceso	70%	<
[op.exp] Explotación	72%	<
[op.ext] Servicios externos	85%	<
[op.cont] Continuidad del servicio	100%	
[op.mon] Monitorización del sistema	76%	<

fase: [target] situación objetivo

control	base	
[op] Marco operacional	100%	
[op.pl] Planificación	100%	
[op.acc] Control de acceso	100%	
[op.exp] Explotación	100%	
[op.ext] Servicios externos	100%	
[op.cont] Continuidad del servicio	100%	
[op.mon] Monitorización del sistema	100%	

3.2.1 [op.pl] Planificación

fase: [current] situación actual

control	base	
[op] Marco operacional	81%	<
[op.pl] Planificación	69%	<
[op.pl.1] Análisis de riesgos	100%	
[op.pl.2] Arquitectura de seguridad	34%	<
[op.pl.3] Adquisición de nuevos componentes	68%	<
[op.pl.4] Dimensionamiento / Gestión de capacidades	81%	<
[op.pl.5] Componentes certificados	62%	<

fase: [target] situación objetivo

control	base	
[op] Marco operacional	100%	
[op.pl] Planificación	100%	
[op.pl.1] Análisis de riesgos	100%	
[op.pl.2] Arquitectura de seguridad	100%	
[op.pl.3] Adquisición de nuevos componentes	100%	
[op.pl.4] Dimensionamiento / Gestión de capacidades	100%	
[op.pl.5] Componentes certificados	100%	

3.2.2 [op.acc] Control de acceso

fase: [current] situación actual

control	base	
[op] Marco operacional	81%	<
[op.acc] Control de acceso	70%	<
[op.acc.1] Identificación	100%	
[op.acc.2] Requisitos de acceso	75%	<
[op.acc.3] Segregación de funciones y tareas	29%	<
[op.acc.4] Proceso de gestión de derechos de acceso	100%	
[op.acc.5] Mecanismo de autenticación	63%	<
[op.acc.6] Acceso local (local logon)	32%	<
[op.acc.7] Acceso remoto (remote login)	82%	<

fase: [target] situación objetivo

control	base	
[op] Marco operacional	100%	
[op.acc] Control de acceso	100%	
[op.acc.1] Identificación	100%	
[op.acc.2] Requisitos de acceso	100%	
[op.acc.3] Segregación de funciones y tareas	100%	
[op.acc.4] Proceso de gestión de derechos de acceso	100%	
[op.acc.5] Mecanismo de autenticación	98%	
[op.acc.6] Acceso local (local logon)	100%	
[op.acc.7] Acceso remoto (remote login)	98%	

3.2.3 [op.exp] Explotación

fase: [current] situación actual

control	base	
[op] Marco operacional	81%	<
[op.exp] Explotación	72%	<
[op.exp.1] Inventario de activos	100%	
[op.exp.2] Configuración de seguridad	81%	<
[op.exp.3] Gestión de la configuración	65%	<
[op.exp.4] Mantenimiento	75%	<
[op.exp.5] Gestión de cambios	80%	<
[op.exp.6] Protección frente a código dañino	56%	<
[op.exp.7] Gestión de incidentes	59%	<
[op.exp.8] Registro de la actividad de los usuarios	28%	<
[op.exp.9] Registro de la gestión de incidentes	71%	<
[op.exp.10] Protección de los registros de actividad	n.a.	
[op.exp.11] Protección de claves criptográficas	100%	

fase: [target] situación objetivo

control	base	
[op] Marco operacional	100%	
[op.exp] Explotación	100%	
[op.exp.1] Inventario de activos	100%	
[op.exp.2] Configuración de seguridad	100%	
[op.exp.3] Gestión de la configuración	100%	
[op.exp.4] Mantenimiento	100%	
[op.exp.5] Gestión de cambios	100%	
[op.exp.6] Protección frente a código dañino	89%	<
[op.exp.7] Gestión de incidentes	100%	
[op.exp.8] Registro de la actividad de los usuarios	100%	
[op.exp.9] Registro de la gestión de incidentes	100%	
[op.exp.10] Protección de los registros de actividad	n.a.	
[op.exp.11] Protección de claves criptográficas	100%	

3.2.4 [op.ext] Servicios externos

fase: [current] situación actual

control	base	
[op] Marco operacional	81%	<
[op.ext] Servicios externos	85%	<
[op.ext.1] Contratación y acuerdos de nivel de servicio	77%	<
[op.ext.2] Gestión diaria	76%	<
[op.ext.9] Medios alternativos		

fase: [target] situación objetivo

control	base	
[op] Marco operacional	100%	
[op.ext] Servicios externos	100%	
[op.ext.1] Contratación y acuerdos de nivel de servicio	100%	
[op.ext.2] Gestión diaria	100%	
[op.ext.9] Medios alternativos		

3.2.5 [op.cont] Continuidad del servicio

fase: [current] situación actual

control	base	
[op] Marco operacional	81%	<
[op.cont] Continuidad del servicio	100%	
[op.cont.1] Análisis de impacto	100%	
[op.cont.2] Plan de continuidad		
[op.cont.3] Pruebas periódicas		

fase: [target] situación objetivo

control	base	
[op] Marco operacional	100%	
[op.cont] Continuidad del servicio	100%	
[op.cont.1] Análisis de impacto	100%	
[op.cont.2] Plan de continuidad		
[op.cont.3] Pruebas periódicas		

3.2.6 [op.mon] Montorización del sistema

fase: [current] situación actual

control	base	
[op] Marco operacional	81%	<
[op.mon] Monitorización del sistema	76%	<
[op.mon.1] Detección de intrusión	89%	<
[op.mon.2] Sistema de métricas	62%	<

fase: [target] situación objetivo

control	base	
[op] Marco operacional	100%	
[op.mon] Monitorización del sistema	100%	
[op.mon.1] Detección de intrusión	100%	
[op.mon.2] Sistema de métricas	100%	

3.3 [mp] Medidas de protección

fase: [current] situación actual

control	base	
[mp] Medidas de protección	84%	<
[mp.if] Protección de las instalaciones e infraestructuras	81%	<
[mp.per] Gestión del personal	n.a.	
[mp.eq] Protección de los equipos	96%	
[mp.com] Protección de las comunicaciones	77%	<
[mp.si] Protección de los soportes de información	100%	

[mp.sw] Protección de las aplicaciones informáticas (SW)	78%	<
[mp.info] Protección de la información	73%	<
[mp.s] Protección de los servicios	79%	<

fase: [target] situación objetivo

control	base	
[mp] Medidas de protección	100%	
[mp.if] Protección de las instalaciones e infraestructuras	100%	
[mp.per] Gestión del personal	n.a.	
[mp.eq] Protección de los equipos	100%	
[mp.com] Protección de las comunicaciones	97%	
[mp.si] Protección de los soportes de información	100%	
[mp.sw] Protección de las aplicaciones informáticas (SW)	100%	
[mp.info] Protección de la información	100%	
[mp.s] Protección de los servicios	100%	

3.3.1 [mp.if] Protección de las instalaciones e infraestructuras

fase: [current] situación actual

control	base	
[mp] Medidas de protección	84%	<
[mp.if] Protección de las instalaciones e infraestructuras	81%	<
[mp.if.1] Áreas separadas y con control de acceso	59%	<
[mp.if.2] Identificación de las personas	56%	<
[mp.if.3] Acondicionamiento de los locales	96%	
[mp.if.4] Energía eléctrica	78%	<
[mp.if.5] Protección frente a incendios	89%	<
[mp.if.6] Protección frente a inundaciones	89%	<
[mp.if.7] Registro de entrada y salida de equipamiento	100%	
[mp.if.9] Instalaciones alternativas		

fase: [target] situación objetivo

control	base	
[mp] Medidas de protección	100%	
[mp.if] Protección de las instalaciones e infraestructuras	100%	
[mp.if.1] Áreas separadas y con control de acceso	94%	
[mp.if.2] Identificación de las personas	100%	
[mp.if.3] Acondicionamiento de los locales	100%	
[mp.if.4] Energía eléctrica	100%	
[mp.if.5] Protección frente a incendios	100%	
[mp.if.6] Protección frente a inundaciones	89%	<
[mp.if.7] Registro de entrada y salida de equipamiento	100%	
[mp.if.9] Instalaciones alternativas		

3.3.2 [mp.per] Gestión del personal

fase: [current] situación actual

control	base	
[mp] Medidas de protección	84%	<
[mp.per] Gestión del personal	n.a.	

[mp.per.1] Caracterización del puesto de trabajo	n.a.	
[mp.per.2] Deberes y obligaciones	n.a.	
[mp.per.3] Concienciación	n.a.	
[mp.per.4] Formación	n.a.	
[mp.per.9] Personal alternativo	n.a.	

fase: [target] situación objetivo

control	base	
[mp] Medidas de protección	100%	
[mp.per] Gestión del personal	n.a.	
[mp.per.1] Caracterización del puesto de trabajo	n.a.	
[mp.per.2] Deberes y obligaciones	n.a.	
[mp.per.3] Concienciación	n.a.	
[mp.per.4] Formación	n.a.	
[mp.per.9] Personal alternativo	n.a.	

3.3.3 [mp.eq] Protección de los equipos

fase: [current] situación actual

control	base	
[mp] Medidas de protección	84%	<
[mp.eq] Protección de los equipos	96%	
[mp.eq.1] Puesto de trabajo despejado	100%	
[mp.eq.2] Bloqueo del puesto de trabajo	100%	
[mp.eq.3] Protección de equipos portátiles	100%	
[mp.eq.9] Medios alternativos	48%	<

fase: [target] situación objetivo

control	base	
[mp] Medidas de protección	100%	
[mp.eq] Protección de los equipos	100%	
[mp.eq.1] Puesto de trabajo despejado	100%	
[mp.eq.2] Bloqueo del puesto de trabajo	100%	
[mp.eq.3] Protección de equipos portátiles	100%	
[mp.eq.9] Medios alternativos	76%	<

3.3.4 [mp.com] Protección de las comunicaciones

fase: [current] situación actual

control	base	
[mp] Medidas de protección	84%	<
[mp.com] Protección de las comunicaciones	77%	<
[mp.com.1] Perímetro seguro	91%	
[mp.com.2] Protección de la confidencialidad	75%	<
[mp.com.3] Protección de la autenticidad y de la integridad	77%	<
[mp.com.4] Segregación de redes	89%	<
[mp.com.9] Medios alternativos		

fase: [target] situación objetivo

control	base	
[mp] Medidas de protección	100%	
[mp.com] Protección de las comunicaciones	97%	
[mp.com.1] Perímetro seguro	100%	
[mp.com.2] Protección de la confidencialidad	84%	<
[mp.com.3] Protección de la autenticidad y de la integridad	76%	<
[mp.com.4] Segregación de redes	100%	
[mp.com.9] Medios alternativos		

3.3.5 [mp.si] Protección de los soportes de información

fase: [current] situación actual

control	base	
[mp] Medidas de protección	84%	<
[mp.si] Protección de los soportes de información	100%	
[mp.si.1] Etiquetado	100%	
[mp.si.2] Criptografía	100%	
[mp.si.3] Custodia	81%	<
[mp.si.4] Transporte	n.a.	
[mp.si.5] Borrado y destrucción	100%	

fase: [target] situación objetivo

control	base	
[mp] Medidas de protección	100%	
[mp.si] Protección de los soportes de información	100%	
[mp.si.1] Etiquetado	100%	
[mp.si.2] Criptografía	100%	
[mp.si.3] Custodia	100%	
[mp.si.4] Transporte	n.a.	
[mp.si.5] Borrado y destrucción	100%	

3.3.6 [mp.sw] Protección de las aplicaciones informáticas (SW)

fase: [current] situación actual

control	base	
[mp] Medidas de protección	84%	<
[mp.sw] Protección de las aplicaciones informáticas (SW)	78%	<
[mp.sw.1] Desarrollo de aplicaciones	92%	
[mp.sw.2] Aceptación y puesta en servicio	65%	<

fase: [target] situación objetivo

control	base	
[mp] Medidas de protección	100%	
[mp.sw] Protección de las aplicaciones informáticas (SW)	100%	
[mp.sw.1] Desarrollo de aplicaciones	100%	
[mp.sw.2] Aceptación y puesta en servicio	100%	

3.3.7 [mp.info] Protección de la información

fase: [current] situación actual

control	base	
[mp] Medidas de protección	84%	<
[mp.info] Protección de la información	73%	<
[mp.info.1] Datos de carácter personal	100%	
[mp.info.2] Calificación de la información	87%	<
[mp.info.3] Cifrado de la información	58%	<
[mp.info.4] Firma electrónica	99%	
[mp.info.5] Sellos de tiempo		
[mp.info.6] Limpieza de documentos	0%	<
[mp.info.9] Copias de seguridad (backup)	85%	<

fase: [target] situación objetivo

control	base	
[mp] Medidas de protección	100%	
[mp.info] Protección de la información	100%	
[mp.info.1] Datos de carácter personal	100%	
[mp.info.2] Calificación de la información	100%	
[mp.info.3] Cifrado de la información	100%	
[mp.info.4] Firma electrónica	53%	<
[mp.info.5] Sellos de tiempo		
[mp.info.6] Limpieza de documentos	100%	
[mp.info.9] Copias de seguridad (backup)	100%	

3.3.8 [mp.s] Protección de los servicios

fase: [current] situación actual

control	base	
[mp] Medidas de protección	84%	<
[mp.s] Protección de los servicios	79%	<
[mp.s.1] Protección del correo electrónico (e-mail)	n.a.	
[mp.s.2] Protección de servicios y aplicaciones web	100%	
[mp.s.8] Protección frente a la denegación de servicio	49%	<
[mp.s.9] Medios alternativos		

fase: [target] situación objetivo

control	base	
[mp] Medidas de protección	100%	
[mp.s] Protección de los servicios	100%	
[mp.s.1] Protección del correo electrónico (e-mail)	n.a.	
[mp.s.2] Protección de servicios y aplicaciones web	100%	
[mp.s.8] Protección frente a la denegación de servicio	100%	
[mp.s.9] Medios alternativos		