Adecuación de una Administración Pública al Nuevo Reglamento Europeo 2016/679

Juan Francisco Claramunt Canet
Máster universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones

Ana María Chulia

Junio 2018

Licencias alternativas (elegir alguna de las siguientes y sustituir la de la página anterior)

A) Creative Commons:

Esta obra está sujeta a una licencia de Reconocimiento-NoComercial-SinObraDerivada 3.0 España de Creative Commons

Esta obra está sujeta a una licencia de Reconocimiento-NoComercial-CompartirIgual 3.0 España de Creative Commons

Esta obra está sujeta a una licencia de Reconocimiento-NoComercial 3.0 España de Creative Commons

Esta obra está sujeta a una licencia de Reconocimiento-SinObraDerivada 3.0 España de Creative Commons

Esta obra está sujeta a una licencia de Reconocimiento-CompartirIgual 3.0 España de Creative Commons

Esta obra está sujeta a una licencia de Reconocimiento 3.0 España de Creative Commons

B) GNU Free Documentation License (GNU FDL)

Copyright © AÑO TU-NOMBRE.

Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.3 or any later version published by the Free

C) Copyright

FICHA DEL TRABAJO FINAL

Título del trabajo:	Adecuación de una Administración Pública al Nuevo Reglamento Europeo 2016/679.
Nombre del autor:	Juan Francisco Claramunt Canet
Nombre del consultor:	Ana María Chulia Cebolla
Fecha de entrega (mm/aaaa):	06/2018
Área del Trabajo Final:	Aspectos legales de la Seguridad informática
Titulación:	Máster universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones

Resumen del Trabajo (máximo 250 palabras):

Este trabajo de final de máster explica la necesidad, dentro de la obligatoriedad, de cumplir y velar por la privacidad y la seguridad a la hora de realizar tratamientos de datos de carácter personal. Para ello, se va a llevar a cabo una adecuación de una administración pública (AP), más en concreto de un ayuntamiento, al nuevo Reglamento Europeo 2016/679 (RGPD). Lo que vamos a hacer para ello es: un estudio de la AP relativo al estado de cumplimiento actual respecto a la Ley Orgánica 15/1999 de Protección de Datos (LOPD) y el Esquema Nacional de Seguridad, seguidamente se llevará a cabo un análisis de riesgos (AARR) de los tratamientos de datos que se realicen en la misma y, a raíz de los resultados obtenidos del estudio y el AARR, se desarrollará un Sistema de Gestión de Protección de Datos (SGPD) para la administración.

Abstract (in English, 250 words or less):

This final master work explains the need, within the obligation, to comply and ensure privacy and security when processing personal data. For this, an adaptation of a Public Administration (AP), more specifically from a town hall, to the new European Regulation 2016/679 (RGPD) will be carried out. What we are going to do for it is: a study of the AP relative to the current state of compliance with the Ley Orgánica 15/1999 de Protección de Datos (LOPD) and the Esquema Nacional de Seguridad, then a Risk Analysis (AARR) of the personal data processing will be carried out and, following the results obtained from the study and the AARR, a System of Management of Data Protection (SGPD) for the administration will be developed.

Palabras clave (entre 4 y 8):
- Administración Pública - Reglamento Europeo 2016/679 - Ley Orgánica 15/1999 de Protección de Datos - Adecuación - Sistema de Gestión de Protección de Datos

Índice

Lista de figuras

No se encuentran elementos de tabla de ilustraciones.

1. Introducción

1.1. Contexto y justificación del Trabajo

El nuevo Reglamento Europeo 2016/679, 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 (RGPD o Reglamento), no resultar ser, únicamente, una actualización de la vigente normativa a nivel europeo en lo que respecta a la protección de datos de carácter personal, sino una revisión de las bases legales en la que se sustenta.

El objetivo de la creación del RGPD es garantizar un nivel coherente respecto a la protección de las personas físicas de la Unión Europea y evitar divergencias que dificulten la libre circulación de datos personales del mercado interior. Es decir, el RGPD ofrece a las personas físicas de todos los Estados de la Unión (o Estados miembros) el mismo nivel de derechos y obligaciones exigibles y de responsabilidades para los responsables y encargados del tratamiento.

Por otra parte, cabe destacar que hay casos en los que el Reglamento establece que sus normas deben ser especificadas o restringidas por los Estados miembros, con el objetivo de conseguir que las disposiciones nacionales sean coherentes y comprensibles para sus destinatarios.

Es por ello que, existiendo en España la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal (LOPD), resulta necesario que se cree una nueva ley para que, tal y como se ha comentado anteriormente, recoja aquellos aspectos que el RGPD deje regular a los Estados miembros. De ahí que el Gobierno español haya elaborado una nueva Ley Orgánica de Protección de Datos.

Tanto las Administraciones Públicas como las empresas privadas españolas deben cumplir con el nuevo RGPD como la nueva LOPD. Es por eso que ambos tipos de entidades tienen que realizar cambios a la hora de llevar a cabo un tratamiento de datos de carácter personal. En este Trabajo de Final de Máster nos vamos a centrar en adecuar una

Administración Pública, en concreto un Ayuntamiento, a lo que dicta el nuevo RGPD.

1.2. Objetivos del Trabajo

El objetivo de este Trabajo de Final de Máster consiste en realizar la adecuación de una administración pública al nuevo Reglamento Europeo 2016/679.

Con esto conseguiremos que la propia administración cumpla con dicha normativa, la cual le resulta de aplicación y, de la misma manera, aumentar la seguridad y privacidad a la hora de realizar dicho tratamiento.

1.3. Enfoque y método seguido

En una primera fase se realizará una recogida de información sobre el Ayuntamiento para inventariar los tratamientos de datos personales que realiza la Administración. Esta recogida de información se llevará a cabo realizando diversas entrevistas con parte del personal de la Administración y, además, partiendo de los ficheros inscritos en la Agencia Española de Protección de Datos (AEPD), lo cual nos dará una primera aproximación de los tratamientos de datos que realiza el Ayuntamiento para, de esta manera, poder crear el Registro de Actividades de Tratamiento.

Para la creación del Registro de Actividades de Tratamiento debemos tener en cuenta que, aunque se parta de los ficheros dados de alta en la AEPD, una actividad de tratamiento no corresponde a un fichero, ya que los tratamientos se dividen según la finalidad de los mismos.

Posteriormente, se realizará un estudio en el que se analizará si los tratamientos de datos que se llevan a cabo en el Ayuntamiento entrañan un alto riesgos para los derechos y libertades de los interesados. En el caso en que así sea, se llevará cabo una Evaluación de Impacto de Protección de Datos (EIPD). En caso contrario, se llevará a cabo un Análisis de Riesgos (AARR) en el que se detectarán las amenazas respectivas a los tratamientos de datos que se realizan en la Administración y, por consiguiente, se realizará un Plan de Tratamiento de Riesgos.

El Plan de Tratamiento de Riesgos incluirá las medidas de seguridad aplicables al Ayuntamiento, la cuales corresponderán con las medidas incluidas en el Esquema Nacional de Seguridad (ENS) ya que, al ser una Administración Pública, le aplica el mismo.

Una vez creado el Registro de Actividades de Tratamiento y el AARR o EIPD, según corresponda, se llevarán a cabo la implantación de un Sistema de Gestión de Protección de Datos (SGPD) con el que conseguiremos implementar los principios y directrices que incorpora el RGPD (principios del artículo 5, principio de transparencia, ejercicio de derechos, etc.).

1.4. Planificación del Trabajo

Tarea	Comienzo	Fin
Diagnóstico de situación	**09/03/2018**	**16/03/2018**
Diagnóstico respecto a LOPD	09/03/2018	16/03/2018
Diagnóstico medidas ENS	09/03/2018	16/03/2018
Gobierno del Sistema de Gestión de Protección de Datos	**12/04/2018**	**13/04/2018**
Desarrollo Política de protección de datos personales	12/04/2018	12/04/2018
Desarrollo y asignación de Roles y responsabilidades en protección de datos	13/04/2018	13/04/2018
Desarrollo del Registro de actividades de tratamiento	**14/04/2018**	**16/04/2018**
Análisis de necesidad de Evaluación de Impacto de Protección de Datos	**17/04/208**	**18/04/2018**
Análisis de riesgos	**19/04/2018**	**22/04/2018**
Elaboración del Análisis de riesgos de los tratamientos	19/04/2018	20/04/2018
Elaboración del Plan de tratamiento de los riesgos detectados	21/04/2018	22/04/2018
Desarrollo del Sistema de Gestión de Protección de Datos	**23/04/2018**	**02/05/2018**
Desarrollo de cláusulas: informativas, encargados de tratamiento, consentimiento, etc.	**03/05/2018**	**07/05/2018**

1.5. Breve sumario de productos obtenidos

Se puede afirmar que la adecuación al Reglamento Europeo ha sido todo un éxito ya que la compañía ya dispone de un Sistema de Gestión de Protección de Datos y además ha logrado disminuir los riesgos a los que estaba expuesta inicialmente.

Durante las fases se han obtenido diferentes documentos que, o bien ha conformado el Sistema de Gestión de Protección de Datos, o bien han sido resultado de alguna tarea realizada durante el proyecto.

1.6. Breve descripción de los otros capítulos de la memoria

1. Introducción al Reglamento Europeo de Protección de Datos:

   En este primer capítulo se realizará una introducción al Reglamento Europeo, nombrando las novedades más significativas que incluye y la necesidad de tener que implantar un Sistema de Gestión de Protección de Datos para adecuarse al mismo.

2. Diagnóstico de situación:

   En este capítulo se realizará un GAP Análisis, mediante entrevistas, dividido en dos vertientes: (1) respecto la antigua Ley Orgánica de Protección de Datos y su Reglamento de Desarrollo y (2) respecto al Esquema Nacional de Seguridad (ENS). Con GAP Análisis obtendremos una visión global del Ayuntamiento en materia de protección de datos y seguridad de la información.

3. Gobierno del Sistema de Gestión de Protección de Datos

   En este capítulo se establecerá la gobernanza de la compañía en materia de protección de datos. Para ello se desarrollará una Política de Protección de Datos y se definirán y asignarán los roles y responsabilidades en materia de protección de datos dentro del Ayuntamiento.

4. Registro de actividades de tratamiento

   En este tercer capítulo, a raíz de las entrevistas llevadas a cabo en el capítulo 2, se desarrollará el Registro de actividades de tratamiento, el cual resulta obligatorio para, entre otras entidades, todas las Administraciones Públicas.

5. Análisis de necesidad de Evaluación de Impacto de Protección de Datos

   En este quinto capítulo se llevará a cabo, mediante una guía proporcionada por la Agencia Española de Protección de Datos, un análisis para evaluar la necesidad de realizar un Evaluación de Impacto de Protección de Datos o no.

6. Análisis de Riesgos

   En este capítulo se realizará una evaluación de riesgos relativa a los tratamientos de datos identificados y el correspondiente Plan de tratamiento de riesgos. Esta evaluación tiene dos vertientes: (1) riesgos asociados a la protección de la información y (2) riesgos asociados al cumplimiento de los requisitos regulatorios relacionados con los derechos y libertades de los interesados.

7. Desarrollo del Sistema de Gestión de Protección de Datos

   En este penúltimo capítulo se desarrollará el resto del Sistemas de Gestión de Protección de Datos (SGPD). Se elaborarán los procedimientos y documentación necesaria para completar el SGPD.

8. Principio de transparencia y obligaciones de información

   En este último capítulo se elaborará toda la documentación necesaria para cumplir con el principio de transparencia y con la obligación de información: clausulas, formularios, etc.

2. Resto de capítulos

2.1. Introducción al Reglamento Europeo de Protección de Datos

El 25 de mayo de 2016 entró en vigor el Reglamento General de Protección de Datos (RGPD), que sustituyó a la normativa vigente en dicho momento, Directiva 95/46 y las correspondientes normas nacionales de desarrollo, y que comenzó a aplicarse el 25 de mayo de 2018. Ese periodo de dos años tuvo como objetivo permitir que los Estados de la Unión Europea, las Instituciones y también las empresas y organizaciones que tratan datos se preparasen y adaptasen para el momento en que el Reglamento fuera aplicable.

El RGPD es una norma directamente aplicable, que no requiere de normas internas de trasposición ni tampoco, en la mayoría de los casos, de normas de desarrollo o aplicación. Por ello, los responsables deben ante todo asumir que la norma de referencia es el RGPD y no las normas nacionales, como venía sucediendo hasta ahora con la Directiva 95/46. No obstante la ley que sustituirá a la actual Ley Orgánica de Protección de Datos (LOPD) sí podrá incluir algunas precisiones o desarrollos en materias en las que el RGPD lo permite.

El RGPD contiene muchos conceptos, principios y mecanismos similares a los establecidos por la Directiva 95/46 y por las normas nacionales que la aplican. Por ello, las organizaciones que en la actualidad cumplen adecuadamente con la LOPD española tienen una buena base de partida para evolucionar hacia una correcta aplicación del nuevo Reglamento.

Sin embargo, el RGPD modifica algunos aspectos del régimen actual y contiene nuevas obligaciones que deben ser analizadas y aplicadas por cada organización teniendo en cuenta sus propias circunstancias.

Tres elementos de carácter general constituyen la mayor innovación del RGPD para los responsables y se proyectan sobre todas las obligaciones de las organizaciones:

- **El principio de responsabilidad proactiva**: el RGPD describe este principio como la necesidad de que el responsable del tratamiento aplique medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el Reglamento.
- **El enfoque a la gestión de riesgos**: las medidas dirigidas a garantizar su cumplimiento deben tener en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como el riesgo para los derechos y libertades de las personas.
- **La designación del DPD**: ha de ser nombrado atendiendo a sus cualificaciones profesionales en las casuísticas descritas en el artículo 37 del RGPD.

El objetivo del presente trabajo es adecuar los tratamientos de datos de carácter personal del **Ayuntamiento de la Inventada** como responsable de tratamiento a los requerimientos establecidos en el nuevo Reglamento General de Protección de Datos (en adelante RGPD) y que comenzó a aplicarse desde el 25 de mayo, sustituyendo así a la Ley Orgánica de Protección de Datos aprobada en el año 1999 y su Reglamento de Desarrollo del año 2007.

Puesto que la adecuación y cumplimiento continuo del RGPD no es una tarea con principio y fin, sino que se ha de entender como un proceso, se considera necesario implementar un Sistema de Gestión de Protección de Datos (SGPD) que permita al cliente establecer un proceso de control, gestión y mejora continua sobre los tratamientos analizados.

2.2. Diagnóstico de situación

Uno de los factores más relevantes que conllevan a la consecución de los objetivos esperado del proyecto, es el conocimiento de la organización del que se dispone de forma previa a la ejecución del proyecto.

Para ello, se ha realizado un Análisis GAP del estado de situación actual del Ayuntamiento respecto a la antigua Ley Orgánica de Protección de Datos y respecto al Esquema Nacional de Seguridad (ENS), ya que como se ha comentado anteriormente serán las medidas técnicas incluidas en el mismo las que se deben implantar en el Ayuntamiento.

Los resultados de los Análisis GAP llevados a cabo se pueden observar en los documentos ***Análisis situación actual Ayuntamiento de la Inventada*** y ***Análisis GAP ENS*** anexo a la memoria del trabajo.

Como resumen de los resultados obtenidos en los mismos, se deduce que, a pesar de disponer de medidas implantadas tanto en materia de LOPD como de ENS, queda un margen de mejora en ambos aspectos. Como prueba de ello, podemos ver el nivel de madurez del Ayuntamiento respecto al ENS:

Codigo	Medida de Seguridad	Estado	Madurez
art.	Art. 29 - Instrucciones técnicas de seguridad y guías de seguridad	50,00%	L2
art.	Art. 35 - Informe del estado de la seguridad	0,00%	L0
art.	Art. 36 - Capacidad de respuesta a incidentes de seguridad de la información	50,00%	L2
art.	Art. 43/44 - Categorías y facultades	33,33%	L1-L2
org.1	Política de seguridad	0,00%	L0
org.2	Normativa de seguridad	50,00%	L2
org.3	Procedimientos de seguridad	0,00%	L0
org.4	Proceso de autorización	16,67%	L1-L2
op.pl.1	Análisis de riesgos	90,00%	L4
op.pl.2	Arquitectura de seguridad	7,14%	L1
op.pl.3	Adquisición de nuevos componentes	62,50%	L2-L3
op.pl.4	Dimensionamiento/Gestión de capacidades	0,00%	L0
op.pl.5	Componentes certificados	No Aplica	No Aplica
op.acc.1	Identificación	42,86%	L1-L2
op.acc.2	Requisitos de acceso	50,00%	L2
op.acc.3	Segregación de funciones y tareas	No Aplica	No Aplica
op.acc.4	Proceso de gestión de derechos de acceso	50,00%	L2
op.acc.5	Mecanismo de autenticación	15,00%	L1-L2
op.acc.6	Acceso local (local logon)	40,00%	L1-L2
op.acc.7	Acceso remoto (remote login)	66,67%	L2-L3
op.exp.1	Inventario de activos	87,50%	L3-L4
op.exp.2	Configuración de seguridad	80,00%	L3
op.exp.3	Gestión de la configuración	50,00%	L2
op.exp.4	Mantenimiento	37,50%	L1-L2
op.exp.5	Gestión de cambios	50,00%	L2
op.exp.6	Protección frente a código dañino	75,00%	L2-L3
op.exp.7	Gestión de incidentes	55,56%	L2-L3
op.exp.8	Registro de la actividad de los usuarios	75,00%	L2-L3
op.exp.9	Registro de la gestión de incidentes	50,00%	L2
op.exp.10	Protección de los registros de actividad	No Aplica	No Aplica
op.exp.11	Protección de claves criptográficas	100,00%	L5

op.ext.1	Contratación y acuerdos de nivel de servicio	50,00%	L2
op.ext.2	Gestión diaria	0,00%	L0
op.ext.9	Medios alternativos	No Aplica	No Aplica
op.cont.1	Análisis de impacto	83,33%	L3-L4
op.cont.2	Plan de continuidad	No Aplica	No Aplica
op.cont.3	Pruebas periódicas	No Aplica	No Aplica
op.mon.1	Detección de intrusión	100,00%	L5
op.mon.2	Sistema de métricas	0,00%	L0
mp.if.1	Áreas separadas y con control de acceso	25,00%	L1-L2
mp.if.2	Identificación de las personas	0,00%	L0
mp.if.3	Acondicionamiento de los locales	16,67%	L1-L2
mp.if.4	Energía eléctrica	37,50%	L1-L2
mp.if.5	Protección frente a incendios	100,00%	L5
mp.if.6	Protección frente a inundaciones	100,00%	L5
mp.if.7	Registro de entrada y salida de equipamiento	0,00%	L0
mp.if.9	Instalaciones alternativas	No Aplica	No Aplica
mp.per.1	Caracterización del puesto de trabajo	12,50%	L1-L2
mp.per.2	Deberes y obligaciones	64,29%	L2-L3
mp.per.3	Concienciación	25,00%	L1-L2
mp.per.4	Formación	0,00%	L0
mp.per.9	Personal alternativo	No Aplica	No Aplica
mp.eq.1	Puesto de trabajo despejado	25,00%	L1-L2
mp.eq.2	Bloqueo de puesto de trabajo	50,00%	L2
mp.eq.3	Protección de equipos portátiles	83,33%	L3-L4
mp.eq.9	Medios alternativos	0,00%	L0
mp.com.1	Perímetro seguro	50,00%	L2
mp.com.2	Protección de la confidencialidad	100,00%	L5
mp.com.3	Protección de la autenticidad y de la integridad	91,67%	L4-L5
mp.com.4	Segregación de redes	No Aplica	No Aplica
mp.com.9	Medios alternativos	No Aplica	No Aplica
mp.si.1	Etiquetado	0,00%	L0
mp.si.2	Criptografía	No Aplica	No Aplica
mp.si.3	Custodia	0,00%	L0
mp.si.4	Transporte	37,50%	L1-L2
mp.si.5	Borrado y destrucción	37,50%	L1-L2
mp.sw.1	Desarrollo de aplicaciones	100,00%	L5
mp.sw.2	Aceptación y puesta en servicio	71,43%	L2-L3
mp.info.1	Datos de carácter personal	50,00%	L2
mp.info.2	Calificación de la información	0,00%	L0
mp.info.3	Cifrado	No Aplica	No Aplica
mp.info.4	Firma electrónica	100,00%	L5
mp.info.5	Sellos de tiempo	No Aplica	No Aplica
mp.info.6	Limpieza de documentos	0,00%	L0

mp.info.9	Copias de seguridad (backup)	66,67%	L2-L3
mp.s.1	Protección del correo electrónico	62,50%	L2-L3
mp.s.2	Protección de servicios y aplicaciones web	100,00%	L5
mp.s.8	Protección frente a la denegación de servicio	100,00%	L5
mp.s.9	Medios alternativos»	No Aplica	No Aplica

Tabla 1 Nivel madurez ENS

2.3. Gobierno del Sistema de Gestión de Protección de Datos

El Sistema de Gestión de Protección de Datos se ha de sustentar sobre unos objetivos definidos a nivel de gobierno, es decir, a nivel de dirección para que pueda ser aceptada y aplicada en la organización. Por ello, se ha desarrollado una Política de Protección de Datos Personales (***SGPD_02 - Política de protección de datos personales***) que dictará los principios y cánones de actuación que regirán en el Ayuntamiento y. Adicionalmente, se ha llevado a cabo la definición de roles y responsabilidades (***SGPD_03 - Roles y Responsabilidades***) que permite a la organización tener definidas las tareas que ha de realizar cada uno de los implicados en el tratamiento de los datos personales, sin dejar lugar a ambigüedades y estableciendo con ello una parte de las medidas organizativas, requeridas por el RGPD, que se creen oportunas.

La política resulta de aplicación a todos los empleados, proveedores, clientes y en definitiva a todas las personas que mantengan cualquier tipo de relación directa en la que se lleven a cabo tratamientos de datos de carácter personal.

Los roles y responsabilidades que se han definido, y que parten de los definidos para la adecuación al ENS ya que es obligatorio para el Ayuntamiento, son los siguientes:

- Responsable de la Información
- Responsable de los Servicios
- Responsable de Seguridad
- Técnico de seguridad de los sistemas
- Usuarios

2.4. Registro de actividades de tratamiento

El Reglamento General de Protección de Datos incluye la obligación para algunas organizaciones de crear y mantener un registro de actividades de los tratamientos de datos personales que llevan a cabo, el cual debe estar compuesto por los siguientes elementos:

- Nombre y datos de contacto del responsable de tratamiento y del Delegado de Protección de Datos si existiese.
- Tratamiento.
- Finalidad del tratamiento
- Base de legitimación.
- Categoría de interesados.
- Categoría de datos personales.
- Periodo de conservación.
- Cesión de datos e identificación de los encargados de tratamiento.
- Transferencia internacional de datos (si aplica) y medidas asociadas a las mismas.
- Medidas de técnicas y organizativas asociadas al tratamiento.

Este registro sustituye a la inscripción de ficheros a la AEPD, siendo ahora opcional por parte de las entidades, y resulta obligatorio para organizaciones:

- Con más de 250 empleados
- Que realicen tratamientos que puedan entrañar un riesgo para los derechos y libertades de los interesados, no sea ocasional o incluya categorías especiales de datos personales o datos personales relativos a condenas e infracciones penales.

Por consiguiente, el Ayuntamiento ha creado su propio registro de actividades de tratamiento, el cual se recoge anexo a la memoria del trabajo en ***SGPD_06 - Registro de Actividades y Tratamientos***.

La base de la que se ha partido para la creación de este registro de actividades de tratamiento han sido los ficheros inscritos por el Ayuntamiento en la AEPD, apoyándose además con Análisis de situación actual con el objetivo de seccionar los ficheros en actividades de tratamiento y, además, detectar posibles tratamientos adicionales no registrados.

2.5. Análisis de necesidad de Evaluación de Impacto de Protección de Datos

El RGPD incluye entre los requerimientos y obligaciones para las organizaciones la necesidad de evaluar el impacto de las actividades de tratamiento en la protección de los datos personales, siempre y cuando sea probable que el tratamiento suponga un riesgo significativo para los derechos y libertades de las personas.

Es por ello que en el Ayuntamiento se debe llevar a cabo un análisis para determinar la necesidad de la realización de una Evaluación de Impacto de Protección de Datos (EIPD) para valorar si los tratamientos iniciados con anterioridad a la fecha de aplicación del RGPD presentan alto riesgo para los derechos o libertades de los interesados a fin de estar en condiciones de poder adoptar las medidas adecuadas para adecuar dichos tratamientos a las exigencias del RGPD.

Adicionalmente, para las nuevas actividades de tratamiento que pueda realizar el Ayuntamiento en un futuro o para llevar a cabo alguna modificación importante en las actividades de tratamiento actuales, se realizará de nuevo este análisis de necesidad de EIPD, con el fin de detectar los riesgos que conlleven dichos tratamientos o modificaciones.

Si el resultado de dicho análisis, reflejado en el propio informe, determina que las actividades de tratamiento que se llevan a cabo en el Ayuntamiento no entrañan un riesgo elevado para los derechos y libertades de los interesados, se tendrá que llevar a cabo un Análisis de Riesgos con el que se gestionarán los riesgos que posea la compañía en materia de tratamiento de datos personales.

Por el contrario, si el resultado del análisis determina que las actividades de tratamiento entrañan un riesgo elevado para los derechos y libertades de los interesados, se llevará a cabo la correspondiente Evaluación de Impacto con la que se detectarán los riesgos propios a los tratamientos y las acciones que se llevarán a cabo para tratarlos.

Se ha realizado como muestra el Análisis de necesidad de EIPD del tratamiento de “Gestión de biblioteca”, el cual se puede ver en ***Análisis de necesidad de EIPD***, anexo a esta memoria. El resultado del análisis dicta que “*Vistas las respuestas proporcionadas en el presente*

formulario definido para analizar la necesidad de realización de una Evaluación de Impacto de Protección de Datos, se determina que ***NO*** *es necesario llevar a cabo la misma, ya que se deduce que el tratamiento no supone un alto riesgo para el interesado*".

Será tarea del Ayuntamiento llevar a cabo la misma tarea para todas las actividades de tratamiento que realice, de forma que se lleve a cabo una Evaluación de Impacto de Protección de Datos en aquellas que se requiera.

2.6. Análisis de riesgos

El Reglamento General de Protección de Datos establece la necesidad de que el responsable o el encargado de tratamiento evalué los riesgos inherentes al tratamiento de datos de carácter personal y aplique medidas para mitigarlos.

Las medidas deben garantizar un nivel de seguridad adecuado, incluida la confidencialidad, teniendo en cuenta el estado de la técnica y el coste de su aplicación con respecto a los riesgos y la naturaleza de los datos personales que deben protegerse.

Al evaluar el riesgo en relación con la seguridad de los datos, se deben tener en cuenta los riesgos que se derivan del tratamiento de los datos personales, como la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos, susceptibles en particular de ocasionar daños y perjuicios físicos, materiales o inmateriales.

Es importante resaltar que el enfoque de riesgos en protección de datos tiene al menos dos vertientes:

- Análisis de riesgos para obtener las medidas de seguridad técnicas y organizativas para proteger los datos personales.
- Análisis de riesgos para los derechos y libertades de las personas.

Las medidas de seguridad a implantar en el Ayuntamiento, se basan en el marco del Esquema Nacional de Seguridad, el cual resulta de aplicación para todas las administraciones públicas del ámbito nacional español tal y como hemos mencionado anteriormente.

Para la realización de este trabajo se ha realizado, como muestra, el análisis de riesgos del tratamiento de "Videovigilancia" que se lleva a cabo en el Ayuntamiento. Para ello se ha utilizado la herramienta PILAR, ya que es la herramienta que el Centro Criptológico Nacional (CCN-CERT) pone a disposición de forma de gratuita a las Administraciones Públicas para que estas lleven a cabo sus análisis de riesgos, la cual está creada partiendo de la metodología análisis y gestión de riesgos MAGERIT.

Los riesgos obtenidos durante esta fase se recogen en ***Informe Análisis Riesgos*** y, en el mismo, se recoge la lista de acciones a realizar por el Ayuntamiento para tratar los riesgos detectados, es decir, el plan de tratamiento de riesgos.

Tal y como se ha comentado anteriormente, los riesgos obtenidos se basan en el tratamiento de "Videovigilancia", por lo que se han analizado los siguientes activos:

CLASE	ACTIVO
[B] Activos esenciales	[T] Videovigilancia
[SW] Aplicaciones	[SV] Software Veoveo
[HW] Equipos	[PC] Equipo usuarios [C] Cámaras
[HWR] Hardware de red	[ROU] Router internet
[COM] Comunicaciones	[ADSL] Internet
[AUX] Elementos auxiliares	[POWER] Fuente de alimentación
[SS] Servicios subcontratados	[ISP] Proveedor internet [PVV] Proveedor Veoveo SL
[P] Personal	[POL] Policía

Para clarificar el motivo del estudio de dichos activos: el sistema de vigilancia está instalado y mantenido por la empresa Veoveo SL, la cual además almacena las imágenes captadas por las cámaras. Por otra parte, para que se puedan ver las imágenes captadas por las cámaras en directo, la empresa proporciona el software Veoveo, el cual se encuentra instalado exclusivamente en un equipo del departamento de la

policía, que es el único personal con acceso a las imágenes. El software tiene configurada una conexión VPN directa con el proveedor para poder emitir las imágenes en directo, para ello se ha contratado a propósito una línea de ADSL para mantener el sistema fuera de la red interna del Ayuntamiento.

Partiendo de este escenario y de los hallazgos detectados del diagnóstico de situación, se han obtenido los siguientes riesgos:

Activo	Amenaza	Riesgo
[T] Videovigilancia	[PR.2i] Problemas relativos los derechos del sujeto: acceso, rectificación, cancelación y oposición	{5,4}
[T] Videovigilancia	[PR.2g] Problemas relativos a la duración del plazo de conservación de los datos recogidos	{5,4}
[T] Videovigilancia	[PR.2c] Problemas relativos a la transparencia del tratamiento	{5,4}
[PVV] Proveedor VeoVeo SL	[A.19] Revelación de información	{2,5}
[PVV] Proveedor VeoVeo SL	[A.15] Modificación de la información	{2,5}
[PVV] Proveedor VeoVeo SL	[A.18] Destrucción de la información	{2,5}
[ADSL] Internet	[E.24] Caída del sistema por agotamiento de recursos	{2,2}
[PVV] Proveedor VeoVeo SL	[I.9] Interrupción de otros servicios o suministros esenciales	{1,9}
[ISP] Proveedor internet	[I.8] Fallo de servicios de comunicaciones	{1,9}
[ROU] Router internet	[I.5] Avería de origen físico o lógico	{1,7}
[C] Cámaras	[I.5] Avería de origen físico o lógico	{1,7}
[PVV] Proveedor VeoVeo SL	[E.19] Fugas de información	{1,3}
[PVV] Proveedor VeoVeo SL	[E.15] Alteración de la información	{1,2}
[PVV] Proveedor VeoVeo SL	[E.18] Destrucción de la información	{1,2}
[POL] Policia	[A.6] Abuso de privilegios de acceso	{0,97}
[PC] Equipo usuario	[I.5] Avería de origen físico o lógico	{0,53}
[SV] Software Veoveo	[E.20] Vulnerabilidades de los programas (software)	{0}
[SV] Software Veoveo	[E.20] Vulnerabilidades de los programas (software)	{0}
[SV] Software Veoveo	[E.21] Errores de mantenimiento / actualización de programas (software)	{0}
[SV] Software Veoveo	[E.21] Errores de mantenimiento / actualización de programas (software)	{0}
[SV] Software Veoveo	[E.20] Vulnerabilidades de los programas (software)	{0}

El criterio que se ha establecido para decidir qué riesgos tratar, es mitigar aquellos que tengan un valor superior a **1** y las acciones que se han definido son las siguientes:

1. Establecer contractualmente las características del servicio prestado y las responsabilidades de las partes. Se detallará lo que se considera calidad mínima del servicio prestado y las consecuencias de su incumplimiento, añadiéndose al contrato la cláusula de encargado de tratamiento.
2. Establecer un sistema rutinario de supervisión de la calidad del servicio, la ejecución de los mantenimientos de los sistemas afectados y la coordinación en caso de incidencias y desastres.
3. Establecer un plazo de conservación de las imágenes de 30 días y comunicar al encargado de tratamiento e incluir en el contrato dicha decisión.
4. Colocar carteles que informen de la existencia de cámaras de manera que el interesado sea consciente de la existencia de la misma y sea capaz de ejercitar sus derechos.

De esta manera, se mitigarán todos los riesgos asociados al tratamiento de “Videovigilancia”. Será tarea del Ayuntamiento llevar a cabo la misma tarea para todas las actividades de tratamiento que realice, de forma que se puedan establecer todas las medidas técnicas y organizativas necesarias para la protección de datos.

2.7. Desarrollo del Sistema de Gestión de Protección de Datos

El Reglamento Europeo requiere el desarrollo de una serie de documentación (procedimientos, cláusulas...) que muestre que se cumple con las normas recogidas en él, según el principio de <<responsabilidad proactiva>>. Dicha documentación es la que compone el Sistema de Gestión de Protección de Datos del Ayuntamiento, e incluye lo siguiente:

- Procedimiento de ejercicio de los derechos ARCO y los nuevos derechos de Portabilidad, derecho al olvido y derecho a la limitación:
    - ***SGPD_04 – Procedimiento ejercicio de derechos***

- Procedimiento de notificación de violaciones de seguridad de los datos personales a la Agencia Española de Protección de Datos y, si corresponde, al interesado:
    - ***SGPD_05 - Procedimiento notificación violación de seguridad***
    - ***SGPD_05_Anexo - Modelo Notificación al Interesado***
- Manual del Sistema de Gestión de Protección de Datos:
    - ***SGPD_01 - Manual Sistema Gestión Protección Datos***

Esta documentación, la cual se ha creado para el Ayuntamiento y se encuentra anexa a esta memoria, completa del Sistema de Gestión de Protección de Datos, que contribuye a que el Ayuntamiento cumpla con el Reglamento Europeo.

2.8. Principio de transparencia y obligaciones de información (cláusulas y formularios)

Otros requerimientos que incluye el Reglamento Europeo y que también llevan implícito la creación documentación adicional para cumplir con el mismo, es el <<*principio de transparencia*>> y la obligación de informar al interesado incluida en los Artículos 12, 13 y 14.

Para cumplir con dichas exigencias, es necesario modificar las cláusulas informativas incluidas en los formularios, contratos, etc. que hacen referencia a la antigua LOPD, de forma que estas se adapten a lo requerido en el RGPD.

Es por ello, que en este proyecto se han creado diferentes cláusulas y formularios tipo para que el Ayuntamiento las incluya en toda la documentación que requiera y que sea utilizada por el Ayuntamiento para el desarrollo de sus funciones (página web, contratos, formularios, etc.). Estas cláusulas y formularios se encuentran anexos a esta memoria y son los siguientes:

- ***Cláusula contratos acceso por terceros***
- ***Cláusula informativa genérica***
- ***Cláusula informativa genérica_adicional***

- ***Cláusula informativa formulario web***
- ***Formulario obtención consentimiento***
- ***Formulario obtención consentimiento menor***

Con todo esto finalizado, se completaría el proyecto de adecuación al Reglamento Europeo del Ayuntamiento de la Inventada.

2.9. Revisión y mejora continua

Resaltar que el Ayuntamiento debe tener en cuenta la necesidad de revisión y mejora continua que requiere el Sistema de Gestión de Protección de Datos implantado. Para ello, debe tener en cuenta que la revisión periódica del SGPD se lleva a cabo mediante tres tareas diferentes:

- La revisión del sistema de gestión.
- Auditorías respecto al cumplimiento del RGPD.
- Estudio de las violaciones de seguridad que puedan llegar a suceder.

La revisión del sistema de gestión se lleva a cabo mediante la revisión del marco documental que compone el mismo y la realización periódica del análisis de riesgos indicado en el apartado 2.5.

De esta manera, unificando los resultados obtenidos de la revisión periódica del SGPD, se obtienen para cada ciclo de revisión una seria de acciones correctivas y mejoras que se implantan y adopta el Ayuntamiento.

3. Conclusiones

Una vez finalizado el proyecto es momento de analizar las lecciones aprendidas durante el transcurso de la adecuación de una Administración Pública al Reglamento Europeo de Protección de Datos.

En primer lugar, considero que el proyecto es una práctica realista, puesto que la adecuación al Reglamento Europeo es una de las tareas más demandadas actualmente en el sector TI debido a su entrada en vigor el 25 de mayo, así como lo eran anteriormente las auditorías de la Ley Orgánica 15/1999 de Protección de Datos y de su reglamento de desarrollo.

Por otro lado, el hecho de haber desarrollado un análisis de riesgos con la herramienta PILAR me ha servido por partida doble. Primero por conocer la metodología MAGERIT, en su versión 3, y las etapas de un análisis de riesgos; segundo por haber conocido la herramienta PILAR y poder saber utilizarla.

Además, el hecho de valorar qué propuestas puede llevar a cabo una entidad para mitigar o reducir los riesgos a los que se encuentra expuesta, te hace reflexionar sobre diferentes medidas que el día de mañana como consultor puedo proponer a una entidad con una casuística similar.

Respecto a las fases del proyecto, el tiempo establecido para desarrollar cada una era acorde al contenido que se demandaba. Por ello, no he tenido ningún problema para ir completando cada etapa del trabajo.

Por último, considero que se trata de un Trabajo Final de Máster muy apropiado para la especialidad de Gestión y auditoría de la seguridad informática, ya que la protección de datos es una parte dentro de la misma.

4. Glosario

En este glosario se han incluido, además de los términos más utilizados en el proyecto, los términos más relevantes relacionados con el tratamiento y seguridad de los datos personales:

- **LOPD**: Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal.
- **RGPD**: Reglamento Europeo 2016/679, 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.
- **ENS**: Esquema Nacional de Seguridad
- **SGPD**: Sistema de Gestión de Protección de Datos
- **Administración Pública**: Conjunto de organismos y personas que se dedican a la administración o el gobierno de los asuntos de un estado. Actividad de este conjunto de organismos y personas.
- **Adecuar**: Acomodar o hacer adecuada una cosa a otra.
- **Datos personales**: toda información sobre una persona física identificada o identificable («**el interesado**»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.
- **Tratamiento**: cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción.
- **Limitación del tratamiento**: el marcado de los datos de carácter personal conservados con el fin de limitar su tratamiento en el futuro.
- **Elaboración de perfiles**: toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses,

fiabilidad, comportamiento, ubicación o movimientos de dicha persona física.

- **Seudonimización**: el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable.

- **Responsable del tratamiento o Responsable**: la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros.

- **Encargado del tratamiento o Encargado**: la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento.

- **Tercero**: persona física o jurídica, autoridad pública, servicio u organismo distinto del interesado, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas para tratar los datos personales bajo la autoridad directa del responsable o del encargado.

- **Destinatario**: la persona física o jurídica, autoridad pública, servicio u otro organismo al que se comuniquen datos personales, se trate o no de un tercero. No obstante, no se considerarán destinatarios las autoridades públicas que puedan recibir datos personales en el marco de una investigación concreta de conformidad con el Derecho de la Unión o de los Estados miembros; el tratamiento de tales datos por dichas autoridades públicas será conforme con las normas en materia de protección de datos aplicables a los fines del tratamiento.

- **Consentimiento del interesado**: toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen.

- **Datos genéticos**: datos personales relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona.

- **Datos biométricos**: datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas,

fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos.

- **Datos relativos a la salud**: datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud.
- **Sistema de información**: conjunto de ficheros, tratamientos, programas, soportes y en su caso, equipos empleados para el tratamiento de datos de carácter personal.
- **Riesgo**: posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias
- **Evaluación de riesgos**: proceso global de identificación, análisis y estimación de riesgos.

5. Bibliografía

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (2016). Reglamento (UE) 2016/679. <http://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/union_europea/reglamentos/common/pdfs/Reglamento_UE_2016-679_Proteccion_datos_DOUE.pdf> [Consulta: enero de 2018]

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (2018). Adaptación al RGPD - Administraciones Públicas (infografía). <http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/infografias/Adaptacion_RGPD_AAPP.pdf> [Consulta: febrero de 2018]

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (2017). El nuevo RGPD y su impacto sobre la actividad de las Administraciones Locales. <http://www.agpd.es/portalwebAGPD/temas/reglamento/common/pdf/Impacto_RGPD_en_AALL.pdf> [Consulta: enero de 2018]

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (2017). El impacto del Reglamento General de Protección de Datos sobre la actividad de las Administraciones Públicas. <http://www.agpd.es/portalwebAGPD/temas/reglamento/common/pdf/Impacto_RGPD_en_AAPP.pdf> [Consulta: febrero de 2018]

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (2017). El delegado de protección de datos en las Administraciones Públicas. <http://www.agpd.es/portalwebAGPD/temas/reglamento/common/pdf/Funciones_DPD_en_AAPP.pdf> [Consulta: enero de 2018]

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (2018). Curso Proceso para la adaptación al RGPD en las Administraciones Pública. <http://www.inap.es/mediateca?p_p_id=contentviewerservice_WAR_alfresco_packportlet&p_p_lifecycle=0&p_p_state=maximized&p_p_mode=view&p_p_col_id=columna-1&p_p_col_pos=1&p_p_col_count=2&_contentviewerservice_WAR_alfresco_packportlet_nodeName=Curso_proteccion_datos_2946347.gcl&_co

ntentviewerservice_WAR_alfresco_packportlet_struts_action=/contentviewer/view&contentType=notice> [Consulta: marzo de 2018]

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (2018). El RGPD y sus implicaciones para la Administración Local (vídeo). AEPD - FEMP. <http://www.agpd.es/portalwebAGPD/temas/reglamento/RGPD_Administracion_Local-ides-idphp.php> [Consulta: marzo de 2018]

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (2018). Novedades en materia de protección de datos (vídeo) – AEPD - INAP. <http://www.inap.es/mediateca?p_p_id=contentviewerservice_WAR_alfresco_packportlet&p_p_lifecycle=0&p_p_state=maximized&p_p_mode=view&p_p_col_id=columna-1&p_p_col_pos=1&p_p_col_count=2&_contentviewerservice_WAR_alfresco_packportlet_struts_action=/contentviewer/view&_contentviewerservice_WAR_alfresco_packportlet_nodeName=JORNADA_NOVEDADES_PROTECCION_DATOS_2753529.gcl&contentType=notice> [Consulta: marzo de 2018]

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (2016). Guía del Reglamento General de Protección de Datos para responsables de tratamiento. <http://www.agpd.es/portalwebAGPD/temas/reglamento/common/pdf/guia_rgpd.pdf#Gu%C3%ADa%20del%20Reglamento%20General%20de%20Protecci%C3%B3n%20de%20Datos%20para%20responsables%20de%20tratamiento> [Consulta: enero de 2018]

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (2016). Guía para el cumplimiento del deber de informar. <http://www.agpd.es/portalwebAGPD/temas/reglamento/common/pdf/modeloclausulainformativa.pdf> [Consulta: enero de 2018]

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (2016). Directrices para la elaboración de contratos entre responsables y encargados del tratamiento. <http://www.agpd.es/portalwebAGPD/temas/reglamento/common/pdf/directricescontratos.pdf> [Consulta: enero de 2018]

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (2018). Guía práctica de Análisis de riesgos. <http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones

/common/Guias/2018/AnalisisDeRiesgosRGPD.pdf> [Consulta: marzo de 2018]

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (2018). Guía práctica de Evaluaciones de impacto. <http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/2018/Guia_EvaluacionesImpacto.pdf> [Consulta: marzo de 2018]

AUTORITAT CATALANA DE PROTECCIÓ DE DADES (2018). Guia sobre l'avaluació d'impacte relativa a la protecció de dades al RGPD (2.0). <http://apdcat.gencat.cat/web/.content/03-documentacio/Reglament_general_de_proteccio_de_dades/documents/GUIA-AIPD-APDCAT.pdf>[Consulta: febrero de 2018]

AUTORITAT CATALANA DE PROTECCIÓ DE DADES (2016). Principals novetats del RGPD. <http://apdcat.gencat.cat/ca/documentacio/RGPD/novetats/> [Consulta: febrero de 2018]

CONGRESO DE LOS DIPUTADOS (2017). Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal. <http://www.congreso.es/backoffice_doc/prensa/notas_prensa/57631_1518684517278.PDF> [Consulta: enero de 2018]

GRUPO DE TRABAJO DEL ARTÍCULO 29 (GT29) (2017). Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento "entraña probablemente un alto riesgo" a efectos del Reglamento (UE) 2016/679. <http://www.agpd.es/portalwebAGPD/canaldocumentacion/docu_grupo_trabajo/wp29/common/Traduc_oficial_ult_version/wp248_rev.01_es.pdf> [Consulta: marzo de 2018]

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (2018). Protección de datos y administración local. <http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/2018/Guia_Proteccion_datos_Administracion_Local.pdf> [Consulta: abril de 2018]

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (2018). Listado de cumplimiento normativo. <http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/2018/LISTADO_DE_CUMPLIMIENTO_DEL_RGPD.pdf>
[Consulta: abril de 2018]

BOLETÍN OFICIAL DEL ESTADO (2018). 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>
[Consulta: abril de 2018]

BOLETÍN OFICIAL DEL ESTADO (2018). Ley 39/1988, de 28 de diciembre, reguladora de las Haciendas Locales. <https://www.boe.es/buscar/doc.php?id=BOE-A-1988-29623>
[Consulta: abril de 2018]

BOLETÍN OFICIAL DEL ESTADO (2018). Real Decreto Legislativo 2/2004, de 5 de marzo, por el que se aprueba el texto refundido de la Ley Reguladora de las Haciendas Locales. <https://www.boe.es/buscar/act.php?id=BOE-A-2004-4214>
[Consulta: abril de 2018]

BOLETÍN OFICIAL DEL ESTADO (2018). Ley 50/1999, de 23 de diciembre, sobre el Régimen Jurídico de la Tenencia de Animales Potencialmente Peligrosos. <https://www.boe.es/buscar/act.php?id=BOE-A-1999-24419>
[Consulta: abril de 2018]

6. Anexos

- Análisis situación actual Ayuntamiento de la Inventada
- Análisis GAP ENS
- Informe Análisis Riesgos
- Análisis de necesidad de EIPD
- SGPD_01 - Manual Sistema Gestión Protección Datos
- SGPD_02 - Política de protección de datos personales
- SGPD_03 – Roles y Responsabilidades
- SGP04 - Registro de Actividades y Tratamientos
- SGPD_05 - Procedimiento notificación violación de seguridad
- SGPD_05_Anexo - Modelo Notificación al Interesado
- SGPD_06 - Registro de Actividades y Tratamientos
- Cláusula contratos acceso por terceros
- Cláusula informativa genérica
- Cláusula informativa genérica_adicional
- Cláusula informativa formulario web
- Formulario obtención consentimiento
- Formulario obtención consentimiento menor