Trabajo Fin de Máster
"Memoria Final"

Adaptación de una pyme a la futura normativa GDPR

Programa docente:	MISTIC. Máster Interuniversitario en Seguridad de las Tecnologías de la información y de las Comunicaciones
Título del TFM:	Adaptación de una PYME a la futura GDPR
Empresa en la que se realiza el proyecto:	INCIBE. Instituto Nacional de Ciberseguridad
Tutor:	Marco Antonio Lozano Merino
Estudiante:	Miguel Ángel Quirós García
Fecha:	1 de enero de 2018

Universidades participantes:

DEDICATORIA Y AGRADECIMIENTOS

Me gustaría empezar dedicando este trabajo a la persona que hizo de mí el hombre que soy hoy, a ti papá allá donde estés.

Por otro lado, se lo quiero dedicar también a mi familia por apoyarme en todo momento y ser tan comprensiva ante los esfuerzos que ha requerido poder sacar horas de estudio para abordar este máster.

Y como no, a mi compañera de viaje por su comprensión y apoyo incondicional, animándome y regalándome siempre una sonrisa cuando más lo necesitaba.

RESUMEN DEL TRABAJO REALIZADO

En mayo de 2016, la unión europea dio un paso importante respecto a la protección de datos, presentando el GDPR (General Data Protection Regulation). Esta nueva normativa viene a sustituir y/o complementar a las leyes nacionales de cada estado miembro referidas a la protección de datos en todos y cada uno de los países de la Unión. Con ella la enorme fragmentación normativa existente se elimina y nuestros datos tienen el mismo tratamiento en los todavía 28 estados que la forman.

Se estableció un período de adaptación de dos años para que todas las empresas pudieran adaptarse al nuevo marco legal y adecuarse a la nueva normativa, pero hasta entonces la actual Ley Orgánica de Protección de Datos (LOPD) sigue vigente en España, siendo por tanto obligatorio su cumplimiento.

Inmersos en un período de transición como en el que nos encontramos, he querido ponerme en la piel de una PYME y afrontar una adecuación en materia de protección de datos, con la finalidad de conocer de primera mano los inconvenientes y dificultades que ello conllevaría a fecha de hoy. Para ello tomé como base una hipotética empresa a la que llamé LK TECHNOLOGY S.A., la cual es una empresa cuya plantilla actual no excede de los veinte trabajadores y está dedicada a la venta de productos tecnológicos.

En primer lugar, procedí a adecuar la empresa a la actual LOPD, realizando una adaptación completa de la misma, lo cual dio como resultado el entregable correspondiente a la PEC3 (Anexo 1). Posteriormente y con el foco puesto en el marco europeo realicé la adaptación en base al GDPR, lo cual como resultado generó el entregable correspondiente a las PEC4 (Anexo 2).

En resumen, a lo largo del TFM he realizado la adaptación de una PYME desde la actual normativa en nuestro país, la conocida LOPD, así como también desde el nuevo marco europeo establecido por el GDPR. En estos meses de trabajo he tenido la oportunidad de conocer las diferentes particularidades de cada una, así como las problemáticas que plantean su puesta en marcha. A lo largo del presente documento, se aborda en detalle la experiencia descrita, terminando con una exposición de conclusiones a las que finalmente he podido llegar tras el trabajo realizado.

SUMMARY OF THE WORK

In May 2016, the European Union took an important step forward regarding data protection, launching the GDPR (General Data Protection Regulation). This new regulation replaces and / or complements the national laws of each member state related to data protection in each and every one of the countries of the Union. With it, the huge existing normative fragmentation is eliminated and our data have the same treatment in the still 28 states that form it.

A period of adaptation of two years was established so that all companies could adapt to the new legal framework and adjust to the new regulations, but until then, the current Organic Law on Data Protection (LOPD) is still valid in Spain, and is therefore mandatory its compliance.

Immersed in a period of transition like in which we are, I wanted to put myself in the shoes of an SME and face an adaptation in terms of data protection, in order to know first-hand the inconveniences and difficulties that it would entail actually. For this, I took a hypothetical company as a starting point, that I called LK TECHNOLOGY S.A., which is a company whose current staff does not exceed twenty workers and is dedicated to the sale of technological products.

First, I proceeded to adapt the company to the current LOPD, making a full adaptation of it, which resulted in the deliverable corresponding to the PEC3 (Appendix 1). Subsequently, with the focus on the European framework, I made the adaptation based on the GDPR, which, as a result, generated the deliverable corresponding to the PEC4 (Appendix 2).

In summary, throughout the TFM I have made the adaptation of an SME from the current regulations in our country, the well-known LOPD, as well as from the new European framework established by the GDPR. In these months of work, I have had the opportunity to know the different characteristics of each one, as well as the problems posed by its implementation. Throughout this document, the described experience is dealt with in detail, ending with an exposition of conclusions to which I have finally been able to reach after the completed project.

ÍNDICE

1.- INTRODUCCIÓN

1.1.- JUSTIFICACIÓN DEL TRABAJO FIN DE MÁSTER

1.1.1.- Introducción a los marcos normativos existentes

Actualmente nos encontramos en un proceso transitorio donde están conviviendo dos marcos normativos: el español y el europeo. A continuación, se describe cada uno de ellos:

LOPD

En el caso de España, fue en el año 1999 cuando entró en vigor la LOPD, que ha regido como la norma básica de la protección de datos de los usuarios hasta hoy día. Ésta tiene por objeto asegurar y resguardar, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos esenciales de las personas físicas. El embrión de esta ley se encuentra en la Constitución de 1978, concretamente en el artículo 18, sobre el derecho a la intimidad familiar y personal y el secreto de las comunicaciones.

Esta ley afecta a toda empresa o autónomo que almacene o recolecte datos de personas físicas, como podrían ser sus empleados, sus clientes, o el curriculum vitae de candidatos. Quedarían exentas de su aplicación aquellas empresas que solo almacenaran datos de otras empresas, pero hoy en día, esto es minoritario.

Así pues, todo usuario, cliente o persona que figure en uno de nuestros archivos tiene una serie de derechos conocidos como ARCO; a saber, Acceso a los Datos, Rectificación de los mismos, Cancelación de los registros y Oposición al uso de los mismos para determinados fines, por ejemplo, publicitarios. La LOPD garantiza asimismo que nuestros datos sean corregidos en un plazo breve de las bases de datos en que figuren, para evitar daños a las personas ahí listados, (por ejemplo borrarnos de una lista de morosos en la que por desidia no se nos eliminó en su momento)

GDPR

En mayo de 2016, la Unión Europea presentó la GDPR. Esta nueva norma viene a sustituir y/o complementar a las leyes nacionales de cada estado miembro referidas a la protección de datos en todos y cada uno de los países de la Unión. Con ella la enorme fragmentación normativa existente se elimina y nuestros datos tienen el mismo tratamiento en los todavía 28 estados que la forman.

Conocida como GDPR (General Data Protection Regulation por sus siglas en inglés), busca dar a los ciudadanos europeos un mayor control sobre su información privada,

además de mejorar la seguridad de las empresas que operan tanto en la UE como en otras partes del mundo pero que almacenan información sobre ciudadanos europeos.

La GDPR plantea novedades en los derechos de las personas sobre sus datos, como es el desarrollo de la noción del derecho al olvido, por el cual podemos solicitar la supresión o rectificación de datos personales en internet, o el derecho a la portabilidad de los mismos. Otra de las grandes novedades de la GDPR es la creación de la figura del DPO (Data Protection Officer), que tiene que ser incorporada en algunas empresas, en aquellas de mayor tamaño (+250 empleados) o en aquellas donde el tratamiento de los datos sea el eje de su estrategia empresarial (en cuyo caso toda empresa, independientemente de su tamaño estaría obligada).

Se estableció un período de adaptación de dos años, y **la norma entrará en vigor en mayo de 2018.**

1.1.2.- SANCIONES POR INCUMPLIMIENTO

El incumplimiento con la LOPD establecía sanciones que iban desde los 600 a los 600.000 Euros, cantidad que se ve superada con las nuevas sanciones establecidas por el GDPR, en cuyo caso las multas pueden llegar a los 20 millones de euros o hasta el 4% de volumen de negocio anual global

1.1.3.- NORMATIVAS QUE FUERON ADOPTADAS EN NUESTRA ADECUACIÓN

La normativa europea supera a la LOPD por lo que el nuevo marco será la GRPD, pero en ningún caso se deroga la LOPD, por lo que a la espera de la adaptación legislativa de la misma se establece el cumplimiento de ambas.

Por tanto, en nuestro supuesto se ha trabajado sobre cómo adecuar el negocio en base al reglamento tecnológico existente LOPD y el que está por llegar GDPR.

1.2.- CONTEXTO DE DESARROLLO

Para el desarrollo del presente TFM, se tomó de base una empresa ficticia a la que se denominó LK TECHNOLOGY S.A. y la cual procedo a presentar a continuación.

Es una empresa cuya plantilla actual no excede de los veinte trabajadores y está dedicada a la venta de productos tecnológicos. La empresa es de reciente creación, y requiere por sus características, una adecuación legal a las normativas TIC. Hay que tener presente que se comercializan productos tecnológicos que se publicitan en Internet, pero que también dispone de una pequeña tienda física en la ciudad de Sevilla, aunque su principal apuesta es centrar su negocio en la venta a través de Internet.

Así la empresa una vez puesta en marcha, debe adaptarse a la normativa vigente que regule su sector, y a aquellas leyes que regulan el tratamiento de datos de carácter personal, concretamente habrá que adecuar el negocio en base al reglamento tecnológico existente en España LOPD, así como también el que está por llegar GDPR.

La empresa cuenta con las siguientes características:

- Su fundadora apuesta por Internet, así está diseñando una página web a través de la cual desarrollará su actividad de comercio electrónico de forma segura. Para alojar la página web ha tenido que adquirir un dominio y contratar un hosting.

- Derivado del anterior punto manejará datos de carácter personal (clientes, publicidad y trabajadores de la empresa).

- Para darse a conocer y aumentar sus ventas la empresa realizará campañas de publicidad en Internet.

- Para la gestión interna de la empresa han desarrollado una intranet propia, la cual ofrece diferentes funcionalidades para su operativa diaria: gestión de compras y ventas, gestión de envíos, gestión de campañas de marketing, gestión de empleados, etc. Todo hecho a medida.

- En base a lo anterior, la intranet contará con una base de datos donde se almacenará información de: Clientes, Proveedores, Trabajadores, etc

- También hay que destacar que para llegar al máximo número posible de clientes, la empresa tendrá presencia en las principales redes sociales.

1.3.- OBJETIVOS

La elaboración del presente Trabajo Final de Máster (TFM), ha tenido como objetivo abordar el estudio de la actual normativa de protección de datos vigente en nuestro país "LOPD" así como también el análisis de la futura normativa europea GDPR.

Para realizar el estudio desde un enfoque práctico, hemos tomado de base una supuesta empresa de venta de productos tecnológicos, la cual se estudió en detalle para poder elaborar un plan de adecuación que cubriese todas las exigencias legales actuales, así como las nuevas recogidas en el GDPR.

Por tanto y en base a lo anterior, se estableció como objetivo final entender el marco europeo referido a la protección de datos, asumiendo su completo entendimiento y su correcta aplicación, lo cual tras varios meses de trabajo puedo concluir en que ha sido alcanzado.

1.4.- METODOLOGÍA

La metodología que se ha seguido durante el desarrollo del presente TFM fué principalmente una primera fase de investigación, donde se marcó como prioridad la recopilación y estudio de documentación que fuese de interés para el desarrollo de la adaptación a realizar. En una segunda fase, y tras haber abordado un estudio que me permitió sentar unas bases sobre las que trabajar, pasé al desarrollo de una documentación que recogió las diferentes partes que establecía el marco normativo objeto del estudio. En una primera entrega recogí lo referido a la LOPD y en una segunda entrega todo lo vinculado al GDPR.

Los diferentes elementos resultantes, se presentaron a través de diferentes entregas que se realizaron a lo largo del semestre tal y como se describe en la planificación.

1.5.- PLANIFICACIÓN

A continuación, paso a detallar la planificación seguida durante la elaboración del presente TFM.

PEC 2. FASE DE ESTUDIO E INVESTIGACIÓN.

(Fecha de Inicio: 10/10/17 - Fecha de Entrega: 06/11/17)

Descripción de la Fase: Durante esta fase abordé el estudio e investigación del diferente material que tomé como base para el TFM.

Entregable: Como resultado obtuve un entregable que recogía las biografías y fuentes consultadas y un borrador con el índice del documento de adecuación que abordaría en las siguientes entregas.

PEC 3. FASE DE DESARROLLO. ADAPTACIÓN A LA LOPD

(Fecha de Inicio: 07/11/17 - Fecha de Entrega: 04/12/17)

Descripción de la Fase: Durante esta fase me centré en la LOPD y trabajé en el desarrollo de la adaptación de la empresa tomada como base para el estudio. Todo el desarrollo se hizo siguiendo el índice elaborado en el entregable citado anteriormente.

Entregable: Como resultado se obtuvo el plan de adecuación a la LOPD de la empresa sobre la que trabajé.

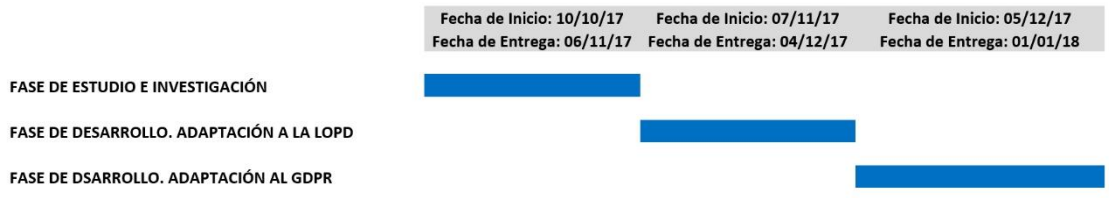
PEC 4. FASE DE DESARROLLO. ADAPTACIÓN A LA GDPR

(Fecha de Inicio: 05/12/17 - Fecha de Entrega: 01/01/18)

Descripción de la Fase: Durante esta fase me centré en el GDPR y trabajé en el desarrollo de la adaptación de la empresa tomada como base para el estudio. Todo el desarrollo se hizo siguiendo el índice elaborado en la PEC2.

Entregable: Como resultado se obtuvo el plan de adecuación al GDPR de la empresa sobre la que trabajamos.

Tabla Resumen de la Planificación



2.- LOPD

En este capítulo, voy a describir brevemente los puntos más destacables que se han trabajado a lo largo de la adaptación de la empresa LK Technology a la Ley Orgánica de Protección de Datos. Para empezar y con la finalidad de mostrar la estructura seguida durante la elaboración de la documentación, en el primer punto se reflejará el índice del documento resultante (ver anexo 1).

2.1.- ÍNDICE DE LA ADAPTACIÓN

I. DOCUMENTO DE SEGURIDAD

1. Introducción

2.- Ámbito de Aplicación
- 2.1 Ámbito Subjetivo
- 2.2 Ámbito Objetivo. Recursos protegidos
- 2.3 Definiciones

3.- Medidas, Normas, Procedimientos, Reglas y Estándares
- 3.1 Control de acceso
- 3.2 Gestión de soportes y documentos
- 3.3 Ejecución del tratamiento fuera de los locales
- 3.4 Ficheros temporales, copias y reproducciones.
- 3.5 Responsable de seguridad
- 3.6 Medidas Alternativas
- 3.7 Identificación y autenticación
- 3.8 Control de acceso físico
- 3.9 Procedimientos de realización de copias de respaldo y de recuperación de los datos.
- 3.10 Redes de comunicaciones

4. -Funciones y Obligaciones del Personal

5.- Ficheros con Datos de Carácter Personal y Descripción de los Sistemas de Información
- 5.1 Ficheros
- 5.2 Sistemas de Información

6.- Procedimiento de Notificación, Gestión y Respuesta ante las Incidencias
- 6.1 Procedimiento de notificación, gestión y respuesta ante incidencias.
- 6.2 Registro de incidencias

7.- Medidas para el transporte, Destrucción, y Reutilización de Soportes y Documentos

II. CLÁUSULAS Y CIRCULARES INFORMATIVAS

1.- Establecimiento
2.- Correo Electrónico
3.- Genérica
4.- Web

III.- PERSONAL

1.- Contratos de confidencialidad

IV.- TERCEROS

1.- Contratos de acceso a datos

V.- DERECHOS ARCO

1.- Cuestiones Generales
2.- Derecho de Acceso
3.- Derecho de Rectificación
4.- Derecho de Cancelación
5.- Derecho de Oposición

2.2.- INSCRIPCIÓN DE LOS FICHEROS

Uno de los primeros pasos que una empresa debe realizar cuando se está adaptando a la LOPD, es la inscripción de los ficheros ante la Agencia Española de Protección de datos (AGPD). Este proceso consiste en informar a la agencia sobre que tipo de información es la que la empresa trata, así como el nivel de la misma.

Los ficheros se catalogan en tres niveles: básico, medio y alto, y dicha categorización va directamente vinculada a la sensibilidad de la información que se trate. Por ejemplo, un fichero de clientes con información básica de facturación, se catalogará como básico, mientras que un fichero de historiales clínicos de pacientes de un hospital será de nivel alto. Esta catalogación de la información, será la que se tome de base posteriormente para saber que medidas de seguridad hay que aplicar.

Volviendo al proceso de inscripción de ficheros, cabe resaltar que la AGPD pone al servicio del usuario que tenga que realizar dicha inscripción una herramienta gratuita que funciona de forma online, mediante la cual se realiza la inscripción de forma telemática. Dicha herramienta es conocida como NOTA.

Link: https://sedeagpd.gob.es/sede-electronica-web/vistas/formNOTA/nt01Inicio.jsf

2.3.- DOCUMENTO DE SEGURIDAD

El documento de seguridad es una de las partes fundamentales de la protección de datos dentro del marco de la LOPD y ha sido el documento que más horas de trabajo ha requerido durante el proceso de adaptación de LK Technology. El documento de seguridad es el documento mediante el cual se elabora y adoptan las medidas técnicas y organizativas necesarias para garantizar la seguridad de los datos de carácter personal, su adopción es de obligado cumplimiento para el responsable del fichero.

El documento de seguridad debe contener las medidas de seguridad, tanto técnicas como organizativas de la empresa, en relación con los datos personales que recoge y trata. Por tanto, el documento de seguridad contendrá:

1) **Identificación de la empresa, sus servicios y ámbito** de aplicación del documento de seguridad.

2) **Los ficheros** que la empresa tiene (clientes, trabajadores, cámaras de seguridad, etc.) y su estructura, es decir, nombre del fichero, origen de los datos, forma de tratamiento de los datos (soporte papel o informático), tipos de datos que se recogen (nombre, apellidos, dirección postal, teléfono, dirección electrónica…), nivel de seguridad del fichero (básico, medio o alto) y la empresa encargada de gestionar el fichero si la hubiere (por ejemplo: la gestoría laboral es la encargada de gestionar el fichero de RRHH, en tanto y en cuanto, elabora las nóminas de los trabajadores).

3) Cuáles son **las medidas de seguridad** que las empresa tiene para proteger esos ficheros, señalar, entre otras: armarios cerrados con llave, despachos cerrados con llave, destructoras de papel en los despachos que contiene documentación en soporte papel, contraseñas personales en los ordenadores con acceso a datos personales, caducidad de las contraseñas, cómo, dónde y cuándo se hacen las copias de seguridad, dónde se guardan las referidas copias de seguridad, con qué periodicidad se hacen, cuál es el procedimiento a seguir en caso de que se produzca una incidencia en la empresa respecto a datos personales, etc.

4) Relación de los **encargados del tratamiento**, es decir, de las empresas a las que se ha contratado la prestación de un servicio y en función de dicha prestación tienen acceso a datos personales. Por ejemplo: la gestoría laboral, gestoría fiscal, la empresa de mantenimiento informático, la empresa de prevención de riesgos laborales, etc.).

5) **Inventario** de los soportes con acceso a datos personales dónde se realizan las copias de seguridad, de los equipos informáticos que tienen acceso a datos y de los programas informáticos.

6) **Lista del personal de la empresa** con acceso a datos y las funciones de cada uno de ellos (a qué ficheros acceden y qué pueden acceder con los datos personales que tratan).

En este sentido el artículo 88.3 del RLOPD, establece:

El documento deberá contener, como mínimo, los siguientes aspectos:

a) Ámbito de aplicación del documento con especificación detallada de los recursos protegidos.

b) Medidas, normas, procedimientos de actuación, reglas y estándares encaminados a garantizar el nivel de seguridad exigido en este reglamento.

c) Funciones y obligaciones del personal en relación con el tratamiento de los datos de carácter personal incluidos en los ficheros.

d) Estructura de los ficheros con datos de carácter personal y descripción de los sistemas de información que los tratan.

e) Procedimiento de notificación, gestión y respuesta ante las incidencias.

f) Los procedimientos de realización de copias de respaldo y de recuperación de los datos en los ficheros o tratamientos automatizados.

g) Las medidas que sea necesario adoptar para el transporte de soportes y documentos, así como para la destrucción de los documentos y soportes, o en su caso, la reutilización de estos últimos.

Y el apartado 4 del mismo artículo añade:

En caso de que fueran de aplicación a los ficheros las medidas de seguridad de nivel medio o las medidas de seguridad de nivel alto, previstas en este título, el documento de seguridad deberá contener además:

a) La identificación del responsable o responsables de seguridad.

b) Los controles periódicos que se deban realizar para verificar el cumplimiento de lo dispuesto en el propio documento.

2.4.- DERECHOS ARCO

La LOPD otorga a los ciudadanos cuatro derechos fundamentales vinculados a la protección de datos y tienen como finalidad garantizar el poder de control sobre sus datos, son conocidos como derechos ARCO, cuyo acrónimo proviene de Acceso, Rectificación, Cancelación y Oposición.

Aunque en la adaptación dedico un capítulo a dichos derechos, quiero reflejar resumidamente en la presente memoria cuáles son:

Derecho de Acceso

Contenido en el art. 15 LOPD, supone que "el interesado tendrá derecho a solicitar y obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento, el origen de dichos datos, así como las comunicaciones realizadas o que se prevén hacer de los mismos". De aquí podemos extraer que, como contrapartida, todo aquél que resulte ser el responsable de un fichero deberá facilitar gratuitamente la información que el titular de los datos solicite. En ocasiones, tal y como bien comprenderéis, la respuesta es fácil (el fichero contiene estos y estos datos, obtenidos por su condición de cliente y no se prevén comunicaciones o cesiones de sus datos a nadie) mientras que, en otras, se puede convertir en un auténtico quebradero de cabeza (imaginad una gran empresa que compra ficheros para completar los suyos propios y que, al conformar un conglomerado empresarial, cede los datos obtenidos a todas las empresas integrantes del grupo).

Por fortuna, la misma ley establece una limitación a este acceso, de forma que solo puede solicitarse con una periodicidad anual, salvo que se acredite un interés legítimo por parte del interesado.

Derechos de Rectificación y Cancelación

Estos derechos e encuentran inextricablemente unidos, pues, en definitiva, no son más que alternativas dadas al interesado (nuestro cliente o titular de los datos que contiene nuestro fichero) en relación con las posibilidades de disposición de los datos. En este sentido, pensad que si yo sé que tal empresa tiene un fichero en el que hay datos míos, bien puedo solicitar que los corrijan por ser erróneos o incompletos o bien que los eliminen del fichero.

Derecho de oposición

Este último derecho otorga al interesado la facultad de obligar a que no se lleve a cabo el tratamiento de sus datos o a que cese el tratamiento que ya se ha iniciado. La aplicación práctica consistiría en evitar que esos datos se utilicen, ya sea para no ser incluido en campañas promocionales o para que no se incluyan en estadísticas, es decir, poco importa el tratamiento que se haga con los datos pues lo importante es que se pone en conocimiento del responsable del tratamiento que no se desea que esa utilización continúe.

2.4.- SANCIONES

La cuantía de las sanciones que impone la LOPD se gradúa atendiendo a la naturaleza de los derechos personales afectados, al volumen de los tratamientos efectuados, a los beneficios obtenidos, al grado de intencionalidad, a la reincidencia, a los daños y perjuicios causados a las personas interesadas y a cualquier otra circunstancia que sea relevante para determinar el grado de culpabilidad.

Son infracciones leves: Sanciones entre 600 € y 60.000 €

- No solicitar la inscripción del fichero en la Agencia Española de Protección de Datos (AEDP)
- Recopilar datos personales sin informar previamente
- No atender a las solicitudes de rectificación o cancelación
- No atender las consultas por parte de la AGPD.

Son infracciones graves: Sanciones entre 60.000 € y 300.000 €

- No inscribir los ficheros en la AGPD.
- Utilizar los ficheros con distinta finalidad con la se crearon.
- No tener el consentimiento del interesado para recabar sus datos personales
- No permitir el acceso a los ficheros.
- Mantener datos inexactos o no efectuar las modificaciones solicitadas
- No seguir los principios y garantías de la LOPD
- Tratar datos especialmente protegidos sin la autorización del afectado
- No remitir a la AGPD las notificaciones previstas en la LOPD.
- Mantener los ficheros sin las debidas condiciones de seguridad.

Son infracciones muy graves: Sanciones entre 300.000 € y 600.000 €

- Crear ficheros para almacenar datos que revelen datos especialmente protegidos.
- Recogida de datos de manera engañosa o fraudulenta.
- Recabar datos especialmente protegidos sin la autorización del afectado.
- No atender u obstaculizar de forma sistemática las solicitudes de cancelación o rectificación.
- Vulnerar el secreto sobre datos especialmente protegidos.
- La comunicación o cesión de datos cuando ésta no esté permitida.
- No cesar en el uso ilegítimo a petición de la AGPD.
- Tratar los datos de forma ilegítima o con menosprecio de principios y garantías que le sean de aplicación.
- No atender de forma sistemática los requerimientos de la AGPD.
- La transferencia temporal o definitiva de datos de carácter personal con destino a países sin nivel de protección equiparable o sin autorización

3.- GDPR

Llegados a este punto, vamos a centraros ahora en comentar los puntos más destacables que se han trabajado a lo largo de la adaptación de la empresa LK Technology al GDPR. Tal y como hice en el apartado anterior, para empezar con el desarrollo de este apartado y con la finalidad de mostrar la estructura seguida durante la elaboración de la documentación, en el primer punto se reflejará el índice del documento resultante.

3.1.- ÍNDICE DE LA ADAPTACIÓN

I. MEDIDAS DE RESPONSABILIDAD ACTIVA

1.- Análisis de riesgo

2.- Registro de actividades de tratamiento

II. MEDIDAS DE SEGURIDAD

1.- Información de interés general

2.- Medidas Organizativas

3.- Medidas Técnicas
  3.1 Identificación
  3.2 Deber de Salvaguarda

III. CLÁUSULAS INFORMATIVAS

1.- Tratamiento de datos de clientes
2.- Tratamiento de datos de potenciales clientes
3.- Tratamiento de datos de candidatos
4.- Tratamiento de datos de proveedores

IV.- PERSONAL

1.- Contratos de confidencialidad

V.- TERCEROS

1.- Contratos de acceso a datos

VI.- DERECHOS

1.- Derecho de Acceso
2.- Derecho al olvido
3.- Limitación de tratamiento
4.- Portabilidad

3.2 ANÁLISIS DE RIESGO

El GDPR condiciona la adopción de las medidas de responsabilidad activa al riesgo que los tratamientos puedan suponer para los derechos y libertades de los interesados.

Se maneja el riesgo de dos maneras:

- En algunos casos, prevé que determinadas medidas solo deberán aplicarse cuando el tratamiento suponga un alto riesgo para los derechos y libertados (por ejemplo, Evaluaciones de impacto sobre la Protección de Datos).

- En otros casos, las medidas deberán modularse en función del nivel y tipo de riesgo que el tratamiento conlleve (por ejemplo, con las medidas de Protección de Datos desde el Diseño o con las medidas de seguridad).

Obligaciones

Todos los responsables deberán realizar una valoración del riesgo de los tratamientos que realicen, a fin de poder establecer qué medidas deben aplicar y cómo deben hacerlo. El tipo de análisis variará en función de:

• los tipos de tratamiento,
• la naturaleza de los datos,
• el número de interesados afectados,
• la cantidad y variedad de tratamientos que una misma organización lleve a cabo.

Grandes organizaciones: como regla general, el análisis deberá llevarse a cabo utilizando alguna de las metodologías de análisis de riesgo existentes.

Organizaciones de menor tamaño y con tratamientos de poca complejidad: el análisis será el resultado de una reflexión, mínimamente documentada, sobre las implicaciones de los tratamientos en los derechos y libertades de los interesados.

En el supuesto tomado como base en el TFM que nos ocupa, al tratarse de una PYME se ha optado por realizar la reflexión documentada, que como se ha descrito anteriormente, se contempla para el caso de pequeñas empresas con tratamientos de poca complejidad.

Para ello se realizó una tabla de valoración del riesgo en la cual se obtuvo que el 100% de las respuestas había sido negativa, y por tanto se concluyó que la organización no realiza tratamientos que generen un elevado nivel de riesgo y que, por tanto, no debe poner en marcha las medidas previstas para esos casos.

3.3.- REGISTRO DE ACTIVIDADS DE TRATMIENTO

Una gran novedad, es que todo apunta a que la obligatoriedad que se tenía en la LOPD respecto a la inscripción de ficheros, será sustituida por la de contar con un registro de actividades.

Según el artículo 30, cada responsable o su representante legal, llevará un registro de actividades de tratamiento efectuadas bajo su responsabilidad. Por lo tanto, el responsable se encuentra de nuevo ante la necesidad de describir:

- los datos del responsable, representante, delegado de protección de datos, etc.
- los datos que recoge,
- descripción y categorías de interesados,
- el fin al que los destina,
- los destinatarios,
- si los transfiere a terceros países,
- medidas técnicas y organizativas adoptadas,
- plazos previstos de supresión.

3.4.- AMPLIACIÓN DE LOS DERECHOS DEL INTERESADO

Los derechos ARCO, con la nueva normativa europea se ven aumentados siendo los cambios más significativos los que describo a continuación.

DERECHO AL OLVIDO

El RGPD incorpora el **derecho al olvido,** como un derecho vinculado al derecho de supresión, el derecho a la limitación del tratamiento y el derecho a la portabilidad:

Los interesados tienen derecho a obtener la supresión de los datos ("derecho al olvido") cuando:

- Los datos ya no sean necesarios para la finalidad para la que fueron recogidos.
- Se revoque el consentimiento en el que se basaba el tratamiento.
- El interesado se oponga al tratamiento.
- Los datos se hayan tratado ilícitamente.

- Los datos se tengan que suprimir para el cumplimiento de una obligación legal.
- Los datos se hayan obtenido en relación con la oferta de servicios de la sociedad de la información dirigidos a menores.

Cuando el responsable haya hecho públicos los datos personales y se tengan que suprimir, adoptará medidas razonables para informar de la supresión a los responsables que están tratando los datos.

Se prevén algunas excepciones al ejercicio de este derecho:

- El ejercicio del derecho a la libertad de expresión e información.
- El cumplimiento de una obligación legal.
- La existencia de fines de archivo en interés público, de investigación científica o histórica o fines estadísticos.
- La formulación, el ejercicio o la defensa de reclamaciones.

DERECHO A LA LIMITACIÓN DEL TRATAMIENTO

La limitación de tratamiento se presenta en el RGPD como un derecho de los interesados. Por ello, no debe confundirse con el bloqueo de datos actualmente existente en la legislación española, aunque su inclusión como nuevo derecho no supone por sí sola la desaparición de la figura del bloqueo.

La limitación de tratamiento supone que, a petición del interesado, no se aplicarán a sus datos personales las operaciones de tratamiento que en cada caso corresponderían. La limitación puede solicitarse cuando:

- El interesado ha ejercido los derechos de rectificación u oposición y mientras el responsable determina si procede atender a la solicitud
- El tratamiento es ilícito, lo que determinaría el borrado de los datos, pero el interesado se opone a ello
- Los datos ya no son necesarios para el tratamiento, lo que nuevamente determinaría su borrado, pero el interesado solicita la limitación porque los necesita para la formulación, el ejercicio o la defensa de reclamaciones

A este derecho se le aplican los mismos plazos y procedimientos que a los restantes derechos previstos en el RGPD.

En el tiempo que dure la limitación, el responsable sólo podrá tratar los datos afectados, más allá de su conservación:

- Con el consentimiento del interesado
- Para la formulación, el ejercicio o la defensa de reclamaciones
- Para proteger los derechos de otra persona física o jurídica
- Por razones de interés público importante de la Unión o del Estado miembro correspondiente

Una consecuencia de esta regulación es que impide una práctica que se sigue en ocasiones y que consiste en borrar los datos cuando se ejercitan otros derechos, como el de acceso, ya que impediría el ejercicio del derecho a la limitación del tratamiento.

DERECHO A LA PORTABILIDAD

El derecho a la portabilidad de los datos es una forma avanzada del derecho de acceso en la que la persona interesada tiene derecho a recibir los datos personales que le afectan que haya facilitado a un responsable del tratamiento en un formato estructurado, de uso común y de lectura mecánica, y transmitirlos a otro responsable, si se cumplen los requisitos siguientes:

- El tratamiento esté basado en el consentimiento o en un contrato
- El tratamiento se haga por medios automatizados
- Cuando el interesado lo solicita respecto a los datos que haya proporcionado al responsable y que le conciernan incluidos los datos derivados de la propia actividad del interesado. Esto supone que no es aplicable a los datos de terceras personas que un interesado haya facilitado a un responsable. Como tampoco se aplicaría si el interesado solicita la portabilidad de datos que le incumban pero que hayan sido proporcionados al responsable por terceros.

Incluye el derecho a que los datos se transmitan directamente de responsable a responsable, cuando sea técnicamente posible.

3.5.- SANCIONES

Sin duda otra los grandes cambios del nuevo reglamento, es el endurecimiento de las sanciones.

Las obligaciones específicas en materia de seguridad están recogidas en la Sección 2 del capítulo IV del RGPD, aunque hay otras medidas técnicas a lo largo del RGPD que pueden estar asociadas a la seguridad. Esta Sección lleva el título de “Seguridad de los datos personales” e incluye tres artículos relaitivos a la seguridad del tratamiento (Artículo 32), la notificación de una violación de la seguridad de los datos personales a la autoridad de control (Artículo 33) y la comunicación de una violación de la seguridad de los datos personales al interesado (Artículo 34).

Las acciones descritas en esta sección y destinadas a garantizar un nivel de seguridad adecuado para el riesgo detectado incluirán, entre otras, las siguientes medidas:

- Seudonimización y el cifrado de datos personales.
- Medidas capaces de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.
- Medidas capaces de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico.
- Proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.
- Evaluación periódica del riesgo de 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.
- Adhesión a un código de conducta aprobado a tenor del artículo 40.
- Adhesión a un mecanismo de certificación aprobado a tenor del artículo 42.
- Medidas para garantizar que cualquier persona que actúe bajo la autoridad del responsable o del encargado y tenga acceso a datos personales solo pueda tratar dichos datos siguiendo instrucciones del responsable.

Una infracción de estas obligaciones establecidas en materia de seguridad, tendría una sanción de hasta 10 millones o el 2% del volumen de negocio ya que afectaría a los artículos 32, 33 y 34, cuyo incumplimiento está considerado como una infracción grave.

En cambio, la mayor parte de las infracciones relacionadas con las obligaciones jurídicas están consideradas como infracciones muy graves. con sanciones de hasta 20 millones o del 4% del volumen de negocio.

4.- CONCLUSIONES

A continuación, expondré las conclusiones a las que he llegado tras el trabajo realizado a lo largo de estos últimos meses

4.1.- Conclusiones LOPD

La experiencia de realizar una adecuación basada en la conocida Ley Orgánica de Protección de Datos (LOPD), así como el reglamento Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, ha sido sin duda muy enriquecedora.

Trabajar bajo este marco normativo, ha sido "cómodo" ya que no hay lugar para interpretaciones puesto que es un marco consolidado donde todo está perfectamente establecido y por tanto no hay lugar a interpretaciones. Igualmente, la cantidad de recursos que se pueden consultar son innumerables, así como la existencia de diferentes herramientas orientadas a cumplir con el marco normativo, todo ello ayuda mucho a que una pyme pueda afrontar un proceso de adaptación de una forma fluida y sin grandes esfuerzos.

Respecto a las medidas de seguridad que establece el reglamento, en mi opinión son asumibles y ello permite que se pueda dar cumplimiento sin realizar un esfuerzo económico excesivo para una empresa.

4.2.- Conclusiones GDPR

Afrontar la adaptación de una PYME al General Data Protection Regulation (GDPR), es sin duda toda una aventura a fecha de hoy.

A diferencia de lo que comentaba anteriormente con la LOPD, en este caso la desinformación generalizada sobre esta nueva normativa así como las miles de interpretaciones que se barajan sobre diferentes puntos es algo abrumador.

Pese a la labor de información que está llevando a cabo la Agencia Española de Protección de Datos, mediante la publicación de diferentes documentos y guías, son muchas las dudas que inundan todavía a quien pretende afrontar un proceso de adecuación a esta nueva normativa.

Otro punto destacable que hay que resaltar, es la dificultad que tienen que afrontar las pequeñas empresas para dar cumplimiento al reglamento. En mi opinión este nuevo marco está orientado a grandes empresas con recursos humanos y tecnológicos que puedan seguir las pautas indicadas, pero para una PYME el perfecto cumplimiento de lo establecido supondrá uno esfuerzos sobredimensionados.

4.3.- Conclusión General

Para concluir, quiero destacar que nos encontramos inmersos en una gran transformación en cuanto a protección de datos se refiere. La inminente publicación del anteproyecto de Ley que actualizará la actual LOPD, hará que los próximos meses sean vitales para definir líneas de actuación y los procedimientos a seguir, de cara a que a partir del próximo día 25 de mayo todos estemos en disposición de dar cumplimento al nuevo marco Europeo con las máximas garantías.

Aun así, el camino empieza ahora y será con el paso del tiempo cuando se vayan dispersando todas las dudas que hoy nos envuelven.

5.- REFERENCIAS

A continuación, hemos recopilado las principales fuentes de información consultadas. Aunque han sido muchísimos los recursos que a lo largo de estos meses he podido revisar, finalmente son los que se referencian a continuación los que he considerado más destacables.

BOE

Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
http://www.boe.es/buscar/doc.php?id=BOE-A-1999-23750

Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.
http://www.boe.es/buscar/doc.php?id=BOE-A-2008-979

DIARIO OFICIAL DE LA UNIÓN EUROPEA

Reglamento (UE) 2016/679 del parlamento Europeo y del Consejo
http://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/union_europea/reglamentos/common/pdfs/Reglamento_UE_2016-679_Proteccion_datos_DOUE.pdf

AGPD

Agencia Española de Protección de Datos. (Diversas secciones de la Web)
http://www.agpd.es

Sección específica con diferentes recursos sobre el nuevo reglamento europeo
https://www.agpd.es/portalwebAGPD/temas/reglamento/index-ides-idphp.php

INCIBE

Dossier de Cumplimiento Legal
https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_cumplimientolegal.pdf

Primeros pasos para cumplir el nuevo RGPD
https://www.incibe.es/protege-tu-empresa/blog/primeros-pasos-cumplir-el-nuevo-rgpd

OTRAS WEBS CONSULTADAS

CuidaTusDatos. Portal formativo sobre protección de datos.
http://www.cuidatusdatos.com

Ayuda y protección de Datos. Blog con diferentes artículos
https://ayudaleyprotecciondatos.es

Blog RGPD
http://rgpd.es

6.- ANEXOS

De forma complementaria a la presente memoria, se adjuntan los entregables resultantes de los procesos de adecuación de la empresa tomada como base LK Technology, S.A., a ambas normativas: LOPD y GDPR.

6.1.- ANEXO 1.- PEC 3 – Adecuación a la LOPD

6.2.- ANEXO 2.- PEC 4 – Adecuación al RGPD

(Los anexos han sido eliminados por contener datos de carácter personal)