LOPD-Elaboración de un Plan de Seguridad y Auditoría Interna

Elena María García Villacorta
Ingeniería Informática
Administración de Redes y Sistemas Operativos

Eduard Marco Galindo

Pierre Bourdin

07/06/2017

FICHA DEL TRABAJO FINAL

Título del trabajo:	*LOPD-Elaboración de un Plan de Seguridad y Auditoría Interna*
Nombre del autor:	*Elena María García Villacorta*
Nombre del consultor:	*Eduard Marco Galindo*
Nombre del PRA:	*Pierre Bourdin*
Fecha de entrega (mm/aaaa):	*24/05/2017*
Titulación:	**Ingeniería Informática**
Área del Trabajo Final:	*Administración de redes y Sistemas Operativos*
Idioma del trabajo	*Castellano*
Palabras clave	**Máximo 3 palabras clave, validadas por el director del trabajo (dadas por los estudiantes o en base a listados, tesauros, etc.)** LOPD Seguridad Auditoria

Resumen del Trabajo (máximo 250 palabras):

El Proyecto Fin de Carrera está enmarcado dentro del Área de Trabajo "**Administración de redes y sistemas operativos**" de la titulación de Ingeniería Informática cursada en la UOC.

El documento comienza describiendo el problema planteado, los objetivos del trabajo, cómo es el proyecto y cuáles son los entregables que se han realizado.

Seguidamente se hará mención al método utilizado y calendario para poder entender la evolución de este trabajo, cuáles son sus límites y objetivos.

El trabajo comienza con la introducción sobre la Ley Orgánica de Protección de Datos, y una breve explicación de la legislación vigente, ya que será fundamental para el desarrollo del trabajo en cuestión y otras cuestiones relevantes.

Esto nos permitirá sumergirnos en todo lo necesario para la realización de un Plan de Seguridad y adaptar nuestra empresa FormacionL según las necesidades encontradas en la realización de una Auditoría Interna.

Realiza un profundo análisis de la empresa, primeramente se ha evaluado la empresa para conocer su situación, después se realiza una auditoría para evaluar cuáles son las amenazas y después se adoptan las medidas para dotar a la misma de un nivel de seguridad adecuado para proteger su información implantando un plan de seguridad adecuado y haciendo las recomendaciones oportunas para conseguir un nivel adecuado de seguridad informática.

Por último se han ofrecido al lector unas conclusiones acerca del proyecto, basándonos en la experiencia del desarrollo del mismo y la bibliografía utilizada para la investigación de este trabajo.

Abstract (in English, 250 words or less):

The End-of-Degree Project is framed within the Work Area "Administration of networks and operating systems" of the Degree in Computer Engineering at the UOC.

The document begins by describing the problem, the objectives of the work, what the project is like and what deliverables have been produced.

Next, the method used and the calendar will be mentioned in order to understand the evolution of this work, as well as what its limits and objectives are.

The work begins with the introduction of the Organic Law on Data Protection, and a brief explanation of the applicable legislation, as it will be fundamental for the development of the work in question, as well as other relevant issues.

This will allow us to get acquainted to everything which is needed for carrying out a Security Plan and adapt our company FormacionL according to the needs found in an Internal Audit.

It carries out a deep analysis of the company, by firstly evaluating the company to know its situation, and then carrying out an audit to evaluate what the threats are, to then adopt measures to provide it with an adequate level of security to protect its Information by implementing an adequate security plan and making the appropriate recommendations to achieve a proper level of IT security.

Finally, the reader has been offered some conclusions about the project, based on the experience of its development and the bibliography used for the research of this work.

Índice

Indice de Diagramas

Índice de Tablas

1.- Introducción

El presente documento constituye la memoria del Proyecto "**LOPD-Elaboración de un Plan de Seguridad y Auditoría interna**" al que, a partir de ahora, haremos referencia como "**Proyecto Final de Carrera o PFC"**.

El PFC está enmarcado dentro del Área de Trabajo "**Administración de Redes y Sistemas Operativos**" de la titulación de Ingeniería Informática cursada en la UOC. Este PFC se ha realizado como asignatura de la carrera dentro de este Área de Trabajo con el fin de poner en práctica los conocimientos adquiridos a lo largo de estos años.

Los elementos que se evaluarán en este proyecto son:

- El Documento, denominado "Plan de Trabajo"
- Dos Pruebas de Evaluación Continua a las que, a partir de ahora, denominaremos "PEC", con su enumeración en el tiempo, nombradas como PEC2 y PEC3. Las entregas de estos documentos van siendo la visibilidad del desarrollo del proyecto en dos tiempos diferentes.

Los **entregables finales del proyecto** consisten en:

- Un documento Memoria (de no más de 90 páginas).
- Una Presentación Virtual (un video de no más 20 minutos, explicando el PFC de forma esquemática).

Las entregas de la PEC2, PEC3 y de la memoria se van a considerar **hitos del Proyecto Final de Carrera**. Por lo tanto, estos hitos como la distribución de las tareas, se va a reflejar en el diagrama de Gantt del PFC.

El PFC trata de la realización de una Auditoría Interna de los diferentes centros de trabajo y de los Sistemas de Información de FormacionL, y según el resultado de esta elaborar un Plan de Seguridad que permita adaptar la empresa al cumplimiento de la LOPD

A continuación, vamos a escribir sobre el Contexto y Justificación para la realización de este PFC.

1.1.- Contexto y justificación del Trabajo

Las necesidades a cubrir en el desarrollo del PFC es el cumplimiento de la normativa legal LOPD sobre datos de carácter personal en la empresa FormacionL, debido a la cantidad de datos de carácter personal existentes para el desarrollo de su actividad. Para ello realizaremos una Auditoría Interna y posteriormente un Plan de Seguridad**.**

Al día de hoy los **datos de carácter personal** para ser usados por parte de una empresa deben seguir la legislación indicada por la Agencia de Protección de Datos, a partir de ahora **AEPD.**

En la actualidad en cualquier empresa uno de los activos más importantes son los Sistemas de Información a los que a partir de ahora denominaremos **SI.** Según la AEPD un **Sistema de información** es "un conjunto de ficheros, tratamientos, programas, soportes y en su caso, equipos empleados para el tratamiento de datos de carácter personal".

Igualmente, los datos que existen y que se tratan son de diversa índole, estos pueden ser datos de información personal, bancarios, numéricos, de geolocalización, …

Estos datos se pueden seguir clasificando de muchas formas según su uso, temporalidad, origen y otras muchas clasificaciones, pero en este PFC nos vamos a centrar en los **datos de carácter personal** y toda su casuística.

La definición de datos de **carácter personal** por parte de la **AEPD** es "**cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables**".

Hasta ahora los ficheros que se protegen los datos de carácter personal son los que están en soporte en papel, y del resto se han ido poco a poco resolviendo el problema, pero ni se ha realizado el estudio en profundidad, ni se han cambiado las herramientas que soportan los datos.

En el Anexo I: Tipología de los datos de carácter personal, hay una relación de los datos de carácter personal y su tipología.

Porque es un tema relevante

La realización de este TFC es por la relevancia que tiene el cumplimiento de la LOPD ya que la empresa **FormacionL** al servicio de la ciudadanía, maneja ingentes cantidades de datos de carácter personal a través de los múltiples dispositivos, tecnológicos y humanos, que tiene a disposición. Es por ello que este **PFC** se pone en marcha, en pos de garantizar el cumplimiento de la normativa vigente e instaurar buenas prácticas en el tratamiento de la información de carácter personal de nuestras personas usuarias y garantizar el derecho a la intimidad, imagen y autodeterminación informativa de las personas.

En nuestro caso nuestra empresa **FormaciónL,** por su delicada situación en cuanto a la cantidad de datos de carácter personal que necesita de las personas usuarias para la realización de dicha actividad. Su actividad es la realización de cursos de formación, analizar problemáticas de las personas usuarias, recopilar datos de posibles alumnos y muchas otras acciones relacionadas con la formación y la actividad profesional de la ciudadanía. Nuestra empresa consta de una serie de centros distribuidos por las diferentes provincias de la comunidad andaluza.

En cualquier empresa, se debe cumplir esta normativa tanto para los datos utilizados para el funcionamiento interno de la empresa, como en el trato con las

personas usuarias para la realización de su actividad (en caso de tratar este tipo de datos).

Resultados

En la medida que habilitemos los procedimientos, medidas y normas en FormacionL a través del Plan de Seguridad, las personas usuarias se sentirán seguras a la hora de facilitar los datos a dicha empresa y, de forma interna, tendremos las garantías suficientes respecto a la calidad, protección y seguridad de los mismos

En el siguiente apartado vamos a tratar los objetivos de trabajos de este **PFC.**

1.2.- Objetivos del Trabajo

FormacionL es una organización viva, y sus **Sistemas de Información** deben ser fiel reflejo de su forma de trabajar, la de no duplicar datos, la fiabilidad, seguridad e integridad de los datos

Por lo tanto, el **objetivo** a conseguir en la realización de este PFC es conseguir que FormacionL sea una **empresa que garantiza la seguridad de los datos, la protección de la intimidad y la autodeterminación informativa de las personas siguiendo la normativa de la AEPD.**

Las medidas que vamos a estudiar e intentar poner en marcha, tienen la intención de **garantizar la protección total de los datos íntimos, personales y que son, en definitiva, propiedad de cada persona.**

Para obtener dicho objetivo, debemos tener en cuenta el cumplimiento de la Ley Orgánica de Protección de Datos a la que haremos referencia a partir de ahora como **LOPD,** y la implantación de un Plan de Seguridad según la información obtenida a través de la elaboración de una Auditoría Interna**.**

Los dos actores que interactúan en este PFC son:

- la actividad de la empresa que presta los servicios
- los ciudadanos que intervienen (a los que llamaremos usuarios, personas usuarias, beneficiaros o alumnos indistintamente)

Para conseguir la **implementación de los objetivos del proyecto**, necesitamos en primer lugar seguir los objetivos descritos en el documento de propuesta.

Los **objetivos estratégicos** de este PFC son:

a) Estudio y conocimiento de la LOPD

b) Auditoría Interna

i. Análisis de los Sistemas de Información de la FormacionL

ii. Análisis del papel realizado por los diferentes actores involucrados en el funcionamiento de la empresa

c) Realización del Plan de Seguridad

i. Implantación de las medidas, procedimientos, cláusulas a incluir. para el cumplimiento de la LOPD

ii. Implantación del Documento de Seguridad

Con ello pretende apoyar las tareas de cumplimiento de la Ley Orgánica, así como incidir en el fomento de las buenas prácticas en lo que se refiere al tratamiento de la información personal de la ciudadanía.

Bajo este supuesto, y a partir de ahora, FormacionL se compromete directamente, con el cumplimiento de una Ley orgánica, y con la ciudadanía en general; en la cooperación para la buena marcha de este proceso.

A continuación siguiente apartado vamos a describir el enfoque y método seguido en nuestro **PFC.**

1.3.- Enfoque y método seguido

Para llevar a cabo nuestro PFC y según los resultados obtenidos en la Auditoría Interna, se realizaran los cambios en los sistemas necesarios y se adoptarán una serie de medidas a fin de adaptar estos sistemas a la normativa vigente, logrando que la empresa cumpla con lo determinado en dicha normativa y garantice, tanto a su personal como a sus personas beneficiarias, la protección de la intimidad y de la información personal que se derive del tratamiento de sus datos personales.

El estudio a realizar es tanto de los datos de carácter personal de los alumnos asistentes a los cursos, como de los datos de carácter personal utilizados para el desarrollo interno de la actividad de la empresa, tales como la gestión de los recursos humanos, proveedores, contabilidad...

Para proceder, a la realización de una Auditoría se entrevista a personal tanto de la organización como a personas usuarias, administradores y personal involucrado; también se analizaran los servidores, equipos de trabajos, redes de comunicaciones, procedimientos, documentación y conocimiento del personal de las políticas de la empresa.

Una relación de algunos elementos analizados son:

- **Seguridad física**

Se verificaran si Cumple las condiciones de seguridad mínima, control de acceso de personas autorizadas, zona restringida, elementos contra incendios, difícil causa de inundación,

- **Estructura informática**

Se verificara si los equipos no están accesibles y se entra con usuario y contraseña, aunque se deben tomar medidas de cambios de contraseñas

En el siguiente apartado vamos a tratar la planificación del trabajo de este **PFC.**

1.4.- Planificación del Trabajo

Para el desarrollo correcto para la realización un **PFC** y para que este concluya a tiempo y con el resultado deseado, es necesario conocer:

- Los requisitos necesarios
- Las tareas a realizar
- La realización de una planificación de las tareas

a) **Los requisitos necesarios** para la realización del PFC son:

Software

- Windows 8, Windows 10 (instalados en 2 equipos diferentes).
- Paquete de Microsoft Office:
  - Word
  - Power Point
  - Project
- Acrobat Reader, Profesional

Hardware:

- PC stándard
- PC portátil Standard
- Ipad

URL:

- UOC http:\\www.uoc.edu
- GoogleDocs https://docs.google.com/?tab=mo&authuser=0&pli=1#home
- Correo electrónico www.uoc.edu
- Buscador Google www.google.es
- Agencia española de Protección de datos www.aepd.es
- Todas las referenciadas a la Bibliografía.

Planificación

En este apartado se va a realizar una descripción de las tareas y actividades en que se va a dividir el Proyecto. Este, debido a su complejidad, lo vamos a descomponer en diferentes fases que nos van a servir para seguir un orden y poder realizar entregas que nos permitan evaluar el desarrollo correcto del proyecto.
Estas fases pueden seguir una lógica normal, como es el conocimiento de las necesidades, y herramientas, análisis del trabajo a desarrollar, propuestas, desarrollo, implementación y documentación.

Para parte de la elaboración de la documentación del proyecto seguiremos las indicaciones dadas en el trabajo de "Navarro, A, 2008".

b) **Desglose de tareas del proyecto**

Las actividades y tareas a realizar son:

i. Realización del plan del proyecto

a) *Lectura y compresión de la propuesta del proyecto, entregada por el consultor*
b) *Descarga y primera lectura del material puesto a disposición para la realización del Proyecto, para poder definir el plan de trabajo*
c) *Descripción y planificación de las tareas e hitos*
d) *Entrega del Plan de Trabajo con las revisiones realizadas*

ii. LOPD- Conocer la normativa LOPD

a) *Descarga y lectura de La Ley Orgánica de 15/1999*
b) *Descarga y lectura del Real Decreto 1.720/2007*
c) *Búsqueda de otras leyes relacionadas con datos de carácter personal*

iii. Auditoría Interna

a) **Sistemas de Información FormacionL. Análisis e implantación:**

i) *Analizar Sistemas Información destinados a las personas usuarias de la empresa*

ii) *Analizar Sistemas Información destinados a las personas trabajadoras de la empresa*

iii) *Implantación de medidas, procedimientos... para resolver la problemática encontrada*

iv. **Prueba de Evaluación continua 2. PEC2**

a) *Revisión de la planificación actual*

b) *Búsqueda de documentación continua según las necesidades que van a ir apareciendo*

c) *Entrega de la PEC2 con las revisiones recibidas*

v. Realización del Plan de Seguridad

a) *Documento de Seguridad*

i) *Realización del Documento de Seguridad*

ii) *Implantación del Documento de Seguridad*

b) *Implantación de las medidas, procedimientos, cláusulas a incluir... para el cumplimiento de la LOPD*

vi. Prueba de Evaluación continua 3. PEC3

a) *Revisión de la planificación actual*

b) *Búsqueda de documentación continua* según las necesidades que van a ir apareciendo

c) *Entrega PEC3 con las revisiones recibidas*

vii. Memoria

a) *Redactar un borrador de la memoria*

b) *Redactar las conclusiones del Proyecto*

c) *Revisión semántica, sintáctica y ortográfica de la memoria*

d) *Realizar el borrador de la Memoria:* escoger los contenidos para la realización de la presentación y realización del borrador con la Revisión de los tiempos, contenidos y forma de la presentación
e) *Realización de la presentación*
f) *Entrega de la memoria* y de la presentación con las revisiones realizadas

c) Cronograma y Diagrama de Gantt

Los hitos a considerar en el proyecto son las entregas parciales, así como el comienzo de estas entregas.

En nuestro caso nos encontramos con los siguientes hitos mostrados en la Tabla 1 "Calendarización de los hitos", estos vienen definidos por el plan de trabajo de la asignatura:

Hito	Fecha
Enunciado Plan de Trabajo	25/02/2017
Inicio Plan de Trabajo	25/02/2017
Entrega Plan de Trabajo	10/03/2017
Inicio PEC 2	11/03/2017
Entrega PEC2	14/04/2017
Inicio PEC 3	15/04/2017
Entrega PEC3	19/05/2017
Inicio Memoria	20/05/2017
Entrega Memoria	07/06/2017

Tabla 1.- Calendarización de los hitos

Para la planificación del proyecto hay que realizar un calendario de trabajo realista según las horas que se va a dedicar el proyecto analizando el resto de tareas realizadas a diario.

Se va a realizar una planificación de horas diarias según el día de la semana:

- **Laborables**: 3 horas diarias, 3 días a la semana.
- **Festivos**: 8 horas, un día a la semana.

Según esta planificación horaria, el número de horas que se va a dedicar a cada entregable está reflejada la tabla 2, Total Horas de dedicación al proyecto:

Tarea	Nº Horas
Plan de trabajo	31
PEC2	68
PEC3	85
Memoria	62
Debate Virtual	34
TOTAL	**280**

Tabla 2.- Total Horas de dedicación al proyecto

La planificación la vamos a reflejar con diagrama de Gantt, el cual se le va a realizar un seguimiento y modificación según el desarrollo del PFC.

El diagrama de Gantt a nivel global según las entregas es el mostrado en el Diagrama 1 ·" Diagrama de Gantt global del proyecto":

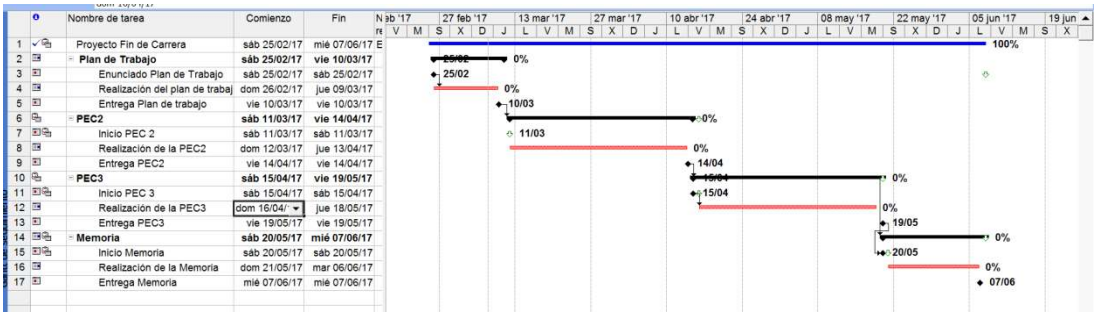

Diagrama 1.- Diagrama de Gantt global del proyecto

Si realizamos el diagrama Gantt del Proyecto, según las tareas y actividades enumeradas anteriormente de una forma estimada tenemos el siguiente Diagrama de Gantt "Diagrama 2.- Diagrama de Gantt detallado del proyecto

	Nombre de tarea	Comienzo	Fin	Fin real
1	Proyecto Fin de Carrera	sáb 25/02/17	vie 29/06/18	vie 29/06/18
2	**Plan de trabajo**	**sáb 25/02/17**	**vie 10/03/17**	**NA**
3	Inicio Plan de Trabajo	sáb 25/02/17	sáb 25/02/17	NA
4	Lectura y compresión de la propuesta del proyecto	sáb 25/02/17	mar 28/02/17	mar 28/02/17
5	Descarga y primera lectura del material	mar 28/02/17	jue 02/03/17	NA
6	Descripción y planificación de las tareas e hitos	lun 27/02/17	jue 09/03/17	NA
7	Entrega Plan de trabajo	vie 10/03/17	vie 10/03/17	NA
8	**Prueba de Evaluación Continua PEC2**	**sáb 11/03/17**	**vie 14/04/17**	**NA**
9	Inicio PEC 2	sáb 11/03/17	sáb 11/03/17	NA
10	Revisión de la planificación actual	sáb 11/03/17	jue 13/04/17	NA
11	Búsqueda de documentación continua	sáb 11/03/17	jue 13/04/17	NA
12	LOPD - Conocer la normativa LOPD	mié 22/03/17	lun 27/03/17	NA
13	Auditoría interna	mar 28/03/17	jue 13/04/17	NA
14	Entrega PEC2	vie 14/04/17	vie 14/04/17	NA
15	**Prueba de Evaluación Continua PEC3**	**sáb 15/04/17**	**vie 19/05/17**	**NA**
16	Inicio PEC 3	sáb 15/04/17	sáb 15/04/17	NA
17	Revisión de la planificación actual	sáb 15/04/17	jue 18/05/17	NA
18	Búsqueda de documentación continua	sáb 15/04/17	jue 18/05/17	NA
19	**Realización del Plan de Seguridad**	**sáb 15/04/17**	**mié 10/05/17**	**NA**
20	Doumento de Seguridad	sáb 15/04/17	jue 27/04/17	NA
21	Implantación de medidas, procedimientos, clausulas..	vie 28/04/17	mié 10/05/17	NA
22	Entrega PEC3	vie 19/05/17	vie 19/05/17	NA
23	**Memoria Proyecto Fin de Carrera**	**sáb 20/05/17**	**mié 07/06/17**	**NA**
24	Inicio Memoria	sáb 20/05/17	sáb 20/05/17	NA
25	Redactar un borrador de la memoria	sáb 20/05/17	dom 28/05/17	NA
26	Redactar las conclusiones del Proyecto	lun 29/05/17	jue 01/06/17	NA
27	Realización de la presentación.	mié 31/05/17	dom 04/06/17	NA
28	Entrega Memoria	mié 07/06/17	mié 07/06/17	NA

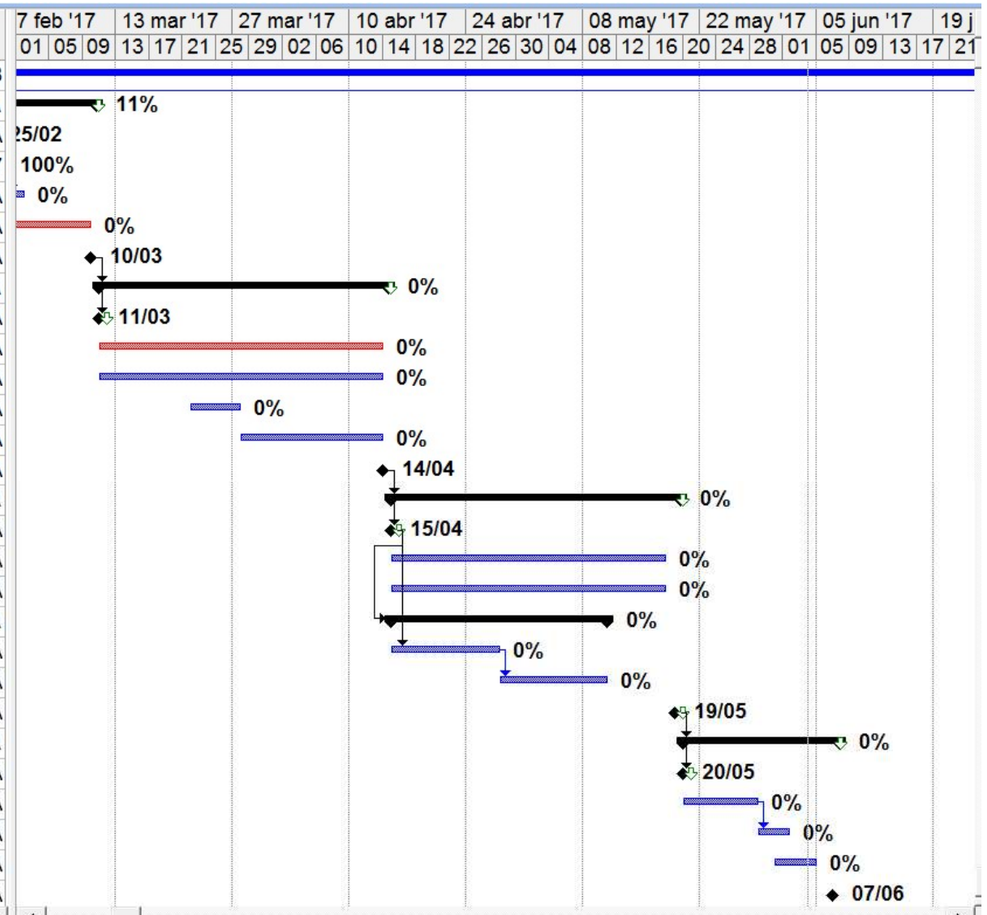

Diagrama 2.- Diagrama de Gantt detallado del proyecto

A continuación se vamos a realizar un Breve Sumario de los Productos obtenidos en la realización de nuestro PFC.

1.5.- Breve sumario de productos obtenidos .....

A continuación vamos a realizar una pequeña descripción de los productos obtenidos como resultado del desarrollo de este PFC, algunos de estos productos serán marcados por ley y otros de uso práctico para el personal de FormaciónL.

Los resultados del PFC se resumen en la siguiente lista de entregables:

1. **Informe de ficheros**, son la relación de ficheros que contienes datos de carácter personal en la empresa, deben estar registrados obligatoriamente en la AEPD (en sus correspondientes formularios) y según el nivel de protección hay que seguir una serie de medidas en el uso de ellos. Incluido en el Anexo II.
2. **Artículos y Acciones descriptivos de Ficheros:** Relación de los artículos de la LODP y su referencia a los ficheros, incluido en el anexo III
3. **Manual de Aplicación Legal LOPD/RD**, Documento recopilatorio de la adaptación de la ley en los trabajos de la Empresa. Manual de referencia para el conocimiento del cumplimiento de la LOPD adaptado a la actividad desarrollada por FormacionL. Incluido en el Anexo IV:
4. **Documento de Seguridad**, en este caso es un documento obligatorio por ley que todas las empresas que trabajen con datos de carácter personal deben cumplir y por lo tanto todo el personal de la empresa debe conocer y adaptar a su trabajo diario. Incluido en el Anexo V.

En el siguiente apartado se realiza una descripción de los otros capítulos que componen la memoria del PFC.

1.6.- Breve descripción de los otros capítulos de la memoria

En este apartado se va a realizar una breve explicación de los contenidos restantes en la memoria del PFC, y su relación con el PFC en su globalidad.

Estos capítulos son los siguientes:

- **Legislación sobre protección de datos de carácter personal. LOPD.**

El objetivo principal de este PFC es que la empresa FormacionL cumpla la normativa LOPD para el buen desarrollo de su actividad.

Para ello este capítulo vamos a proceder a contextualizar la LOPD, antecedentes, normativa actual…, en todo lo referente a la actividad de nuestra empresa

- **FormacionL**

Para desarrollar este PFC se necesita conocer la actividad, estructura, centros,.. y todo lo relevante a la empresa FormacionL para poder realizar la Auditoría y su posterior Plan de Seguridad

  - Actividad

    En este apartado vamos a centrarnos en la actividad de FormacionL, centrándonos en los concerniente a la LOPD

  - Sedes de la empresa

    En este apartado se dará un mapa de los centros físicos pertenecientes a la empresa, la actividad que se realiza y todo lo concerniente a Seguridad Física e Informática de estos centros.

  - Personal

    En este apartado se describe el personal que compone la empresa y la estructura que de estos, organigrama y responsables de LOPD

  - Sistemas de Información

    Se va a realizar un mapa de los Sistemas de Información de la empresa de cara a realizar su actividad interna y dar servicio a las personas usuarias, en cuanto a lo concerniente a la LOPD.

- **Auditoría interna**

Vamos a realizar la una Auditoría Interna de Seguridad de FormacionL, de cara al conocimiento del tratamiento de datos de carácter personal por los

trabajadores de FormacionL y poder realizar con posterioridad el Plan de Seguridad.

- **Plan de Seguridad**

Una vez realizada la Auditoría Interna se realizará el Plan de Seguridad de FormacionL para que esta cumpla en la medida de lo posible la LOPD

  - Introducción: Descripción de lo relacionado con el Plan de Seguridad de FormacionL
  - Documento de Seguridad: Documento legal de obligado cumplimiento e implantación en todas las empresas que tratan datos de carácter personal.

- **Conclusiones**

En este capítulo se va a describir las conclusiones a las que se ha llegado en este PFC, al realizar la Auditoría y el Plan de Seguridad y sobre todo en qué medida se puede llegar a cumplir con la LOPD, en qué plazos, qué se ha aprendido al realizar el PFC, en qué estado la empresa estaba realizando su actividad en cuanto a cumplimiento LOPD, en qué grado hemos cumplido los objetivos inicialmente propuestos, el por qué no se ha conseguido en este caso, en qué líneas futuras se puede trabajar para una optimización de tareas, procedimientos,....

- **Glosario**

En este capítulo se recoge un listado con Definición de los términos y acrónimos más relevantes utilizados dentro de la Memoria.

- **Bibliografía**

En este capítulo se recoge una lista numerada de las referencias bibliográficas utilizadas dentro de la memoria.

- **Anexos**

En este capítulo se detalla un listado de apartados que son demasiado extensos para incluir dentro de la memoria y tienen un carácter autocontenido (por ejemplo, manuales de usuario, manuales de instalación, etc.)

En el siguiente capítulo vamos a realizar el resto de tareas a realizar en nuestro PFC.

2.- Resto de capítulos

Vamos a realizar las tareas propias de este PFC.

2.1.- Legislación sobre protección de datos de carácter personal. LOPD

Para la realización de este PFC, es necesario un conocimiento profundo de la **LOPD** y del uso que se hacen de los datos de carácter personal de las personas usuarias de dicha empresa y de otros de carácter personal para el funcionamiento interno de la empresa.

La AEPD es la responsable de las indicaciones legales a seguir, por lo que vamos a justificar de forma legal la realización de este PFC, con las siguientes referencias legales:

- La Ley Orgánica de 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal es una ley aún desconocida, a pesar de llevar en vigor ya 18 años, motivado principalmente por la inexistencia de un reglamento en que desarrollara dicha Ley.
- En 2008 entró en vigor el Real Decreto 1.720/2007, de 21 de diciembre, que desarrolla la Ley de Protección de Datos de Carácter Personal (RLOPD). Este reglamento ha venido a interpretar la literatura de dicha Ley, de forma que ha moldeado toda la casuística que contempla y marca los principios y medidas a implementar para cumplir con dicha normativa. A partir de este momento, las organizaciones han de poner énfasis en el cumplimiento de la LOPD como garantía de protección de los datos tanto de forma interna, como de cara a las personas usuarias de la organización.

El tratamiento, recogida, almacenamiento de datos de carácter personal en una Organización está amparado por la anterior normativa legal

Este marco normativo abarca mucho más de la mera protección de la intimidad del individuo, tal como marca el artículo 18 de la Constitución Española, si no que añade un nuevo derecho de la ciudadanía para poder controlar qué pasa con su información. Es el llamado derecho a la autodeterminación informativa, distinto e independiente al derecho de la intimidad y de la propia imagen.

Es el derecho fundamental que tienen todos los ciudadanos a que sus datos personales no sean utilizados por parte de terceros sin la autorización debida. Se trata de evitar que, a través de un tratamiento automatizado o manual, se pueda llegar a confeccionar información identificable con la persona titular de los datos que pueda afectar a su intimidad, a su entorno social o profesional.

Es un **derecho fundamental** consistente en el **ejercicio de control** por parte del titular de los datos sobre **quién, cómo, para qué, dónde y cuándo** son tratados los datos relativos a su persona.

“Una persona educada en seguridad es la base de cualquier entorno fiable en la seguridad de la información.

Sin una adecuada educación se convierte en el eslabón más débil, que rompe cualquier política de seguridad.”

En el siguiente Diagrama 3 “Principios LOPD” se reflejan los 7 principios de la LOPD,

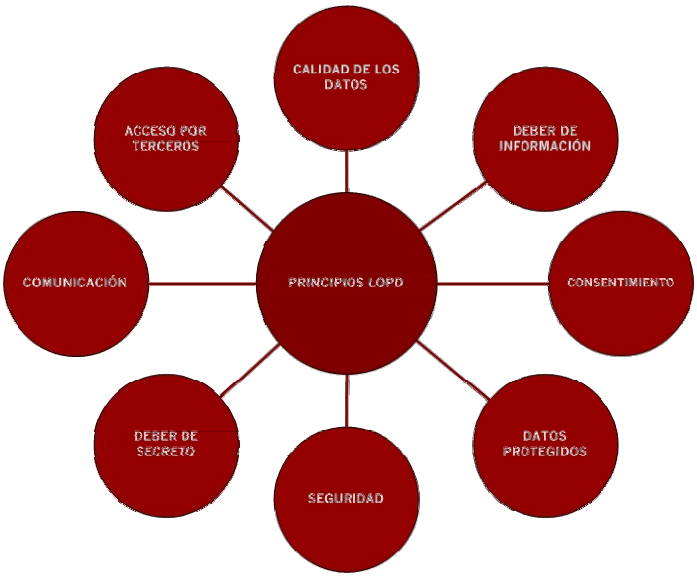

Diagrama 3. Principios LOPD

La Constitución Española, en su artículo 18 garantiza el derecho al honor, la intimidad personal y familiar y a la propia imagen. En particular, en su apartado cuarto, establece la necesidad de proteger estos derechos fundamentales, dentro del ámbito relacionado con el uso de la informática. De esta manera, el artículo 18.4 de nuestra Constitución dispone:

"La Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos".

Como consecuencia de este mandato y para desarrollar el contenido del mismo, se promulgó la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de Datos de Carácter Personal, más conocida como LORTAD.

En el ámbito europeo, el rápido desarrollo de las técnicas de tratamiento informático fue, igualmente, motivo de preocupación en los Organismos de ámbito internacional. Reflejo de esta preocupación, representa la publicación del Convenio 108 (28/01/1981) del Consejo de Europa, que tenía como objetivo garantizar el respeto de los derechos y libertades fundamentales del individuo, concretamente su derecho a la vida privada con respecto al tratamiento automatizado de los datos de carácter personal. España ratificó este Convenio el 27 de Enero de 1984.

Posteriormente, se promulgó en el marco de la Unión Europea, la Directiva 95/46/CEE relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, que tenía como objetivo armonizar la legislación de los países miembros de la Unión en materia de protección de datos, garantizando, de esta manera, la protección y el

respeto en todos los países de la Unión de este derecho fundamental del individuo, también conocido como “autodeterminación informativa”. Para ello, el Parlamento Europeo elaboró la mencionada Directiva, en la que se recogen los principios mínimos de protección que todos los países de la Unión Europea deberían garantizar en su legislación nacional interna.

En cumplimiento de esta Directiva, España promulgó la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante, **LOPD**), que supone la transposición de la Directiva 95/46/CE al derecho interno de nuestro país. La regulación contenida en la LOPD se complementaba hasta hace poco, con el Reglamento de Medidas de Seguridad, aprobado por Real Decreto 994/1999, de 11 de junio.

Actualmente, la norma reglamentaria que desarrolla la LOPD es el RD 1.720/2007 de 21 de diciembre, por el que se aprueba el Reglamento de Desarrollo de la LOPD, (en adelante **RLOPD**) en cuya Disposición Derogatoria deja sin efecto el RD 994/1999, de 11 de junio, (RMS) y el RD 1332/1994, de 20 de junio.

Resulta trascendente la toma de conciencia de todas las personas con acceso a los datos, dada la responsabilidad que conlleva el tratamiento de los mismos. El Responsable del fichero tiene la obligación de implementar y verificar las normas de seguridad, así como adoptar las medidas necesarias e implementar los procedimientos precisos para que tanto la normativa, como las consecuencias en caso de incumplimiento, sean conocidas por el personal afectado.

Para centrarnos, a modo de introducción, en la trascendencia de lo que conlleva el respeto a los principios establecidos por la Ley, tendremos en cuenta que ya el Tribunal Constitucional en su sentencia 292/2000, vino a reconocer la protección de datos de carácter personal como un derecho constitucionalmente autónomo e independiente a la intimidad, siguiendo así la línea de lo previsto en la Carta de Derechos Fundamentales de la Unión Europea, firmada en Niza el 7 de diciembre de 2000, cuyo artículo 8 establece que toda persona tiene derecho a la protección de datos de carácter personal que la conciernen.

Así, el derecho fundamental a la protección de los datos personales presenta ya unos perfiles definidos por la jurisprudencia constitucional:

a) Su objeto va más allá de los datos íntimos, lo que significa que comprende en el ámbito protector del derecho fundamental los datos personales públicos, y en general a todos los que identifiquen o permitan la identificación de una persona.

   En este sentido, El objeto de protección del derecho fundamental a la protección de datos no se reduce sólo a los datos íntimos de la persona, sino a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales, porque su objeto no es sólo la intimidad individual (protegida por el artículo 18.1 CE), sino los datos de carácter personal. Asimismo, también alcanza a aquellos datos personales públicos (son accesibles al conocimiento de cualquiera).

   Que los datos sean de carácter personal no significa que sólo tengan protección los relativos a la vida privada o íntima de la persona, sino que los datos amparados por este derecho son todos aquellos que identifiquen o permitan la identificación de la persona.

b) El objeto del nuevo derecho fundamental no se limita a los datos personales procesados o almacenados por sistemas informáticos, sino también a cualesquiera otros datos personales.

c) El ejercicio del derecho comporta un conjunto de facultades positivas relativas a la disposición y de control sobre los datos personales. Éstas no se limitan tampoco a garantizar la protección de la intimidad, pues aunque ambos derechos fundamentales –el derecho a la intimidad y el derecho a la protección de los datos personales- persiguen un objetivo común, su función, su objeto y su contenido son diferentes.

d) Estas facultades de disposición y control de los datos se concretan en el derecho a consentir y a conocer su posesión y su uso por parte de terceros (es un derecho fundamental **consistente en el ejercicio de control por parte del titular de los datos sobre quién, cómo, para qué, dónde y cuándo son tratados los datos relativos a su persona**). Este control y

poder de disposición se hace efectivo a su vez a través del ejercicio de los derechos de acceso, rectificación, cancelación y oposición.

Los principios generales de la protección de datos constituyen el eje fundamental de la normativa. Partiendo de ellos, se desarrolla el resto de la regulación de obligado cumplimiento para todo aquél que trate datos de carácter personal y los correspondientes derechos otorgados a la persona titular de los mismos. En consecuencia, cualquier incumplimiento de estos principios o la falta de observancia de los mismos, supondrá la comisión de una infracción y la consiguiente sanción por parte de la Agencia Española de Protección de Datos.

En esta Ley se configura la Agencia Española de Protección de Datos como ente con personalidad jurídica propia y plena capacidad pública y privada, destinado a velar por el cumplimiento de la legislación sobre protección de datos.

Las infracciones en materia de protección de datos aparecen tipificadas en el artículo 44 de la Ley. Se establece una clasificación en infracciones leves, infracciones graves e infracciones muy graves, tipificándose multas que ascienden hasta los 601.000 €, tal como se representa en la Tabla 3"*Infracciones (art 44 LOPD)*.

Infracciones (art. 44 LOPD)		Sanciones (art. 45 LOPD)
Infracción Leve	.....	**de 601,01 a 60.101,21 €**
Infracción Grave	.....	**de 60.101,21 a 300.506,05 €**
Infracción Muy Grave	.....	**de 300.506,05 a 601.012,10 €**

Tabla 3.- Infracciones (art 44 LOPD)

Tal y como se ha referenciado, la AEPD es el órgano estatal encargado de velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación. Tiene potestad de inspección pudiendo recabar cuantas informaciones precise para el cumplimiento de sus cometidos.

De esta forma, la AEPD podrá solicitar la exhibición o el envío de documentos y datos, así como la inspección de los equipos físicos y lógicos utilizados para el tratamiento de los datos, accediendo a los locales donde se hallen instalados. También podrá requerir a los responsables y los encargados de los tratamientos la adopción de las medidas necesarias para la adecuación del tratamiento a las

exigencias de la Ley y ordenar, en su caso, la cesación de dichos tratamientos y la cancelación de los ficheros, que vemos en la Tabla 4 "*Infracciones Art. 44.2,44,3 y 44,4 LOPD*".

INFRACCIÓN	*Art. 44.2. Son infracciones leves:* *b) No proporcionar la información que solicite la Agencia Española de Protección de Datos en el ejercicio de las competencias que tiene legalmente atribuidas, en relación con aspectos no sustantivos de la protección de datos.*
SANCIÓN	*Art. 45.1: Multa de 601,01 a 60.101,21 €*
INFRACCIÓN	*Art. 44.3. Son infracciones graves:* *i) No remitir a la Agencia Española de Protección de Datos las notificaciones previstas en esta Ley o en sus disposiciones de desarrollo, así como no proporcionar en plazo a la misma cuantos documentos e informaciones deba recibir o sean requeridos por aquél a tales efectos.* *j) La obstrucción al ejercicio de la función inspectora.*
SANCIÓN	*Art. 45.2: Multa de 60.101,21 a 300.506,05 €*
INFRACCIÓN	*Art. 44.4. Son infracciones muy graves:* *d) No cesar en el uso ilegítimo de los tratamientos de datos de carácter personal cuando sea requerido para ello por el Director de la Agencia Española de Protección de Datos o por las personas titulares del derecho de acceso.*
SANCIÓN	*Art.45.3: Multa de 300.506,05 € a 601.012,10 €*

Tabla 4.- "Infracciones Art. 44.2,44,3 y 44,4 LOPD"

En el ámbito empresarial, la primera acción que ha de llevar a cabo una organización que se proponga la implantación de la política de protección de datos, es la determinación del grado de involucración que quiere asumir la empresa o entidad respecto del hecho de asegurar la información como valor, como el activo más importante de la empresa.

Así, las políticas de protección de datos de las empresas, fundaciones, asociaciones, no tienen por qué ser idénticas entre sí, sino que van a depender muy mucho de las necesidades que se planteen y del marco en el que se pretendan encuadrar, pudiendo abordar o no, una política integral de protección de toda la

información almacenada por la empresa, independientemente de que esta contenga o no datos de carácter personal.

A continuación tenemos una relación de diversos artículos que determinan todo esto en la ley:

- **Art. 3. a) de la Ley Orgánica 15/1999 de la LOPD:**

… cualquier información que concierne a personas físicas, identificadas e identificables".

Dicho concepto abarca toda información numérica, alfabética, gráfica, acústica o de cualquier otro tipo, susceptible de recogida, registro, tratamiento o transmisión concerniente a una persona física identificada o identificable.

- **El art. 2.1 de la LOPD establece que**

"*La ley será de aplicación a los datos de carácter personal* **registrados en soporte físico** *que los haga susceptible de* **tratamiento**, *y a toda modalidad de* **uso posterior** *de estos datos por los sectores público y privado".*

- **Artículo 4 LOPD.**

1.- Solo se podrán recoger datos adecuados, pertinentes y no excesivos para la finalidad establecida.

2.- No podrán usarse para finalidades incompatibles para la que fueron recogidos.

3.- Los datos serán exactos y puestos al día.

4.- Serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad establecida.

- **El artículo 5 de la LOPD nos obliga a informar al interesado/a o parte solicitante de:**
    - la existencia de un **fichero**.
    - la **finalidad** de la recogida de los datos.
    - los **destinatarios** de la información.
    - la **identidad y dirección** del responsable del tratamiento.
    - la posibilidad de ejercitar los **derechos de acceso, oposición,**
    - **rectificación y cancelación de los datos**.

Esta actividad de información, se ha se hacer de **forma expresa, precisa e inequívoca.**

- **Artículo 10 LOPD**

"El responsable del fichero y quienes intervengan en **cualquier fase del tratamiento** de los datos de carácter personal están obligados al **secreto profesional** respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun **después de finalizar sus relaciones** con el titular del fichero o, en su caso, con el responsable del mismo."

CLÁUSULA O COMPROMISO DE CONFIDENCIALIDAD CON LAS PERSONAS EMPLEADAS

- **Artículo 11 LOPD.**

para el cumplimiento de **fines directamente relacionados con las funciones** legítimas del cedente y del cesionario con el previo **CONSENTIMIENTO del interesado**

… CONSENTIMIENTO EXPRESO

- **Artículo 12 LOPD.**

¿Se pueden ceder datos a un tercero?

La respuesta es SÍ, cuando el acceso de un tercero a los datos sea necesario para prestar un servicio al responsable del fichero

Esta relación deberá estar regulada en un **CONTRATO** que deberá constar **por escrito** o en alguna otra forma acreditada donde se detallen **los deberes y obligaciones** de las dos partes en cuanto a la protección de datos

- Procedimientos de tutela de Derechos
    - Procedimiento de **acceso.**
    - Procedimiento de **oposición.**
    - Procedimiento de **rectificación.**
    - Procedimiento de **cancelación.**
- **Art. 9 LOPD**

"El responsable del fichero, y, en su caso, el encargado del tratamiento deberán adoptar las medidas de índole técnico y organizativas necesarias que garanticen la

seguridad de los datos [...] habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos,[...].”

OBJETIVOS:

Garantizar la seguridad de los datos, es decir los siguientes aspectos:

- Confidencialidad
- Disponibilidad
- Integridad
- Mantener el nivel de seguridad alcanzado
- Mantenimiento de los sistemas y los procedimientos asociados.

En el Anexo IV: Documento de Aplicación Legal LOPD FormacionL y en el Anexo V: Documento de Seguridad se tratan ampliamente los artículos LOPD relacionados con el tratamiento de datos por la empresa y su aplicación en dicha actividad.

Y lo más importante para la Organización, que es el cambio cultural, concienciación por parte del persona que todos los Datos de Carácter Personal de las Personas Beneficiaria o Recursos Humanos de la Empresa, son datos protegidos por unas leyes y que no consiste en dejar de trabajar con ellos, hay que seguir unas medidas de seguridad y un control diferente.

En el siguiente apartado se describe la Empresa FormacionL

2.2.- FormacionL

La estructura organizativa y de gestión de FormacionL, a través de la cual se produce la actividad de la gestión de la información comao activo propio es la siguiente:

2.2.1.- Actividad

FormacionL, es una empresa dedicada a las acciones de formación, elaboración de material didáctico y organización de encuentros, seminarios y jornadas

adaptadas a los requerimientos y necesidades de las entidades con las que colabora.
Es una organización capaz de impulsar y dinamizar el tejido productivo, mediante la cualificación profesional de los recursos humanos, el desarrollo de programas de fomento del empleo y de asistencia técnica a entidades públicas y privadas.

Los dos actores que interactúan en la actividad de la empresa FormacionL de la que objeto este PFC es:

- la actividad de la empresa que presta los servicios
- y los ciudadanos que la intervienen, a los que vamos a llamar como usuarios, beneficiarios y que son alumnos en su mayoría.

El **PFC** va a analizar, resolver e implantar la problemática del uso de los **datos de carácter personal** en una empresa dedicada a la realización de cursos de formación para la ciudadanía, ya sean de ámbito privado como cursos provenientes del ámbito público..

Toda la recogida de datos e información viene motivada por el cumplimiento de los fines empresariales. En FormacionL, entre sus fines, según figura en los Estatutos, se encuentran los siguientes:

- Ser un instrumento para el fomento de la formación y el empleo,
- Ofrecer una oferta formativa especializada en Formación Profesional
- La cooperación con las autoridades e instituciones locales, provinciales, autonómicas y nacionales

Nuestra empresa ofrece a instituciones y empresas públicas y privadas, acciones en todos los campos vinculados al empleo y la formación, sobre el principio de diseñar y producir servicios a medida, adaptados a los requisitos y las necesidades actuales.

En relación directa con estos fines, los servicios que presta a los distintos sectores y a la actividad que despliega en todo el territorio andaluz, **FormacionL** tiene necesidad de recoger y tratar una gran cantidad datos de carácter personal.

Como organización tiene ya implantadas y certificadas las normas ISO 9001:2000 y la ISO 14001:2004, con el alcance: "*Diseño, gestión e impartición y evaluación de acciones de formación continua y ocupacional", la de Responsabilidad Social 8000:2001* .

Los datos a estudiar van a ser tanto de los datos de carácter personal de los usuarios de los diferentes proyectos y de los alumnos asistentes a los cursos, como de los datos de carácter personal utilizados para el desarrollo interno de la actividad de la empresa, tales como la gestión de los recursos humanos, proveedores, contabilidad...

La información es uno de los activos más importantes de toda organización, requiere junto a los procesos y sistemas que la manejan, ser protegidos convenientemente frente a amenazas que puedan poner en peligro la continuidad de los niveles de competitividad, rentabilidad y conformidad legal necesarios para alcanzar los objetivos de la organización.

Actualmente resulta posible disminuir de forma significativa el impacto de los riesgos sin necesidad de realizar grandes inversiones en software y sin contar con una gran estructura de personal. Para ello se hace necesario conocer y afrontar de manera ordenada los riesgos a los que está sometida la información, y a través de la participación activa de toda la organización, contemplar unos procedimientos adecuados y planificar e implantar controles de seguridad basados en una evaluación de riesgos y en una medición de la eficacia de los mismos.

La estructura de la empresa es la siguiente:

- Dirección General Técnica: sólo está formada por el Director General Técnico y su equipo, y es el órgano de decisión
- Dirección de Organización: Dirección que se dedica a la organización interna y de comunicación con el exterior. Entre sus tareas:
    - Aparición en medios de comunicación

    - Asesoramiento en eventos, y a través de la Intranet se informa de que se quiere realizar en cada momento.
- Dirección de Sistemas: Dirección de Informática y de Sistemas de Información
- Dirección Económica: Dirección que se dedica al gestión económica de la empresa. Entre sus funciones se encuentran:
    - Gestión de pago de nóminas a los trabajadores.
    - Justificación de gastos.
- Dirección de Recursos Humanos: es la dirección que se ocupa del personal de la organización. Entre las funciones se encuentran:
    - La administración de personal.
    - Desarrollo del personal (planes de carrera)
    - Servicio de prevención propio
- Dirección de Actividad: Dirección que se ocupa de la gestión, contratación de la actividad con el cliente
- Dirección de Desarrollo Territorial: Dirección encargada de desarrollar la actividad de formación y empleo en el territorio, y que posteriormente ejecutan las Gerencias Provinciales.
- Gerencias: existe una en cada territorio, provincia andaluza. Se dedica a ejecutar la actividad, cursos, programas de empleo y a la relación con el beneficiario (alumno, usuario, ..)
- Centros especializados: en cada provincia según las características de esta y las necesidades del momento se pueden crear centros especializados en algún sector de formación. Por ejemplo:
    - Jaen: madera
    - Sevilla: aeronaútica

En general, la Información y por añadidura los datos de carácter personal en la Dirección General Técnica, se recogen tanto desde la distintas Direcciones, como desde las distintas Gerencias.

La relación de Ficheros (y el detalle de los datos que pueden contener) de responsabilidad por cada Dirección y relacionados en el Anexo II son:

1.- Ficheros responsables de la Dirección de Desarrollo Territorial

- **Usuarias Autorientación**: Personas atendidas para su inserción en los recursos de empleo y formación curricular. Su formato de almacenamiento es una BD y cuestionarios en papel
- **Usuarias**: para el alumnado y otros usuarios de proyectos diferentes. Pero los datos recogidos y el fin es el mismo por lo que sólo creamos un solo fichero. Su formato de almacenamiento es una BD, cuestionarios en papel, listado de asistentes, cuestionarios de satisfacción, registro en web ..

2.- Ficheros responsables de la Dirección de Recursos Humanos

- **Recursos Humanos**: Fichero que recoge los datos del personal de la organización. Su formato de almacenamiento es la aplicación corporativa SAP, registro en LDAP para identificación en red corporativa, cuestionarios en papel, fotografía de eventos, jornadas..
- **Curriculos FormacionL**: Fichero que recoge los Curriculum de personas que desean trabajar en la empresa. Se recogen exclusivamente a través de la página web de un cuestionario en PDF que se guarda en la BD de la aplicación corporativa SAP.

3.-Ficheros responsables de la Dirección Económica

- **Clientes y Proveedores**: Ficheros que recogen la información de clientes y proveedores con los que trabaja FormacionL. Se almacenan en la aplicación corporativa Navision, y hojas de excell.
- **Contabilidad y Hacienda Pública**: Fichero que almacena la información legal de FormacionL. Se recoge en formato Bd en la aplicación corporativa Navision y se trabaja con parte de estos datos en aplicaciones ofimáticas.

4.-Ficheros responsables de la Dirección de Organización

- **Agenda Corporativa**: Fichero que almacena los contactos de FormacionL. Se recogen en la agenda de contactos de Microsoft Outlook.
- **Eventos:** Fichero que almacena los eventos que organiza FormacionL para trabajadores o clientes. Se almacena en BD.
- **Comunicación y Marketing:** Fichero que almacena la relación con los medios de comunicación y clientes. Se usa en formato BD,

2.2.2.- Sedes de la Empresa

Ahora bien, FormacionL tiene su sede social en Sevilla, donde se encuentra la Dirección General Técnica,(calle FormacionL 11, dirección ficticia) y un total de 21 Centros, entre propios y gestionados, repartidos por todo el territorio andaluz. De entre estos centros 8 son las sedes de las Gerencias Provinciales, situadas en cada una de las ocho capitales de provincia de la Comunidad Autónoma Andaluza Hemos de considerar por tanto que la gestión de la información se realiza desde todas estas sedes físicas de FormacionL.

Para el desarrollo de su actividad FormacionL, cuenta con una estructura de centros que le capacita para actuar sobre la realidad concreta y las peculiaridades de cada provincia de la Comunidad Autónoma Andaluza.
La Empresa, se divide en una Sede Central (a la que llamaremos Dirección General Técnica o DGT), ocho centros provinciales (a los que llamaremos Gerencias Provinciales) y centros especializados.

Los espacios reservados en los edificios para el almacenamiento de estos ficheros automatizados y no automatizados son:

- La sala de servidores central con todo el equipamiento se encuentra en la Dirección General Técnica, y cuenta con las siguientes características:
  Espacio aislado con control de acceso restringido por teclado, con log de accesos, aire acondicionado, protección contra incendios, alarma antiintrusión y todos los demás sistemas de seguridad exigidos

- Existe una sala de servidores de respaldo en la Gerencia de Málaga en la que se replican todos los servicios con sus copias e seguridad programadas.
- En el resto de centros existe una pequeña sala con un único servidor de ficheros en el que almacena la información centralizada del personal del centro.
- Igualmente existen unas salas de archivo, armarios y otros equipamientos para la protección de los ficheros en papel con datos de carácter personal.

Más tarde en el capítulo de la auditoría veremos si cumplen las medidas de seguridad necesarias para la protección de datos de carácter personal.

2.2.3- Personal

En el siguiente Diagrama 4 "Esquema de Responsabilidad del personal de FormacionL" vamos a representar las diferentes responsabilidades del personal de nuestra empresa en cuanto al cumplimiento de la LOPD

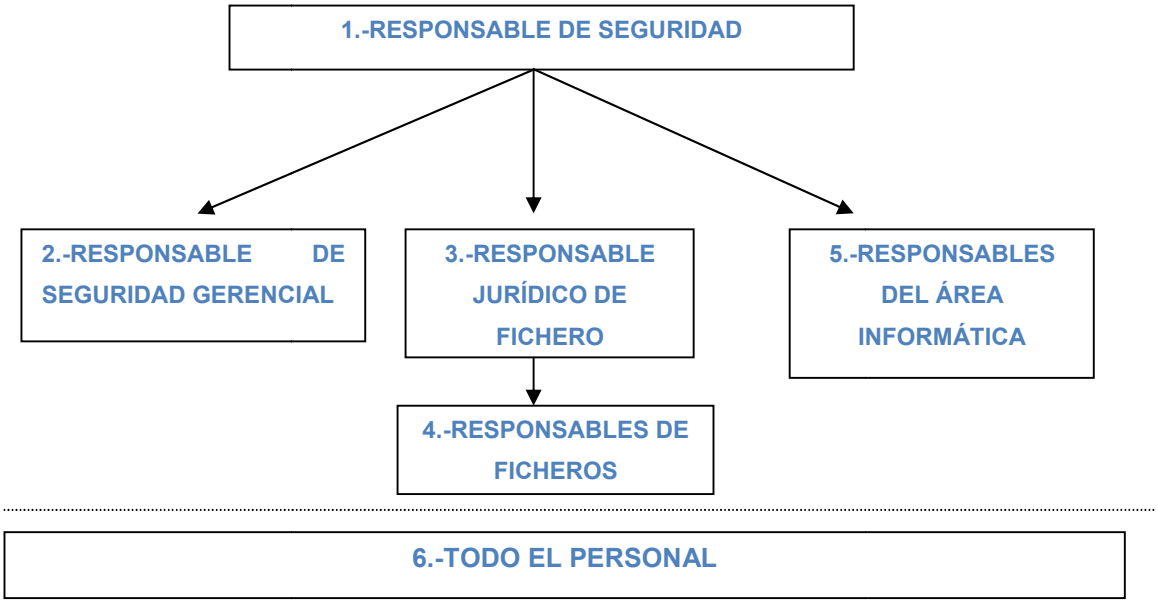

Diagrama 4.- Esquema de Responsabilidad del personal de FormacionL

Las funciones y obligaciones del personal de FormacionL vendrán recogidas en el Documento de Seguridad y son de obligado cumplimiento.

2.2.4.- Sistemas de Información

Vamos a hacer una descripción de los Sistemas de Información de FormacionL indicando en su caso si tratan o almacenan datos de carácter personal, para conocer su uso y así saber su importancia cuándo se haga referencia a ellos en el resto del PFC.

La mayor parte de la información reside en equipos informáticos, redes de datos y soportes de almacenamiento, encuadrados todos dentro de lo que se conoce como sistemas de información (a partir de ahora SI). Estos sistemas de información están sujetos a riesgos e inseguridades tanto desde dentro de la propia organización como desde fuera. A los **riesgos físicos** (accesos no autorizados a la información, catástrofes naturales – fuego, inundaciones, terremotos, vandalismo, etc.) hay que sumarle los **riesgos lógicos** (virus,ataques de denegación de servicio, etc.).
Los datos de carácter personal pueden estar en formato físico (papel) o en archivos electrónicos (bd, archivos ofimáticos, páginas web..). Vamos a realizar un inventario de los Sistemas de Información dónde se almacenan estos datos de carácter personal, para posteriormente en el capítulo de Auditoría comprobar si cumplen las medidas de seguridad necesarias dictadas por la AEPD y en el capítulo de Plan de Seguridad proponer las medidas oportunas en caso de ser necesarias.
La empresa dispone de los siguientes Sistemas de Información:

- **Intranet:** Es un escenario excelente para la intercomunicación de los sistemas y la principal herramienta de trabajo del personal. A través de su interfaz se accede a diferentes BD centralizadas y se gestionan estos datos. La puerta de entrada en un interfaz web al que se accede por identificación de usuarios LDAP y según los permisos del trabajador accederá a diferentes aplicaciones con diferentes acciones. Estos servicios y sus accesos a datos de carácter personal son:

- Registro de incidencias: Accede a datos de carácter personal
- Portal del personal: Accede a datos de carácter personal del fichero de Recursos Humanos y del fichero de CV de la ciudadanía.
- Seguimiento actividad: No accede a datos de carácter personal
- Noticias : Accede a datos de carácter personal del fichero de Eventos
- Foro: No accede a datos de carácter personal
- Correo electrónico web: Accede a datos del fichero de Agenda corporativa

- **Página web de FormacionL:** su dirección url (ficticia en el estudio del pfc) www.formacionL.pfc. Es la cara visible, para la publicidad, comunicación, intercomunicación de la empresa en Internet con sus clientes, proveedores y ciudadanía en general.

  Es una web en su mayoría informativa, pero a través de ella el ciudadano puede:

  - Introducir los curriculum vitae en la BD de SAP, para la Dirección de Recursos Humanos. Accede al fichero de CV.
  - Inscribirse en los cursos de formación y otras actividades. Accede al fichero de Usuarias.

- **SAP**: Aplicación corporativa ERP, que gestiona y almacena toda la información relativa al personal de la organización. Accede al fichero de Recursos Humanos y CV. Su funcionamiento es el siguiente:

  La BD está almacenada en los servidores centrales

  - El personal de Recursos Humanos trabaja con los datos a través de un cliente instalado en su PC, pero los datos son los almacenados en la BD central. Hay informes y datos que trabajan con ellos en aplicaciones ofimáticas
  - Todo el personal accede y gestiona sus datos tales como vacaciones, formación, nómina.. a través de la intranet que

accede a los datos de la BD central directamente, sin realizar ninguna copia.

- **Navision:** Aplicación corporativa ERP que accede a los datos económicos financieros de la empresa. Accede al fichero de clientes y Proveedores y de Contabilidad y Hacienda Pública.
- **Aplicaciones ofimáticas:** Estas aplicaciones Word, excell, Access.. se utilizan para el tratamiento de diferentes datos entre ellos los de carácter personal. Estos ficheros deben estar almacenados en los servidores centrales, en el servidor de fichero y en los PC de los trabajadores en el caso de ficheros temporales que deben ser eliminado al acabar su finalidad y tiene una duración limitada de tiempo.

El personal debe trabajar en los servidores de ficheros, su información debe ser almacenada en los servidores de fichero en la red de la Organización.

En el siguiente apartado veremos la Auditoría Interna realizada en FormacionL

2.3.- Auditoría Interna

Uno de los objetivo de este PFC es realizar una auditoría para cumplir lo determinado por ley y que por supuesto la información de nuestra empresa sea segura y eficiente.

La Empresa FormacionL al día de hoy no ha pasado ninguna auditoría, por lo que está incumpliendo la LOPD de la AEPD.

2.3.1.- Introducción

Respecto a las auditorías necesarias en materia de protección de datos de carácter personal, el 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 (en adelante RLOPD), es tajante en este aspecto. En su artículo 96.1 dice textualmente:

A partir del nivel medio los sistemas de información e instalaciones de tratamiento y almacenamiento de datos se someterán, al menos cada dos años, a una auditoría interna o externa que verifique el cumplimiento del presente título.

Por ello, y dado que la empresa cuenta con múltiples ficheros de nivel medio, será necesario realizar **una auditoría bienal**, en la que se revisen las medidas de índole técnico y organizativas recogidas en el documento de seguridad, los ficheros tratados, los sistemas de comunicaciones, centros de proceso de datos así como la relación de personas usuarias autorizadas, copias de seguridad y demás controles establecidos en el título VIII del RLOPD.

Nuestro PFC constituiría la primera fase de la auditoría. Es recomendable en posteriores fases del PFC completar las fases de la Auditoría, tal como marca el artículo 96.2, debe consistir en lo siguiente:

El *informe de auditoría deberá dictaminar sobre la adecuación de las medidas y controles a la Ley y su desarrollo reglamentario, identificar sus deficiencias y proponer las medidas correctoras o complementarias necesarias. Deberá, igualmente, incluir los datos, hechos y observaciones en que se basen los dictámenes alcanzados y las recomendaciones propuestas.*

Así, la auditoría **deberá ser reflejada en un informe**, que recoja los resultados de la misma, identificando las debilidades detectadas y las posibles recomendaciones para la mejora de las medidas..

Por último, el proceso de auditoría finaliza a través del responsable de seguridad global, que **elevará a los responsables de fichero y otras personas responsables de las medidas técnicas y organizativas las medidas**

correctoras necesarias, además de custodiar el informe a fin de que esté disponible para la Agencia de Protección de datos (AEPD) u otras autoridades. Así lo refleja el artículo 96.3 del RLOPD:

Los informes de auditoría (...) elevará las conclusiones (…) para que adopte las medidas correctoras adecuadas (…) quedarán a disposición de la Agencia Española de Protección de Datos o, en su caso, de las autoridades de control de las comunidades autónomas.

Según la LOPD se debe realizar:

- Una Auditoría regular ordinaria, al menos cada dos años
- Una Auditoría extraordinaria cuando se produzcan modificaciones Sustanciales

Su objetivo es apoyar las tareas de cumplimiento de la Ley Orgánica, así como incidir en el fomento de las buenas prácticas en lo que se refiere al tratamiento de la información personal de la ciudadanía que maneja FormacionL.

A grandes rasgos, **se van a comprobar los mecanismos adoptados para la adopción de los procedimientos y medios de índole técnicos y organizativos**, las medidas de seguridad recogidas en el reglamento, los ficheros registrados en la Agencia de Protección de datos, la gestión de soportes y los medios adaptados para la difusión y formación del personal.
Se detallan los aspectos evaluados y, si procede, las recomendaciones y acciones necesarias para el cumplimiento de la normativa.

Estas acciones exigen un esfuerzo a corto plazo, ya que suponen vulnerabilidades en los procedimientos de gestión de los ficheros que contienen datos de carácter personal. Por su parte, las recomendaciones son medidas que se han de adoptar progresivamente o acciones de mantenimiento para garantizar al 100% de la seguridad de los datos.

2.3.2.- Metodología y Plan de Trabajo

La petición de documentación inicial requerida (anterior a las entrevistas personales) para un análisis y mejor desarrollo de la auditoría, es:

- Organigrama de FORMACIONL.
- Direcciones, departamentos, gerencias provinciales, centros especializados de FORMACIONL y funciones.
- Definición del objeto principal de la entidad y sus competencias.
- Formularios de recogida de datos de carácter personal de cada una de las Direcciones/Gerencias.
- Modelos de carta de contestación al currículo enviados a los solicitantes de empleo.
- Modelos de contratos (indefinidos, a tiempo parcial, etc.) suscritos por empleados, personal en prácticas, becarios, etc.
- Compromiso de confidencialidad y secreto firmado con los empleados, becarios, personal en prácticas, personal subcontratado.
- Modelo de pie de firma de confidencialidad en los mensajes de correo electrónico del personal.
- Modelo de autorización para la realización de análisis clínicos o revisiones médicas del personal (previos y anuales).
- Modelo de solicitud de descuento de cuota sindical en nómina.
- Modelo de consentimiento del personal de la entidad para difundir su imagen a través de la web de la entidad.
- Modelo de modificación de datos de empleados (cambio de domiciliación bancaria, etc.)
- Acuerdo marco o contrato con la Mutua de accidentes de trabajo (FRE)
- Acuerdos marco o contratos con entidades para la Prevención de Riesgos laborales.
- Contrato o acuerdo con compañía de Seguros para empleados y copia de boletín de adhesión del trabajador.
- Captura de pantallas de la aplicación o base de datos de los empleados.

- Copias de medios de comunicación remitidos a los empleados y cliente desde el FORMACIONL de Prensa (Revista, Boletín, Gaceta, Circulares informativas, Memoria, Anuario de entidad, etc.)
- Captura de pantallas de todas las herramientas o aplicaciones donde se recaben datos de carácter personal (aplicación de gestión de empleados y clientes, formación, actos sociales, bolsa de trabajo, etc.) y copia de los documentos donde se recaban datos personales.
- Si existen, adjuntar modelo de documentos donde se soliciten datos de carácter personal a los usuarios o ciudadanos, teniendo en cuenta los distintos tipos de servicios.
- Cláusulas deber información cámaras de video vigilancia, si existiera. Carteles zona video vigilada, si existiera.
- Relación de ficheros inscritos ante la AEPD

2.3.2.1.- Puntos auditados

Los siguientes aspectos son los que vamos a auditar

2.3.2.1.1.- Verificación de características a nivel de Sistemas de Información

En la auditoría se han verificado los siguientes aspectos:

- **Identificación y clasificación de ficheros con datos de carácter personal.**
- **Mecanismos de identificación y autenticación de las aplicaciones**: Hay que distinguir entre lo que son “ficheros jurídicos”, creados por la Organización y notificados a la Agencia Española de Protección de Datos y los “ficheros lógicos” que están basados en las aplicaciones informáticas. Las aplicaciones de un fichero jurídico declarado pueden modificarse sin que tenga que modificarse a su vez la declaración realizada.
- **Tratamiento de seguridad en las comunicaciones**.

2.3.2.1.2.- Análisis de documentos de seguridad a nivel de sistemas de información

Se ha procedido de acuerdo con el Documento de Seguridad de la Organización, a revisar que se cumple todo lo que en el mismo se consigna y en especial los siguientes aspectos:

- **Medidas, normas, procedimientos, reglas y estándares orientados a garantizar el nivel de seguridad establecido:** Para ello se ha revisado la política de contraseñas, los accesos de los usuarios, las altas y bajas, etc., es decir todos aquellos puntos que contribuyen a garantizar la seguridad de los ficheros, sean de nivel básico, medio o alto.
- **Funciones, obligaciones y responsabilidades del personal que accede o custodia el fichero:** Todas ellas han de aplicarse a todos los niveles jerárquicos, sean de carácter político o técnico, incluyendo el usuario de base. Adquieren gran importancia los Responsables de Unidad, como responsables de unidad usuaria.
- **Procedimiento de notificación, gestión y respuesta a incidencias sobre ficheros**: Este procedimiento se considera que debe ser conocido por todos los usuarios.

2.3.2.1.3.- Revisión de los Procedimientos técnicos y organizativos

El día 21 de diciembre de 2007 el Consejo de Ministros aprobó el Real Decreto 1720/2007 sobre el Reglamento de Desarrollo de la Ley Orgánica de Protección de Datos, que sustituye al Reglamento de Medidas de Seguridad de 1999. Real Decreto que entró en vigor el 18 de abril de 2008, de modo que se realizará un especial hincapié en revisar si los procedimientos implantados cumplen con los requerimientos establecidos por el mismo.

Dado que la seguridad en la Organización se ha diseñado sobre el Reglamento anterior; se han auditado todos aquellos aspectos que modifican sustancialmente procedimientos, acompañados de una propuesta de medidas para una paulatina adecuación de la empresa al nuevo Reglamento. Por ello, se han revisado desde el

punto de vista organizativo los procedimientos generales recogidos en el nuevo Reglamento.

Estos procedimientos generales se incluyen en el Documento de Seguridad de la Organización, destacándose los puntos que tendrán mayor incidencia en la auditoría:

- Existencia de políticas, directrices, normativa y procedimientos de seguridad implantados y difundidos.
- Organización interna de la seguridad, definición de funciones y responsabilidades.
- Existencia, utilización y protección de las medidas y procedimientos para la gestión de usuarios y mantenimiento de contraseñas.
- Procedimientos de control de acceso a través de redes de comunicaciones.
- Gestión de incidencias de seguridad.

2.3.2.1.4.- Revisión de las Medidas de Seguridad exigidas en el Reglamento

Se ha realizado una revisión de las medidas particulares de seguridad que se hayan implantado para llevar a cabo las políticas y directrices de seguridad.
En concreto, se han analizado aquellas medidas técnicas específicas que debieran estar implantadas sobre los ficheros de carácter personal y sistemas que los tratan, de acuerdo con el nivel de seguridad que le corresponde. Los principales parámetros que se han revisado, comprenden:

- Medidas de protección de los principales ficheros de los sistemas operativos.
- Medidas de protección de las aplicaciones y bases de datos que gestionen información de carácter personal.
- Medidas de identificación y autenticación de usuarios.
- Activación de las herramientas de control de acceso.
- Activación de las herramientas de registro de incidencias.

- Medidas de seguridad y control en la transferencia de datos.
- **Seguridad física**: Dentro de la seguridad física ha adquirido especial relevancia las auditorías de los Centros de Proceso de Datos. El resultado de esta auditoría de CPD no es parte del objetivo de este PFC.

2.3.2.1.5.- Realización del censo de ficheros en soporte no automatizados de cada Centro

En octubre de 2007 terminó el período de exención de declaración de ficheros no automatizados o manuales.

En la presente Auditoría se han revisado todos aquellos conjuntos organizados de datos de carácter personal que se encuentren en papel u otro formato que no permita su automatización informática.

2.3.2.2.- Procedimiento de Trabajo

El procedimiento empleado en la auditoría ha sido el siguiente:

- Formación preliminar sobre la LOPD y Reglamento de desarrollo.
- Reunión en cada Dirección para auditar sus responsabilidades en protección de datos de carácter personal, conocimiento y práctica de los procedimientos que le afectan y otros puntos del Documento de Seguridad que le conciernen.
- Reunión con Responsable de Sistemas de Información para auditar el CPD y los procedimientos y puntos del Documento de Seguridad que conciernen al Departamento.

2.3.2.3.- Ámbito de Aplicación

El ámbito de aplicación es toda la Organización, sedes y personas que tratan datos de carácter personal

2.3.3.- Auditoría

2.3.3.1.- Verificación de características a nivel sistema de información

2.3.3.1.1.- Identificación y clasificación de ficheros

USUARIAS AUTOORIENTACIÓN

Ante la AEPD se ha declarado que la finalidad de este fichero es *"registro de usuarios beneficiarios del servicio de auto orientación para acceso al área de PCS"*. Fichero que continúa en uso.

Recomendaciones. Ninguna.

RECURSOS HUMANOS

Ante la AEPD se ha declarado que la finalidad de este fichero es *"relaciones laborales con la organización; formación interna y expedientes judiciales o extrajudiciales"*. Fichero que continúa en uso.

En la estructura de datos del fichero declarado al Registro General de Protección de Datos de la Agencia Española, los datos de afiliación sindical y salud están declarados y hacen referencia a la transferencia dineraria y al grado de discapacidad respectivamente.

El fichero se ha modificado y en la actualidad está declarado de nivel alto, cuando anteriormente estaba declarado de nivel medio.

Atendiendo al nivel en el que se debe declarar este fichero, se le deberían aplicar las medias de nivel alto pero según el artículo 81.5 y 81.6 del RD 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 a este fichero se le pueden aplicar las medidas de nivel básico.

Artículo 81.5. En caso de ficheros o tratamientos de datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual bastará la implantación de las medidas de seguridad de nivel básico cuando:

a) Los datos se utilicen con la única finalidad de realizar una transferencia dineraria a las entidades de las que los afectados sean asociados o miembros.

b) Se trate de ficheros o tratamientos no automatizados en los que de forma incidental o accesoria se contengan aquellos datos sin guardar relación con su finalidad.

Artículo 81.6. También podrán implantarse las medidas de seguridad de nivel básico en los ficheros o tratamientos que contengan datos relativos a la salud, referentes exclusivamente al grado de discapacidad o la simple declaración de la condición de discapacidad o invalidez del afectado, con motivo del cumplimiento de deberes públicos.

Recomendaciones. Ninguna

CLIENTES Y PROVEEDORES

Ante la AEPD se ha declarado que la finalidad de este fichero es *"relación comercial con los clientes proveedores y profesionales"*. Fichero que continúa en uso.

Recomendaciones. Ninguna.

AGENDA CORPORATIVA

Ante la AEPD se ha declarado que la finalidad de este fichero es *"facilitar el contacto con las personas y entidades incluidas"*. Fichero que continúa en uso.

Recomendaciones. Ninguna.

EVENTOS

Ante la AEPD se ha declarado que la finalidad de este fichero es *"registro de asistentes a eventos"*. Fichero que continúa en uso.

Recomendaciones. Ninguna.

CONTABILIDAD Y HACIENDA PÚBLICA

Ante la AEPD se ha declarado que la finalidad de este fichero es *"gestión y control de los datos personales relacionados con subvenciones becas y cualesquiera otras obligaciones fiscales y contables de la Organización"*. Fichero que continúa en uso.

El fichero está declarado de nivel medio cuando debe estar declarado de nivel básico, por el tipo de datos que contiene y están declarados.

Recomendaciones

Modificar el nivel del fichero a básico en el documento de seguridad y proceder a la modificación del fichero

CURRICULOS FORMACIONL

Ante la AEPD se ha declarado que la finalidad de este fichero es *"gestión y control de los currículos profesionales de las personas que los ceden a la Organización en los procesos de selección"*. Fichero que continúa en uso.
Recomendaciones. Ninguna.

COMUNICACIÓN Y MARKETING

Ante la AEPD se ha declarado que la finalidad de este fichero es *"gestión y control de los datos relacionados con la comunicación interna y externa de la Organización"*. Fichero que continúa en uso.
Recomendaciones. Ninguna.

USUARIAS

Ante la AEPD se ha declarado que la finalidad de este fichero es *"gestión control de los datos de las personas que participan en los proyectos y programas que gestiona la Organización con arreglo a los fines contemplados en sus estatutos"*. Fichero que continúa en uso.
Recomendaciones. Ninguna.

2.3.3.1.2.- Mecanismos de identicación y autenticación de aplicaciones

La Organización para acceder a las distintas aplicaciones y sistemas tiene implantado dos sistemas de identificación y autentificación que han de emplear los usuarios.

- En primer lugar se ha implantado el sistema de identificador y contraseña soportado a través del sistema operativo y que emplea contraseñas alfanuméricas.
- En segundo lugar para acceder a aquellas aplicaciones corporativas que son empleadas por el personal de la Organización se emplea un identificador y contraseña gestionada por las propias aplicaciones.

Los sistemas empleados garantizan la identificación y autentificación de forma individualizada de cada uno de los accesos que realizan los usuarios a las aplicaciones y al dominio, siempre que los usuarios garanticen la confidencialidad de la contraseña que posean.

Recomendaciones

Realizar acciones divulgativas y de concienciación dirigidas a todo el personal a fin de transmitirles el mensaje de la importancia de que no se compartan las contraseñas por parte de los usuarios, así como otros instrumentos de identificación y validación de los usuarios.

2.3.3.1.3.- Tratamiento de la seguridad de las comunicaciones

No se realizan transmisiones electrónicas de datos clasificados de nivel alto por parte del personal de la Organización, de modo que en las mismas no resulta exigible que se adoptan medidas de cifrado específicas para lograr que las comunicaciones sean ininteligibles frente a terceros.

Asimismo el acceso remoto a los sistemas de información desde las Gerencias sólo se puede realizar a través de la red de la Organización. No se permite el acceso a la red desde redes públicas, ni desde redes inalámbricas, excepto a cierto personal de la Dirección de Sistemas que lo utiliza para tareas de mantenimiento y administración de los sistemas desde el exterior de la red de la Organización.

Recomendaciones. Ninguna.

2.3.3.2.- Análisis del Documento de Seguridad a nivel de Sistemas de Información

Se ha auditado:

- Cumplimiento de las medidas, normas, procedimientos, reglas y estándares orientados a garantizar el nivel de seguridad establecido.
- Cumplimiento de las funciones, obligaciones y responsabilidades del personal que accede o custodia el documento.
- Procedimientos de notificación, gestión y respuesta a incidencias sobre los ficheros.

De las entrevistas realizadas durante el trabajo de campo se pueden extraer las siguientes conclusiones:

En las reuniones mantenidas con los Responsables de las Direcciones se ha observado en general un alto nivel de concienciación y conocimiento de la normativa interna (Documento de Seguridad, procedimientos, normativas, etc.) relacionada con la protección de datos de carácter personal.

No se han encontrado recomendaciones específicas en las siguientes Direcciones:

- **Dirección General Técnica**
- **Desarrollo Territorial**
- **Actividad**
- **Sistemas**

Vamos a detallar en las diferentes Direcciones que hay recomendaciones y cuáles:

- **Organización**

  Dentro de la responsabilidad de esta Dirección recae la del fichero de *"comunicación y marketing"*. Con la información que se dispone en este fichero se están realizando envíos de correos masivos, por lo que si resulta aplicable la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la sociedad de la información y del comercio electrónico. Esta ley en su artículo 21 prohíbe las comunicaciones comerciales no solicitadas a través de correo electrónico o medios de comunicación electrónica equivalente.

  Artículo 21 .Queda prohibido el envío de comunicaciones publicitarias o promocionales por correo electrónico u otro medio de comunicación electrónica equivalente que previamente no hayan sido solicitadas o expresamente autorizadas por los destinatarios de las mismas.

  Recomendaciones

  1.- Para no incumplir el artículo 21 de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y del comercio electrónico se hace preciso solicitar el consentimiento incluyendo una cláusula en el momento de recabar los datos, en los siguientes términos:

  "Consiente que por parte de la Organización se le remitan envíos/mensajes publicitarios incluidos a través de medios electrónicos (artículo 21 de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la sociedad de la

información y del comercio electrónico), acerca de las actividades, servicios, ofertas, promociones especiales y documentación de diversa naturaleza y por diferentes medios de información comercial, además de la gestión de la información de la que se disponga para la promoción de eventos, seminarios, cursos o conferencias que pudieran resultar de interés para los inscritos, de acuerdo con las labores de segmentación y obtención de perfiles relativas a los mismos, todo ello al objeto de personalizar el trato conforme a sus características y/o necesidades."

2.- Incluir al final del texto de los correos electrónicos enviados una cláusula en los siguientes términos:
Para dar de baja próximas comunicaciones similares a ésta, por favor responda a este correo electrónico en el asunto "BAJA DE INFORMACIÓN".

3- En los eventos se suelen realizar fotografías de los asistentes a los mismos. Para poder publicar estas fotos en revistas internas, en la página web, etc., en necesario solicitar el consentimiento de los titulares de los datos de carácter personal.

- **RECURSOS HUMANOS**

  1.- El Desarrollo del Personal se realiza o bien a través de la formación continuada o bien a través de formación puntual (a través del portal del empleado se realiza la gestión de esta formación de cada uno de los empleados). Para la realización de formación superior o de postgrado se envía un escrito con la información del curso para conocimiento de RRHH,
  2.- Informes de accidentes, por ley se deberían investigar exclusivamente aquellos en los que se han producido bajas, pero se investigan todos los accidentes y también los incidentes (por mejora continua). La información se les envía a los Gerentes de los trabajadores. A los Delegados de Prevención se le envía el informe en pdf y no se controla lo que se hace con ellos.

  Recomendaciones

  1.- Concienciar a los Delegados de Prevención de que una vez revisados los informes recibidos por correo electrónico (concepto de fichero temporal), los

eliminen ya que si en algún momento necesitan un informe, este puede ser solicitado a Prevención y así evitar disponer dentro de la Empresa de copias incontroladas de documentos con datos de carácter personal.
Todas estas evaluaciones e informes se archivan en armarios que se encuentran siempre cerrados con llave.

2.- A todo el personal que se incorpora a FormacionL se le hace firmar un compromiso de confidencialidad que en sus puntos 7 y 8 que incluye las cláusulas del derecho de información (artículo 5 de la LOPD) y la solicitud de consentimiento para tratar las fotografías (artículo 12 del RDLOPD). Estas cláusulas se deben sacar de las cláusulas de confidencialidad y ser informados y solicitar el consentimiento en puntos diferentes. 6.4.4.3.- Cláusula del deber de Secreto: COMPROMISO DE CONFIDENCIALIDAD

3.- Para la participación en jornadas de formación se incluye una cláusula para la inclusión de fotos en medios de comunicación, página web.. y es: *6.4.4.4.- Cláusula del deber de información y consentimiento para la recogida de imágenes como dato personal*

- **ECONÓMICA**

Toda la relación, para las compras y mantenimiento, es con personas jurídicas y profesionales autónomos, que en virtud de los artículos 2.2 y 2.3 del RD 1720/2007 quedan excluidos del ámbito de aplicación del Reglamento.
Los contratos se firman todos en la DGT, y su información se encuentra en NAVISION.
Artículo 2.2. *Este reglamento no será aplicable a los tratamientos de datos referidos a personas jurídicas, ni a los ficheros que se limiten a incorporar los datos de las personas físicas que presten sus servicios en aquéllas, consistentes únicamente en su nombre y apellidos, las funciones opuestos desempeñados, así como la dirección postal o electrónica, teléfono y número de fax profesionales.*
Artículo 2.3*. Asimismo, los datos relativos a empresarios individuales, cuando hagan referencia a ellos en su calidad de comerciantes, industriales o navieros,*

también se entenderán excluidos del régimen de aplicación de la protección de datos de carácter personal.

Recomendaciones

Incluir en todos los contratos con los proveedores las cláusulas del artículo 12 de la LOPD.

2.3.3.2.1.- Recomendaciones del Documento de Seguridad a nivel de SI

- Seguir dando a conocer al personal que se incorpore nuevo a la Organización el Documento de Seguridad y proceder a su implantación, como documento de obligado cumplimiento.
- Seguir divulgando a través de la Intranet o de jornadas de divulgación que permitan al personal realizar consultas y resolver cuestiones que les afecte en su trabajo diario.
- Seguir dando a conocer al personal que se incorpore nuevo, e implantar todas aquellas normativas y procedimientos que afecten a la seguridad de la información y especialmente aquellos que estén relacionados con las medidas técnicas y organizativas para la protección de los datos de carácter personal.
- Realizar periódicamente charlas divulgativas sobre protección de datos, especialmente con la incorporación de nuevo personal a la Organización.
- Concienciar al personal de la Organización sobre la necesidad de bloquear los terminales para evitar la suplantación de la personalidad de los usuarios legítimos y con acceso autorizado a los datos de carácter personal.

2.3.3.3.- Revisión de los Procedimientos Técnicos y Organizativos

2.3.3.3.1.- Identificación, Autenticación y Control de Acceso

2.3.3.3.1.1.- Política de Gestión de Control de Accesos

Esta política **se encuentra implantada** en la Organización, ya que se aplican las políticas descritas en el mismo de mínimo privilegio, identificador y clave de accesos comunes, accesos anónimos y número máximo de intentos fallidos.

2.3.3.3.1.2.- Normas para la generación y gestión de identificadores de las personas

Esta normativa **se encuentra implantada** en la Organización, pues los identificadores de acceso son creados por los responsables siguiendo las pautas marcadas en la norma.

2.3.3.3.1.3.- Normas para la generación y gestión de contraseñas

Esta normativa **se encuentra implantada** en la Organización, ya que las personas usuarias de los sistemas de información deben cambiar la contraseña a través de la Intranet en el momento que es dada de alta en el sistema (in situ).

2.3.3.3.1.4.- Procedimiento de alta/baja/modificación de las personas usuarias

El procedimiento que se sigue es el siguiente:

- Alta: en personal es dado de alta en SAP, el nuevo empleado y se crea la cuenta en el directorio activo (DGT) y través de la Intranet (in situ) debe cambiar la contraseña.
- Modificación: se solicita a través de correo electrónico (cambio de permisos en accesos a las aplicaciones).
- Baja: Se emite un listado de SAP con las bajas producidas en la empresa (se comprueba con RRHH), si la baja es temporal se bloquea y si es definitiva se elimina.

Este procedimiento **se encuentra implantado** en la Organización (cumplimiento legal de la identificación, autenticación y control de accesos), aunque el

procedimiento descrito en el documento de seguridad nada tiene que ver con el procedimiento operativo que se sigue.

Recomendaciones. Reescribir el procedimiento 6.5.3.3.4 del documento de seguridad adaptándolo a la realidad de la identificación, autenticación y control de accesos, tal y como se realiza en la Organización.

2.3.3.3.1.5.- Control de accesos a puestos informatizados

Este control **se encuentra implantado** en la Organización, tal y como ya se ha expuesto en el punto 2.3.3.1.2.

2.3.3.3.1.6.- Control de Acceso físico a salas de servidores

Este control **se encuentra implantado** en la Organización, aunque no es objeto de este PFC, se verá en una posterior fase en el informe de situación actual del CPD (ISACPD).

2.3.3.3.1.7.- Control de Acceso físico a salas de archivos-papel

Este control **se encuentra implantado** en la Organización, ya que este control de acceso físico se realiza exactamente igual que el acceso físico a los CPD y este quedará reflejado en el informe ISACPD del CPD que no es objeto de este PFC.

2.3.3.3.1.8.- Control de Acceso a través de redes de comunicaciones

Este control **se encuentra implantado** en la Organización, tal y como ya se ha expuesto en el punto 2.3.3.1.3.

2.3.3.3.2.- Gestión de soportes y documentos

2.3.3.3.2.1. Inventario de documentos papel

El inventario de documentos en papel (ficheros no automatizados) **se encuentra implantado** tal y como indica la normativa del documento de seguridad estableciendo un nivel de una seguridad más alto al crear un código para acceder a los datos de carácter personal.

2.3.3.3.2.2.- Inventario y Etiquetado de soportes electrónicos

El inventario y etiquetado de soportes electrónicos (ficheros automatizados) **se encuentra implantado** tal y como indica la normativa del documento.

2.3.3.3.2.3. Registro de entrada/salida de soportes

El registro de entrada/salida de soportes **se encuentra implantado** en la Organización, ya que se dispone de un libro Excel en el servidor con el registro:
Las personas con autorización en el documento de seguridad para sacar los soportes (normalmente papel al cliente), no deben registrar el soporte. Las personas con autorización en el documento de seguridad para sacar los soportes (normalmente papel a otro centro de la Organización), no deben registrar el soporte. Otros soportes, además de por correo electrónico, no están autorizados salvo necesidad, que se debe comunicar y hasta la fecha no se ha comunicado.

2.3.3.3.2.4.- Controles para el envío y transporte de soportes

El control para el envío y transporte de soportes **se encuentra implantado** tal como se indica en el documento de seguridad, ya que el único envío que se realizando es el de las copias a la Gerencia de Sevilla (en el documento de seguridad se refleja el envío a Cajax) y este se realiza por personal de FORMACIONL. No es necesario que para el control de este envío se disponga de autorización del Responsable del fichero ya que este envío no sale de los locales bajo el control del Responsable del Fichero.

Recomendaciones

Se ha sustituido en el Documento de Seguridad en el apartado *6.5.5.1.- Política de copias de respaldo en la Dirección General Técnica,* incorporando el almacenamiento en la Gerencia de Sevilla.

2.3.3.3.3.- Régimen de trabajo fuera de las oficinas de FormacionI

Este procedimiento **se encuentra implantado** en la Organización, ya que por norma general no se realiza trabajo fuera de las oficinas de la Organización y en caso de ser necesario se necesitará autorización del Responsable del fichero.

Recomendaciones. Ninguna.

2.3.3.3.4.- Ficheros Temporales

Este procedimiento **se encuentra implantado** en la Organización, ya que existe una concienciación por parte de los usuarios de los sistemas de información de lo que se considera un fichero temporal a parte de disponer de una base de datos en la que todos los ficheros temporales existentes en la Organización están controlados (vivos o muertos).

Recomendaciones. Ninguna.

2.3.3.3.5.- Notificación de Incidencias

Este procedimiento **se está implantando** en la Organización, a través de una aplicación en la cual se va a poder registrar toda la información que obligan los artículos 90 y 100 del Reglamento de desarrollo de la LOPD.

Recomendaciones. Ninguna.

2.3.3.3.6.- Gestión de copias de respaldo y recuperación de datos personales

Este procedimiento **se encuentra implantado** en la Organización, pues se realizan copias de forma diaria, semanal, mensual y anual.

Pero su custodia no se realiza tal como se especifica en el Documento de Seguridad, ya que la copia semanal se envía a la Gerencia de Sevilla, en vez de a la sucursal de Cajax (pero ya se ha rectificado).
Recomendaciones. Ver punto 2.3.3.3.2.4

2.3.3.3.7.- Auditorías y controles periódicos

Esta normativa no se ha realizado anteriormente en la Organización, pero al día de hoy con esta Auditoria ya **se encuentra implantada** en la Organización.
En la normativa no se recoge un formato de puntos a auditar.
Recomendaciones. Detallar los puntos que se deben tratar en las auditorías.

2.3.3.3.8.- Ejercicio derechos en materia de protección de datos

Este procedimiento **se encuentra implantado** en la Organización, ya que se puede ejercer el derecho de rectificación, estando a disposición de los interesados los formularios para poder ejercer cualquiera de los derechos ARCO.
La contestación a la solicitud realizada debe hacerse en un plazo máximo de 10 días.
Recomendaciones. Ninguna.

2.3.3.4.- Revisión de las medidas de seguridad exigidas en el reglamento

El cálculo del porcentaje del cumplimiento de las medidas se realiza de la siguiente forma:
Medida:
Si se cumple valor 1.
Si se cumple parcialmente valor 0,5.
Si no se cumple valor 0.
Cumplimiento: suma de los valores obtenidos * 100 / nº de medidas exigidas por el Reglamento

2.3.3.4.1.- Medidas de nivel básico

2.3.3.4.1.1.- Reglamento de desarrollo de la LOPD

Artículo 89. Funciones y obligaciones del personal. Ver punto 2.3.3.2.2
Artículo 90. Registro de incidencias. Ver punto 2.3.3.3.5
Artículo 91. Control de acceso. Ver punto 2.3.3.3.1
Artículo 92. Gestión de soportes y documentos. Ver punto 2.3.3.3.2
Artículo 93. Identificación y autenticación. Ver punto 2.3.3.3.1
Artículo 94. Copias de respaldo y recuperación. Ver punto 2.3.3.3.6

2.3.3.4.1.2-. Grado de cumplimiento de las medidas de nivel básico

Las medidas de seguridad de nivel básico según el reglamento se cumplen en un 100 %.

2.3.3.4.2.- Medidas de nivel medio

2.3.3.4.2.1.- Reglamento de desarrollo de la LOPD

Artículo 95. Responsable de seguridad. Existe Responsable de Seguridad de la Organización.
Artículo 96. Auditoría. Se realizan auditorías.
Artículo 97. Gestión de soportes y documentos. Ver punto 2.3.3.3.2
Artículo 98. Identificación y autenticación. Ver punto 2.3.3.3.1
Artículo 99. Control de acceso físico. Esta información no está disponible en la actualidad. Es la situación actual del CPD (ISACPD) y de todas formas cumple la normativa actual LOPD.
Artículo 100. Registro de incidencias. Ver punto 2.3.3.3.5

2.3.3.4.2.2.- Grado de cumplimiento de las medidas de nivel medio

Las medidas de seguridad de nivel medio según el reglamento se cumplen en un 100 %.

2.3.3.4.3.- Medidas de nivel alto

2.3.3.4.3.1.- Reglamento de desarrollo de la LOPD

Artículo 101. Gestión y distribución de soportes. Ver punto 2.3.3.3.2
Artículo 102. Copias de respaldo y recuperación. Ver punto 2.3.3.3.6
Artículo 103. Registro de accesos. Se realiza registro de accesos a los ficheros con datos de nivel alto.
Artículo 104. Telecomunicaciones. Ver punto 2.3.3.1.3

2.3.3.4.3.2.- Grado de cumplimiento de las medidas de nivel alto

Las medidas de seguridad de nivel alto según el reglamento se cumplen en un 100 %.

2.3.3.5.- Censo de ficheros en soporte no automatizado

2.3.3.5.1.- Censo de ficheros

Se ha detectado **un fichero** en soporte papel:

Expedientes de personal.

Expedientes sancionadores

2.3.3.5.2.- Expedientes de Personal

Estos expedientes se encuentran ordenados alfabéticamente y están guardados en armarios que se encuentran cerradas con llave. A este fichero sólo accede el personal que por necesidad de su trabajo necesita acceder a él.
De este tratamiento de datos no se está realizando el registro de accesos que marca el RD 1720/2007 en su artículo 113.
Recomendaciones. Registrar los accesos que se realizan a este tratamiento de datos no automatizado de nivel alto.

2.3.3.5.3.- Expedientes Sancionadores

Estos expedientes se encuentran guardados en carpetas independientes en armarios que se encuentran cerradas con llave y dentro de un despacho que tiene llave.

2.3.3.5.4.- Consideración sobre expedientes administrativos que contengan datos de carácter personal

El resto de la documentación debe estar ordenada cuando no se esté trabajando con ella, ya que esto evitaría que personal no autorizado, acceda a datos de carácter personal que puedan contener dichos papeles.
Los expedientes y documentos que no se están utilizando en el día a día se encuentran en armarios cerrados con llave durante toda la jornada laboral en los despachos y salas correspondientes. Los papeles del día a día se encuentran encima de las mesas, se recogen al finalizar la jornada laboral y se encuentran muy ordenados, existiendo una política de mesas limpias.
Este criterio de confidencialidad no debe ser únicamente para los datos personales, sino cualquier dato que no sea de uso público y que esté contenido en un expediente administrativo.

2.3.3.5.5.- Medidas de seguridad en los ficheros en soporte no automatizado

El cálculo del porcentaje del cumplimiento de las medidas se realiza de la siguiente forma:
Medidas:
Si se cumple valor 1.
Si se cumple parcialmente valor 0,5.
Si no se cumple valor 0.
Cumplimiento: suma de los valores obtenidos * 100 / nº de medidas exigidas por el Reglamento

2.3.3.5.5.1.- Medidas de nivel básico

2.3.3.5.5.1.1.- Reglamento de desarrollo de la LOPD

Artículo 105. Obligaciones comunes.
Serán aplicables por el principio jurídico de analogía las medidas de seguridad dirigidas a proteger los ficheros en soporte automatizado; sin perjuicio de la obligación legal de que le responsable del fichero realice los adaptaciones que sean precisos.
Artículo 106. Criterios de archivo.
La compañía deberá establecer una serie de criterios de archivo que garanticen la correcta conservación de la documentación, su localización, consulta, así como el ejercicio de los derechos ARCO.
Artículo 107. Dispositivos de almacenamiento.
Dispondrán de mecanismos que obstaculicen la apertura para su acceso; ya sean cerraduras u otros sistemas análogos.
Artículo 108. Custodia de los soportes.
Se deberá velar por la adecuada custodia de los documentos.

2.3.3.5.5.1.2.- Grado de cumplimiento

Las medidas de seguridad de nivel básico según el reglamento se cumplen en un 100 %.

2.3.3.5.5.2.- Medidas de nivel medio

2.3.3.5.5.2.1.- Reglamento de desarrollo de la LOPD

Artículo 109. Responsable de seguridad. Existe Responsable de Seguridad de la Organización.
Artículo 110. Auditoría. Se realizan auditorías.

2.3.3.5.5.2.2.- Grado de cumplimiento

Las medidas de seguridad de nivel medio según el reglamento se cumplen en un 100 %.

2.3.3.5.6.- Medidas de nivel alto

2.3.3.5.6.1.1.- Reglamento de desarrollo de la LOPD

Artículo 111. Almacenamiento de la información. Los armarios deberán encontrarse en salas de acceso restringido.
Artículo 112. Copia o reproducción. La generación copias y reproducciones de los documentos deberá ser autorizada y controlada
Artículo 113. Acceso a la documentación.
Se deberán adoptar procedimientos de trabajo que cuando realicen traslado de documentos impidan físicamente el acceso a los mismos.
Artículo 114. Traslado de documentación.
Siempre que se proceda al traslado físico de la documentación deben adoptarse medidas para impedir el acceso o la manipulación de la información contenida.

2.3.3.5.6.1.2.- Grado de cumplimiento

Las medidas de seguridad de nivel alto según el reglamento se cumplen en un 75 %.

2.3.4.- Auditoría Documento de Seguridad

El artículo 88.1 del RDLOPD exige a la FormacionL (en su calidad de responsable de fichero) que proceda a elaborar un documento de seguridad que recogerá las medidas de índole técnica y organizativa acordes a la normativa de seguridad vigente que será de obligado cumplimiento para el personal con acceso a los sistemas de información.

El artículo 88, apartados 7 y 8 exigen a la Organización que mantenga el Documento de Seguridad debidamente actualizado y revisado, especialmente frente a los siguientes cambios:

- Sistema de información.
- Sistema de tratamiento.
- Organización.
- Contenido de la información recogida.
- Operatividad de las medidas de seguridad.
- Legales o normativos.

La Organización tiene en vigor el Documento de Seguridad, en el cual no se sabe en qué versión se encuentra y en qué fecha. Este es el Documento de Seguridad que se ha procedido a auditar. Este documento ha sido actualizado a fin de reflejar las distintas mediciones y cambios que se han producido.

Incluir en el documento de seguridad un cuadro de control de versiones que incluya:

- Nº de versión.
- Fecha versión.
- Motivo versión.

2.3.4.1.- Resumen de ficheros inscritos en el R.G.P.D. (Anexo II)

Se ha actualizado la tabla de ficheros y nivel de seguridad de los mismos que se encuentra en el Anexo II y en el Documento de Seguridad, de acuerdo a las modificaciones que se realicen como resultado de esta informe de auditoría bienal.

2.3.4.2.- Identificación, autenticación y control de accesos

Sustituir la referencia al **"6.5.- Anexo II – Personas usuarias autorizadas con acceso a los ficheros"** ya que este anexo no hace referencia a esta información y si en el punto **"6.5.8.5.4. Autorización y control de acceso a las aplicaciones"**.

2.3.4.3.- Procedimiento de alta/baja/modificación de las personas usuarias

Redactar esta normativa según se está realizando tal como se indica en el punto **2.3.3.3.1.4** de esta auditoría bienal.

2.3.4.4.- Punto 6.5.8.5.4 "autorización y control de acceso a las aplicaciones"

Incluir en la tabla del fichero de "RECURSOS HUMANOS" las personas autorizadas a acceder a los expedientes de personal.

2.3.4.5.- Procedimiento a seguir en el ejercicio de derechos en materia de protección de datos

Modificar en la tabla en el derecho de acceso, el plazo de comunicación efectiva de información de **"1 mes"** a **"10 días"**. Se ha rectificado y está correcto.

2.3.5.- Conclusiones Auditoría

La protección de datos de carácter personal en la Dirección General Técnica de la Organización se puede considerar **MUY SATISFACTORIA**.
Desde FormacionL, se debe:

- Mantener el nivel de seguridad alcanzado para el tratamiento con datos de carácter personal.
- Mantener el nivel de concienciación y divulgación para el tratamiento con datos de carácter personal.
- Impulsar el conocimiento, por parte de todos los usuarios, de la nueva herramienta de gestión de incidencias.
- Respecto a los ficheros no automatizados. Es necesario el **sistema de inventariado y etiquetado de los soportes, y que los mecanismos de acceso y apertura** estén custodiados por la persona autorizada con acceso a los mismos, pues son una pieza fundamental para garantizar la seguridad de los datos.

- El **registro de incidencias**, otro de los puntos importantes de la normativa, estará cubierto con un **Centro de Atención Integral en la Intranet**, servicio de atención que permitirá informar a todo el personal de la Organización y llevar un registro de incidencias acorde a lo obligado por el Reglamento.
- Y por último, la **formación a todo el personal**, que sólo se ha abordado por encima y buscará **la implicación del mismo y capacitación en el tratamiento de datos de carácter personal,** pues son las personas el primer eslabón en la cadena de tratamiento y, con toda seguridad, el más débil.
- Por tanto, se puede afirmar que **tras los pasos dados para adaptar la Empresa a la normativa vigente** en materia de protección de datos de carácter personal, **la empresa se encuentra en un buen estado de salud respecto al tratamiento de datos de carácter personal.**
- Las medidas que se han visto quedan por implantar o mejorar, **garantizarán la protección total de los datos íntimos, personales y que son, en definitiva, propiedad de cada persona**.
- No se ha realizado el informe de situación actual del **CPD (ISACPD)**, que no era objeto de esta Auditoría, pero se ha comprobado que el CPD cumple las medidas de seguridad requeridas por el Reglamento.
- Los Ficheros se han rectificado en la AEPD y están correctamente definidos en el Documento según los resultados de la Auditoría.

A continuación vamos a describir el Plan de Seguridad elaborado para FormacionL.

2.4.- Adaptación del Plan de Seguridad a la Organización

Acciones a realizar por FormacionL para implantar un Plan de Seguridad

Para ello, algunas acciones a realizar que son obligatorias por Ley son:

- Inscribir los ficheros de datos de carácter personal que existen en la Organización en la Agencia Española de Protección de Datos (AEPD)

- Pasar una auditoría interna o externa cada 2 años, y tenerla a disposición de un requerimiento de la AEPD
- Elaborar e implantar la normativa de seguridad mediante **Documento de Seguridad** vivo, a disposición de la AEPD y de obligado cumplimiento para el personal con acceso a los datos de carácter personal.
- Implantación de procedimientos
- Comunicación al personal de la empresa de:
    - Las personas responsables en la empresa
    - Normas a cumplir por parte del personal, extracto del Documento de Seguridad
    - Procedimientos establecidos por la ley
    - Derechos ARCO, derecho de la ciudadanía a pedir explicaciones a las Organizaciones sobre sus datos de carácter personal
    - Obligación de informar de las incidencias que la ley establece
- Implantación de una herramienta para la comunicación de las incidencias que la ley exige, a la que denominamos **Centro de Atención Integral**
- Implantación de unas medidas de seguridad física tanto en los espacios de almacenamiento de documentación en papel: archivo, armarios con llaves,..
- Implantación de unas medidas de seguridad física en los Centros de Proceso de Datos de los centros de la Empresa
- Eliminación de los datos, en papel o automatizados una vez finalizada la función para la que se recogieron
- Cambio de las claves de todos los Sistemas de información con datos de carácter personal, una vez al año como mínimo.
- Los usuarios y claves de acceso a los Sistemas de información o a los espacios físicos deben ser únicos, y debe conocer sólo la persona autorizada-
- En cuanto a las personas beneficiarias de la FormacionL, hay que pedir una serie de consentimiento (recogida en clausulas), para cualquier acción no recogida en la relación con la persona beneficiaria (fotos, comunicaciones posteriores, cesión de sus datos a terceras personas,…)

- Para ello hay que tener una serie de instrumentos para cumplir físicamente esta ley: destructoras de papel, controles de accesos en los espacios físicos en lo que se almacenan datos de carácter personal, copia y custodia seguridad de estos datos de carácter personal, alarmas, armarios y/o cajoneras con llaves.
- Formación a todo el personal de la Empresa.

Además de ello, para facilitar la compresión de la LOPD:

- Elaboración de documento con la información y normas más usuales: documento de buenas prácticas
- El procedimiento de incidencias, se va a realizar a través de la Intranet, con una herramienta a tal efecto que lleva incluido los procedimientos a los que la Ley obliga.

Vamos a detallar algunos de estos puntos que se han implantados:

1. ***Documento de Aplicación Legal LOPD (Anexo IV). Creación de modelos para las cláusulas de los distintos procedimientos***

Para ello se ha creado un **Documento de Aplicación Legal** de uso interno del personal de la empresa en el que se incluyen todas las cláusulas a incluir en todos los procedimientos de trabajo con datos de carácter personal, para el desarrollo del trabajo diario de la empresa con los trabajadores, clientes, proveedores y ciudadanía en general

Dichas cláusulas extraídas son de obligado cumplimiento, y aparte de crear dicho documento, han sido publicadas en la intranet para facilitar dicho uso al personal de la empresa. Estas cláusulas están incluidas en el **Anexo IV**, **y cada una de ellas** hace referencia al artículo (o artículos) de la LOPD por la que se crean y son las siguientes:

- Modelo de respuesta a curriculum vitae
- Cláusula del deber de información y consentimiento para la recogida de datos de carácter personal

- Cláusula del deber de información y consentimiento para la recogida de imágenes como dato personal
- Contratos con terceros que tratan datos de FormacionL
- Contratos con Terceros que no acceden a datos pero si a los Centros o a la Dirección General Técnica
- Contratos en los que FormacionL es Encargado de Tratamiento
- Formulario de acceso a los datos para el personal
- Formulario de acceso a los datos para personas beneficiarias
- Formulario de rectificación de los datos para el personal
- Formulario de rectificación de los datos para Usuarias
- Formulario de cancelación de los datos para el personal
- Formulario de cancelación de los datos para personas beneficiarias

2. Documento de Seguridad Anexo V

El Documento de Seguridad está incluido en el Anexo 5 de este Documento.
El artículo 88.1 del RDLOPD exige a la Organización (en su calidad de responsable de fichero) que proceda a elaborar un documento de seguridad que recogerá las medidas de índole técnica y organizativa acordes a la normativa de seguridad vigente que será de obligado cumplimiento para el personal con acceso a los sistemas de información.
Como primer paso para asegurar la integridad, seguridad y calidad de los datos, el Documento de Seguridad define una serie de normas, medidas y procedimientos de seguridad respecto a los Sistemas de Información que, cada persona usuaria de FormacionL, debe seguir.

Las normas especificadas en el documento de seguridad están agrupadas en cinco bloques:

1. Normas de uso aceptable de los Sistemas de Información (pc, portátiles, antivirus, impresoras…)
2. Normas para la identificación y control de acceso de las personas ante los sistemas de información

3. Gestión de soportes y documentos que almacenan datos de carácter personal
4. Normas relativas a los datos tratados fuera de centros no pertenecientes a la Empresa
5. Reglamentación y procedimientos para los ficheros temporales.

Es necesario hacer especial hincapié en las normas de Gestión de soportes y documentos, y en el lado opuesto, están las normas generales y las relativas a los datos tratados fuera de centros de la empresa, cuyo nivel de cumplimiento es bastante elevado.

Aspectos mínimos recogidos en el Documento de Seguridad:

- Ámbito de Aplicación
- Medidas, normas y procedimientos definidos e implantados
- **Funciones y obligaciones del personal**
- Estructura de los ficheros y descripción de los sistemas que los tratan
- **Procedimiento de Notificación, gestión y respuesta ante incidentes**
- Procedimientos para realización de copias de respaldo y de recuperación de los datos.
- Medidas de protección para el transporte de soportes y documentos
- Declaración de tratamientos y/o accesos a datos por terceros

También debe recoger (*obligatorio para niveles medio y alto*)

- Identificación de los responsables de los datos: *Responsables de Seguridad*
- Controles para verificar el cumplimiento de las medidas.

3. Centro de Atención Integral: Registro de incidencias

Dicho centro se está desarrollando en la Intranet de la Organización y vamos a ver algunas características en este apartado.

El RLOPD recoge, en los artículos 90 y 100 la obligatoriedad de llevar un registro de incidentes relacionados con los ficheros y soportes que contienen datos de carácter personal.

Además de estos procedimientos, no hay que olvidar los derechos **ARCO** (acceso, rectificación, cancelación y oposición de los datos) de las personas. Estos procedimientos se tienen que articular a través de un canal eficiente, rápido y directo que permita ejercer dichos derechos en el plazo estipulado por la ley (1 mes).

La solución completa para el soporte se denomina **Servicio de atención integral.**

La composición del Servicio de atención integral se resume en el siguiente Diagrama 5"Servicio de Atención Integral"

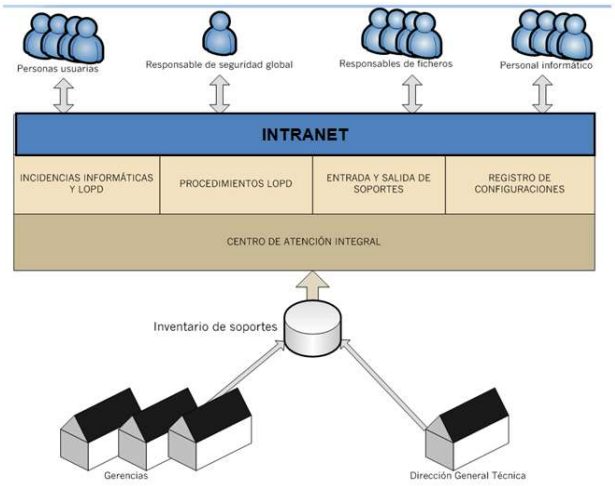

Diagrama 5 Servicio de Atención Integral

Estará alojado en la Intranet de FormacionL, y dará soporte a los siguientes procedimientos, requeridos por la LOPD:

- Consultas – Consultas informáticas
- Consultas – Consultas LOPD
- Informática – Asistencia técnica aplicaciones FormacionL
- Informática – Asistencia técnica en el puesto de trabajo
- Informática – Instalación de software
- Informática / LOPD – Solicitud de copia de seguridad
- LOPD – Identificación y autenticación de personas
- LOPD – Derecho de acceso a los datos
- LOPD – Gestión de soportes

- LOPD – Ficheros no automatizados (en papel)
- LOPD – Cumplimiento de normas de seguridad
- LOPD – Cualquier otra incidencia
- LOPD – Solicitud de tratamiento de datos de carácter personal
- Entrada y salida de soportes

A continuación se describen las conclusiones de la realización de este PFC.

3.- Conclusiones

En el desarrollo de este PFC se ha estudiado bastante sobre la LOPD y todo el reglamento que trata datos de carácter personal y **lo importante del cumplimiento** para las empresas, y para la vida cotidiana del ciudadano en general.

Es por lo que se ha desarrollado la Ley, se ha recalcado la gran importancia del cumplimiento de esta y su aplicación práctica en FormacionL, una empresa ficticia creada a tal efecto para poder realizar nuestro PFC.

Hemos cumplido en gran parte los objetivos inicialmente propuestos, aunque hubiera completado el objetivo si se hubiera realizado todas las fases de la Auditoría y realizado un Plan de Formación completo.

Los plazos previamente establecidos en la Planificación Inicial han tenido algún desfase por motivos externos, pero se ha podido desarrollar el PFC con los mínimos establecidos.

Por tanto, se puede afirmar que **tras los pasos dados para adaptar la Empresa a la normativa vigente** en materia de protección de datos de carácter personal, **la empresa se encuentra en un buen estado de salud respecto al tratamiento de datos de carácter personal.**

Las medidas que están en marcha y las que se pondrán en breve, **garantizarán la protección total de los datos íntimos, personales y que son, en definitiva, propiedad de cada persona**.

Por lo tanto una **ampliación de este PFC** con posterioridad debería ser:

- completar las fases de la **Auditoría.**
  - Se ha detallado los resultados de la Auditoría pero no se ha realizado el ***informe de auditoría*** tal como marca el artículo 96.2, y que es obligatorio realizarlo por LOPD.
  - Tampoco se ha realizado la comunicación del informe anteriormente citado y su custodia por el Responsable de Seguridad para la disponibilidad por parte de las autoridades, acción que es obligatoria por ley, lo refleja el artículo 96.3 del RLOPD
- Realizar un Plan de Formación
- Realizar un informe de situación actual del CPD (ISACPD) y Escaneo de Vulnerabilidades, que aunque no sean de obligatorio cumplimiento para nuestra Auditoría, si lo es para tener una Organización segura.

A continuación vamos a ver el Glosario de nuestro PFC

4.- Glosario

Agencia Española de Protección de Datos (AEPD): Organismo Oficial Estatal que regula y controla el cumplimiento de la Ley y la protección de los derechos de los ciudadanos. La Ley dedica su Título VI a la regulación de este ente de derecho público

Accesos autorizados: autorizaciones concedidas a un usuario para la utilización de los diversos recursos. En su caso, incluirán las autorizaciones o funciones que tenga atribuidas un usuario por delegación del responsable del fichero o tratamiento o del responsable de seguridad.

Afectado o interesado: Persona física titular de los datos que sean objeto del tratamiento.

Autenticación: procedimiento de comprobación de la identidad de un usuario.

Bloqueo de datos: La identificación y reserva de los datos de carácter personal con el fin de impedir su tratamiento.

Cancelación: Procedimiento en virtud del cual el responsable cesa en el uso de los datos. La cancelación implicará el bloqueo de los datos, consistente en la identificación y reserva de los mismos con el fin de impedir su tratamiento excepto para su puesta a disposición de las Administraciones públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento y sólo durante el plazo de prescripción de dichas responsabilidades. Transcurrido ese plazo deberá procederse a la supresión de los datos.

Comunicación o cesión de datos: Toda revelación de datos realizada a una persona distinta del interesado.

Consentimiento del interesado: Toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen.

Contraseña: información confidencial, frecuentemente constituida por una cadena de caracteres, que puede ser usada en la autenticación de un usuario o en el acceso a un recurso.

Control de acceso: mecanismo que en función de la identificación ya autenticada permite acceder a datos o recursos.

Copia de respaldo: copia de los datos de un fichero automatizado en un soporte que posibilite su recuperación.

Datos de carácter personal: Cualquier información concerniente a personas físicas identificadas o identificables. Cualquier dato que identifique a una persona de forma única. Nombre y apellidos, NIF, dirección, email, foto, ….

Datos de carácter personal relacionados con la salud: Las informaciones concernientes a la salud pasada, presente y futura, física o mental, de un individuo. En particular, se consideran datos relacionados con la salud de las personas los referidos a su porcentaje de discapacidad y a su información genética.

Dato disociado: Aquél que no permite la identificación de un afectado o interesado.

Declarante: Persona física que cumplimenta la solicitud de inscripción y actúa como mediador entre la Agencia y el titular/responsable del fichero. No debe necesariamente coincidir con el titular/responsable.

Derecho de Acceso: Derecho de la persona interesada a solicitar y obtener información de sus datos de carácter personal incluidos en los ficheros, el origen de los mismos, así como las comunicaciones realizadas o que se prevean realizar.

Derecho de consulta: Es el Derecho a conocer la existencia de ficheros automatizados de datos de carácter personal, sus finalidades y la identidad del responsable del tratamiento. Este derecho se ejercita ante el Registro General de la Agencia Española de Protección de Datos, recabando la información oportuna. (el Registro se compone de todos los ficheros públicos y privados inscritos en la Agencia Española de Protección de Datos)

Derecho de consulta: Es el Derecho a conocer la existencia de ficheros automatizados de datos de carácter personal, sus finalidades y la identidad del responsable del tratamiento. Este derecho se ejercita ante el Registro General de la Agencia Española de Protección de Datos, recabando la información oportuna. (el Registro se compone de todos los ficheros públicos y privados inscritos en la Agencia Española de Protección de Datos).

Derecho de oposición: Se trata del derecho a no utilizar sus datos con fines de publicidad y prospección comercial.

Derecho de rectificación y cancelación: Derecho de la persona interesada a que sus datos de carácter personal sean rectificados o cancelados, en su caso, cuando su tratamiento no se ajuste a lo dispuesto en la Ley. Especialmente, cuando sean inexactos, incompletos, inadecuados, excesivos.

Destinatario o cesionario: La persona física o jurídica, pública o privada u órgano administrativo, al que se revelen los datos.

Podrán ser también destinatarios los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.

Documento: todo escrito, gráfico, sonido, imagen o cualquier otra clase de información que puede ser tratada en un sistema de información como una unidad diferenciada.

Encargado del tratamiento: La persona física o jurídica, pública o privada, u órgano administrativo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento o del responsable del fichero, como consecuencia de la existencia de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación para la prestación de un servicio.

Podrán ser también encargados del tratamiento los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.

Exportador de datos personales: La persona física o jurídica, pública o privada, u órgano administrativo situado en territorio español y responsable del tratamiento de los datos de carácter personal que son objeto de transferencia internacional a un país tercero.

Fichero: Todo conjunto organizado de datos de carácter personal, con arreglo a criterios determinados cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.

Al hablar de fichero se distingue:

- Fichero no automatizado: se refiere a toda documentación en papel.
- Fichero automatizado: se refiere a todo documento electrónico. Base de datos, documentos de Excel, Word,…

Ficheros temporales: ficheros de trabajo creados por los usuarios o procesos que son necesarios para un tratamiento ocasional o como paso intermedio durante la realización de un tratamiento.

Ficheros de titularidad privada: los ficheros de los que sean responsables las personas, empresas o entidades de derecho privado, con independencia de quien ostente la titularidad de su capital o de la procedencia de sus recursos económicos, así como los ficheros de los que sean responsables las corporaciones de derecho público, en cuanto dichos ficheros no se encuentren estrictamente vinculados al ejercicio de potestades de derecho público que a las mismas atribuye su normativa específica.

Ficheros de titularidad pública: los ficheros de los que sean responsables los órganos constitucionales o con relevancia constitucional del Estado o las instituciones autonómicas con funciones análogas a los mismos, las Administraciones públicas territoriales, así como las entidades u organismos

vinculados o dependientes de las mismas y las Corporaciones de derecho público siempre que su finalidad sea el ejercicio de potestades de derecho público.

Fichero no automatizado: todo conjunto de datos de carácter personal organizado de forma no automatizada y estructurado conforme a criterios específicos relativos a personas físicas, que permitan acceder sin esfuerzos desproporcionados a sus datos personales, ya sea aquél centralizado, descentralizado o repartido de forma funcional o geográfica.

Fuentes accesibles al público: Aquellos ficheros cuya consulta puede ser realizada por cualquier persona, no impedida por una norma limitativa, o sin más exigencia que, en su caso, el abono de una contraprestación. Tienen la consideración de fuentes de acceso público, exclusivamente, el censo promocional, los repertorios telefónicos en los términos previstos por su normativa específica y las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo. Asimismo, tienen el carácter de fuentes de acceso público, los Diarios y Boletines oficiales y los medios de comunicación.

Identificación: procedimiento de reconocimiento de la identidad de un usuario.

Identificación del afectado: Cualquier elemento que permita determinar directa o indirectamente la identidad física, fisiológica, psíquica, económica, cultural o social de la persona afectada.

Importador de datos personales: La persona física o jurídica, pública o privada, u órgano administrativo receptor de los datos en caso de transferencia internacional de los mismos a un tercer país, ya sea responsable del tratamiento, encargada del tratamiento o tercero.

Incidencia: cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos.

Perfil del usuario: accesos autorizados a un grupo de usuarios.

Persona identificable: Toda persona cuya identidad pueda determinarse, directa o indirectamente, mediante cualquier información referida a su identidad física, fisiológica, psíquica, económica, cultural o social. Una persona física no se

considerará identificable si dicha identificación requiere plazos o actividades desproporcionados.

Procedimiento de disociación: Todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona identificada o identificable.

Recurso: cualquier parte componente de un sistema de información.

Responsable de seguridad: persona o personas a las que el responsable del fichero ha asignado formalmente la función de coordinar y controlar las medidas de seguridad aplicables.

Responsable del fichero o tratamiento: Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento, aunque no lo realizase materialmente.

Podrán ser también responsables del fichero o del tratamiento los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.

Sistema de información: conjunto de ficheros, tratamientos, programas, soportes y en su caso, equipos empleados para el tratamiento de datos de carácter personal.

Sistema de tratamiento: modo en que se organiza o utiliza un sistema de información. Atendiendo al sistema de tratamiento, los sistemas de información podrán ser automatizados, no automatizados o parcialmente automatizados.

Soporte: objeto físico que almacena o contiene datos o documentos, u objeto susceptible de ser tratado en un sistema de información y sobre el cual se pueden grabar y recuperar datos.Puede ser cualquier contenedor de datos PC, portátil, USB, CD, carpetas de papeles, cuaderno, teléfono móvil,..

Tercero: la persona física o jurídica, pública o privada u órgano administrativo distinto del afectado o interesado, del responsable del tratamiento, del responsable del fichero, del encargado del tratamiento y de las personas autorizadas para tratar los datos bajo la autoridad directa del responsable del tratamiento o del encargado del tratamiento.

Podrán ser también terceros los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.

Transferencia de datos: El transporte de los datos entre sistemas informáticos por cualquier medio de transmisión, así como el transporte de soportes de datos por correo o por cualquier otro medio convencional.

Transferencia internacional de datos: Tratamiento de datos que supone una transmisión de los mismos fuera del territorio del Espacio Económico Europeo, bien constituya una cesión o comunicación de datos, bien tenga por objeto la realización de un tratamiento de datos por cuenta del responsable del fichero establecido en territorio español.

Transmisión de documentos: cualquier traslado, comunicación, envío, entrega o divulgación de la información contenida en el mismo.

Tratamiento de datos: cualquier operación o procedimiento técnico, sea o no automatizado, que permita la recogida, grabación, conservación, elaboración, modificación, consulta, utilización, modificación, cancelación, bloqueo o supresión, así como las cesiones de datos que

Resulten de comunicaciones, consultas, interconexiones y transferencias.

Usuario: sujeto o proceso autorizado para acceder a datos o recursos. Tendrán la consideración de usuarios los procesos que permitan acceder a datos o recursos sin identificación de un usuario físico.

5.- Bibliografía

Básica sobre Ley Orgánica de Protección de Datos

- **Assunmpció Guasch Petit, Ernesto Martinez de Carvajal Hedrich, Manuel Peiró Mir, Joaquín Ríos Boutin, Jordi Roca i Marimon,** R. (2008) Auditoria, Peritaje y Aspectos legales para informáticos (en línea) FUOC. Barcelona. Disponible en http://cv.uoc.edu/continguts/ XP07_81063_02691 /index.html

Elaboración del Trabajo de Fin de Carrera:

- **Bataller Díaz, A., Beneito Montagut,R., Pérez Navarro, A. (Coord), Sáenz Higueras, N.,Vidal Oltra, R**. (2008) Trabajo Final de Carrera. (en línea) FUOC. Barcelona. Disponible en http://cv.uoc.edu/continguts/XW08_89018_00443/index.html

URL:

- UOC http:\\www.uoc.edu [Consultado 25/02/2016]
- Agencia española de Protección de datos www.aepd.es [Consultado 01/03/2016]

6.- Anexos

6.1.- Anexo I. Tipología de los datos de carácter personal

DATOS DE CARÁCTER PERSONAL	
TIPO DE DATOS	**NOMBRE DE LOS DATOS**
Datos especialmente protegidos	Ideología, afiliación sindical, religión, creencias, origen racial o étnico, salud, vida sexual.
Datos de carácter identificativo	DNI/NIF, NºSS/Mutualidad, nombre y apellidos, dirección (postal electrónica), teléfono, firma/huella digitalizada, imagen/voz, marcas físicas, firma electrónica.
Datos de características personales	Datos de estado civil, datos de familia, fecha de nacimiento, lugar de nacimiento, edad, sexo, nacionalidad, lengua materna, características físicas o antropométricas.
Datos de circunstancias sociales	Características de alojamiento/vivienda, situación militar, propiedades, posesiones, aficiones y estilos de vida, pertenencia a clubes/asociaciones, licencias, permisos, autorizaciones.
Datos académicos y profesionales	Formación, titulaciones, historial del estudiante, experiencia profesional, pertenencia a colegios o asociaciones profesionales.
Datos de detalle de empleo	Profesión, puesto de trabajo, datos no económicos de nómina, historial del trabajador.
Datos de información comercial	Actividades y negocios, licencias comerciales, suscripciones a publicaciones/medios de comunicación, creaciones artísticas, literarias, científicas o técnicas.

Datos económico-financieros y de seguros	Ingresos, rentas, inversiones, bienes patrimoniales, créditos, préstamos, avales, datos bancarios, planes de pensiones, jubilación, datos económicos de nómina, datos deducciones impositivas/impuestos, seguros, hipotecas, subsidios, beneficios, historial de créditos, tarjetas de crédito.
Datos de transacciones	Bienes y servicios suministrados por el afectado, bienes y servicios recibidos por el afectado, transacciones/indemnizaciones.

6.2.- Anexo II: Ficheros inscritos en la Agencia de Protección de Datos

A continuación está la relación de ficheros inscritos en la Agencia de Protección de Datos, su descripción, finalidad y nivel.

Está definida la posible Dirección Responsable del fichero, según la ronda de reuniones y el estudio realizado anteriormente.

6.2.1.- Ficheros responsables de la Dirección de Desarrollo Territorial

Fichero	**Usuarias autorientación**
Nivel	Medio
Datos carácter identificativo	d.n.i./n.i.f.; teléfono; firma electrónica; nombre y apellidos; dirección de e-mail; contraseña; identificador de acceso; alta como demandante de empleo de beneficiarios del servicio de auto-orientación para el empleo.
Otros tipos de datos	datos de características personales; datos de empleo
Finalidad	registro de usuarios beneficiarios del servicio de auto-orientación para acceso al área de PC

Fichero	**Usuarias**
Nivel	Básico
Datos carácter identificativo	nombre y apellidos; dirección; teléfono; d.n.i/n.i.f.; imagen/voz; nº ss/mutualidad; firma/huella; firma electrónica; correo electrónico de personas beneficiarias de los servicios de formación
Otros tipos de datos	características personales; circunstancias sociales;

	académicos y profesionales; detalles del empleo
Otros tipos de datos	tarjeta de demanda; edad; situación laboral de familiares; carnet de conducir; cuenta bancaria; sexo; nacionalidad; cargo; responsabilidad
Finalidad	Gestión y control de los datos de las personas que participan en los proyectos y programas que gestiona la empresa con arreglo a los fines contemplados en sus estatutos, en la mayoría son los alumnos de los cursos.

6.2.2.- Ficheros responsables de la Dirección de Recursos Humanos

Fichero	**Recursos Humanos**
Nivel	Alto
Datos carácter identificativo	d.n.i. /n.i.f.; num. s. s. /mutualidad; nombre y apellidos; dirección; teléfono; credenciales (personas usuarias y contraseña); firma electrónica; imagen/voz; firma/huella; firma electrónica
Otros tipos de datos	datos de características personales; datos de circunstancias sociales; datos académicos y profesionales; datos de detalles de empleo; datos económicos financieros y de seguros; nº de hijos; nombres de los hijos; estado civil; minusvalía; grado de minusvalía; cuenta bancaria; cónyuge afiliación sindical
Finalidad	relaciones laborales con la empresa

Fichero	**Curriculos FormacionL**
Nivel	Medio
Datos carácter identificativo	nombre y apellidos; dirección; teléfono; d.n.i/nif; firma/huella; nº s.s./mutualidad; imagen/voz; correo electrónico
Otros tipos de datos	características personales; académicos y profesionales; detalles del empleo
Finalidad	gestión y control de los currículos profesionales de las personas que los ceden a la empresa, en los procesos de selección

6.2.3.-Ficheros responsables de la Dirección Económica

Fichero	**Clientes y Proveedores**
Nivel	Básico
Datos carácter identificativo	d.n.i./n.i.f.; nombre y apellidos; dirección; teléfono; otros datos de carácter identificativo; num.s.s./mutualidad; persona de contacto; firma/huella; firma electrónica
Otros tipos de datos	num.s.s./mutualidad; persona de contacto; transacciones de bienes y servicios; datos académicos y profesionales; correo electrónico; imagen y voz; nº de colegiado
Finalidad	relación comercial con los clientes y proveedores

Fichero	**Contabilidad y Hacienda pública**

Nivel	Medio
Datos carácter identificativo	dirección; teléfono; d.n.i/n.i.f.; nombre y apellidos; firma/huella; firma electrónica; correo electrónico
Otros tipos de datos	datos de información comercial; transacciones de bienes y servicios; cuentas bancarias
Finalidad	Gestión y control de los datos personales relacionados con las subvenciones, becas y la contabilidad de la empresa.

6.2.4.-Ficheros responsables de la Dirección de Organización

Fichero	**Agenda Corporativa**
Nivel	Básico
Datos carácter identificativo	Nombre y apellidos; dirección; teléfono; imagen/voz; d.n.i; firma/huella; firma electrónica; correo electrónico.
Otros tipos de datos	personas de contacto; cargos públicos
Finalidad	facilitar el contacto con las personas y entidades incluidas

Fichero	**Eventos**
Nivel	Básico
Datos carácter identificativo	d.n.i./n.i.f.; teléfono; dirección; nombre y apellidos; firma / huella; firma electrónica; correo electrónico; imagen / voz
Otros tipos de datos	

Finalidad	Registro de asistentes a eventos

Fichero	**Comunicación y Marketing**
Nivel	Básico
Datos carácter identificativo	nombre y apellidos; dirección; teléfono; imagen/voz; correo electrónico
Otros tipos de datos	características personales; académicos y profesionales
Finalidad	Gestión y control de los datos relacionados con la comunicación interna y externa de la empresa.

6.3.- Anexo III: Artículos y Acciones descriptivos de Ficheros

Relación de Artículos y medidas a tomar con ellos según el nivel de tratamiento del Fichero:

6.3.1.- Medidas Aplicables a los Ficheros de Nivel Bajo Automatizados

- **Artículo 89:** Funciones y obligaciones del personal
    - Los deberes y obligaciones del personal deben estar claramente definidos
        - Han sido definidas de forma clara y concisa en el documento de seguridad
        - El personal directamente implicado como responsable ha sido formado
    - El personal debe conocer de forma comprensible las normas de seguridad que afecten al desarrollo de funciones

      Se publicará en la intranet un apartado exclusivo para el tratamiento de datos de carácter personal, en el que serán definidos los siguientes conceptos:
        - Normas básicas
        - Buenas prácticas
        - Cómo solicitar el tratamiento de datos de carácter personal
        - Cómo utilizar los ficheros que contengan datos de carácter personal
        - Cómo tratar los datos de carácter personal
        - Cuándo eliminar los datos de carácter personal
        - Formación extensible a todo el personal: todo el personal de la Empresa recibirá formación en materia de protección de datos de carácter personal
- **Artículo 90: REGISTRO DE INCIDENCIAS**

- Debe existir un procedimiento de notificación y gestión de incidencias que afecten a los ficheros con datos de carácter personal : Implantar en la intranet un Centro de Atención Integral, que permita notificar, realizar seguimiento y solventar las incidencias que se produzcan, así como llevar un inventario de todos los dispositivos susceptibles de almacenar datos de carácter personal, y las personas que los utilizan.

- **Artículo 91: Control de acceso.**
  - Las personas sólo podrán acceder a los recursos necesarios para el desarrollo de sus funciones:
    - Todas las Direcciones trabajarán en red, con un sistema de permisos personalizado, que garantizará el acceso por persona de únicamente los ficheros necesarios para el desarrollo de su trabajo.
    - En las Gerencias, esto ya está implementado.
  - El responsable del fichero se encargará de mantener una relación de las personas y permisos que éstas tienen
    - A través de la gestión de usuarios centralizada se podrá obtener esta información.
  - Sólo el personal autorizado podrá modificar los permisos
    - A través de la gestión de usuarios centralizada se podrá implementar

- **Artículo 92: Gestión de soportes y documentos**
  - Los soportes deberán ser identificados, inventariados y sólo de acceso al personal autorizado:
    - A través del Centro de Atención Integral se inventariarán los soportes para ficheros automatizados.
    - A través de una base de datos se inventariarán los soportes que almacenen datos en papel.

        - Sólo los responsables de ficheros y personas autorizadas tendrán acceso a la documentación almacenada en estos soportes
    - La entrada y salida de datos de carácter personal ha de estar registrada
        - A través del Centro de Atención Integral se solicitará y autorizará la entrada y salida de datos de carácter personal
    - La entrada y salida de datos de carácter personal ha de estar registrada
        - A través del Centro de Atención Integral se solicitará y autorizará la entrada y salida de datos de carácter personal
    - Destrucción de la información no utilizada
        - Serán puestas en conocimiento de todo el personal y de obligado cumplimiento los plazos para la eliminación de los datos de carácter personal.
        - Estos plazos estarán determinados por la propia LOPD, atendiendo a la naturaleza de la información contenida en los ficheros.
            - Plazos de resoluciones
            - Contratos con cliente privados
            - Gestión interna de la Organización: RRHH; calidad, PRL,..

- **Artículo 93: Identificación y autenticación**
    - Será necesario adoptar las medidas que garanticen la identificación y autenticación de las personas de forma inequívoca.
    - Se procederá al cambio de las contraseñas de todo el personal de la organización en los siguientes sistemas:
        - Ordenador personal
        - Correo electrónico

        - Intranet
        - Portal del personal
        - SAP
        - Navision

- **Artículo 94: Copias de respaldo y recuperación**
    - Deberán establecerse procedimientos de copia :
        - Dirección General Técnica: La información almacenada en el servidor de ficheros tendrá una copia de seguridad y respaldo.
        - Gerencias: Ya se realizan las copias de seguridad necesarias. Para garantizar aún más la seguridad de las mismas, serán transferidas, a través de la VPN, a la Dirección General Técnica
    - Se deben verificar las copias de seguridad cada seis meses
        - Se llevará un registro en el Centro de Atención Integral de las verificaciones de las copias de seguridad.
    - Procedimiento de restauración de copias de seguridad
        - Se publicará un documento con el procedimiento de restauración de las copias de seguridad para cada uno de los sistemas

6.3.2.- Medidas Aplicables a los Ficheros de Nivel Medio Automatizados

- **Artículo 95: Responsable de seguridad**
    - Se deben designar uno o varios responsables de seguridad
        - Se han designado los responsables de seguridad en las gerencias y direcciones. Esta información se encuentra en el documento de seguridad
- **Artículo 96: Auditoría**
    - Se deben realizar una auditoría al menos cada 2 años

- **Artículo 97:** Gestión de soportes y documentos
  - Es necesario un registro de entrada de soportes, que permita conocer el contenido del mismo, la fecha y número de documentos.
    - A través del Centro de Atención Integral se habilitará este registro de entrada y procedimiento asociado al mismo.
  - Es necesario un registro de salida de soportes, que permita conocer el contenido del mismo, la fecha y número de documentos
    - A través del Centro de Atención Integral se habilitará este registro de entrada y procedimiento asociado al mismo.
- **Artículo 98: Identificación y autenticación**
  - Si existen continuos intentos de acceso no autorizados, se ha de limitar la posibilidad de continuar con dichos intentos
    - Se establecerá una política en los servidores de la DGT y las Gerencias para habilitar esta funcionalidad
- **Artículo 99: Control de acceso físico**
  - Sólo el personal autorizado por el documento de seguridad podrá acceder al lugar donde se encuentran los sistemas de información
    - DGT: Norma aplicada. Existe un control de acceso
    - Gerencias: Se instalará progresivamente el control de acceso a los sistemas de información
- **Artículo 100: Registro de incidencias**
  - Se debe indicar el procedimiento para, cuando sea aplicable, recuperar datos. Será necesaria la autorización del responsable de seguridad para restaurar los datos
    - Es de obligado cumplimiento por el documento de seguridad. Esto se articulará a través del Centro de Atención Integral

- **Artículo 101: Gestión y distribución de soportes**
  - Los soportes deben estar etiquetados e identificados
    - Se establecerá un mecanismo de identificación único de los soportes a través del Centro de Atención Integral
  - La distribución de los soportes se ha de realizar de manera encriptado siempre que contengan datos de carácter personal
    - Se utilizará winrar para la encriptación de la información. Los detalles de su utilización vendrán especificados en el documento de buenas prácticas y ampliados en la formación.
- **Artículo 102: Copias de respaldo y configuración**
  - Ubicación de las copias de seguridad
    - Es necesario ubicar las copias de seguridad en un edificio diferente a la sede central.

6.3.3.- Medidas Aplicables a los Ficheros de Nivel Bajo No Automatizados

- Artículo 105: Obligaciones comunes
  - Serán de obligado cumplimiento por el personal
    - Se comunicará a través de la intranet, documento de buenas prácticas y formación.
- **Artículo 106: Criterios de archivo**
  - Garantizar la localización y seguridad de la documentación
    - Se establecerá un procedimiento para ubicar de forma inequívoca todos los almacenes de papel y quién tiene acceso a los mismos
- **Artículo 107: Dispositivos de almacenamiento**
  - Control de acceso

- Tanto los armarios como demás dispositivos sólo serán accesibles por los responsables definidos en el documento de seguridad y las personas autorizadas.

- **Artículo 108: Custodia de soportes**
  - La documentación, si está fuera de los soportes, deberá estar custodiada.
    - Dentro de las normas de seguridad está establecido al obligación de custodiar la documentación en papel por las personas responsables de su tratamiento.

6.3.4.- Medidas Aplicables a los Ficheros de Nivel Medio No Automatizados

- **Artículo 109: Responsable de seguridad**
  - Se definirán responsables de seguridad
    - Descrito en el documento de seguridad
- **Artículo 110: Auditoría**
  - Los ficheros en papel deberán ser sometidos a la misma auditoría interna
    - Recibiremos una auditoría

6.3.5.- Medidas Aplicables a los Ficheros de Nivel Alto No Automatizados

- **Artículo 111: Almacenamiento de la información**
  - Los armarios, archivadores y elementos deberán encontrarse en áreas protegidas
    - Los ficheros con datos de carácter personal de nivel alto se almacenarán en los archivos de la DGT y las Gerencias
- **Artículo 112:**

- **Copia y reproducción**
  - Deberá estar bajo el control del responsable de seguridad
    - Se articulará dentro del Centro de Atención Integral
- **Destrucción de los datos**
  - Destrucción de la información no utilizada
    - Serán puestas en conocimiento de todo el personal y de obligado cumplimiento los plazos para la eliminación de los datos de carácter personal.

- **Artículo 113: Acceso a la documentación**
  - El acceso a la documentación se limitará exclusivamente al personal autorizado
    - Especificado en el documento de seguridad y en el inventario de permisos de acceso
- **Artículo 114: Traslado de documentación**
  - Se deberán adoptar las medidas dirigidas a impedir el acceso o manipulación de la información objeto de traslado
    - Autorización del responsable de seguridad global, que dictaminará las medidas que se han de aplicar.
    - Este procedimiento se articulará desde el Centro de Atención Integral

6.4.- Anexo IV: Documento de Aplicación Legal LOPD FormacionL

Documento de Aplicación Legal LOPD

en la Actividad de FormacionL

Índice

6.4.1.- Anexo del artículo 4: PRINCIPIO DE CALIDAD DE LOS DATOS

Deber de Conservación de los Datos.

La cancelación no implica la destrucción del dato, que deberá ser conservado hasta el transcurso del plazo de prescripción de las posibles responsabilidades derivadas de su tratamiento.

Por lo tanto, procede:

1º.- mantener los datos en **activo** mientras estén efectivamente siendo tratados

2º.- pasar los datos a situación de **bloqueo** cuando termine el tratamiento efectivo

El periodo de tiempo en el que los datos habrán de conservarse bloqueados, antes de su extinción física o del borrado, dependerá del tipo de contrato y la legislación que le sea aplicable en cada caso.

3º.- por último cabe la **cancelación** una vez haya transcurrido el plazo de prescripción de cuantas responsabilidades hubieran podido derivar del tratamiento.

PLAZOS DE PRESCRIPCIÓN EN FUNCIÓN DE LOS DATOS PERSONALES:

1. **FICHERO DE CLIENTES Y PROVEEDORES y FICHERO AGENDA CORPORATIVA.**

Plazo de Conservación:

Como mínimo durante **TRES AÑOS,** una vez finalizado el tratamiento y sin perjuicio de la aplicación de los posibles plazos de prescripción, de las responsabilidades determinadas en la normativa contable y tributaria correspondiente.

2. **FICHERO DE CONTABILIDAD Y HACIENDA PÚBLICA:**

Plazo de Conservación:

Al menos durante **SEIS AÑOS,** a partir de la fecha del último asiento realizado en los libros contables.

Las facturas en las que el emisor o receptor sea persona física, se deben, conservar durante un periodo de **CINCO AÑOS** a partir de su emisión.

3. FICHERO DE DATOS DE EMPLEADOS/AS: RRHH.

Plazo de Conservación:

a) Plazos de prescripción en materia Tributaria

Los Derechos y Garantías de los Contribuyentes, prescriben a los **CUATRO AÑOS**

b) Plazos de prescripción en la legislación laboral y de la Seguridad Social

Contratos de trabajo:

"*1. Las acciones derivadas del contrato de trabajo que no tengan señalado plazo especial prescribirán **AL AÑO** de su terminación".*

Seguridad Social:

***CINCO AÑOS**, a contar desde la fecha en que preceptivamente debieron ser ingresadas".*

"*Las infracciones en el orden social a que se refiere la presente Ley, prescriben a los **TRES AÑOS** contados desde la fecha de la infracción, salvo en materia de Seguridad Social y de protección por desempleo en que el plazo de prescripción es de **CINCO AÑOS**".*

CINCO AÑOS, para la documentación que acredite el cumplimiento de las obligaciones en materia de afiliación, altas, bajas o variaciones que, en su caso, se produjeran en relación con dichas materias, así como los documentos de cotización y los recibos justificativos del pago de salarios y del pago delegado de prestaciones".

4. FICHERO DE CURRÍCULOS FORMACIONL.

Plazo de Conservación:

Los datos del CV que hubieran sido facilitados, serán cancelados automáticamente, transcurrido **UN AÑO** desde la fecha de entrega.

5. **FICHERO COMUNICACIÓN Y MARKETING.**

Plazo de Conservación:

TRES AÑOS establecido con carácter general y sin perjuicio del derecho de cancelación específico en relación con los tratamientos vinculados a actividades de publicidad y prospección comercial y al derecho de oposición en esta clase de tratamientos

6. **FICHERO USUARIOS AUTOORIENTACIÓNL.**

Plazo de Conservación:

UN AÑO en el sistema automatizado

7. **FICHERO EVENTOS.**

Plazo de Conservación:

UN AÑO, inmediato a la finalización del acto o evento.

En cambio si el fin último, es el de Publicidad y Prospección comercial (tal y como consta en tipificación de la finalidad, que tiene el fichero inscrito en el RGPD) habría que atenerse a las mismas cautelas antes señaladas para el fichero de Comunicación y Marketing, es decir el de **TRES AÑOS** para su cancelación.
Con respecto a la financiación del evento, si este, se encuentra subvencionado, y por lo tanto sujeto a futuras inspecciones se recomienda que se guarden durante un periodo prudencial de más de **CINCO AÑOS.**

8. **FICHERO USUARIAS**

Plazo de Conservación:

Serán cancelados atendiendo al plazo de **TRES AÑOS** establecido con carácter general, sin perjuicio de que se necesitara atender a cualquier inspección y para ello venga establecido en la norma correspondiente un plazo mayor de **CINCO AÑOS**. (Proyectos y programas subvencionados)

Se recomienda que el Responsable de Seguridad recuerde cada 6 meses la obligación de destruir el papel inservible que contenga datos personales a través de las distintas destructoras de papel de los Centros Provinciales y de la Sede General.

OBSERVACIONES RESPECTO DE LOS DOCUMENTOS RECIBIDOS POR VÍA ELECTRÓNICA

Será necesario:

- Establecer políticas precisas tanto sobre los correos y documentos que deben archivarse como sobre la manera de archivarlos, a fin de poder acceder a estos documentos y correos con posterioridad.
- Tomar conciencia de que el registro de ficheros y correos electrónicos en un programa puede acarrear consecuencias en su recuperación posterior.
- Archivar los documentos y correos electrónicos utilizando un formato generalmente aceptado para garantizar la legibilidad ulterior y la conservación en su versión original.

El Responsable de Seguridad comprobará que la firma del correo electrónico del personal de **FORMACIONL** incluye la leyenda de confidencialidad apropiada a los fines y en relación con los datos con los que se trabaja.

6.4.2.- Anexo del artículo 5 LOPD y 18 RLOPD: EL DEBER DE INFORMACIÓN.

6.4.2.1.- Tratamiento de los CV de solicitantes de empleo.

FORMACIONL ha establecido como canal único y exclusivo para la recogida de los Currículos el formulario que figura al efecto en la página www.FormacionL.pfc

A) En caso de recepcionar un cv por otra vía. Respuesta

D. / Dña.
Domicilio
Código Postal. Provincia

SEVILLA, ___ de ___ de _____ 2017

Estimado/a Sr. / Sra.:

Le agradecemos la confianza que ha depositado en nosotros al entregarnos su Currículum Vitae. Sin embargo, la empresa FormacionL**,** sólo procede a recoger información profesional exclusivamente mediante el formulario informático, que se encuentra a su disposición en nuestra página www.FormacionL.pfc por lo que en respeto absoluto a nuestra política de privacidad y a la vigente Ley Orgánica 15/1999, de 13 de diciembre de Protección de Datos de Carácter Personal, nos vemos obligados a informarle que su Currículo Vitae ha sido debidamente cancelado.

Agradeciendo cordialmente el interés que se ha tomado por nuestra FormacionL.

Le saluda atentamente,

FORMACIONI

6.4.2.2.- Formularios de recogida de información escrita de las persona beneficiaras de los programas/proyectos

Relación de ejemplos donde se debe de utilizar:

1. Ficha del alumno en solicitud de admisión a los cursos de Formacion.
2. Documentos de las encuestas de satisfacción.
3. Formulario de recogida de datos de las personas usuarias. *(Centros de usuarios)*
4. Listado de asistentes a la visita de Institutos, Colegios, otras entidades.
5. Registro inicial para orientación.

Así, por ejemplo, un formulario para la recogida de datos de la ficha del alumno/a de solicitud de admisión a los cursos de Formacion, deberá incluir una cláusula como sigue:

> Conforme a **la Ley Orgánica 15/1.999, de Protección de Datos de Carácter Personal**, le informamos que:
>
> 1. Sus datos personales recogidos en este documento, cualesquiera otros que nos puedan ser proporcionados con posterioridad con motivo de las relaciones que mantenga con **FORMACIONL,** serán incorporados a un fichero titularidad de **FORMACIONL.**
> 2. La finalidad para la que se recogen es la de gestión y control de los datos personales relativos a las personas que se inscriben en los cursos de formación.
> 3. Los datos incorporados a estos ficheros no serán comunicados a terceros ni siquiera para su conservación, sin perjuicio de aquellas cesiones que fueren consentidas por la persona interesada en cada caso o que estuvieren previstas o autorizadas a la Administración por Ley o aquellos supuestos en los que nos autorice expresamente.

4. Si desea podrá ejercer los derechos de acceso, rectificación, cancelación y oposición solicitándolo por escrito, previa acreditación de su identidad, a FormacionL, en la siguiente dirección: Calle FormacionL 1 SEVILLA.

Para poder cumplir con el deber de informar, a través de medíos telefónicos, se aconseja que el que atienda a la llamada por parte de FORMACIONL lea con claridad a la persona interesada, la siguiente cláusula informativa (acorde con el Art. 5 LOPD):[1]

"Le informamos que para poder recabar la información de la persona interesada, , necesitamos grabar esta llamada para tratar los datos personales, con el fin de rellenar una ficha y abrir un expediente. Estos datos formaran parte de un fichero propiedad de la FormacionL, con la siguiente dirección: FormacionL 11 SEVILLA. Los datos serán utilizados con la finalidad mencionada.

En cumplimiento de la Ley Orgánica 15/1999, de Protección de Datos Personales, tiene derecho a acceder a este fichero para solicitar información, rectificación, oposición o cancelación de sus datos. Sólo tiene que indicárnoslo por escrito, acreditando su identidad."2.3Clausulado del Art.5 y el Derecho de información para las personas usuarias del servicio de "AUTORIENTACION" de FORMACIONL y Advertencias legales.

Cláusula a incluir en la aplicación de las áreas de autoorientación. Se puede reutilizar para cualquier otra funcionalidad parecida.

En cumplimiento de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y su normativa de desarrollo, le informamos que los datos personales facilitados por usted para acceder serán incorporados a un fichero automatizado cuyo responsable y titular es **FORMACIONL.**

[1] En caso de no poder garantizar la grabación y su correcto archivo y almacenamiento, sólo se recabe el consentimiento por medios escritos

Puede ejercitar los derechos de acceso, rectificación, cancelación y oposición solicitándolo por escrito, previa acreditación de su identidad, a la Dirección de FormacionL, en la siguiente dirección: Calle FormacionL SEVILLA

6.4.3.- Anexo del artículo 6 y 11 LOPD: CONSENTIMIENTO y COMUNICACIÓN

Cuando los datos se recaben directamente de la persona interesada por medio de una entrevista personal, se puede entender que este da su consentimiento de forma tácita, al ser él mismo el que nos facilita la información, siempre que se hayan cumplido los principios que establece la LOPD para el tratamiento de datos, es decir, siempre que además se cumpla con el deber de información del artículo 5 y adecuación de los datos del artículo 4 LOPD.

Así, en función del caso específico, deberá analizarse cuando es necesario obtener el consentimiento del titular de los datos y cuando no lo es.
Por otra parte, no es necesario recabar el consentimiento de los empleados para realizar el tratamiento de sus datos con la finalidad del mantenimiento de su relación contractual. Se trata de un supuesto encuadrado dentro de las excepciones al consentimiento que establece el artículo 6.2 LOPD (*"No será preciso el consentimiento cuando los datos de carácter personal se refieran a las partes de una relación laboral y sean necesarios para su mantenimiento o cumplimiento"*).

6.4.3.1.- Cláusula para recabar el Consentimiento por escrito

FORMACIONL, debe por lo tanto solicitar el consentimiento en aquellos casos en los que sea necesario. Para facilitar la tarea de identificar cuando se debe solicitar el consentimiento y cuando este se entiende tácito o presunto, especificar, que para los programas donde las personas beneficiarias sean los pertenecientes a **colectivos especiales**, será siempre necesario a la hora de recabar la información, solicitar el consentimiento de manera expresa, al tratarse datos especialmente protegidos, como el origen racial, o la salud, con un nivel de medidas de protección Alto.

CONSENTIMIENTO PARA COMUNICACIÓN DE DATOS A TERCEROS

En _____, a ____ de _____ de 201_

A los efectos previstos en la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal y en cumplimiento de los artículos 6 y 11 del citado cuerpo legal, **FORMACIONL,** solicita a

D. /Dª....., su consentimiento para proceder a la comunicación de sus siguientes datos:

* (___incluir los datos que se comunican__)

* Otros (Ver qué datos pide el tercero y facilitar exclusivamente los necesarios, específicamente profesionales y estrictamente relacionados con la finalidad de la comunicación solicitada)

Los datos van ser comunicados a (____incluir el nombre de la empresa, banco, otra, FormacionL, etc. ____), con la finalidad de (_____explicar la finalidad de modo general_____)

1. Podrá revocar su consentimiento en cualquier momento y ejercitar los derechos de acceso, impugnación, rectificación, cancelación u oposición de sus datos deberá dirigirse por escrito, previa acreditación de su identidad, a la FORMACIONL, con la siguiente dirección: FormacionL 11 SEVILLA

Yo, D/Dª (nombre y apellidos), D.N.I. nº: **.....,** habiendo sido informado/a sobre la comunicación de datos que antecede, expreso por la presente mi consentimiento.

Fdo: Nombre y apellidos.

6.4.3.2.- Cláusula para recabar el consentimiento de los trabajadores en los reconocimientos médicos voluntarios.

Cláusula que deberá de incluirse en unos nuevos documentos que sustituirían al actual que tiene **FORMACIONL**, titulado "Negativa a pasar un reconocimiento médico" :

EMPRESA: **FORMACIONL**

CENTRO DE TRABAJO: Calle FormacionL SEVILLA

LOCALIDAD: SEVILLA FECHA: _____

Documento de renuncia/consentimiento informado para la realización de examen de salud, en cumplimiento de la obligación empresarial contenida en el artículo 22 de la Ley de Prevención de Riesgos Laborales

D./Dª. (Nombre y apellidos del trabajador)

Estimado señor/a:

La Ley 31/1995, de 8 de noviembre, de Prevención de Riesgos Laborales (BOE del 10 de noviembre de 1995), en su artículo 22, establece la obligación del empresario de garantizar la vigilancia periódica del estado de salud a cada trabajador a su servicio. Ello, en función de los factores de riesgo en el trabajo que no hayan podido ser eliminados y a los que el trabajador pudiera estar expuesto.

Para cumplir dicha obligación, tanto el mencionado artículo de la citada Ley, como el apartado 3 del artículo 37 del RD 39/1997, de 17 de enero, Reglamento de los Servicios de Prevención (BOE de 31 de enero de 1997) determina que, entre otras actuaciones, se ha de someter al trabajador a exámenes, es decir, a reconocimientos o pruebas, que permitan, preventivamente, evitar que la salud se vea alterada como consecuencia de la exposición a dichos factores de riesgo.

Tales exámenes, reconocimientos o pruebas necesarias para la vigilancia y control de la salud, se llevarán a cabo causando las menores molestias al trabajador, y siempre que éste preste su consentimiento, garantizando el derecho a su intimidad, a su dignidad personal y a la protección de sus datos personales.

Así, en cumplimiento de lo establecido en la mencionada normativa, le comunicamos que sus reconocimientos médicos de la FormacionL (exámenes médicos para la vigilancia de la salud del empleado) son de carácter voluntario, por lo que requerimos de Vd. el consentimiento expreso para realizar el citado reconocimiento médico con el Servicio de Prevención Ajeno contratado, con la Sociedad de Prevención de **FRE** en virtud del Concierto de la actividad preventiva de riesgos laborales, suscrita con FORMACIONL.

Asimismo, de acuerdo con la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal (LOPD), le informamos que en caso de acceder, los resultados de dichos reconocimientos serán tratados en **FRE** con la finalidad de la vigilancia de su salud.

Desde el punto de vista del ejercicio de los derechos de acceso, rectificación y cancelación de sus datos médicos que le reconoce la LOPD, Vd. podrá ejercitarlos mediante escrito dirigido a la Sociedad de Prevención de **FRE** en la siguiente dirección: (*Calle, número, CP, localidad, provincia*).

En virtud de lo anteriormente expuesto, requerimos que preste su consentimiento expreso, o por el contrario, manifieste su expresa renuncia a que se le efectúen las pertinentes pruebas médicas de carácter preventivo que materializarán su derecho a una protección eficaz de su seguridad y de su salud y el cumplimiento de la correspondiente obligación del empresario, firmando y haciendo constar, de su puño y letra su nombre, apellidos, nº de DNI en el espacio 1 ó 2 correspondiente a la decisión adoptada.

1. Presto expresamente mi CONSENTIMIENTO a ser sometido a un examen de salud por FRE en los términos legal y reglamentariamente establecidos en la normativa vigente de Prevención de Riesgos Laborales. Firma: Nombre:	**2. Renuncio expresamente** a ser sometido a un examen de salud por FRE, en los términos legal y reglamentariamente establecidos en la normativa vigente de Prevención de Riesgos Laborales. Firma: Nombre:

Apellidos: Puesto de trabajo:	Apellidos: Puesto de trabajo:

En este sentido, recordamos que los resultados médicos sólo serán comunicados al empleado por FRE y FORMACIONL, por el contrario, sólo será informado de las conclusiones que se deriven de los reconocimientos efectuados (apto/no apto) en relación con la aptitud del trabajador para el desempeño del puesto de trabajo o con la necesidad de introducir o mejorar las medidas de protección y prevención, a fin de que puedan desarrollar correctamente sus funciones en materia preventiva.

6.4.3.3.- El procedimiento de disociación en la recogida y entrega de los datos.

En principio, y según el régimen de las cesiones de datos contenido en el art. 11 de la LOPD será necesario recabar el previo consentimiento de la persona interesada para poder comunicar los datos en cuestión. Asimismo, aquél a quien se comuniquen los datos queda obligado a observar las disposiciones de la LOPD.

No obstante, si antes de realizar esta comunicación sometemos los datos a un procedimiento de disociación, no deberemos aplicar lo anterior pues la disociación nos permitiría la comunicación de los mismos, sin la necesidad de recabar el previo consentimiento del afectado.

Disociar es eliminar los datos que identiquen a una persona: nombre, nif,..

6.4.4.- Anexo del Art.10 LOPD: DEBER DE SECRETO

6.4.4.1.- Cláusula de Confidencialidad del Correo Electrónico/Fax.

En relación con el DEBER DE SECRETO, y al tener la consideración de datos de carácter personal las direcciones de correo electrónico, el pie de firma de todos los integrantes de **FORMACIONL** que figure en el envío de los e-mails o igualmente de los faxes, deberá consignar este deber de confidencialidad de los datos y la adecuación del tratamiento de estos a la LOPD.

A tal fin, se utilizará esta clausula:

El presente correo electrónico/fax[2] ha sido enviado por la FORMACIONL. En cumplimiento de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, ponemos en su conocimiento que los datos incluidos en este mensaje están exclusivamente dirigidos al destinatario o destinatarios designados, por lo que si lo ha recibido por error, le rogamos nos lo haga saber a la mayor brevedad posible, y elimine inmediatamente el original, no estando permitido hacer ningún uso del mensaje.

Asimismo, ponemos en su conocimiento la posibilidad de ejercer sus derechos de acceso, rectificación, cancelación y especificación, en los términos establecidos en la legislación vigente, que podrá hacer efectivos dirigiéndose por escrito, acreditando su identidad, a la FORMACIONL, en la siguiente dirección: Calle FormacionL SEVILLA

[2] Dejar lo que proceda en cada caso.

6.4.4.2.- Confidencialidad del Correo Electrónico del personal de FORMACIONL.

El uso del correo electrónico por parte del personal de FORMACIONL ha de ser considerado como herramienta de trabajo puesta a disposición del trabajador y en base a unos criterios ciertos analizados en un contexto que al mismo tiempo que determina los límites que sean necesarios, permita la ejecución de las tareas asignadas, sin vulneración de los derechos fundamentales de la persona.

En conclusión, podemos señalar que el artículo 20.3 del Estatuto de los Trabajadores habilita al Empresario a controlar el correo electrónico que él otorga a los trabajadores para el desarrollo de sus funciones, pero siempre que previamente haya informado sobre dicho extremo y cumpla de ese modo el deber de informar previsto en el artículo 5.1 de la Ley Orgánica 15/1999.

El personal de FORMACIONL deberá asumir y responsabilizarse de la política y las medidas recogidas en el Documento de Seguridad respecto al uso y tratamiento del correo electrónico con dominio corporativo.

6.4.4.3.- Cláusula del deber de Secreto: COMPROMISO DE CONFIDENCIALIDAD

En **FORMACIONL**, la actividad diaria requiere, además de la intervención directa del personal propio, la colaboración de distintos tipos de profesionales que van a integrar el equipo de orientadores, formadores o educadores, empresas de seguridad, reciclaje de papel, etc. Todos ellos, en algún momento, acceden o pueden tener acceso a los sistemas de información o documentación que contienen datos personales de los alumnos o las personas usuarias de **FORMACIONL.**

COMPROMISO DE CONFIDENCIALIDAD

El abajo firmante, D._____, número de empleado: ____, con D.N.I. _____ y domicilio en _____, en el marco de la relación (___laboral__) que le une con la **FORMACIONL**, en orden a

dar cumplimiento efectivo a la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, expone que:

1. Se compromete a no revelar a persona alguna ajena a **FORMACIONL**, sin autorización expresa, la información y en especial la relativa a datos de carácter personal, a la que haya tenido acceso en el desempeño de sus funciones, excepto en el caso de que ello sea necesario para dar debido cumplimiento a las obligaciones del abajo firmante o de **FORMACIONL**, impuestas por las leyes o normas que resulten de aplicación, o sea requerido para ello por mandato de la autoridad competente con arreglo a Derecho.
2. No utilizará la información a que alude el apartado anterior, únicamente en la forma que exija el desempeño de sus funciones en **FORMACIONL** y no disponer de ella de ninguna otra forma o finalidad.
3. No utilizar en forma alguna, cualquier otra información que hubiese podido obtener prevaliéndose de su condición[3] de (__empleado/ colaborador__) de la FormacionL, y que no sea necesaria para el desempeño de sus funciones en **FORMACIONL.**
4. Cumplirá en el desarrollo de sus funciones en **FORMACIONL** con la normativa vigente, nacional y comunitaria, relativa a la protección de datos de carácter personal y, en particular, la Ley Orgánica 15/1999, de 13 de diciembre, disposiciones complementarias o cualquier otra norma que las sustituya en un futuro.
5. Cumplirá los compromisos anteriores incluso después de extinguida, por cualquier causa, (Ej: la relación laboral) que le une con **FORMACIONL.**
6. (El empleado/profesional)[8] firmante es consciente de que el ordenador, el correo electrónico, Internet, así como cualesquiera otros dispositivos, teléfonos móviles, soportes electromagnéticos, etc. son herramientas de trabajo que

[3] Indicar la condición, (Empleado, personal Auxiliar, Profesionales)

pone **FORMACIONL** a su disposición y que pueden, en caso de necesidad, ser inspeccionados en el modo y forma que se acuerde y se le comunique por **FORMACIONL.**

7. (El empleado/profesional)[4] ha sido debidamente informado de que sus datos del carácter personal, forman parte de un fichero titularidad de **FORMACIONL,** con la finalidad de llevar a cabo la gestión y control del personal empleado por **FORMACIONL**. Con idénticas finalidades el empleado consiente en la cesión o comunicación a terceros de sus datos en los supuestos contemplados por Ley. Los derechos de acceso, rectificación, cancelación u oposición, pueden ser ejercitados por escrito, previa acreditación de identidad, en la **FORMACIONL,** en la siguiente dirección: Calle FormacionL SEVILLA.
8. (El empleado/profesional)[8] conoce que **FORMACIONL** necesita incluir eventualmente las imágenes-fotografías en (__especificar el medio__) para uso interno o externo. A tal fin determina que NO [ ] SI [ ] (marcar la casilla que proceda) consiente y autoriza el tratamiento de su imagen con las finalidades antedichas.
9. El abajo firmante se hace responsable frente a **FORMACIONL** y frente a terceros, de cualquier daño que pudiera derivarse para unos u otros, del incumplimiento de los compromisos anteriores y resarcirá a **FORMACIONL** de las indemnizaciones, sanciones o reclamaciones que ésta se vea obligada a satisfacer como consecuencia de dicho incumplimiento.

La infracción de este deber de confidencialidad, independientemente de las sanciones administrativas a que puede dar lugar conforme a la Ley Orgánica de Protección de Datos de Carácter Personal, que configura la vulneración del deber de secreto respecto a los datos de carácter personal, dependiendo del tipo de dato revelado, como falta leve, grave o muy grave, sancionada con multa que van desde

[4] Colocar uno u otro dependiendo de si la persona es profesional ajeno o personal propio de FORMACIONL

los 601,01 € a 601012,10 €, puede dar lugar a responsabilidad penal tipificada en el Titulo X del Libro II del vigente Código Penal.

Y para que surta plenos efectos, declaro conocer el presente documento de compromiso de confidencialidad y de conformidad plena con su contenido lo firmo en SEVILLA, a __ de _____ de 201_.

Fdo: (El nombre del empleado/profesional) D.N.I._____

6.4.4.4.- Cláusula del deber de información y consentimiento para la recogida de imágenes como dato personal

Para los supuestos en que la FormacionL necesite solicitar consentimiento al personal, se utilizará un formulario que contenga el siguiente contenido:

Le informamos conforme a la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD), que los datos que nos facilita serán incluidos en un fichero, titularidad de la FORMACIONL.

FORMACIONL recoge imágenes (fotos) de las personas que prestan servicio en sus instalaciones para dar a conocer los eventos, actos, jornadas, etc., a través de distintos medios de comunicación propios, Intranet y página Web y a otros medios de comunicación de terceros, a los que se ceden las imágenes. Igualmente recoge imágenes con la finalidad de realizar entrevistas personales en el ámbito de la formación y para la información y divulgación de distintas actividades relacionadas con los fines y objetivos de sus Estatutos.

Usted consiente[5] y autoriza expresamente a FORMACIONL (marcar la casilla que proceda):

SI [ ]

NO [ ]

en el tratamiento, cesión y comunicación de su imagen con las finalidades antedichas.

En cualquier momento, usted tiene derecho a acceder, rectificar, oponerse y cancelar los datos referentes a su persona dirigiendo su solicitud firmada y por escrito, previa acreditación de identidad, a FORMACIONL, en la siguiente dirección: .

[5] Marque la casilla que proceda. En caso de no marcar ninguna casilla FORMACIONL entenderá que SI consiente, sin perjuicio de la revocación de su consentimiento por escrito en cualquier momento.

6.4.5.- Anexo del Art. 12 LOPD: ACCESO A LOS DATOS POR TERCEROS

La realización de tratamiento por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, en el que se deberán contemplar los requisitos exigidos por el antedicho artículo 12 de la LOPD.

6.4.5.1.- Contratos con terceros que tratan datos de FORMACIONL

En este apartado se analizan las relaciones contractuales suscritas o no en documento escrito, por **FORMACIONL** relacionadas con acceso a información de carácter personal que se encuentra afectada por la normativa en materia de protección de datos (LOPD). En concreto, se refiere a los servicios prestados por terceras empresas a través de contratos de arrendamientos de servicios que impliquen necesariamente un acceso a datos de carácter personal y responsabilidad de **FORMACIONL.** [6]

Así pues, como se ha expuesto, la Ley exige la forma escrita como requisito esencial. Este incumplimiento supone un elevado riesgo de sanción. por lo que respecta a **FORMACIONL**.

"PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL Y CONFIDENCIALIDAD DE LA INFORMACIÓN

[6] Así, quedan fuera del presente análisis los proyectos y servicios realizados donde no se requiera acceder a datos personales, o se trabaje con datos ficticios o disociados de FORMACIONL

1. El contratista (Encargado del Tratamiento de los Datos) se compromete expresamente a cumplir la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y, en particular a lo dispuesto en el artículo 12 de dicho texto legal e igualmente y a las obligaciones exigidas por el R.D. 1.720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de Desarrollo de la LOPD. El contratista tendrá acceso a datos de los ficheros propiedad de la **FORMACIONL**, a los únicos y específicos fines de la ejecución de los servicios objeto del presente contrato.

Todo el material al que tenga acceso el contratista para prestar los servicios, contenga o no datos de carácter personal, se considera de carácter estrictamente confidencial a todos los efectos, y no podrá ser utilizado para fines distintos del estrictamente cumplimiento del presente contrato.

2. El contratista únicamente tratará los datos conforme a las instrucciones de **FORMACIONL** y no los aplicará o utilizará con un fin distinto al que figure en el presente contrato, ni los comunicará, ni siquiera para su conservación, a terceras personas y/o Entidades.

3. El contratista asume el compromiso de adoptar las medidas necesarias para que todo su personal asignado al objeto del presente contrato, conozca su deber de confidencialidad y secreto de los datos que trata y la responsabilidad personal derivada en caso de incumplimiento. El personal deberá ser plenamente consciente de que esta obligación de secreto es de carácter indefinido y le vincula incluso terminada la relación con el responsable del tratamiento.

Si se vulnerara la confidencialidad, **FORMACIONL** se reserva el derecho de proceder a la resolución anticipada del contrato por incumplimiento, sin perjuicio de iniciar las acciones jurídicas oportunas.

4. El contratista debe devolver a **FORMACIONL** o destruir todos los datos de carácter confidencial (tratamientos automatizados o no, incluidas copias de respaldo y/o seguridad) a los que tenga acceso una vez finalizado el servicio contratado, sin conservar copia alguna de los mismos. Se hará efectiva esta medida también a cualquier fichero o soporte intermedio utilizado durante el tratamiento.

5. El contratista se compromete a adoptar las medidas técnicas y organizativas, necesarias para garantizar la seguridad de los datos de carácter confidencial de **FORMACIONL** y evitar así su alteración, divulgación, pérdida, tratamiento o acceso no autorizado a los mismos, teniendo en cuenta el estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, provengan éstos de la acción humana o del medio físico o natural, de conformidad con la normativa vigente en la materia y sobre todo en consideración al nivel de medidas de seguridad de los datos recogidos en soporte físico, que en este caso son de nivel (DETERMINAR ENTRE BÁSICO/MEDIO/ALTO).

Específicamente se determinan de aplicación al caso concreto, las siguientes: (__).

6. Las incidencias que se produzcan y que supongan un riesgo para la confidencialidad, integridad o disponibilidad de los datos de carácter personal a los que tiene acceso deberán ser comunicadas inmediatamente a **FORMACIONL**, a ser posible en el mismo día en que tenga lugar la incidencia.

7. El contratista no podrá en ningún caso duplicar o reproducir ningún dato de carácter personal de **FORMACIONL**, ni utilizarlos de manera diferente a la que imponga la estricta prestación de los servicios contratados. En el caso de que el contratista destine los datos a otra finalidad, los comunique o los utilice incumpliendo lo dispuesto en el presente contrato, será considerado a su vez Responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente.

8. El contratista deberá colaborar con **FORMACIONL** en la gestión de la Tutela de Derechos de las personas interesadas. Estos derechos son los contemplados en los artículos 15 y siguientes de la LOPD, relativos al acceso, rectificación, cancelación y oposición a los datos de carácter personal y su tratamiento.

Para ello, el contratista tendrá que realizar aquellas operaciones sobre los datos de carácter personal que les sean requeridas por **FORMACIONL** a tenor de las solicitudes de ejercicio de derechos que se produzcan.

11. **FORMACIONL** podrá exigir al contratista previamente a la contratación, la presentación del informe de la Auditoria Bienal exigida por la normativa vigente."

6.4.5.2.- Contratos con Terceros que no acceden a datos pero si a los Centros o a la Dirección General.

Cuando se trate de personal ajeno, **el contrato de prestación de servicios recogerá expresamente la prohibición de acceder a datos personales y la obligación de secreto** a los datos que el personal hubiera podido conocer con motivo de la prestación de servicio.

A tal fin hay que utilizar la siguiente cláusula

Cláusula del artículo 83 del RLOPD

Las partes firmantes declaran que, en virtud del servicio concertado a través del contrato no se comunica ni se accede a datos de carácter personal de los ficheros de los que es responsable **FORMACIONL.** No obstante queda expresamente prohibido que el personal de (____)[7] acceda a los datos personales que se encuentren en los centros o instalaciones y/o sistemas informáticos de **FORMACIONL.**

(____)[8] se obliga a exigir al personal propio destinado y/o designado, el deber de secreto respecto de los datos que hubiera podido conocer con motivo de la prestación de servicio conforme a las exigencias del artículo 10 LOPD.

[7] Insertar el nombre del tercero sin acceso a datos

[8] Idem

6.4.5.3.- Contratos en los que FORMACIONL es Encargado de Tratamiento

En estos casos es **FORMACIONL** quien presta un servicio a algún cliente y esa prestación de servicio supone un acceso a datos y un tratamiento por cuenta de ese tercero, por lo que con arreglo a lo anterior, deberá firmarse igualmente un contrato del art. 12 LOPD por escrito.

A tal fin hay que utilizar la siguiente clausula

ANEXO al contrato de (Nombre de la empresa)

RÉGIMEN DEL TRATAMIENTO DE DATOS DE CARÁCTER PERSONAL para ACCEDER A DATOS DE OTRO RESPONSABLE DE FICHERO

En _____ a_____de _____ de _____,

De una parte _____, con domicilio en _____, y CIF _____, (en adelante EL CLIENTE) representada en este acto por D. _____ apoderamiento que acredita en virtud de escritura de poder otorgada a su favor el día _____ante Notario de _____ D. _____ con el número _____ de su protocolo y,

De otra parte, la **FORMACIONL** con C.I.F. nº _____, domiciliada en C/ _____, inscrita en el Registro de Empresas _____, tomo ____, Libro _, Folio __; Hoja _____, representada en este acto por D. _____, apoderamiento que acredita en virtud de escritura de poder otorgada a su favor el día _____ ante el Notario de _____ D. _____ con el número _____ de su protocolo,

Ambas partes se reconocen mutuamente la capacidad para suscribir el presente acuerdo y cumplir las obligaciones derivadas del mismo.

MANIFIESTAN QUE:

PRIMERO: que en <LA FECHA> (__EL CLIENTE__) adjudicó un contrato a FORMACIONL con el objetivo de <EXPLICACIÓN DE LA OFERTA>.

SEGUNDO: Que las partes convienen la necesidad de mejorar la regulación de su relación jurídico-mercantil con una serie de cláusulas accesorias, a efectos de que entre ambos se de cumplimiento a la legislación vigente y la normativa en materia de protección de datos personales. Con dicho fin establecen los siguientes

PACTOS:

PRIMERO. Deber de secreto y confidencialidad.

Las partes acuerdan proteger el secreto de la información que EL CLIENTE suministre a **FORMACIONL** o a las que **FORMACIONL** pueda acceder durante el desarrollo del contrato.

En especial, toda la información relativa a datos personales de EL CLIENTE y a los trabajos ejecutados para (__EL CLIENTE__) será considerada como información confidencial.

SEGUNDO. Protección de datos personales

La prestación de servicios por parte de **FORMACIONL** a (__EL CLIENTE__) implica necesariamente el acceso por el primero a datos de carácter personal de los que es responsable (__EL CLIENTE__) que, en cualquier caso, deben protegerse de conformidad con lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre,

de Protección de Datos de Carácter Personal (en adelante LOPD) y demás normativa de desarrollo.

1. EL CLIENTE en su calidad de responsable de los ficheros de datos personales declara y garantiza frente a **FORMACIONL** que los datos de carácter personal que se dispone a comunicar en virtud de la prestación del servicio contratado, han sido íntegramente obtenidos y tratados de forma legal y de conformidad a lo establecido en la LOPD, y que forman parte de los ficheros que tiene inscritos en el Registro General de la Agencia de Protección de Datos. Por ello, **FORMACIONL** no asume ni se responsabiliza de cuántas obligaciones y/o sanciones pudieran derivarse por incumplimientos de la normativa de protección de datos en los que pudiera incurrir o hubiera incurrido (__EL CLIENTE__) como responsable de los referidos datos.

2. **FORMACIONL** tratará de modo confidencial cualesquiera datos e información de carácter personal que le sean proporcionados por (__EL CLIENTE__) con motivo de la prestación de los servicios. En este sentido, **FORMACIONL** como encargado del tratamiento de los datos a los que accede en virtud del objeto de la contratación, declara que:

- Tiene debidamente inscritos en el Registro General de la Agencia Española de Protección de Datos, los ficheros automatizados y no automatizados
- Tiene su Documento de Seguridad, actualizado y adecuado a lo dispuesto por el artículo 88 del Reglamento.
- Su personal conoce y es consciente de la obligación y deber de guardar secreto respecto de los datos personales a los que acceda.
- Aplica las medidas de seguridad correspondientes en función de la naturaleza de los datos y el tratamiento correspondiente, que en este caso son de nivel (BÁSICO/MEDIO/ALTO)[9]

[9] Elegir la que proceda y eliminar el resto.

- Que en función de esos datos y de las medidas de seguridad determinadas **FORMACIONL** aplica las siguientes específicamente**:**

  - ✓ Definición y comunicación de funciones y obligaciones del personal, tal y como establece el artículo 89 del mencionado texto legal.(__especificar las que procedan__)
  - ✓ Registro de incidencias, según lo previsto en el artículo 90 del Real Decreto.
  - ✓ Procedimiento de identificación y autenticación, a tenor de lo establecido en el artículo 93 del Reglamento de desarrollo de la LOPD
  - ✓ Control y Registro de accesos ajustado al artículo 91 del Reglamento.
  - ✓ Gestión de Soportes en cumplimiento del artículo 92.
  - ✓ Gestión de copias de respaldo y recuperación ajustada al artículo 94 del Real Decreto.

TERCERO. Duración y resolución del acuerdo.

El presente Acuerdo entrará en vigor en la fecha de su firma y tendrá una duración indefinida. Para el supuesto que cualquiera de las partes desistiese unilateralmente del contrato de prestación de servicios al que se hace mención en el primer manifestando de este documento, las obligaciones de confidencialidad y relativas al tratamiento de datos personales no se verán resueltas y tendrán plena efectividad durante el tiempo establecido en el presente acuerdo. El deber de secreto respecto de los datos tratados será de duración indefinida.

CUARTO. Ley aplicable y jurisdicción.

El presente Acuerdo se regirá por la Ley Española.

Las partes intervinientes, con renuncia expresa a su propio fuero, se someten a la jurisdicción y competencia de los Juzgados competentes territorialmente para cuantas cuestiones o litigios se susciten con motivo de la interpretación, aplicación, cumplimiento o incumplimiento del presente Acuerdo.

En prueba de lo cual, las partes firman el presente Acuerdo en dos ejemplares y a un solo efecto en el lugar y fecha indicados en el encabezamiento.

En (__ciudad__), en (__fecha__):

6.4.6.- Procedimiento para la atención al ejercicio de derechos

6.4.6.1.- Circular Informativa

MODELO DCIRCULAR INFORMANDO DEL PROCEDIMIENTO A SEGUIR EN EL EJERCICIO DE DERECHOS EN MATERIA DE PROTECCIÓN DE DATOS

1.- INTRODUCCIÓN.

La Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante LOPD), dedica los artículos 15 y siguientes a los derechos de acceso, rectificación, cancelación, y los artículos 30.4 y 31.3 al nuevo derecho de oposición. Tales derechos se configuran como uno de los ejes fundamentales sobre los que se articula la protección al honor, la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos, en desarrollo de lo dispuesto en el artículo 18.4 de la Constitución Española.

La presente circular tiene por objeto aclarar las disposiciones relativas a los derechos de los afectados, así como servir de punto de partida para establecer el procedimiento que debe seguirse ante las solicitudes de los mismos por los diversos canales de entrada, ya sean de acceso, rectificación, cancelación u oposición; analizando los plazos establecidos legalmente para su contestación y los requisitos de contenido mínimo que deberán de reunir las solicitudes de los afectados.

Deberá tenerse en consideración, para el correcto ejercicio de los derechos, las siguientes definiciones que establece la LOPD:

- ✓ *Responsable del Fichero o tratamiento*: persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento.
- ✓ *Agencia Española de Protección de Datos (AEPD)*: Organismo Oficial Estatal que regula y controla el cumplimiento de la Ley y la protección de los

derechos de los ciudadanos. La Ley dedica su Título VI a la regulación de este ente de derecho público.

- ✓ *Afectado o persona interesada*: persona física titular de los datos que sean objeto de tratamiento.
- ✓ *Derecho de consulta*: Es el Derecho a conocer la existencia de ficheros automatizados de datos de carácter personal, sus finalidades y la identidad del responsable del tratamiento. Este derecho se ejercita ante el Registro General de la Agencia Española de Protección de Datos, recabando la información oportuna. (el Registro se compone de todos los ficheros públicos y privados inscritos en la Agencia Española de Protección de Datos).
- ✓ *Derecho de Acceso*: Derecho de la persona interesada a solicitar y obtener información de sus datos de carácter personal incluidos en los ficheros, el origen de los mismos, así como las comunicaciones realizadas o que se prevean realizar.
- ✓ *Derecho de rectificación y cancelación:* Derecho de la persona interesada a que sus datos de carácter personal sean rectificados o cancelados, en su caso, cuando su tratamiento no se ajuste a lo dispuesto en la Ley. Especialmente, cuando sean inexactos, incompletos, inadecuados, excesivos.
- ✓ *Derecho de oposición*: Se trata del derecho a no utilizar sus datos con fines de publicidad y prospección comercial.

Se ha designado como Servicio de Atención al ejercicio de los derechos de **FORMACIONL**, que se encargará de contestar todas las solicitudes de estos derechos de tutela de la LOPD.

Por ello, todos los trabajadores de **FORMACIONL** que en su labor diaria traten datos de carácter personal, deberán conocer y seguir el procedimiento que se expone a continuación para el correcto cumplimiento de dichas obligaciones.

2.- PROCEDIMIENTO A SEGUIR PARA EL EJERCICIO DE LOS DERECHOS DE ACCESO, RECTIFICACIÓN, CANCELACIÓN Y OPOSICIÓN DE LAS PERSONAS INTERESADAS

La Ley prevé que cualquier persona física incluida en un fichero tiene derecho a acceder, rectificar, cancelar u oponerse al tratamiento de sus datos de carácter personal. Del mismo modo, la Ley configura el ejercicio de derechos como independientes – de tal forma que no se puede entender que el ejercicio de alguno de ellos sea requisito previo para el ejercicio de otro- y personalísimos – es decir, sólo pueden ejercitarse por el titular de los datos -. Existen dos excepciones donde se permite el ejercicio de derechos por parte del representante legal del afectado: incapacidad y minoría de edad; para atender estos casos, deberá tenerse en cuenta el punto 3 de la presente circular.

Como medida general cualquier solicitud o cuestión relacionada con el ejercicio del derecho de tutela, deberá ser tramitada internamente con carácter URGENTE. Así, cada Centro, Gerencia Provincial o Unidad Operativa remitirá a través de una persona designada expresamente al efecto, a la Dirección General a la atención de (____) los escritos, solicitudes, formularios, etc. que lleguen relacionados con el acceso, rectificación, oposición y cancelación de los datos personales.

A continuación se detalla el procedimiento que deben conocer **todos los trabajadores de FORMACIONL,** ante la solicitud de un ejercicio de derechos. Para la máxima comprensión de este procedimiento, se ha procedido a clasificar los medios en que pueden recibir dichas solicitudes.

1) Visita personal en las oficinas de atención de los derechos:

Calle FormacionL 11 Sevilla.

El personal que atienda la visita, le entregará un modelo de ejercicio de acceso, cancelación, rectificación u oposición, dependiendo de la solicitud de la persona interesada. Dichos formularios se anexan en esta circular.

a) Se deberá adjuntar copia del DNI (o cualquier otro medio de identificación válido en derecho), y documentación acreditativa de la petición que formula, en caso de poseerla y ser necesaria.

b) Si la persona interesada no firmara la solicitud, ésta no estuviera correctamente cumplimentada o no aporte la fotocopia de su DNI o pasaporte, se deberá solicitar la subsanación de los mismos. En caso de que dichos requisitos no fueran subsanados, se tramitará la solicitud igualmente y según el procedimiento establecido a continuación.

c) Una vez cumplimentada la solicitud deberá plasmarse el sello de la Corporación indicando la fecha de entrada de la solicitud. De esta forma, se controlará el cumplimiento de los plazos legales exigidos para el ejercicio de derechos.

Se exponen los plazos legales a modo de resumen:

Derecho ejercitado	**Plazo de contestación (a partir de la recepción de solicitud)**
Derecho de Acceso	Plazo de comunicación concesión/denegación del acceso: **1 mes** Plazo de comunicación efectiva de información: **10 días** siguientes a comunicación anterior.[10]
Derecho de Rectificación	**10 días**
Derecho de Cancelación	**10 días**
Derecho de oposición	**10 días**

d) En caso de que la persona interesada lo solicite, se le informará de que **FORMACIONL** procederá a contestar su solicitud, con independencia de que figuren o no datos personales del mismo en los ficheros.

e) Asimismo, debe informarse a la persona interesada que su contestación se hará efectiva como máximo en el plazo legal establecido, aunque siempre

que el volumen de trabajo lo permita, se intentará elaborar y entregar la carta contestación en un tiempo inferior. Los plazos legales de contestación aparecen reflejados en los modelos anexos.

f) En el supuesto que la persona interesada lo solicite, se le deberá entregar una copia sellada de la solicitud formulada, con el sello de entrada de **FORMACIONL**. Este hecho deberá informarse en el expediente.

2) Correo postal / Fax.

a) En el momento de entrada de una solicitud por escrito, deberá plasmarse el sello de la FormacionL indicando la fecha de entrada de la solicitud. De esta forma, se controlará el cumplimiento de los plazos legales exigidos para el ejercicio de derechos.

b) Deberá conservarse el sobre o documento en el que se haya efectuado el envío y anexarlo al expediente. En dicho soporte deberá plasmarse el sello de entrada con la fecha de recepción y se grapará a la solicitud formulada.

c) Las solicitudes y la documentación anexa a las mismas (fotocopia del DNI, documentación aportada por la persona interesada, etc.) deberán enviarse, en caso de recibirse por otra Dirección / Gerencia, el mismo día de su cumplimentación, con el sello de entrada y con indicación de la fecha de su presentación, a la Dirección / Gerencia designado para la atención al ejercicio de derechos por el siguiente medio..... (valija interna, etc.)

d) Los medios de recepción pueden ser: burofax, correo certificado, correo ordinario, acuse de recibo, fax, servicios de mensajería, etc.

4) Teléfono

a) En cuanto a las personas que solicitan el acceso, cancelación, rectificación u oposición, no se facilitará información telefónicamente. Se comunicará que para el ejercicio de sus derechos deberán dirigirse por escrito a la dirección del responsable del fichero (**FORMACIONL**), en la siguiente forma:

- ✓ Envío de petición expresa firmada y acompañada de la dirección a la que deba ser remitida la contestación (sólo por la persona interesada, salvo en los casos de representación legal en las excepciones de incapacidad o minoría de edad, que se especificarán en apartados siguientes).
- ✓ Deberá acompañar a su solicitud fotocopia del DNI o cualquier documento acreditativo de su identidad válido en derecho (pasaporte, carné de conducir, etc.).

b) En su caso, se informará de los medios a través de los que puede dirigir su petición, fundamentalmente deberá señalarse los establecidos en la Dirección / Gerencia designado para la atención al ejercicio de derechos.

c) Las llamadas informativas de contenido general respecto a la normativa relativa a Protección de Datos, deberán trasladarse a la Dirección / Gerencia designado para la atención al ejercicio de derechos o facilitar los medios (teléfono, correo, fax, etc.) para que la persona interesada se ponga en contacto con la mencionada Dirección / Gerencia.

5) E-mail

En caso de recepción de cualquier solicitud formulada por este medio, deberá remitirse contestación a su dirección de correo, facilitando la misma información reflejada en el apartado anterior para las solicitudes telefónicas (se trata de otro medio por el cual no puede acreditarse la identidad del afectado, salvo que adjuntara su DNI escaneado y pudiera corroborarse además que le identifica a través de cualquier otro medio, al mismo tiempo).

3.- TRATAMIENTO DE LOS REPRESENTANTES (EJERCICIO DE DERECHO POR PERSONA DISTINTA A LA PERSONA INTERESADA)

Conforme al artículo 23.2 del Real Decreto 1720/2007 y la Norma primera, apartado 1º párrafo 2º de la Instrucción 1/1998 se otorga a un representante, tanto legal como voluntario, la posibilidad de ejercer los derechos de tutela en nombre de otro: "*Podrá, no obstante, actuar el representante legal del afectado cuando éste se encuentre en situación de incapacidad o minoría de edad que le imposibilite el ejercicio personal de los mismos; en cuyo caso será necesario que el representante*

legal acredite tal condición". Para ello, la solicitud deberá reunir los siguientes requisitos:

- ✓ Documento acreditativo de la condición de representante del menor de edad o incapacitado.
- ✓ La solicitud deberá contener el nombre y apellidos del representante, domicilio a efectos de notificaciones, fecha, firma y petición en que se concreta la solicitud. A esta solicitud deberá acompañarse la fotocopia del DNI o pasaporte del representante y, en su caso, los documentos acreditativos de la petición que se formula.

Podrá actuar igualmente un representante designado por la persona interesada –representante voluntario o mandatario (por ejemplo, abogado)- siempre que se cumplan los requisitos establecidos, tanto la declaración de voluntad del afectado, como el negocio de apoderamiento:

Requisitos de la declaración de voluntad del afectado:

- ✓ El ejercicio de los derechos deberá efectuarse por el representante "en nombre y por cuenta" del afectado.
- ✓ Sólo al propio afectado corresponde la delimitación de los concretos términos en que el derecho pueda ser ejercitado en cada ocasión, partiendo del conocimiento de las circunstancias en cada caso concreto y de los diversos ficheros ante los que se quieran ejercitar los derechos.

Requisitos del apoderamiento:

- ✓ El apoderamiento deberá ser expreso y original (escrito del titular de los datos, facultando a su representante para recibir la carta contestación).
- ✓ Referido al concreto derecho que se pretende ejercitar.
- ✓ Con expresa mención del fichero ante el que tal derecho pretende ejercitarse.
- ✓ Expresa mención del objeto de cada actuación concreta.

Se adjuntará a la solicitud, la fotocopia del DNI o Pasaporte (no es válido el Carné de Conducir como documento identificativo y acreditativo de la identidad). Se acompañará la documentación acreditativa de la petición que formula en su caso.

Si la solicitud se realiza telefónicamente, se comunicará al afectado los requisitos exigidos y el plazo previsto para la respuesta a su solicitud.

4.- EJERCICIO DE DERECHOS DE LOS TRABAJADORES DE FORMACIONL

El procedimiento interno diseñado para el ejercicio de los derechos de los trabajadores de **FORMACIONL**, con el objetivo de evitar formalismos innecesarios (adjuntar documento acreditativo de su identidad) debido al volumen de empleados existente, y en aras de una mayor agilidad en su tramitación, es el siguiente:

- Todo empleado que pretenda ejercitar sus derechos, podrá dirigirse a la Dirección General Técnica, por alguno de estos dos canales:
  - Personalmente acudiendo a **FORMACIONL**
  - Mediante el e-mail corporativo: tuteladatos@FormacionL.pfc
- **FORMACIONL** facilitará a la persona interesada el modelo de solicitud, relativo al derecho que pretenda ejercitarse, el cual deberá ser cumplimentado y suscrito por el trabajador.
- Una vez contestado por **FORMACIONL,** se comunicará con la persona interesada para su recogida, firmando original y copia (la cual será archivada en su expediente) de la carta de contestación.
- Si el derecho ejercitado requiriera, a juicio de **FORMACIONL**, aportar documentación justificativa, la persona interesada será informado para que la anexe junto al modelo de solicitud cumplimentado.
- Los plazos de contestación a las solicitudes son los legales establecidos en el cuadro anterior.

5.- OTROS ASPECTOS

Para cualquier tipo de pregunta o duda sobre el procedimiento a seguir, deberán ponerse en contacto con **la FORMACIONL**, a través de los siguientes medios: ..... (Números de teléfono y direcciones de correo electrónico de los responsables designados para atender los derechos ejercitados, etc.).

6.4.6.2.- Modelos de solicitud de ejercicio de derechos

Se establecen los siguientes modelos. Los presentes modelos han sido elaborados para cualquiera de los diferentes colectivos de titulares de datos registrados en los ficheros de FORMACIONL. Los modelos estarán a disposición de las personas interesadas en todos los centros de FORMACIONL.

MODELO DE SOLICITUD DE DERECHO DE ACCESO

EJERCICIO DEL DERECHO DE ACCESO

Petición de información sobre los datos personales incluidos en el fichero

DATOS DEL FICHERO[11]

Nombre del fichero: _____ Código AEPD: _____

DATOS DEL RESPONSABLE DEL FICHERO O TRATAMIENTO

Nombre: FORMACIONL **Domicilio**: *Calle FormacionL 11 Sevilla.*

Oficina de Acceso: FORMACIONL

DATOS DEL SOLICITANTE

Nº de Empleado: ..... [12]

---

[11] Los datos del fichero serán modificados para cada uno de los ficheros restantes, insertando su correspondiente código de inscripción asignado por el RGPD, notificado a la AEPD.

[12] En otros ficheros diferentes a PERSONAL se sustituye este dato por el número de empleado, código de proveedor, etc.

D. / Dª....., mayor de edad, con domicilio en la C/..... nº....., Localidad..... Provincia..... C.P. ..... con DNI....., del que acompaña fotocopia[13], por medio del presente escrito manifiesta su deseo de ejercer su derecho de acceso, de conformidad con los artículos 15 de la Ley Orgánica 15/1999, de Protección de datos, y el artículo 28 del Real Decreto 1720/2007.

SOLICITA

1.- Que se le facilite el acceso al fichero en el plazo máximo de un mes a contar desde la recepción de esta solicitud, entendiendo que si transcurre este plazo sin que de forma expresa se conteste a la mencionada petición de acceso se entenderá denegada.

2.- Que si la solicitud del derecho de acceso fuese estimada, se remita por correo la información a la dirección arriba indicada en el plazo de diez días desde la resolución estimatoria de la solicitud de acceso.

3.- Que esta información comprenda de modo legible e inteligible los datos de base que sobre mi persona están incluidos en su fichero, y los resultantes de cualquier elaboración, proceso o tratamiento, así como el origen de los datos, los cesionarios y la especificación de los concretos usos y finalidades para los que se almacenaron.

En SEVILLA, a.....de.....de 2017

Fdo: .....

[13] La mención a copia del DNI, se deja como modelo, pero para los empleados deberá eliminarse.

MODELO DE SOLICITUD DE DERECHO DE RECTIFICACIÓN.

EJERCICIO DEL DERECHO DE RECTIFICACIÓN

Petición de corrección de datos personales inexactos o incorrectos objeto de tratamiento incluido en el fichero.

DATOS DEL FICHERO[14]

Nombre del fichero: _____ Código AEPD: _____

DATOS DEL RESPONSABLE DEL FICHERO O TRATAMIENTO

Nombre: FORMACIONL

Domicilio: *Calle FormacionL 11 Sevilla.*

Oficina de Acceso:

DATOS DEL SOLICITANTE

D/Dª..... mayor de edad, con domicilio en la calle..... nº....., Localidad ....., Provincia .....C.P. ..... con DNI....., del que acompaña fotocopia, por medio del presente escrito manifiesta su deseo de ejercer su derecho de rectificación, de conformidad con el artículo 16 de la Ley Orgánica 15/1999 de Protección de Datos, y los artículos 31 y 32 del Real Decreto 1720/2007.

SOLICITA

1. Que se proceda a la efectiva corrección en el plazo de diez días desde la recepción de esta solicitud, de los datos inexactos relativos a mi persona que se encuentren en su fichero.

---

[14] Los datos del fichero serán modificados para cada uno de los ficheros restantes, insertando su correspondiente código de inscripción asignado por el RGPD, notificado a la AEPD.

2. Los datos que hay que rectificar se enumeran en la hoja anexa, haciendo referencia a los documentos que se acompañan a esta solicitud y que acreditan, en caso de ser necesario, la veracidad de los nuevos datos.

3. Que me comuniquen de forma escrita a la dirección arriba indicada, la rectificación de los datos una vez realizada.

4. Que, en el caso de que **FORMACIONL** considere que la rectificación no procede, lo comunique igualmente, de forma motivada y dentro del plazo de diez días señalado.

En SEVILLA, a..... de..... de 2017

Fdo.....

ANEXO EJERCICIO DERECHO DE RECTIFICACIÓN

DATOS QUE DEBEN RECTIFICARSE:

DATO INCORRECTO	DATO CORRECTO	DOCUMENTO ACREDITATIVO
1)		
2)		
3)		
4)		
5)		
6)		
7)		
8)		
9)		
10)		
11)		

MODELO DE SOLICITUD DE EJERCICIO DE CANCELACIÓN

EJERCICIO DEL DERECHO DE CANCELACIÓN

DATOS DEL FICHERO[15]

Nombre del fichero: _____

Código AEPD: _____

DATOS DEL RESPONSABLE DEL FICHERO O TRATAMIENTO

Nombre: FORMACIONL

Domicilio: *Calle FormacionL 11 Sevilla.*

Oficina de Acceso:

DATOS DEL SOLICITANTE

Nº de Candidato: ..... [16]

D./ Dª ....., mayor de edad, con domicilio en la C/..... nº....., Localidad .....Provincia .....C.P. ..... con DNI....., del que acompaña fotocopia, por medio del presente escrito manifiesta su deseo de ejercer su derecho de cancelación, de conformidad con el artículo 16 de la Ley Orgánica 15/1999, de Protección de Datos, y los artículos 31 y 32 del Real Decreto 1720/2007.

SOLICITA

1. Que en el plazo de diez días desde la recepción de esta solicitud, se proceda a la efectiva cancelación de cualesquiera datos relativos a mi persona que se encuentren en su fichero, en los términos previstos en la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal y me lo comuniquen de forma escrita a la dirección arriba indicada.

---

[15] Los datos del fichero serán modificados para cada uno de los ficheros restantes, insertando su correspondiente código de inscripción asignado por el RGPD, notificado a la AEPD.

[16] En otros ficheros diferentes se sustituye este dato por el número de proveedor, empleado, etc.

2. Que, en el caso de que **FORMACIONL**, considere que dicha cancelación no procede, lo comunique igualmente, de forma motivada y dentro del plazo de diez días señalado.

En SEVILLA, a..... de..... de 2017

Fdo:.....

ANEXO EJERCICIO DERECHO DE CANCELACIÓN

DATOS QUE DEBEN CANCELARSE: (para el supuesto de cancelar sólo alguno de los datos registrados en el fichero)

DATO A CANCELAR	DOCUMENTO ACREDITATIVO
1)	SI/NO
2)	
3)	
4)	
5)	
6)	
7)	
8)	
9)	
10)	
11)	
12)	
13)	

6.4.6.3.- Contestación al ejercicio de derechos

Dicho modelo sirve para cualquiera de los ficheros existentes.

MODELO DE CONTESTACIÓN CONCESIÓN DERECHO DE ACCESO

SEVILLA, a __ de_____.de 2017

D. (nombre y apellidos del solicitante).

C/ (nombre de la calle, nº, portal, escalera).

C. P. (nº de código postal) - Población

EXP. (nº de expediente)

Muy Sr. /Sra. Nuestro/a,

Con relación a su petición registrada en la **FORMACIONL,** con fecha 00/00/00, en la que nos solicita el acceso a los datos que figuran en el fichero _____, referentes a su persona, le comunicamos que son los siguientes:

✓

✓

Asimismo, le informamos que sus datos, no han sido comunicados a ninguna entidad/han sido comunicados a las siguientes entidades:

Nombre de la entidad 1: _____

Dirección: _____

Nombre de la entidad 2: _____

Dirección: _____

Igualmente le informamos que los usos y finalidades previstos del fichero son: _____

Si usted considera que los datos anteriores son inexactos o incompletos podrá solicitar el derecho de rectificación o cancelación conforme a lo estipulado en el artículo 32 del Real Decreto 1720/2007, de 21 de diciembre, adjuntando a su solicitud documentación acreditativa de la rectificación a efectuar.

Por último, le rogamos haga referencia al número de expediente que figura en la carta, en cualquier comunicación posterior que desee realizar.

Atentamente,

FORMACIONL

Fdo:.....

MODELO DE CARTA DENEGANDO EL ACCESO/RECTIFICACIÓN/CANCELACIÓN DE MANERA PROVISIONAL

SEVILA, a __ de_____.de 2017

D. (nombre y apellidos del solicitante).

C/ (nombre de la calle, nº, portal, escalera).

C.P. (nº de código postal) - Población

EXP. (nº de expediente)

Muy Sr./Sra. Nuestro/a,

En contestación a su atento escrito registrado en **la FORMACIONL,** con fecha 00/00/00, en el que solicitaba el **acceso/rectificación/cancelación** de los datos

incluidos en el Fichero _____[17] relativos a usted, le comunicamos que para poder proporcionarle el mismo es necesario que[18]:

- ✓ Firme la petición.
- ✓ Acompañe a su escrito fotocopia del DNI.
- ✓ Hayan transcurrido doce meses desde la última petición sin que se acredite un interés legítimo (sólo en caso de acceso).
- ✓ Acompañe documentos acreditativos de la petición que formula.

Una vez subsanado ese requisito procederemos a atender su solicitud de acceso/rectificación/cancelación.

Así mismo, le rogamos haga referencia al número de expediente que figura en la carta, en cualquier comunicación posterior que desee realizar.

Por último, le informamos que, en cualquier caso, tiene derecho a recabar la tutela de la Agencia Española de Protección de Datos (Artículos 30.3 y 33.3 del Real Decreto 1720/2007, de 21 de diciembre) o, en su caso, de las autoridades de control de las comunidades autónomas, conforme a lo dispuesto en el artículo 18 de la Ley Orgánica 15/1999, de 13 de diciembre.

Atentamente,

FORMACIONL

Fdo:.....

[17] Se designará el fichero al que solicitó acceso/rectificación/cancelación.

[18] Detallar la deficiencia formal que motiva la denegación del acceso/rectificación/cancelación.

MODELO DE CARTA INFORMANDO DE LA RECTIFICACIÓN DE DATOS EFECTUADA

SEVILLA, a __ de_____ de 2017

D. (nombre y apellidos del solicitante).

C/ (nombre de la calle, nº, portal, escalera).

C. P. (nº de código postal) - Población

EXP. (nº de expediente)

Muy Sr./Sra. Nuestro/a,

De acuerdo con su petición de **rectificación** registrada en la **FORMACIONL,** con fecha 00/00/00, le comunicamos que tras las comprobaciones pertinentes hemos procedido a la rectificación de sus datos en el Fichero _____[19], en el sentido que nos indicó en su escrito. Los datos rectificados son los siguientes:

✓ ..

✓ ..

Asimismo le comunicamos que sus datos,

- no han sido comunicados a ninguna entidad
- han sido comunicados a las siguientes entidades:

- Nombre de la entidad 1: _____
- Dirección: _____
- Nombre de la entidad 2: _____
- Dirección: _____

Igualmente le informamos que los usos y finalidades previstos del fichero son: .....

_____

[19] Se designará el fichero al que solicitó rectificación.

Por último, le rogamos haga referencia al número de expediente que figura en la carta, en cualquier comunicación posterior que desee realizar.

Atentamente,

FORMACIONL

Fdo:.....

MODELO DE CONTESTACIÓN COMUNICANDO LA CANCELACIÓN DE DATOS[20]

SEVILLA, a __ de_____ de 2017

D. (nombre y apellidos del solicitante).

C/ (nombre de la calle, nº, portal, escalera).

C.P. (nº de código postal) - Población

EXP. (nº de expediente)

Muy Sr./Sra. Nuestro/a,

De acuerdo con su petición de cancelación registrada en la **FORMACIONL** con fecha 00/00/00, le comunicamos que tras las comprobaciones pertinentes hemos procedido a la **cancelación**, en el Fichero _____[21], de sus datos.

[20] Señalar que ningún trabajador podrá ser ejercitar su derecho de cancelación mientras mantenga su relación (social o laboral, respectivamente). No obstante una vez finalizada si podrá ejercitar dicho derecho, aunque deberá tenerse en cuenta los plazos determinados para el bloqueo de los datos.

[21] Se designará el fichero al que solicitó la cancelación.

Asimismo, le informamos de que dicha cancelación dará lugar al bloqueo de los datos, conservándose únicamente a disposición de las Administraciones Públicas, Jueces y Tribunales para la atención de posibles responsabilidades nacidas de la relación jurídica mantenida con FORMACIONL, durante el plazo de prescripción de las mismas.

Asimismo le comunicamos que sus datos,

- no han sido comunicados a ninguna entidad
- han sido comunicados a las siguientes entidades:

- Nombre de la entidad 1: _____
- Dirección: _____
- Nombre de la entidad 2: _____
- Dirección: _____

Igualmente le informamos que los usos y finalidades previstos del fichero son: .....

Por último, le rogamos haga referencia al número de expediente que figura en la carta, en cualquier comunicación posterior que desee realizar.

Atentamente,

FORMACIONL

Fdo:.....

MODELO DE COMUNICADO DENEGANDO EL ACCESO A LOS DATOS

SEVILLA, a __ de_____ de 2017

D. (nombre y apellidos del solicitante).

C/ (nombre de la calle, nº, portal, escalera).

C.P. (nº de código postal) - Población

EXP. (nº de expediente)

Muy Sr. /Sra. Nuestro/a,

En contestación a su atento escrito registrado **en FORMACIONL,** con fecha 00/00/00, en el que nos solicita **el acceso** a los datos más abajo indicados vinculados a su persona, le comunicamos que no podemos atender a su solicitud de cancelación por el siguiente motivo:

( ) Falta de garantía de identificación[1].

( ) Haber ejercitado este derecho en los doce meses anteriores a esta solicitud, y no acreditarse interés legitimo alguno.

( ) Por preverlo o imponerlo, así la Ley_____o la norma de derecho Comunitario_____de aplicación directa.

A continuación, le comunicamos que sus datos:

1. No han sido comunicados a ninguna entidad

2. Han sido comunicados a las siguientes entidades:

Nombre de la entidad 1: (por ejemplo Tesorería General de la Seguridad Social)

Dirección:

Nombre de la entidad 2: (por ejemplo INEM, Agencia Tributaria, etc.)

Dirección:

Nombre de la entidad 3:

Dirección:

[1] No haber aportado fotocopia del D.N.I. o documento equivalente que acredite la identidad y sea considerado válido en derecho. En caso de que se actúe a través de representación legal deberá aportarse, además, DNI y documento acreditativo de la representación del representante.

Igualmente le informamos que los usos y finalidades previstos del fichero son: "...".

Así mismo, le rogamos haga referencia al número de expediente que figura en la carta, en cualquier comunicación posterior que desee realizar.

Por último, le informamos que, en cualquier caso, tiene derecho a recabar la tutela de la Agencia Española de Protección de Datos (Artículos 30.3 y 33.3 del Real Decreto 1720/2007, de 21 de diciembre) o, en su caso, de las autoridades de control de las comunidades autónomas, conforme a lo dispuesto en el artículo 18 de la Ley Orgánica 15/1999, de 13 de diciembre.

Atentamente,

FORMACIONL

Fdo:.....

MODELO DE COMUNICADO DENEGANDO LA CANCELACIÓN O RECTIFICACIÓN DE LOS DATOS

SEVILLA, a __ de_____ de 2017

D. (nombre y apellidos del solicitante).

C/ (nombre de la calle, nº, portal, escalera).

C.P. (nº de código postal) - Población

EXP. (nº de expediente)

Muy Sr. /Sra. Nuestro/a,

En contestación a su atento escrito registrado en la **FORMACIONL,** con fecha 00/00/00, en el que nos solicita la **cancelación/rectificación** de los datos más

abajo indicados vinculados a su persona, le comunicamos que no podemos atender a su solicitud de cancelación por el siguiente motivo:

( ) Falta de garantía de identificación[1].

( ) Los datos deben ser conservados durante los plazos previstos en las disposiciones aplicables.

( ) Los datos deben ser conservados durante los plazos previstos en la relación contractual entre el responsable del tratamiento y la persona interesada.

( ) Por preverlo o imponerlo, así la Ley_____o la norma de derecho Comunitario_____de aplicación directa.

A continuación, le comunicamos que sus datos:

1. No han sido comunicados a ninguna entidad

2. Han sido comunicados a las siguientes entidades:

Nombre de la entidad 1: (por ejemplo Tesorería General de la Seguridad Social)

Dirección:

Nombre de la entidad 2: (por ejemplo INEM, Agencia Tributaria, etc.)

Dirección:

Nombre de la entidad 3:

Dirección:

Igualmente le informamos que los usos y finalidades previstos del fichero son: "...".

Así mismo, le rogamos haga referencia al número de expediente que figura en la carta, en cualquier comunicación posterior que desee realizar.

Por último, le informamos que, en cualquier caso, tiene derecho a recabar la tutela de la Agencia Española de Protección de Datos (Artículos 30.3 y 33.3 del Real Decreto 1720/2007, de 21 de diciembre) o, en su caso, de las autoridades de

[1] No haber aportado fotocopia del D.N.I. o documento equivalente que acredite la identidad y sea considerado válido en derecho. En caso de que se actúe a través de representación legal deberá aportarse, además, DNI y documento acreditativo de la representación del representante.

control de las comunidades autónomas, conforme a lo dispuesto en el artículo 18 de la Ley Orgánica 15/1999, de 13 de diciembre.

Atentamente,

FORMACIONL

Fdo:.....

MODELO DE COMUNICADO INFORMANDO QUE NO EXISTE INFORMACIÓN A SU NOMBRE

SEVILLA, a __ de_____ de 2017

D. (nombre y apellidos del solicitante).

C/ (nombre de la calle, nº, portal, escalera).

C.P. (nº de código postal) - Población

EXP. (nº de expediente)

Muy Sr. /Sra. Nuestro/a,

Con relación a su escrito registrado en la**,** con fecha 00/00/00 en las que nos solicita el **acceso/rectificación/cancelación**, le comunicamos que, hechas las comprobaciones pertinentes, a esta fecha, los datos relativos al DNI.0000000, no están registrados en el Fichero _____[22]

[22] Constatar el fichero al que se dirige el titular de los datos

Igualmente le informamos que los usos y finalidades previstos del fichero son: "...".[23]

Por último, le rogamos haga referencia al número de expediente que figura en la carta, en cualquier comunicación posterior que desee realizar.

Atentamente,

FORMACIONL

Fdo:.....

[23] Reflejar los usos y finalidades del fichero correspondiente.

MODELO DE CONTESTACIÓN DENEGANDO EL ACCESO/RECTIFICACIÓN/ CANCELACIÓN A LOS REPRESENTANTES DEL TITULAR DE LOS DATOS

SEVILLA, a __ de_____.de 2017

D. (nombre y apellidos del solicitante).

C/ (nombre de la calle, nº, portal, escalera).

C.P. (nº de código postal) - Población

EXP. (nº de expediente)

Muy Sr./Sra. Nuestro/a,

En contestación a su atento escrito registrado en la **FORMACIONL,** con fecha 00/00/00, en el que solicitaba el **acceso/rectificación/cancelación**, le comunicamos que, conforme al artículo 23.3 del Real Decreto 1720/2007, de 21 de diciembre, no es posible que ejercite ese derecho en calidad de representante.

Lamentamos no haber podido atender su solicitud y quedamos a su entera disposición y a la de D. _____ por si personalmente quisiera ejercitar ese Derecho, enviando para ello escrito de solicitud firmada por la persona interesada, acompañado de fotocopia del DNI.

Por último, le rogamos haga referencia al número de expediente que figura en la carta, en cualquier comunicación posterior que desee realizar.

Atentamente,

FORMACIONL

Fdo:.....

6.4.7.- Anexo: AVISO LEGAL Y POLÍTICA DE PRIVACIDAD.

Aviso legal y Política de privacidad en la página web e Intranet de FormacionL.

AVISO LEGAL y POLÍTICA DE PRIVACIDAD

INFORMACIÓN GENERAL

Titular: FORMACIONL

Dirección: *Calle FormacionL 11 Sevilla*. ESPAÑA.

Telf: 999 999 999 9

Fax: 999 999 999 8

CIF: z999999999999

El presente documento tiene por objeto establecer las Condiciones Generales de Uso del Portal de Internet (en adelante el Portal) www.FormacionL.pfc

FORMACIONL se reserva el derecho a modificar las Condiciones Generales de Uso para adecuarlas a la legislación vigente aplicable en cada momento, las novedades jurisprudenciales y las prácticas habituales de mercado.

La utilización por parte de la Persona usuaria de cualquiera de los Servicios del Portal supone y expresa su adhesión y aceptación expresa a todas las Condiciones Generales de Uso en la versión publicada en el Portal en el momento en que la persona usuaria acceda al Portal, así como a las Condiciones Particulares que, en su caso, sean de aplicación y se publicaran.

POLÍTICA DE PRIVACIDAD

En cumplimiento de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y su normativa de desarrollo, FORMACIONL le informa

de que los datos personales facilitados a este Portal, serán incorporados a un fichero automatizado cuyo responsable y titular es la **FORMACIONL.**

Le comunicamos que tiene usted la posibilidad legal de ejercitar si desea los derechos de acceso, rectificación, cancelación y oposición solicitándolo por escrito, previa acreditación de su identidad, a la Dirección de la FormacionL, en la siguiente dirección: Calle Sevilla 11 SEVILLA

AVISO LEGAL

FORMACIONL mantiene los contenidos de este Portal como servicio de información y comunicación de las actividades promovidas por esta entidad y/o relacionadas con la Formación para el Empleo.

El acceso al Portal debe realizarse teniendo en cuenta las siguientes condiciones de uso:

Uso del Portal y sus Servicios.

La Persona usuaria reconoce y acepta que el uso de los contenidos y/o servicios ofrecidos por el Portal será bajo su exclusivo riesgo y/o responsabilidad.

La Persona usuaria se compromete a utilizar el Portal y todo su contenido y Servicios conforme a lo establecido en la ley, la moral, el orden público y en las Condiciones Generales de Uso, y en las Condiciones Particulares que, en su caso, le sean de aplicación.

Asimismo, se compromete hacer un uso adecuado de los servicios y/o contenidos del Portal y a no emplearlos para realizar actividades ilícitas o constitutivas de delito, que atenten contra los derechos de terceros y/o que infrinjan la regulación sobre propiedad intelectual e industrial, o cualesquiera otras normas del ordenamiento jurídico aplicable.

La Persona usuaria se compromete a no trasmitir, introducir, difundir y poner a disposición de terceros, cualquier tipo de material e información (datos contenidos,

mensajes, dibujos, archivos de sonido e imagen, fotografías, sofware…etc.) que sean contrarios a la ley, la moral, el orden público y las presentes Condiciones Generales de Uso y, en su caso, a las Condiciones Particulares que le fueran de aplicación.

Propiedad Intelectual

Todo el contenido del Portal, así como el diseño del mismo, logos, composición y los Derechos de Propiedad Industrial de los productos y servicios de la pertenecen a **FORMACIONL**. En consecuencia el acceso a éstos contenidos o elementos no otorga a la Persona usuaria el derecho de alteración, modificación, explotación, reproducción, distribución o comunicación pública o cualquier otro derecho que corresponda al titular del derecho afectado.

La Persona usuaria se compromete a utilizar los contenidos y/o elementos a los que acceda a través de los Servicios del Portal para su propio uso y necesidades, y a no realizar en ningún caso una explotación comercial, directa o indirecta de los mismos.

Exclusión de Garantías. Responsabilidad.

Disponibilidad y Servicios:

FORMACIONL no garantiza la disponibilidad, acceso y continuidad, del funcionamiento del Portal y de sus Servicios.

FORMACIONL no será responsable, con los límites establecidos en el Ordenamiento Jurídico vigente, de los daños y perjuicios causados a la Persona usuaria como consecuencia de la indisponibilidad, fallos de acceso y falta de continuidad del Portal y sus Servicio.

FORMACIONL responderá única y exclusivamente de los Servicios que preste por sí misma y de los contenidos directamente originados por FORMACIONL e identificados con su copyright. Dicha responsabilidad quedará excluida en los casos

en que concurran causas de fuerza mayor o en los supuestos en que la configuración de los equipos de la Persona usuaria no sea la adecuada para permitir el correcto uso de los servicios de Internet prestados por FORMACIONL. En cualquier caso, la eventual responsabilidad de FORMACIONL frente a la persona usuaria por todos los conceptos EXCLUIRÁ en todo caso de responsabilidad por daños indirectos o por lucro cesante.

FORMACIONL no será responsable, ni indirectamente ni subsidiariamente, de los daños y perjuicios de cualquier naturaleza causados a la Persona usuaria como consecuencia de la presencia de virus u otros elementos en los contenidos y Servicios prestados por terceros que puedan producir alteraciones en el sistema informático, documentos electrónicos o ficheros de las personas usuarias.

La exoneración de responsabilidad señalada en el párrafo anterior será de aplicación en el caso que, FORMACIONL no tenga conocimiento efectivo de que la actividad o la información almacenada es ilícita o de que lesiona bienes o derechos de un tercero susceptibles de indemnización o si la tuviesen actúen con diligencia para retirar los datos y contenidos o hacer imposible el acceso a ellos.

Conducta de las Personas usuarias

FORMACIONL no garantiza que las Personas usuarias del Portal utilicen los contenidos y/o servicios del mismo de conformidad con la ley, la moral, el orden público, ni las presentes Condiciones Generales y, en su caso, las condiciones Particulares que resulten de aplicación Asimismo no garantizan la veracidad y exactitud, exhaustividad y/o autenticidad de los datos proporcionados por las Personas usuarias.

FORMACIONL no será responsable, indirecta ni subsidiariamente, de los daños y perjuicios de cualquier naturaleza derivados de la utilización de los Servicios y Contenidos de del Portal por parte de las Personas usuarias o que puedan derivarse de la falta de veracidad, exactitud y/o autenticidad de los datos o informaciones proporcionadas por las Personas usuarias o de la suplantación de la

identidad de un tercero efectuada por una Persona usuaria en cualquier clase de actuación a través del Portal.

Dispositivos Técnicos de enlace.

El Portal pone a disposición de las Personas usuarias el acceso a Web sites titularidad de otras entidades. (web sites enlazadas).

La Persona usuaria reconoce y acepta que la utilización de los Servicios y contenidos de las Web Sites enlazadas será bajo su exclusivo riesgo y responsabilidad y exonera a FORMACIONL de cualquier responsabilidad sobre disponibilidad técnica de las web sites enlazadas, la calidad, fiabilidad, exactitud y/o veracidad de los servicios, informaciones, elementos y/o contenidos a los que la Persona usuaria pueda acceder en las mismas y en los directorios de búsqueda incluidos en el Portal.

La exoneración de responsabilidad señalada en el párrafo anterior será de aplicación en el caso que, FORMACIONL no tenga conocimiento efectivo de que la actividad o la información a la que remite es ilícita o de que lesiona bienes o derechos de un tercero susceptibles de indemnización o si la tuviesen actúen con diligencia para retirar los datos y contenidos o hacer imposible el acceso a ellos.

Varios:

Modificaciones.

FORMACIONL se reserva el derecho a efectuar las modificaciones que estime oportunas, pudiendo modificar, suprimir e incluir, unilateralmente y sin previo aviso, nuevos contenidos y/o servicios, así como la forma en que éstos aparezcan presentados y localizados.

Derecho de exclusión

FORMACIONL se reserva el derecho a denegar o retirar el acceso al portal y/o los servicios ofrecidos, sin necesidad de preaviso a instancia propia o de un tercero, a aquellas personas usuarias que incumplan las presentes Condiciones Generales de Uso y/o las condiciones Particulares que, en su caso, resulten de aplicación.

Menores de edad.

Con carácter general, para hacer uso de los Servicios del Portal los menores de edad deben haber obtenido previamente la autorización de sus padres, tutores o representantes legales, quienes serán responsables de todos los actos realizados a través del portal por los menores a su cargo. En aquellos Servicios en los que expresamente se señale, el acceso quedará restringido única y exclusivamente a mayores de 18 años.

Duración y terminación

La prestación de los servicios y/o contenidos del portal tiene una duración indefinida. Sin perjuicio de lo anterior FORMACIONL está facultada para dar por terminada, suspender o interrumpir unilateralmente, en cualquier momento y sin necesidad de preaviso, la prestación del servicio del portal y/o de cualquiera de los servicios.

Ley aplicable y Jurisdicción

Estas Condiciones Generales se rigen por la legislación española de aplicación en la materia. FORMACIONL y la persona usuaria, con renuncia expresa a cualquier otro fuero, se someten al de los Juzgados y Tribunales del domicilio de la sociedad para cualquier controversia que pudiera derivarse de la prestación de los servicios objeto de estas Condiciones Generales. En el caso de que la persona usuaria tenga su domicilio fuera de España, FORMACIONL y la persona usuaria se someten, con renuncia expresa a cualquier otro fuero, a los juzgados y tribunales de la ciudad de Sevilla (España).

6.5.- Anexo V: Documento de Seguridad

DOCUMENTO DE SEGURIDAD DE FORMACIONL

Índice

Índice de Diagramas

6.5.1.- Introducción

El artículo 9 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter personal (LOPD), establece en su punto 1 que "el Responsable del Fichero, y, en su caso, el encargado del tratamiento, deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural".

El 21 de diciembre de 2007 se publicó el RD 1720/2007 (RLOPD), por el que se aprobó el Reglamento de desarrollo de la Ley Orgánica 15/1999, que deroga el RD 994/1994 y tiene por objeto "garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal", extendiendo su aplicación no sólo al tratamiento automatizado, sino también al no automatizado de los datos de carácter personal.

6.5.1.1.- Definiciones y términos

A fin de homogeneizar los términos y su significante, este Documento emplea la terminología recogida en la redacción del RLOPD, y que se incluye como Anexo IV en el "**Documento de aplicación LOPD FORMACIONL**".

6.5.1.2.- Objeto de este documento

Según el artículo 88 del antedicho RLOPD, el Responsable del Fichero o tratamiento de datos personales elaborará un documento de seguridad que recogerá las medidas de índole técnica y organizativa acordes a la normativa de seguridad vigente que será de obligado cumplimiento para el personal con acceso a los sistemas de información.

El objeto del presente documento es el cumplimiento de dicha obligación por parte de **FORMACIONL (**o la Organización) en su calidad de **Responsable de Ficheros de Datos Personales**.

6.5.1.3.- Ámbito de aplicación

Este documento será de aplicación a **todos los recursos que contienen y/o tratan datos de carácter personal** que se hallan bajo la responsabilidad de **FORMACIONL**, incluyendo los sistemas de información, soportes y equipos empleados para su tratamiento, **automatizado o no**, que deban ser protegidos de acuerdo a lo dispuesto en la normativa vigente.

Se incluyen dentro de este ámbito:

- Las **personas** que intervienen en el tratamiento.
- Los **centros de tratamiento y locales** donde se encuentren ubicados los ficheros y se almacenen los soportes que los contengan.
- Los **archivos y los equipos servidores** donde se ubican los Ficheros, así como el entorno (despachos, armarios, software, hardware) de los mismos.
- Los **puestos de trabajo**, bien locales o remotos, desde los que se puede tener acceso a los ficheros.
- Los **sistemas de información y aplicaciones** utilizados para el acceso a los ficheros y tratamiento de los datos.

🕮 En el *6.5.- Anexo II – Relación de las Personas usuarias Autorizados con acceso a los ficheros* se establece la relación de las personas usuarias autorizados a acceder a datos de cada uno de los Ficheros declarados.

🕮 En el apartado *"6.5.0 – 6.5.8.- Estructura de los Sistemas* de Información*"* se establece la relación detallada de dichos recursos.

6.5.1.4.- Resumen de Ficheros inscritos en el R.G.P.D.

La siguiente tabla resume los ficheros declarados por **FORMACIONL** ante el Registro General de Protección de Datos (R.G.P.D.).

Nombre del Fichero	Nivel (1)
USUARIAS AUTOORIENTACION	**MEDIO**
DATOS DE EMPLEADOS/AS --> RRHH	**MEDIOS**
CLIENTES Y PROVEEDORES	BÁSICO
AGENDA CORPORATIVA	BÁSICO
EVENTOS	BÁSICO
CONTABILIDAD Y HACIENDA PÚBLICA	**MEDIO**
CURRICULOS FORMACIONL	**MEDIO**
COMUNICACIÓN Y MARKETING	**BÁSICO**
USUARIAS	**BÁSICO**

La información detallada sobre estos ficheros, incluyendo sus datos registrales, se desarrolla en el apartado *"0 - 6.5.7.- Relación de Ficheros inscritos en la AEPD y Descripción* detallada de su estructura*"*.

6.5.1.5.- Actualización del Documento de Seguridad

Debido a la continua evolución y cambios relevantes de los sistemas de información, y a la propia complejidad de la Organización, el documento intentará ser un marco estable y a la vez flexible, en lugar de una descripción estática, en cuyo caso se vería sometido a continuas actualizaciones.

El presente documento se mantendrá en todo momento actualizado y será revisado siempre que:

- Se produzcan cambios relevantes en los sistemas de información que contienen o tratan datos de carácter personal;
- Existan cambios en la organización de **FORMACIONL** que afecten a los procedimientos y medidas recogidos en este documento;
- Se modifiquen las disposiciones vigentes en materia de seguridad de los datos de carácter personal.

El Responsable del Fichero mantendrá permanentemente actualizada toda la información y documentación incluida en este Documento de Seguridad, o que se derive de él. A este fin, **FORMACIONL** delega las tareas de mantenimiento y actualización del Documento de Seguridad -y sus anexos- en el Responsable de Seguridad, designado en el apartado "*0 - 6.5.2.3.- Responsables de Seguridad - Designación"*.

6.5.1.6.- Comunicación al personal

El "**Documento de Aplicación Legal LOPD FORMACIONL**" que complementa el presente Documento de Seguridad, contiene un "**Modelo De Circular**" informando del "**Procedimiento a Seguir en el Ejercicio de Derechos en Materia de Protección de Datos**", donde se detalla el procedimiento que deben conocer todos los empleados/colaboradores de **FORMACIONL**, ante la solicitud de un ejercicio de derechos de acceso, rectificación, cancelación y oposición por parte de los interesados.

Además de dicho modelo, se adjuntarán, para su **entrega al personal**, copia de un documento que se habrá de llamar "**Política de Seguridad de la Información de FORMACIONL**" (que se elaborará en una posterior fase del pfc) y que habrá de contener copia de los siguientes apartados de este documento:

- 6.5.3.1 - 6.5.3.1.- Normas de uso aceptable de los Sistemas *de Información*
- 6.5.6.5.3.3.3.- Normas para la generación y gestión de contraseñas
- 6.5.0. - 6.5.2.4.5.- Personas Usuarias de los ficheros de datos personales – *Obligaciones*
- 6.5.0. - 6.5.4.1.- Tipo de Incidencias que se deben *notificar*
- 6.5.4.2. - Procedimiento de notificación de Incidencias
- 6.5.5.4. - Protocolo de recuperación/restauración de datos

6.5.2.- Funciones y obligaciones del personal

FORMACIONL define en este documento las funciones y obligaciones del personal autorizado a acceder a datos propiedad de **FORMACIONL** y a la utilización de sus sistemas.

Dada la estructura organizativa, a fin de cumplir lo requerido en la LOPD y su Reglamento de Desarrollo, se constituye un **Comité de Seguridad**, presidido y coordinado por un **Responsable de Seguridad Global LOPD**.

6.5.2.1.- El Comité de Seguridad

El Comité de Seguridad estará compuesto por personas representando a los siguientes tipos de perfiles:

- **Responsable de Seguridad Global LOPD** (coordinador del comité)
- **2 Responsables de Seguridad de entre las Gerencias Provinciales**
  - Responsable de Seguridad Gerencia de Almería
  - Responsable de Seguridad Gerencia de Cádiz
  - Responsable de Seguridad Gerencia de Córdoba
  - Responsable de Seguridad Gerencia de Granada
  - Responsable de Seguridad Gerencia de Huelva
  - Responsable de Seguridad Gerencia de Jaén
  - Responsable de Seguridad Gerencia de Málaga
  - Responsable de Seguridad Gerencia de Sevilla
- **Responsables de Dirección General Técnica (DGT)**
    - Responsable de Dirección General Técnica
    - Responsable de Dirección de Organización
    - Responsable de Dirección Económica
    - Responsable de Dirección de Recursos Humanos
    - Responsable de Dirección de Actividad

- Responsable de Dirección de Sistemas
- Responsable de Dirección de Desarrollo Territorial

Ya que el Responsable de Seguridad Global es el encargado de dar las directrices y asegurar que se realizan los procedimientos de seguridad, pero no tiene por qué ser el encargado de ejecutarlos personalmente, en el Comité de Seguridad podrá participar, a petición de este, otro personal de la Organización. Sirva como ejemplo, el siguiente personal de la Dirección de Sistemas, como:

- Responsable de Backups centrales
- Responsable de Soportes de almacenamiento centrales
- Responsable de Incidencias LOPD centrales
- Responsable de Autenticación de Personas usuarias / Derechos de Acceso centrales
- Responsable de Control de Acceso Físico (áreas centrales de almacenamiento de soportes de datos electrónicos)
- Responsable de Controles Mensuales centrales (auditorías, etc.)
- Responsable de Controles Mensuales provinciales (auditoría de soportes, personas usuarias, eliminación de ficheros temporales, etc.)
- Responsable de Registro de Logs centrales
- Responsable de Cifrado de Telecomunicaciones

Así mismo, en el Comité de Seguridad podrá participar el Responsable de Control de Acceso Físico a los Archivos Centrales de documentos-papel.

A continuación se indican las obligaciones y las designaciones de cada uno de ellos.

6.5.2.2.- Responsable del Fichero / Responsables de Ficheros de la DGT - Obligaciones

FORMACIONL, como responsable jurídico de la seguridad de los ficheros con datos de carácter personal, es el responsable frente a la Agencia Española de Protección de Datos

(AEPD) de la implantación de las medidas establecidas en el presente documento y de que estas sean conocidas por todo el personal afectado.

En particular:

- Notificará al Registro General de Protección de Datos los ficheros con datos de carácter personal de **FORMACIONL** y el mantenimiento posterior de los asientos registrales.
- Implantará las medidas de seguridad establecidas en este Documento.
- Garantizará la difusión de este Documento y adoptará las medidas necesarias para que el personal afectado por este documento conozca las normas que afecten al desarrollo de sus funciones.
- Mantendrá actualizado el Documento, siempre que se produzcan cambios relevantes en el sistema de información o en la organización del mismo.
- Adecuará, en todo momento, el contenido del Documento de Seguridad a las disposiciones vigentes en materia de seguridad de datos.
- Designará un o más Responsables de Seguridad de **FORMACIONL**, como se referencia en *el apartado "6.5.0 - 6.5.2.3.- Responsables de Seguridad - Designación"*.
- Establecerá los criterios generales para la asignación de niveles de acceso, según funciones del puesto de trabajo del personal, etc.
- Establecerá los criterios generales para la determinación de los niveles de copia de seguridad a realizar y archivar.
- Autorizará expresamente la salida de soportes informáticos que contengan datos personales fuera de los locales donde están ubicados los ficheros.
- Autorizará expresamente el tratamiento de datos fuera de los locales de la ubicación de los ficheros (portátiles, etc.) tras recibir del Responsable de Seguridad la valoración sobre la pertinencia de la solicitud.
- Establecerá una **auditoría bienal,** obligatoria para los ficheros de nivel medio y alto que determine el grado de cumplimiento del presente Documento.
- Adoptará las medidas correctoras adecuadas, en virtud de las conclusiones que el Responsable de Seguridad elevará tras el análisis de auditoría bienal.

Según el artículo 9 de la LOPD:

El responsable de ficheros, y en su caso el encargado del tratamiento, deberá adoptar las medidas de índole técnica y organizativa necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, teniendo en cuenta el estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a los que estén expuestos ya provengan de la acción humana o del medio físico o natural

Las figuras de los Responsables de Ficheros de la DGT desarrollan las mismas funciones y obligaciones mencionadas, pero limitadas al ámbito de los ficheros bajo su responsabilidad, según se indica en el 6.5.- Anexo II.

6.5.2.3.- Responsables de Seguridad - Designación

De acuerdo al RLOPD art. 95), **FORMACIONL** ha designado a una serie de Responsables de Seguridad, como encargados de implantar y actualizar esta normativa de seguridad de obligado cumplimiento, si bien, la designación de un Responsable de Seguridad no supone una exoneración de las responsabilidades que corresponden al Responsable del Fichero o al Encargado del Tratamiento.

Según el Artículo 95 de la LOPD: Responsable de seguridad.

En el documento de seguridad deberán designarse uno o varios responsables de seguridad encargados de coordinar y controlar las medidas definidas en el mismo. Esta designación puede ser única para todos los ficheros o tratamientos de datos de carácter personal o diferenciado según los sistemas de tratamiento utilizados, circunstancia que deberá hacerse constar claramente en el documento de seguridad.

En ningún caso esta designación supone una exoneración de la responsabilidad que corresponde al responsable del fichero o al encargado del tratamiento de acuerdo con este reglamento.

Entre las funciones del responsable destacan la de analizar los informes de auditoría y elevar al responsable del fichero las recomendaciones y medidas correctoras oportunas, mantener el control de los registros de acceso, revisión de los registros de incidencias, y actualización del documento de seguridad.

Resumiendo, que no surja al pánico si nos hacen responsable de seguridad ya que la responsabilidad final recaerá siempre sobre el Responsable del Fichero

Es el encargado de coordinar y controlar las medidas definidas en el documento de seguridad.

📖 En el 6.5.- ***Anexo V – Responsables de Seguridad: Comunicación***, se incluye la circular informativa en la que **FORMACIONL** comunica a todo su personal el nombramiento de sus Responsables de Seguridad, así como sus datos de contacto.

Tanto el presente Documento de Seguridad como los documentos referenciados en él, están custodiados por el **Responsable de Seguridad Global**, quien se encargará de facilitarlos, en caso de requerimiento, a la Agencia de Protección de Datos u organismos de control autonómicos.

6.5.2.4.- Responsables de Seguridad

6.5.2.4.1.- Responsables de Seguridad – Funciones y Obligaciones

De acuerdo con el artículo 95 del RLOPD, las funciones del Responsable de Seguridad Global serán las de:

- Coordinar y controlar la implantación y seguimiento de las medidas definidas en este Documento de Seguridad.
- Actuar como enlace con el Responsable del Fichero, sin que esto suponga en ningún caso una delegación de la responsabilidad de este último.
- Presidir y coordinar el Comité de Seguridad, cuya composición se ha definido anteriormente.
- Mantener actualizado el Documento de Seguridad y revisarlo cuando se produzcan cambios relevantes en los sistemas de información.
- Actualizar los mecanismos de seguridad establecidos para que cumplan, en todo momento, con la legislación vigente en materia de seguridad de datos de carácter personal.

- Detectar todas aquellas circunstancias que afecten al Documento de Seguridad o al ejercicio de los derechos fundamentales de los afectados.

6.5.2.4.2 Responsable de Seguridad de Gerencias Provinciales - Funciones y Obligaciones

La función básica de los Responsables de Seguridad Provinciales es realizar en su Gerencia Provincial la implantación y seguimiento de las medidas establecidas en este Documento de Seguridad, actuando siempre bajo las directrices del Responsable Global de Seguridad.

En particular, serán responsables de:

RESPONSABILIDADES		BAJO AUTORIZACIÓN DE /REPORTANDO A	
		Responsable Seguridad	Responsables Ficheros respectivos
COMUNES A TODOS ELLOS	• Supervisión de los Centros de cada Gerencia Provincial, respectivamente	✓	
	• Interlocución y coordinación con Responsable de Seguridad Global en el Comité de Seguridad	✓	
	• Difusión de normas de seguridad y protección de datos al personal	✓	
ADMDOR. SOPORTES.	• Custodia y actualización de backups, así como autorización para restauración de backups “in situ”	✓	✓
	• Control del inventario permanente de soportes de datos (electrónicos y papel) y medidas sobre soportes desechados o reutilizados	✓	

	• Registro de entradas/salidas de soportes		✓
ADMDOR. INCIDENCIAS	• Supervisión del registro de incidencias de seguridad de los datos:	✓	
	➢ Ejercicio del derecho de rectificación de datos		
	➢ Atención a los derechos de tutela		
ADMDOR. USUARIOS.	• Alta / baja / modificación de las personas usuarias y de sus derechos de acceso a los sistemas		✓
CONTROLADOR DE ACCESO FISICO	• Control de Acceso Físico (áreas de almacenamiento de soportes de datos electrónicos y papel)	✓	
CONTROLADOR DE FICHEROS TEMPORALES	• Eliminación de Ficheros Temporales	✓	

6.5.2.4.3.- Encargados del Tratamiento – Designación, Funciones y Obligaciones

Las funciones y obligaciones de seguridad de los *Encargados De Tratamiento* (terceros) están indicados en el documento "**Documento de aplicación Legal LOPD FORMACIONL**", párrafo "6.4.*1.2.6 - Acceso a los datos por cuenta de terceros (artículo 12 LOPD)*".

📖 En el 6.5.- ***Anexo IV-1: Tratamiento de datos por Terceros para FORMACIONL***, se incluyen los encargados de tratamiento para los distintos servicios contratados por **FORMACIONL**, para cuya prestación tengan acceso o traten datos protegidos de este último.

6.5.2.4.4.- Administradores de Sistemas de la Dirección de Sistemas - Funciones y Obligaciones

Son miembros de la Dirección de Sistemas encargados de operar y mantener los entornos operativos de los sistemas de tratamiento automatizado de los ficheros.

Los distintos Administradores de Sistemas serán co-responsables junto con el Responsable Global de Seguridad de:

RESPONSABILIDADES	**BAJO AUTORIZACIÓN DE /REPORTANDO A**	
	Responsable Seguridad	**Responsables Ficheros respectivos**
• Interlocución y coordinación con Responsable de Seguridad Global	✓	
• Asesorar al Responsable de Seguridad Global sobre normas de seguridad y protección de datos al personal	✓	
• Custodia y actualización de backups, así como autorización para restauración de backups en la DGT	✓	✓
• Control del inventario permanente de soportes de datos (electrónicos y medidas sobre soportes desechados o reutilizados en la DGT	✓	
• Control del Registro de entradas/salidas de soportes en sistemas centrales		✓
• Control del Registro de incidencias de seguridad de los datos en la DGT	✓	
➢ Ejercicio del derecho de rectificación de datos		
➢ Atención a los derechos de tutela		
• Alta / baja / modificación de las personas usuarias y de sus derechos de acceso en la DGT		✓

• Control de Acceso Físico a las áreas de almacenamiento centrales de soportes de datos electrónicos		✓	
• Eliminación de Ficheros Temporales en la DGT		✓	
NIVEL MEDIO	• Realización de Controles Mensuales en sistemas centrales (auditoría de soportes, personas usuarias, eliminación de ficheros temporales, etc.)	✓	•
NIVEL ALTO	• Implantación y Revisión del Registro de Logs centrales	✓	
	• Implantación y Revisión del Cifrado de Telecomunicaciones	✓	

Este personal se encuentra explícitamente relacionado en los Anexos, ya que por sus funciones pueden disponer de herramientas que permitan el acceso a los datos protegidos, saltándose las medidas y barreras de acceso implantadas para proteger los datos personales.

Se engloba bajo este rol al personal informático que puede tener acceso de administración tanto de los entornos informáticos como de los entornos físicos donde se ubican los ficheros con datos personales.

Los Administradores de Sistemas de **FORMACIONL** no permitirán que ninguna persona usuaria ni administrador no autorizado pueda tener acceso a herramientas o utilidades que permitan el acceso a aquellos ficheros para los cuales no están autorizados.

6.5.2.4.5.- Personas Usuarias de los ficheros de datos personales – Obligaciones

"Personas Usuarias" son todo el personal propio o subcontratado por **FORMACIONL** que utiliza los sistemas establecidos por **FORMACIONL** para el acceso a los ficheros protegidos (traten o no los datos contenidos en ellos) y que no puedan ser categorizados en los anteriores roles.

Las siguientes **obligaciones** son aplicables a todas las personas usuarias de **FORMACIONL**:

- Las personas usuarias que accedan a los datos de carácter personal está obligado a conocer y observar las medidas, normas, procedimientos, reglas y estándares recogidas en el Documento de Seguridad, con especial atención a aquellas que afecten a las funciones que cada uno desarrolla.
- Todas las personas usuarias deberán guardar el debido secreto y confidencialidad sobre los datos personales de los que puedan tener conocimiento en el desempeño de su actividad laboral.
- Constituye una obligación de todas las personas usuarias notificar al Responsable de Seguridad cualquier incidencia de seguridad de la que tengan conocimiento respecto de los recursos protegidos. Ver sección *"6.5.**0** -* **6.5.4.- Procedimiento ante** incidencias*"*.
- El conocimiento y la no notificación de una incidencia por parte de una persona usuaria será considerado como una falta grave contra la seguridad del Fichero por parte de esa persona usuaria.
- Los soportes (informatizados o no) que contengan datos de los ficheros deberán ser almacenados en lugares a los que no tengan acceso personas no autorizadas para el uso del Fichero.
- Todas las personas usuarias de los sistemas de **FORMACIONL** confirmarán por escrito que conocen la política y las obligaciones de carácter general recogidos en este Documento de Seguridad y que se comprometen a cumplirlos..

📖 En el 6.5.- ***Anexo II – Personas usuarias autorizadas con acceso a los ficheros,*** se encuentra la relación de todas las personas usuarias por **FORMACIONL** para acceder a los datos protegidos de cada uno de los Ficheros.

6.5.3.- Normas, medidas y procedimientos de seguridad

Bajo este título se recogen las normas y procedimientos referentes a las medidas de seguridad establecidas por **FORMACIONL** para el cumplimiento de lo establecido por el RLOPD.

6.5.3.1.- Normas de uso aceptable de los Sistemas de Información

Cada persona usuaria de **FORMACIONL** (empleados o personal subcontratado) debe seguir las normas en vigor referentes al uso / configuración del ordenador y del puesto de trabajo, principalmente las indicadas a continuación.

6.5.3.1.1.- Normas Generales

- La persona usuaria debe realizar sus actividades de acuerdo con todas las legislaciones y reglamentos aplicables, incluyendo las normas de **FORMACIONL** (como las indicadas en este Documento) y cualquier instrucción específica dictada por la Organización.
- Todas las personas usuarias deberán guardar el debido secreto y confidencialidad sobre los datos personales de los que puedan tener conocimiento en el desempeño de su actividad laboral.
- El sistema informático, la red de la Organización y todos los recursos utilizados por cada persona usuaria son propiedad de **FORMACIONL**. Dichos recursos tienen la consideración de herramientas de trabajo puestas a su disposición para el desempeño necesario para sus funciones en FORMACIONL.
- Cada persona usuaria es responsable del uso que realiza de los recursos de **FORMACIONL** (hardware, software, acceso a redes, etc.). Este uso debe ser honesto y racional para no interrumpir operaciones y evitar el desvío hacia fines ilícitos o no profesionales.
- El uso personal no se puede considerar en ningún caso como un derecho, sino como algo que es tolerado por la Organización. Debe ser razonable y ocasional y no debe afectar al funcionamiento de las operaciones de **FORMACIONL**, a la seguridad de los Sistemas de Información, ni a los intereses de la Organización.
- Todas las personas usuarias deben contribuir a la seguridad general de la Organización:
    - La persona usuaria sólo debe acceder a la información a la que ha sido expresamente autorizado.
    - La persona usuaria no debe transmitir información confidencial, ni hacerla disponible u ofertarla a individuos no autorizados, incluido compañeros de trabajo.

- Cada persona usuaria es responsable de las credenciales de acceso que le han sido asignadas y debe mantenerlas en secreto y no revelarlas.

- Si una persona usuaria considera que su nivel de autorización es insuficiente, debe solicitar a su superior la modificación de los permisos de acceso.
- En ningún caso, la persona usuaria debe intentar acceder a información a la que no está autorizado, ya sea empleando herramientas para evitar las restricciones impuestas, utilizando las credenciales de acceso o la sesión abierta de otra persona usuaria, o utilizando cualquier otro medio.
- Si, en el cumplimiento de sus deberes, una persona usuaria debe crear archivos de datos que contengan información personal, debe asegurarse previamente que tales archivos, así como su uso, están conformes con la legislación actualmente en vigor. En caso de duda debe consultarlo con su Dirección/Gerencia.
- Queda prohibido la conexión a los sistemas informáticos (incluyendo la red) de la Organización de cualquier dispositivo (PC, portátil, dispositivo wifi, etc) que no haya sido previamente aprobado por el Responsable del Dirección de Sistemas.
- **FORMACIONL** se reserva el derecho de revisar, sin previo aviso, el uso que las personas usuarias realizan de los sistemas, con el fin de comprobar el cumplimiento de estas normas y prevenir actividades que puedan afectar a **FORMACIONL** como responsable civil subsidiario.
- Constituye una obligación de todo el personal notificar al Responsable de Seguridad o a los responsables provinciales cualquier incidencia de seguridad de la que tengan conocimiento respecto de los recursos protegidos. Ver sección *"6.5.0 - 6.5.4.1.- Tipo de Incidencias que se deben notificar"*.
- El conocimiento y la no notificación de una incidencia de seguridad por parte de una persona usuaria será considerado como una falta grave contra la seguridad del Fichero por parte de esa persona usuaria.
- Los soportes (informatizados o no) que contengan datos de los Ficheros de Datos Personales deberán ser almacenados en lugares a los que no tengan acceso personas no autorizadas para el uso del Fichero.

6.5.3.1.2.- Uso del PC de trabajo y dispositivos portátiles

- Los ordenadores personales y los dispositivos móviles (portátiles, PDAs, etc.) de **FORMACIONL** tienen una configuración fija en sus aplicaciones y sistema operativo, que sólo podrá ser cambiada por los Administradores de Sistemas indicados en el 6.5.- Anexo II, mediando autorización del Responsable de Seguridad.
- Todos los PCs y dispositivos portátiles habilitados para conectarse con los servicios corporativos de FORMACIONL (correo corporativo, etc.), deberán tener activado un sistema de protección basado en contraseña que cumpla las reglas indicadas en el apartado "***0 – 6.5.6.5.3.3.3.- Normas para la generación y gestión de*** contraseñas".
- Queda prohibido descargar o instalar software adicional en los PC's de los personas usuarias. El software sólo podrá ser instalado por personal informático de la Dirección/gerencia, mediando autorización del Responsable de Seguridad. Si la persona usuaria requiere software adicional, deberá solicitarlo a su superior.
- La persona usuaria no instalará ni ejecutará aplicaciones no aprobadas por los Administradores de Sistemas. Se incluyen aquí aquellas aplicaciones que pudieran ser recibidas vía correo electrónico, mediante memorias USB o CDs promocionales o de demostración.
- Cuando la persona usuaria abandone el puesto de trabajo, bien temporalmente, bien al finalizar su turno de trabajo, deberá dejarlo apagado o utilizar un protector de pantalla con contraseña.
- **Queda expresamente prohibido** el uso de ordenadores y dispositivos portátiles no específicamente habilitados por **FORMACIONL** para cualquier tipo de acceso o tratamiento de datos de carácter personal del cual **FORMACIONL** sea responsable.

6.5.3.1.3.- Medidas adicionales de seguridad en dispositivos portátiles

La persona usuaria debe proteger su portátil y dispositivos móviles contra riesgos, incluyendo hurto, pérdida, accidentes o uso no autorizado. Para ello, se proporcionan las siguientes recomendaciones:

- Nunca debe dejarlos sin vigilancia.

- Nunca debe dejarlos en vehículos. Si no es posible, debe asegurarse que no son visibles desde el exterior, asegurando el cierre del vehículo.

- Cuando en los dispositivos portátiles se almacenen datos personales, la persona usuaria es responsable de la protección de la misma. Para ello, deberá almacenar la información usando un software de cifrado. Si la información se almacena en memorias USB o similares, estas deberán permanecer cifradas.

6.5.3.1.4.- Control antivirus

Queda **expresamente prohibida** la desactivación de los sistemas antivirus de los ordenadores (fijos o portátiles) por parte de las personas usuarias, así como cualquier acción que impida la actualización de los mismos.

- Cuando se use un ordenador portátil o un dispositivo móvil, la persona usuaria debe conectarlo regularmente a la red de la Organización para asegurar que las medidas de protección y de seguridad del antivirus se mantienen actualizadas.

6.5.3.1.5.- Uso del correo electrónico de la Organización

- Se considerará correo de formacionL a aquellos que sean enviados o recibidos en el dominio **formacionL.pfc**.
- El uso del correo electrónico de formacionL por parte de la persona usuaria se limitará únicamente a la actividad de **FORMACIONL** y a los cometidos del puesto de trabajo de la persona usuaria.
- Las personas usuarias aceptan que **FORMACIONL** podrá acceder a sus mensajes de correo electrónico y sus archivos / registros de uso de Internet, cuando esto sea necesario para:
  - la protección del patrimonio de **FORMACIONL.**
  - la protección del resto de las personas usuarias de la red informática de **FORMACIONL.**
  - facilitar razonablemente las operaciones de la Organización.
  - cuando exista sospecha fundada de violación de esta política.

- En el caso de que los mensajes de correo electrónico de formacionL y sus archivos fueran accedidos, los siguientes requisitos adicionales se aplicarán:

- Si existen medios de menor impacto para la persona usuaria, y con un coste razonable para la Organización, la Organización hará uso preferente de ellos.
- El trabajador ha de conocer expresamente por escrito, con una antelación de 48 horas, el lugar, fecha y hora en la que se llevará a cabo la inspección, así como la duración, el alcance de la misma, y las personas que intervendrán.
- El correo electrónico y los archivos serán inspeccionados en el puesto de trabajo durante horas de trabajo normales con la asistencia del empleado afectado, de un representante del empleado, si lo tuviera, o, en su ausencia, de otro empleado de la Organización.

- Esto incluye tanto los mensajes enviados entre terminales de la red de la Organización, como el externo, dirigido o proveniente de otras redes públicas o privadas hacia direcciones de correo corporativo de **FORMACIONL**.
- Cada persona usuaria debe comprobar antes de enviar un correo:
  - El nivel de confidencialidad del contenido de sus correos y/o documentos. En caso de duda debe consultarlo con su Dirección/Gerencia.
  - La exactitud de las direcciones destinatarias.
- **FORMACIONL** prohíbe el uso de correos de dominio diferente a formaciónL.pfc para la realización de actividades y cometidos propios del trabajo en **FORMACIONL**
- Cualquier fichero introducido en la red de la Organización o en el terminal de la persona usuaria a través de mensajes de correo electrónico, deberá cumplir los requisitos establecidos en estas normas y, en especial, las referidas a propiedad intelectual e industrial y a control antivirus

.

6.5.3.1.6.- Acceso a Internet y otras redes de datos

- Las redes públicas de comunicación –incluida Internet- y los sistemas y redes privadas de **FORMACIONL** no son zonas sin ley.
- El uso de los sistemas informáticos de **FORMACIONL** para acceder a redes públicas (acceso a páginas web (www), grupos de noticias (Newsgroups) y otras

fuentes de información como FTP, etc.), se limitará a los temas directamente relacionados con la actividad de **la Organización** y los cometidos del puesto de trabajo de la persona usuaria.

- El acceso a debates en tiempo real (Chat / IRC) es especialmente peligroso, ya que facilita la instalación de utilidades que permiten accesos no autorizados al sistema, por lo que su uso **queda estrictamente prohibido**.
- Solo está autorizado el acceso a páginas web (www), grupos de noticias (Newsgroups) y otras fuentes de información como FTP, etc. que contengan información relacionada con la actividad de la Organización o con los cometidos del puesto de trabajo de la persona usuaria.
- Queda **prohibido expresamente**:
    - Descargar cualquier fichero, como juegos, música o videos, si no son imprescindibles para el desempeño de las funciones del puesto de trabajo.
    - Tomar parte en actividades poco éticas o ilegales, como envío de spam, copias ilegales de software, intercambio de pornografía, etc.
    - Acceso a páginas que promuevan actividades ilegales o poco éticas, entre las que se incluyen portales de contenido adulto y juego online.
- Cualquier fichero introducido en la red de la Organización o en el terminal de de la persona usuaria desde Internet, deberá cumplir los requisitos establecidos en estas normas y, en especial, las referidas a propiedad intelectual e industrial y a control de virus.
- Especialmente **se prohíbe el uso de programas P2P** de intercambio de ficheros, como eMule, Ares, BitTorrent,…
- Como norma general, todos los equipos de trabajo informáticos (PCs, portátiles, dispositivos móviles, etc.) que puedan conectarse a redes públicas deben tener instalado y activado un *firewall* personal.
- **Se prohíbe expresamente** el empleo de herramientas y/o aplicaciones que hagan posible evitar las restricciones de acceso impuestas.
- **FORMACIONL** se reserva el derecho de monitorizar y comprobar sin previo aviso, cualquier sesión de acceso a Internet iniciada por una persona usuaria de la red de la Organización.

6.5.3.1.7.- Procedimientos de obtención de copias de respaldo

- La persona usuaria deberá mantener copia de toda la información de trabajo en los servidores centrales de **FORMACIONL**, evitando almacenar información de trabajo en su ordenador personal.
- **Queda estrictamente prohibido** el uso de programas informáticos sin la correspondiente licencia, así como el uso, reproducción, cesión, transformación o comunicación pública de cualquier tipo de obra o invención protegida por las leyes de propiedad intelectual o industrial.

6.5.3.1.9.- Puestos de trabajo

- **FORMACIONL** promueve una ***política de escritorios limpios***. Por ello, establece que en los puestos de trabajo donde se traten datos personales, cuando el responsable del puesto lo abandone, bien temporalmente o bien al finalizar su turno de trabajo, deberá dejarlo en un estado que garantice la confidencialidad de los datos personales. Para ello, debe asegurar la recogida de todos los soportes y su guarda en algún espacio protegido, como puede ser un cajón o un armario con llave.
- **Queda expresamente prohibido** el uso de puestos de trabajo no específicamente habilitados por **FORMACIONL** para cualquier tipo de acceso o tratamiento de datos de carácter personal.

6.5.3.1.10.- Uso de impresoras, copiadoras, scáneres y faxes

- Tanto en el uso de las impresoras como en el de las copiadoras (fotocopiadoras, faxes, escáneres, etc.), la persona usuaria deberá asegurarse de que no quedan originales ni copias (especialmente aquellas que contengan datos protegidos) en la bandeja de salida de documentos.

- Si la impresora, fax, escáner, etc es compartido con otras personas usuarias no autorizados para acceder a los datos del correspondiente fichero, las personas usuarias deberán retirar los documentos conforme vayan siendo impresos.
- Si se emplea una copiadora, fax, escáner, etc. y las copias no las realiza la persona usuaria, este debe asegurar que la persona que las realice esté autorizada para acceder a los datos que se van a copiar.

6.5.3.1.11.- Destrucción de soportes con datos personales

- Como norma general, los soportes que contengan datos personales no podrán ser reutilizados.
- Cuando una persona usuaria deba desechar soportes -en papel o automatizados- que contengan datos personales, deberá hacerlo de manera que garantice que la información que contienen resulte ilegible.
- Para ello, la persona usuaria hará uso de las destructoras habilitadas en cada centro de trabajo o de los contenedores dispuestos por **FORMACIONL** para tal fin. Dichos contenedores aseguran, mediante contrato con la empresa contratada al efecto, la confidencialidad de los datos que contienen hasta su destrucción.

6.5.3.2.- Autorización de Prestaciones de Servicios con y sin acceso a datos

La normativa interna aplicada por **FORMACIONL** a las prestaciones de servicios de tratamiento de datos por parte de terceros dentro o fuera de sus locales, reguladas bajo el artículo 12 de la LOPD, y artículo 83 del Reglamento, ha sido recogida por la organización en el "**Documento de Aplicación LOPD FORMACIONL"**.

📖 En este Documento de Seguridad***, 6.5.- Anexo IV-1: Tratamiento de datos por terceros para FORMACIONL*** se recogen las prestaciones de servicios con acceso a datos protegidos, así como la referencia al contrato bajo el que se suscribe dicha prestación.

6.5.3.3.- Identificación, autenticación y control de accesos

El objetivo de este procedimiento es definir y establecer la operativa para la gestión de las restricciones de acceso a los sistemas de información de **FORMACIONL** susceptibles de contener datos de carácter personal, describiendo los procedimientos generales y los protocolos de identificación y autenticación de acceso, con el fin de evitar accesos no autorizados.

El Responsable del Fichero (y, por delegación de este, el Responsable de Seguridad) es el encargado de definir los criterios de autorización de acceso que se deben conceder a cada persona usuaria (a qué ficheros debe tener acceso cada uno, con qué limitaciones, etc.).

El **Responsable de Seguridad Global**, apoyado por los **Responsables de Seguridad Gerenciales** son los encargados de mantener la relación actualizada de las personas usuarias y derechos de accesos concedidos a cada uno de ellos sobre los datos protegidos, siguiendo las políticas y procedimientos indicados a continuación.

📖 En el 6.5.- ***Anexo II – Personas usuarias autorizadas con acceso a los ficheros*** se recoge la relación de las personas usuarias y derechos de acceso autorizados.

6.5.3.3.1.- Política de gestión de control de accesos

- **Política de mínimo privilegio**. Las personas usuarias recibirán derechos de acceso únicamente a aquellos datos (automatizados o no) y recursos que precisen estrictamente para el desarrollo de sus funciones.
- **No se permiten identificadores ni claves de acceso comunes**, es decir, no existirán identificadores/claves de acceso que sean utilizados por más de una persona usuaria. A cada persona usuaria se le asignará una credencial (par "identificador-clave de acceso) para su uso exclusivo.
- **No se permiten accesos anónimos**. Todo acceso a los Ficheros debe ir precedido por la autenticación de la persona usuaria ante el sistema de tratamiento de dicho fichero.

- **Sólo se permiten cinco intentos de acceso fallidos como máximo.** Tras superar dicho número de intentos de acceso fallidos, la persona usuaria en cuestión quedará bloqueada. Los Administradores de Sistemas respectivos (ver 6.5.- **Anexo II**) se encargarán de desbloquearlo tras aclarar convenientemente el incidente y asegurarse de que no se ha tratado de un intento de acceso fraudulento.

6.5.3.3.2.- Normas para la generación y gestión de identificadores de la persona usuaria

FORMACIONL impone las siguientes restricciones en el uso de identificadores:

- **Eliminar todos aquellos identificadores de acceso que vienen por defecto** en los sistemas operativos y en las aplicaciones de software. Si no fuera posible su eliminación, la contraseña de estos identificadores deberá modificarse. Ejemplos: *root*, etc.

  Las normas para la creación y gestión de identificadores de las personas usuarias. Son las siguientes:

  - **Para los nombres simples**, los identificadores estarán formados por el nombre de la Persona usuaria y su primer apellido. Si existiera, se utilizaría el segundo apellido en lugar del primero. Ej: nombre+1erApellido nombre+2ºApellido
  - **Para los nombres compuestos**, los identificadores estarán formados por el primer nombre de la Persona usuaria, el primer carácter del segundo nombre y su primer apellido. Si existira, se utilizaria el segundo apellido en lugar del primero. Ej: nombre+1ercaracter2ºNombre+1erApellido nombre+1ercaracter2ºNombre+2ºApellido

6.5.3.3.3.- Normas para la generación y gestión de contraseñas

FORMACIONL impone las siguientes restricciones para la asignación de contraseñas:

- Las contraseñas deben cumplir los siguientes requisitos de seguridad:
  - Las contraseñas deberán tener una longitud mínima de 8 caracteres
  - Las contraseñas estarán compuestas por una combinación de minúsculas y números
  - No podrá repetirse como nueva contraseña la última empleada
  - Las contraseñas tendrán una validez máxima de 1 año (vigencia)

Además de las restricciones para la creación de contraseñas, **FORMACIONL** establece las siguientes medidas a fin de mejorar la seguridad de las contraseñas.

- Cuando se introduzca una contraseña, esta no será visible por pantalla.
- Toda persona usuaria podrá cambiar su contraseña de acceso a los sistemas de información o podrá solicitar al Administrador del Sistema que le active la posibilidad de cambiarla; **en cualquier momento..**
- Los sistemas de información están configurados para notificar y obligar a las personas usuarias a cambiar de contraseña antes de que venza.
- Cuando una contraseña vence (al no ser cambiada dentro del periodo establecido), la cuenta de la persona usuaria se bloqueará automáticamente.
- Todo el software usado en **FORMACIONL** para identificación y validación de las personas usuarias debe almacenar las contraseñas de forma ininteligible (a través de un algoritmo *hash* de una sola vía o similar) para garantizar la confidencialidad de las mismas.
- No emplear las contraseñas por defecto, debiendo cambiarse aquellas que vinieran previamente definidas por el fabricante o instalador para cualquier dispositivo, sistema operativo u aplicación que permita el acceso (directa o indirectamente) a los datos protegidos o a los sistemas que los contengan.

6.5.3.3.4.- Procedimiento de Alta / Baja / Modificación de las personas usuarias

- Cuando se requiera dar de alta / baja / modificar a una persona usuaria, **el Director /Gerente** correspondiente deberá **solicitarlo por escrito al Responsable de Seguridad Global**, indicando el perfil específico de acceso a

establecer / modificar / denegar para la persona usuaria en cuestión, en cada una de los sistemas / aplicaciones / ficheros a tratar solicitados.

- El responsable de Seguridad Global valorará si las solicitudes se ajustan a la **Política de mínimo privilegio de FORMACIONL**. Si tienen dudas, lo consultarán con el cada Responsable de Fichero.
- Las solicitudes aprobadas se notificarán por el Administrador de Sistemas-Responsable de Autenticación , quien:
    - Comunicará a la persona usuaria sus credenciales de acceso, de forma confidencial y previa acreditación de la personalidad de la persona usuaria, obligando a la persona usuaria, en todo caso, a cambiar la contraseña en el primer acceso.
    - Anotará la concesión de permisos en el registro del 6.5.- **ANEXO II: Personas usuarias autorizadas con acceso a los ficheros**.
    - Almacenará información histórica sobre los perfiles de acceso concedidos, así como sobre la cancelación de permisos de acceso, durante el tiempo requerido para cumplir obligaciones legales y para auditoría (al menos **5 años**).

6.5.3.3.5.- Control de acceso a puestos informatizados

- Todos los puestos informáticos se han configurado por el personal de la Dirección de Sistemas o al personal informático de las Gerencias; para requerir la identificación y autenticación de la persona usuaria antes de poder hacer uso de los mismos.
- Como medida adicional, todos los ordenadores están configurados para bloquear la sesión de la persona usuaria y ocultar la información de la pantalla tras un periodo de inactividad de **5 minutos**, requiriéndose la introducción de una contraseña para poder desbloquear la sesión.

6.5.3.3.6.- Control de acceso físico a salas de servidores (CPDs)

Las salas donde se encuentran ubicados los contenedores de datos de carácter personal de nivel medio o alto, han sido dotadas de medidas de protección para garantizar la disponibilidad y confidencialidad de los datos protegidos.

Estas salas ***de la DIRECCIÓN GENERAL TÉCNICA, de las Gerencias Provinciales y de los Centros*** están protegidas de las siguientes maneras

- La sala del CPD dispone de puerta con control de acceso que requiere tarjeta y alarma con clave de acceso.
- Las tarjetas son individuales y no se comparten entre personas usuarias.
- El acceso está restringido al personal expresamente autorizado por el Responsable de Seguridad Global / Gerencias (ver 6.5.- **Anexo II**).
- Cualquier otra persona que necesite acceder a dichas salas será acompañada por una persona usuaria autorizada. Se incluye bajo este punto, pero no exclusivamente, al personal que realiza labores de limpieza y de mantenimiento general (electricidad, conducciones, instalaciones de nuevos equipos, etc.).

6.5.3.3.7.- Control de acceso físico a salas de Archivos-Papel

- ***Archivos-Papel en la Dirección General Técnica, Gerencia de Málaga y Gerencia de Sevilla***
  - Dispone de puerta con control de acceso que requiere tarjeta y alarma con clave de acceso.
  - Las tarjetas son individuales y no se comparten entre personas usuarias.
  - El acceso está restringido al personal expresamente autorizado por el Responsable de Seguridad Global / Gerencias (ver 6.5.- **Anexo II**).
  - Cualquier otra persona que necesite acceder a dichas salas será acompañada por una persona usuaria autorizada. Se incluye bajo este punto, pero no exclusivamente, al personal que realiza labores de limpieza y de mantenimiento general (electricidad, conducciones, instalaciones de nuevos equipos, etc.).
- ***Archivos-Papel de las Gerencias Provinciales***
  - Dispone de sala con acceso restringido

- El acceso está restringido al personal expresamente autorizado por el Responsable de Seguridad Global / Gerencias (ver 6.5.-**Anexo II**).
- Cualquier otra persona que necesite acceder a dichas salas será acompañada por una persona usuaria autorizada. Se incluye bajo este punto, pero no exclusivamente, al personal que realiza labores de limpieza y de mantenimiento general (electricidad, conducciones, instalaciones de nuevos equipos, etc.).

6.5.3.3.8.- Control de acceso a través de redes de comunicaciones

- El acceso remoto a los sistemas de información de **FORMACIONL** desde las Gerencias Provinciales sólo se puede realizar a través de la red de la Organización, requiriendo a todas sus personas usuarias:
  - Utilizar los servicios de acceso remoto proporcionados por personal del Dirección de Servicios Generales y Sistemas.
  - Que se autentiquen con un identificador de red único ante el servidor de dominio de la red.
- **FORMACIONL** no permite el acceso a su red desde redes públicas, ni desde redes inalámbricas, excepto a cierto personal del Dirección de Sistemas que lo utiliza para tareas de mantenimiento y administración de los sistemas desde el exterior de la red de la Organización. Este personal esta identificado en 6.5.-Anexo II.
- **FORMACIONL** permite el acceso desde su red a Internet. Para controlar dichos accesos, la Dirección General Técnica de **FORMACIONL** ha implementado las correspondientes reglas de filtrado en sus *firewalls* y proxys corporativos:
  - Las Gerencias utilizan como salida a Internet la propia red de la Organización, cuya IP pública esta enmascarada. Para filtrado de contenidos y balanceo de carga existe un Proxy o un enrutador encargado de redireccionar las salidas a exterior.
  - En los centros donde existe una línea de conexión alternativa (ADSL, Cable, etc.) esta implantado un Proxy que filtra el acceso a Internet, en

cuanto a la entrada no esta permitida. La entrada es impedida por los propios router que tienen todos lo puertos cerrados.

- La salida a Internet desde la DGT se hace a través de un Proxy encargado del filtrado de contenidos así como del balanceo de carga.
- En la DGT existen varios Firewall que filtran las entradas desde hasta distintos puntos:
  - Firewall Internet, este filtra el acceso desde exterior a los servicios corporativos. Es un servidor gestionado por GNU/Linux distribución Debian, el proceso de filtrado se hace desde el propio núcleo con script de IPTABLES.
  - Firewall VPN, este filtra el acceso desde las sedes (Gerencias) a los servicios corporativos. Es un servidor gestionado por GNU/Linux distribución Debian, el proceso de filtrado se hace desde el propio núcleo con script de IPTABLES.
  - Firewall LAN DGT, este filtra el acceso desde los puestos de trabajo de las personas usuarias en la DGT a los servicios corporativos. Es un servidor gestionado por GNU/Linux distribución Debian, el proceso de filtrado se hace desde el propio núcleo con script de IPTABLES.

📖 Las características generales del entorno de red de **FORMACIONL** se muestran en el apartado *"6.5.0* - 6.5.8.3.- Entorno de *red"*.

FORMACIONL provee a persona el acceso a Internet. El acceso es a través de sistemas de acceso estándar (ADLS, Cable, etc). Para proteger de accesos no deseados, virus, etc, se han instalado proxys entre las distintas redes locales e Internet, basados en Linux (Debian) y Squid.

6.5.3.4.- Gestión de soportes y documentos

Soporte: objeto físico que almacena o contiene datos o documentos[24], u objeto susceptible de ser tratado en un sistema de información y sobre el cual se pueden grabar y recuperar datos.

Según el artículo 92 del RLOPD, "*los soportes y documentos que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen, ser inventariados y solo deberán ser accesibles por el personal autorizado para ello en el documento de seguridad*".

Dado que la mayor parte de los soportes que hoy en día se utilizan, (disquetes, CD-ROMs, etc.), son fácilmente transportables, reproducibles y/o copiables, es evidente la importancia que para la seguridad de los datos de los ficheros tiene el control de estos medios. Para ello, **FORMACIONL** ha establecido procedimientos para la gestión de todo lo relativo a los soportes y documentos que contengan datos de carácter personal.

6.5.3.4.1.- Inventario de documentos-papel

Todos los documentos-papel que contengan datos personales irán protegidos por una carpeta en cuyo exterior llevarán adherida una etiqueta que identificará:

Con una herramienta informática se generará un código autonumérico compuesto por el código de fichero, unidad de negocio, año, secuencial

Tipo de fichero, identificando el tipo de fichero de datos personales que contiene:

- **AUTO** para identificar datos del fichero de USUARIAS AUTOORIENTACION
- **RRHH** para identificar datos del fichero de RR.HH.
- **CLI** para identificar datos del fichero CLIENTES Y PROVEEDORES
- **AGE** para identificar los datos del fichero AGENDA CORPORATIVA

[24] Se debe entender que se emplea la palabra "soporte" respecto a los documentos, para referirse al continente (normalmente, papel) y no al contenido (los datos sobre el papel).

- **EVE** para identificar los datos del fichero EVENTOS
- **CONTA** para identificar los datos del fichero CONTABILIDAD
- **CV** para los datos del fichero CURRICULOS FORMACIONL
- **MKT** para los datos del fichero COMUNICACIÓN Y MARKETING
- **BEN** para los datos del fichero USUARIAS

✓ **Unidad de negocio**, de la Organización a la que corresponde la información.

✓ **Año de creación del documento**

✓ **Número secuencial.**

De todos estos documentos-papel existirá una relación actualizada y cuyo acceso estará restringido a:

- los Responsables de Seguridad (Global y Provinciales, respectivamente)
- los Responsables de Ficheros de la DGT
- los Responsables de Dirección/Gerencia/Centros respectivos

Sólo estos responsables pueden autorizar la eventual entrada / salida de dichos soportes de las oficinas de **FORMACIONL**.

6.5.3.4.2.- Inventario y Etiquetado de Soportes Electrónicos

El Administrador de Sistemas-Responsable de Soportes se encargará de inventariar todos los soportes electrónicos (portátiles, copias de seguridad, etc.).

El inventario actualizado será mantenido de acuerdo al modelo indicado en el apartado ***"6.5.9.2 Inventario de Soportes Electrónicos Removibles – Formato".***

Con una herramienta informática se generará un código autonumérico compuesto por el código de fichero, unidad de negocio, año, secuencial

Tipo de fichero, identificando el tipo de fichero de datos personales que contiene:

- **AUTO** para identificar datos del fichero de USUARIAS AUTOORIENTACION
- **RRHH** para identificar datos del fichero de RR.HH.

- **CLI** para identificar datos del fichero CLIENTES Y PROVEEDORES
- **AGE** para identificar los datos del fichero AGENDA CORPORATIVA
- **EVE** para identificar los datos del fichero EVENTOS
- **CONTA** para identificar los datos del fichero CONTABILIDAD
- **CV** para los datos del fichero CURRICULOS FORMACIONL
- **MKT** para los datos del fichero COMUNICACIÓN Y MARKETING
- **BEN** para los datos del fichero USUARIAS

✓ **Unidad de negocio**, de la Organización a la que corresponde la información.

✓ **Año de creación del documento**

✓ **Número secuencial.**

6.5.3.4.3.- Registro de Entrada / Salida de Soportes

El Responsable de Soportes de Almacenamiento Central de la Organización / Responsables de Seguridad de las Gerencias asegurarán el mantenimiento de un registro de los soportes / documentos que se reciben / envían fuera de la Organización, utilizando para ello los formularios indicados en el apartado *"6.5.**0 - 6.5.9.3.- Registro de entrada / salida de soportes y documentos -** Formato.*

6.5.3.4.4.- Controles para el envío y transporte de soportes

La salida de soportes fuera de las oficinas de **FORMACIONL** deberá ser siempre autorizada por el Responsable de Seguridad / Responsables de Seguridad de las Gerencias y, en principio, sólo será autorizada en los siguientes casos:

- Traslado de copias de respaldo entre los locales indicados en el apartado "6.5.0
- 6.5.8.1.- Centros de tratamiento *y locales*" como medida encaminada a garantizar la disponibilidad de la información.
- Reparaciones de dispositivos averiados para por proveedores de servicio técnico autorizado (ver 6.5.- **Anexo IV-1**:*Tratamiento de datos por Terceros para FORMACIONL)*.

Para el traslado de soportes fuera de los locales de **FORMACIONL**, se establecen como únicos medios de transporte autorizados los siguientes:

- A través de personal propio de **FORMACIONL.**
- A través de mensajería externa, subcontratada por **FORMACIONL** con proveedores autorizados (ver 6.5.- **Anexo IV-1**: *Tratamiento de datos por Terceros para FORMACIONL)*.

6.5.3.5.- Régimen de trabajo fuera de las oficinas de FORMACIONL

Este título aborda aquellas situaciones bajo las que el personal, para el cumplimiento de sus funciones, deba acceder a datos de los Ficheros fuera de los locales habilitados para ello por **FORMACIONL,** esto es, **fuera de:**

- Dirección General Técnica
- Gerencias Provinciales
- Centros de la Organización

Estas situaciones son excepcionales en **FORMACIONL,** por lo que se establece que es necesario la autorización explicita del Responsable de Seguridad o del Responsable de Seguridad de la Gerencia correspondiente.

Así pues, como **norma general**, está **prohibido hacer uso de datos personales en formato papel fuera de los locales habilitados a tal fin por FORMACIONL**.

En caso necesario, el acceso se realiza a través de:

- ✓ NAVISIÓN, a través de CITRIX
- ✓ Webmail, a través de HTTPS con certificado de VERISIGN
- ✓ Portal del Empleado, a través de HTTPS con certificado de VERISIGN
- ✓ Intranet, a través de HTTPS con certificado de VERISIGN
- ✓ SAP, cliente de encriptación de nivel 2.

6.5.3.6.- Ficheros temporales

Con la intención de minimizar riesgos, **FORMACIONL** ha tratado de cubrir, en el sentido más amplio, el concepto de fichero temporal.

En **FORMACIONL** se determina que la condición de fichero temporal la cumplen, al menos, los siguientes tipos de ficheros automatizados tratados:

a. **Ficheros *batch***: ficheros de trabajo o intermedios que pudieran generar automáticamente las aplicaciones (por medio de procesos *batch*).
b. **Colas de impresión**: ficheros que se generan automáticamente en las colas de impresión.
c. **Ficheros Ofimáticos**: ficheros que las propias personas usuarias finales pudieran generar personalmente (ej.: vía MS-Office), utilizando herramientas de recuperación masiva de información desde BBDD centralizadas (ej.: vía *export*) o bien, simplemente por haberlos recibido por correo electrónico.
d. **Datos-papel:** copias de documentos en papel que contengan datos personales (fotocopias, transcripciones manuscritas para realizar alguna actividad, etc.).

Atendiendo al planteamiento expuesto, a continuación se describen las obligaciones y normas para el tratamiento de cada uno de los tipos de ficheros mencionados:

a. Ficheros *batch*

Si en algún momento llegaran a generarse ficheros *batch*, el personal informático encargado de supervisar la puesta en producción del software desarrollado para **FORMACIONL** asegurará que se programa la eliminación de los ficheros *batch* tras finalizar de forma correcta la ejecución del/los proceso/s que los hubieran creado.

b. Colas de impresión

Los Administradores de Sistemas han configurado las colas de impresión para que estos ficheros sean automáticamente eliminados, tras finalizar el proceso de impresión o tras la cancelación del mismo.

c. Ficheros Ofimáticos

El uso de herramientas de recuperación masiva de información ha sido prohibido en **FORMACIONL** a las personas usuarias finales.

Por otra parte, TODOS los ficheros ofimáticos que generen las personas usuarias deben cumplir los siguientes requisitos:

- Su creación y tratamiento deberá haber sido previamente autorizado por alguno de los Responsables de Seguridad de la Organización.
- No deberán almacenarse en ordenadores personales, sino en directorios departamentales o personales, pero **SIEMPRE** localizadas en un servidor central (de la Dirección General Técnica o de la Gerencia Provincial), sometidos a los controles de acceso definidos por el Responsable de Seguridad, que serán en todo caso equivalentes a los controles aplicables a los ficheros declarados con los que se relacionen sus datos.

d. Datos-papel

- Ninguna persona usuaria hará copias de datos personales si no es estrictamente necesario para el desempeño de sus funciones.
- Cuando sea necesario hacer copias de datos personales, la persona usuaria **está obligado** a aplicar las mismas medidas para su protección contra accesos no autorizados que las que corresponden para el nivel del fichero del que hubieran sido extraídos.
- Una vez finalizado su uso, la persona usuaria **debe** destruir dichas copias.

6.5.4.- Procedimiento ante incidencias

Definición de Incidencia

Según la Agencia Española de Protección de Datos, se considera "incidencia de seguridad", entre otras, cualquier incumplimiento de la normativa desarrollada en este Documento de Seguridad, así como a cualquier anomalía que afecte o pueda afectar a la seguridad de los datos de carácter personal.

Con el objeto de dar debido cumplimiento a lo establecido en el RLOPD art. 88.3.e), **FORMACIONL** dispone este procedimiento de notificación, gestión y respuesta de las incidencias.

6.5.4.1.- Tipo de Incidencias que se deben notificar

A continuación se presenta una lista de incidencias que serán inexcusablemente registradas. Esta lista podrá ser ampliada con otro tipo de incidencias que pudieran haber quedado omitidas:

1. Incidencias que afecten a la identificación y autenticación de las personas usuarias:
    - Pérdida de confidencialidad de contraseñas.
    - Detección de accesos irregulares (intentos fallidos de accesos, accesos fuera de horas de oficina, etc.) tras la revisión de "logs".
    - Períodos de desactivación de las herramientas de seguridad.
    - Comunicación de las personas usuarias de sospechas de que alguien ha suplantado su identificación en la Organización.
2. Incidencias que afecten a los derechos de acceso a los datos:
    - Solicitudes de modificación de derechos de acceso sobre datos.

- Solicitudes de modificación de derechos de acceso sobre herramientas de gestión de acceso y utilidades con accesos privilegiados.

3. Incidencias que afecten a la gestión de soportes.
   - Comunicación de pérdida de soportes.
   - Comunicación de localización de soportes en lugares inadecuados.
   - Errores de contenido en soportes recibidos y enviados.
4. Incidencias que afecten a los procedimientos de copias de salvaguarda y recuperación:
   - Errores detectados en los procesos de realización de copias de salvaguarda.
   - Procedimientos de recuperación de datos realizados.
5. Incidencias que afecten a ficheros no automatizados (en papel)
   - Soportes o documentos con datos hallados fuera de la Organización sin custodia.
   - Detección de copias no autorizadas de datos del Fichero.
6. Incidencias que afecten al cumplimiento de las normas de seguridad establecidas:
   - Cualquier incumplimiento de medidas de las medidas de seguridad y protección de datos personales.
7. Cualquier otra incidencia de las observadas como consecuencia de la ejecución de los controles definidos para garantizar el cumplimiento de lo dispuesto en el Documento de Seguridad (auditorías bienales, revisiones mensuales, etc).

6.5.4.2.- Procedimiento de Notificación de Incidencias

Toda persona usuaria (definido en 6.5.2.7) de **FORMACIONL** deberá notificar inmediatamente, al Responsable de Seguridad Global o al Responsable de Seguridad de las Gerencias, cualquier incidencia que detecte y que estime pueda afectar a la seguridad de los datos y recursos protegidos.

La notificación la hará a través de cualquiera de los medios dispuestos para ello por **FORMACIONL** y que se han comunicado a todo el personal mediante circular interna., a través del Centro de Soporte en la Intranet.

📖 En el 6.5..- ***Anexo V – Responsable de Seguridad: Comunicación***, se incluye la circular informativa en la que se **FORMACIONL** comunica al personal el nombramiento del Responsable de Seguridad, así como los medios de contacto con el mismo, los cuales son los únicos medios habilitados para la notificación de incidencias.

El retraso en la notificación de incidencias constituirá un quebranto de la buena fe contractual, sancionable según la normativa laboral aplicable.

6.5.4.3.- Registro de Incidencias

El Responsable de Seguridad, de conformidad con el RLOPD artículos 90 y 100, mantiene un registro en formato electrónico de las incidencias, en el cual se hace constar la siguiente información relativa a las mismas:

- Tipo de incidencia (según la clasificación del apartado 0).
- Fecha y hora en la cual se ha producido la incidencia.
- Persona que realiza la notificación.
- Personas a quienes se le comunica la incidencia.
- Efectos derivados de dicha incidencia.
- Medidas correctoras aplicadas. En caso de ser necesaria la recuperación de datos:
    - Procedimientos de recuperación de datos efectuados
    - Personas que los llevan a cabo
    - Datos restaurados
    - Datos grabados manualmente

En el apartado *"6.5.0 - 6.5.9.1.- Registro de Incidencias - Formato"* se adjunta el modelo de formato que el Responsable de Seguridad utilizará para el registro de incidencias. Dichos registros serán almacenados, por el Responsable de Seguridad, a efectos históricos durante el tiempo requerido para cumplir obligaciones legales y de auditoría (al menos **5 años**).

6.5.4.4.- Respuesta a Incidencias

Es obligación del Responsable de Seguridad gestionar las incidencias de seguridad que pudieran producirse, debiendo **iniciar su resolución en un plazo inferior a 10 días desde la notificación**.

También es obligación del Responsable de Seguridad supervisar el trabajo de subsanación de la anomalía detectada y anotar en el registro de la incidencia todas las acciones y medidas tomadas para resolver o minimizar dicha incidencia.

A efectos de control, se incluye en el propio registro de la incidencia la información que permite verificar el cumplimiento del tiempo de respuesta ante incidencias.

6.5.5.- Gestión de copias de respaldo y recuperación de datos personales

Las tareas asociadas a la obtención y recuperación de copias de respaldo son delegadas por el Responsable de Seguridad en los respectivos "**Responsables Administradores de Copias de Respaldo**", indicados en el 6.5.- **Anexo II**.

6.5.5.1.- Política de copias de respaldo en la Dirección General Técnica

La Dirección General Técnica dispone de un sistema de copias de respaldo, proporcionado como servicio central, basado en cintas-cartucho (ver apartado "***0 – 6.5.6.5.8.4.8.- Servicio de realización de copias de*** respaldo").

La Dirección General Técnica ha establecido, de común acuerdo con el Responsable de Seguridad Global, la siguiente política para la obtención y archivo de copias de respaldo de ficheros de datos contenidos en sus servidores centrales:

1) **Diarias**. Las copias de respaldo realizadas de lunes a domingo son completas. Las copias diarias serán conservadas durante 15 días y después se sobreescriben.
2) **Semanales.** La copia diaria correspondiente al 7 día de cada semana será la copia semanal, por tanto, completa. Las copias semanales serán conservadas durante un mes y después se sobreescriben.
3) **Mensuales**. La copia semanal correspondiente a la semana 4 de cada mes será la copia mensual, por tanto, completa. Las copias mensuales serán conservadas durante 12 meses y después se borran.
4) **Anuales**. La copia mensual correspondiente al mes 12 de cada año será reservada como copia anual. Las copias anuales serán conservadas durante 5 años y después se borran.
5) **Inventario de copias**. El software de backup mantiene de forma automática el inventario de copias y soportes utilizados para cada una de ellas. Si la operación de copia falla, el Administrador de Copias de Respaldo deberá realizarla nuevamente. Si

falla por dos veces consecutivas, deberá notificarlo como incidencia al Responsable de Seguridad y proceder a la destrucción del soporte, dándolo de baja en el inventario.

6) **Almacenamiento de copias**. Las copias realizadas en cintas se almacenan en un armario en el CDP y semanalmente en una caja de seguridad en una caja de seguridad en la Gerencia de Sevilla (se prevé incluir en una sucursal de Cajax); manteniendo el Administrador de Copias de Respaldo para el Responsable de Seguridad un registro de entrada-salida de estos soportes (ver 6.5.0. 6.5.9.3.- Registro de entrada / salida de soportes y documentos - *Formato*". La llave los armarios está custodiada por el Administrador de Copias de Respaldo.

6.5.5.2.-Política de copias de respaldo en las Gerencias Provinciales.

La Dirección General Técnica ha establecido, de común acuerdo con el Responsable de Seguridad Global y sus Gerencias, una política para la obtención y archivo de copias de respaldo de los servidores de las Gerencias Provinciales semejante a la definida para la Dirección General Técnica, según lo descrito en el apartado anterior.

6.5.5.3.- Autorización para restauración de datos desde copias de respaldo

Según el RLOPD art. 100.2), cuando sea necesaria la recuperación de datos de ficheros de nivel medio y alto, es obligatoria la autorización por escrito del Responsable del Fichero.

Por norma, cuando los Responsables de una Dirección / Gerencia / Centro de Referencia necesiten la recuperación de datos contenidos en copias de seguridad, lo notificarán al **Responsable de Seguridad Global / Responsables de Seguridad de Gerencias**, como una **incidencia**.

Los Responsables de Seguridad tratarán la incidencia, analizando y verificando la necesidad real y el motivo por el que se solicita la restauración de los datos, antes de autorizar la restauración al Administrador de Copias de Respaldo.

6.5.5.4.- Restauración manual de datos

Cuando la pérdida de datos de datos no pueda ser restaurada íntegramente desde la copia de respaldo electrónica y se requiera la re-grabación manual de los datos, los Responsables de Seguridad registrarán este hecho como una incidencia, analizando y verificando la necesidad real y el motivo por el que se solicita la restauración de los datos, antes de autorizar la restauración a los Responsables de Dirección / Gerencia / Centro de Referencia solicitantes.

6.5.5.5.- Registro de realización de copias de respaldo

El sistema de copias de respaldo utilizado por **FORMACIONL**, Veritas 10.0 asegura la existencia y mantenimiento de un registro-inventario de las copias de respaldo que se realicen, tanto en la Dirección General Técnica y en las Gerencias Provinciales el Backup de Windows. El Administrador de Copias de Respaldo/ los Responsables de Seguridad de las Gerencias serán los encargados de asegurar que se mantiene actualizado dicho inventario.

Dicho inventario incluirá:

- Ficheros de datos personales incluidos en cada copia
- Fecha de realización
- Identificador (y nº de secuencia) del soporte donde se ha realizado
- Tipo de copia (diaria, semanal, …)

6.5.5.6.- Registro de restauración de datos personales

El Administrador de Copias de Respaldo/ los Responsables de Seguridad de las Gerencias asegurarán la existencia y mantenimiento actualizado de un registro que identifique la relación de las restauraciones de datos personales que se realicen.

Dicho registro incluirá:

- Ficheros de datos personales afectados por la restauración
- Fecha de restauración
- Nº de incidencia que ha dado origen a la restauración
- Datos restaurados (registros, campos, etc.)

6.5.5.7.- Pruebas de software con copias de respaldo

FORMACIONL establece la prohibición expresa de realizar pruebas de nuevos programas software con copias de seguridad que contengan datos reales.

Excepcionalmente, en caso de ser necesaria la realización de pruebas con copias de respaldo, las pruebas deberán estar autorizadas expresamente por los Responsables de Seguridad, debiendo quedar el hecho registrado como una incidencia. En tal caso, los Responsables de Seguridad deberán asegurar que dichas pruebas se realizan con el mismo nivel de seguridad que exigen los datos originales, o bien que los datos utilizados hayan sido previamente disociados de los datos identificativos de personas.

6.5.6.- Auditorías y controles periódicos

6.5.6.1.-Auditorías

En cumplimiento de lo dispuesto en el del RLOPD art. 96, de forma periódica, **cada 2 años**, se realizará una auditoría de los sistemas de información y del personal objeto del alcance del documento de Seguridad para los ficheros de nivel medio u alto. La auditoría podrá ser interna o externa, según se considere oportuno en el momento de su realización.

También será necesaria la realización de una auditoría cuando se produzcan modificaciones sustanciales en los sistemas de información y organizativos con repercusión en la seguridad de los datos protegidos.

El objeto de la auditoría será medir el grado de cumplimiento de las medidas de seguridad establecidas por el RLOPD y de los procedimientos, instrucciones y políticas desarrolladas en el Documento de Seguridad.

El Responsable de Seguridad analizará el informe de auditoría y elevará las conclusiones obtenidas, junto con propuestas de mejora, al Responsable del Fichero para que adopte las medidas correctoras adecuadas.

El informe de auditoría será custodiado por el Responsable de Seguridad, por si fuera requerido por la Agencia de Protección de Datos.

Todo el personal de **FORMACIONL** y los proveedores de servicios externos que tengan acceso a los datos personales deberán prestar en todo momento su colaboración para llevar a cabo los controles necesarios y su correspondiente auditoría a requerimiento del Responsable de Seguridad.

6.5.6.2.- Controles periódicos para verificar cumplimiento de normas (solo para nivel medio y alto)

En cumplimiento de lo dispuesto en el RLOPD, art. 88.4, para los ficheros de nivel medio y alto, el **Responsable de Seguridad** realizará los siguientes controles:

- **Mensualmente**:
  - Analizará las incidencias registradas, asegurando que se han tomado las medidas oportunas para su resolución en los plazos previstos.
  - Revisará los controles de acceso físico a ficheros (electrónicos y papel), y elaborará un informe con las comprobaciones realizadas y los problemas detectados.
  - Revisará la integridad de las copias de respaldo
- **Mensualmente (solo nivel alto)**:
  - Revisará los registros de intentos de acceso (logs) a ficheros y elaborará un informe con las comprobaciones realizadas y los problemas detectados.
- **Cada seis meses**
  - Verificará los permisos de acceso concedidos a las personas usuarias para cada fichero, para asegurar que coinciden con los autorizados.
  - Verificará la definición y correcta aplicación de los procedimientos de copia de seguridad definidos en el apartado “6.5.0 - 6.5.5.- Gestión de copias de respaldo y recuperación de datos personales”.

6.5.7.- Relación de Ficheros inscritos en la AEPD y Descripción detallada de su estructura

En la siguiente tabla se recoge la información de los ficheros declarados en el Registro General de Protección de Datos (RGPD), indicando el sistema de tratamiento (manual, automatizado o mixto) y el nivel de seguridad asignado:

(En este caso los códigos de inscripción y fechas son ficticios)

Nombre de Fichero	Código inscripción R.G.P.D.	Fecha de inscripción	Sistema de tratamiento	Nivel seguridad
USUARIAS AUTOORIENTACION	1111111111z	Esperando respuesta de AEPD	mixto	MEDIO
RECURSOS HUMANOS	1111111111a	Esperando respuesta de AEPD	mixto	MEDIO
CLIENTES Y PROVEEDORES	1111111111a	Esperando respuesta de AEPD	mixto	BÁSICO
AGENDA CORPORATIVA	1111111111a	Esperando respuesta de AEPD	mixto	BÁSICO
EVENTOS	1111111111a	Esperando respuesta de AEPD	mixto	BÁSICO
CONTABILIDAD Y HACIENDA PÚBLICA	1111111111a	Esperando respuesta de	mixto	MEDIO

		AEPD		
CURRICULOS FORMACIONL	1111111111a	Esperando respuesta de AEPD	Mixto	MEDIO
COMUNICACIÓN Y MARKETING	1111111111a	Esperando respuesta de AEPD	Mixto	BÁSICO
USUARIAS	1111111111a	Esperando respuesta de AEPD	Mixto	BÁSICO

Los ficheros inscritos por **FORMACIONL** en el RGPD son ficheros lógicos, por lo que debe entenderse que, si bien la ubicación de los ficheros está acotada, esta puede no ser única.

Todos los ficheros se conservan tanto en papel como en formato electrónico. A continuación se presenta la **estructura lógica** de los datos contenidos en los ficheros.

6.5.7.1.- Descripción detallada de los Ficheros

FICHERO	**USUARIAS AUTOORIENTACION**
NIVEL	MEDIO
DATOS CARÁCTER IDENTIFICATIVO	D.N.I./N.I.F.;TELEFONO; FIRMA ELECTRONICA; NOMBRE Y APELLIDOS; DIRECCIÓN DE E-MAIL; CONTRASEÑA; IDENTIFICADOR DE ACCESO; ALTA COMO DEMANDANTE DE EMPLEO de beneficiarios del servicio de **Auto-Orientación para el Empleo**.
OTROS TIPOS DE DATOS	DATOS DE CARACTERISTICAS PERSONALES; DATOS DE EMPLEO

FICHERO	RECURSOS HUMANOS
NIVEL	MEDIO
DATOS CARÁCTER IDENTIFICATIVO	D.N.I. /N.I.F.; NUM. S. S. /MUTUALIDAD; NOMBRE Y APELLIDOS; DIRECCION; TELEFONO; CREDENCIALES (personas usuarias y contraseña); FIRMA ELECTRÓNICA; IMAGEN/VOZ; FIRMA/HUELLA; FIRMA ELECTRONICA
OTROS TIPOS DE DATOS	DATOS DE CARACTERISTICAS PERSONALES; DATOS DE CIRCUNSTANCIAS SOCIALES; DATOS ACADEMICOS Y PROFESIONALES; DATOS DE DETALLES DE EMPLEO; DATOS ECONOMICOS FINANCIEROS Y DE SEGUROS; Nº DE HIJOS; NOMBRES DE LOS HIJOS; ESTADO CIVIL; MINUSVALÍA; GRADO DE MINSUVALÍA; CUENTA BANCARIA; CÓNYUGE **AFILIACION SINDICAL**

FICHERO	CLIENTES Y PROVEEDORES
NIVEL	BÁSICO
DATOS CARÁCTER IDENTIFICATIVO	D.N.I./N.I.F.;NOMBRE Y APELLIDOS; DIRECCION; TELEFONO; OTROS DATOS DE CARACTER IDENTIFICATIVO; NUM.S.S./MUTUALIDAD;; FIRMA/HUELLA; FIRMA ELECTRONICA;
OTROS TIPOS DE DATOS	NUM.S.S./MUTUALIDAD; PERSONA DE CONTACTO; TRANSACCIONES DE BIENES Y SERVICIOS; DATOS ACADEMICOS Y PROFESIONALES; CORREO ELECTRÓNICO; IMAGEN Y VOZ; Nº DE COLEGIADO

FICHERO	AGENDA CORPORATIVA
NIVEL	BÁSICO
DATOS CARÁCTER IDENTIFICATIVO	NOMBRE Y APELLIDOS; DIRECCION; TELEFONO; IMAGEN/VOZ; D.N.I; FIRMA/HUELLA; FIRMA ELECTRONICA; CORREO ELECTRONICO.
OTROS TIPOS DE DATOS	PERSONAS DE CONTACTO; CARGOS PÚBLICOS

FICHERO	EVENTOS
NIVEL	BÁSICO
DATOS CARÁCTER IDENTIFICATIVO	D.N.I./N.I.F.;TELEFONO; DIRECCION; NOMBRE Y APELLIDOS; FIRMA / HUELLA; FIRMA ELECTRONICA; CORREO ELECTRONICO; IMAGEN / VOZ;
OTROS TIPOS DE DATOS	

FICHERO	CONTABILIDAD Y HACIENDA PÚBLICA
NIVEL	MEDIO
DATOS CARÁCTER IDENTIFICATIVO	DIRECCION; TELEFONO; D.N.I/N.I.F.; NOMBRE Y APELLIDOS; FIRMA/HUELLA; FIRMA ELECTRONICA; CORREO ELECTRONICO
OTROS TIPOS DE DATOS	DATOS DE INFORMACION COMERCIAL; TRANSACCIONES DE BIENES Y SERVICIOS; CUENTAS BANCARIAS

FICHERO	**CURRICULOS FORMACIONL**
NIVEL	MEDIO
DATOS CARÁCTER IDENTIFICATIVO	NOMBRE Y APELLIDOS; DIRECCION; TELEFONO; D.N.I/NIF; FIRMA/HUELLA; Nº S.S./MUTUALIDAD; IMAGEN/VOZ; CORREO ELECTRONICO
OTROS TIPOS DE DATOS	CARACTERÍSTICAS PERSONALES; ACADEMICOS Y PROFESIONALES; DETALLES DEL EMPLEO

FICHERO	**COMUNICACIÓN Y MARKETING**
NIVEL	BÁSICO
DATOS CARÁCTER IDENTIFICATIVO	NOMBRE Y APELLIDOS; DIRECCIÓN; TELEFONO; IMAGEN/VOZ; CORREO ELECTRONICO
OTROS TIPOS DE DATOS	CARACTERÍSTICAS PERSONALES; ACADEMICOS Y PROFESIONALES

FICHERO	**USUARIAS**
NIVEL	BÁSICO
DATOS CARÁCTER IDENTIFICATIVO	NOMBRE Y APELLIDOS; DIRECCION; TELEFONO; D.N.I/N.I.F.; IMAGEN/VOZ; Nº SS/MUTUALIDAD; FIRMA/HUELLA; FIRMA ELECTRONICA; CORREO ELECTRONICO **de personas beneficiarias de los servicios de Formación**
OTROS TIPOS DE DATOS	CARACTERÍSTICAS PERSONALES; CIRCUNSTANCIAS SOCIALES; ACADEMICOS Y PROFESIONALES; DETALLES DEL EMPLEO

OTROS TIPOS DE DATOS	TARJETA DE DEMANDA; EDAD; SITUACIÓN LABORAL DE FAMILIARES; CARNE DE CONDUCIR; CUENTA BANCARIA; SEXO; NACIONALIDAD; CARGO; RESPONSABILIDAD

6.5.8.- Estructura de los Sistemas de Información

El presente título recoge los recursos, que, por servir de medio directo o indirecto para acceder o tratar datos de carácter personal de **FORMACIONL**, están protegidos para el cumplimiento de las disposiciones vigentes.

6.5.8.1.- Centros de tratamiento y locales

A través de la siguiente relación, se establecen los centros y locales de **FORMACIONL** donde se tratan o almacenan los Ficheros de Datos de Carácter Personal.

Local	Dirección	Descripción
DIRECCIÓN GENERAL TÉCNICA		Dirección General Técnica de FORMACIONL, desde la que se proporcionan servicios centrales.
Gerencias Provinciales	**FORMACIONL** dispone de una Gerencia Provincial en cada una de las provincias de la C.A. de Andalucía, así como varios centros asociados (📖 ver lista completa en el 6.5.- Anexo VI).	

6.5.8.2.- Protección frente a prestadores de Servicios de Desarrollo

Dada la complejidad de la infraestructura de los Sistemas Informáticos, **FORMACIONL** tiene contratado servicios de desarrollo de aplicaciones y soporte a los mismos, para crear, adaptar y mantener aplicaciones informáticas (software) desarrolladas a medida acorde a sus necesidades.

Como medida de protección frente a estos proveedores, FORMACIONL tendrá firmados con estos los correspondientes contratos de prestación de servicios, con las cláusulas

LOPD indicadas en el **Manual de Aplicación Práctica de los Principios Jurídicos LOPD- Anexo del Art. 12 LOPD: ACCESO A LOS DATOS POR TERCEROS.**

Los prestadores de estos servicios no tendrán acceso a los sistemas y aplicaciones de producción.

Acorde a la norma anterior, si en algún momento los desarrolladores requirieran acceso en modo persona usuaria o administrador a los equipos o servidores (especialmente a los de producción), será un administrador autorizado por **FORMACIONL** quien realizará las tareas con el asesoramiento de los desarrolladores.

En ningún caso se entregarán al prestador de servicios las contraseñas de las personas usuarias administradores de **FORMACIONL** para cualquier sistema en producción.

6.5.8.3.- Entorno de red

FORMACIONL dispone de una red de la Organización que une las distintas Gerencias Provinciales entre sí y con la Dirección General Técnica, solucionando su necesidad de transmisión de datos entre aquellas oficinas dispersas geográficamente, dotadas de Redes de Área Local (RAL) Ethernet 10 Base T, y la Dirección General Técnica con una RAL del mismo tipo, definiendo un grupo cerrado con topología mallada o en estrella.

También a través de dicha red de la Organización, el personal dispone de acceso a las siguientes redes externas:

- Internet

La red de la Organización está implementada a través de dos circuitos **Net-LAN** balanceado de **Telefónica**. Se trata de una solución tipo “redes privadas virtuales IP (RPV-IP)” que se despliegan sobre infraestructura compartida perteneciente a Telefónica.

La red de la Organización de **FORMACIONL** sólo permite el acceso por cable. No existe conectividad mediante redes inalámbricas a la red de la Organización de forma permanente..

El siguiente diagrama 6 “Esquema de Alto nivel de la red” de **FORMACIONL**.

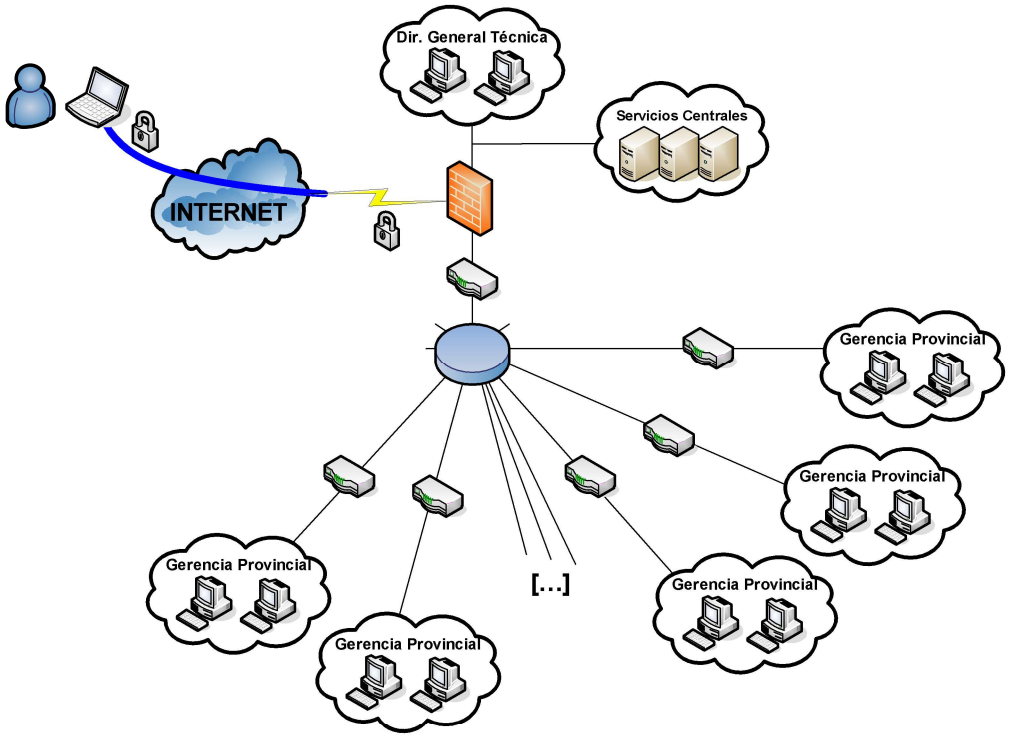

diagrama 6 "Esquema de Alto nivel de la red

6.5.8.4.- Servicios disponibles en Dirección General Técnica y en Gerencias Provinciales

A continuación se recoge la relación exhaustiva de los servicios prestados desde los servidores centrales de **FORMACIONL** que proporcionan acceso a las aplicaciones/sistemas de tratamiento de datos protegidos.

6.5.8.4.1.- Identificación de personas usuarias – Active Directory

La identificación y autenticación de las personas usuarias se realiza contra un repositorio central Active Directory que emplea el protocolo LDAP (*Lightweight Directory Access Protocol*) especifico de Microsoft.

La validación de la persona usuaria contra este sistema le da acceso al equipo informático (PC, portátil, etc.) desde el que la realiza, así como acceso a la red de la Organización. También proporciona el acceso a la Intranet basada en Web

independientemente del punto de entrada, utilizando como validación un sistema de acceso cifrado SSL a 128 bits.

No obstante, el acceso al resto de los servicios y recursos centrales (incluyendo aplicaciones remotas) y a los datos personales que contienen requiere además que la persona usuaria disponga de los correspondientes perfiles con derecho de acceso a los mismos.

6.5.8.4.2.- Servicios de acceso remoto a aplicaciones – NAVISION y SAP-RRHH

Para NAVISION el acceso remoto se realiza empleando ***Citrix Presentation y Citrix XP Metaframe***.

Para SAP R3/R3 se emplea un componente propio de SAP.

Cualquier acceso a la red de la Organización o aplicaciones corporativas requiere una autenticación en los Directorios (Active Directory).

6.5.8.4.3.- Correo electrónico – Microsoft Exchange

FORMACIONL proporciona un servicio de correo electrónico corporativo a través de *Microsoft Exchange* (Microsoft), permite el acceso a este servicio a través del cliente de correo *Outlook* (Microsoft). También es permitido el acceso a través de la Web de Exchange conocida por Microsoft como **OWA**.

La identificación y autenticación de las personas usuarias de este servicio se realiza contra un servidor ***MS Active Directory.***

6.5.8.4.4.- Servicio antivirus

FORMACIONL cuenta con un software antivirus corporativo para proteger la información que reside en sus sistemas. El software utilizado es **McAfeee Viruscan Enterprise y Karpesky.**

Dicho software está instalado tanto en los PCs de las personas usuarias, incluidos portátiles, como en los servidores de la Organización. Excepto en el servidor de correo corporativo que tiene instalado **Symantec Mail Security for Microsoft Exchange**.

Diariamente, el controlador de este antivirus actualiza la base de firmas de virus y la distribuye de forma automática a todos los equipos (PCs y servidores).

Como medida adicional, se han configurado los equipos para que las personas usuarias no puedan desactivar la protección antivirus.

6.5.8.4.5.- Servicio de Actualización Windows Update (WUS)

En aras de la seguridad, **FORMACIONL** mantiene actualizados los puestos de trabajo (PCs y portátiles) que disponen como sistema operativo Microsoft Windows.

Para cumplir esta medida y con el visto bueno del Responsable Global de Seguridad, se ha implantado un servidor dedicado "**Windows Server Updates Services**", que permite el despliegue de las actualizaciones de Microsoft de forma centralizada.

Como medida adicional, se han configurado los equipos para que las personas usuarias no puedan desactivar las actualizaciones del sistema.

6.5.8.4.6.- Servicio de disco compartido

Como parte de los servicios corporativos, **FORMACIONL** dispone de recursos de disco compartidos (almacenamiento en red) alojados en los servidores centrales de la Organización.

Estos recursos se distinguen en tres tipos:

- **Recursos de disco personal**: Cada persona usuaria dispone de un recurso de almacenamiento (carpeta) personal y cifrado, no accesible por otras personas usuarias.
- **Recursos de disco global**: Este disco es accesible por todo el personal con acceso a los servicios centrales.
- **Recursos de disco de grupo de trabajo**: En caso necesario, es posible definir recursos de disco comunes a grupos de trabajo. Sólo podrán acceder a la información de este recurso las personas usuarias que pertenezcan al grupo de trabajo.

6.5.8.4.7.- Servicio de Digitalización / Gestor Documental

Para reducir el espacio ocupado por los soportes papel, **FORMACIONL** ha iniciado un proceso de digitalización de documentos. Para apoyar este servicio **FORMACIONL** ha dispuesto un servidor para la Digitalización de Documentos y un software Gestor Documental Adobe Acrobat.

Los documentos digitalizados están protegidos por el servicio LDAP.

6.5.8.4.8.- Servicio de realización de copias de respaldo

FORMACIONL dispone de un servicio de copias de respaldo centralizado, compuesto por un robot de cintas **HP MSL 5000**, que usa el software **Veritas 10.0**.

Los **Responsables Administradores de Copias de Respaldo** han programado el sistema para la realización automática de copias de respaldo conforme a lo establecido en el apartado "**0 - 6.5.5.- Gestión de copias de respaldo y recuperación de datos personales**".

En las Gerencias disponen de dispositivos de **copias de cinta HP SLT320 con el software Windows Backup.**

FORMACIONL provee a sus trabajadores y trabajadoras de acceso a Internet. El acceso es a través de sistemas de acceso estándar (ADLS, Cable, etc). Para proteger de accesos no deseados, virus, etc, se han instalado proxys entre las distintas redes locales e Internet, basados en Linux (Debian) y Squid.

Aplicaciones para el tratamiento automatizado

La siguiente tabla lista las aplicaciones para el tratamiento automatizado establecidas y autorizadas por **FORMACIONL**

	Aplicación	Fabricante	Descripción
01	Outlook + Exchange	Microsoft	Cliente de correo y Libreta de direcciones de contacto. Servidor de correo electrónico
02	Internet Explorer	Microsoft	Navegador Web corporativo
03	MS Office	Microsoft	Software de ofimática. Word, Excel, …
04	NAVISION	Microsoft	ERP para Contabilidad y Gestión Financiera
05	SAP R/3 – RRHH	SAP AG	ERP para la gestión de los RRHH
06	SAP Portal del personal	SAP AG	Portal del personal de la Organización. Ofrece distintas funcionalidades en relación con la gestión de personal
07	Adobe Document Server	Adobe Systems Incorporated	Servidor de documentos pdf
08	INTRANET	Alkacon (software libre) Portal interno desarrollado internamente	Portal Web interno para el uso del colectivo trabajador de la Organización.
09	www.formacionL.pfc	Desarrollo propio de FORMACIONL realizado con Java, OpenCMS	Portal web de FORMACIONL

6.5.8.5.1.- Ficheros usados por cada Área/Aplicación

La siguiente tabla resume, para cada Fichero protegido, los departamentos que tratan los datos de forma automatizada y el nº de aplicación que se usa para tratar los datos del fichero:

ÁREAS FICHEROS ↴	Dirección General Técnica	Gerencias Provinciales	Centros
RECURSOS HUMANOS	SAP Portal del Personal MS-OFFICE Servidor de Documentos	SAP Portal del Personal 03 MS-OFFICE Servidor de Documentos	SAP Portal del Personal
CLIENTES Y PROVEEDORES	MS-OFFICE NAVISION Servidor de Documentos	MS-OFFICE NAVISION Servidor de Documentos	
AGENDA CORPORATIVA	OUTLOOK	OUTLOOK	OUTLOOK
EVENTOS	MS-OFFICE	MS-OFFICE	MS-OFFICE

CONTABILIDAD Y HACIENDA PUB.	MS-OFFICE NAVISION Servidor de Documentos	MS-OFFICE NAVISION Servidor de Documentos	MS-OFFICE NAVISION
CURRICULOS FORMACIONL	SAP R3 www.formacionL.pfc Servidor de Documentos	SAP R www.formacionL.pfc Servidor de Documentos	www.formacionL.pfc
COMUNICACIÓN Y MARKETING	OUTLOOK	OUTLOOK	OUTLOOK
USUARIAS	MS- OFFICE NAVISION	MS- OFFICE NAVISION	MS-OFFICE

6.5.8.5.2.- Requerimientos especiales para Aplicaciones que tratan datos de nivel medio y alto

Las aplicaciones que tratan datos de nivel medio y alto cumplen los requisitos acordes al nivel de los datos que tratan.

- Para datos de **nivel medio (SAP R3, SAP PORTAL y NAVISION)**
  - Limitan el número de intentos de acceso fallidos reiterados
  - Se requiere autorización por escrito del Responsable de Seguridad para la recuperación de copias de seguridad, indicando:
    - Persona que ejecuta el proceso
    - Datos restaurados
    - Datos re-grabados manualmente si fuera el caso
  - Se lleva un Registro de Entradas / Salidas de soportes y documentos

6.5.8.5.3.- Servidores de Ficheros automatizados

A continuación se recoge la relación exhaustiva de los servidores que albergan los ficheros con datos de carácter personal, así como las aplicaciones que tratan dichos datos:

FICHERO	Ubicación	S.O.
RECURSOS HUMANOS	Servidor de **SAP R3-RRHH** en CPD de la DGT	Windows Server 2003
CLIENTES Y PROVEEDORES	Servidor de **NAVISION** en CPD de la DGT	Windows 2000 Server
AGENDA CORPORATIVA	Servidor **Exchange**. en CPD de la DGT	Windows Server 2003
EVENTOS	Servidor **web** (Tomcat) en CPD de la DGT	Linux Debian 4.0r0
CONTABILIDAD Y HACIENDA PUB.	Servidor de **NAVISION** en CPD de la DGT	Windows 2000 Server
CURRICULOS FORMACIONL	Servidor de **SAP R3** en CPD de la DGT	Windows Server 2003
	Servidor **web** (Apache y Tomcat) en CPD de la DGT	Linux Debian 4.0r0
USUARIAS	Servidor **POSTGRESQL Externo** en CPD de la DGT	Linux Debian 4.0r0
COMUNICACIÓN Y MARKETING	Servidor de **Exchange** en CPD de la DGT	Windows Server 2003

Todos los ficheros digitalizados por el Servidor Documental se encuentran alojados en el mismo servidor. El Gestor Documental se basa en permisos de archivos y carpetas de Windows, si bien, la configuración de recursos (en carpetas de red) restringe de forma lógica el acceso de las personas usuarias a cada uno de los ficheros.

6.5.8.5.4.- Autorización y control de accesos a las aplicaciones

En las siguientes tablas se resume, para cada fichero-aplicación, el personal con capacidad para autorizar el uso de las aplicaciones para el tratamiento, y el personal encargado de realizar dicha tarea:

Fichero: RECURSOS HUMANOS		
Sistemas/aplicaciones que tratan este fichero	**Personal que puede autorizar los accesos**	**Personal autorizado a acceder**
NAVISION	Responsable de Ficheros / responsable de seguridad global	Todo El Personal De Finanzas
SAP R3-RRHH	Responsable de Ficheros / responsable de seguridad	Todo El Personal De RRHH
SAP Portal (del empleado)	Responsable de Ficheros / responsable de seguridad /	Todo el `personal de FORMACIONL

Fichero: CLIENTES Y PROVEEDORES		
Sistemas/aplicaciones que tratan este fichero	**Personal que puede autorizar los accesos**	**Personal autorizado a acceder**
NAVISION	Responsable de Ficheros / responsable de seguridad	Todo El Personal De Finanzas

	global	
SAP R3-RRHH	Responsable de Ficheros / responsable de seguridad	Todo El Personal De RRHH

Fichero: AGENDA CORPORATIVA		
Sistemas/aplicaciones que tratan este fichero	**Personal que puede autorizar los accesos**	**Personal autorizado a acceder**
OUTLOOK	Responsable de Ficheros / responsable de seguridad global/	Personal De la Dirección de Organización y Desarrollo Territorial Todo el personal de la Organización
MS_OFFICE	Responsable de Ficheros / responsable de seguridad global/	Personal De la Dirección de Organización y Desarrollo Territorial Todo el personal de la Organización

Fichero: AGENDA EVENTOS		
Sistemas/aplicaciones que tratan este fichero	**Personal que puede autorizar los accesos**	**Personal autorizado a acceder**
"MS.OFFICE	Responsable de Ficheros / responsable de seguridad global/	Personal De la Dirección de Organización y Desarrollo Territorial Todo el personal de la

		Organización

Fichero: CONTABILIDAD Y HACIENDA PÚBLICA		
Sistemas/aplicaciones que tratan este fichero	**Personal que puede autorizar los accesos**	**Personal autorizado a acceder**
MS-Office en Servidor de Ficheros compartidos de la DGT	Responsable de Seguridad Global / Responsable de ficheros	Todo el personal de FORMACIONL a sus directorios respectivos
NAVISION	Responsable de Ficheros / Responsable de seguridad /Dir. De Finanzas	Todo El Personal De Finanzas

Fichero: CURRICULOS FORMACIONL		
Sistemas/aplicaciones que tratan este fichero	**Personal que puede autorizar los accesos**	**Personal autorizado a acceder**
SAP R3-RRHH	Responsable de Ficheros / Responsable de seguridad global	Todo El Personal De RRHH / Gerencias Provinciales del área de personal

Fichero: COMUNICACIÓN Y MARKETING		
Sistemas/aplicaciones que tratan este fichero	**Personal que puede autorizar los accesos**	**Personal autorizado a acceder**
OUTLOOK Y EXCHANGE	Responsable de Ficheros / Responsable de seguridad global	Todo El Personal De la Organización

MS-OFFICE	Responsable de Ficheros / Responsable de seguridad global	Todo el personal de la Organización

Fichero: USUARIAS		
Sistemas/aplicaciones que tratan este fichero	**Personal que puede autorizar los accesos**	**Personal autorizado a acceder**
MS-OFFICE	Responsable de Gerencias Provinciales/ Responsable de seguridad/	Personal de Gerencias Provinciales asignado a los proyectos
NAVISION	Responsable de Ficheros / Responsable de seguridad/ Dir. Gestión y Evaluación Económica	Todo El Personal De Finanzas

6.5.8.6.- Almacenamiento de Ficheros-Papel (no automatizados)

Para los ficheros-papel, no automatizados, existentes en sus instalaciones, **FORMACIONL** ha dispuesto salas y armarios/archivos con llave para prevenir accesos de personas no autorizadas. Dichos armarios/archivos deben permanecer cerrados con llave, excepto el tiempo mínimo necesario para el acceso a los documentos requeridos.

Estos armarios / archivos con llave se han clasificado en dos grupos:

- **Archivos departamentales**: aquellos armarios / archivos asignados a cada departamento para la custodia de sus ficheros.

- **Archivo central**: aquellos armarios / archivos donde se almacenan los datos de ficheros protegidos que no estén en uso diario por las personas usuarias que

tratan los datos (p. ej. documentos que deban mantenerse hasta su prescripción legal, etc.).

Para estos archivos-papel, **FORMACIONL** establece:

- De cada armario / archivo, existirán sólo dos copias de la llave, que guardarán el Director del Área/Gerentes y el Responsable de Seguridad Global/Responsable de Seguridad de la Gerencia.
- El Director del Área/Departamento tiene potestad para controlar y autorizar el acceso a los armarios / archivos departamentales.
- El Responsable de Seguridad Global tiene potestad para controlar y autorizar el acceso al Archivo Central.
- El Responsable de Seguridad Global / Gerencias mantendrá una relación de los armarios / archivos habilitados por **FORMACIONL** que contengan datos protegidos, así como las personas con copia de las llaves de los mismos.

6.5.9.- Modelos y plantillas

6.5.9.1.- Registro de Incidencias - Formato

A continuación, se presenta el formato-estándar para el registro de incidencias, para cualquier nivel de seguridad (no incluye encabezados ni pie de página).

Sus datos se pueden obtener del Help-Desk corporativo de FORMACIONL:

REGISTRO DE INCIDENCIA	**Cerrada [**SI/NO**]**
Incidencia Nº: _____	(generada automáticamente por sistema HelpDesk)
Fecha notificación: _____	(fecha en que se registra la incidencia)
Ficheros afectados: _____	(indicar nivel de seguridad)

Tipo de incidencia: _____ (usar categorías pre-codificadas en apartado **0**)

DETALLE DE LA INCIDENCIA

Fecha y hora en que se produjo la incidencia:

Personas que realizan la notificación: (Especificar si son personas usuarias autorizadas o no del Fichero)

Descripción detallada de la incidencia

ANÁLISIS DE LA INCIDENCIA

Persona/s a quien se le/s notifica:

Efectos que puede producir: (En caso de no subsanación o incluso independientemente de ella)

Medidas correctoras y preventivas aplicadas: (Indicar fecha en la que se implanta)

RECUPERACIÓN DE DATOS (Rellenar este apartado sólo para ficheros de nivel alto)

Procedimientos efectuados para la recuperación de los datos:

Persona encargada de la recuperación:

_____

Datos restaurados

_____

_____

Datos grabados manualmente en el proceso de recuperación: (cuando sea aplicable)

_____

Autoriza recuperación: _____

6.5.9.2.- Inventario de Soportes Electrónicos Removibles – Formato

El Administrador de Sistemas-Soportes inventariará aquí todos los soportes electrónicos que permitan la movilidad de datos, como por ejemplo: unidades de cinta, CD's, ordenadores portátiles, etc.

INVENTARIO DE SOPORTES ELECTRÓNICOS REMOVIBLES

Nº Identificación / Nº Serie	Tipo de Soporte (Cinta LTO/ CD-ROM, …)	Lugar de almacenamiento	Tipo de Información que contiene	Fichero/s de datos personales de donde procede la información	Fecha de creación

INVENTARIO DE ORDENADORES PORTÁTILES, PDA's, etc.

Nº Identificación / Nº Serie	Persona que recibe el Portátil, PDA, … (Nombre y DNI).	Firma Receptor (recibido)	Firma Responsable de Seguridad (autorizador)	Fichero/s de datos personales autorizados	Fecha de asignación

6.5.9.3.- Registro de entrada / salida de soportes y documentos - Formato

IMPORTANTE: Este registro debe debe incluir entradas/salidas de datos vía correo electrónico

REGISTRO DE ENTRADA / SALIDA DE SOPORTES

Fecha de entrada / salida[25] del Soporte dd/mm/aaaa

SOPORTE	
Identificación	
Tipo de Soporte	
Tipo de Información	
Fichero/s de donde proceden los datos	
Fecha de creación	

ORIGEN / DESTINO Y FINALIDAD	
Organización de Origen / Destino	
Emisor / Destinatario	
Finalidad	

FORMA DE ENVÍO	
Medio de envío	

[25] Táchese lo que no proceda

Remitente	
Precauciones especiales para el transporte	<ej.: persona que hará de custodio, maletín de seguridad, … >

REGISTRO DE FIRMAS	
Responsable de la entrega (firma)	
Nombre / Cargo	
Responsable del Fichero / Responsable de Seguridad que autoriza (firma)	
Observaciones	
Fecha y Firma	

6.5.- ANEXOS

Junto a este Documento, se incluyen los siguientes anexos:

6.5.- Anexo I. *Correspondencia con el Registro General de Protección de Datos*, que incluye:

Solicitudes de Inscripción de los Ficheros-Firmadas.

Se incluirán las capturas de pantallas una vez incluidos en la página web de la AEPD.

Confirmaciones de Notificación generadas por la web de la APD cuando los ficheros fueron inscritos vía Internet.

Se incluirán las capturas de pantallas una vez grabados en la página web de la AEPD.

Resoluciones remitidas por la APD, determinando código asignado a cada fichero.

Se incluirá la tabla recibida por la AEPD con los códigos referentes a cada fichero y el documento de salida de la AEPD de cada fichero.

6.5.- Anexo II: Relación de Personas usuarias Autorizadas con acceso a los ficheros

Personas usuarias Responsables de Seguridad / Responsables de Ficheros

RESPONSABLE DE SEGURIDAD GLOBAL	
Nombre y apellidos	
	Dir. Sistemas
RESPONSABLES COORDINADORES DE SEGURIDAD DE LAS GERENCIAS.	
Nombre y apellidos	**Cargo**
	Responsable de Seguridad Gerencia de Almeria. Coordinador
	Responsable de Seguridad Gerencia de Cádiz. Coordinador
	Responsable de Seguridad Gerencia de Córdoba. Coordinador
	Responsable de Seguridad Gerencia de Granada. Coordinador
	Responsable de Seguridad Gerencia de Huelva. Coordinador
	Responsable de Seguridad Gerencia de Jaén. Coordinador
	Responsable de Seguridad Gerencia de Málaga. Coordinador
	Responsable de Seguridad Gerencia de Sevilla. Coordinador
RESPONSABLES COORDINADORES DE FICHEROS DE LA DGT.	
Nombre y apellidos	
	RESPONSABLE DE FICHEROS DE LA DIRECCIÓN DE RECURSOS HUMANOS:

	• **RECURSOS HUMANOS** • **CURRICULOS FORMACIONL**
	RESPONSABLE DE FICHEROS DE LA DIRECCIÓN DEDESARROLLO TERRITORIAL.: • **USUARIAS DE AUTOORIENTACION** • **USUARIAS**
	RESPONSABLE DE FICHEROS DE DIRECCIÓN DE ORGANIZACIÓN • **AGENDA CORPORATIVA** • **EVENTOS** • **COMUNICACIÓN Y MARKETING**
	RESPONSABLE DE FICHEROS DE DIRECCIÓN ECONÓMICA • **CONTABILIDAD Y HACIENDA PÚBLICA**
	RESPONSABLE DE FICHEROS DE LA DIRECCIÓN DE SISTEMAS • **CLIENTES Y PROVEEDORES**

Responsables Servicios Centrales de la Dirección General Ténica	
Nombre y apellidos	**Cargo**
	Responsable de Backups centrales
	Responsable de Soportes de almacenamiento centrales
	Responsable de Incidencias LOPD centrales
	Responsable de Autenticación de Personas usuarias / Derechos de Acceso centrales
	Responsable de Control de Acceso Físico (áreas centrales de almacenamiento de soportes de datos electrónicos y papel)
	Responsable de Controles Mensuales centrales (auditorías, etc.)

PERSONAS USUARIAS CON ACCESO FÍSICO A ZONAS RESTRINGIDAS		
Nombre y apellidos	**Cargo**	**Zonas a las que tiene acceso**
	Responsable de Seguridad Global	**CPD, Archivo**
	Directora de Sistemas	**CPD, Archivo**
	Personal técnico informático de la Dirección Sistemas	**CPD, Archivo**
	Personal de la Dirección de Desarrollo Territorial	**Archivo**
	Personal de la Dirección General Técnica	**Archivo**
	Personal de la Dirección de	**Archivo**

	Organización	
	Personal de la Dirección Económica	**Archivo**
	Personal de la Dirección de Recursos Humanos	**Archivo**
	Personal de la Dirección de Actividad	**Archivo**

6.5.- Anexo III: Relación de Personas usuarias autorizadas para tratamiento de datos fuera de las oficinas del Responsable del Fichero

PERSONAS USUARIAS AUTORIZADOS	
Cargos	**Ficheros tratados**
Directores Gerentes Coordinadores	**1. RECURSOS HUMANOS**
Directores Gerentes Coordinadores	**2. CLIENTES Y PROVEEDORES**
	3. AGENDA CORPORATIVA
Personal encargado de los eventos	**4. EVENTOS**
Directores Gerentes Coordinadores	**5. CONTABILIDAD Y HACIENDA PUB.**

Directores Gerentes Coordinadores Coordinadores del proyecto	**6. USUARIAS**

6.5.- Anexo IV-1:Tratamiento de datos por cuenta de terceros para FORMACIONL

Este anexo recoge la relación servicios contratados por **FormacionL** a proveedores que, para su prestación, tienen acceso o tratan datos protegidos del primero.

FICHEROS TRATADOS POR TERCEROS		Empresa encargada del tratamiento	Finalidades	Tratamiento Exclusivo	CONTRATO
Ficheros	Datos tratados				Si/No
RRHH	Todos	Gestoría	Aspectos legales	No	Si

.5.- Anexo IV-2:Tratamiento de datos por FORMACIONL para terceros

Este anexo recoge la relación, suscrita bajo contrato, para el tratamiento de datos de terceros por parte de personal de **FormacionL**.

Esta relación se formaliza al amparo del artículo 12 de la Ley Orgánica 15/1999 de 13 de diciembre.

ORGANIZACIÓN QUE RECIBE EL SERVICIO	FICHERO TRATADO	Nivel de Seguridad	Tratamiento exclusivo	CONTRATO SI/NO

6.5.- Anexo V: Responsable de Seguridad: Comunicación

<CABECERA>

.....
.

CIRCULAR INFORMATIVA

En fecha 1 de Mayo de 2017, **FORMACIONL**, como responsable jurídico de la seguridad de los ficheros con datos de carácter personal, designa un nuevo Responsable de Seguridad, en cumplimiento de la Ley Orgánica 15/1999, de Protección de Datos, y el artículo 95 del Real Decreto 1720/2007.

A efectos de comunicación a todo el personal, se elabora y envía esta circular[1]. Se incluyen los medios de contacto del nuevo responsable.

Responsable de Seguridad	
Teléfonos de contacto:	
Correo electrónico	tuteladatos@formacionL.PFC
Fax	
Intranet	www.formacionL.pfc

Con este nombramiento, el actual Responsable de Seguridad asume las funciones y obligaciones de dicho cargo y que se hallan recogidas en el Documento de Seguridad.

Almería	
Cádiz	
Córdoba	
Granada	
Huelva	
Jaén	
Málaga	
Sevilla	

A fin de facilitar la interlocución con el Responsable de Seguridad, este nombra los siguientes Representantes para las distintas provincias.

Notificación de incidencias:

Los datos de contacto con el Responsable de Seguridad o sus Responsables Provinciales recogidos en la presente circular son los únicos medios admitidos por ***FORMACIONL*** *para la notificación de incidencias de seguridad –relativas a datos de carácter personal-.*

<fecha>

<firma>

---

[1] Esta circular está incorporada en el Documento de Seguridad.

.....

.

6.5.- Anexo VI: Delegaciones de FORMACIONL

Dirección General Técnica

SEVILLA

Gerencia de Sevilla

,,,,,,,