Plan de adaptación a la Ley Orgánica de Protección de datos (L.O.P.D.) en un sistema de formación de un curso y diseño de una asignatura para su formación

José Luis Rivas
Autor

Manel Llopart
Consultor

18 de junio de 2014

A mi familia.

FICHA DEL TRABAJO FINAL

Titulo del Trabajo:	**Plan de adaptación a la Ley Orgánica de Protección de datos (L.O.P.D.) en un sistema de formación de un curso y diseño de una asignatura para su formación**
Nombre del autor:	José Luis Rivas López
Nombre del consultor:	Manel Llopart
Fecha de entrega (mm/aaaa):	06/2014
Área del Trabajo Final:	Herramienta web para la enseñanza de ingeniería distancia
Titulación:	*Ingeniería de Telecomunicaciones*

Resumen del Trabajo (máximo 250 palabras):

En este trabajo se desarrollara el "Plan de adaptación de la Ley Orgánica de Protección de Datos en un curso y una asignatura para que en un futuro se pueda estudiar", más conocida como L.O.P.D., así como su Reglamento de Medidas de Seguridad (R.D. 1720/2007, RDLOPD) en el proyecto de desarrollo del sistema telemático de un curso de un master.

Para ello, se estudiaran la directiva europea para la protección de datos de carácter personal, así como las transposiciones que se han realizado sobre ella en España. Una vez realizado dicho estudio y comprendido dicha leyes, se aplicaran para poder adaptar dicho sistema a la legislación vigente.

Después se diseñara una asignatura para que futuros alumnos puedan estudiar no sólo la parte técnica en las carreras de ingeniería sino introducirse al campo legislativo. En la actualidad se suelen trabajar con proyectos transversales, donde la parte más difícil es comunicarse con gente jurídica por este motivo se desarrolla dicho proyecto.

Finalmente, se realizaran unas conclusiones tras la realización de dicho TFG y se esbozaran las líneas para futuras actuaciones.

Abstract (in English, 250 words or less):

In this work the "PAR to protecting data in a course and to create a subject for a future that students can be studied," better known as the Data Protection Act and its Regulation on Security Measures (RD 1720 / 2007 RDLOPD) in the proposed development of a telematics system during a master degree.

To this end, we will be studied the protection of personal data European directive and the transpositions in Spain. Once this study will be finished and understand what laws are applied to adapt the system to the current legislation.

After we will create a course so that future students can study not only the technical part in engineering careers but introduced the legislative field. It is now often work with cross-cutting projects, where the hardest part is to contact legal people for this reason the project develops.

Finally, conclusions will be made after the completion of the TFG and the lines for outlining future actions

Palabras clave (entre 4 y 8):

LOPD, RD 1720/2007, Privacidad, Sistema, Adaptación, Seguridad, Base de datos, Moodle, Curso

Índice de Contenidos

CAPITULO 1

INTRODUCCIÓN

1.1 CONTEXTO Y JUSTIFICACIÓN DEL TRABAJO

1.1.1 JUSTIFICACIÓN

La sociedad actual se caracteriza no sólo por la gran cantidad de conocimiento a la que tiene acceso, sino, también por disponer de las herramientas necesarias para acceder él y procesarlo. A modo de ejemplo baste decir que poco después de 1980, cuando un ciudadano iba a la administración y pedía que calculasen su pensión tenía que esperar de 9 a 12 meses a pesar de que dicho cálculo lo efectuaban al menos 3 funcionarios. Hoy día sin embargo, gracias al avance tecnológico, sólo se tardan unos minutos en procesar toda tu vida laboral.

Ahora pensemos en la gran herramienta de trabajo y de ocio hoy día existente, la gran red de redes, Internet. Cuando la utilizamos (leyendo el correo-e, conversando en un chat, navegando o simplemente comprando) dejamos un rastro, una información a partir de la cual, con los medios tecnológicos actuales, se puede sacar un perfil de nuestra personalidad. Es decir, esta información, que en principio la dejamos diseminada, puede ser organizada para entrever nuestros gustos y determinar nuestro perfil sin previo consentimiento.

Aunque esta aplicación esta siendo revolucionaria, la idea de la que se partió para ella no es completamente nueva, pues ya hace tiempo que viene explotándose de manera más primitiva, con el bien conocido presente “gratis sólo por asistir” que para acceder a él únicamente resulta necesario dejar nuestros datos y realizar una pequeña encuesta, dando de este modo, sin ser plenamente conscientes de ello, datos de nuestra personalidad a una empresa de la que desconocemos sus intenciones y que quizás tenga por objetivo venderlos a una segunda empresa.

Un razonamiento idéntico puede aplicarse a los técnicos que a veces se preocupan más de dar un servicio que de la protección de la información a la cual puede accederse desde un terminal. De este modo, puede darse el caso de que una aplicación que diseñen e implementen funcione perfectamente pero no se proporcionen los controles de acceso que los usuarios tanto aborrecen, por lo que todos los empleados pueden disponer de información sin ningún tipo de restricción. Frecuentemente, dicha despreocupación es debida a la formación que han recibido, no preocupándose en absoluto de la importancia de la información, siendo la protección de los datos de carácter personal un derecho fundamental, equiparable al de la intimidad. Por ello es necesario plantearnos cualquier desarrollo desde la dicotomía técnica y legislativa, esto además ahorrara a la empresa costes futuros, al ser ya una realidad la política de protección de

datos personales, que hace posible que un técnico del estado pueda denunciar una de estas irregularidades, o que un usuario se ampare en el derecho de acceso, siendo éste el derecho que tiene todo ciudadano para conocer los datos que sobre su persona figuren en un fichero determinado y hayan sido sometidos a tratamiento, cuál ha sido el origen de éstos, y qué cesiones se han realizado o se prevean realizar en el futuro.

1.1.2 PUNTO DE PARTIDA

En la actualidad existe una legislación española para la protección de datos, la cual es una transposición de la directiva europea y aunque dicha legislación existe desde el 1999, no se ha publicado texto algo alguno que la explique de una manera sencilla para los técnicos ni se da formación en las carreras sobre proyectos transversales técnico-jurídicos.

1.1.3 APORTACIÓN AL TFG

Este texto aportara un Documento de Seguridad para el proyecto de desarrollo del sistema de teleformación de un master y las propuesta pertinente en el diseño de un curso para paliar dicha deficiencia a los alumnos de ingeniería

1.2 OBJETIVOS DEL TRABAJO

El objetivo de este proyecto es estudiar y desarrollar las medidas técnico – organizativas que marca la L.O.P.D. y su RMS. Para ello se estudiara el funcionamiento de un sistema y se explicara como acometer los distintos puntos que marca la ley y su Reglamento de Medidas.

Los objetivos parciales para lograrlo son los siguientes:

- Estudio de la legislación vigente en cuanto a la protección de datos
- Estudio del modo de funcionamiento de un sistema
- Identificación de los ficheros existentes así como su nivel (bajo, medio o alto)
- Realización del documento de seguridad marcado por el RMS

- Montar una asignatura donde se explique como acometer dicha problemática para futuros alumnos.

1.3 ENFOQUE Y METODO SEGUIDO

1.3.1 ENFOQUE

El enfoque que se le quiere dar a este TFC es un enfoque técnico-jurídico dada la gran deficiencia que tienen los técnicos en cuestiones jurídicas.

1.3.2 METODOLOGIA SEGUIDA

La metodología utilizada en este trabajo fin de grado se fundamenta en cuatro fases fundamentales:

1) Análisis de la situación de los ficheros. En esta fase se comprobará el nivel de cumplimiento de la normativa sobre Protección de Datos Personales.

2) Elaboración y supervisión de la documentación. Se procederá a elaborar los documentos que preceptúa el Reglamento sobre medidas de seguridad para los ficheros, según el nivel de protección exigido.

3) Evaluación de la aplicación de la normativa. Se evaluará la ejecución de las medidas de adaptación a la normativa de ejecución.

4) Creación de un curso de formación para paliar dicha necesidad.

1.4 PLANIFICACIÓN DEL TRABAJO

	Semana	Actividad	Memoria
1	26-5marzo	Definición del proyecto	
2	6-12 marzo	Entrega PEC 1	
3	13-19 marzo	Recopilación de información	Índice
4	20-26 marzo	Comparativa teórica	
5	27 marzo – 2 abril	Entrega PEC 2 Análisis del problema y de los ficheros	Pec 2
6	3-9 de abril	Análisis del problema y de los ficheros	
7	10-16-abril	Objeto del documento y ámbito aplicación	
8	17-23 abril	Funciones y obligaciones del personal, etc.	
9	24- 30 abril	Procedimientos de respaldo, controles periódicos	

		anexos	
10	1 – 7 mayo	Creación del curso	
11	8 – 14 mayo	Diseño del curso	
12	15-21 mayo	Entrega PEC 3	PEC3
13	22-28 mayo	Glosario, bibliografía, conclusiones	
14	29- 4 junio	Modificaciones solicitadas por el director TFG	
15	5 – 11 junio	Modificaciones solicitadas por el director TFG	
16	12-18 junio	Entrega TFG	TFG

1.5 BREVE SUMARIO DE PRODUCTO OBTENIDOS

El producto obtenido, es un documento de seguridad bajo el marco de la legislación española que podrá ser usado para el sistema en cuestión. Además de una asignatura donde se explique como acometerlo para futuros alumnos.

1.6 BREVE DESCRIPCIÓN DE LOS CAPTIULOS DE LA MEMORIA

A continuación se explica de una manera sencilla los capítulos de la memoria:

- En el capitulo 2 se explicara el origen de esta ley y el lector será iniciado en la misma para que pueda entender un documento de seguridad y el Reglamento de Medidas de Seguridad. También se explicara el sistema usado por el departamento (LABSEGTEL).

- En el capitulo 3 se seguirán los pasos marcados por la Ley redactando el documento de seguridad

- En el capitulo 4 se explicarán el curso de seguridad con la materia y los tiempos para poder conocer la legislación vigente en relación a privacidad

- En el capitulo 5 se diseñara el curso.

- En el capitulo 6 se explicaran las conclusiones tras haber realizado el TFG.

CAPITULO 2

ESTADO DEL ARTE

2.1 ¿QUÉ ES LA L.O.P.D.?

LOPD son las siglas abreviadas de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Esta Ley fundamentalmente tiene el objetivo de proteger a las personas físicas con respecto al tratamiento que se pueda realizar de sus datos propios por distintos sujetos, ya sean públicos o privados.

Dicha regulación pretende, fundamentalmente, establecer un control sobre quién tiene dichos datos, para qué los usa y a quién se los cede. Para ello, impone una serie de obligaciones a los responsables de dichos ficheros de datos: como son las de recabar el consentimiento de los titulares de los datos para poder tratarlos, comunicar a un Registro especial la existencia de dicha base de datos y su finalidad, así como mantener unas medidas de seguridad mínimas de la misma, en función del tipo de datos recogidos. Por otro lado, la LOPD reconoce una serie de derechos al individuo sobre sus datos como son los de información, acceso, rectificación e, incluso, de cancelación de los mismos en determinados supuestos.

Finalmente, se designa a una entidad: la Agencia de Protección de Datos, como órgano administrativo encargado de hacer cumplir la LOPD y sus reglamentos, pudiendo inspeccionar e imponer fuertes sanciones a aquellos sujetos que no cumplan con la misma.

A continuación veremos los orígenes y el fundamento de dicha regulación.

2.2 ¿POR QUÉ SURGIO?

La enorme capacidad de tratamiento y transmisión de la información que ofrecen las nuevas tecnologías hacen más acuciante la necesidad de proteger los derechos

fundamentales del individuo, en concreto: el *derecho al honor, a la intimidad personal y familiar y a la propia imagen*. Estos derechos están recogidos en las constituciones de los Estados Miembros[1], así como en el artículo 8 del Convenio Europeo para la protección de los Derechos Humanos y de las Libertades Fundamentales[2].

En lo que se refiere a la legislación nacional, el apartado 4º del artículo 18 de la Constitución Española dice que: *"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"*. Tal era la concienciación de nuestro constituyente del 78 sobre la posible incidencia perjudicial de las nuevas tecnologías sobre estos derechos.

---

[1] Artículo 18 de la Constitución Española de 1978:

> *"1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.*
>
> *(...)*
>
> *4. 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."*

[2] Artículo 8 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, adoptado en Roma el 4 de noviembre de 1950:

> *"1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia.*
>
> *2. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho sino en tanto en cuando esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás."*

Para cumplir con dicha disposición, se adoptó la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal (LORTAD)[3].

En desarrollo de la LORTAD, se han dictado diversos reglamentos: el Real Decreto 1332/1994, de 20 de junio, por el que se desarrollan determinados aspectos de la misma; el Real Decreto 428/1993, de 26 de marzo, modificado por el Real Decreto 156/1996, de 2 de febrero, que regula el Estatuto de la Agencia de Protección de Datos; y, especialmente destacado, el Real Decreto 994/1999, de 11 de junio, de Medidas de Seguridad aplicables a los ficheros con Datos de carácter personal, cuyo análisis nos ocupará la mayor parte de esta obra.

2.3 DIFERECIAS ENTRE LA L.O.P.D. Y LA L.O.R.T.A.D.

La LORTAD se adoptó teniendo en cuenta los trabajos preparatorios del Proyecto de Directiva del Parlamento Europeo y del Consejo 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[4].

Por tanto, con posterioridad a la promulgación de la LORTAD, se aprobó la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995,

[3] Ley Orgánica 5/1992, de 29 de octubre, de *Regulación del Tratamiento Automatizado de los Datos de Carácter Personal*. Boletín Oficial de Estado de 31 de octubre de 1992.

[4] Dicho proyecto desembocó en la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, 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*. Diario Oficial nº L 281, de 23 de noviembre de 1995. Pág. 31.

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[5].

Dicha Directiva debía ser transpuesta al Derecho español, en un plazo fijado, para que surtiera plenamente sus efectos. Debido a ello, y a las diferencias fundamentales detectadas entre la directiva y la LORTAD, posteriormente se aprobó la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal (LOPD) que derogó y sustituyó a la LORTAD, pero no así a sus reglamentos de desarrollo, los cuales siguen vigentes en todo lo que no se opongan a la nueva Ley.

A pesar de lo que pueda parecer en primera instancia, por el hecho de que sea una nueva ley, la LOPD es muy similar a la LORTAD. Es más, prácticamente el 85% de su redacción y de sus artículos coinciden "punto por punto" con la de su predecesora.

Entonces... ¿Cuáles son sus diferencias?. La primera y más destacada tiene que ver con su nombre: si nos fijamos, la LORTAD se llamaba "Ley Orgánica Reguladora del Tratamiento Automatizado de Datos de carácter personal" mientras que la LOPD se denomina, simplemente, "Ley Orgánica de Protección de Datos de carácter personal". Por tanto, la diferencia está en el término "automatizado": así, mientras que la LORTAD se centraba solamente en las bases de datos informatizadas, la nueva LOPD se extiende también a las bases de datos en otro tipo de soportes: papel, filminas, etc.

Las otras diferencias más significativas, son las siguientes:

- Incorporación de la figura del "Encargado del Tratamiento", diferenciándose del "Responsable del Fichero", que se define como "la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento".
- Cambio del concepto de "cesión de datos" por el de "comunicación de datos" e introducción de un artículo nuevo (art. 12) que regula específicamente el "acceso a los datos por cuenta de terceros".

[5] V. Nota nº4.

- Modificación del Tratamiento de los ficheros privados con fines de publicidad y prospección comercial y creación del llamado “Censo Promocional” (artículos 30 y 31 LOPD).
- Ampliación y modificación del régimen aplicable al “Movimiento Internacional de Datos” (artículo 33 y 34 LOPD).
- Autorización de la creación de Órganos correspondientes de la Comunidades Autónomas en materia de Protección de Datos, parcialmente homólogos de la Agencia de Protección de Datos (artículo 41 LOPD).
- Obligación de registrar y adaptar a la LOPD los ficheros de datos personales en soportes no automatizados (papel, filminas, etc.) antes del 24 de octubre del 2007 (Disposición Transitoria Primera LOPD).

2.4 DIFERENCIAS ENTRE LOS REGLAMENTOS DE SEGURIDAD 994/99 Y 1720/2007

A pesar de lo que pueda parecer en primera instancia, por el hecho de que sea un nuevo Reglamento, RD 1720/2007 es muy similar al RD 994/99. Las innovaciones más destacables son:

- La norma incluye expresamente en su ámbito de aplicación a los ficheros y tratamientos de datos no automatizados (en papel) y fija criterios específicos sobre medidas de seguridad de los mismos.

- Igualmente, regula todo un procedimiento para garantizar que cualquier persona, antes de consentir que sus datos sean recogidos y tratados, pueda tener un pleno conocimiento de la utilización que estos datos vayan a tener.

- Aunque la norma no es de aplicación a personas fallecidas, para evitar situaciones dolorosas a sus allegados se prevé que éstos puedan comunicar al responsable del fichero el fallecimiento y solicitar la cancelación de los datos.

- Para mejor garantizar el derecho de las personas a controlar la exactitud y utilización de sus datos personales, se exige de manera expresa al responsable de esos ficheros de datos que conceda al interesado un medio sencillo y gratuito para permitir a aquéllas ejercitar su derecho de acceso, rectificación, cancelación y oposición. En la misma línea, se prohíbe exigir al interesado el envío de cartas certificadas o semejantes, o la utilización de medios de telecomunicaciones que impliquen el pago de una tarifa adicional.

- Un incremento de medidas de seguridad:

    - Pasan de un nivel básico de seguridad al nivel medio los ficheros de las Entidades Gestoras y Servicios Comunes de la Seguridad Social que tengan relación con sus competencias y las mutuas de accidentes de trabajo y de enfermedades profesionales de la Seguridad Social. También pasan al nivel medio de seguridad los ficheros que contengan datos de carácter personal sobre características o personalidad de los ciudadanos que permitan deducir su comportamiento.

    - Igualmente, desde un nivel básico pasan al nivel alto los ficheros de los que son responsables los operadores de servicios de comunicaciones electrónicas disponibles al público o exploten redes públicas de comunicaciones electrónicas sobre datos de tráfico y de localización. Además, se exige a estos operadores establecer un registro de acceso a tales datos para determinar quien ha intentado acceder a esos datos, fecha y hora en que se ha intentado este acceso y si ha sido autorizado o denegado.

    - Desde el nivel básico de seguridad pasan a un nivel alto todos los datos derivados de la violencia de género.

    - Sobre éstos y los restantes datos personales incluidos en el nivel alto de seguridad se incorpora la obligación de cifrar estos datos si se encuentran almacenados en dispositivos portátiles.

- Para facilitar a los obligados a cumplir las medidas de seguridad, se exige que los productos de software destinados al tratamiento de datos personales incluyan en su descripción el nivel de seguridad, ya sea básico, medio o alto, que permiten alcanzar de acuerdo con el Reglamento.

  Por otra parte, se establecen ciertas especialidades para facilitar la implantación de medidas de seguridad, que incidirán sobre todo en el ámbito de las PYMES. Por ejemplo, bastará con aplicar las medidas de seguridad de nivel básico, en lugar de las de nivel alto, respecto a datos especialmente protegidos cuando sólo se utilicen para el pago de cuotas a las entidades de las que los titulares de los datos sean miembros. Lo mismo se permite respecto a los datos referentes exclusivamente al grado de discapacidad o la simple declaración de la condición de discapacidad o invalidez, cuando tengan por única finalidad cumplir una obligación legal. Esto es particularmente aplicable a los datos relativos a la afiliación sindical o respecto a la salud en los ficheros de nóminas.

- Medidas de seguridad específicas para ficheros y tratamientos no informatizados (papel)

- El Reglamento concede una atención especial a estos dispositivos de almacenamiento y custodia de documentos, con el fin de que se garantice la confidencialidad e integridad de los datos que contienen.

- Se exigirá la aplicación de unos criterios de archivo que garanticen la correcta conservación de los documentos y el ejercicio del derecho de oposición al tratamiento, rectificación y cancelación de los datos.

- Los armarios, archivadores y demás elementos de almacenamiento, deberán disponer de mecanismos adecuados

de cierre (llave) que impidan el acceso a la documentación por personas no autorizadas. Mientras esa documentación no esté archivada, la persona que esté a su cargo deberá custodiarla, impidiendo que acceda a ella quien no esté autorizado.

- Cuando estos ficheros contengan datos incluidos en un nivel de seguridad alto (ideología, afiliación sindical, religión, creencias, origen racial, salud, vida sexual, datos recabados por la policía sin consentimiento de los afectados o actos derivados de violencia de género), deberán estar en áreas cerradas con el dispositivo de seguridad pertinente (puertas con llave), pero, si por las características de los locales, no puede cumplirse esta medida, se permite aplicar otra alternativa que impida a las personas que no están autorizadas el acceso a esta documentación.

- Como regla general, se prohíbe pedir o tratar datos de menores de catorce años sin el consentimiento de sus padres Si son mayores de esa edad, no se exige dicho consentimiento, salvo que sean actos que los menores de dieciocho años no puedan realizar sin permiso paterno. Sí, además, se pretende recoger datos con información relativa a los miembros del grupo familiar o sus características, será necesario que los titulares de los mismos den su consentimiento.

  Además, los menores de edad deberán ser informados con un lenguaje claro, que les sea fácilmente comprensible y se tendrá que garantizar que se ha comprobado la edad del menor y la autenticidad del consentimiento prestado.

- Se introducen importantes novedades en el tratamiento Ficheros sobre solvencia patrimonial y crédito. Para la inclusión de estos datos, además de la existencia previa de una deuda cierta, vencida y exigible que haya resultado impagada, es necesario que no se haya entablado una reclamación de tipo judicial, arbitral o administrativa sobre la misma. Además, es precisa la notificación de la inclusión, impuesta por la Ley Orgánica de Protección de Datos, de forma que no se incluyan aquellas deudas respecto de las que no conste la recepción de dicha notificación.

  En cuanto que la deuda haya sido pagada, deberán ser cancelados de manera inmediata los datos relativos a ella. También se prohíbe mantener en los ficheros al respecto el denominado "saldo cero". Se establece la responsabilidad del acreedor, o persona que actúe por su cuenta, si aporta datos inexactos para su inclusión en el fichero.

- Se regula de forma detallada el deber de información al deudor. En primer lugar, deberá ser advertido de su posible inclusión en el fichero en el momento de suscribir un contrato del que pueda derivarse una deuda futura. En caso de impago, deberá informarse al deudor, tanto con carácter previo a la inclusión del dato en el fichero, como en los treinta días siguientes a la inclusión.

  La entidad que contrate con una empresa la realización de una campaña publicitaria estará obligada a asegurarse de que ésta ha recabado los datos cumpliendo con todo lo establecido en la Ley. Será obligatorio el consentimiento del afectado para que los responsables de distintos ficheros puedan cruzar sus datos para promocionar o comercializar productos o servicios.

  Se regulan las denominadas "listas de exclusión" o "listas Robinson" para que cualquier afectado, que obligatoriamente debe ser informado de su existencia, pueda comunicar al responsable de un fichero que no desea recibir publicidad. Estas listas serán de obligada consulta previa por parte de quienes realicen actividades de publicidad o prospección comercial.
- Ante la creciente externalización de estos servicios de obtención de datos, se regulan de manera detallada las relaciones entre el responsable del tratamiento y el encargado del mismo. Así, el responsable del fichero que encargue esa contratación tendrá que vigilar que el encargado al que va a contratar reúne las garantías para cumplir el régimen de protección de los datos, en especial en cuanto a su conservación y seguridad.

- Como regla general, para que el encargado del tratamiento contratado pueda a su vez subcontratar algunos de los servicios, debe estar autorizado por el responsable del fichero o tratamiento. Se exigen determinados requisitos de actuación por parte del subcontratista, a fin de que el responsable del fichero nunca pierda el conocimiento y control acerca de los tratamientos realizados, en última instancia, en su nombre y su cuenta.

- Sobre la potestad sancionadora de la Agencia Española de Protección de Datos, no se modifican las infracciones, sanciones o cuantía de las multas, pero sí se introduce un límite temporal de doce meses a la duración de la incoación de un expediente sancionador. Transcurrido ese plazo sin un procedimiento sancionador, estas actuaciones previas se entenderá como caducadas.

2.5 CUANDO SE APLICA LA L.O.P.D.

El ámbito de aplicación de la LOPD viene determinado en su artículo 2º. En su párrafo 1º, se establece la regla general para, a continuación, determinar una serie de excepciones en los párrafos siguientes. Este sistema de excepciones va a ser la tónica

general de la Ley, contribuyendo al oscurecimiento de su articulado y a la limitación de su alcance.

Regla general:

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

En este punto es necesario saber lo que la Ley entiende por "datos de carácter personal":

El artículo 3 de la LOPD define a los mismos como *"cualquier información concerniente a personas físicas identificadas o identificables".*

Es de destacar que solo se refiere a las personas *físicas*, dejando de lado a las *jurídicas* cuyos datos no se ven protegidos por esta Ley. Asimismo dichas personas no necesitan estar identificadas plenamente, sino que basta con que se pueda deducir su identidad con relativa facilidad.

Ejemplos de estos datos son: nombre, apellidos, dirección, edad, estado civil, profesión, sexo, edad, etc.

Excepciones:

El párrafo 2º del artículo 2 excluye la aplicación de la LOPD para los siguientes ficheros:

- A los ficheros mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas.
- A los ficheros sometidos a la normativa sobre protección de materias clasificadas.
- A los ficheros establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada. No obstante, en estos supuestos el responsable del fichero comunicará previamente la

existencia del mismo, sus características generales y su finalidad a la Agencia de Protección de Datos.

2.6 REGLAMENTO DE MEDIDAS DE SEGURIDAD

Tal y como adelantamos en el epígrafe 1.2, entre las normas reglamentarias que se aprobaron en desarrollo de la antigua LORTAD, destaca especialmente el Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de las Medidas de Seguridad que deben cumplir los ficheros con datos de carácter personal.

Como vimos también anteriormente, la aprobación de la nueva LOPD no derogó dicho reglamento, a pesar de referirse a la antigua LORTAD, sino que lo mantuvo en vigor en todo lo que no se oponga a la nueva Ley.

El objeto de este reglamento es desarrollar el (antiguo y nuevo) artículo 9 de la LORTAD/LOPD. El párrafo primero del mismo dice lo siguiente:

> *"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 incumplimiento de esta obligación, es decir *"Mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad"*, supone una falta grave sancionable con una multa de entre 10 y 50 millones de pesetas, en base a los artículos 44.3 y 45.2 de la LOPD.

2.7 NIVELES DE PROTECCIÓN

Dentro del Reglamento de Medidas de Seguridad, existen tres niveles de seguridad distintos: el básico, el medio y el alto. Para saber qué nivel debemos de aplicar, debemos de referirnos al tipo de datos personales almacenados en el fichero. Para ello, estaremos a lo dispuesto en el artículo 81 del Reglamento, de él se deduce lo siguiente:

1- Nivel básico:

- Aplicable a todos los sistemas con datos personales en general.

2- Nivel Medio:

- Datos de comisión de infracciones administrativas o penales,
- Datos de Hacienda Pública,
- Datos de servicios financieros,
- Datos sobre solvencia patrimonial y crédito y
- Conjunto de datos de carácter personal suficientes que permitan obtener una evaluación de la personalidad del individuo.

3- Nivel Alto: para datos referidos a la

- Ideología,
- Religión,
- Creencias,
- Origen racial,
- Salud o vida sexual y
- Datos recabados para fines policiales.
- Violencia de genero

Estas medidas de seguridad se aplican de forma acumulativa, así el nivel alto deberá cumplir también las reguladas para el nivel medio y el nivel bajo de seguridad. Véase el esquema siguiente.

2.8 CERTIFICACIONES

En la actualidad existe un único sello de calidad sobre privacidad, seguridad y protección de datos el cuál está auspiciado por la Unión Europea llamado Europrise (www.european-privacy-seal.eu) . En dicho sello se diferencia los expertos en dos: juristas y técnicos. Para la obtención de ser experto por la Unión Europea en privacidad, seguridad y protección de datos por dicho sello hay que pasar un curso y una evaluación.

EuroPriSe European Privacy Seal

Para los expertos técnicos deberán acreditar los conocimientos técnicos para aplicar la normativa existente además de conocerla a nivel legal.

2.9 ANÁLISIS DE LOS TRABAJOS ACTUALES EN LOPD

Desde la entrada en vigor de dicha normativa se ha escrito diferentes manuales debido al poco entendimiento de dicha norma por parte de los juristas y de los técnicos en dicha materia. Hay que tener en cuenta que es una ley que hay que tener conocimientos jurídicos y técnicos para poder aplicarla correctamente. A continuación se ponen algunos ejemplos de los documentos usados:

- La antigua Agencia de Protección de Datos de la Comunidad de Madrid la cual desapareció hace un par de años publico las primeras guías oficiales desde un punto jurídico. Hasta la creación de dicha Agencia y siendo su Director Antonio Troncoso empezó a aparecer la luz en este mundo tan oscurantista.

- Aplicación de la LOPD en las empresas. Libro escrito José Luis G. Rambla y editado por Informática 64 siendo su ISBN. 978-84.613-3574-9. En el explica de una manera sencilla como adaptar un sistema telemático a los escenarios de la LOPD.

- RedIRIS desde su revista y sus foros técnicos y de seguridad se ha preocupado de dicha problemática dando cabida a diversos expertos en la materia para explicar y dar sus experiencias. Esto ha sido debido a que la comunidad universitaria desde la creación de dicha legislación ha estado preocupada por dicha problemática es decir, adaptar sus sistemas de información a la normativa de protección de datos.

2.10 HERRAMIENTAS USADAS EN LA GESTIÓN DEL CURSO A ANALIZAR

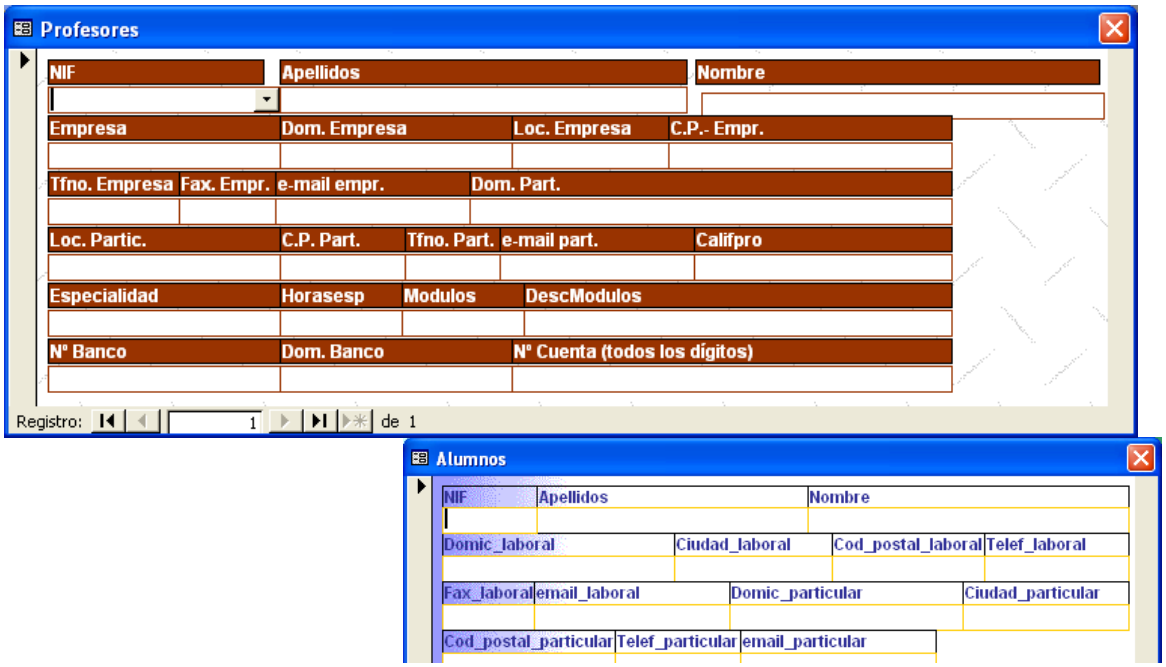
MOODLE

Moodle es una aplicación web para la formación, de distribución libre que ayuda a los profesores a crear comunidades de aprendizaje en la Red.

GESTIÓN DE ESTUDIANTES Y PROFESORES

Para la gestión de curso muchos departamentos usan herramientas propias basadas en Microsoft Office más concretamente en Excel o en Access. A continuación se

muestra un ejemplo la base de datos de un curso propio para gestionar los profesores y los alumnos.



2.11 HERRAMIENTAS PARA LA FORMACIÓN

Como se pueden ver existen numerosos herramientas que se describen a continuación:

MOODLE

Moodle es una aplicación web para la formación, de distribución libre que ayuda a los profesores a crear comunidades de aprendizaje en la Red. Dicha plataforma fue creada por Martin Dougiamas, quien fue administrador en la Universidad Tecnológica de Curtin. La primera versión de dicho aplicativo aparece a mediados del 2002. Actualmente se emplea en más de 46.000 sitios muchos de ellos universidades.

En la administración de cursos es el profesor quien tiene el control total sobre todas las opciones del curso. Se puede elegir en varios formatos de curso tales como. semanal, por temas o en formato social basado en debates.

Alguno de los módulos con los que se cuenta son:

- De tareas: puede especificarse la fecha final de entrega de una tarea y la calificación máxima que se le podrá asignar, los estudiantes pueden subir sus tareas (en cualquier formato de archivo) al servidor.

- De consulta: puede usarse para votar algo, para pedir consentimiento, etc.
- De foro: para la creación de un foro de debates.
- De recurso: Admite la presentación de un importante numero de formatos (pdf, Word, Excel, etc.)
- Soporta formato SCORM

CLAROLINE

Claroline es una plataforma de aprendizaje de teleformación y un groupware de código abierto, por tanto permite a cientos de instituciones de todo el mundo crear y administrar cursos y espacios de colaboración en línea.

Algunas de las herramientas con la que cuenta son las siguientes:

- Escribir una descripción del curso
- Publicar documentos en cualquier formato
- Administrar foros
- Desarrollar itinerarios de aprendizaje
- Poner una agenda con tareas y fechas limite
- Publicar anuncios
- Crear una wiki

BLACKBOARD ACADEMIC SUITE

Blackboard desarrollo aplicaciones de programas empresariales y de teleformación. Es un software que no es de distribución libre.

Blackboard academic suite incluye:

- Un entorno de manejo de cursos
- Un sistema para manejo de contenido

2.12 HERRAMIENTAS ELEGIDA

Como se pueden ver existen numerosos herramientas que se describen en el punto anterior. Pero elegimos Moodle por que:

- Es de la mas usables según el ranking realizado por:

  Ruiz N, Vera P, García R, Viciana R, Cañedas, F, Reche P. “Comparing open-source e-Learning platforms from adaptivity point of view.” 2009, EAEEIE Annual Conference, 22-24 Jun 2009,IEEE, ISBN: 978-1-4244-5386-3

- Es software libre

- Tiene una amplia comunidad (https://moodle.org/)

- Permite distintos tipos de aprendizaje

- Es muy intuitivo

- Esta por delante en términos de adaptabilidad según plataformas de enseñanza virtual libres y sus características de extensión: Desarrollo de un bloque para la gestión de tutorías en Moodle" por Diego Macías Álvarez 2010

CAPITULO 3

DOCUMENTO DE SEGURIDAD

3.1 OBJETO DEL DOCUMENTO

El presente documento responde a la obligación establecida en el artículo 8 del Real Decreto 1720/2007 de 19 de diciembre en el que se regulan las medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal.

3.2 AMBITO DE APLICACIÓN

El presente Documentos de Seguridad se aplica en los siguientes ámbitos del LABSEGTEL:

- Ámbito Jurídico – Técnico: el Documento de Seguridad se elabora bajo la responsabilidad de la UOC la cual implantará las medidas jurídicos – técnicas bajo unas normas y procedimientos.

- Ámbito Personal: dicho Documento de Seguridad afecta a todas las personas que tengan acceso a los datos del Fichero, bien a través del sistema informático habilitado para al mismo, o bien a través de cualquier otro medio automatizado del acceso al Fichero, se encuentran obligadas por ley a cumplir lo establecido en este documento, y sujetas a las consecuencias que pudieran incurrir en caso de incumplimiento.

Una copia de este documento con la parte que le afecte será entregada, para su conocimiento, a cada persona autorizada a acceder a los datos del Fichero, siendo requisito obligatorio para poder acceder a esos datos el haber firmado la recepción del mismo.

3.3 RECURSOS PROTEGIDOS

Los recursos protegidos, de LABSEGTEL, a los efectos de este documento de seguridad son los siguientes aunque en los Anexos punto 3.11 se describen más detalladamente.:

- Locales de tratamiento y almacenamiento de datos: aquellas ubicaciones donde están ubicados los servidor, equipos telemáticos,, etc. que contienen datos de carácter personal.

- Servidores: Dispositivo que resuelve las peticiones de otros elementos del sistema conocidos como clientes. En este caso son dispositivos que contienen los datos de carácter personal.

- Equipos informáticos: Son aquellos dispositivos informáticos con los cuales podemos acceder a los datos de carácter personal: equipos de sobremesa, portátiles, PDA.

- Sistemas operativos y aplicaciones informáticas: Son aquellos programas y/o aplicaciones con los que se puede acceder a los datos de carácter personal.

- Soportes de almacenamiento: son aquellos elementos empleados para contener en su interior copias de los datos de carácter personal.

- Red de comunicación interna y externa: Los medios y canales de comunicación por el que circulan los datos de carácter personal garantizando la disponibilidad y confidencialidad de los mismos.

- Ficheros automatizados: Son aquellos ficheros son aquellos son conjuntos de datos de carácter personal y están organizados y cuyo soporte físico es de tipo informático.

- Ficheros no automatizados: Son aquellos ficheros cuyo soporte físico no es informático es decir, cualquier fichero cuyo utiliza un soporte convencional.

3.4 FUNCIONES Y OBLIGACIONES DEL PERSONAL

3.4.1 RESPONSABLE DEL FICHERO

El responsable del fichero es la persona física o jurídica que decide sobre la finalidad, contenido y uso del tratamiento de los datos de carácter personal. Entre sus funciones se encuentran:

- Velar por el cumplimiento de las disposiciones legales en materia de protección de datos de carácter personal y supervisar el acatamiento de las previsiones contenidas en el presente documento.

Sus obligaciones son las siguientes:

- Adoptar las medidas técnicas y organizativas que garanticen la seguridad de los y que eviten su alteración, pérdida, tratamiento o acceso no autorizados, mediante la implantación de Normas y Procedimientos de Seguridad.

- Elaborar e implantar la Normativa de Seguridad, creando un documento de obligado cumplimiento para el personal con acceso a los datos y a los Sistemas de Información: el Documento de Seguridad.

- Mantener actualizado el Documento de Seguridad en todo momento y revisarlo cuando se produzcan cambios relevantes en los Sistemas de Información.

- Notificar a la Agencia Española de Protección de Datos los Ficheros de Datos Personales que se creen, así como sus modificaciones relevantes o su eliminación.
- Designar uno o más Responsables de Seguridad.

- Establecer, de forma personalizada a cada Usuario del Sistema de Información, las Funciones y Obligaciones en relación con la confidencialidad y protección de los datos que ha de procesar, manipular o custodiar, en función de su puesto de trabajo.

- Establecer los mecanismos oportunos para que los Sistemas de Información tengan un acceso restringido.

- Autorizar expresamente, en los casos en los que sea necesario, la salida de soportes que contengan datos de carácter personal fuera de las instalaciones.

- Verificar la definición y correcta aplicación de los Procedimientos de Copias de Respaldo y de Recuperación de los datos de carácter personal.

3.4.2 RESPONSABLE DE SEGURIDAD

El responsable de seguridad es la persona o personas a las que el responsable del fichero ha asignado formalmente. Entre sus funciones se encuentran:

- coordinar y contralar las medidas de seguridad aplicables

Sus obligaciones son las siguientes:

- Coordinar y Controlar la Implantación y Puesta en Marcha de las Medidas de Seguridad establecidas en el presente Documento de Seguridad.

- Verificar que los accesos a los Sistemas de Información a través de redes de comunicaciones garantizan un nivel de seguridad equivalente al correspondiente a los accesos en modo local.

- Verificar que se aplican las medidas de seguridad oportunas sobre los ficheros temporales que contengan datos de carácter personal.

- Habilitar y gestionar el Registro de Incidencias a disposición de todos los Usuarios.

- Habilitar y gestionar el Registro de Soportes para identificar, registrar y almacenar todos los soportes.

- Realizar las copias de seguridad y comprobarlas trimestralmente.

3.4.3 USUARIOS

Los usuarios son aquellas personas que en el ejercicio de su actividad profesional están autorizadas para utilizar el sistema informático en el que se ubican los ficheros de datos de carácter personal. Sus obligaciones son:

- Firmar el conocimiento y el compromiso de cumplimiento de las normas y procedimientos establecidos en la política de seguridad.

- Utilizar los datos de carácter personal a los que tengan acceso en virtud de sus funciones.

- Guardar secreto y la confidencialidad.

- A almacenar los datos de carácter personal sobre los que realicen tratamiento de una manera centralizada.

- No realizar copias en soportes sin autorización por escrito del responsable del fichero o de seguridad.

3.5 NORMAS Y PROCEDIMIENTOS DE SEGURIDAD

3.5.1 SISTEMAS DE INFORMACIÓN

- Estará disponible en la dirección del proyecto LABSEGTEL un registro de usuarios autorizados para utilizar los ficheros existentes en los sistemas de información (ficheros automatizados y no automatizados).

- Los usuarios autorizados dispondrán de un nombre de entrada asociado a una contraseña, dicho nombre de entrada y contraseña es único por usuario serán por tanto personales e intransferibles.

- Se prohíbe la instalación en cualquier equipo propiedad del proyecto LABSEGTEL de cualquier aplicación en los sistemas de información sin la autorización expresa del responsable de seguridad o del fichero.

- Se prohíbe el uso de los sistemas de información con fines privados o con cualquier otro fin diferente a los estrictamente laborales, sin la correspondiente autorización del Responsable del Fichero.

- Se prohíbe utilizar cualquier información que hubiese podido ser obtenida por la condición de empleado del proyecto LABSEGTEL con

cualquier otro fin que no sea el estrictamente necesario para el desempeño de las funciones que desempeñe en dicho proyecto.

- Se prohíbe la conexión a redes externas desde equipos que contengan o tengan acceso a los datos de carácter personal, sin la autorización previa del Responsable del Fichero.

3.5.2 LOS LOCALES

- Estará disponible en la dirección del proyecto LABSEGTEL un Registro de Locales existentes acompañado de una Lista de Personas Autorizadas para acceder a los mismos.

- Los locales donde se ubiquen los equipos que almacenen los datos de carácter personal deberán estar cerrados con llave en ausencia de personal autorizado. Dichos locales principalmente son: administración, dirección del proyecto, conserjería ya que son donde están ubicados los equipos con acceso a los ficheros donde se encuentran datos de carácter personal.

- En el caso de locales para atención al público, se limitará la presencia del mismo a las áreas habilitadas para tal efecto. Además, en estos locales nunca se dejará un equipo informático operativo sin la presencia de un Usuario autorizado o si fuera el caso se bloquearía la pantalla. Dicho locales son: conserjería y administración del proyecto LABSEGTEL

- Se establecerán las normas oportunas para permitir el acceso a los locales de otras empresas de servicios subcontratadas. Dichas empresas deberán formalizar cláusulas que garanticen las actuaciones de su personal.

3.6 GESTION DE INCIDENCIAS

Una incidencia es cualquier evento que pueda producirse esporádicamente y que pueda suponer un peligro para la seguridad del Fichero, entendida bajo sus tres vertientes de confidencialidad, integridad y disponibilidad de los datos.

El mantener un registro de las incidencias que comprometan la seguridad de un Fichero es una herramienta imprescindible para la prevención de posibles ataques a esa seguridad, así como para persecución de los responsables de los mismos.

El responsable de Fichero llevará un registro de estas, en el que habrán de constar todas las que se produzcan. A continuación se muestran los pasos a seguir una vez detectada una incidencia:

- Aquella persona la cual detecte la incidencia deberá notificarla inmediatamente al responsable de Fichero, informando de la incidencia

concreta producida, el momento y circunstancias en que se produjo y a qué afecta.

- El responsable de Fichero procederá a hacer constar la incidencia en el registro. Una vez hecho esto deberá adoptar las medidas para subsanar dicha incidencia.

- Tanto la incidencia, como sus efectos y las medidas adoptadas para su resolución se notificaran.

3.7 GESTION DE SOPORTES

Soportes informáticos son todos aquellos medios de grabación y recuperación de datos que se utilizan para realizar copias o pasos intermedios en los procesos de la aplicación que gestiona el Fichero.

Dado que la mayor parte de los soportes que hoy en día se utilizan, como disquetes o CD-ROMs, son fácilmente transportables, reproducibles y/o copiables, es evidente la importancia que para la seguridad de los datos del Fichero tiene el control de estos medios.

- Los soportes que contengan datos del Fichero, bien como consecuencia de operaciones intermedias propias de la aplicación que los trata, o bien como consecuencia de procesos periódicos de respaldo o cualquier otra operación esporádica, deberán estar claramente identificados con una etiqueta externa que indique de qué fichero se trata, que tipo de datos contiene, proceso que los ha originado y fecha de creación.

- Aquellos medios que sean reutilizables, y que hayan contenido copias de datos del Fichero, deberán ser borrados físicamente antes de su reutilización, de forma que los datos que contenían no sean recuperables.

- Los soportes que contengan datos del Fichero deberán ser almacenados en lugares a lo que no tengan acceso personas no autorizadas para el uso del Fichero.

- La salida de soportes informáticos que contengan datos del Fichero fuera de los locales donde está ubicado el Fichero deberá ser expresamente autorizada por el responsable del Fichero.

- El responsable del Fichero mantendrá un Libro de registro de entradas y salidas donde se guardarán los formularios de entradas y de salidas de soportes, con indicación de tipo de soporte, fecha y hora, emisor, número de soportes, tipo de información que contienen, forma de envío,

destinario, o persona responsable de la recepción que deberán estar debidamente autorizadas.

- Cuando los soportes vayan a salir fuera de los locales en que se encuentren ubicados los ficheros como consecuencia de operaciones de mantenimiento, se adoptarán las medidas necesarias para impedir cualquier recuperación indebida de la información almacenada en ellos.

3.8 ENTRADA Y SALIDA DE DATOS POR RED

La transmisión de datos por red, ya sea por medio de correo electrónico o mediante sistemas de transferencia de ficheros, se está convirtiendo en uno de los medios más utilizados para el envío de datos, hasta el punto de que está sustituyendo a los soportes físicos. Por ello merecen un tratamiento especial ya que, por sus características, pueden ser más vulnerables que los soportes físicos tradicionales.

- Todas las entradas y salidas de datos del Fichero que se efectúen mediante correo electrónico se realizarán desde una única cuenta o dirección de correo controlada por un usuario especialmente autorizado por el responsable del Fichero. Igualmente si se realiza la entrada o salida de datos mediante sistemas de transferencia de ficheros por red, únicamente un usuario o administrador estará autorizado para realizar esas operaciones.

- Se guardarán copias de todos los correos electrónicos que involucren entradas o salidas de datos del Fichero, en directorios protegidos y bajo el control del responsable citado. Se mantendrán copias de esos correos durante al menos dos años. También se guardará durante un mínimo de dos años, en directorios protegidos, una copia de los ficheros recibidos o transmitidos por sistemas de transferencia de ficheros por red, junto con un registro de la fecha y hora en que se realizó la operación y el destino del fichero enviado.

- Cuando los datos del Fichero vayan a ser enviados por correo electrónico o por sistemas de transferencia de ficheros, a través de redes públicas o no protegidas, se recomienda que sean encriptados de forma que solo puedan ser leídos e interpretados por el destinatario.

3.9 PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN

La seguridad de los datos personales del Fichero no sólo supone la confidencialidad de los mismos sino que también conlleva la integridad y la disponibilidad de esos datos.

Para garantizar estos dos aspectos fundamentales de la seguridad es necesario que existan unos procesos de respaldo y de recuperación que, en caso de fallo del sistema informático, permitan recuperar y en su caso reconstruir los datos del Fichero.

La realización de la copia de seguridad se realizarán a las dos de la madrugada en una cinta DAT.

DIARIA

La Copia de Seguridad Completa Diaria se efectuará en cinta, de forma programada, con los ficheros al completo, de lunes a viernes. Se utilizará el sistema de rotación de dos semanas para el que se precisan 10 cintas que se identificarán con las series 1 y 2 y los números 1 al 5.

El Operador deberá escribir sus iniciales sobre el formulario de Registro de Copias de Seguridad al finalizar la comprobación de que la copia se ha efectuado

SEMANAL

La Copia de Seguridad Completa Semanal se efectuará en cinta, de forma programada, con los ficheros al completo, todos los viernes y se almacenará en la caja fuerte. Se utilizará el sistema de rotación mensual para el que se precisan 4 cintas que se identificarán con la serie 3 y los números 1 al 4. En los meses que cuentan con 5 semanas se guardará directamente la cinta del plan de copia mensual.

El Operador deberá escribir sus iniciales sobre el formulario de Registro de Copias de Seguridad al finalizar la comprobación de que la copia se ha efectuado.

MENSUAL

La Copia de Seguridad Completa Mensual se efectuará en cinta, de forma programada, con los ficheros al completo, el último día de cada mes y se almacenará en la caja fuerte. Se utilizará el sistema de rotación anual para el que se precisan 12 cintas que se identificarán con la serie 4 y los números 1 al 12.

El Operador deberá escribir sus iniciales sobre el formulario de Registro de Copias de Seguridad al finalizar la comprobación de que la copia se ha efectuado

PRUEBA DE RECUPERACIÓN ALEATORIA MENSUAL

La Prueba de Recuperación Aleatoria Mensual deberá realizarse al finalizar la copia de seguridad mensual. Se deberán recuperar 10 ficheros de forma aleatoria de todos los servidores de los que se estén realizando copias de seguridad, incluyendo los servidores de base de datos. Los ficheros deberán ser recuperados en un entorno de pruebas, sin sobrescribir los ficheros válidos depositados en el disco de producción

Para comprobar la integridad de las cintas, se recuperarán archivos de la cinta mensual, de una de las cintas semanales y de una de las cintas diarias

El Operador deberá escribir sus iniciales sobre el formulario de Registro de Copias de Seguridad al finalizar la comprobación de que la restauración se ha efectuado correctamente.

RECUPERACIÓN ANTE DESASTRES

Este Plan de Seguridad deberá efectuarse cada vez que se instale un nuevo servidor o se reinstale el sistema operativo. Se efectuará una copia completa del sistema, con el fin de recuperar una máquina rápidamente en caso de avería grave de disco

Cada servidor deberá disponer de una cinta individual conteniendo la información necesaria para su restauración rápida

Debido a la problemática actual de actualizaciones permanentes de los sistemas operativos (Service Packs) se actualizarán las cintas de este plan de forma mensual

El Operador deberá escribir sus iniciales sobre el formulario de Registro de Copias de Seguridad al finalizar la comprobación de que la restauración se ha efectuado correctamente

3.10 CONTROLES PERIÓDICOS DE VERIFICACIÓN DEL CUMPLIMIENTO

El documento debe mantenerse en todo momento actualizado y debe ser revisado siempre que se produzcan cambios relevantes en el sistema de información o en la organización del mismo.

El Responsable de los Ficheros como el Responsable de Seguridad revisarán este documento de seguridad de manera periódica con el fin de que el contenido del documento deberá adecuarse, en todo momento, a las disposiciones vigentes en materia de seguridad de los datos de carácter personal.

CAPITULO 4

PROPUESTA PLAN DE FORMACIÓN

4.1 INTRODUCCIÓN

Una vez analizada la plataforma de teleformación, los equipos donde se van a trabajar tanto administración como los usuarios que realizan el contenido del curso se ha realizado lo que marca la Ley Orgánica de Protección de Datos:

- Cumplir las medidas técnicas y organizativas del RD 1720/2007 de los ficheros de nivel básico (copias de seguridad, sistemas de autenticación, control de acceso, etc.)
- Inscribir los ficheros en el RGPD
- Redactar el documento de seguridad con las medidas técnicas y organizativas adoptadas para cumplir con la legislación

Finalizada esa parte, en esté capitulo plantearemos un posible curso online para que se pueda aprender lo realizado de una manera más sencilla por parte de otros alumnos.

Dicha formación tendría una duración de unas 90 horas de duración

4.2 TEMAS PROPUESTOS

TEMAS	HORAS LECTIVAS	HORAS DE TRABAJO DEL ALUMNO
Fundamentos a la privacidad (España, Europa, etc.)	3	1
La Agencia Española de Protección de Datos y su Registro	4	3
Medidas técnicas y organizativas	20	10
Documento de Seguridad	20	20
Derechos de los usuarios	2	2
Sanciones e Infracciones	5	5
Practicum de asignatura	0	15

4.3 DESARROLLO LECTIVO

Las clases serán por teleformación:

- Contenido de desarrollo teórico junto con el material de apoyo y la bibliografía de la materia
- Planificación de conferencias impartidas por expertos en la materia mediante videos en streaming
- Evolución basada en examen tipo test a la conclusión de cada tema.

Por el contrario cada alumno deberá en cada tema el desarrollo de trabajos orientados por el tutor y dichos trabajos son orientados a la puesta en práctica de los contenidos teóricos y a que el alumno tenga que pensar con lógica técnico-jurídica.

Al finalizar la asignatura tendrá que realizar un trabajo elaborando un plan de adaptación de casos prácticos desde el principio hasta el desarrollo del documento de seguridad.

4.4 DESCRIPCIÓN DE TEMAS

Tema	1	Titulo	Fundamentos a la privacidad
Objetivos			
• Comprender la evolución histórica de la privacidad desde la I guerra mundial hasta nuestro tiempo • Comprender los conceptos básicos asociados a la seguridad de la información: confidencialidad, disponibilidad e integridad • Introducción del concepto de activo de información • Fundamentos y principios básicos de la privacidad • La privacidad: Europa vs Estados Unidos			
Trabajo del alumno			
• Trabajo de investigación sobre al menos una URL donde se pueda comprar información penal en Europa y en Estados Unidos. Explicar los resultados			
Carga lectiva			

Presencial	3	Trabajo del alumno	1

Tema	2	Titulo	La Agencia Española de Protección de Datos y su Registro General

Objetivos

- Introducción del la Agencia Española de Protección de Datos
- Introducción del Registro General
- Fichero de titularidad Publica y Privada
- Procesos para dar de alta un fichero

Trabajo del alumno

- Dar de alta un fichero de titularidad publica con todos sus pasos y un fichero de titularidad privada.

Carga lectiva

Presencial	4	Trabajo del alumno	3

Tema	3	Titulo	Medidas técnicas y organizativas

Objetivos

- Introducción a los diferentes niveles de seguridad
- Ficheros automatizados y no automatizados
- Descripción de las diferentes medidas para los tres niveles y los tipos de ficheros según marca el RD 1720/2007

Trabajo del alumno
• Montar un sistema y demostrar que cumple con las medidas técnicas y organizativas • Auditar un sistema en sus medidas técnicas • Buscar ejemplo de ficheros y explicar que tipo de nivel tiene por ejemplo (clientes videoclub, veterinario, nominas)

Carga lectiva			
Presencial	20	Trabajo del alumno	10

Tema	4	Titulo	Documento de Seguridad

Objetivos

- Introducción a los diferentes documentos de seguridad
- Redacción de los documentos de seguridad

Trabajo del alumno
• Redactar un documento de seguridad de fichero: nivel bajo/medio/alto

Carga lectiva			
Presencial	20	Trabajo del alumno	20

Tema	5	Titulo	Derechos de los usuarios

Objetivos

- Introducción de los derechos de los usuarios
- Derecho de información
- Derecho de Acceso, Rectificación, Cancelación y Oposición (ARCO)
- Derecho de tutela

Trabajo del alumno

- Protocolizar los derechos ARCO
- Redactar y protocolizar el derecho de información

Carga lectiva

Presencial	2	Trabajo del alumno	2

Tema	6	Titulo	Sanciones e Infracciones

Objetivos

- Introducción a las Sanciones
- Introducción a las infracciones
- Protocolos a seguir antes las sanciones e infracciones

Trabajo del alumno

- Buscar en Internet diferentes tipos de sanciones e infracciones: leves, graves y muy graves y explicar su motivación y si están de acuerdo con ellas.

Carga lectiva			
Presencial	5	Trabajo del alumno	5

Tema	7	Titulo	Practicum de la asignatura
Objetivos			
• Asimilar todos los conceptos introducidos: técnicos y jurídicos			
Trabajo del alumno			
• Hacer un plan de adaptación al reglamento de una empresa o de un proyecto			
Carga lectiva			
Presencial	0	Trabajo del alumno	15

4.5 CICLO DE CONFERENCIAS

Como detallábamos al inicio de este capitulo, uno de los posibles ciclos de videoconferencias sobre seguridad seria:

- La privacidad en internet
- El derecho fundamenta de la protección de datos en cloud computing
- Sistemas de gestión de la seguridad de la información
- Visión pragmática de la protección de datos
- Experiencia práctica sobre el desarrollo de un plan de adaptación al reglamento.

4.6 HERRAMIENTAS

Una vez realizado el análisis de cómo realizar la formación para que los alumnos de ingeniería, no sólo tengan el conocimiento técnico que se le da en sus estudios si no también conocimientos jurídicos ya que a lo largo de su trayectoria profesional cada proyecto que realicen va estar involucrado por legislación en está materia. No hay que olvidarse que dentro de la Unión Europea España es un estado de los más modernos en relación a legislación tecnológica.

El problema que nos encontramos que a la hora de conversar con los especialistas juristas no nos han trasmitido en nuestros estudios la jerga legal por lo que la mayoría de las veces se están hablando dos idiomas diferentes donde no se comunican dos profesionales a pesar de hablar el mismo idioma: español, inglés, francés, catalán, gallego, etc.

Por otro punto, no ocurre lo mismo cuando hablamos con compañeros de otras ingenierías porque los conceptos son parecidos y el lenguaje es parecido. Por tanto, para el desarrollo del curso se ha usado la herramienta antes auditada Moodle.

En Moodle le hemos tenido que analizar a fondo para ver si cumplía la legislación vigente realizando una auditoria para después poder realizar el documento de seguridad. Por tanto, una vez hecho el estudio previo, el documento de seguridad pasamos a realizar y a volcar la formación a la herramienta antes mencionada.

4.7 ESTRUCTURA DEL CURSO EN MOODLE

Una vez realizado el análisis anterior de cómo realizar la formación para que los alumnos tenemos que preparar la formación en un entorno de teleformación. Por tanto, el temario antes mencionado lo hemos divido en 4 semanas. La primera de ellas se estudiara los fundamentos de privacidad y la AEPD y su Registro. En esta formación no se le quiere dar todo de manera sencilla al estudiante sino que con un hilo conductor y una pequeña formación pueda buscar recursos en internet y sepa auto aprender y auto gestionarse como en la vida cotidiana. En la segunda semana mirarán las medidas técnicas y organizativas y la redacción de un documento de seguridad. En la tercera semana se estudiará los derechos de los usuarios y las sanciones e infracciones. Finalmente en la última semana se realizará el practicum.

En todas las fases de estudio tendrán algún examen sea de cuestionario, sea de desarrollo que será enviado al tutor para su corrección. En el examen final como es la realización de un plan de adaptación al reglamento se le introduce una pequeña

introducción de dos casos en donde tiene que elegir uno y preguntarle al tutor como si un auditor fuese y el tutor el responsable del fichero.

CAPITULO 5

DISEÑO

5.1 ARQUITECTURA PROPUESTA

La arquitectura del sistema propuesto escogida será una arquitectura web (MVC) de 3 capas. En el entorno de desarrollo, la aplicación ha sido creada y probada con la siguiente infraestructura:

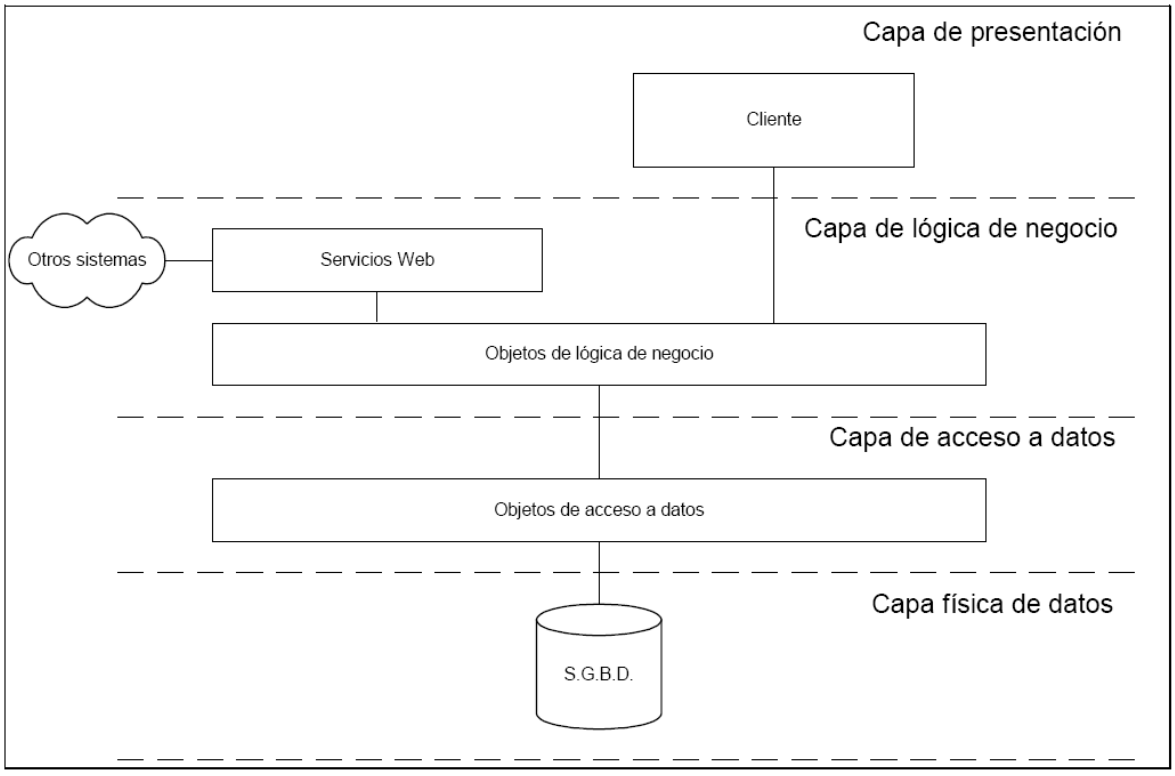
- Servidor web: Apache 2 con php 5.2.6
- Gestor de Base de Datos: Mysql 5.0.77
- Navegador Web: Podrá ser cualquier browser que implemente los estándares definidos por W3C e ISO/IEC:
    - W3C DOM Level 3: El Modelo de Objetos del Documento (DOM) es una interfaz neutral de lenguaje y plataforma que permite que los programas y secuencias accedan de forma dinámica y actualicen el contenido, estructura y estilo de documentos Web.
    - W3C HTML 4.01: lenguaje de marcado estándar para la WWW. Este lenguaje es implementado por la mayor parte de los navegadores existentes en el mercado.
    - ISO/IEC 16262 (ECMA-262): Estándar JavaScript: lenguaje de script que será empleado para implementar la lógica del GUI que se ejecutará en el navegador web.
    - W3C CSS 2.1: Las hojas de estilo establecen cómo se va a mostrar la información en una pantalla, en documentos impresos, o quizá cómo va a ser pronunciada a través de un dispositivo de lectura. El W3C ha promovido activamente la utilización de hojas de estilo en la Web desde que el Consorcio fue fundado en 1994. El W3C está desarrollando el lenguaje CSS (Hojas de Estilo en Cascada) para poder satisfacer diferentes necesidades estándar

para la elaboración de hojas de estilo en aplicaciones web.

- Adobe Reader

5.2 DEFINICIÓN DE LA ESTRUCTURA VERTICAL

Atendiendo a la clasificación lógica de los subsistemas que compondrán el aplicativo, podemos organizar estos elementos constituyentes en N capas que desempeñan distintos cometidos dentro de la arquitectura del sistema. Cada una de estas capas proporciona a la capa inmediatamente superior unos servicios de infraestructura. Estos servicios serán de mayor nivel a medida que ascendemos en la jerarquía de capas, desde la capa física de datos hasta la capa de presentación.



Cada uno de los subsistemas definidos podríamos representarlo mediante el Diagrama de componentes 1 que figura a continuación. En el que se muestran los siguientes elementos:

- Cliente: agrupa los distintos elementos que componen la interfaz de usuario y la lógica para su utilización.

- Lógica de negocio: contiene los objetos que encapsulan las reglas de negocio.

- Servicios web: objetos que facilitan la interoperabilidad con otros sistemas.

5.3 ALCANCE FUNCIONAL

En el sistema existirán tres tipos de usuarios del mismo:

- **Administradores**: Serán los responsables de crear, mantener, bloquear y eliminar a los usuarios de tipo "*profesor*" y "alumno" del sistema. Además de poder crear los cursos y administrar el sistema.

- **Profesores/Tutores**: Serán los responsables en el curso, de gestionar la formación:

- **Alumnos**: Serán los usuarios finales que realizan la formación.

5.3.1 REQUISITOS FUNCIONALES

- **RF-001**: Los usuarios deberán autenticarse en la plataforma según el siguiente criterio: Vía login/passwd.

- **RF-002**: Todos los usuarios podrán cambiar sus propia contraseña.

- **RF-003**: Todos los accesos (fallidos o no), deberán quedar registrados en un fichero, con información de IP desde dónde se han intentado loguear y fecha y hora del acto.

- **RF-004**: Gestión de usuarios por parte de profesores/administradores del LABSEGTEL.
  - asignar curso a un alumno.
  - permitirá confirmar y modificar el estado de una prueba

- **RF-005**: El profesor y el administrador entrar en un alumno y ver todos los estadísticos: veces que a entrado en el aula, veces que ha realizado el examen, etc.

- **RF-006**: El administrador crea un curso y asigna profesores

5.3.2 REQUISITOS NO FUNCIONALES

Además de los requisitos funcionales, necesarios para el funcionamiento normal de la aplicación, se establecen los siguientes requisitos no funcionales.

Requisitos de Seguridad

- **RNF-001**: Todas las comunicaciones (cliente-servidor) han de estar cifradas, mediante HTTPS.
- **RNF-002**: Se aplicarán las medidas necesarias para cumplir la LOPD, según el nivel de seguridad que corresponda.
- **RNF-003**: La aplicación tendrá una política centralizada de autorización, que establezca los roles o permisos necesarios para ejecutar cada acción en la capa de negocio de la aplicación, controlándose y validándose dichos accesos.
- **RNF-004**: La aplicación será inmune a ataques de "SQL Injection" y "Cross Site Scripting".

Requisitos de interfaz de usuario, usabilidad y accesibilidad.

- **RNF-005**: Se respetará lo establecido en la legislación vigente sobre accesibilidad (en los casos en lo que sea necesaria).
  - Real Decreto 1494/2007, de 12 de noviembre, , por el que se aprueba el Reglamento sobre las condiciones básicas para el acceso de las personas con discapacidad a la sociedad de la información.
  - Normativa UNE 139803:2004: Aplicaciones informáticas para personas con discapacidad. Requisitos de accesibilidad para contenidos en la Web
  - eEurope 2002. "Accesibilidad de los sitios Web públicos y de su Contenido".
  - eEurope 2005. "Una sociedad de la información para todos".
  - La accesibilidad electrónica Bruselas, 13.09.2005.
  - Directrices de **Accesibilidad** para el Contenido Web (**WCAG** 2.0) del W3C definidos por la Iniciativa de Accesibilidad Web (**WAI**).

- **RNF-006**: El idioma del interfaz por defecto será el español.
- **RNF-007**: La aplicación deberá establecer un tiempo de seguridad (time-out) transcurrido el cual si no ha detectado actividad se finalizará la sesión.

Requisitos de rendimiento

- **RNF-008**: La aplicación proporcionará unos tiempos de respuesta aceptables que permitan un trabajo fluido y eficaz.

5.4 BATERÍAS DE PRUEBAS

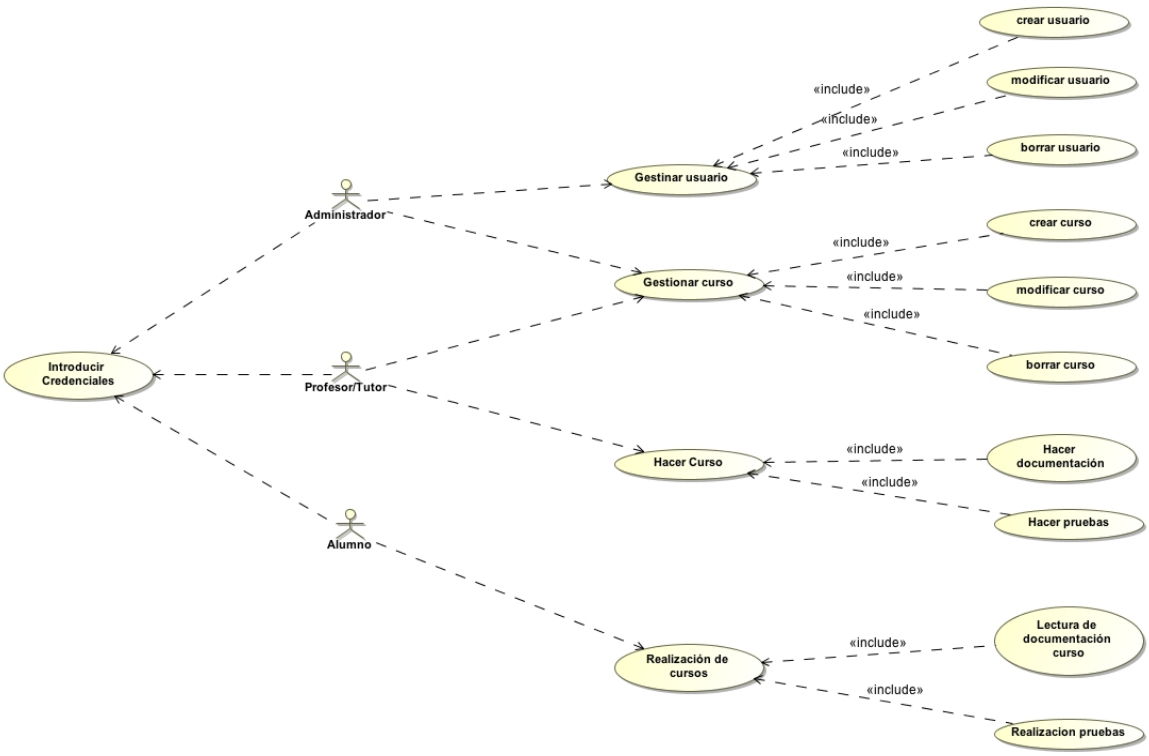
Pruebas unitarias y de integración

No se exige ninguna batería de pruebas en especial, ni cobertura, si bien es recomendable la realización de las mismas para garantizar el correcto funcionamiento del producto a entregar.

Pruebas de aceptación del cliente

No se ha facilitado ninguna batería de pruebas a superar, previa entrega, como prueba de cumplimiento del contrato de los casos de uso acordados.

5.5 CASOS DE USO



5.6 CASOS DE USOS DESCRIPTIVOS

5.6.1 AUTENTICACIÓN

RF-001	**Autenticación vía usuario/password**	
Descripción	El sistema deberá permitir a los usuarios autenticarse vía web, mediante usuario y contraseña	
Precondición		
Secuencia Normal	**Paso**	**Acción**
	1	El usuario accede a la aplicación
	2	El sistema le solicita el usuario
	3	El usuario introduce la contraseña
	4	El sistema comprueba que las credenciales sean correctas y no esté caducado la contraseña
	5	El sistema comprueba que el usuario pertenece al LABSEGTEL

	6	El sistema guarda los datos de autenticación: fecha, hora
	7	El sistema le muestra la pantalla inicial de bienvenida al usuario
Postcondición		
Excepciones	**Paso**	**Acción**
	4’	La contraseña no es válida
		4’.1 El sistema informa al usuario y aborta la operación
	4’’	La cuenta del usuario está caducada o bloqueada
		4’’.1 El sistema informa al usuario y aborta la operación
Rendimiento		
Frecuencia		
Importancia		
Urgencia		
Comentarios	NOTA: El sistema guardará un registro (log), de todos los intentos de autenticación (correctos o fallidos)	

5.6.2 CAMBIO DE CONTRASEÑA

RF-002	**Cambio de contraseña**	
Descripción	El sistema deberá permitir a los usuarios cambiar la contraseña	
Precondición	Usuario autenticado y dentro de la aplicación	
Secuencia Normal	**Paso**	**Acción**
	1	El usuario accede a la pestaña de cambio de contraseña
	2	El sistema le solicita la contraseña actual
	3	El usuario introduce la nueva contraseña
	4	El usuario vuelve a introducir la nueva contraseña
	5	El sistema le muestra la pantalla inicial el aviso de cambio de contraseña correcta
Postcondición		
Excepciones	**Paso**	**Acción**
	2’	La contraseña no es válida
		4’.1 El sistema informa al usuario y aborta la operación
	4’’	La contraseña no es igual a la introducida en el paso 3
		4’’.1 El sistema informa al usuario y aborta la operación
Rendimiento		
Frecuencia		
Importancia		
Urgencia		
Comentarios	NOTA: El sistema guardará un registro (log), de todos los intentos de cambio de contraseña (correctos o fallidos)	

5.6.3 GESTION DE USUARIOS

RF-004	**Gestión de usuarios**
Descripción	El sistema deberá permitir a los profesores/administradores gestionar a un usuario: asignar curso a un alumno, permitir modificar estado de una prueba
Precondición	Usuario autenticado y dentro de la aplicación

Secuencia Normal	**Paso**	**Acción**
	1	El usuario accede a la pestaña de usuarios
	2	El sistema le solicita usuario sobre quien quiere hacer la acción
	3	El profesor/administrador busca y selecciona al usuario
	4	Entra en la ficha del usuario y cambia roles
	5	El sistema le muestra la pantalla inicial el aviso de modificación de atributos
Postcondición		
Excepciones	**Paso**	**Acción**
	2’	El usuario no es valido
		4’.1 El sistema informa al usuario y aborta la operación
	4’’	El rol no se puede cambiar
		4’’.1 El sistema informa al usuario y aborta la operación
Rendimiento		
Frecuencia		
Importancia		
Urgencia		
Comentarios	NOTA: El sistema guardará un registro (log).	

5.6.4 VER ESTADISTICOS

RF-005	**Ver estadísticos**	
Descripción	El sistema deberá permitir a los profesores/administradores ver los estadísticos de un alumno	
Precondición	Usuario autenticado y dentro de la aplicación	
Secuencia Normal	**Paso**	**Acción**
	1	El usuario accede a la pestaña de estadísticos
	2	El sistema le solicita usuario sobre quien quiere hacer la acción
	3	El profesor/administrador busca y selecciona al usuario
	4	Entra en la ficha de estadísticos del alumno
Postcondición		
Excepciones	**Paso**	**Acción**
	2’	El usuario no es valido
		4’.1 El sistema informa al usuario y aborta la operación
Rendimiento		
Frecuencia		
Importancia		
Urgencia		
Comentarios	NOTA: El sistema guardará un registro (log).	

5.6.5 CREACION DE CURSOS

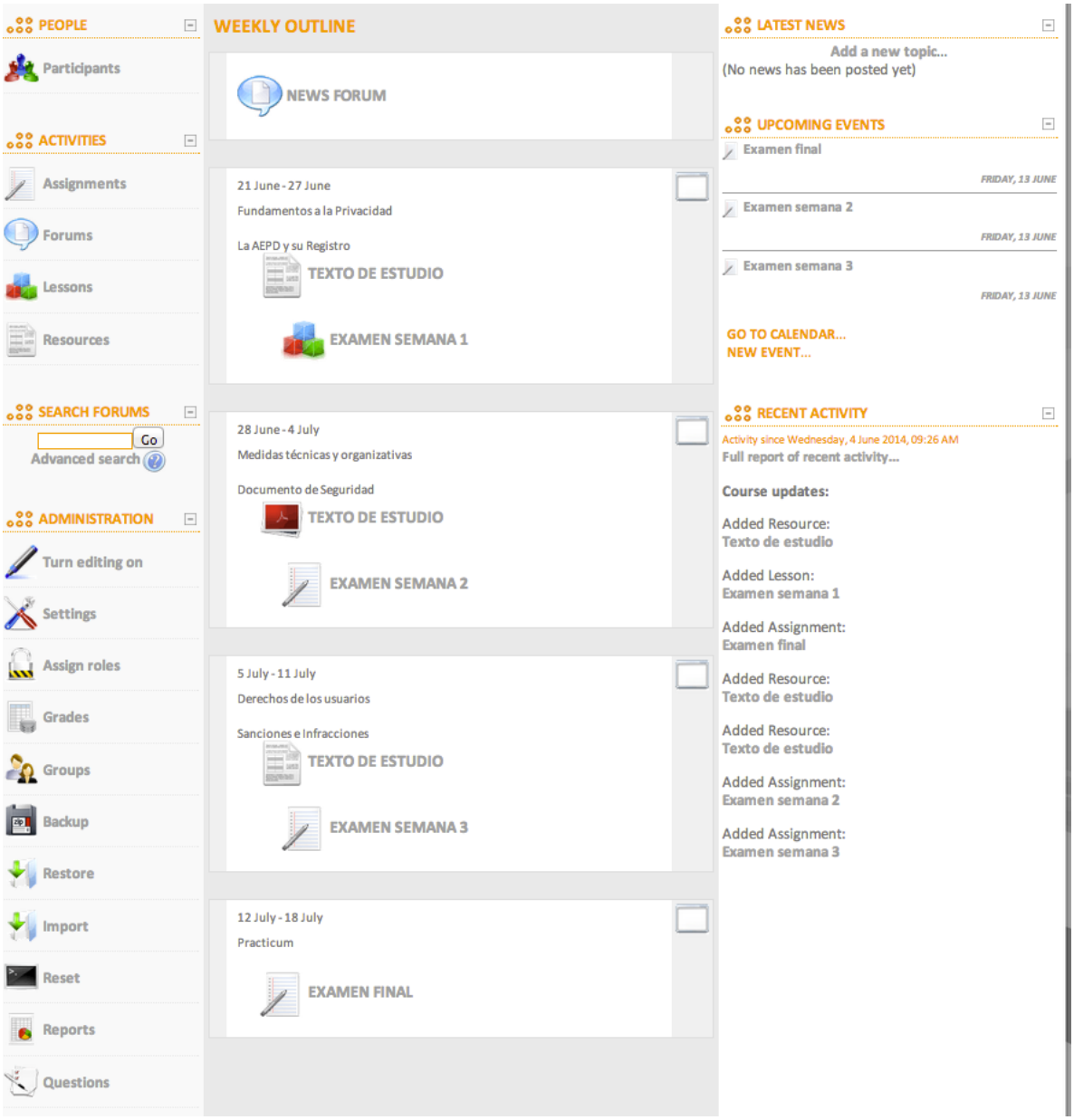
RF-006	**Creación de cursos**

Descripción	El sistema deberá permitir a los administradores crear un curso y asignar profesores	
Precondición	Usuario autenticado y dentro de la aplicación	
Secuencia Normal	**Paso**	**Acción**
	1	El usuario accede a la pestaña de gestión
	2	El usuario crea un curso clicando en creación y rellenando los datos
	3	El usuario asigna profesores
Postcondición		
Excepciones	**Paso**	**Acción**
Rendimiento		
Frecuencia		
Importancia		
Urgencia		
Comentarios	NOTA: El sistema guardará un registro (log).	

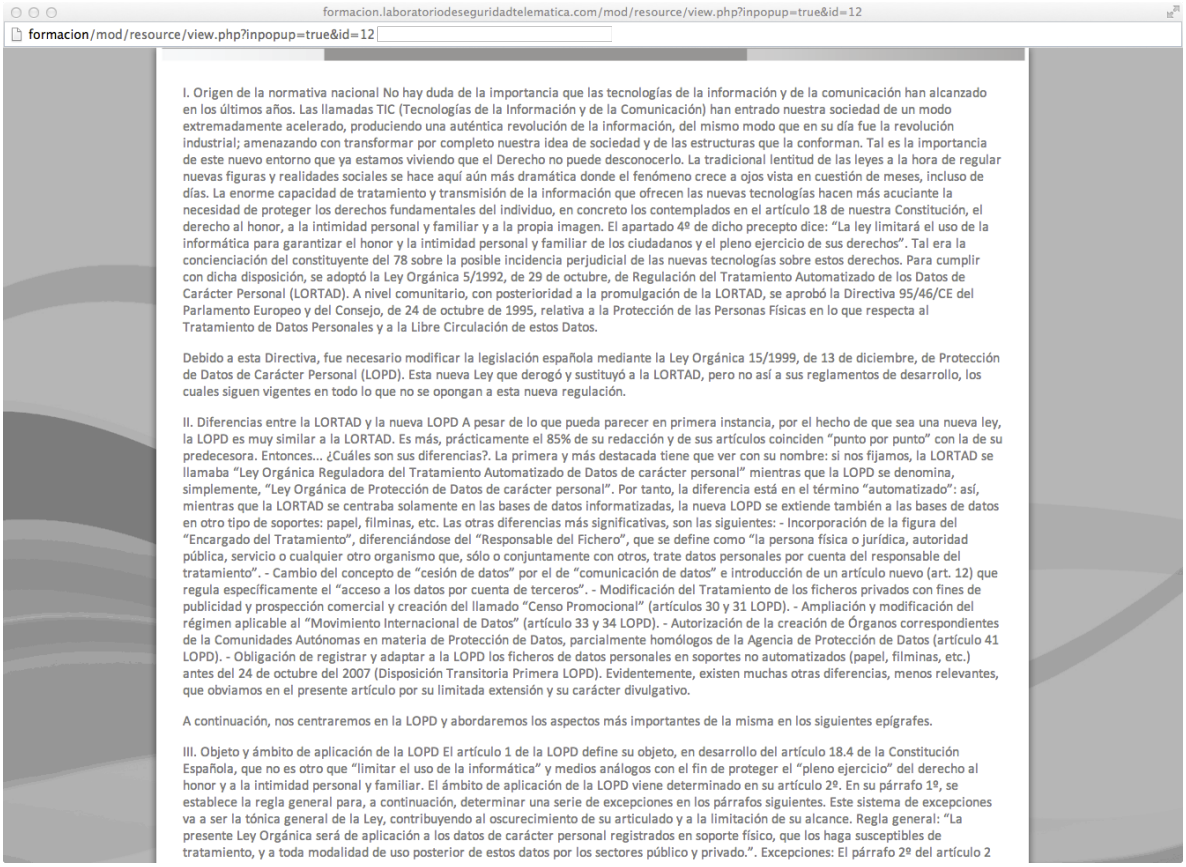
5.7 INTERFACES DE USUARIO (GUI)

5.7.1 Curso online

En esta pantalla se puede ver estructurado el curso: las semanas con sus textos de estudio, exámenes parciales, fórum, etc.


PEOPLE
Participants
ACTIVITIES
Assignments
Forums
Lessons
Resources
SEARCH FORUMS
Go
Advanced search
ADMINISTRATION
Turn editing on
Settings
Assign roles
Grades
Groups
Backup
Restore
Import
Reset
Reports
Questions
WEEKLY OUTLINE
NEWS FORUM
21 June - 27 June
Fundamentos a la Privacidad
La AEPD y su Registro
TEXTO DE ESTUDIO
EXAMEN SEMANA 1
28 June - 4 July
Medidas técnicas y organizativas
Documento de Seguridad
TEXTO DE ESTUDIO
EXAMEN SEMANA 2
5 July - 11 July
Derechos de los usuarios
Sanciones e Infracciones
TEXTO DE ESTUDIO
EXAMEN SEMANA 3
12 July - 18 July
Practicum
EXAMEN FINAL
LATEST NEWS
Add a new topic...
(No news has been posted yet)
UPCOMING EVENTS
Examen final
FRIDAY, 13 JUNE
Examen semana 2
FRIDAY, 13 JUNE
Examen semana 3
FRIDAY, 13 JUNE
GO TO CALENDAR...
NEW EVENT...
RECENT ACTIVITY
Activity since Wednesday, 4 June 2014, 09:26 AM
Full report of recent activity...
Course updates:
Added Resource:
Texto de estudio
Added Lesson:
Examen semana 1
Added Assignment:
Examen final
Added Resource:
Texto de estudio
Added Resource:
Texto de estudio
Added Assignment:
Examen semana 2
Added Assignment:
Examen semana 3

5.7.2 Texto de estudio para la semana 1 relativo a fundamentos de la privacidad



formacion.laboratoriodeseguridadtelematica.com/mod/resource/view.php?inpopup=true&id=12

formacion/mod/resource/view.php?inpopup=true&id=12

I. Origen de la normativa nacional No hay duda de la importancia que las tecnologías de la información y de la comunicación han alcanzado en los últimos años. Las llamadas TIC (Tecnologías de la Información y de la Comunicación) han entrado nuestra sociedad de un modo extremadamente acelerado, produciendo una auténtica revolución de la información, del mismo modo que en su día fue la revolución industrial; amenazando con transformar por completo nuestra idea de sociedad y de las estructuras que la conforman. Tal es la importancia de este nuevo entorno que ya estamos viviendo que el Derecho no puede desconocerlo. La tradicional lentitud de las leyes a la hora de regular nuevas figuras y realidades sociales se hace aquí aún más dramática donde el fenómeno crece a ojos vista en cuestión de meses, incluso de días. La enorme capacidad de tratamiento y transmisión de la información que ofrecen las nuevas tecnologías hacen más acuciante la necesidad de proteger los derechos fundamentales del individuo, en concreto los contemplados en el artículo 18 de nuestra Constitución, el derecho al honor, a la intimidad personal y familiar y a la propia imagen. El apartado 4º de dicho precepto dice: "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". Tal era la concienciación del constituyente del 78 sobre la posible incidencia perjudicial de las nuevas tecnologías sobre estos derechos. Para cumplir con dicha disposición, se adoptó la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal (LORTAD). A nivel comunitario, con posterioridad a la promulgación de la LORTAD, se aprobó la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, 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.

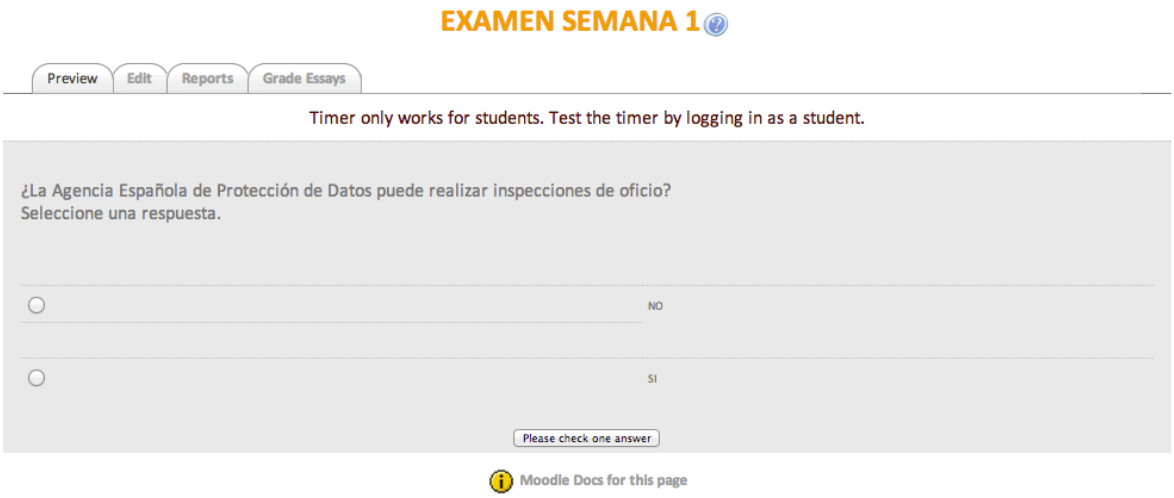
Debido a esta Directiva, fue necesario modificar la legislación española mediante la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD). Esta nueva Ley que derogó y sustituyó a la LORTAD, pero no así a sus reglamentos de desarrollo, los cuales siguen vigentes en todo lo que no se opongan a esta nueva regulación.

II. Diferencias entre la LORTAD y la nueva LOPD A pesar de lo que pueda parecer en primera instancia, por el hecho de que sea una nueva ley, la LOPD es muy similar a la LORTAD. Es más, prácticamente el 85% de su redacción y de sus artículos coinciden "punto por punto" con la de su predecesora. Entonces... ¿Cuáles son sus diferencias?. La primera y más destacada tiene que ver con su nombre: si nos fijamos, la LORTAD se llamaba "Ley Orgánica Reguladora del Tratamiento Automatizado de Datos de carácter personal" mientras que la LOPD se denomina, simplemente, "Ley Orgánica de Protección de Datos de carácter personal". Por tanto, la diferencia está en el término "automatizado": así, mientras que la LORTAD se centraba solamente en las bases de datos informatizadas, la nueva LOPD se extiende también a las bases de datos en otro tipo de soportes: papel, filminas, etc. Las otras diferencias más significativas, son las siguientes: - Incorporación de la figura del "Encargado del Tratamiento", diferenciándose del "Responsable del Fichero", que se define como "la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento". - Cambio del concepto de "cesión de datos" por el de "comunicación de datos" e introducción de un artículo nuevo (art. 12) que regula específicamente el "acceso a los datos por cuenta de terceros". - Modificación del Tratamiento de los ficheros privados con fines de publicidad y prospección comercial y creación del llamado "Censo Promocional" (artículos 30 y 31 LOPD). - Ampliación y modificación del régimen aplicable al "Movimiento Internacional de Datos" (artículo 33 y 34 LOPD). - Autorización de la creación de Órganos correspondientes de la Comunidades Autónomas en materia de Protección de Datos, parcialmente homólogos de la Agencia de Protección de Datos (artículo 41 LOPD). - Obligación de registrar y adaptar a la LOPD los ficheros de datos personales en soportes no automatizados (papel, filminas, etc.) antes del 24 de octubre del 2007 (Disposición Transitoria Primera LOPD). Evidentemente, existen muchas otras diferencias, menos relevantes, que obviamos en el presente artículo por su limitada extensión y su carácter divulgativo.

A continuación, nos centraremos en la LOPD y abordaremos los aspectos más importantes de la misma en los siguientes epígrafes.

III. Objeto y ámbito de aplicación de la LOPD El artículo 1 de la LOPD define su objeto, en desarrollo del artículo 18.4 de la Constitución Española, que no es otro que "limitar el uso de la informática" y medios análogos con el fin de proteger el "pleno ejercicio" del derecho al honor y a la intimidad personal y familiar. El ámbito de aplicación de la LOPD viene determinado en su artículo 2º. En su párrafo 1º, se establece la regla general para, a continuación, determinar una serie de excepciones en los párrafos siguientes. Este sistema de excepciones va a ser la tónica general de la Ley, contribuyendo al oscurecimiento de su articulado y a la limitación de su alcance. Regla general: "La presente Ley Orgánica será de aplicación a los datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado.". Excepciones: El párrafo 2º del artículo 2

5.7.3 Test de la semana 1



EXAMEN SEMANA 1

Preview | Edit | Reports | Grade Essays

Timer only works for students. Test the timer by logging in as a student.

¿La Agencia Española de Protección de Datos puede realizar inspecciones de oficio?
Seleccione una respuesta.

NO

SI

Please check one answer

Moodle Docs for this page

5.7.4 Practicum

'ORMACIÓN LABORATORIO DE SEGURIDAD TELEMÁTICA ▶ CF101 ▶ ASSIGNMENTS ▶ EXAMEN FINAL

Update this Assignment

No attempts have been made on this assignment

CASO 1:

La base de datos MPRL.mdb ubicada en un ordenador de la institución que da un master. Hay dos personas autorizadas a usar la base de datos desde el mismo ordenador. No esta dada de alta en la AGENCIA DE PROTECCIÓN DE DATOS. No se añaden ni modifican los datos con mucha frecuencia. La copia de seguridad se realiza una vez cada dos semanas y se guardan en la misma sala. Están cifrados.

CASO 2:

Una empresa de servicios ubica las páginas web (http://www.lsi.uvigo.es/didega/) de otra. El servidor realiza una copia de seguridad total una vez a la semana. Las copias se ubican en la misma sala. Para las copias de seguridad se emplea el propio software que viene con el sistema operativo (LINUX) y usa cintas DAT cuyo lector está ubicado en la misma CPU. Para subir las nuevas páginas la empresa usan el servicio de ftp. El servidor es Linux.

Elija uno de los dos casos y haga un documento de seguridad completo. Cualquier duda o cuestión realizará al tutor de la asignatura como si fuese una toma de datos ante un Plan de Adaptación al Reglamento.

NOTAS:

1) NO SUPONGA NADA QUE NO ESTE ESCRITO POR TANTO CONTEMPLE CUALQUIER CASO AUNQUE NO ESTE ESPÉCIFICADO.

2) LEA TODO EL CASO ANTES DE EMPEZAR A SOLUCIONAR EL PROBLEMA.

Available from: Friday, 6 June 2014, 09:10 AM

Due date: Friday, 13 June 2014, 09:10 AM

CAPITULO 6

CONCLUSIONES

Después de haber desarrollado el TFG “Plan de adaptación a la L.O.P.D. de un sistema de formación de un curso de Protección de Datos y diseño de una asignatura para su formación” he podido sacar las siguientes conclusiones:

1) Aunque existe documentación sobre la Ley Orgánica de Protección de Datos y su Reglamento de Medidas de Seguridad, dicha documentación está orientada solamente a juristas, con la dificultad que conlleva a los que somos técnicos.

2) Los técnicos que no tengan conocimientos jurídicos, deberían de asesorarse o asociarse con juristas para tratar dichos temas, a ser posible especializados en derecho administrativo, dado que esta Ley pertenece a dicha especialidad del derecho. Debido a que no solo hay que saber leer e interpretar la ley, sino saber cuando y como hay que aplicarla, que leyes están relacionadas, etc.

3) Existe una falta de entendimiento entre técnicos y juristas, a pesar de que esta ley, igual que otras, como la Ley de la Sociedad de los Sistemas de Información y Comercio Electrónico (L.S.S.I.-C.E) o la firma electrónica, nos obliga a entendernos y trabajar en proyectos transversales.

4) La existencia de una metodología reconocida y certificada que los auditores en L.O.P.D. puedan seguir reconocida a nivel internacional. Dicha metodología se recoge mediante un sello europeo auspiciado por la U.E. conocido como Europrise. Esto favorece y reduce el intrusismo en este sector. A pesar de esto es poco conocido y existe un gran intrusismo existiendo multitud de planes de adaptación y de auditoria.

5) Resulta sorprendente y negativo que diferentes productos de grandes multinacionales del software, desarrollen aplicaciones y sistemas operativos para la Unión Europea, sin aplicar nuestras directivas sobre la protección de la información.

Por último, indicar que este proyecto puede ser la base para el desarrollo de otros muchos como: Deficiencias en la actual Ley y en el Reglamento de Medidas de Seguridad frente a la tecnología existente; Planes de adaptación a la LOPD en las universidades, privacidad en entornos cloud en las universidades, etc.

CAPITULO 7

GLOSARIO

Hay que tener en cuenta que para elaborar y redactar el presente manual, se han utilizado términos que bien, por ser de uso poco común en el lenguaje cotidiano, bien porque en el ámbito de la Protección de Datos adquieren una significación propia, es necesario definir y detallar para que todo aquel que tenga acceso a la documentación aportada pueda adquirir una adecuada comprensión del mismo.

Accesos autorizados: Autorizaciones concedidas a un usuario para la utilización de diversos recursos.

Alteración: Modificación física de las señales representativas de los datos registrados en soportes informatizados por causas accidentales o intencionadas.

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

Cesión o comunicación de datos: Toda revelación de datos realizada a una persona distinta del interesado.

Código de identificación de usuario: Cadena de caracteres utilizados para identificar a un usuario.

Confidencialidad: Propiedad de la información que hace que ésta sólo pueda ser revelada a individuos, personas, entidades o procesos autorizados, en el momento y forma previstos.

Contraseña: Información confidencial, frecuentemente constituida por una cadena de caracteres, que puede ser usada en la autenticación de un usuario.

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

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

Dato de carácter personal: Comprende cualquier información concerniente a personas físicas identificadas o identificables.

Datos especialmente protegidos: Datos de carácter personal relativos a la ideología, afiliación sindical, religión, creencias, origen racial, salud, vida sexual, comisión de infracciones penales o administrativas y que son objeto de las disposiciones del artículo 7 de la LOPD.

Disponibilidad: Propiedad que requiere que los recursos de un sistema sean accesibles y puedan ser utilizados por un usuario autorizado, en todo momento o dentro de un tiempo razonable.

Encargado del tratamiento: Persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento.

Entorno: Conjunto de bienes, muebles e inmuebles, fungibles o no, externos al equipo físico, lógico y datos mediante los cuales son posibles las distintas operaciones que, según el artículo 3 de la LOPD, integran el tratamiento de los datos.

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

Fichero Temporal: Comprende todo fichero de datos cuyo uso sea accesorio o auxiliar y que es necesario sólo mientras dure un concreto trabajo o proceso.

Identificación: Procedimiento de reconocimiento de la identidad de un usuario o proceso.

Incidencia: Cualquier anomalía que afecte o pueda afectar a la seguridad de datos, desde el punto de vista de su confidencialidad, integridad y/o disponibilidad.

Integridad: Propiedad de la información que garantiza que esta es completa, exacta y válida.

Pérdida: Desaparición física de las señales representativas de los datos registrados en soportes informatizados, por causas accidentales o intencionadas.

Perfil de acceso de un usuario: Recursos informáticos y tipos de acceso a los mismos, autorizados para un usuario.

Plan de contingencia: Conjunto documentado de medidas a tomar y de los responsables de las mismas, ante situaciones anómalas o síntomas de estas.

Plan de seguridad: Documento que describe cómo una Organización gestiona y organiza sus requisitos de seguridad.

Red de telecomunicación: Conjunto de canales de transmisión, circuitos y, en su caso, dispositivos o centrales de conmutación, que proporcionan conexiones entre dos o más puntos definidos para facilitar la telecomunicación entre ellos.

Recurso: Cualquier parte componente de un sistema de información

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.

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.

Salvaguarda: Proceso de realización de una copia preventiva o de reserva, o la propia copia que resulta del proceso.

Sistemas de Información: Conjunto de ficheros automatizados, programas, soportes y equipos empleados para el almacenamiento y tratamiento de datos de carácter personal.

Soporte: Objeto físico susceptible de ser tratado en un Sistema de Información y sobre el cual se pueden grabar y/o recuperar datos que se utilizan para realizar copias o pasos intermedios en los procesos de la aplicación que gestiona los Ficheros.

Usuario: Toda persona, sujeto o proceso que hay sido expresamente autorizado para acceder a datos, información o recursos.

CAPITULO 8

RECURSOS

[1] AEPD: http://www.agpd.es/

Resumen: Web corporativa del máximo responsable sobre la LOPD y su RD 1720/2007 con el nombre de Agencia Española de Protección de Datos. Donde podemos encontrar todo lo referente a dicha legislación y la manera de implementarla,

Aspectos relevantes que sean de interés: Encontrar todo tipo de información relacionado con el tema de que nos ocupa.

[2]: http://www.inteco.es/Formacion/Legislacion/Ley_Organiza_de_Proteccion_de_Datos/

Resumen: INTECO explica desde su punto de vista la Ley y como aplicarla

Aspectos relevantes que sean de interés: Otros puntos de vista de cómo afrontar el proyecto

[3] http://www.microsoft.com/business/es-es/content/paginas/article.aspx?cbcid=236

Resumen: Web de Microsoft donde explica como adaptar la LOPD cuando se usan entornos de dicho fabricante.

Aspectos relevantes que sean de interés: Explica de una manera sencilla y clara como adaptar los sistemas telemáticos de información la dicha legislación

[4] Pintos & Salgado: http://www.pintos-salgado.com

Resumen: Bufete referente a nivel nacional e internacional relacionado con las nuevas tecnologías y en concreto sobre la LOPD

Aspectos relevantes que sean de interés: explica de una manera clara y sencilla como adaptar los sistemas a la LOPD

[5] Titulo de recurso: Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal"

Autores: Varios (director y coordinador Antonio Troncoso Reigada)

Año: 2010

Fuente de información: Aranzadi y la Agencia de Protección de Datos de la Comunidad de Madrid (ISBN 978-84-470-3423-9)

Resumen: Expertos nacionales e internacionales de la privacidad y de la seguridad explican la L.O.P.D. y su RD 1720/2007
Aspectos relevantes que sean de interés: todo lo referido a la legislación está explicado desde el punto de vista de los expertos en esta materia.

ANEXO A1

DESARROLLO DOCUMENTO DE SEGURIDAD

A1.1 RECURSOS PROTEGIDOS

SISTEMAS OPERATIVOS

Los sistemas operativos empleados en los sistemas de información del proyecto LABSEGTEL son diferentes, en función de su ámbito de aplicación:

Servidor de datos (1):

- HP PROLIANT ML 350 G4, 2GB Xeon
  Windows 2003 Server

Terminales de trabajo y de toma de datos (11):

- Ordenadores personales de sobremesa. Terminales de trabajo:
  IBM Netvista M42 8307 P4 1.8 GHz 256 MB
  Windows XP Pro

Ordenador Portátil (1):

- Ordenador personal. Terminales de trabajo:
  IBM Cambrige Type 2645-760 PII 233 MHz
  Windows 2000 Pro.

Los usuarios se identifican en el sistema operativo mediante un nombre de entrada y una contraseña.

APLICACIONES O PROGRAMAS QUE ACCEDEN A DATOS DE CARÁCTER PERSONAL

Las aplicaciones informáticas empleadas para acceder a los datos de carácter personal que se manejan en el proyecto LABSEGTEL son diferentes, en función de su ámbito de aplicación:

Ámbito de contabilidad:

- Gestión contable general de los clientes, proveedores de la asociación, etc…
  - Aplicación contaplus (GrupoSP), para mantener datos históricos de la contabilidad del proyecto.

Ámbito de Gestión:

Para la gestión se útiiza las herramientas propias desarrolladas para LABSEGTEL basadas en Microsoft Office.

Ámbito ofimático:

- Entorno de trabajo de la asociación:
  Cliente de correo electrónico (outlook), procesador de textos (word), hoja de cálculo (excel), base de datos (access).

Ambito de Teleformación:

Para la teleformación se usa el software libre Moodle.

EQUIPOS INFORMÁTICOS QUE TIENEN ACCESO A DATOS DE CARÁCTER PERSONAL

Los equipos informáticos que tienen acceso a datos de carácter personal están ubicados en avda Tibidabo, nº. 39-43 (08035 Barcelona, España).

Servidor de datos (1)

- Servidor de Datos, Antivirus y Copias de Seguridad, Windows 2003 Server :
  Almacena los datos que se manejan en el proyecto LABSEGTEL documentos relacionados con los usuarios (documentos de texto generados con word, hojas de cálculo generadas con excel, etc…) utilizados en el trabajo diario.
  Almacena el antivirus Symantec empleado en el proyecto y además desde el servidor se realizan las copias de Seguridad (en Cintas de Datos). También gestiona todo el sistema de moodle para la teleformación.

Terminales de trabajo (11):

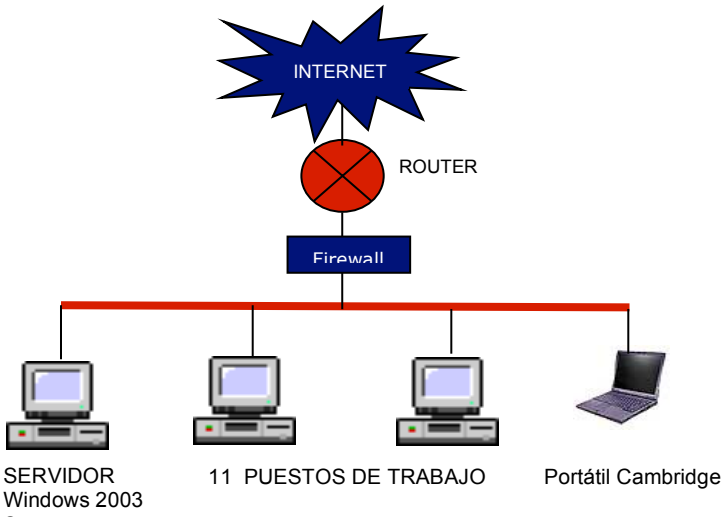
- Ordenadores personales utilizados en las áreas gestión,contabilidad, ofimática, programación…: equipos informáticos que se utilizan principalmente para realizar tareas de gestión del proyecto. También se destinan a realizar trabajos habituales de oficina.

Ordenador Potátil (1):

- Ordenador empleado para principalmente para formación, congresos, cursos, etc.

DESCRIPCIÓN DEL ENTORNO DE RED DE LOS SISTEMAS DE INFORMACIÓN

El entorno de red del proyecto está formado por los siguientes elemenCRIPCIÓN DEL ENTORNO DE RED. Como se puede observar en el gráfico utiliza una topologia en estrella como arquitectura LAN ya que los puntos extremos de una red se conectan aun switch de capa de la marca Allied Telesyn con su modelo Rapier 24i. Esta topologia es conveniente por razones de seguridad y acceso restringido aunque puede ser susceptible a problemas en el nodo central de la estrella.



- En servidor de datos y aplicaciones y terminales de trabajo, ambos conectados a un switch al que también se conectan otros elementos de la red de la empresa; estos elementos son: un **firewall** que protege a empreaques externos. A este firewall va conectado el **router de un proveedor de servicios** a este switch también va conectada por impresoras en red. Dicho cortafuegos usa una tecnoligia embebida en Linux (128 Mb de RAM, disco duro de 20 GB y 3 interfaces de red) además permite la realización de redes virutales privadas (VPNs) con OPENVPN.

- Con todos estos elementos del proyecto constituye un sistema de información bastante seguro de cara a las instrusiones, lo cual protege muy bien el acceso por entidades ajenas a los datos de carácter personal.

	RESPONSABLE DEL FICHERO **Fdo.:**

A1.2 REGISTROS DE FICHEROS

NOMBRE DE FICHERO Logs del sistema	**FECHA NOTIF.**	**TIPO NOTIFICACIÓN** Creación	**NIVEL DE SEGURIDAD** BAJO
FINALIDAD DEL FICHERO Logs creados por el sistema LABSEGTEL		**CÓDIGO ASIGNADO POR LA A.E.P.D.**	
NOMBRE DE FICHERO Agenda del proyecto	**FECHA NOTIF.** / /	**TIPO NOTIFICACIÓN** Creación	**NIVEL DE SEGURIDAD** BAJO
FINALIDAD DEL FICHERO Gestión de la agenda de los miembros del proyecto		**CÓDIGO ASIGNADO POR LA A.E.P.D.**	
NOMBRE DE FICHERO Personal docente	**FECHA NOTIF.** / /	**TIPO NOTIFICACIÓN** Creación	**NIVEL DE SEGURIDAD** BAJO
FINALIDAD DEL FICHERO Gestión y control del personal docente del proyecto		**CÓDIGO ASIGNADO POR LA A.E.P.D.**	
NOMBRE DE FICHERO Usuarios	**FECHA NOTIF.** / /	**TIPO NOTIFICACIÓN** Creación	**NIVEL DE SEGURIDAD** BAJO
FINALIDAD DEL FICHERO Gestión y control del personal usuarios del proyecto de teleformación LABSEGTEL		**CÓDIGO ASIGNADO POR LA A.E.P.D.**	
NOMBRE DE FICHERO Proveedores	**FECHA NOTIF.** / /	**TIPO NOTIFICACIÓN** Creación	**NIVEL DE SEGURIDAD** BAJO
FINALIDAD DEL FICHERO Seguimiento y control de las empresas suministradoras		**CÓDIGO ASIGNADO POR LA A.E.P.D.**	
NOMBRE DE FICHERO	**FECHA NOTIF.** / /	**TIPO NOTIFICACIÓN**	**NIVEL DE SEGURIDAD**
FINALIDAD DEL FICHERO		**CÓDIGO ASIGNADO POR LA A.E.P.D.**	
NOMBRE DE FICHERO	**FECHA NOTIF.** / /	**TIPO NOTIFICACIÓN**	**NIVEL DE SEGURIDAD**
FINALIDAD DEL FICHERO		**CÓDIGO ASIGNADO POR LA A.E.P.D.**	
		RESPONSABLE DEL FICHERO Fdo.	

A1.3 ESTRUCTURA DE FICHEROS

NOMBRE DE FICHERO	Logs del sistema
DATOS PERSONALES QUE CONTIENE	
De caracter identificativo IP Nombre usuario Fecha y hora de los accesos	
UBICACIÓN DEL FICHERO	
Este fichero y sus datos de carácter personal se encuentran ubicados en el sistema de información en la avda Tibidabo, nº. 39-43 (08035 Barcelona, España).	
EQUIPOS INFORMÁTICOS Y SOPORTES RELACIONADOS CON EL FICHERO	
El sistema de información del proyecto	
PROCEDENCIA Y PROCEDIMIENTO DE RECOGIDA	
El propio interesado o su representante legal, otras personas físicas distintas del afectado o su representante, recogiendo los datos en formularios o entrevistas o cupones o transmisión electrónica de datos. En soporte informático/magnético o via telemática.	

RESPONSABLE DEL FICHERO
Fdo.:

NOMBRE DE FICHERO	Agenda proyecto
DATOS PERSONALES QUE CONTIENE	
De caracter identificativo Nombre y apellidos Dirección(postal, electrónica) Teléfono E-mail	
UBICACIÓN DEL FICHERO	
Este fichero y sus datos de carácter personal se encuentran ubicados en el sistema de información en la Tibidabo, nº. 39-43 (08035 Barcelona, España).	
EQUIPOS INFORMÁTICOS Y SOPORTES RELACIONADOS CON EL FICHERO	
El sistema de información del proyecto	
PROCEDENCIA Y PROCEDIMIENTO DE RECOGIDA	
El propio interesado o su representante legal, otras personas físicas distintas del afectado o su representante, recogiendo los datos en formularios o entrevistas o cupones o transmisión electrónica de datos. En soporte papel, soporte informático/magnético o via telemática.	

RESPONSABLE DEL FICHERO
Fdo.:

NOMBRE DE FICHERO	Personal docente

DATOS PERSONALES QUE CONTIENE

De caracter identificativo DNI Nombre y apellidos Telefono Dirección Nº Registro personal **Datos de caracteristicas personales** Estado civil Familia Nacionalidad Sexo Fecha de nacimiento Lugar de nacimiento Edad	**Datos de circunstancias sociales** Licencias Permisos Autorizaciones **Datos académicos y profesionales** Formación Titulaciones Experiencia profesional **Datos de detalles dle empleo** Cuerpo/escala Categoría/grado Puestos de trabajo Historial del trabajador

UBICACIÓN DEL FICHERO

Este fichero y sus datos de carácter personal se encuentran ubicados en el sistema de información en la Avda. Tibidabo, nº. 39-43 (08035 Barcelona, España).

PROCEDENCIA Y PROCEDIMIENTO DE RECOGIDA

El sistema de información del proyecto (moodle, aplicación en access para la gestión)

PROGRAMAS ASOCIADOS AL FICHERO

El propio interesado o su representante legal, otras personas físicas distintas del afectado o su representante, recogiendo los datos en formularios o entrevistas o cupones o transmisión electrónica de datos. En soporte papel, soporte informático/magnético o via telemática.

RESPONSABLE DEL FICHERO

Fdo.:

NOMBRE DE FICHERO	Usuarios
DATOS PERSONALES QUE CONTIENE	
De caracter identificativo DNI Nombre y apellidos Telefono Dirección Nombre de usuario Contraseña **Datos de caracteristicas personales** Sexo Fecha de nacimiento Lugar de nacimiento Edad	
UBICACIÓN DEL FICHERO	
Este fichero y sus datos de carácter personal se encuentran ubicados en el sistema de información en la Avda. Tibidabo, nº. 39-43 (08035 Barcelona, España).	
PROCEDENCIA Y PROCEDIMIENTO DE RECOGIDA	
El sistema de información del proyecto de teleformacion (moodle, aplicación en access para la gestión)	
PROGRAMAS ASOCIADOS AL FICHERO	
El propio interesado o su representante legal, otras personas físicas distintas del afectado o su representante, recogiendo los datos en formularios o entrevistas o cupones o transmisión electrónica de datos. En soporte papel, soporte informático/magnético o via telemática.	

RESPONSABLE DEL FICHERO
Fdo.:

NOMBRE DE FICHERO	Proveedores
DATOS PERSONALES QUE CONTIENE	
De caracter identificativo DNI Nº SS/mutualidad Nombre y apellidos Telefono Dirección **Datos de información comercial** Actividades y negocios	**Datos económico-financieros** Datos bancarios (cuentas)
UBICACIÓN DEL FICHERO	
Este fichero y sus datos de carácter personal se encuentran ubicados en el sistema de información en la Avda. Tibidabo, nº. 39-43 (08035 Barcelona, España).	
PROCEDENCIA Y PROCEDIMIENTO DE RECOGIDA	
El sistema de información del proyecto	
PROGRAMAS ASOCIADOS AL FICHERO	
El propio interesado o su representante legal, o bien de fuentes accesibles al público (listas de personas pertenecientes a grupos profesionales), recogiendo los datos de encuestas, o entrevistas, o en formularios o cupones. En soporte papel, soporte informático/magnético o vía telematica.	

RESPONSABLE DEL FICHERO
Fdo.:

A1.4 RESPONSABLE DE SEGURIDAD Y ADMINISTRADORES DEL SISTEMA

NOMBRE Y APELLIDOS	ID. USUARIO	FECHA DE ALTA	FECHA DE BAJA
José Luis Rivas López	Jlrivas		
FUNCIONES Responsable de seguridad del proyecto LABSEGTEL		**FIRMA**	
NOMBRE Y APELLIDOS Ruben Martin	**ID. USUARIO** martin	**FECHA DE ALTA**	**FECHA DE BAJA**
FUNCIONES Director del proyecto LABSEGTEL		**FIRMA**	
NOMBRE Y APELLIDOS Santiago Perez	**ID. USUARIO** Sperez	**FECHA DE ALTA**	**FECHA DE BAJA**
FUNCIONES Administrador de los sistemas del proyecto LABSEGTEL		**FIRMA**	
NOMBRE Y APELLIDOS	**ID. USUARIO**	**FECHA DE ALTA**	**FECHA DE BAJA**
FUNCIONES		**FIRMA**	
NOMBRE Y APELLIDOS	**ID. USUARIO**	**FECHA DE ALTA**	**FECHA DE BAJA**
FUNCIONES		**FIRMA**	
		RESPONSABLE DEL FICHERO	
		Fdo.:	

A1.5 PERSONAL CON ACCESO A LOS FICHEROS

La lista del personal con acceso a los ficheros esta accesible en el servidor de dominio del proyecto LABSEGTEL. Dicha lista esta en un directorio activo de un Microsoft Windows 2003 Server en el centro de procesos de datos del proyecto LABSEGTEL.

A1.6 REGISTRO DE SOPORTES

IDENTIFICACIÓN DEL SOPORTE Serie:1 Numero: X	**FECHA DE ALTA**	**FECHA DE BAJA**
CONTENIDO DEL SOPORTE Todos los datos de carácter personal que existen en el servidor		**FINALIDAD DEL SOPORTE** Realización de la copia de respaldo diaria de los datos de carácter personal del proyecto LABSEGTEL.
IDENTIFICACIÓN DEL SOPORTE Serie:2 Numero:X	**FECHA DE ALTA**	**FECHA DE BAJA**
CONTENIDO DEL SOPORTE Todos los datos de carácter personal que existen en el servidor		**FINALIDAD DEL SOPORTE** Realización de la copia de respaldo diaria de los datos de carácter personal del proyecto LABSEGTEL.
IDENTIFICACIÓN DEL SOPORTE Serie:3 Numero:Y	**FECHA DE ALTA**	**FECHA DE BAJA**
CONTENIDO DEL SOPORTE Todos los datos de carácter personal que existen en el servidor		**FINALIDAD DEL SOPORTE** Realización de la copia de respaldo semanal (viernes) de los datos de carácter personal del proyecto LABSEGTEL.
IDENTIFICACIÓN DEL SOPORTE Serie:4 Número: Z	**FECHA DE ALTA**	**FECHA DE BAJA**
CONTENIDO DEL SOPORTE Todos los datos de carácter personal que existen en el servidor		**FINALIDAD DEL SOPORTE** Realización de la copia de respaldo mensual (último día de cada mes) de los datos de carácter personal del proyecto LABSEGTEL.
IDENTIFICACIÓN DEL SOPORTE Disaster Recovery Servidor	**FECHA DE ALTA**	**FECHA DE BAJA**
CONTENIDO DEL SOPORTE Contiene una copia tal cual del servidor del proyecto LABSEGTEL.		**FINALIDAD DEL SOPORTE** Recuperar todas las configuraciones del servidor así como su funcionalidad lo antes posible.
		RESPONSABLE DE SEGURIDAD
		Fdo.:

A1.7 PERSONAL CON ACCESO AUTORIZADO A LOS SOPORTES

NOMBRE Y APELLIDOS José Luis Rivas López	**FECHA DE ALTA**	**FECHA DE BAJA**
NIVEL DE ACCESO AUTORIZADO TOTAL		**FUNCIONES PERMITIDAS** TODAS
NOMBRE Y APELLIDOS Rubén Martin	**FECHA DE ALTA**	**FECHA DE BAJA**
NIVEL DE ACCESO AUTORIZADO TOTAL		**FUNCIONES PERMITIDAS** TODAS
NOMBRE Y APELLIDOS Santiago Pérez	**FECHA DE ALTA**	**FECHA DE BAJA**
NIVEL DE ACCESO AUTORIZADO TOTAL		**FUNCIONES PERMITIDAS** TODAS
NOMBRE Y APELLIDOS	**FECHA DE ALTA**	**FECHA DE BAJA**
NIVEL DE ACCESO AUTORIZADO		**FUNCIONES PERMITIDAS**
NOMBRE Y APELLIDOS	**FECHA DE ALTA**	**FECHA DE BAJA**
NIVEL DE ACCESO AUTORIZADO		**FUNCIONES PERMITIDAS**
NOMBRE Y APELLIDOS	**FECHA DE ALTA**	**FECHA DE BAJA**
NIVEL DE ACCESO AUTORIZADO		**FUNCIONES PERMITIDAS**
NOMBRE Y APELLIDOS	**FECHA DE ALTA**	**FECHA DE BAJA**
NIVEL DE ACCESO AUTORIZADO		**FUNCIONES PERMITIDAS**
NOMBRE Y APELLIDOS	**FECHA DE ALTA**	**FECHA DE BAJA**
NIVEL DE ACCESO AUTORIZADO		**FUNCIONES PERMITIDAS**
NOMBRE Y APELLIDOS	**FECHA DE ALTA**	**FECHA DE BAJA**
NIVEL DE ACCESO AUTORIZADO		**FUNCIONES PERMITIDAS**
NOMBRE Y APELLIDOS	**FECHA DE ALTA**	**FECHA DE BAJA**
NIVEL DE ACCESO AUTORIZADO		**FUNCIONES PERMITIDAS**
		RESPONSABLE DEL FICHERO
		Fdo.:

AUTORIZACIÓN PARA LA SALIDA DE SOPORTES

FECHA DE ENTREGA	/ /

En la fecha señalada, se autoriza a Dn./Dña.:..... , para realizar la entrega del Soporte con Datos de Carácter Personal que se describe en el apartado siguiente. Deberá estar correctamente registrada la devolución del citado Soporte, mediante la cumplimentación del apartado correspondiente.

DESCRIPCIÓN DEL SOPORTE Y DEL RECEPTOR	
( ) Tipo de Soporte.	
( ) Finalidad del Soporte	
( ) Precauciones tomadas	
( ) Datos del Receptor / Destinatario	Firma del Receptor Fdo.:
FECHA DE DEVOLUCIÓN	**/ /**

En la fecha arriba señalada, Dn./Dña. ..... realiza la recepción del Soporte con Datos de Carácter Personal que se describe en el apartado anterior.

RESPONSABLE DE LA RECEPCIÓN	RESPONSABLE DEL FICHERO
Fdo.:	**Fdo.:**

A1.8 REGISTRO DE ENTRADA/SALIDA DE SOPORTES

( ) ENTRADA SOPORTE ( ) SALIDA SOPORTE			
FECHA	/ /	**HORA**	

DATOS DEL SOPORTE
( ) Tipo de Soporte. ( ) Fecha de Creación. ( ) Persona que recepciona/realiza el Soporte:

FINALIDAD DEL SOPORTE Y ORIGEN DE LOS DATOS
( ) Finalidad del Soporte.
( ) Origen de los Datos.

FORMA DE ENVÍO DEL SOPORTE
( ) Medio de Envío del Soporte.
( ) Remitente/Destinatario del Soporte.
( ) Precauciones tomadas.
( ) Observaciones

RESPONSABLE DE LA RECEPCIÓN/ENVIO	**RESPONSABLE DEL FICHERO**
Fdo.:	**Fdo.:**

A1.9 VALIDACIÓN Y CONTROL DE ACCESO DE USUARIOS

FECHA	/ /

PROCEDIMIENTO

La validación de los usuarios de los sistemas de información de se realiza a dos niveles:

1).- validación a nivel de sistema operativo: el método de validación de los usuarios son: **nombre de entrada y una contraseña.**

Los usuarios autorizados para efectuar tratamiento de datos, cuando inician una sesión, se validan (mediante nombre de entrada y contraseña) en un dominio de sistema operativo servidor windows: *2003 server*.

FORMATO DEL NOMBRE DE ENTRADA:
identificador específico para cada usuario (primera letra del nombre y el apellido).
FORMATO DE LA CONTRASEÑA:
contraseña formada por un conjuto de caracteres alfanuméricos (máximo de 8 caracteres). No se admiten contraseñas en blanco.
MODIFICACIONES EN EL NOMBRE DE ENTRADA Y LA CONTRASEÑA:
Se establece un período de validez para las contraseñas de dos meses.

2).- validación a nivel de aplicaciones informáticas que realizan tratamiento de datos el método de validación de los usuarios son: **identificación de usuarios a través de un nombre de entrada**

el ***supervisor*** del entorno de trabajo de cada una de las aplicaciones es quien define los diferentes usuarios de las mismas, habilitando los permisos asociados a cada uno de los usuarios.

El control de acceso de los usuarios de los sistemas de información se realiza tambien en dos niveles:

1).- control de sacceso a nivel de sistema operativo: el método de validación de los usuarios son: **control de acceso a los recursos mediante listas de control de acceso.**

Los usuarios autorizados para efectuar tratamiento de datos, cuando inician una sesión de trabajo, heredan los permisos de acceso a los recursos que les hayan sido asignados.

GRUPOS DE USUARIOS:
No se realiza clasificación de usuarios autorizados en grupos de usuarios. La asignación de permisos de acceso se realiza de forma individual para cada usuario, ya que sus tareas no permiten el agrupamiento de los mismos.
ACCESO A RECURSOS:
Cada usuario tiene acceso a todos los recursos locales del equipo informático que utiliza para su trabajo. además, dispone de permisos de acceso a los recursos compartidos del servidor que les hayan sido asignados. Existen carpetas compartidas en diferentes equipos informáticos de los sistemas de información.
ADMINISTRADORES DEL SISTEMA:
Solamente dispone de privilegios de administrador aquel usuario habilitado para ello.

2).- control de acceso a nivel de aplicaciones informáticas que realizan tratamiento de datos: el método de control de acceso de los usuarios son: **control de acceso a través de un nombre de entrada.**

El ***supervisor*** del entorno de trabajo de las aplicaciones que realizan tratamiento de datos personales es quien define los diferentes usuarios de las mismas, habilitando los permisos asociados a cada uno de los usuarios. Los diferentes usuarios de las aplicaicones de tratamiento de datos personales podrán acceder a aquellas utilidades de dichas aplicaciones que les hayan sido activadas por el supervisor.

RESPONSABLE DE SEGURIDAD	RESPONSABLE DEL FICHERO
Fdo.:	**Fdo.:**

A1.10 AUTORIZACIÓN PARA LA RECUPERACIÓN DE ARCHIVOS

FECHA	/ /

Se autoriza a Dn./Dña. ..... , para realizar el/los Procedimiento/s de Recuperación, descrito/s en el Documento de Seguridad sobre Datos de Carácter Personal correspondientes a los siguientes archivos :

MOTIVO PARA APLICAR EL PROCEDIMIENTO DE RECUPERACIÓN

DESCRIPCIÓN DE LOS SOPORTES DE RECUPERACIÓN

( ) Etiqueta de Identificación.

( ) Tipo de Soporte.

( ) Fecha y Hora de Creación del Soporte.

( ) Mecanismo y/o Procedimiento de Creación.

RESPONSABLE DEL FICHERO

Fdo.:

A1.11 REGISTRO Y SOLUCIÓN DE INCIDENCIAS

FECHA	/ /	**NÚMERO DE INCICENCIA**	
HORA		**USUARIO QUE NOTIFICA**	

RECEPTOR DE LA NOTIFICACIÓN	

DESCRIPCIÓN DE LA INCIDENCIA

Tipo de Incidencia

( ) Intrusión ( ) Pérdida de datos

( ) Otro tipo de incidencia (especificar)

Descripción detallada de la Incidencia

Efectos detectados en el Sistema

NOTIFICANTE	**RESPONSABLE DE SEGURIDAD**
Fdo.:	**Fdo.:**

FECHA	/ /	NÚMERO DE INCICENCIA	

RESPONSABLE DE LA RESOLUCIÓN	

RESOLUCIÓN DE LA INCIDENCIA
Medidas adoptadas y pasos realizados

RESPONSABLE DE LA RESOLUCIÓN	RESPONSABLE DE SEGURIDAD
Fdo.:	Fdo.: