

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

CONSULTOR:
Manel Llopart

AUTOR:
José Luis Rivas

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

INDICE

 UOC

www.uoc.edu

www.uoc.edu

- Objetivos del TFG
- Metodología seguida en el TFC
- Introducción LOPD
- Ficheros detectados en el curso
- Creación de la asignatura de formación
- Conclusiones

OBJETIVO DEL TFG



- 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 explicarar 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 en el sistema y su nivel (bajo, medio o alto)
 - ❖ Realización del documento de seguridad marcado por el RMS
 - ❖ Montar una asignatura donde se explique como acometer dicha problematica para futuros alumnos

METODOLOGIA SEGUIDA EN EL TFG



- La metodología utilizada en este trabajo fin de grado se fundamenta en cuatro fases fundamentales:
 - 1) Analisis 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.

Parte 1: Estudio de la Ley Orgánica de Protección de Datos y su RMS



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

INTRODUCCIÓN

¿QUÉ ES LA LOPD?

UOC

www.uoc.edu

www.uoc.edu

- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal
- Pretende establecer un control sobre quién tiene dichos datos, para qué los usa y a quién se los cede.

INTRODUCCIÓN

¿POR QUÉ SURGIÓ?

- Para proteger los derechos fundamentales del individuo (honor, a la intimidad personal y familiar y a la propia imagen).
- La enorme capacidad de tratamiento de la información que ofrecen las nuevas tecnologías.

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

INTRODUCCIÓN

NIVELES DE PROTECCIÓN

UOC

www.uoc.edu

www.uoc.edu

NIVEL ALTO

NIVEL MEDIO

NIVEL BÁSICO

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

FICHEROS DETECTADOS EN EL SISTEMA DE TELEFORMACIÓN

UOC

www.uoc.edu

www.uoc.edu

Nombre Fichero	Nivel	Finalidad
Logs del sistema	Bajo	Logs creados por el sistema
Agenda del proyecto	Bajo	Gestión de la agenda de los miembros del sistema
Personal docente	Bajo	Gestión y control del personal docente
Usuarios	Bajo	Gestión y control del personal usuarios del sistema
Proveedores	Bajo	Seguimiento y control de las empresas suministradoras

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

LAS MEDIDAS DE SEGURIDAD APLICADAS EN EL SISTEMA DE TELEFORMACIÓN

 UOC

www.uoc.edu

www.uoc.edu

Reglamento de Desarrollo de la LOPD

NIVEL BÁSICO

UOC

www.uoc.edu

www.uoc.edu

- Aplicable a todos los sistemas con ***datos personales*** en general.
- Según el artículo 3, apartado a), de la LOPD, se definen como “cualquier información concerniente a personas físicas identificadas o identificables”

NIVEL BÁSICO

IDENTIFICACIÓN Y AUTENTIFICACIÓN



- Cuando el mecanismo de autenticación se base en la existencia de contraseñas existirá un procedimiento de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad
- Por tanto, la mejor opción es el cifrado de dichos datos (contraseñas).
- El *responsable del fichero* es el encargado de mantener actualizada la lista de los usuarios autorizados y diseñar su procedimiento de acceso.
- Las claves son cambiadas con la periodicidad que determine el documento de seguridad. En el sistema lo hacen cada par de meses.
- No hay nada escrito en el reglamento de cómo debe ser las contraseñas aunque en el sistema las contraseñas están formadas por un conjunto de caracteres alfanuméricos. No admitiendo contraseñas en blanco

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

NIVEL BÁSICO

CONTROL DE ACCESO

 UOC

- Los usuarios tendrán acceso únicamente a aquellos datos y recursos que precisen para el desarrollo de sus funciones
- Para que sea más sencillo su administración y control se dividen en grupos de trabajo: administradores, director del proyecto, investigadores, becarios, administrativos.

NIVEL BÁSICO

COPIAS DE SEGURIDAD



- Deberán realizarse copias de respaldo, al menos semanalmente, salvo que en dicho período no se hubiera producido ninguna actualización de los datos
- Los procedimientos establecidos para la realización de copias de respaldo y para la recuperación de los datos deberá garantizar su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción
- En el sistema realizan la siguiente método.
 - ❖ **DIARIA** : La Copia de Seguridad Completa Diaria se efectuará en cinta DDS5, 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.
 - ❖ **SEMANAL**: La Copia de Seguridad Completa Semanal se efectuará en cinta DDS5, 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.
 - ❖ **MENSUAL**: La Copia de Seguridad Completa Mensual se efectuará en cinta DDS5, 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.
- Cuando en el sistema reutiliza o desecha alguna de las cinta adoptan las medidas para evitar la recuperación posterior de la información personal. Para ello usan la opción recycled de la aplicación para la realización de las copias de seguridad.

Parte 2: Creación y Diseño de una Asignatura de LOPD



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

ASIGNATURA PROPUESTA (I)

UOC

www.uoc.edu

www.uoc.edu

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

ASIGNATURA PROPUESTA (II)

UOC

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 o pregunta de desarrollo

ARQUITECTURA PROPUESTA



La arquitectura del sistema propuesto escogida será una arquitectura web (MVC) de 3 capas. 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

ALCANCE FUNCIONAL



www.uoc.edu

www.uoc.edu

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.

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

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

REQUISITOS NO FUNCIONALES

UOC

www.uoc.edu

www.uoc.edu

- Requisitos de seguridad
- Requisitos de interfaz de usuario, usabilidad y accesibilidad
- Requisitos de rendimiento

BATERIA DE PRUEBAS



www.uoc.edu

www.uoc.edu

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.

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

INTERFAZ DE USUARIO

The screenshot displays a Moodle course interface. On the left is a navigation menu with sections like PEOPLE, ACTIVITIES, SEARCH FORUMS, and ADMINISTRATION. The main content area is titled 'WEEKLY OUTLINE' and shows a 'NEWS FORUM' with a post from June 21-27 about 'Fundamentos a la Privacidad'. Below this is a 'TEXTOS DE ESTUDIO' section with three items: 'EXAMEN SEMANA 1', 'EXAMEN SEMANA 2', and 'EXAMEN SEMANA 3'. A document viewer is open, showing a document titled 'formacion.laboratoriodeseguridaddelematica.com/mod/resource/view.php?popup=true&id=12'. The document text discusses the origin of national normative, the impact of ICTs, and the implementation of the LOPD. It mentions that the LOPD is very similar to the LORTAD and that the new LOPD extends to various data formats. The document also lists differences between the LORTAD and the new LOPD, such as the inclusion of the 'Encargado del Tratamiento' and the 'Responsable del Fichero'. The interface includes a 'LATEST NEWS' section with no news, an 'UPCOMING EVENTS' section with 'Examen final' and 'Examen semana 2', and a 'GO TO NEW EVENT' section. At the bottom right, there is an 'Update this Assignment' button and a message: 'No attempts have been made on this assignment'.

NOTAS:

- 1) NO SUPONGA NADA QUE NO ESTE ESCRITO POR TANTO CONTEMPLA 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

CONCLUSIONES



- 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.
- 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.
- 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.
- 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.
- 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.

LINEAS FUTURAS

- 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.