

© Darío Álvarez 2005-2008

Introducción a la LOPD y al Reglamento de Medidas de Seguridad

*Aspectos Sociales, Legales, Éticos y Profesionales
de la Informática (ASLEPI)*

Escuela Universitaria de Ingeniería Técnica en Informática de Oviedo

Darío Álvarez Gutiérrez

© Darío Álvarez 2005-2008

Introducción a la Ley Orgánica de Protección de Datos

© Darío Álvarez 2005-2008

Normativa aplicable y conceptos fundamentales

- Ley Orgánica de Protección de Datos Personales (LOPD) 1999 - LORTAD 1992
- Reglamento de Medidas de Seguridad
- Datos personales
- Fichero de Datos
- Responsable del Tratamiento / Fichero
- Tratamiento de datos y encargado del tratamiento

Principios de la LOPD

- Necesidad de consentimiento del afectado
- Calidad de los datos
- Deber de información
- Derecho de:
 - Acceso
 - Rectificación y cancelación
 - Oposición
- Deber de secreto
- Prohibición cesión de datos sin consentimiento

Datos especialmente protegidos

- Afiliación sindical, ideología, religión, creencias
- Salud, origen racial, vida sexual

Otros aspectos

- La Agencia de Protección de Datos (APD)
 - Instrucciones, informes sectoriales, etc.
- Necesidad de inscribir los ficheros en la Agencia de Protección de Datos
- Sanciones
 - Leves (de 601 a 60.101 €)
 - No solicitar la inscripción, ...
 - Graves (de 60.101 a 300.506 €)
 - No cumplir el reglamento de medidas de seguridad, ...
 - Muy Graves (300.506 - 601.012 €)
 - Cesión de datos no permitida, ...

Introducción al Reglamento de Medidas de Seguridad

de los ficheros automatizados que contengan datos de carácter personal

(ojo, DEROGADO por el R.D 1720/2007

Reglamento Desarrollo LOPD Medidas de Seguridad)

© Dario Álvarez 2005-2008

Contexto

- LORTAD 1992
- Reglamento de Medidas de Seguridad 1999
- LOPD 1999
 - Pone expresamente en vigor el RMS
 - RMS desarrolla el artículo 9

© Dario Álvarez 2005-2008

¿Qué es?

- Conjunto de buenas prácticas de administración de sistemas informáticos
 - Medidas de seguridad conducentes a mantener:
 - Confidencialidad
 - Integridad
 - Disponibilidad
- de los datos personales almacenados en sistemas informáticos para cumplir los fines para los que fueron recabados

© Dario Álvarez 2005-2008

Niveles de seguridad de datos

- Medidas se incrementan según naturaleza datos
- Nivel básico (todos los casos)
- Nivel medio
 - Servicios financieros y Hacienda Pública
 - Infracciones administrativas y penales
- Nivel alto
 - Ideología, religión, creencias
 - Origen racial, salud, vida sexual
 - Fines policiales recabados sin consentimiento

© Darío Álvarez 2005-2008

Medidas Organizativas (Resumen - 1)

- Documento de Seguridad
 - Normas y procedimientos de seguridad
 - Funciones y obligaciones del personal
 - Descripción del sistema de información y los ficheros de datos
 - Relación de usuarios autorizados
- Auditoría bianual
 - Realizada por un experto en informática
 - Queda a disposición de la Agencia de PD
- Responsable de seguridad

© Darío Álvarez 2005-2008

Medidas Organizativas (Resumen - 2)

- Registro de incidencias
- Registro de Entrada/Salida de soportes
- Gestión de Soportes
- Autorizaciones responsable del fichero
 - Tratamiento fuera de los locales, etc.

© Darío Álvarez 2005-2008

Medidas Técnicas (Resumen - 1)

- Identificación y autenticación
 - Contraseñas almacenadas de forma cifrada
 - Cambio periódico de contraseñas
- Control de acceso lógico a los recursos
- Control de acceso físico
- Pruebas con datos ficticios
- Control de ficheros temporales
- Accesos remotos con seguridad equivalente al acceso local

© Darío Álvarez 2005-2008

Medidas Técnicas (Resumen - 2)

- Control de la reutilización y acceso a los soportes de datos
- Cifrado de datos de nivel alto en telecomunicaciones
- Registro de todos los accesos a datos de nivel alto
- Almacenamiento de copias de datos de nivel alto en segunda ubicación

© Darío Álvarez 2005-2008

¿Por qué aplicarlo?

- Obligación ética y legal
- Reducción del riesgo en la empresa
 - Sanciones (infracción grave entre 60.000 y 300.000 euros)
 - Riesgo informático
- Mejora de la organización y funcionamiento del sistema informático

© Darío Álvarez 2005-2008

Equivocaciones comunes

- Aplicar el RMS garantiza que sea imposible la aparición de problemas (filtraciones de datos, pérdida de datos, etc.) - NO
 - Esto es imposible de garantizar
 - Sí permite reducir el riesgo de que aparezcan problemas y permite trazarlos si aparecen
- La auditoría bianual tiene que pasarse "limpia" - NO
 - El objetivo de las auditorías es precisamente encontrar los problemas
 - La entidad debe tomar las medidas adecuadas para corregir los problemas detectados

Formación de usuarios finales

- Es imprescindible poner en marcha las medidas técnicas y legales, pero no se debe parar aquí
- De la correcta operativa de los usuarios finales depende gran parte del éxito de la implantación de la protección de datos
 - Aplicación de medidas de seguridad en la operativa diaria
 - Es necesaria formación en materia de medidas de seguridad para la protección de datos para los usuarios finales
 - Presencial / A distancia

Pilares del comportamiento de los usuarios finales

- Concienciación sobre la importancia de la protección de datos personales
- Sentido común
- Preguntar a un responsable en caso de duda
- Formación en técnicas concretas

Introducción al Reglamento Desarrollo LOPD Medidas de Seguridad Reglamento de Medidas de Seguridad (R.D 1720/2007)

© Dario Álvarez 2005-2008

Novedades principales del nuevo Reglamento

- Aplicación a ficheros y tratamientos no automatizados ("papel")
- Aclaraciones y concreciones en la aplicación de la LOPD y las medidas de seguridad
 - Jurisprudencia, resoluciones AGPD, concreciones
 - Ej: nivel básico para ficheros de nóminas

© Dario Álvarez 2005-2008

Novedades principales del nuevo Reglamento

- Apartados adicionales a medidas de seguridad
 - Disposiciones generales (título I)
 - Principios de protección de datos (título II)
 - Derechos (título III)
 - Ficheros específicos (título IV)
 - Creación y notificación de ficheros (título V)
 - Transferencias internacionales (título VI)
 - Códigos tipo (título VII)
 - *Medidas de seguridad (título VIII)*
 - Procedimientos de la AGPD (título IX)
- Productos Software: indicación nivel seguridad

© Dario Álvarez 2005-2008

Novedades principales del nuevo Reglamento (medidas seguridad)

- Retoques en medidas de seguridad (niveles, nuevas medidas)
 - Ej: Etiquetado "codificado" de soportes con datos sensibles
 - Ej: Desaparición cuentas "genéricas" (identificación unívoca en todos los niveles).
 - Ej: Agrupación en un único Documento de Seguridad de varios ficheros (por Sistema de Información, medidas equivalentes, etc.)
