IX Congreso de Ingeniería de Organización
Gijón, 8 y 9 de septiembre de 2005

Auditoría y propuesta de medidas correctoras para el cumplimiento de la Ley Orgánica de Protección de Datos (LOPD) en una empresa aseguradora

Manuel Expósito Langa[1], Yolanda Cascant Catalá[2], Josep Capó Vicedo[1], José Vicente Tomás Miquel[1]

[1] Departamento de Organización de Empresas. Universidad Politécnica de Valencia. Plaza Ferrándiz y Carbonell, 2. 03801 Alcoy (Alicante). maexlan@omp.upv.es, pepcapo@omp.upv.es, jotomi@doctor.upv.es
[2] Licenciatura en Administración y Dirección de Empresas. Universidad Politécnica de Valencia. Plaza Ferrándiz y Carbonell, 2. 03801 Alcoy (Alicante). yocasca@epsa.upv.es

Resumen

El objeto del presente trabajo consiste en determinar la importancia que la Ley Orgánica de Protección de Datos (LOPD) tiene en la actualidad y la progresiva aplicación de ésta en las organizaciones. De esta forma, se analizan cuestiones relacionadas con la seguridad y protección de datos de carácter personal con el fin de garantizar la integridad y la privacidad de los ciudadanos. Como aplicación, se ha llevado a cabo un proceso de auditoría interna sobre el nivel de cumplimiento de los niveles exigibles por la LOPD en una empresa aseguradora. Este proceso ha permitido la obtención de datos sobre el conocimiento y la forma de aplicación de la ley que está llevando a cabo la empresa.

Palabras clave: Auditoría, LOPD, Integridad de datos, Responsable de seguridad, Reglamento de medidas de seguridad, Agencia protección de Datos (APD)

1. Introducción

En la actualidad, por pequeña o grande que sea una empresa, cuenta con ficheros donde maneja información sobre sus empleados, clientes, proveedores, etc. Por otra parte, el artículo 18.4 de la Constitución Española señala lo siguiente:

> *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.*

Con el punto de partida anterior, el 11 de junio de 1999 se aprobó el RD 994/1999 donde aparece el Reglamento de medidas de seguridad de los ficheros automatizados que contienen datos de carácter personal que junto con otras disposiciones han dado lugar más tarde al desarrollo de la Ley Orgánica 15/1999 de Protección de Datos (LOPD). Esta ley, afecta en su conjunto a todas las empresas que manejan ficheros con referencias a datos personales, en cualquier soporte físico y automatizados o no, susceptibles del tratamiento o uso posterior.

La LOPD ha permitido abordar el problema del aumento en el tratamiento masivo de datos de carácter personal y la propia intimidad de las personas, ya que hasta el momento en que apareció la ley, el uso de dichos datos era absolutamente libre y en ocasiones totalmente abusivo y sin el consentimiento, e incluso conocimiento de sus propietarios. Por tanto, se hacía evidente definir con urgencia un marco legal que regulara y permitiera la convivencia

entre los intereses comerciales o simplemente organizativos de las entidades que utilizaban dichos datos y los intereses y derechos de los propietarios de los mismos.

De esta manera, la ley obliga a las empresas a registrar la estructura de sus ficheros en la Agencia de Protección de Datos (http://www.agpd.es) y establecer una política de seguridad interna en el denominado Documento de Seguridad, así como tomar las medidas técnicas necesarias para garantizar el nivel de protección adecuado de dichos datos.

Sin embargo, esta circunstancia, que resulta de obligado cumplimiento desde el año 2002, bien debido a la falta de concienciación de las organizaciones, bien debido a las pocas medidas de control y penalización tomadas por la Agencia, no ha sido tomada con la suficiente atención por parte de las empresas.

De esta forma, el presente trabajo lleva a cabo una auditoría sobre el nivel de desempeño de la ley en una empresa aseguradora, donde como se verá más adelante el nivel de medidas de seguridad que debe cubrir es el más alto de los que exige la ley en algunos de sus ficheros internos.

2. Situación actual de la ley

Para Del Peso (2000), la seguridad adquiere en el contexto de las redes sin fronteras una nueva y esencial dimensión desde el momento mismo en que se multiplican los riesgos, como es el caso de situaciones donde aparecen filtrado y fuga de datos en las corporaciones. De esta forma, un dato de carácter personal sólo podrá ser tratado por una organización si dispone del consentimiento de su propietario (el afectado) y además deberá hacerlo en unas determinadas condiciones que garanticen la confidencialidad y seguridad del mismo, así como que le está dando el uso estrictamente consentido por la persona implicada.

De esta forma, no se trata simplemente de asegurar que los tratamientos automatizados de una máquina se efectúan correctamente, es decir, de manera fiable, sino que es necesario tratar de asegurar que a través de las redes que cubren el mundo entero, ninguna información se pierda de forma voluntaria o fortuita en dirección a terceros no autorizados, así como que no se convierta en inaccesible para sus legítimos poseedores o sea modificada sin su consentimiento.

La aprobación del Reglamento de Medidas de Seguridad de los Ficheros Automatizados que contienen Datos de Carácter Personal puede suponer una concienciación de la sociedad sobre la necesidad de disponer de una información veraz y segura, más aun con las importantes iniciativas en comercio electrónico, principalmente a través de Internet, a las que estamos cada día más habituados.

2.1. Comparación entre la LORTAD y la LOPD

El 14 de enero de 2000 entró en vigor en España de forma definitiva la Ley Orgánica 15/1999 de 13 diciembre de Protección de Datos de Carácter Personal (LOPD) que derogó la Ley Orgánica 5/1992 de 29 de octubre de regulación del tratamiento automatizado de los datos de carácter personal (conocida como LORTAD) y vigente en nuestro país hasta esa fecha.

La aprobación de dicha ley volvió a plantear el debate sobre cuál debía ser el punto de equilibrio entre la protección de la privacidad de los ciudadanos y los legítimos intereses de todos aquellos que precisan datos de carácter personal para el desarrollo de sus actividades.

Si bien existen pequeñas diferencias entre la antigua LORTAD y la actual LOPD, la más importante es que en el nuevo texto el objeto es mucho más amplio, ya que se refiere al tratamiento de datos personales en general y no sólo a los automatizados. De esta forma, la palabra "automatizados" desaparece en casi todos los artículos de la actual ley.

Sin embargo, esto puede acarrear problemas en la interpretación, debido a que la LORTAD sigue sobreviviendo en la actual en un gran número de artículos. Así, si la LORTAD fue creada para frenar el mal uso de las tecnologías de la información, que con su rápido avance técnico propiciaban la construcción de grandes bases de datos y su transmisión poniendo en peligro la intimidad de los ciudadanos, la LOPD ha ampliado el rango de aplicación haciendo más ardua su aplicación.

En cuanto a la cuantía de las sanciones, éstas no han sufrido ninguna variación, pero sí que aparecen cambios en lo referente a la graduación de éstas, así, además de los casos que figuraban en la LORTAD, la LOPD también responde a los siguientes:

- Daños y perjuicios causados a las personas interesadas
- Daños y perjuicios causados a terceras personas
- Cualquier otra circunstancia que sea relevante para determinar el grado de antijuricidad y de culpabilidad

2.2. El Reglamento de Medidas de Seguridad

Adicionalmente a la publicación de la LOPD aparece el Reglamento de Medidas de Seguridad de los Ficheros Automatizados que Contienen Datos de Carácter Personal. Este Reglamento, tal y como se deduce por su título, se centra en establecer las medidas de seguridad de cada uno de los niveles de seguridad de la ley en lo que a los ficheros electrónicos, redes de comunicación, y tratamiento informatizado de los datos se refiere. Por tanto, dependiendo de su naturaleza y del grado de necesidad de garantía de su confidencialidad e integridad, las medidas de seguridad se clasifican en tres niveles:

- Nivel básico: corresponde a todos los ficheros que contienen datos de carácter personal
- Nivel medio: se mantienen a este nivel de seguridad los ficheros que contienen datos relativos a comisión de infracciones administrativas o penales, Hacienda Pública, servicios financieros y solvencia patrimonial y crédito
- Nivel alto: se protege mediante este nivel a los ficheros que contienen datos sobre ideología, religión, creencias, origen racial, salud, vida sexual y aquellos recabados para fines policiales sin consentimiento de las personas afectadas

2.3 Descripción de los niveles de infracción en el cumplimiento de la LOPD

Como se observa, la LOPD tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar. De esta forma, establece un régimen sancionador al que se encuentran sujetos tanto los responsables de los ficheros como los encargados de los tratamientos. Este régimen fija tres niveles de infracción, clasificados en leves, graves y muy graves y citados en el punto anterior. Así, se consideran las siguientes infracciones entre las más destacables:

- Infracciones leves: no atender solicitudes de rectificación o cancelación de datos personales de nivel bajo, no inscribir los ficheros en la Agencia de Protección de Datos o recopilar datos sin autorización de los implicados o incumplir el derecho de secreto.

- Infracciones graves: utilizar datos personales con finalidades distintas a las que los originaron, recabar datos sin consentimiento, la negativa a facilitar información, mantener datos no exactos, no mantener las debidas medidas de seguridad u obstruir la función inspectora.

- Infracciones muy graves: la recogida de datos de forma engañosa y fraudulenta, la cesión de datos personales sin autorización, el tratamiento ilegítimo de datos o con menosprecio de los derechos fundamentales de las personas o no atender el deber legal de notificar datos de nivel alto.

Por tanto, aquellas entidades responsables de ficheros con datos personales están sujetas al régimen sancionador de la ley, cuyos niveles de infracciones se califican a su vez en:

- Leves, con sanciones de 600€ a 60.000€

- Graves, de 60.000€ a 300.000€

- Muy graves, de 300.000€ a 6.000.000€

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

2.4. Medidas de seguridad a adoptar

El Documento de Seguridad es un documento que debe ser elaborado por una persona designada como responsable y contiene la normativa de seguridad, cuyo cumplimiento es obligatorio para todo el personal con acceso a datos de carácter personal y a los sistemas de información. Su contenido se centra básicamente en los siguientes puntos:

- Ámbito de aplicación (por ejemplo, bases de datos en donde se encuentra la información)

- Política de seguridad
- Funciones y obligaciones del personal
- Estructura de los ficheros y descripción de los sistemas de información que los tratan
- Procedimientos de notificación, gestión y respuesta de las incidencias
- Procedimientos de realización de copias de respaldo

El responsable del fichero debe dar a conocer al personal con permisos de acceso las normas de seguridad que afectan al desarrollo de sus funciones así como las consecuencias de su incumplimiento. El nivel de seguridad establecido para los datos, indicará las medidas que deberá adoptar para el debido cumplimiento de la ley. De esta forma, se destacan algunas de las más importantes:

- A nivel básico, deberá existir un mecanismo de autentificación de usuarios mediante contraseña personal, así como una relación actualizada de éstos con sus derechos de acceso, un inventario de soportes con datos de carácter personal y un almacén restringido donde estarán las copias de seguridad
- A nivel medio, además de las anteriores, la empresa será auditada cada dos años en materia de seguridad informática, tendrá establecido un procedimiento de desechado y reutilización de soportes, limitará el número de intentos de acceso no autorizados, limitará el acceso físico a sus servidores, establecerá un sistema de registro de entrada y salida de soportes informáticos y no realizará pruebas en sus sistemas con juegos de datos reales
- A nivel alto, además de las anteriores, la distribución de soportes así como la transmisión de datos se realizará mediante el cifrado previo de los mismos u otro mecanismo que garantice que sean ininteligibles, establecerá un control (usuario, fecha y hora de acceso, operaciones realizadas) de los accesos a los soportes con datos de nivel alto y mantendrá dichos registros durante al menos 2 años, por otra parte deberá almacenar las copias de seguridad en un lugar distinto de donde están sus instalaciones

3. Descripción de la empresa objeto de estudio

La Unión Alcoyana (http://www.unionalcoyana.com), ubicada en la localidad de Alcoy (Alicante), representa una sociedad anónima de seguros y reaseguros constituida el 25 de julio de 1877 y sujeta a la ley 30/1995 de 8 de noviembre de Ordenación y Supervisión de Seguros Privados y demás disposiciones vigentes.

La empresa nació con el objeto de asegurar contra incendios involuntarios a “prima fija” fincas rústicas y urbanas, así como edificios industriales y los géneros, máquinas y muebles contenidos y todos los objetos que se consideraran admisibles con arreglo a sus estatutos. En la actualidad opera en los ramos de No Vida enfocándose principalmente en tres áreas:

- Riesgos industriales
- Protección patrimonial

- Riesgos patrimoniales

A continuación se muestra las distintas áreas de trabajo de la empresa.

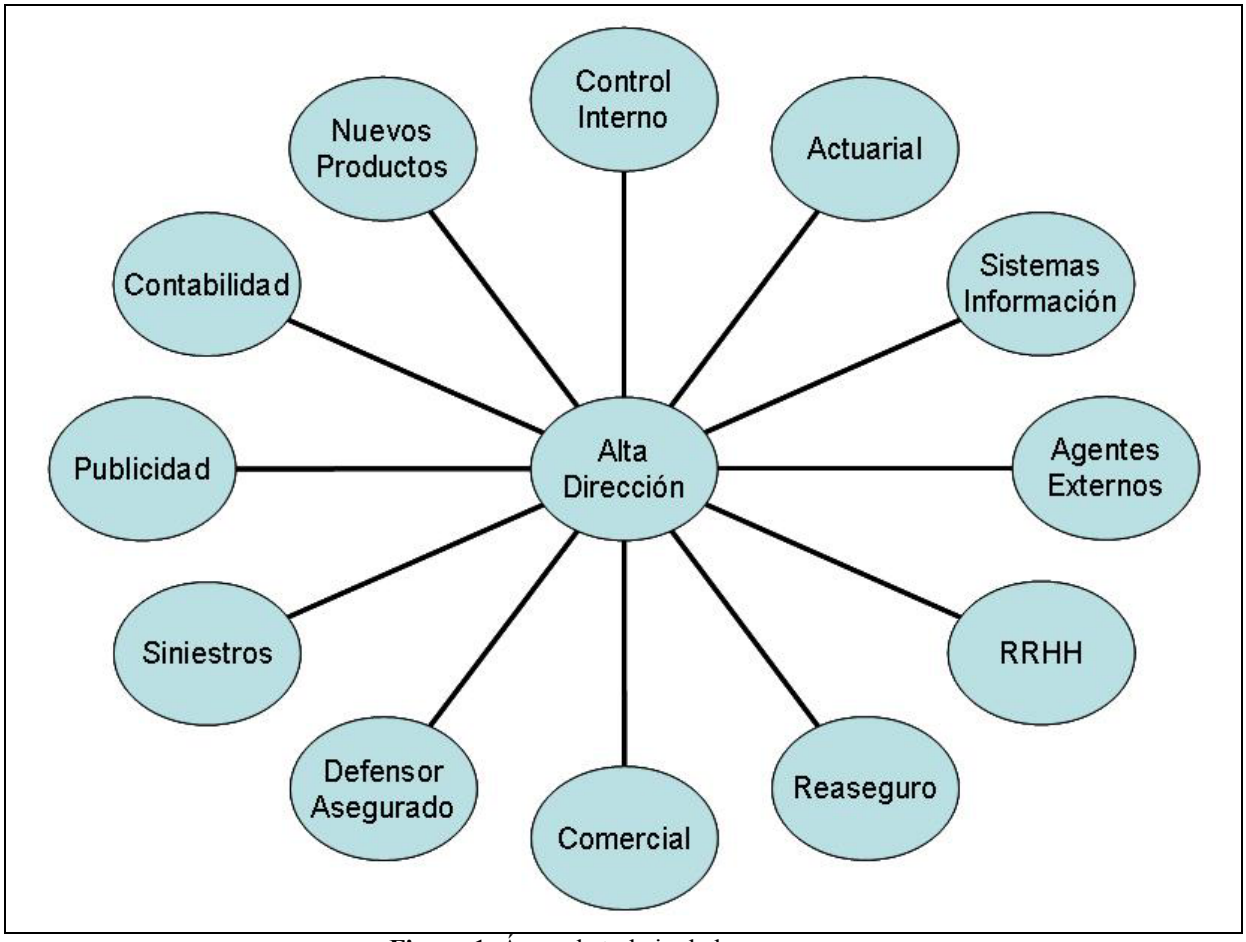

Figura 1: Áreas de trabajo de la empresa

Debido al tipo específico de servicio que ofrece, la mayoría de datos que maneja pertenecen al nivel básico o medio, sin embargo en determinados seguros o en el caso de siniestros con parte médico almacenará información de nivel alto. Esto le obligaría a cumplir para dichos ficheros las medidas de nivel alto que establece el Reglamento de Seguridad.

4. Metodología de trabajo

Para llevar a cabo el análisis del cumplimiento de la LOPD en la empresa se ha llevado a cabo un proceso de auditoría interno basado en la realización de diversos cuestionarios que han permitido la identificación de aquellos ficheros susceptibles del tratamiento de seguridad así como su nivel de seguridad necesario y el aplicado en la actualidad.

El cuestionario ha estado formado por un total de 37 preguntas cerradas relacionadas con las exigencias de los diferentes artículos de la ley. Cabe señalar que se han realizado a personal de los distintos departamentos de la organización y no sólo al personal informático, cumpliendo un planning acordado con la dirección de la empresa. De esta forma se ha intentado captar los distintos flujos de datos de carácter personal de forma independiente al tratamiento automático que tengan.

El proceso ha permitido generar un diagnóstico de la situación de la empresa con relación a la normativa que ha dado lugar a un informe final con una lista de factores críticos junto a las fortalezas y debilidades de la empresa con respecto a la ley.

5. Principales resultados obtenidos

Tras el análisis de las respuestas de los cuestionarios se ha podido observar que la entidad tiene un alto conocimiento de la ley, sin embargo, ésta no ha sido implantada todavía en su totalidad. A continuación se muestra dos tablas resumen donde se refleja qué ficheros son susceptibles de tratamiento y qué medidas de seguridad están siendo aplicadas en la actualidad en la empresa.

Tabla 1: Ficheros comunicados a la APD

Tipo fichero	Datos que contiene	Nivel de seguridad
Empleados	Personales, Económicos	Nivel medio
Empresas clientes	Responsabilidad civil	Nivel medio
Clientes particulares	Datos personales	Nivel bajo
Siniestros	Siniestros con personas heridas	Nivel alto
Comunidades de vecinos	Datos personales	Nivel bajo
Asociaciones deportivas y festeras	Datos personales	Nivel bajo
Agentes, mediadores y corredores	Datos personales	Nivel bajo

Tabla 2: Aplicación de medidas de la LOPD

	Nivel Bajo	Nivel Medio	Nivel Alto
Existe documento escrito con las normas de seguridad	Sí	--	--
Existe normativa interna con las obligaciones de los trabajadores	Sí	--	--
Existe plan de seguridad informática	Sí	--	--
Comunicación APD de ficheros con datos personales	Sí	--	--
Procedimiento realización copias de seguridad	Sí	--	--
Identificación de usuarios con acceso al sistema	Sí	--	--
Cambio de contraseñas de usuarios	Sí	--	--

Existe un responsable de seguridad de los datos	No	--	--
Documento de seguridad establece controles para verificar la LOPD	--	No	--
Documento de seguridad describe las medidas para desechar soporte informático	--	No	--
Existen medidas de control físico a los locales con sistemas de información	--	No	--
Sistema de registro de entradas y salidas de soportes informáticos	--	No	--
Limitación de acceso no autorizado indefinidamente	--	No	--
Distribución de soportes con datos personales son cifrados	--	--	No
Registro de usuarios a ficheros personales con fecha, hora, nombre usuario.	--	--	No
Responsable de seguridad controla los mecanismos de registro de datos	--	--	No
Conserva backups al menos dos años	--	--	Sí
Responsable de seguridad elabora informes sobre la revisión de contraseñas	--	--	No
Se conserva copia de seguridad en un lugar distinto de los sistemas de información	--	--	Sí
Existe cifrado de datos entre redes de comunicación (correo electrónico, intranet)	--	--	Sí

6. Conclusiones y propuestas de mejora

Como se observa en las tablas de resultados, si bien la entidad tiene establecidas medidas de seguridad para la protección de datos de carácter personal como la existencia de un documento escrito con las normas de seguridad informática, una normativa interna en la que se especifican las obligaciones de los trabajadores con respecto al uso de sistemas informáticos o realización de copias de seguridad, todavía le quedan medidas importantes por establecer. A continuación se muestra cuáles son sus principales fortalezas y debilidades de cara a establecer un plan de acción.

Fortalezas:

- La empresa está concienciada acerca de la necesidad de cumplir la ley vigente
- La empresa cuenta con un departamento de sistemas de información propio
- Ha empezado a tomar medidas y ha comunicado a la AGP los ficheros con datos de carácter personal

- Las medidas de nivel básico están prácticamente cubiertas y cumple algunas medidas de nivel alto
- Todo usuario que accede al sistema está correctamente identificado
- La empresa posee un proceso sistémico de realización de copias de seguridad
- Las contraseñas de los usuarios se cambian con periodicidad
- Las contraseñas se almacenan de forma cifrada para que personas ajenas a los distintos departamentos de la empresa no puedan acceder al sistema
- Los datos registrados se conservan durante más de dos años

Debilidades:

- No tiene definido de forma explícita un responsable de seguridad, se considera en general al departamento de sistemas de información
- La empresa debe establecer un control de entradas y salidas de soportes informáticos
- Debe establecer en sus aplicaciones un límite de accesos no autorizado
- Es necesario establecer un sistema de cifrado de datos para las comunicaciones y los soportes magnéticos autorizados
- Debe programar un seguimiento de usuarios que acceden a ficheros con datos personales de nivel alto y las operaciones de consulta que realizan
- No existe un control de la salida de la empresa de soportes informáticos que contengan datos de carácter personal.
- No posee medidas de control de acceso físico a los locales donde están ubicados los sistemas de información con datos de carácter personal

En base a sus capacidades y sus propias limitaciones, la empresa debería establecer un calendario de trabajo con el objetivo de cubrir los hitos identificados en las debilidades, así como un equipo de personas adecuadamente formado y sensibilizado hacia el desempeño de la ley y la obtención del certificado Normadata, con el que la Agencia de Protección de Datos acredita una vez pasada la auditoría. Para finalizar, es interesante destacar la importancia de llevar a cabo este trabajo, pues el desconocimiento de la ley no exime de su cumplimiento.

Referencias

Aparicio, J. (2002). *Estudio sobre la Ley Orgánica de protección de datos de carácter personal*. Aranzadi, Navarra.
Del Peso, E.; Ramos, M. A. (2002). *La seguridad de los datos de carácter personal*. Díaz de Santos, Madrid.
Herrán, A. I. (2001). *El derecho a la intimidad en la nueva ley orgánica de protección de datos personales*. Dykinson, Madrid.
Vizcaíno, M. (2001). *Comentarios a la Ley orgánica de protección de datos de carácter personal*. Civitas, Madrid.

Enlaces Web consultados

www.agpd.es
www.delitosinformaticos.com
www.leydatos.com
www.mir.es
www.unionalcoyana.es