Datos personales y tecnología

Esther Cerdeño Argüelles
Diplomada en Informática. Universidad Politécnica de Madrid
Subdirectora de Informática
Técnica de MAPFRE RE (Madrid – España)

La información contenida en los archivos informáticos de las empresas, organismos públicos, centros escolares y sanitarios, entre otros, representa un acervo de enorme valor, pues supone una parte muy apreciada del conocimiento acumulado en el desarrollo de su actividad. En lo que se refiere a las personas, la generalización del uso de instrumentos informáticos hace que las empresas dispongan de datos cada vez más complejos, sofisticados y relevantes. Aunque siempre han existido ficheros con datos de carácter personal recogidos en papel, la informática permite ya recogerlos en bases de datos que pueden ser objeto de tratamiento automático con unas posibilidades de análisis y utilización mucho mayores. En el mundo empresarial se está haciendo un esfuerzo considerable para adaptar sus estructuras y procedimientos a los requerimientos de las leyes específicas.
Un sector sobre el que afecta de manera considerable son las empresas de seguros y reaseguros.

Ideas básicas de la LOPD española

Disposiciones Generales

- Se aplica a datos personales registrados en ***cualquier soporte físico*** susceptibles de tratamiento.
- Protege la ***intimidad personal y familiar*** de personas físicas, titulares de los datos, interesados o afectados.
- Define qué son datos personales y los especialmente protegidos; ficheros, sus responsables y tratamientos; afectado, cesión de datos...
- Establece la calidad de datos: adecuados, pertinentes y no excesivos.
- Dispone el derecho de información y consentimiento de los afectados si sus datos no son recabados directamente del afectado, teniendo que ser informado de forma expresa, salvo que la Ley prevea lo contrario.
- Ordena el derecho de impugnación de valoraciones, acceso a los datos, rectificación y cancelación.

Disposiciones Sectoriales

- Creación, notificación, inscripción, tratamiento de ficheros de titularidad pública y privada.

Movimiento Internacional de Datos

- Prohibido a aquellos países que no tengan un nivel de protección equiparable al que proporciona la LOPD. En principio se requiere autorización del director de la Agencia de Protección de Datos.

Agencia de Protección de Datos

- Ente de derecho público con personalidad jurídica propia y plena capacidad pública y privada, que actúa con independencia de las Administraciones Públicas de conformidad con la Ley 30/1992, de 26 de noviembre.

Infracciones y Sanciones

- Clasificación de infracciones sobre el tratamiento de los datos, sanciones y plazos de prescripción:

Leves:	EUR	601,01	a	EUR 60.101,21	prescriben al año
Graves:	EUR	60.101,21	a	EUR 300.506,05	prescriben a los 2 años
Muy graves:	EUR	300.506,05	a	EUR 601.012,10	prescriben a los 3 años

Legislación

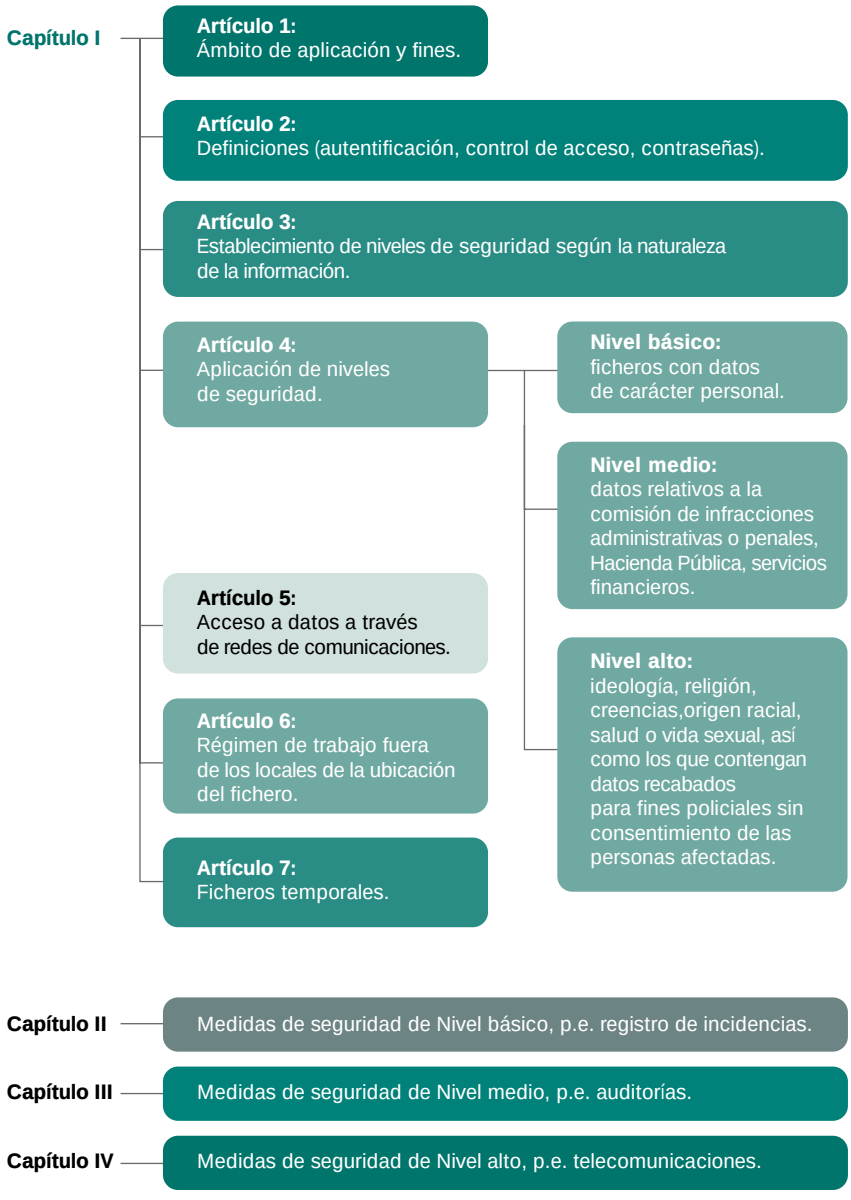
El uso indebido de las Bases de Datos personales puede dañar o causar perjuicios a los interesados. Por ello, los Estados han desarrollado una amplia normativa. En España, dicha normativa está recogida en la Ley Orgánica de Protección de Datos (LOPD). En otros países europeos también se han adoptado normativas similares.

- ESPAÑA: Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal

En 1978, la Constitución española limitó el uso de la informática para preservar la intimidad de sus ciudadanos en el artículo 18.4, dictado cuando el avance de la tecnología y el abaratamiento de los sistemas hicieron necesario promulgarla para garantizar y proteger los datos de carácter personal.

En 1992, se aprobó la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal (LORTAD). Esta Ley ha sido sustituida por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD).

ESPAÑA: Real Decreto 994/1999 Reglamento de Medidas de Seguridad de los Ficheros Automatizados con Datos Personales



Una medida recomendable en cualquier entorno empresarial es establecer una estrecha relación entre los *departamentos tecnológico, jurídico, de seguridad física y de recursos humanos*, al objeto de definir cuáles son los niveles de los datos existentes y las posibles medidas de seguridad que hay que implementar.

El coste de una implantación técnica que proteja la privacidad de los datos personales, no debe supeditarse a una posible sanción económica, o lo que es peor aún, a la pérdida de imagen empresarial.

En ayuda del cumplimiento de la LOPD española, se establece el Real Decreto 994/1999, por el que se aprueba el Reglamento de Medidas de Seguridad de los ficheros automatizados que contengan datos de carácter personal.

El reglamento se encuentra dividido en cuatro capítulos donde se establecen medidas técnicas y organizativas necesarias para garantizar la seguridad que deben reunir los ficheros automatizados, los centros de tratamiento, ubicaciones, equipos, sistemas, programas y las personas que intervengan en el tratamiento automatizado de los datos de carácter personal.

En dicho reglamento se define la elaboración de un *documento de seguridad* con especificaciones para cada nivel, con todas las medidas que garanticen la confidencialidad de los datos de carácter personal, así como cualquier incidencia en su tratamiento. Estas medidas pueden ser de carácter técnico u organizativo, según la naturaleza de los datos y la necesidad de garantizar su integridad y confidencialidad.

UNIÓN EUROPEA: Directiva 2002/58/CE del Parlamento Europeo y del Consejo

En el seno de la Unión Europea existen varias normas relativas a la protección de datos personales. El 12 de julio de 2002 se aprobó la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, relativa al tratamiento de los datos personales y protección de la intimidad en comunicaciones electrónicas. El pasado 19 de noviembre del 2003, el Parlamento Europeo ha llegado a un acuerdo sobre la propuesta de creación de ENISA (European Network and Information Security Agency) con el objetivo de coordinar entre los Estados miembros la seguridad de la información.

Adecuación de la LOPD a un entorno corporativo

El avance de la tecnología ha dado lugar a herramientas que facilitan el cumplimiento de la LOPD. La diagnosis de confidencialidad de los datos contenidos en

Aspectos fundamentales de un documento de seguridad

- **Ámbito** de aplicación del documento con especificación de los recursos protegidos.
- **Normativa** y medidas encaminadas a garantizar el nivel de seguridad exigido en el Reglamento.
- **Funciones** y obligaciones del personal.
- **Estructura** de los ficheros con datos de carácter personal y descripción de los sistemas de información que los tratan.
- **Procedimiento** de notificación, gestión y respuesta ante incidencias.
- **Procedimiento** de realización de copias de respaldo y recuperación de datos.

los ficheros (nivel bajo, medio o alto), determinará el tipo de medidas que se deben implementar. A continuación, se muestra un esquema que ilustra una serie de medidas tecnológicas acordes con la LOPD española, que se pueden poner en marcha en un entorno corporativo, sin olvidar que aquí se comparten los recursos de los sistemas, pero donde a su vez, se debe *garantizar el correcto acceso* a los datos de carácter personal.

Empresas aseguradoras y reaseguradoras

Las compañías aseguradoras tienen en su poder, y tratan, datos personales de importancia, como pueden ser los referidos a la salud, accidentes y propiedades, entre otros. Por ello, en España surge en este sector la preocupación respecto del adecuado cumplimiento de la LOPD, garantizando así la protección de los datos personales de sus clientes, empleados y proveedores, y evitando, además, sanciones de elevada importancia.
Como medida específica de la LOPD y para datos de nivel medio y alto en todo el entorno empresarial, está establecida la obligación de someterse a una auditoría (interna o externa) cada dos años. Se lleva a cabo con herramientas informáticas adecuadas que permiten, entre otros objetivos, consultar los accesos a los sistemas y reproducir situaciones representativas de incidencias, descubriendo cuál era el estado del dato en el momento de la modificación.

"El coste de una implantación técnica que proteja la privacidad de los datos personales, no debe supeditarse a una posible sanción económica, o lo que es peor aún, a la pérdida de imagen empresarial."

En el contexto asegurador se destacan los siguientes aspectos:

Principio de finalidad

El principio de finalidad establece que una empresa no puede utilizar los datos para una finalidad diferente a la prevista.

Cesión de los datos durante la vigencia del contrato

La cesión de los datos personales de un asegurado sólo puede hacerse cuando haya sido consentida por el interesado, sobre todo cuando se trate de información relativa a su salud y, en general, cualquier dato que contenga la condición de "especialmente protegido".

La cesión de dichos datos a las empresas reaseguradoras se podrá amparar en la necesidad intrínseca de información básica de un contrato de reaseguro sobre la persona o personas objeto de cobertura, de forma que pueda ser adecuadamente diseñado y cotizado por el reasegurador.

Conclusiones

Es importante establecer un adecuado flujo de información sobre el contenido de las legislaciones actuales respecto del tratamiento de datos de carácter personal en las empresas. En todos los ámbitos están apareciendo diversas alternativas para garantizar la seguridad en los datos personales y el derecho a la intimidad. Este trabajo ha desarrollado el caso actual de España en el contexto de la Unión Europea, ejemplificándolo en un entorno corporativo y destacando algunos puntos de aplicación al sector asegurador y reasegurador.

El mundo empresarial ha de entender que el desconocimiento de las leyes o el coste de una implantación de política de seguridad sobre datos personales, no justifica su incumplimiento.

Direcciones de interés

- www.rediris.es/cert/links/legal.es.html
- www.upco.es
- www.microsoft.com/spain/seguridad
- www.agpd.es
- www.delitosinformaticos.com
- www.portaley.com/protecciondatos/

Esquema de medidas tecnológicas en entorno corporativo

Información sobre los procedimientos para el cumplimiento de la Ley	**Creación** de un portal interno que permita difundir información sobre la Ley y cómo aplicarla. **Avisos** al arrancar los equipos que permitan a los usuarios conocer las normas de seguridad.
Identificación y autentificación	**Identificación** del usuario ante el sistema mediante usuario-clave. **Utilización** de Servicios de Directorio (Estándares LDAP: *Lightweight Directory Access Protocol*): único punto de entrada para la administración de usuarios, localización de ficheros, impresoras para usuarios autentificados. **Definición** de grupos y/o perfiles de usuarios de acceso a aplicaciones.
	Establecimiento de políticas de claves seguras: **Longitud** mínima de seis caracteres. **Claves** de tipo usuario-mes o mes-usuario no admitidas. **Caducidad** obligatoria cada 45 días y margen de cinco días para cambiar la clave desde entonces. **Uso** no permitido de la misma clave hasta producirse «n» cambios. **Bloqueo** de cuentas de usuario si la clave se teclea incorrectamente cinco veces seguidas.
Control de acceso lógico	**Utilización** de registros de ficheros (*logs*) de eventos de acceso correcto, fallido o no permitido, generados por los sistemas de red. **Uso** de procedimientos o funciones en Bases de Datos para el almacenamiento de los registros accedidos en tablas. **Empleo** de herramientas para identificación accesos de usuarios y capacidad de reproducir el estado del dato en cualquier instante.
Copias de respaldo y recuperación	**Automatización** y sistematización de creación de copia y recuperación de ficheros. **Inventario** y etiquetado de soportes (juegos de cintas). **Mantenimiento** de registro de acceso a los datos contenidos en los dispositivos de cara a recuperación de ficheros. **Formularios** de petición de recuperación de datos. **Almacenamiento** en armarios especiales protegidos por llaves y contraseñas, separados en salas distintas de los ordenadores e, incluso, en distintos edificios. **Encriptación** de datos de nivel alto cuando los soportes salgan fuera del edificio. **Registro** de entrada y salida de dispositivos.
Declaración de ficheros	**A través** de un programa cedido por la Agencia de Protección de Datos para generación de documentos asociados a ficheros donde se define el responsable, acceso, nombre, seguridad, finalidad y estructura. **Declaración** de los ficheros por vía telemática. **Recepción** por correo postal de confirmación de registro.
Auditoría: Nivel alto y medio	**Auditoría** obligatoria, interna o externa, del tratamiento de datos con herramienta que permita consultar accesos, reproducir situaciones, etc. **Verificación** de procedimientos e instrucciones vigentes.
Control de acceso físico	**Salas** de ordenadores de acceso restringido a personal registrado, administradores y personal de seguridad. **Sistema** de acceso con claves o tarjetas. **Registro** de accesos correctos e incorrectos. **Cámaras** en las puertas de acceso.
Telecomunicaciones: Nivel Alto	**Cifrado** de datos si viajan por redes no locales. **Utilización** de VPN (Redes Virtuales Privadas – *Virtual Private Network*). **Utilización** de protocolos IPSES (*Internet Protocol Security*). **Tecnologías** de integridad y encriptación.