Cumplimiento LOPD

LOPD (1)

Fecha revisión: *15/02/2010*

Resumen ejecutivo

La LOPD viene a regular el derecho fundamental a la protección de datos de las personas físicas, esto es, el derecho a disponer de sus propios datos sin que puedan ser utilizados, tratados o cedidos sin su consentimiento salvo las excepciones legalmente previstas.

Esta ley es obligatoria para todas las empresas y autónomos, independiente de su tamaño o actividad.

La LOPD obliga a adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos personales y eviten su alteración, pérdida o acceso no autorizado.

El cumplimiento de la LOPD nos permitirá evitar las elevadísimas sanciones, pero es muy importante no olvidar que al cumplir la ley, mejoramos la seguridad de nuestra información, la productividad de nuestros empleados, y la imagen fiel frente a terceros, respetando la privacidad y el derecho a la intimidad.

El riesgo de una inspección de la AEPD es altísimo ya que nueve de cada diez denuncias provienen de los trabajadores de la empresa o de empresas de la competencia.

Esta nota técnica de "**Cumplimiento LOPD – LOPD**" forma parte de la documentación para uso interno de Microsa de aclaración de conceptos para la implantación de la normativa de protección de datos en una empresa privada

Índice:

Notas técnicas de aclaración de conceptos para la implantación de la normativa de protección de datos en una empresa privada con una visión práctica:

Marco Legal

- **LOPD**: Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal
- **RLOPD**: Real Decreto 1720/2007 por el que se aprueba el Reglamento de desarrollo de la LOPD
- **LSSICE**: Ley 34/2002 de Servicios de la Sociedad de la Información y de Comercio Electrónico
- Sentencias que dicta en la materia la **Audiencia Nacional** y la jurisprudencia que emite el **Tribunal Supremo** y el **Tribunal Constitucional**
- Memorias, Informes Jurídicos, Resoluciones, Recomendaciones e Instrucciones que emite la **AEPD (Agencia Española de Protección de Datos)**.
- **Normas sectoriales** que regulan o hacen referencia a diversos aspectos de los tratamientos de datos
- **LGT**: Ley 32/2003 General de Telecomunicaciones
- **RSUT**: Real Decreto 424/2005 por el que se aprueba el Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios
- **Código Penal**: Ley Orgánica 10/1995 de Código Penal
- **ET**: Real Decreto Legislativo 1/1995 por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores
- **Instrucción 1/2006** de la AEPD
- **LSP**: Ley 23/1992 de Seguridad Privada
- **RSP**: Real Decreto 2364/1994 por el que se aprueba el Reglamento de Seguridad Privada
- **LOSC**: Ley Orgánica 1/1992 de Seguridad Ciudadana

1. Introducción

El objetivo de esta nota técnica es dar una **visión práctica sobre el cumplimiento en la empresa privada de la normativa legal de protección de datos personales**.

La Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal (LOPD) y su reglamento de desarrollo RLOPD vienen a regular **el derecho fundamental a la protección de datos de las personas físicas**, esto es, **el derecho a disponer de sus propios datos sin que puedan ser utilizados, tratados o cedidos sin su consentimiento** salvo las excepciones legalmente previstas.

Esta ley es obligatoria para todas las empresas y autónomos, independiente de su tamaño o actividad, ya que por pequeña que sea maneja datos personales sobre sus clientes, proveedores, colaboradores o empleados.

A pesar de que esta ley de 1999 lleva diez años en vigor y es muy conocida, **sólo el 14% de las pymes cumplen con la LOPD**.

El incumplimiento de esta ley se sanciona con elevadísimas multas de hasta 600.000 €, siendo estas sanciones las más elevadas de nuestro entorno europeo

La LOPD obliga a 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.

Al tratar el **cumplimiento de la LOPD** en la empresa privada, nos encontramos con otros dos frentes muy relacionados, la **seguridad de la información** y la **productividad** de nuestros empleados.

En el cumplimiento de la LOPD estamos obligados a adoptar unas medidas de seguridad para los datos de carácter personal, pero para una empresa de lo que se trata es de garantizar la seguridad de toda la información, datos personales y no personales.

La **seguridad de la información** tiene como fin **la protección de la información**, garantizando la **confidencialidad** (sólo accederán a la información las personas autorizadas), la **integridad** (la información no puede sufrir alteraciones no queridas) y la **disponibilidad** (asegurando que los usuarios autorizados tienen acceso a la información).

Por otro lado, en relación a la seguridad informática, **más del 80% de los ordenadores del mundo están infectados de algún virus** y **casi todos los ordenadores**, salvo los instalados en entornos corporativos u organismos públicos, **trabajan con permiso de administrador**.

Desde hace muchos años, los ordenadores por defecto trabajan con permiso de administrador con idea de priorizar la compatibilidad con anteriores sistemas operativos y porque muchas aplicaciones fueron desarrolladas sin tomar en cuenta los usuarios sin privilegios de administrador.

En este último semestre de 2009, las páginas web han pasado a ser el modo más importante de infección de los ordenadores. Del mismo modo que no hace mucho

tiempo fue el correo electrónico o la mensajería instantánea, en la actualidad, la posibilidad de que el usuario quede infectado simplemente visitando una página web se ha convertido en el modo más habitual de actuar para los atacantes.

Por lo tanto, hoy en día, **el principal agujero de seguridad es trabajar en un ordenador con permiso de administrador** ya que estamos totalmente desprotegidos y un ordenador se infecta por el mero hecho de visitar una página web legítima infectada. **Debemos protegernos de delincuentes organizados en mafias que se introducen en nuestros ordenadores, con el objetivo de robarnos dinero e información, así como cometer delitos con nuestra responsabilidad legal**.

Como buena práctica es muy importante recordar que **no debemos navegar jamás por Internet ni abrir correos electrónicos con usuario administrador** por su alta peligrosidad. Solo debe usarse usuario administrador cuando vaya a instalarse un nuevo programa o se tenga que actualizar, el resto del tiempo se debe de utilizar un ordenador sin privilegios de administrador.

Las **recomendaciones básicas de seguridad** son: trabajar con **usuario sin permiso de administrador**, tener instalado un buen **antivirus** bien configurado y permanentemente actualizado (es preferible una suite de seguridad a tener solamente un antivirus), instalación de un **cortafuegos** y mantener **actualizado** el sistema operativo y los programas.

La mayoría de las empresas no han implantado **una política de uso de los medios electrónicos** con medidas de seguridad de protección de la información y los empleados suelen navegar por páginas de ocio, instalan programas como el eMule para descarga de archivos y pueden acceder a toda la información de la empresa sin dificultad alguna y sin que quede constancia.

Estos ordenadores infectados de virus y de programas de ocio van mucho más lentos y requieren intervenciones técnicas más frecuentemente. Un ordenador sin permiso de administrador que solo tenga instalados los programas necesarios va a su máximo rendimiento. Por otro lado, estas descargas de archivos y troyanos actuando están consumiendo ancho de banda y el resto de la empresa sufre la lentitud del uso de Internet. Y por último, el empleado dedica parte de su jornada laboral a tareas de ocio en vez de desempeñar sus funciones.

Es decir, ordenadores e Internet más lentos y empleado dedicado a tareas de ocio, en definitiva, más baja **productividad**, que es el tercer frente relacionado con la LOPD.

No tiene sentido abordar el cumplimiento de la LOPD si al mismo tiempo no se abordan medidas de seguridad de la información, ya que la propia ley lo obliga. De hecho todas las resoluciones de la AEPD con penas de multas son a empresas que tenían inscritos sus ficheros en el Registro General de Protección de Datos (RGPD) y disponían del documento de seguridad, pero en cambio no habían implantado las medidas adecuadas de seguridad.

Lo que habitualmente están realizando la mayoría de las empresas a través de consultoras o despachos de abogados es la adaptación al cumplimiento de la Ley Orgánica de Protección de Datos en papel, ya que en la realidad las medidas de seguridad recogidas en el documento de seguridad no se han implementado en el sistema informático.

Para el cumplimiento de la LOPD se debe abordar la parte legalista o formal así como la parte tecnológica o práctica.

El cumplimiento de la LOPD nos permitirá evitar las elevadísimas sanciones, pero es muy importante no olvidar que al cumplir la ley, **mejoramos la seguridad de nuestra información, la productividad de nuestros empleados, y la imagen fiel frente a terceros, respetando la privacidad y el derecho a la intimidad**. De todas maneras, la principal razón que mueve a las empresas a adaptarse a la LOPD es el temor a las elevadísimas sanciones, como por ejemplo:

- No solicitar la inscripción del fichero de datos de carácter personal en el Registro General de Protección de Datos, tiene un sanción de 600 a 60.000 €
- Incumplir el deber de guardar secreto, tiene un sanción de 600 a 60.000 €
- Mantener los ficheros o programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad, tiene un sanción de 60.000 a 300.000 €
- La comunicación o cesión de los datos de carácter personal, fuera de los casos permitidos, tiene un sanción de 300.000 a 600.000 €

2. Sanciones por incumplimiento LOPD

La Agencia Española de Protección de Datos (AEPD) es el organismo público encargado de velar por el cumplimiento de la ley y cuenta con un amplio cuerpo de inspectores que tienen la consideración de autoridad pública en el desempeño de sus funciones. **Estos inspectores actúan de oficio o mediante denuncia de cualquier afectado y pueden llegar a imponer multas de hasta 600.000 euros**.

Una de las obligaciones de esta ley es la inscripción de los ficheros en el Registro General de Protección de Datos, y a través de la página www.agpd.es de la AEPD **cualquiera puede consultar si una empresa tiene o no inscrito sus ficheros**.

En la página de la AEPD en la opción: Canal del ciudadano / Denuncias y Reclamaciones, se puede formular cualquier denuncia, incluso aunque no se tenga ninguna relación con la empresa denunciada.

Hay muchas denuncias cuya queja es que la empresa denunciada no tiene inscritos sus ficheros en el Registro General de Protección de Datos y que no ha adoptado las medidas técnicas obligatorias para garantizar la seguridad de los datos personales.

Es habitual comentar que el riesgo de una inspección por parte de la AEPD es muy bajo, pero no se tiene en cuenta que cualquiera puede conocer si tiene sus ficheros inscritos en el Registro General de Protección de Datos y puede ponerle una denuncia, con lo cual el riesgo es mucho más alto.

Según la AEPD, nueve de cada diez denuncias provienen de los trabajadores de la empresa o de empresas de la competencia, con lo cual el riesgo de denuncia es altísimo.

3. Obligaciones LOPD

Las obligaciones legales en materia de protección de datos personales están recogidas en la LOPD y en su reglamento de desarrollo RLOPD, en las Sentencias que dicta en la materia la Audiencia Nacional y la jurisprudencia que emite el Tribunal Supremo y el Tribunal Constitucional, en las Memorias, Informes Jurídicos, Resoluciones, Recomendaciones e Instrucciones que emite la AEPD y en Normas sectoriales que regulan o hacen referencia a diversos aspectos de los tratamientos de datos.

El titular o propietario de los datos no es quien los posee en un fichero, sino la persona a quien se refieren los datos. Se entiende por fichero, según la LOPD, a todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso. Ejemplos de ficheros en una empresa privada son los de clientes, proveedores o personal.

En el momento que una empresa va a proceder al tratamiento de datos personales asume una serie de responsabilidades que implican deberes y obligaciones recogidos en la normativa legal, siendo las principales obligaciones las siguientes:

- **Notificación de ficheros en el Registro General de Protección de Datos**

Toda persona o entidad que proceda a la creación de ficheros de datos de carácter personal lo notificará previamente a la AEPD (Art. 26 LOPD)

- **Cumplimiento de principios relativos a la protección de datos:**

  - **Calidad de los datos** (Art. 4 LOPD y 8 RLOPD)

    El principio de calidad de los datos, que, ligado al principio de proporcionalidad de los datos, exige que los mismos sean adecuados a la finalidad que motiva su recogida. Los datos de carácter personal serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado.

  - **Derecho de información en la recogida de datos** (Art. 5 LOPD y 18 RLOPD)

    Los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco. El deber de información se debe de cumplir incluso en aquellos casos en que no sea necesario el consentimiento del afectado.

  - **Consentimiento del afectado** (Art. 6 LOPD y 12 RLOPD)

    El consentimiento del interesado es toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen.

  - **Seguridad de los datos** (Art. 9 LOPD y Título VIII RLOPD)

    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.

No se registrarán datos de carácter personal en ficheros que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas.

- **Deber de guardar secreto** (Art. 10 LOPD)

El responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo.

Es muy importante concienciar a todas las personas que intervienen en cualquier fase del tratamiento de los datos sobre su deber de secreto profesional así como que quede por escrito su obligación de secreto y confidencialidad.

- **Deber de colaboración con la AEPD** (Art. 44 LOPD)

Se considera infracción el no proporcionar la información que solicite la AEPD en el ejercicio de las competencias que tiene legalmente atribuidas, en relación con aspectos no sustantivos de la protección de datos.

- **Atención de los derechos de los ciudadanos**:

- **Derecho de acceso** (Art. 15 LOPD y 27-30 RLOPD)

El interesado tendrá derecho a solicitar y obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento, el origen de dichos datos, así como las comunicaciones realizadas o que se prevén hacer de los mismos.

- **Derecho de rectificación y cancelación** (Art. 16 LOPD y 31-33 RLOPD)

El derecho de rectificación es el derecho del afectado a que se modifiquen los datos que resulten ser inexactos o incompletos.

El ejercicio del derecho de cancelación dará lugar a que se supriman los datos que resulten ser inadecuados o excesivos, sin perjuicio del deber de bloqueo conforme a este reglamento.

- **Derecho de oposición** (Art. 17 LOPD y 34-36 RLODP)

El derecho de oposición es el derecho del afectado a que no se lleve a cabo el tratamiento de sus datos de carácter personal o se cese en el mismo en determinados supuestos.

En relación al **principio de seguridad**, el título VIII del RLOPD desarrolla **las medidas de seguridad** a adoptar en el tratamiento de datos personales, con la obligación de elaborar un **documento de seguridad** que recoja las medidas de índole técnica y organizativa que será de obligado cumplimiento para el personal con acceso a los datos personales.

4. Servicios Microsa de adaptación al cumplimiento LOPD

4.1 Adaptación al cumplimiento LOPD

En la adaptación al cumplimiento de la LOPD hay dos fases consistentes en el Diagnóstico de la situación y la Adecuación al cumplimiento que detallamos a continuación:

- **Diagnóstico de la situación de cumplimiento LOPD:**
  - **Identificación de los ficheros** de datos de carácter personal, de su finalidad y de su tratamiento por parte de los diferentes departamentos.
  - **Clasificación de los ficheros identificados** según los tres niveles establecidos en la LOPD (básico, medio y alto).
  - **Análisis de los documentos empleados para recabar datos** de carácter personal y sus coberturas formales.

- **Adecuación al cumplimiento LOPD:**
  - Colaboración en la **inscripción de los ficheros de carácter personal en el Registro General de Protección de Datos**.
  - Revisión de las **cláusulas y contratos referentes a la LOPD**:
    - Cláusula "Derecho de Información LOPD"
    - Cláusula "Derecho de Consentimiento e Información LOPD en nuevos contratos clientes-proveedores"
    - Modelo de "Compromiso de confidencialidad y secreto"
    - Modelo de "Contrato de encargo de tratamiento de acceso a datos por cuenta de terceros"
    - Modelo de "Contrato de cesión de bases de datos personales"
    - Modelos para el ejercicio por los afectados de sus derechos de acceso, rectificación, cancelación y oposición
    - Modelo de "Aviso Legal de correo electrónico"
    - Modelos de Videovigilancia
    - Modelo de "Política de usos de medios tecnológicos" para los empleados de la empresa
  - **Recomendar 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.
  - Desarrollo del **documento de seguridad**.
  - Recomendar la **incorporación de la protección de datos a la cultura de la empresa** y al diseño de los diferentes procesos departamentales. Siendo necesaria la formación en protección de datos a todos los empleados que tengan relación con el tratamiento de datos personales para que conozcan sus deberes de seguridad y secreto profesional y se contribuya a crear una cultura de compromiso con la protección de datos.
  - **Recomendaciones prácticas** en los temas donde hay mayor número de sanciones por incumplimiento de la LOPD:
    - **Ámbito laboral**: la instalación de programas como el Emule provocan la difusión de datos personales en Internet

        - **Comunicados comerciales**: la ilegalidad del envío de comunicaciones comerciales no solicitadas por correo-e, fax o sms
        - **Videovigilancia**: infracciones de videovigilancia en centros de trabajo y establecimientos
    - Entrega de **documentación para el cumplimiento en la empresa privada de la LOPD con una visión práctica**:
        - 1 Cumplimiento LOPD
        - 2 Ley Orgánica de Protección de Datos
        - 3 Cláusulas y modelos de contratos
        - 4 Datos especialmente protegidos
        - 5 Ámbito laboral
        - 6 Aviso legal correo electrónico
        - 7 Comunicados comerciales
        - 8 Videovigilancia

4.2 Implementación medidas seguridad protección de datos

Se trata de **implementar las recomendaciones de 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, indicadas en la adaptación al cumplimiento de la LOPD.

El **no implementar las medidas de seguridad necesarias supone una infracción grave**.

Las principales medidas técnicas de seguridad son:

- **Securización ordenador**: consiste en configurar el ordenador con usuario sin permiso de administrador en los diferentes programas instalados y a través de la utilidad **SecMicrosa** se permite promover y despromover los privilegios de administrador de un usuario. En definitiva que la empresa tenga el control de lo que se instala en sus ordenadores. Hoy en día, **el principal agujero de seguridad es trabajar en un ordenador con permiso de administrador** ya que se está totalmente desprotegido y cualquier virus se instala en nuestro ordenador y toma el control del mismo.

- **Cifrado**: para impedir el acceso a los datos. La LOPD obliga al cifrado (encriptado) de dispositivos portátiles para ficheros de nivel alto.

- **Identificación y Autenticación**: todos los usuarios se tienen que identificar y autenticar con una contraseña personalizada y confidencial con periodicidad de cambio anual al menos.

- **Control de Acceso**: los usuarios sólo tendrán acceso a la información que precisen para el desarrollo de sus funciones. En el caso de ficheros de nivel alto se debe llevar un registro de accesos.

- **Copias de seguridad**: copias de seguridad al menos semanal y verificación semestral de procedimiento de recuperación de datos.

4.3 Auditoría protección de datos

Aunque las auditorías de protección de datos sólo son obligatorias para los ficheros de nivel medio y alto de seguridad, **es recomendable realizarlas para todos los ficheros y niveles de seguridad**, como único instrumento que puede detectar en su conjunto los incumplimientos en materia de seguridad de los datos y la debida aplicación de las medidas técnicas y organizativas prescritas en el RLOPD.

El informe de auditoría deberá dictaminar sobre la adecuación de las medidas y controles a la Ley y su desarrollo reglamentario, identificar sus deficiencias y proponer las medidas correctoras o complementarias necesarias. Deberá, igualmente, incluir los datos, hechos y observaciones en que se basen los dictámenes alcanzados y las recomendaciones propuestas.

5. Incumplimiento de la LOPD

El incumplimiento de las obligaciones en la normativa legal de protección de datos personales está penalizado con **sanciones económicas muy elevadas**, como por ejemplo:

- **Son infracciones leves con sanciones de 600 a 60.000 €:**
    - No solicitar la inscripción del fichero de datos de carácter personal en el Registro General de Protección de Datos, cuando no sea constitutivo de infracción grave.
    - Proceder a la recogida de datos de carácter personal de los propios afectados sin proporcionarles la información que señala el artículo 5 de la presente Ley.
    - Incumplir el deber de secreto establecido en el artículo 10 de esta Ley, salvo que constituya infracción grave.

- **Son infracciones graves con sanciones de 60.000 a 300.000 €:**
    - Proceder a la creación de ficheros de titularidad privada o iniciar la recogida de datos de carácter personal para los mismos con finalidades distintas de las que constituyen el objeto legítimo de la empresa o entidad.
    - Proceder a la recogida de datos de carácter personal sin recabar el consentimiento expreso de las personas afectadas, en los casos en que éste sea exigible.
    - El impedimento o la obstaculización del ejercicio de los derechos de acceso y oposición y la negativa a facilitar la información que sea solicitada.
    - Mantener datos de carácter personal inexactos o no efectuar las rectificaciones o cancelaciones de los mismos que legalmente procedan cuando resulten afectados los derechos de las personas que la presente Ley ampara.
    - Mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen.

- **Son infracciones muy graves con sanciones de 300.000 a 600.000 €:**
    - La recogida de datos en forma engañosa y fraudulenta.
    - La comunicación o cesión de los datos de carácter personal, fuera de los casos en que estén permitidas.
    - Tratar los datos de carácter personal de forma ilegítima o con menosprecio de los principios y garantías que les sean de aplicación, cuando con ello se impida o se atente contra el ejercicio de los derechos fundamentales.

Según la AEPD el mayor número de sanciones por incumplimiento de la LOPD en la empresa privada es por:

1) **Difusión de datos personales** a través de sistemas P2P, como el programa eMule.

Una de las principales preocupaciones de la AEPD sigue siendo **el continuo hallazgo de ficheros con datos personales en Internet en redes P2P** y, en particular en eMule. Esta situación es consecuencia, fundamentalmente, de las descargas de todo tipo, como películas, música, etc., realizadas por empleados durante su tiempo de trabajo sin que se hayan adoptado medidas de seguridad por parte de la empresa.

En estos casos, las sentencias de la AEPD han sido por incumplimiento de las medidas de seguridad y la vulneración del deber de secreto, sancionándose en función de la naturaleza de la información divulgada. Las actuaciones inspectoras afectan a entidades privadas y a organismos públicos, como por ejemplo, centros de salud o bufete de abogados o partido político o sindicato. Los ficheros difundidos por Internet, incluso, contienen datos sensibles como los de salud.

2) **Envío de comunicaciones comerciales no solicitadas** por correo electrónico, fax o mensajes SMS.

   Es ilegal el envío de un solo fax o correo electrónico con comunicaciones comerciales que no hayan sido previamente solicitadas o expresamente autorizadas por el destinatario antes de su envío.

3) **Infracciones de Videovigilancia** en centros de trabajo y establecimientos.

   Para la instalación de videovigilancia en los centros de trabajo, la empresa debe de comunicar previamente a sus empleados las reglas de uso de Internet, del correo electrónico de empresa y de los medios tecnológicos.

   El tratamiento de imágenes en establecimientos, salvo en situaciones específicas, deben realizarse por empresas de seguridad privada.

Según la AEPD el **control de acceso a la información** es una de las deficiencias más relevantes, destacando:

- no disponer de una relación escrita de usuarios con acceso a los datos
- no controlar la caducidad de las contraseñas
- disponer de contraseñas genéricas utilizadas por más de un usuario
- no tener registro de accesos
- no guardar las consultas realizadas

Un **incumplimiento del deber de secreto** se produce cuando se envía un correo electrónico con las direcciones de sus destinatarios a la vista sin disponer del consentimiento para ello. De ahí, que se deba de utilizar el campo CCO “Con Copia Oculta” en vez del campo CC “Con Copia”. Se vulnera el deber de secreto en el tratamiento de datos personales al difundirse direcciones de correo electrónico sin consentimiento del interesado.

Son **encargados de tratamiento** con acceso a datos por cuenta de terceros para la prestación de un servicio, por ejemplo, una asesoría fiscal, contable o laboral, una empresa de mantenimiento informático, una empresa de envío de correspondencia o una empresa de transporte de mercancías. Conforme al art. 12 LOPD debe de **formalizarse un contrato por escrito con el encargo de tratamiento** en el que deberá quedar delimitada la necesidad, objeto y ámbito en el que se desarrolle la prestación de sus servicios, así como las medidas de seguridad que está obligado a

implementar. El encargado del tratamiento puede ser responsable de una infracción de la LOPD, bien por inobservancia e incumplimiento de las estipulaciones del contrato con el responsable del fichero o tratamiento, bien por la inexistencia del contrato.

Se debe de firmar un **contrato de confidencialidad** con todas las empresas cuya actividad suponga un contacto directo o indirecto con el sistema de información y/o su entorno físico o lógico, y que pueda ser susceptible de poner en riesgo la seguridad de los datos, por ejemplo, limpieza, seguridad, mantenimiento o reparación de instalaciones que no se refieran al propio sistema de información.

La **cesión de datos** no permitida, a pesar de ser una infracción muy grave, resulta ser una de las conductas que por ignorancia o inobservancia, resulta más común, como por ejemplo:

- La cesión de bases de datos de clientes o simplemente un listado.
- El flujo de datos entre empresas de un mismo grupo empresarial.
- Las prestaciones de servicios con acceso a datos de carácter personal, sin mediar el preceptivo contrato y sin disponer del consentimiento del interesado.
- Las prestaciones de servicios sin acceso a datos, que se desarrollan en los centros del responsable del tratamiento, sin contrato de confidencialidad.
- El flujo de datos entre corredores de seguros y las compañías aseguradoras en las renovaciones, ofertas y cambios de compañía.
- El uso por los Colegios Profesionales de datos de sus afiliados para cederlos a terceras entidades.

6. Preguntas más frecuentes cumplimiento LOPD

¿Por qué Microsa me ofrece la adaptación al cumplimiento de la LOPD al mismo tiempo que me plantea la seguridad de la información?

Porque la LOPD obliga a adoptar las medidas de seguridad y su incumplimiento supone una infracción grave.

Y por otro lado porque creemos que la información es el principal activo de una empresa e independiente de las obligaciones legales hay que proteger la información.

¿La LOPD es obligatoria para una pyme?

Sí. Esta ley es obligatoria para todas las empresas y autónomos, independiente de su tamaño o actividad, ya que por pequeña que sea una empresa maneja datos personales sobre sus clientes, proveedores, colaboradores o empleados

¿Si la LOPD es de hace 10 años, por qué me tengo que adaptar ahora?

Por tres razones:

1) Por el aumento del número de denuncias y por el riesgo del elevadísimo importe de las multas (hasta 600.000 euros).
2) Porque las medidas de seguridad de hace años no son suficientes y es necesaria una concienciación de la gravedad de la situación y que la información de casi todas las empresas está en manos de delincuentes.
3) Porque es necesario que la empresa tome el control de sus ordenadores, y no estén en manos de delincuentes o de empleados irresponsables.

Objetivamente, la principal razón debería ser garantizar la seguridad de la información y la productividad de sus empleados, aunque en realidad, la principal motivación de adaptación a la LOPD es evitar las elevadísimas multas.

Pienso que el riesgo de una inspección de la AEPD es muy bajo, ¿tengo razón?

No. Los inspectores de la AEPD actúan de oficio o mediante denuncia y según la AEPD, nueve de cada diez denuncias provienen de los trabajadores de la empresa o de empresas de la competencia, con lo cual el riesgo de denuncia es altísimo.

Si siempre hemos trabajado con ordenadores con permiso de administrador, ¿por qué ahora se plantea que es el principal riesgo de seguridad?

Desde hace muchos años, los ordenadores por defecto trabajan con permiso de administrador con idea de priorizar la compatibilidad con anteriores sistemas operativos y porque muchas aplicaciones fueron desarrolladas sin tomar en cuenta los usuarios sin privilegios de administrador.

En este último semestre de 2009, las páginas web han pasado a ser el modo más importante de infección de los ordenadores. Del mismo modo que no hace mucho tiempo fue el correo electrónico o la mensajería instantánea, en la actualidad, la posibilidad de que el usuario quede infectado simplemente visitando una página web se ha convertido en el modo más habitual de actuar para los atacantes.

Salvo los ordenadores instalados en entornos corporativos u organismos públicos, el resto de los ordenadores han trabajado erróneamente con permiso de administrador, pero esta vulnerabilidad está siendo aprovechada en los últimos tiempos por los ciberdelincuentes y un ordenador se infecta por el mero hecho de visitar una página web legítima infectada.

Los privilegios de administrador sólo se deberían haber usado para tareas de administración ya que al trabajar con permiso de administrador estamos totalmente desprotegidos.

Los delincuentes organizados en mafias se introducen en nuestros ordenadores, con el propósito de robarnos dinero e información, así como cometer delitos desde nuestro ordenador con nuestra responsabilidad legal, al mismo tiempo que perdemos la privacidad y confidencialidad de toda nuestra información.

Si trabajo sin permiso de administrador ya no necesitaré antivirus

No. El antivirus siempre es necesario. Al trabajar sin permiso de administrador se garantiza que no se instalará ningún programa sin control de la empresa, con lo cual además no se corrompe el Windows y el ordenador va al máximo de sus prestaciones. Pero gracias al antivirus puedo detectar que algún archivo pueda estar infectado.

Aunque a todo el software malicioso (malware) se le llame virus, en realidad hay muchos tipos de software que tienen como objetivo infiltrarse en el sistema y dañar el ordenador con finalidades muy diversas, y nos encontramos desde un troyano a un spyware.

No solo es necesario tener instalado un buen antivirus bien configurado y permanente actualizado, sino que sería recomendable tener una suite de seguridad, que incluye además del antivirus, otros productos de seguridad como anti-spyware, anti-spam, etc.

Al trabajar su empresa con ordenadores sin permiso de administrador, además de que ningún delincuente puede instalar ningún programa, tampoco ningún empleado de su empresa puede instalar ningún programa de ocio que quiera.

En su día una consultora me registró los ficheros en el Registro General de Protección de Datos y me entregó un documento llamado de seguridad, ¿mi empresa cumple con la LOPD?

Si no se ha realizado ninguna medida de seguridad que garantice la seguridad de los datos y evite su alteración, pérdida, tratamiento o acceso no autorizado y las medidas descritas en el documento de seguridad son falsas, evidentemente, no se está cumpliendo con la LOPD.

Ante una denuncia, la AEPD va a revisar su sistema informático y su documento de seguridad, por lo tanto si no se han llevado a cabo las medidas de seguridad

necesarias, la sanción está garantizada y nuestro sistema informático está desprotegido.

Además de la propuesta de Microsa, tengo otra oferta de una consultora para el cumplimiento de la LOPD que no plantea nada sobre la seguridad de la información, ¿por qué?

Inicialmente, la adaptación al cumplimiento de la LOPD la ofrecieron consultoras y despachos de abogados, pero solo abordaban la parte formal o legalista.

El cumplimiento total de la LOPD necesita la intervención de técnicos informáticos para la implementación de las medidas de seguridad que obliga la ley.

La propuesta de Microsa de adaptación al cumplimiento de la LOPD, ¿puedo abordarla por fases o necesariamente debe ser completa?

Evidentemente puede llevarse a cabo por fases. En algunos clientes hemos comenzado con la parte legalista o formal y por fases vamos continuando con la parte tecnológica o práctica.