



PROTECTION REPORT S.L.

ESPECIALISTAS EN PROTECCIÓN DE DATOS

Consultores Especialistas en Protección de Datos
Personales y Seguridad de la Información



**Presupuesto adaptación y mantenimiento respecto a la Ley
Orgánica 15/1999, de Protección de Datos de carácter personal
y normativa complementaria :**

Paseo del Violón, 8. Local - GRANADA
Torneo-P.Empres., C/ Arquitectura, 4. Torre 10 - Pl. 6º Mod. 4 - SEVILLA
Valle De Pinares Llanos, 8 B. 2º B - MADRID

Tlf. Atención al cliente 902364585



**Asociación Profesional Española
de Privacidad**

1- INTRODUCCIÓN:

El artículo 2 de la Ley Orgánica 15/1999 de Protección de Datos, en el que se desarrolla el ámbito de aplicación de la Ley, se establece literalmente:

1- La presente Ley Orgánica será de aplicación a los datos de carácter personal registrados en soporte físico que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado.

Por tanto dicha Ley es de obligado cumplimiento para todas las empresas, entidades y profesionales, que archiven datos de personas físicas (nombre, dirección, teléfono, email, DNI, etc, ...) en cualquier tipo de soporte, sean éstos pertenecientes a clientes, empleados, proveedores o cualesquiera otras relaciones, están obligadas a cumplir con una serie de medidas a nivel técnico, organizativo y legal para su protección y confidencialidad.

Como consecuencia de esta ley, el organismo que se encarga de su cumplimiento, la **Agencia Española de Protección de Datos (AEPD)** impuso en el año 2011 sanciones por valor de casi 30 millones de euros, a causa de las denuncias presentadas directamente ante la Agencia que pueden llegar a hacerse incluso anónimas, con lo que esto supone, o a través de las Hojas de Reclamaciones que toda empresa o establecimiento debe tener que luego la O.C.U. derivará a la AEPD, o por los procedimientos iniciados de oficio por la propia AEPD. Todo ello como pueden ver, motivo más que suficiente para tener en cuenta el cumplimiento de dicha normativa.

Nuestra consultora está formada por expertos en Seguridad Informática y por expertos en Derecho Informático y Protección de Datos, con amplia experiencia en la implantación de políticas de seguridad de empresas y entidades.

Estamos especializados en ofrecer soluciones globales de adaptación a la LOPD y LSSI para cualquier tipo de empresa y profesional, por ello ofrecemos al finalizar nuestros trabajos un certificado final de garantía, que se encuentra ampliamente respaldado por una póliza de seguro de responsabilidad civil especialmente suscrita por PROTECTION REPORT S.L., para cubrir a nuestros clientes ante cualquier contingencia.



2- ¿POR QUÉ PROTEGER LOS DATOS DE SU EMPRESA?

A) La Protección de la información y de los datos generados o recabados por su entidad ha sido siempre una cuestión de crucial importancia, que se ha convertido en una obligación legal con la entrada en vigor de la Ley 15/1999, para los datos de carácter personal.

B) La información de su empresa o entidad es uno de sus principales activos y como tal debe ser salvaguardada frente a intrusiones externas e incluso conductas internas de los empleados, que puedan poner en peligro su confidencialidad y conservación. Son muchos los intereses que hoy en día pueden amenazar la seguridad de la información que almacenamos, desde los comerciales, hasta los meramente dañinos y destructivos. Por ello, es indispensable para la supervivencia de nuestra empresa que implantemos las máximas medidas de seguridad, las cuales habrán de ser necesariamente de carácter técnico, organizativo y legal.

C) Duro régimen sancionador (el más duro de la Unión Europea), al que no le importa el volumen de la empresa.

Con sanciones económicas de hasta 600.000 euros, pudiendo llegar al bloqueo de los ficheros, paralizando de esta forma la actividad de la empresa; sanciones que se pueden utilizar con mala fe (con intención de causar un daño económico o de imagen a la entidad).

D) Reforzar la confianza del CLIENTE; la implantación de las medidas que garanticen la seguridad de la información de su empresa no es sólo una obligación legal, sino también una oportunidad de ganar la confianza del cliente, que considerará como un valor añadido, la máxima seguridad de sus datos y transacciones. La satisfacción del cliente debe ser la primera consigna para el crecimiento de su empresa.

3- ¿QUÉ BENEFICIOS LE REPORTA EL ADAPTARSE A LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS?

1º Legalidad de los tratamientos de datos personales efectuados por su entidad. Esta legalidad se manifestará por el cumplimiento de la regulación establecida por la Ley 15/1999 de Protección de Datos y su Reglamento.

2º Control de las actuaciones que sus empleados lleven a cabo sobre la información de la entidad, sea de carácter personal o comercial. Este control no sólo se manifestará a través de la implantación de las medidas técnicas necesarias, tendentes a permitir que sólo tengan acceso a los ficheros las personas estrictamente autorizadas y el control y registro de dichos accesos, sino también a través de la elaboración de clausulados específicos para cada cargo y función en la empresa, en los que se determinarán las obligaciones de cada empleado, así como



las consecuencias de carácter laboral y responsabilidades que le correspondan por el incumplimiento de las normas de seguridad que debe aplicar.

3º Conocimiento de sus sistemas, la seguridad de los mismos y las carencias y riesgos que presentan. PROTECCIÓN REPORT realizará una revisión pormenorizada de sus sistemas, para la detección de amenazas y riesgos.

4º Adopción de medidas que ante sucesos que afecten a una parte importante de sus sistemas, permitan a su entidad continuar su actividad con el mínimo perjuicio para la misma. Medidas de carácter técnico y organizativo.

5º Que todo su personal tenga la formación adecuada para llevar a cabo las tareas que en materia de seguridad le corresponden, por razón del cargo que desempeñan. La formación de sus empleados será una pieza esencial en el rompecabezas de la seguridad de su empresa. Desde el máximo dirigente al empleado menos cualificado, deben tener claras sus tareas para preservar la información tratada. La formación alcanzará tanto al personal con funciones informáticas como al que no las tiene.

6º Mejora la Gestión de la entidad y de sus procesos internos. Todo ello como parte de un proyecto más amplio enfocado a la reconstrucción de la estructura organizativa y técnica de la entidad, acelerando y documentando procedimientos, perfeccionando los gestores de información, mejorando la atención al cliente, etc...

7º Cobertura legal ante perjuicios sobrevenidos. Actualmente, una empresa puede sufrir ataques internos y externos dirigidos a dañar sus sistemas o a extraer la información de la que dispone. El asesoramiento legal especializado es vital para poder perseguir a los que llevan a cabo estas conductas, para lo cual utilizaremos tanto la vía penal como la civil.

4- NORMATIVA APLICABLE A SU ORGANIZACION

- *“Ley Orgánica 15/1999, de 13 de diciembre de 1999, de Protección de Datos de Carácter Personal (L.O.P.D.)”*
- *“Ley Orgánica 5/1992, de regulación del tratamiento Automatizado de Datos de Carácter Personal (L.O.R.T.A.D.)” del año 1992 (por remisión de la L.O.P.D).*
- *R.D. 1720/2007, que desarrolla la Ley Orgánica 15/1999, de 13 de diciembre de Protección de Datos de Carácter Personal*
- *Reglamento de Medidas de Seguridad de los Ficheros Automatizados que Contengan Datos de Carácter Personal, Real Decreto 994/1999, de 11 de junio de 1999 (a cuya redacción alude el artículo 9.2 de la L.O.P.D.).*



- *Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.*
- *Instrucciones, Informes Jurídicos, Consultas y Jurisprudencia dictada por la AEPD, así como la normativa concreta que afecte al sector empresarial en que nos movamos.*

5- PLAN DE ACTUACIÓN

Para llevar a cabo todo el proceso, y de acuerdo a nuestra metodología para proyectos similares, las etapas a realizar serían las que se detallan a continuación:

A) DETERMINACIÓN DE LAS NECESIDADES DE LA ENTIDAD

- Identificación del nivel de seguridad adecuado de Ficheros y Bases de Datos.
- Indicación de las medidas de seguridad correspondientes al nivel exigido.
- Identificación de los mecanismos y procedimientos que deberían detallarse y contemplarse en el Documento de Seguridad.

B) ANÁLISIS DE LA SITUACIÓN ACTUAL

- Identificación de los ficheros objeto de estudio, analizando su estructura y modelo de datos, su finalidad y los procesos que los utilizan, el Responsable del Fichero, el método de obtención de datos, los tipos de soporte, la inscripción en el Registro General de la Agencia Estatal Protección de Datos.
- Usuarios: determinación de perfiles de trabajo y accesos de personal y terceros a los ficheros.
- Sistemas de Información: programas de tratamiento de los datos, procesos de identificación y autenticación para acceder a los datos.
- Equipos: número, ubicación, control de acceso.
- Procedimientos aplicados: información a interesados, acceso o cancelación, copias de seguridad, transmisión de información, etc.
- Sistemas y medidas de seguridad existentes: control de accesos, back-ups, soporte, transmisión de datos, etc.
- Información a interesados en el momento de obtención de los datos.

El análisis consiste, por lo tanto, en la realización de una revisión inicial de la situación de la entidad, orientada a la identificación de las acciones a realizar de acuerdo a los niveles de seguridad requeridos, con la finalidad de preparar, dirigir y canalizar el desarrollo del plan de actuación propiamente dicho.

C) PLAN DE ACTUACIÓN PROPIAMENTE DICHO

- Determinación de los ficheros y tipo de datos tratados, a los efectos de su calificación (nivel básico, medio o alto) para la adopción de las medidas de seguridad que les correspondan.
- Inscripción de ficheros con datos personales de la entidad en el Registro de la Agencia Española Protección de Datos (Art. 26.1 LOPD).
- Elaboración de una normativa de la entidad respecto a la seguridad de los ficheros con datos de carácter personal, conocida como “documento de seguridad” (Art. 9.1 LOPD y Art. 88 R.D. 1720 Reglam. Medidas Seguridad)
- Definición y puesta en práctica de procedimientos informáticos y organizativos que debe aplicar la entidad para la seguridad de los tratamientos que efectúa:
 - Procedimiento de identificación y autenticación.
 - Procedimiento de gestión de soportes.
 - Procedimiento de gestión de incidencias.
 - Procedimiento de copias de respaldo y seguridad.
 - Procedimiento de seguridad física.
 - Seguridad de telecomunicaciones.
- Realización de los contratos de encargo de tratamiento para cesiones de datos a terceros que presten un servicio a la entidad (Art. 12.2 LOPD).
- Adaptación documental en lo que afecta a la recogida y consentimiento del interesado para el tratamiento de datos de carácter personal (Art. 5 LOPD).
- Procedimientos de acceso, rectificación, modificación y cancelación de datos.
- Comprobación de la legitimidad de ficheros, proporcionalidad y carácter no excesivo de los tratamientos (Art. 4 LOPD).
- Adaptación de la página web a la Ley Orgánica de Protección Datos y Ley 34/2002, de Servicios de Sociedad de la Información y correo electrónico.
- Otras...

D) FORMACIÓN

Una vez adoptadas todas las medidas anteriormente descritas, es necesario, para garantizar el efectivo cumplimiento de todas ellas y la completa implantación de la protección de datos en la entidad, llevar a cabo una última fase de *Formación o Comunicación* orientada a:

- Proporcionar formación sobre la normativa de Protección de Datos a los Responsables de Fichero y Responsable/s de Seguridad.
- Proporcionar formación sobre la normativa de Protección de Datos al resto de la organización (Explicando y consensuando las funciones, obligaciones y responsabilidades derivadas de la normativa de Protección de Datos para todos los usuarios o empleados de la entidad en función del cargo o puesto que ocupan).
- Proporcionar formación específica acerca del Documento de Seguridad a los Responsables de Fichero y Responsable/s de Seguridad, quienes transmitirán posteriormente el proceso al resto de la organización, en un efecto en *cascada*.

Esta última fase de formación se desarrollará una vez implantadas todas las medidas necesarias para adaptar la entidad a la normativa vigente. Dicha formación se proporcionará por personal especializado en materia de protección de datos.

E) DETERMINACION DE MEDIDAS TÉCNICAS INFORMÁTICAS

PROTECTION REPORT prestará asesoramiento respecto a las medidas técnicas de carácter informático (programas o aplicaciones de seguridad que se consideren imprescindibles para la efectividad de los procedimientos legalmente exigidos) que sean necesarias para el total cumplimiento con la normativa sobre Protección de Datos de Carácter Personal. Sólo una vez realizado el análisis de la situación actual, se conocerá el alcance de las necesidades que a este respecto tiene la entidad y en el mismo se le pondrán de manifiesto claramente.

F) MANTENIMIENTO Y AUDITORIA

Plan de seguimiento anual y control de las Medidas adoptadas para asegurar el correcto cumplimiento de las obligaciones marcadas por la ley en el día a día y consiste principalmente en:

- 1) Atención de consultas y apoyo al responsable del tratamiento en las dudas que tenga en el ejercicio de sus tareas.
- 2) Modificaciones y nuevas Inscripciones de ficheros en el Registro de la AEPD.
- 3) Actualizaciones de todo tipo de documentación (documento seguridad, contratos con empresas que accedan a nuestros datos, cláusulas a clientes, etc ...)
- 4) Realización de los controles presenciales periódicos de los sistemas de tratamiento para verificar el cumplimiento del Reglamento y de los procedimientos e instrucciones vigentes en esta materia.
- 5) Asesoramiento jurídico continuo en caso de inspecciones de la A.E.P.D., o ante denuncias o reclamaciones de particulares a causa de una supuesta vulneración de la LOPD (dicho asesoramiento no incluye los servicios de defensa jurídica asistencial in situ durante procesos judiciales que podrán ser contratados adicionalmente en condiciones preferentes para el cliente).
- 6) Realización de la preceptiva auditoria bianual exigida por el Reglamento con una periodicidad máxima de dos años, informe que deberá quedar depositado en la empresa por si fuera requerido por la Agencia Española de Protección de Datos y que consta de tres fases que concluyen con el Informe de Auditoria. El Informe examina el tratamiento, eleva conclusiones y propone medidas correctoras.

Las tres fases en las que distribuimos el trabajo para la elaboración de un Informe de Auditoria objetivo y eficaz, son las siguientes:



I FASE. Petición de Documentos y revisión de programas, aplicaciones, procedimientos y medidas organizativas en la sede de la empresa, con entrevistas con responsables y empleados que realicen tratamientos de datos.

II FASE. Examen de documentación obtenida y trabajo en despacho.

III FASE. Entrega del Informe, con recomendaciones y medidas correctoras.

El objetivo del servicio es asumir la labor de que la entidad cumpla en todo momento la normativa de Protección de Datos, asumiendo una labor preventiva, formativa y de revisión para evitar posibles sanciones respecto a la normativa sobre protección de datos.

6- CERTIFICADO DE GARANTÍA

Mediante este Certificado de Garantía las empresas, asociaciones y profesionales, certifican el cumplimiento de las prescripciones legales mencionadas, pudiéndolos incorporar a sus documentos o páginas Web, y aseguran a los consumidores y usuarios el uso leal y lícito de sus datos personales.

7- ¿ POR QUÉ CONTRATAR CON PROTECTION REPORT?

- Porque prestamos única y exclusivamente este servicio, solamente de esa forma se consigue estar en el pequeño grupo de empresas punteras en este sector.

Añadiendo además una serie de ventajas:

- **GARANTIA DE CUMPLIMIENTO DE LA LEY:** cumplirá con las obligaciones exigidas por la L.O. 15/1999, de Protección de Datos y su normativa de desarrollo.
- **AMPLIA EXPERIENCIA:** Contrastada por nuestra amplia cartera de clientes distribuida por toda España (especialmente en Andalucía), con más de 10.000 ficheros inscritos en el Registro de la A.E.P.D.
- **SEGURO RESPONSABILIDAD CIVIL EN VIGOR QUE CUBRE LA SANCIÓN MÁS ALTA QUE PUEDA IMPONER LA A.E.P.D.:** que respalda la calidad de nuestro trabajo y responderá por una defectuosa prestación de nuestros servicios.
- **ATENCIÓN PERSONALIZADA Y DISPONIBILIDAD:** Nos adaptamos a su situación, dándole una asistencia personalizada presencial permanente, desplazándonos hasta sus instalaciones para la solución de problemas de la manera más eficiente.
- **FORMACIÓN:** Todo su personal tendrá la formación adecuada para garantizar la protección de datos de su empresa.



- **CONFIANZA:** Sus clientes, asociados, etc, reforzarán la confianza en su entidad ante la garantía de confidencialidad de sus datos y transacciones.
- **COBERTURA LEGAL.** Dispondrá de cobertura legal ante perjuicios sobrevenidos a causa de una supuesta vulneración de la L.O.P.D.
- **CONSULTORA EN PROCESO DE CERTIFICACIÓN COMO AUDITOR INFORMÁTICO C.I.S.A.:** Que nos va a destacar del resto de consultoras andaluzas especializadas en Protección de Datos.

8- SITUACIÓN ACTUAL DE LA EMPRESA

Gracias a la información facilitada, en un primer análisis de su entidad hemos detectado las siguientes infracciones que le facilitamos a continuación:

1)	Carece de ficheros inscritos en el R.G.P.D., Infracción LEVE,
2)	Se incumplen los deberes legales para con los terceros con acceso a ficheros con datos personales de la empresa, Infracción GRAVE,
3)	Se recogen datos personales de clientes, trabajadores, proveedores, etc, sin cumplir con los deberes de información y consentimiento, Infracción LEVE,
4)	No se cumplen con las medidas de seguridad de índole técnica y organizativas que exige el RMS, Infracción GRAVE,

9- PLANING DE TRABAJO

El Proyecto de cumplimiento de la L.O.P.D. y L.S.S.I. que le presentamos para su empresa tiene una duración aproximada de entre 30 y 45 días. La distribución de los plazos se distribuirá conforme a los siguientes criterios:

FASE 1.- ENTREVISTAS 1 al 5º día.

FASE 2.- ANÁLISIS E INSCRIPCIÓN DE FICHEROS, del 5º al 10º día.

FASE 3.- REALIZACIÓN DE INFORMES, del 10º al 15º día.

FASE 4.- REUNIÓN INFORMATIVA (ENTREGA DOCUMENTACION, FORMACION, ETC ...), del 15º al 20º día.

FASE 5.- CERTIFICADO Y CONSULTAS, del 20º al 30º día.

PARA MAS INFORMACION PUEDEN CONTACTAR CON NOSOTROS EN:



PROTECTION REPORT S.L.



ESPECIALISTAS EN PROTECCIÓN DE DATOS Y SEGURIDAD DE LA INFORMACIÓN

PASEO DEL VIOLON, 8. LOCAL - 18006 - GRANADA

*TORNEO PARQUE EMPRESARIAL, C/ ARQUITECTURA, 4. TORRE 10, PLANTA 6ª, MODULO 4
41015 - SEVILLA*

VALLE DE PINARES LLANOS, 8B, 2º B - 28009 - MADRID

Tlf. Atención al Cliente: 958 294383 / 902 364585

www.protectionreport.com

info@protectionreport.com

