DOSSIER INFORMATIVO A CLIENTES
EN MATERIA DE PROTECCIÓN DE DATOS

INDICE

ITnor Tecnologías de la Información del Noroeste

Asesor Autorizado PROGESDATOS
JOSE GARRIDO
M: 646 207 380
josegarrido@progesdatos.com

San Paio, 1 Entlo. B
36680 – A Estrada
T: 986 57 30 05 – Fax: 986 57 38 24
sanmartingestion@sanmartingestion.es
www.sanmartingestion.es

1- ¿Qué es la Ley Orgánica de Protección de Datos y porqué tienen que adaptarse las empresas, organismos y organizaciones a la LOPD?

- La ley Orgánica 15/1999 de 13 de diciembre de Protección de Datos de Carácter Personal, (L.O.P.D.), es una Ley Orgánica española que 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, intimidad y privacidad personal y familiar. Quedan excluidos por tanto cualquier tipo de datos relativos a personas jurídicas.

- Su objetivo principal es regular el tratamiento de los datos y ficheros, de carácter personal, independientemente del soporte en el cual sean tratados (manual o automatizado), los derechos de los interesados sobre esos datos y las obligaciones de aquellos que los crean o tratan.

- La Ley Orgánica de Protección de Datos obliga a toda persona física o jurídica (organismos tanto privados como públicos) que dispongan de datos de carácter personal o ficheros de sus empleados, clientes, proveedores, etcétera a implantar una serie de medidas técnicas y organizativas que garanticen la confidencialidad de estas informaciones.

1- Normativa Aplicable además de la L.O.P.D.:

- Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, inició el desarrollo de la legislación en materia de protección de datos e impuso la obligación de su trasposición a todos los estados miembros, para garantizar el derecho fundamental a la autodeterminación informativa.

- Reglamento de Desarrollo, Real Decreto 1720/2007.

- Ley Orgánica 34/2002 de servicios de la Sociedad de la información y el Comercio electrónico.

2- ¿Quién vela por su cumplimiento?

- La Agencia Española de Protección de Datos: es un organismo público independiente de las administraciones públicas, con personalidad jurídica propia, encargada de hacer cumplir la normativa en protección de datos.
Se financia exclusivamente con las sanciones que impone.

- Sanciones que impone:

. Infracciones leves: 900 a 40.000 euros.
. Infracciones graves: 40.001 a 300.000 euros.
. Infracciones muy graves: 300.001 a 600.000 euros

3- Obligaciones que impone:

a) Obligación de redactar el Documento de Seguridad en el que se recojan las medidas de seguridad que tiene que adoptar la empresa. Contenido;

√ Ámbito de aplicación del documento especificando los recursos protegidos: ficheros que contengan datos de carácter personal, soportes y equipos empleados para el tratamiento de datos de carácter personal, personas que intervienen en el tratamiento y los locales en los que se ubican.

√ Medidas de seguridad que garanticen el nivel de seguridad correspondiente: (básico, medio y alto):

-Funciones y obligaciones del personal: las funciones y obligaciones de los usuarios con acceso a los sistemas de información de la entidad deben estar claramente definidas.

-Registro de incidencias: procedimiento de registro de las incidencias que afecten a datos personales

-Control de acceso: relación actualizada de usuarios, perfiles de usuario y accesos autorizados para cada uno de ellos.

-Gestión de soportes y documentos: los soportes que contengan datos personales deberán ser inventariados.

-Identificación y autenticación: sistema de identificación de usuarios y periodicidad en el cambio de las contraseñas (como máximo anual).

-Copias de respaldo y recuperación: procedimiento de realización de las copias de respaldo (realización como mínimo semanal).

-Responsable de Seguridad: a partir del nivel medio, habrá que designar a una persona para coordinar y controlar las medidas del Documento de Seguridad.

-Auditoría: a partir del nivel medio, cada dos años al menos, es obligatoria la verificación interna y externa del cumplimiento de las medidas de seguridad.

-Telecomunicaciones: si se transmiten datos personales de nivel alto a través de comunicaciones electrónicas, se tendrán que utilizar métodos de cifrado.

- Régimen de trabajo fuera de los locales en los que esté ubicado el fichero: protocolo de actuación para los ficheros contenidos en dispositivos que puedan salir de los locales de la empresa.

- Ficheros temporales: Los ficheros creados para la realización de trabajos temporales o auxiliares deberán cumplir con el nivel de seguridad que corresponda y ser borrados o destruidos una vez que hayan dejado de ser necesarios.

√ Procedimiento para hacer efectivos los derechos de los afectados.

√ Firma de contratos de acceso a datos por cuenta de terceros que correspondan.

√ Cláusulas legales referentes a recursos humanos, al uso de internet, correo electrónico, compromisos de confidencialidad, etc.

b) Inscripción en el Registro General de Protección de Datos de los ficheros que contengan los datos personales que esté tratando la empresa. Es de vital importancia puesto que si no se declaran todos los ficheros que se están utilizando, se estará incurriendo en una infracción objeto de sanción de las contempladas en la Ley y será lo primero que consulte la Agencia en caso de que haya una denuncia o una inspección de oficio. (infracción leve con sanción que puede oscilar entre los 900 y los 40.000 euros).

c) Aplicar las medidas de seguridad recogidas en el Documento de Seguridad:

√ Interesados a los que se soliciten datos personales: Cumplir con el deber de información sobre la finalidad del tratamiento de los mismos, cuáles son sus derechos en caso de que no se desee que sus datos sigan siendo tratados y cómo puede ejercitarlos.

√ Empleados: consentimientos necesarios para tratar los datos de carácter personal de los empleados, asegurar su confidencialidad, formación al personal con acceso a datos personales…

√ Proveedores: información del procedimiento con los proveedores (recoger el consentimiento exigido en los casos necesarios).

√ Encargados de tratamiento: Contratos de prestación de servicios.
Redactar los documentos necesarios para legitimar las cesiones de datos que se realicen, redactar los contratos de tratamientos de datos por parte de terceros…).

4- Beneficios que aporta estar adaptado:

a) Seriedad: La empresa/organización queda adaptada a una norma de obligado cumplimiento.

b) Organización: Se cuenta con toda la documentación que la Agencia Española solicita en caso de ser objeto de una inspección.

c) Bueno gobierno: Se mejora la imagen de la empresa/organización adaptada: los clientes verán que están contratando con una empresa moderna con inquietud por las nuevas tecnologías y sensibilizada con el respeto de los derechos de las personas y con el cumplimiento de la normativa.

d) Marketing: Tener el consentimiento de clientes y proveedores le da a la empresa y al profesional la posibilidad de utilizar sencillas herramientas de marketing (fax, correo electrónico…) sin riesgos legales, así como una imagen favorable al respetar los derechos individuales.

e) Se evitan sanciones directas o el apercibimiento como medida no sancionadora para corregir la irregularidad cometida. (Es una medida excepcional y limitada de la Agencia, la cual requiere la adopción de las medidas correctoras adecuadas con carácter precio a la sanción siempre que no se trate de infracciones muy graves o el sujeto haya sido sancionado o apercibido con anterioridad).

2- Ley de Servicios de la Sociedad de la información y Comercio Electrónico.

1- Resumen de Obligaciones (Ley Orgánica, 34/2002):

- Análisis sobre el cumplimiento de la LSSI-CE.
- Registro de nombre de dominio: trámites necesarios para la inscripción pertinente a través de agente registrador autorizado.
- Cláusulas y datos de inclusión necesaria en la Web para cumplir con las obligaciones de información:
  - Aviso legal para la Web.
  - Modelo para los enlaces (derechos de propiedad intelectual, links o hiperenlaces).
  - Condiciones generales de contratación Web.

3- Nuestra Empresa: PROGESDATOS.

1- Descripción

PROGESDATOS es un despacho especializado en servicios de Consultoría, Auditoría y Outsourcing. Operamos en todo el territorio nacional. Utilizar nuestros servicios significa contar con el apoyo de un equipo multidisciplinar, integrado por profesionales con una dilatada experiencia en el sector.

2- ¿Por qué nosotros?

- Por nuestra profesionalidad y experiencia: equipo de trabajo único constituido por abogados especialistas en LOPD y LSSI-CE encargados de la parte jurídica y auditores informáticos y consultores de seguridad encargados de la parte organizativa y técnica.
- Por nuestra especialización: puesto que damos única y exclusivamente este tipo de servicios.
- Por la personalización de nuestras actuaciones: nos permite conocer las necesidades reales que tienen nuestros clientes.
- Por la completa gama de servicios: cubriendo cualquier necesidad en materia de protección de datos.
- Porque adaptamos y no solo redactamos la documentación
- Por nuestra inmejorable relación calidad/precio.
- Por el seguimiento: nuestra metodología nos permite asegurar que nuestros clientes quedan correctamente adaptados a la Ley.

3- Servicios

A) Gestiones:

1- Alta de Ficheros
2- Redacción del Documento de Seguridad
3- Auditoría Anual
4- Controles de Seguimiento
5- Redacción de la Documentación Jurídica
6- Cláusulas legales, contratos de prestación de servicios
7- Acreditación de adaptación a la L.O.P.D. como valor añadido para la empresa.

B) Prestaciones:

1- Defensa Jurídica
2- Asesoría Jurídica
3- Gestión de reclamaciones ante la AEPD
4- Servicio personal y presencial
5- Profesionalidad
6- Especialización
7- Años de experiencia
8- Seguro de Responsabilidad Civil (RC)

Implantar un Servicio Personalizado de Adaptación a la L.O.P.D con Progesdatos protección y gestión de datos

La propuesta que le puede solicitar al asesor autorizado (ITnor) **desarrollaría el proyecto en su conjunto**. La parte jurídica es llevada por **abogados especialistas** en LOPD y LSSI-CE mientras que la parte organizativa y técnica es realizada por **auditores informáticos y consultores de seguridad**.

Todo ello con un equipo de trabajo único y con una experiencia de muchos años respaldado por la figura de **Carlos Martínez García**, abogado especialista en materia de protección de datos, con una **experiencia profesional** de casi diez años **dedicada en exclusiva** a esta materia y la intervención personal en **grandes proyectos públicos y privados** para algunos clientes como la Sociedad de Prevención de FREMAP, el Excmo. Concello de A Estrada, el grupo UNILEVER, el grupo THALES/ALCATEL, la CAJA RURAL DE CIUDAD REAL, el grupo CLESA ó ING, entre otros.

Objetivos y pilares de la Adaptación

- **Adecuar y adaptar** a la empresa a toda la reglamentación impuesta por la Ley Orgánica de Protección de Datos – LOPD – y su Reglamento de Desarrollo.
- **Declarar los ficheros** con los datos de carácter personal resultantes y crear los Documentos de Seguridad en base a los ficheros declarados finalmente para cada una de las áreas del alcance del proyecto.
- Definir un **plan de acción** para implantar las medidas de seguridad informática y las de índole legal.
- **Concienciar** al personal con responsabilidades en el tratamiento de datos de carácter personal.
- Establecer un **plazo** para realizar la **auditoría** obligatoria en caso de que fuera necesario.

ITnor Tecnologías de la Información del Noroeste
Asesor Autorizado PROGESDATOS
JOSE GARRIDO
M: 646 207 380
josegarrido@progesdatos.com
San Paio, 1 Entlo. B
36680 – A Estrada
T: 986 57 30 05 – Fax: 986 57 38 24
sanmartingestion@sanmartingestion.es
www.sanmartingestion.es

- El enfoque con el que realizamos los proyectos de la LOPD, se basa en tener en cuenta que para conseguir una adecuada adaptación es necesario abordarla desde tres pilares claramente definidos y mutuamente integrados:

  - ✓ Organizativo
  - ✓ Técnico
  - ✓ Jurídico

- Evaluación de la estructura de la organización de seguridad:

  - Organización general.
  - Controles permanentes.
  - Planes de informática de seguridad.
  - Reglamento y auditoría.
  - Personal informático.

- Análisis de la situación actual de las medidas organizativas de protección de datos personales y desarrollo de medidas, normas, procedimientos, reglas y estándares internos de seguridad, definidos en el Documento de Seguridad.

- Análisis del nivel de formación del personal y definición de sus funciones y obligaciones para garantizar el cumplimiento de la normativa.

- Concienciación del correcto uso de los datos de carácter personal y de las buenas prácticas en materia de su protección.

- Análisis de seguridad de las instalaciones y sistemas de las diferentes ubicaciones indicadas en el alcance del proyecto, donde existen datos de carácter personal.

- Normativa de Seguridad de obligado cumplimiento. Documento de Seguridad.

  - o Inventario de recursos a proteger (datos, equipos, sistemas, soportes, personas, usuarios, etc.).
  - o Medidas y normas, procedimientos de control sobre cada Recurso inventariado.
  - o Funciones y obligaciones del personal.
  - o Procedimiento de notificación y gestión de incidencias.
  - o Medidas del Responsable del fichero que garanticen que el documento es conocido y cumplido por el personal.
  - o Documentación de aplicaciones y estructura de datos personales.
  - o Arquitectura de seguridad lógica y descripción de accesos y derechos.
  - o Autenticación y control de acceso lógico.
  - o Control de soportes de información y registro de salida y entrada.
  - o Dispositivos móviles (Portátiles).
  - o Realización de las Copias de seguridad y su recuperación.
  - o Controles periódicos y auditorías. Procedimientos.
  - o Control de acceso físico a las instalaciones (en el ámbito del reglamento) .

- Principio de información y consentimiento.

  - Información, tanto en el proceso de recogida inicial de los datos como, en su caso, durante el transcurso de los distintos tratamientos y consentimiento cuando es necesario.

- Principio de calidad.
  - Tipología de los datos y su actualización.
  - Datos personales que se almacenan, su antigüedad y si disponen de procedimientos de cancelación y bloqueo.

- Derechos en materia de protección de datos (acceso, rectificación, cancelación y oposición).

- Posición ante la solicitud de un ciudadano ejerciendo cualquiera de los derechos de acceso, rectificación, cancelación u oposición.

- Inscripción de ficheros.

- Datos especialmente protegidos.

- Si disponen del consentimiento respectivo o si la recogida y tratamiento de los mismos obedece a disposiciones legales.

- Cesiones de datos.

  - o Comunicaciones de datos a terceros y si se recaba el necesario consentimiento o existe una habilitación legal.

- Prestaciones de servicios.

Anexo - INFORMACION SOBRE EL DOCUMENTO DE SEGURIDAD

Índice:

1- Introducción:

El Reglamento de Medidas de Seguridad tiene por objeto establecer las medidas de índole técnica y organizativa necesarias para garantizar la seguridad que deben reunir los ficheros, los centros de tratamiento, locales, equipos, sistemas, programas y las personas que intervengan en el tratamiento de los datos de carácter personal.
Por lo tanto las medidas técnicas y organizativas desarrolladas y descritas en el documento de seguridad tienen como finalidad asegurar los datos de carácter personal evitando concretamente:

- La alteración de los datos
- La pérdida de los datos
- El tratamiento o acceso no autorizado
- Vulneración

2- Normativa en la que se fundamenta la adaptación de protección de datos:

- Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, inició el desarrollo de la legislación en materia de protección de datos e impuso la obligación de su trasposición a todos los estados miembros, para garantizar el derecho fundamental a la autodeterminación informativa.
- Ley Orgánica, 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
- Reglamento de Desarrollo, Real Decreto 1720/2007.

3- Obligatoriedad de elaboración de Documento de Seguridad dentro de la citada normativa

El Documento de Seguridad es un documento de obligado cumplimiento para todas las personas físicas o jurídicas que posean datos personales y los sometan a cualquier tipo de tratamiento. En él se establecen las normas, procedimientos y estándares encaminados a garantizar el nivel de seguridad que exige la normativa, establece procedimientos organizativos y técnicos, copias de seguridad, registro de incidencias y gestión de soportes .

Las medidas de seguridad son diferentes según la naturaleza de los datos. Por ello, se establecen tres niveles de seguridad (básico, medio, alto) y en el Documento de Seguridad se contienen todas las medidas de seguridad obligatorias del nivel de seguridad correspondiente.

Todas las personas o empresas que posean datos personales de clientes, proveedores, empleados, CV, etc., aunque sea de una sola persona y aunque se trate del nombre y los apellidos, está dentro del ámbito de aplicación de la Ley Orgánica de Protección de Datos (LOPD) y esto viene determinado jurídicamente en los artículos 88 y siguientes del Reglamento de desarrollo de la Ley Orgánica de protección de Datos 1720/2007.

4- Artículo 88. El documento de seguridad:

1. El responsable del fichero o tratamiento elaborará un documento de seguridad que recogerá las medidas de índole técnica y organizativa acordes a la normativa de seguridad vigente que será de obligado cumplimiento para el personal con acceso a los sistemas de información.

2. El documento de seguridad podrá ser único y comprensivo de todos los ficheros o tratamientos, o bien individualizado para cada fichero o tratamiento. También podrán elaborarse distintos documentos de seguridad agrupando ficheros o tratamientos según el sistema de tratamiento utilizado para su organización, o bien atendiendo a criterios organizativos del responsable. En todo caso, tendrá el carácter de documento interno de la organización.

3. El documento deberá contener, como mínimo, los siguientes aspectos:

a) Ámbito de aplicación del documento con especificación detallada de los recursos protegidos.

b) Medidas, normas, procedimientos de actuación, reglas y estándares encaminados a garantizar el nivel de seguridad exigido en este reglamento.

c) Funciones y obligaciones del personal en relación con el tratamiento de los datos de carácter personal incluidos en los ficheros.

d) Estructura de los ficheros con datos de carácter personal y descripción de los sistemas de información que los tratan.

e) Procedimiento de notificación, gestión y respuesta ante las incidencias.

f) Los procedimientos de realización de copias de respaldo y de recuperación de los datos en los ficheros o tratamientos automatizados.

g) Las medidas que sea necesario adoptar para el transporte de soportes y documentos, así como para la destrucción de los documentos y soportes, o en su caso, la reutilización de estos últimos.

4. En caso de que fueran de aplicación a los ficheros las medidas de seguridad de nivel medio o las medidas de seguridad de nivel alto, previstas en este título, el documento de seguridad deberá contener además:

a) La identificación del responsable o responsables de seguridad.

b) Los controles periódicos que se deban realizar para verificar el cumplimiento de lo dispuesto en el propio documento.

5. Cuando exista un tratamiento de datos por cuenta de terceros, el documento de seguridad deberá contener la identificación de los ficheros o tratamientos que se traten en concepto de encargado con referencia expresa al contrato o documento que regule las condiciones del encargo, así como de la identificación del responsable y del período de vigencia del encargo.

6. En aquellos casos en los que datos personales de un fichero o tratamiento se incorporen y traten de modo exclusivo en los sistemas del encargado, el responsable deberá anotarlo en su documento de seguridad. Cuando tal circunstancia afectase a parte o a la totalidad de los ficheros o tratamientos del responsable, podrá delegarse en el encargado la llevanza del documento de seguridad, salvo en lo relativo a aquellos datos contenidos en recursos propios. Este hecho se indicará de modo expreso en el contrato celebrado al amparo del artículo 12 de la Ley Orgánica 15/1999, de 13 de diciembre, con especificación de los ficheros o tratamientos afectados.

En tal caso, se atenderá al documento de seguridad del encargado al efecto del cumplimiento de lo dispuesto por este reglamento.

7. El documento de seguridad deberá mantenerse en todo momento actualizado y será revisado siempre que se produzcan cambios relevantes en el sistema de información, en el sistema de tratamiento empleado, en su organización, en el contenido de la información incluida en los ficheros o tratamientos o, en su caso, como consecuencia de los controles periódicos realizados. En todo caso, se entenderá que un cambio es relevante cuando pueda repercutir en el cumplimiento de las medidas de seguridad implantadas.

8. El contenido del documento de seguridad deberá adecuarse, en todo momento, a las disposiciones vigentes en materia de seguridad de los datos de carácter personal.

5- Artículo 95. Responsable de seguridad:

En el documento de seguridad deberán designarse uno o varios responsables de seguridad encargados de coordinar y controlar las medidas definidas en el mismo.

Esta designación puede ser única para todos los ficheros o tratamientos de datos de carácter personal o diferenciada según los sistemas de tratamiento utilizados, circunstancia que deberá hacerse constar claramente en el documento de seguridad.

En ningún caso esta designación supone una exoneración de la responsabilidad que corresponde al responsable del fichero o al encargado del tratamiento de acuerdo con este reglamento.
No disponer del Documento de Seguridad supone una infracción grave tipificada en el Art. 44.3.h) de la LOPD, sancionada con una multa de 60.000 a 300.000 Euros.

6- Conclusiones

<u>Las obligaciones en el tratamiento de los datos</u>

Todo el personal debe conocer y cumplir las medidas de índole técnica y organizativa necesarias para garantizar la seguridad de los datos de carácter personal de conformidad con el nivel de seguridad asignado y que constan en el Documento de Seguridad. Tanto para los tratamientos automatizados como no automatizados con el fin de evitar la pérdida, uso ilícito o robo de la información.

Quienes participen en el tratamiento de los datos deben guardar confidencialidad incluso después de terminadas sus relaciones con el responsable del fichero

Por todo esto y como conclusión hay que decir que el Documento de Seguridad es el soporte en el que se especifican las medidas que se han adoptado para proteger los datos personales, pues el artículo 9 LOPD impone el principio de seguridad de los datos y es obligatorio tenerlo en todas las empresas que traten datos de carácter personal.