CADERNOS PRÁCTICOS DE XESTIÓN

A qué me obriga a lei de protección de datos

XUNTA DE GALICIA

A qué me obriga a Lei de Protección de Datos

CADERNOS PRÁCTICOS. XESTIÓN EMPRESARIAL

AUTOR	PROMOVE CONSULTORIA E FORMACIÓN SLNE
COORDINACIÓN	Roberto Vieites Rodríguez (CEEI Galicia, S.A)
EDITA	C.E.E.I GALICIA, S.A. (BIC GALICIA)
PORTADA	Producciones khartum SL
DESEÑO E MAQUETACIÓN	gifestudio.com
(C) da edición	C.E.E.I GALICIA, S.A. (BIC GALICIA)
DEPÓSITO LEGAL	
IMPRIME	

Santiago de Compostela, CEEI GALICIA, S.A. 2012

Quedan estrictamente prohibidos sen o consentimento por escrito ou autorización dos titulares do "copgright" baixo as penas previstas pola lei, a reprodución total ou parcial desta obra por calquera medio ou procedemento, incluidas a repografía e o tratamento informático e a súa distribución a través de aluguer ou préstamo de exemplares dela mediante aluguer ou préstamos públicos..

ÍNDICE

1. INTRODUCIÓN 5
1.1 Para saber mais 9

2. A PROTECCIÓN DE DATOS 11
2.1 Axencia Española de Protección de Datos (AEPD) 13
2.2 A Lei Orgánica de Protección de Datos (LOPD) 14
2.3 A qué me obriga a LOPD? 15

3. CONCEPTOS BÁSICOS SOBRE A PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL 17
3.1 Os ficheros de datos personais 19
3.2 Quen é quen na protección de datos 20
3.3 Actuacións sobre os datos de carácter personal 20

4. INSCRIPCIÓN DOS FICHEIROS 23
4.1 Que se debe de facer antes de inscribir un ficheiro 25
4.2 Modelos de cláusulas tipo 27
4.3 Cómo inscribir os ficheros 28
4.4 Modificación e supresión de ficheiros 32

5. A SEGURIDADE DOS DATOS DE CARÁCTER PERSONAL 33
5.1 Os niveis de seguridade e os datos aos que se aplica 35
5.2 Documento de seguridade 36
5.3 Medidas de seguridade 38
5.4 Ficheiros e tratamentos non automatizados 43
5.5 Funcions e obligacions do persoal 44
5.6 Controis: Auditoría e controis periódicos 46
5.7 Modelos de formulario 47

6. DEREITOS DOS TITULARES DOS DATOS (A.R.C.O.) 49
6.1 Disposicións comuns 51
6.2 Derecho de acceso 53
6.3 Dereito de rectificación e cancelación 55
6.4 Dereito de oposición 56
6.5 Tutela dos derechos e indemnización 58
6.6 Modelo de formulario para o exercicio de dereitos ARCO 59

7. ACCESO A DATOS POR CONTA DE TERCEIROS E PRESTACIÓN DE SERVIZOS SEN ACCESO A DATOS 61
7.1 Acceso a datos por conta de terceiros 63
7.2 Prestacións de servizos sen acceso a datos persoais 64

8. PARTICULARIDADES DE DETERMINADOS TIPOS DE FICHEIROS 65
8.1 Ficheiros de información sobre solvencia patrimonial ou crédito 67
8.2 Tratamento de datos relativos ás obrigas dinerarias 67
8.3 Tratamento para actividades de publicidade e prospección comercial 69

9. TRANSFERENCIAS INTERNACIONAIS DE DATOS 73
9.1 Autorización e notificación 75
9.2 Transferencias a Estados que non proporcionen un nivel axeitado de protección 76
9.3 Procedemento de autorización transferencias internacionais de datos 77

10. INFRACCIÓNS E SANCIONS 79
10.1 Infraccións en materia de protección de datos de carácter persoal 81
10.2 Sancións en materia de protección de datos de carácter persoal 83

11. A PÁXINA WEB DE LA AEPD 85
12. CONSELLOS E RECOMENDACIÓNS 89
13. BIBLIOGRAFÍA 93

1 Introdución

1 Introdución

Introdución

Esta publicación forma parte da colección de **"Cadernos Prácticos de Xestión empresarial",** un novo recurso que Bic Galicia pon a disposición de emprendedores, empresarios e técnicos e apoio á creación de empresas.

A colección está integrada por unha serie documentos nos que se abordan distintas áreas temáticas sobre actividades relacionadas coa xestión empresarial:

- Desenvolver a política comercial da empresa e medir a súa efectividade.
- Deseñar a planificación estratéxica da empresa.
- Mellorar a posta en marcha e seguimento da política de recursos humanos.
- Xestionar os recursos financeiros.
- Implementar elementos 2.0 na empresa.
- Etc.

Na súa elaboración utilizáronse as publicacións Bic Galicia, hibridando os seus distintos contidos para crear un novo produto que dea resposta a preguntas ou temas concretos e específicos da xestión empresarial.

Por iso, todos os cadernos prácticos contan cun apartado específico no que se indica que ferramentas de Bic Galicia permitirán ampliar información sobre o tema analizado.

Metodoloxía

O proceso de elaboración dos cadernos, desde o punto de vista metodolóxico, baseouse en:

- a utilización de fontes secundarias, especialmente aquelas ferramentas, publicacións e documentos desenvolvidos e deseñados por Bic Galicia e outras fontes secundarias especializadas sempre que o contido destas achegue valor engadido ao caderno;

- a utilización de información obtida directamente a través de fontes de información primaria, concretamente achegas, opinións, consellos e suxestións realizadas por expertos/as na materia tratada no caderno.

A través desta nova colección, o Bic Galicia pretende:

- Responder de forma concreta e específica ás demandas de información ou dúbidas das persoas emprendedoras e empresarios/as facilitando o acceso á información desagregada en diferentes publicacións.

- Mellorar a difusión e o coñecemento dos recursos xa existentes de Bic Galicia, que serían as fontes sobre as que ampliar información e afondar no tema que se analiza.

- Facilitar a xestión empresarial e a posta en marcha de medidas e accións concretas necesarias no ámbito empresarial.

- Optimizar o uso dos seus recursos recuperando e reutilizando a súa base de publicacións para desenvolver novos contidos que respondan a novas necesidades de emprendedores, empresarios e técnicos de promoción económica.

Obxectivos deste caderno

Este caderno recolle aspectos básicos da xestión e aplicación da Lei orgánica 15/1999 do 13 de decembro, de protección de datos de carácter persoal nas empresas. Explícanse de forma sinxela os principais aspectos que regula a norma ademais de presentar modelos tipo para algunha das accións que se deben realizar::

- Conceptos básicos.

- A xestión de ficheiros e a súa seguridade.

- Os dereitos dos titulares dos datos.

- Trasferencias internacionais de datos.

- Sancións.
- Etcétera..

1.1 Para saber máis

Para ampliar a información sobre a Lei orgánica de protección de datos e sobre a súa xestión, obrigas e sancións para os empresarios, poderanse consultar os seguintes recursos de Bic Galicia no seu portal www.bicgalicia.org.

- Fichas informativas. Protección de datos
- *Manual práctico de xestión: Conceptos xurídicos básicos*

2 A protección de datos

2 A protección de datos

2.1 Axencia Española de Protección de Datos (AEPD)

Natureza e funcións:

A Axencia Española de Protección de Datos é, tal e como se recolle no Real decreto 428/1993, do 26 de marzo, polo que se aproba o Estatuto da Axencia Española de Protección de Datos, un ente de dereito público, con personalidade xurídica propia e plena capacidade pública e privada, que actúa coa plena independencia das Administracións públicas no exercicio das súas funcións, relacionándose co Goberno a través do Ministerio de Xustiza.

A súa principal función é velar polo cumprimento da lexislación sobre protección de datos e controlar a súa aplicación, en especial que os cidadáns poidan exercer os dereitos de información, acceso, rectificación, oposición e cancelación dos seus datos de carácter persoal e o control do cumprimento por parte dos responsables dos seus ficheiros das súas obrigas.

Entre as súas funcións máis importantes están a de inscribir os ficheiros de datos de carácter persoal no Rexistro Xeral de Protección de Datos, atender as peticións e reclamacións formuladas polas persoas afectadas, requirir os responsables e os encargados dos tratamentos para que adopten as medidas necesarias para a adecuación do tratamento de datos ás disposicións da Lei orgánica de protección de datos, realizar labores de inspección sobre os ficheiros que teñan datos de carácter persoal e exercer a potestade sancionadora.

Esa facultade de sancionar, unida a que as infraccións poden ser sancionadas con multas que van dende os 900 ata os 600.000 euros, fan que a obriga legal de protección dos datos de carácter persoal adquira unha dimensión similar dentro da empresa ás obrigas fiscais ou da Seguridade Social.

Normativa reguladora:

- Lei orgánica 15/1999, do 13 de decembro, de protección de datos de carácter persoal.
- Real decreto 1720/2007 polo que se aproba o Regulamento de desenvolvemento da Lei orgánica 15/1999, do 13 de decembro, de protección de datos de carácter persoal.
- Real decreto 428/1993, do 26 de marzo, polo que se aproba o Estatuto da Axencia Española de Protección de Datos.

2.2 A Lei orgánica de protección de datos (LOPD)

Antecedentes

Esta lei ten o seu precedente na Lei orgánica 5/1992, do 29 de outubro, de regulación do tratamento automatizado dos datos de carácter persoal, a cal nacía para facer fronte aos riscos que para os dereitos da personalidade pode supoñer a recolección e o tratamento de datos por medios informáticos; o avance da tecnoloxía puxo de manifesto que nunha sociedade cada vez máis conectada e con maior capacidade de almacenamento de datos era case imposible conseguir borrar "a nosa historia"; polo que se facía imprescindible articular modos para protexer a honra e a intimidade das persoas. Non obstante, aquela primeira lei, que tiña por obxecto limitar o uso da informática e outras técnicas e medios de tratamento automatizado dos datos de carácter persoal, viuse pronto superada polo avance das novas tecnoloxías e en especial pola expansión da Internet.

A ley

A Lei orgánica 15/1999, do 13 de decembro, de protección de datos de carácter persoal (en diante, LOPD), entrou en vigor o 14 de xaneiro do ano 2000, e ten por obxecto garantir e protexer, no que concirne ao tratamento dos datos persoais, as liberdades públicas e os dereitos fundamentais das persoas físicas e, especialmente, da súa honra e intimidade persoal e familiar.

Cando se aplica a lei?

- Cando o tratamento sexa efectuado en territorio español no marco das actividades dun establecemento do responsable do tratamento (a práctica totalidade das empresas que operan no noso país).
- Cando ao responsable do tratamento non establecido en territorio español lle sexa de aplicación a lexislación española en aplicación de normas de Dereito Internacional Público.
- Cando o responsable do tratamento non estea establecido en territorio da Unión Europea e utilice no tratamento de datos medios situados en territorio español, salvo que tales medios se utilicen unicamente con fins de tránsito.

A lei NON se aplica a:

- Aos ficheiros mantidos por persoas físicas no exercicio de actividades exclusivamente persoais ou domésticas.
- Aos ficheiros sometidos á normativa sobre protección de materias clasificadas.
- Aos ficheiros establecidos para a investigación do terrorismo e de formas graves de delincuencia organizada. Non obstante, nestes supostos, o responsable do ficheiro comunicará previamente a existencia deste, as súas características xerais e a súa finalidade á Axencia Española de Protección de Datos.

Desenvolvemento da lei

A lei é desenvolvida polo Real decreto 1720/2007, do 21 de decembro, polo que se aproba o Regulamento de desenvolvemento da Lei orgánica 15/1999 do 13 de decembro, de protección de datos de carácter persoal.

2.3 A que me obriga a LOPD?

- A notificar á Axencia Española de Protección de Datos (AEPD) a creación de ficheiros de datos de carácter persoal e a inscribir os ficheiros no Rexistro Xeral de Protección de Datos.
- A informar previamente as persoas cuxos datos se solicitan.
- A solicitar o consentimento das devanditas persoas, tanto para o tratamento dos datos persoais coma para proceder a cedelos a terceiros.
- A establecer as medidas de seguridade necesarias para protexer os datos de carácter persoal.
- A regular mediante un contrato a realización de tratamentos dos datos por conta dun terceiro.
- A atender debidamente o exercicio dos dereitos de acceso, rectificación, cancelación e oposición polos interesados.
- A formar o responsable de seguridade e aos usuarios que teñen acceso aos datos de carácter persoal.

3 Conceptos básicos sobre a protección de datos de carácter persoal

3 Conceptos básicos sobre a protección de datos de carácter persoal

3.1 Os ficheiros de datos persoais

Que se considera datos de carácter persoal:

Considérase datos de carácter persoal calquera información numérica, alfabética, gráfica, fotográfica, acústica ou de calquera outro tipo concernente a persoas físicas identificadas ou identificables:

- Datos de carácter identificativo: NIF/CIF, teléfono, dirección electrónica etc.
- Datos de carácter persoal: estado civil, data de nacemento, idade, lugar de nacemento, nacionalidade, sexo etc.
- Datos de circunstancias sociais: servizo militar, propiedades, afeccións, estilo de vida, pertenza a asociacións etc.
- Datos académicos ou profesionais: formación, titulación, historial académico, experiencia profesional etc.
- Datos profesionais: profesión, posto de traballo, vida laboral etc.
- Datos de información comercial: actividades e negocios, licenzas comerciais, subscricións a publicacións etc.
- Económico-financeiros: ingresos, rendas, investimentos, préstamos, avais, datos bancarios etc.
- Especialmente protexidos: ideoloxía, afiliación sindical, relixión, crenzas, saúde, vida sexual etc.

Qué é un ficheiro:

É todo conxunto organizado de datos de carácter persoal, sen importar o soporte no que se encontren ou a forma en que os devanditos datos se organicen e almacenen; a modo de exemplo, a axenda onde gardamos os teléfonos dos nosos clientes e provedores, as bases de datos de provedores e clientes, os seus expedientes, os currículos que se utilizan na selección e promoción do persoal.

3.2 Quen é quen na protección de datos

El responsable del fichero o tratamiento es toda persona física o jurídica, pública o privada u órgano administrativo que, solo o conjuntamente con otros, decida sobre la finalidad, contenido y uso del tratamiento.

- O **interesado** é a persoa titular dos datos que sexan obxecto do tratamento.
- O **responsable do ficheiro** ou **tratamento** é toda persoa física ou xurídica, pública ou privada, ou órgano administrativo que, só ou conxuntamente con outros, decida sobre a finalidade, contido e uso do tratamento.
- O **encargado do tratamento** é a persoa física ou xurídica, autoridade pública ou calquera outro organismo que trate os datos persoais por conta do responsable do tratamento.
- O **responsable de seguridade** é a persoa encargada de que se adopten e cumpran todas as medidas de seguridade requiridas segundo o nivel de protección dos datos.
- O **cesionario** é a persoa física ou xurídica, pública ou privada, ou órgano administrativo, ao que se revelen os datos.
- O **usuario** é o persoal ao servizo do responsable do ficheiro ou encargado do tratamento que teña acceso aos datos de carácter persoal como consecuencia de ter encomendadas tarefas de utilización material dos datos almacenados ou que se almacenarán nos ficheiros.

A relación entre o responsable do arquivo e o encargado do tratamento débese regular nun contrato por escrito, no que se debe establecer que o encargado do tratamento unicamente tratará os datos conforme ás instrucións dadas polo responsable do tratamento, que non os aplicará ou utilizará para fins distintos aos que figuren no contrato nin os comunicará a outras persoas. Tamén se deben establecer as medias de seguridade que debe cumpir o encargado do tratamento.

3.3 Actuacións sobre os datos de carácter persoal

As actuacións poden ser o tratamento de datos, a cesión e a comunicación de datos, e a cancelación de datos.

O tratamiento de datos

Son aquelas operacións e procedementos técnicos de carácter automatizado ou non que permitan a recollida, gravación, conservación, elaboración, modificación, bloqueo e cancelación, así como as cesións de datos que resulten de comunicacións, consultas, interconexións e transferencias.

A cesión ou comunicación de datos

É o tratamento de datos que supón a súa revelación a unha persoa distinta do interesado.

A cancelación dos datos

É o procedemento polo cal o responsable do ficheiro cesa no uso dos datos; implicará que se bloqueen os datos e a súa reserva co fin de impedir o seu tratamento agás para a súa posta a disposición das Administracións públicas, xuíces e tribunais, para a atención das posibles responsabilidades nacidas do tratamento e só durante o prazo de prescrición das devanditas responsabilidades. Transcorrido ese prazo, deberá procederse á supresión dos datos.

Se a xestión de nóminas, contratación, tramitación de documentación á Seguridade Social etc. está subcontratada a unha xestoría, considérase a esta como **encargado do tratamento dos datos de carácter persoal** mentres que a túa empresa se considera **responsable do tratamento**. Deberás redactar un contrato.

4 Inscripción dos ficheiros

4 Inscripción dos ficheiros

4.1 Que se debe de facer antes de inscribir un ficheiro

4.1.1 Estándares de calidade

O responsable do ficheiro deberá asegurarse de que os datos contidos nos devanditos ficheiros cumpren os seguintes estándares de calidade:

Os datos persoais deben ser:

- axeitados;
- pertinentes;
- non excesivos;
- non poden usarse para finalidades diferentes daquelas para as que foron recollidos;
- exactos e postos ao día, de non ser exactos ou estar incompletos deben ser eliminados ou substituídos polos correctos;
- útiles, no momento en que deixen de ser útiles para a función para a que foron recollidos deben eliminarse..

Principios relativos á calidade dos datos; os datos de carácter persoal:

- Deberán ser tratados de forma leal y lícita. Se prohíbe la recogida de datos por medios fraudulentos, desleales o ilícitos.
- Sólo podrán ser recogidos para el cumplimiento de finalidades determinadas, explícitas y legítimas del responsable del tratamiento.
- No podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos.

4.1.2 Información previa ao interesado

Os interesados aos que se soliciten datos persoais deberán ser previamente informados de **modo expreso, preciso e inequívoco:**

- Da existencia dun ficheiro ou tratamento de datos de carácter persoal
- Da finalidade da recollida dos datos.
- Dos destinatarios da información.
- Do carácter obrigatorio ou facultativo da súa resposta ás preguntas que lles sexan formuladas.
- Das consecuencias da obtención dos datos ou da negativa a subministralos.
- Da posibilidade de exercitar os dereitos de acceso, rectificación, cancelación e oposición.
- Da identidade e dirección do responsable do tratamento ou, no seu caso, do seu representante. Cando o responsable do tratamento non estea establecido no territorio da Unión Europea e utilice no tratamento de datos medios situados en territorio español, deberá designar, salvo que tales medios se utilicen con fins de tránsito, un representante en España, sen prexuízo das accións que puidesen emprenderse contra o propio responsable do tratamento.

Cando se utilicen cuestionarios ou outros impresos para a recollida, figurarán nestes, en forma claramente lexible, as advertencias a que se refire o apartado anterior.

O artigo 18 do Regulamento de desenvolvemento da LOPD obrigaba a que se conservase a acreditación do cumprimento do deber de información mentres persistise o tratamento dos datos do interesado; o devandito artigo foi anulado pola sentenza da Sala 3ª do Tribunal Supremo do 15 de xullo de 2010.

4.1.3 Consentimento do interesado

Debe solicitarse o consentimento do titular dos datos para poder proceder ao seu tratamento.

Cando se solicite o consentimento, debe referirse a un tratamento ou tratamentos concretos e debe quedar constancia de cal é a finalidade para a que se solicitan os datos.

Se non consta de forma inequívoca cal é a finalidade para a que se solicitan eses datos, o consentimento considerarase nulo e, polo tanto, non válido.

En caso de recollida de datos de menores de 14 anos, o consentimento deberá ser prestado por pais ou titores; se é maior de 14 anos, poderá prestar directamente o consentimento, salvo nos casos que

a lei dispoña outra cousa. En ningún caso se poderán obter dun menor datos que permitan obter información sobre os demais membros do grupo familiar, ou sobre as características deste (información económica, actividade profesional dos pais) sen o consentimento destes, coa excepción dos datos de identificación e dirección da nai, pai ou titor, co obxecto de conseguir a súa autorización.

Salvo que o consentimento teña que constar de forma expresa, entenderase que o afectado consente o tratamento dos datos se despois de informalo debidamente da inclusión dos seus datos no ficheiro non mostra a súa negativa nun prazo de 30 días.

Hai que dar ao afectado, polo tratamento dos seus datos de carácter persoal, a posibilidade de revogar o seu consentimento a través dun medio sinxelo e gratuíto:

- Considérase que cumpren os devanditos requisitos un envío prefranqueado ao responsable do tratamento ou a posta a disposición dun número de teléfono gratuíto.

- Non o cumpren cando se esixe o envío de cartas certificadas, utilización de servizos de telecomunicacións ou calquera outro medio que implique un custo adicional para o interesado.

Aínda que a lei non esixe solicitar o consentimento por escrito, é altamente recomendable, xa que a carga de probar a existencia do devandito consentimento recae no responsable do tratamento dos datos.

4.2 Modelos de cláusulas tipo

4.2.1 Cláusula de información e consentimento expresa

En cumprimento co establecido na Lei orgánica 15/1999, do 13 de decembro, de protección de datos de carácter persoal, informámoslle de que os seus datos persoais serán tratados e quedarán incorporados en ficheiros cuxo titular é (nome da empresa), rexistrados na Axencia Española de Protección de Datos, cuxa finalidade é (poñer a finalidade para a que se crea o ficheiro).
Vostede consente expresamente a recollida e o tratamento destes para a citada finalidade.
En todo caso, pode exercitar os dereitos de acceso, rectificación, cancelación e oposición remitindo un escrito xunto á fotocopia do seu DNI a (dirección á que poden remitir os escritos).
Pregámoslle que no suposto de producirse algunha modificación nos seus datos de carácter persoal, nolo comunique co fin de mantelos actualizados.

4.2.2 Cláusula de información e consentimento xenérica

Os datos persoais facilitados serán incorporados a un ficheiro titularidade de (nome da empresa) coa finalidade de (poñer a finalidade perseguida coa creación do ficheiro). Así mesmo, unha finalidade é a de poder enviar, de xeito periódico, información e publicidade sobre os nosos produtos e servizos. Se no prazo de 30 días, vostede non nos manifesta a súa negativa mediante (envío da comunicación prefranqueada que achega/chamada ao número 900xxxxxxx), entenderemos que presta o seu consentimento para o tratamento dos datos facilitados.
De acordo coa Lei orgánica 15/1999, de protección de datos de carácter persoal, pode exercer os dereitos de acceso, rectificación, cancelación e, no seu caso, oposición, enviando unha solicitude por escrito acompañada da fotocopia do seu DNI á seguinte dirección (poñer dirección).

4.2.3 Cláusula de consentimento para correos electrónicos

Esta mensaxe e os seus ficheiros anexos son confidenciais. Estes conteñen información reservada que non pode ser difundida e ampáranse na Lei de servizos da sociedade da información e de comercio electrónico 34/2002 do 11 de xullo (LSSICE). Se vostede recibiu este correo por erro, reenvíeo ao remitente e elimíneo do seu sistema. Non deberá copiar a mensaxe nin divulgar o seu contido.
A súa dirección de correo electrónico xunto aos seus datos constan nun ficheiro inscrito no Rexistro Xeral de Protección de Datos, cuxo responsable é XXXXXXX. A finalidade é manter o contacto con vostede. Poderá exercitar os seus dereitos de acceso, rectificación, cancelación ou oposición dirixíndose por escrito a XXXXX.

4.3 Cómo inscribir os ficheros

4.3.1 Notificar a AEPD a existencia dos ficheros

Quen debe notificar?

Calquera persoa física ou xurídica que vaia proceder á creación dun ficheiro que conteña datos de carácter persoal debe proceder á súa notificación á AEPD.

Que se debe notificar?

A creación dun ficheiro con datos de carácter persoal que resulta necesario para o logro do obxecto ou finalidade da empresa, xunto aos datos referentes ao responsable e encargado do tratamento, dirección onde se poden exercer os dereitos da LOPD, nome dos ficheiros, a súa finalidade, o nivel de seguridade dos datos e categorías dos interesados.

Cando se debe notificar?

A notificación do ficheiro debe realizarse antes da súa creación.

Como se debe notificar?

A través do sistema de notificacións telemáticas da AEPD (sistema NOTA) e do seu formulario, que permite tanto a presentación telemática da notificación con certificado dixital coma a súa descarga para a súa presentación en papel.

Descarga del formulario NOTA:
https://www.agpd.es/portalwebAGPD/canalresponsable/inscripcion_ficheros/Notificaciones_tele/obtencion_formulario/index-ides-idphp.php

Onde se debe notificar?

- Telemáticamente:
  - con certificado dixital a través da páxina web da AEPD:www.agpd.es;
  - sen certificado dixital remitindo á Axencia a folla de solicitude correspondente ao envío realizado debidamente asinada.

En formulario de papel ante a AEPD.

Por que se debe notificar?

Se non se notifica a existencia dun ficheiro, podería incorrerse en falta leve ou grave, e quedaría suxeito ao réxime sancionador previsto na LOPD, que prevé multas nestes supostos de 900 a 300.000 euros.

4.3.2 Como cubrir o formulario NOTA

Datos necesarios para cubrir o formulario NOTA

A notificación deberá indicar a identificación do responsable do ficheiro; a identificación do ficheiro; as súas finalidades e os usos previstos; o sistema de tratamento empregado na súa organización; o colectivo de persoas sobre o que se obteñen os datos; o procedemento e procedencia dos datos; as categorías de datos; o servizo ou unidade de acceso; a indicación do nivel de medidas de seguridade básico, medio ou alto esixible; e, no seu caso, a identificación do encargado do tratamento onde se encontre situado o ficheiro e os destinatarios de cesións e transferencias internacionais de datos.

Como cubrir o formulario NOTA?

- Identificación do responsable dos ficheiros:

Nome ou denominación social da persoa responsable do ficheiro. Cómpre recordar que é quen decide sobre a finalidade, contido e uso que se vai dar a ese ficheiro; non poden ter a consideración de responsables do ficheiro as persoas vinculadas mediante unha relación contractual de carácter laboral co responsable do ficheiro.

Hai que indicar a actividade á que se dedica a empresa e os demais datos identificativos (dirección, CIF/NIF e, se se desexa, pódese achegar o teléfono, fax ou correo electrónico do responsable dos ficheiros)..

- Dirección á que se poden dirixir os titulares dos datos para exercer os seus dereitos de oposición, acceso, rectificación e cancelación:

É o lugar (oficina, dirección postal ou apartado de correos) a onde poden dirixirse os titulares dos datos para exercer os dereitos amparados pola LOPD, só debe indicarse expresamente cando sexa distinto ao domicilio do responsable do ficheiro.

- Identificación do encargado do tratamento:

Cando exista un terceiro que realiza o tratamento por conta do responsable e implique unha situación do ficheiro fóra do domicilio deste (como exemplos: a asesoría laboral, a empresa que se encargue do mantemento informático).

Cómpre recordar que ese tratamento dos datos por conta de terceiros debe estar regulado contractualmente, e recoméndáse a súa constancia por escrito, xa que é o medio máis sinxelo para acreditar a súa celebración.

Os traballadores da empresa non teñen a consideración de encargados do tratamento para os efectos da LOPD.

- Identificación dos ficheiros e a súa finalidade:

Debe indicarse un nome que identifique o ficheiro (por exemplo: axenda e contactos, clientes, provedores, expedientes, currículos).

Hai que describir de modo detallado a finalidade do ficheiro e o uso que se vai facer del (a título de exemplo, descrición da finalidade e o uso do ficheiro de axenda e contactos: contén datos que permiten manter o contacto por teléfono, fax, correo electrónico ou ordinario co persoal, clientes, provedores e outros contactos de terceiros, en xeral necesarios para o mantemento da relación con estes).

- Orixe e procedencia dos datos e colectivos ou categorías de interesados:

Deberá indicarse de onde proceden os datos contidos (do propio interesado ou do seu representante legal, rexistros públicos, outras persoas físicas, fontes accesibles ao público, entidade privada ou Administracións públicas).

As fontes accesibles para o público son aqueles ficheiros que poden ser consultados por calquera persoa sen máis limitación que, se é o caso, o aboamento dunha contraprestación. Teñen a consideración de fontes de acceso público o censo promocional; os repertorios telefónicos nos termos previstos pola súa normativa específica; as listas de persoas pertencentes a grupos de profesionais que conteñan unicamente os datos de nome, título, profesión, actividade, grao académico, dirección e indicación da súa pertenza ao grupo; os diarios e boletíns oficiais, e os medios de comunicación.

Hai que especificar a que colectivo ou categoría pertencen os titulares dos datos: traballadores, clientes, provedores, pacientes etc...

- Tipos de datos, estrutura e organización do ficheiro:

Hai que indicar ante que tipo de datos nos encontramos:

  - Datos especialmente protexidos: ideoloxía, afiliación sindical, relixión e crenzas. É importante recordar que este tipo de datos só se poden tratar cando se conseguiu o consentimento expreso e por escrito do afectado.

  - Outros datos especialmente protexidos: orixe racial ou étnica, saúde e vida sexual.

  - Datos de carácter identificativo: nome e apelidos, dirección, teléfono, firma, DNI, tarxeta sanitaria, número de afiliación á Seguridade Social, imaxe/voz, marcas físicas ou firma electrónica.

  - Outros datos: características persoais, circunstancias sociais, académicos, profesionais, económicos, financeiros etc…

- Sinalar cal é o sistema de tratamento dos datos (modo en que organiza a información ou utiliza un sistema de información): automatizado, manual ou mixto.

- Medidas de seguridade:

Hai que indicar o nivel de medidas de seguridade esixible ao ficheiro. Existen tres niveis: básico, medio, alto.

- Cesión ou comunicación de datos:

Cando se prevexa que se van realizar cesións ou comunicacións de datos, hai que indicar a que categoría pertence o destinatario da cesión (Seguridade Social, rexistros públicos, Administración tributaria, notarios, bancos etc.).

Non se considera cesión de datos a prestación dun servizo polo encargado do tratamento.

- Transferencias internacionais:

Cando se realicen tratamentos de datos fóra do territorio do Espazo Económico Europeo, hai que indicar en que países e os destinatarios dos datos.

4.3.3 Inscribir os ficheiros no Rexistro Xeral de Protección de Datos.

Se a notificación realizada a través do formulario NOTA se axusta aos requisitos esixibles, o Rexistro Xeral de Protección de Datos procederá sen máis trámites á inscrición do ficheiro. O habitual é que a inscrición se notifique por escrito; non obstante, se transcorrido un mes dende a presentación da solicitude da inscrición, a AEPD non resolveu sobre esta, entenderase a todos os efectos inscrito o ficheiro.

Se non se cumpren os requisitos, deberán pedirnos por escrito que se completen os datos ou que se proceda á emenda dos defectos apreciados.

A inscrición no Rexistro só acredita que se cumpriu coa obriga de notificación prevista na LOPD, mais o responsable do tratamento dos datos deberá cumprir ademais co resto das obrigas previstas na Lei e nas disposicións regulamentarias.

4.4 Modificación e supresión de ficheiros

A inscrición do ficheiro deberá encontrarse actualizada en todo momento. Calquera modificación da inscrición dun ficheiro debe ser notificada á AEPD.

Cando se proceda a suprimir un ficheiro, tamén se debe notificar á AEPD, a cal, logo de comprobación de que a devandita notificación é correcta, procederá á cancelación da inscrición correspondente ao devandito ficheiro.

Tanto a modificación coma a supresión notificaranse a través do formulario NOTA, e poderanse utilizar os mesmos medios de envío que para a inscrición.

5 A seguridade dos datos de carácter persoal

5 A seguridade dos datos de carácter persoal

5.1 Os niveis de seguridade e os datos aos que se aplica

As medidas de seguridade esixibles adáptanse a tres niveis: alto, medio e básico.

Nivel alto:

- Ficheiros que conteñan datos referentes á ideoloxía, afiliación sindical, relixión, crenzas, orixe racial, saúde ou vida sexual.
- Os solicitados para fins policiais sen o consentimento da persoa afectada.
- Os que conteñan datos derivados de actos de violencia de xénero.

Nivel medio:

- Ficheiros que conteñan datos sobre a comisión de infraccións administrativas ou penais.
- Os que posúan as persoas que se dediquen á prestación de servizos de información sobre solvencia patrimonial ou crédito e sempre que os obtivesen das Administracións públicas, de fontes accesibles ao público ou se os datos se facilitasen polo interesado ou co seu consentimento.
- Os da Axencia Tributaria en tanto teñan relación co exercicio das súas potestades tributarias.
- Ficheiros que posúan as entidades financeiras en relación cos servizos financeiros que presten.
- Os que en exercicio das súas competencias posúan a Seguridade Social e as mutuas de accidentes de traballo e enfermidades profesionais da Seguridade Social.
- Ficheiros que permitan avaliar a personalidade dos cidadáns.

Nivel básico:

- É aplicable a todos os ficheiros ou tratamentos de datos de carácter persoal.

5.2 Documento de seguridade

O responsable do ficheiro ten a obriga de elaborar un documento de seguridade; nel deberán figurar as medidas de índole técnica e organizativa adaptadas á normativa que o persoal con acceso aos sistemas de información deberá cumprir obrigatoriamente.

O documento de seguridade terá o carácter de documento interno da empresa.

Pode terse un único documento de seguridade para todos os ficheiros, un para cada ficheiro, ou tamén poden elaborarse documentos de seguridade agrupando ficheiros segundo o sistema de tratamento ou atendendo a criterios organizativos do responsable.

O documento de seguridade debe manterse en todo momento actualizado e revisarse sempre que se produzan cambios relevantes no sistema de información, no sistema de tratamento empregado, na súa organización, no contido da información incluída nos ficheiros ou tratamentos, ou como consecuencia dos controis periódicos realizados. Sempre se entenderá que un cambio é relevante cando poida repercutir no cumprimento das medidas de seguridade implantadas.

O contido do documento de seguridade deberá adecuarse, en todo momento, ás disposicións vixentes en materia de seguridade dos datos de carácter persoal.

5.2.1 Contido mínimo do documento de seguridade

- Ámbito de aplicación do documento detallando os recursos protexidos

Sinalar as persoas obrigadas a cumprir as medidas de seguridade (persoal con acceso aos datos, encargados de tratamento...) e os ficheiros aos que se aplican as devanditas medidas de seguridade. Tamén deben de relacionarse os recursos que deben acharse protexidos, ben porque conteñen fisicamente os medios cos que se tratan os datos, os medios en si ou os que serven para acceder directa ou indirectamente ao ficheiro (como exemplos, os locais onde se encontren fisicamente situados os ficheiros, os ordenadores dende os que se pode ter acceso aos ficheiros, o contorno de rede, os servidores, as aplicacións que permitan ter acceso a datos de carácter persoal etc…).

- Medidas, normas, procedementos de actuación, regras e estándares encamiñados a garantir a seguridade

Deben establecerse as medidas de seguridade concretas aplicables aos ficheiros (control de accesos, tanto físicos coma lóxicos; rexistros de accesos; copias de seguridade; rexistro de incidencias; destrución de ficheiros físicos...); procedementos de actuación (procedemento de control de accesos, para a entrada ou saída de datos dos ficheiros, en caso de exercicio dos dereitos de acceso, rectificación, oposición ou cancelación do titular dos datos, de copia de documentos, de arquivo etc.), regras e es-

tándares (autorización previa para almacenar datos en dispositivos portátiles para realizar traballo fóra dos locais pertencentes ao responsable do ficheiro, políticas de uso do correo electrónico etc…).

- **Funcións e obrigas do persoal en relación co tratamento dos datos de carácter persoal incluídos no ficheiro:**

Pode nomearse un ou varios responsables de seguridade, se a estrutura da empresa é complexa (ben porque o desenvolvemento das tarefas afecta a varias áreas concretas, ben porque a empresa teña diversos establecementos), poden delegarse funcións derivadas tanto das obrigas do responsable do tratamento coma do responsable de seguridade.

- **Estrutura dos ficheiros con datos de carácter persoal e descrición dos sistemas de información que os tratan**:

Hai que identificar o ficheiro, describilo, indicar a súa finalidade, os campos do ficheiro (que tipo de datos inclúe), o nivel de seguridade que lle corresponde a ese ficheiro (básico, medio ou alto), a calidade de quen efectúa o tratamento do ficheiro (responsable do ficheiro, responsable de seguridade, encargado de tratamento...). Deben describirse os sistemas de información que os tratan (servidores e postos de traballo que aloxan o ficheiro, aplicacións informáticas vinculadas ao tratamento do ficheiro…).

- **Procedemento de notificación, xestión e resposta ante as incidencias:**

Deberá elaborarse un procedemento de notificación e xestión das incidencias que afecten aos datos de carácter persoal; crearase un rexistro onde se fará constar que tipo de incidencia se produciu (perda dun expediente, cesión non consentida de datos, acceso a un ficheiro por unha persoa non autorizada, saída de datos sen autorización etc.), o momento en que se produce ou detecta a incidencia, a persoa que a notifica, os efectos derivados desta e que medidas se tomaron para paliar as posibles consecuencias producidas pola existencia da incidencia.

- **Procedementos de realización de copias de respaldo e de recuperación dos datos nos ficheiros ou tratamentos automatizados:**

Debe establecerse un procedemento polo cal se realicen copias de seguridade polo menos unha vez por semana. Tamén se establecerán procedementos de recuperación de datos que permitan reconstruír os ficheiros tal e como estaban antes do momento da súa destrución ou perda.

- **Procedementos para o transporte de soportes e documentos, así como para a destrución dos documentos e soportes ou, no seu caso, a reutilización destes últimos:**

En caso de que se proceda ao traslado de documentación ou soportes dun ficheiro, deben establecerse medidas que impidan que se acceda ou modifique a información nel contida.

É moi importante que se estableza o procedemento de destrución de ficheiros; se están contidos en papel, debe preverse a súa destrución mediante o uso dunha destrutora de papel e prohibir expresamente a súa reutilización cando conteñan datos de carácter persoal. En caso de que se desboten ou se reutilicen soportes de ficheiros automatizados, debe comprobarse o seu correcto borrado ou a súa destrución de modo que se impida o acceso á información contida nos devanditos soportes ou a súa posible recuperación.

5.2.2 Outros contidos en casos especiais:

- Ficheiros aos que se lles debe aplicar medidas de seguridade de nivel medio e alto:

Identificación do responsable ou responsables de seguridade e establecer a realización de controis periódicos para verificar o cumprimento do establecido no documento de seguridade.

- Cando exista un tratamento de datos por conta de terceiros:

O documento de seguridade deberá conter a identificación dos ficheiros ou tratamentos que se traten en concepto de encargado con referencia expresa ao contrato ou documento que regule as condicións do encargo, identificación do responsable e período de vixencia do encargo.

5.3 Medidas de seguridade

Distínguense as medidas de seguridade que cómpre adoptar segundo se trate de ficheiros e tratamentos automatizados ou non automatizados.

5.3.1 Ficheiros e tratamentos automatizados

As distintas medidas de seguridade que deben adoptarse variarán en función de se os datos que protexen son de nivel básico, medio ou alto.

5.3.1.1 Xestión de soportes

Soporte é o obxecto físico susceptible de ser tratado nun sistema de información e sobre o cal se poden gravar ou recuperar datos.

- Identificación, inventario e almacenamento.

  - Nivel alto: a identificación dos soportes deberase realizar utilizando sistemas de etiquetaxe comprensibles e con significado que permitan aos usuarios con acceso autorizado aos citados soportes e documentos identificar o seu contido, e que dificulten a identificación para o resto de persoas.

  - Nivel básico: debe realizarse un inventario dos soportes que conteñen datos de carácter persoal no que conste a identificación de cada un deles, a información que almacenan e realizar unha relación do persoal autorizado a acceder aos devanditos soportes.

Saídas de soportes.

- Nivel alto-Cifrado na distribución de soportes e portátiles:
  A identificación dos soportes deberase realizar utilizando sistemas de etiquetaxe comprensibles e con significado que permitan aos usuarios con acceso autorizado aos citados soportes e documentos identificar o seu contido, e que dificulten a identificación para o resto de persoas.

- Nivel básico-Autorización para a saída de soportes:
  A saída de soportes e documentos que conteñan datos de carácter persoal, incluídos os comprendidos ou anexos a un correo electrónico, fóra dos locais baixo o control do responsable do ficheiro ou tratamento deberá ser autorizada polo responsable do ficheiro ou encontrarse debidamente autorizada no documento de seguridade.

- Nivel medio-Rexistro de saída de soportes:
  Deberá establecerse un sistema de rexistro de entrada de soportes que permita, directa ou indirectamente, coñecer o tipo de documento ou soporte, a data e hora, o emisor, o número de documentos ou soportes incluídos no envío, o tipo de información que conteñen, a forma de envío e a persoa responsable da recepción que deberá estar debidamente autorizada.

- Dispositivos portátiles
  Deberá evitarse o tratamento de datos de carácter persoal en dispositivos portátiles que non permitan o seu cifrado. En caso de que sexa estritamente necesario, farase constar motivadamente no documento de seguridade e adoptaranse medidas que teñan en conta os riscos de realizar tratamentos en ámbitos desprotexidos.

Entrada de soportes.

- Nivel medio: dispoñerase dun sistema de rexistro de saída de soportes que permita, directa ou indirectamente, coñecer o tipo de documento ou soporte, a data e hora, o destinatario, o número de documentos ou soportes incluídos no envío, o tipo de información que conteñen, a forma de envío e a persoa responsable da entrega que deberá estar debidamente autorizada.

Desbotado e reutilización.

- Nivel básico: sempre que se vaia desbotar calquera documento ou soporte que conteña datos de carácter persoal, deberá procederse á súa destrución ou borrado, mediante a adopción de medidas dirixidas a evitar o acceso á información contida neste ou a súa recuperación posterior.

5.3.1.2 Control de acceso

- **Control de acceso físico:**

  - Nivel medio:
    Só o persoal autorizado no documento de seguridade poderá ter acceso aos lugares onde se achen instalados os equipos físicos que dean soporte aos sistemas de información.

- **Control de acceso lóxico:**

  - Nivel básico:
    O responsable do ficheiro encargarase de que exista unha relación actualizada de usuarios e perfís de usuarios, e os accesos autorizados para cada un deles —que serán aos recursos que precisen para o desenvolvemento das súas funcións— e establecerá mecanismos para evitar que un usuario poida acceder a recursos con dereitos distintos dos autorizados.
    Exclusivamente o persoal autorizado para iso no documento de seguridade poderá conceder, alterar ou anular o acceso autorizado aos recursos, conforme aos criterios establecidos polo responsable do ficheiro.
    En caso de que exista persoal alleo ao responsable do ficheiro que teña acceso aos recursos, deberá estar sometido ás mesmas condicións e obrigas de seguridade que o persoal propio.

- **Identificación e autenticación:**

  - Nivel medio:
    O responsable do ficheiro ou tratamento establecerá un mecanismo que limite a posibilidade de intentar reiteradamente o acceso non autorizado ao sistema de información.

  - Nivel básico:
    O responsable do ficheiro ou tratamento deberá adoptar as medidas que garantan a correcta identificación e autenticación dos usuarios, establecendo un mecanismo que permita a identificación de forma inequívoca e personalizada de todo aquel usuario que intente acceder ao sistema de información e a verificación de que está autorizado.
    Cando o mecanismo de autenticación se basee na existencia de contrasinais, existirá un procedemento de asignación, distribución e almacenamento que garanta a súa confidencialidade e integridade. O documento de seguridade establecerá a periodicidade, que en ningún caso será superior a un ano, coa que teñen que ser cambiados os contrasinais que, mentres estean vixentes, se almacenarán de forma inintelixible.

- **Rexistro de accesos:**

  - Nivel alto:
    De cada intento de acceso gardaranse, como mínimo, a identificación do usuario, a data e hora en que se realizou, o ficheiro accedido, o tipo de acceso e se foi autorizado ou denegado.
    No caso de que o acceso fose autorizado, será preciso gardar a información que permita identificar o rexistro accedido.

Os mecanismos que permiten o rexistro de accesos estarán baixo o control directo do responsable de seguridade competente sen que deban permitir a desactivación nin a manipulación destes.
O período mínimo de conservación dos datos rexistrados será de dous anos.
O responsable de seguridade encargarase de revisar polo menos unha vez ao mes a información de control rexistrada e elaborará un informe das revisións realizadas e os problemas detectados.
Non será necesario o rexistro de accesos definido neste artigo en caso de que concorran as seguintes circunstancias:

- Que o responsable do ficheiro ou do tratamento sexa unha persoa física.
- Que o responsable do ficheiro ou do tratamento garanta que unicamente el ten acceso e trata os datos persoais.

A concorrencia das dúas circunstancias ás que se refire o apartado anterior deberá facerse constar expresamente no documento de seguridade.

5.3.1.3 Copias de seguridade e recuperación de datos.

- Nivel básico:
  Deberán realizarse copias de respaldo como mínimo unha vez á semana, salvo que non se tivese producido ningunha actualización dos datos.
  Hai que establecer procedementos para a recuperación dos datos que garantan en todo momento a súa reconstrución no estado en que se encontraban ao tempo de producirse a perda ou destrución. Unicamente no caso de que a perda ou destrución afectase a ficheiros ou tratamentos parcialmente automatizados, e sempre que a existencia de documentación permita alcanzar o obxectivo ao que se refire o parágrafo anterior, deberase proceder a gravar manualmente os datos e quedará constancia motivada deste feito no documento de seguridade.
  O responsable do ficheiro encargarase de verificar cada seis meses a correcta definición, funcionamento e aplicación dos procedementos de realización de copias de respaldo e de recuperación dos datos.
  Deberase realizar unha copia de seguridade antes de realizar probas con datos reais.

- Nivel alto:
  Deberá conservarse unha copia de respaldo dos datos e dos procedementos de recuperación destes nun lugar diferente daquel en que se encontren os equipos informáticos que os tratan, para a devandita copia dispoñeranse as mesmas medidas de seguridade que para os datos e os equipos que os tratan.

5.3.1.4 Acceso a través de redes de telecomunicacións.

- Nivel básico:
  As medidas de seguridade esixibles aos accesos a datos de carácter persoal a través de redes de comunicacións, sexan ou non públicas, deberán garantir un nivel de seguridade equivalente ao correspondente aos accesos en modo local.

- Nivel alto:
  A transmisión de datos de carácter persoal a través de redes públicas ou redes inarámicas de comunicacións electrónicas realizarase cifrando os devanditos datos ou ben utilizando calquera outro mecanismo que garanta que a información non sexa intelixible nin manipulada por terceiros.

5.3.1.5 Xestión de incidencias.

- Nivel básico:
  Deberá existir un procedemento de notificación e xestión das incidencias que afecten aos datos de carácter persoal e establecer un rexistro en que se faga constar o tipo de incidencia, o momento en que se produciu ou, se é o caso, o momento en que se detectou, a persoa que realiza a notificación, a quen se lle comunica, os efectos que se derivasen desta e as medidas correctoras aplicadas.

- Nivel medio:
  En caso de datos de nivel medio e alto, deberán consignarse, ademais, os procedementos realizados de recuperación dos datos, indicando a persoa que executou o proceso, os datos restaurados e, se é o caso, que datos foi necesario gravar manualmente no proceso de recuperación.
  Para a execución dos procedementos de recuperación dos datos, será necesaria a autorización do responsable do ficheiro.

5.3.1.6 Probas con datos reais.

- Nivel básico:
  As probas anteriores á implantación ou modificación dos sistemas de información que traten ficheiros con datos de carácter persoal non se realizarán con datos reais, salvo que se asegure o nivel de seguridade correspondente ao tratamento realizado e se anote a súa realización no documento de seguridade. Previamente ás probas, deberá realizarse unha copia de seguridade.

5.3.1.7 Traballo fóra dos locais.

- Nivel básico:
  Cando os datos persoais se almacenen en dispositivos portátiles ou se traten fóra dos locais do responsable de ficheiro ou tratamento, ou do encargado do tratamento, será preciso que exista unha autorización previa do responsable do ficheiro ou tratamento, a cal terá que constar no documento de seguridade, e en todo caso deberá garantirse o nivel de seguridade correspondente ao tipo de ficheiro tratado.
  A autorización poderá establecerse para un usuario ou para un perfil de usuarios e determinando un período de validez para esta.

5.3.1.8 Ficheiros temporais ou copias de traballo de documentos.

- Nivel básico:
  Aqueles ficheiros temporais ou copias de documentos que se creasen exclusivamente para a realización de traballos temporais ou auxiliares deberán cumprir o nivel de seguridade que lles corresponda e serán borrados ou destruídos unha vez que deixen de ser necesarios para os fins para os que se crearon.

5.4 Ficheiros e tratamentos non automatizados

Aos ficheiros non automatizados aplicaránselles as mesmas previsións que aos ficheiros automatizados respecto aos niveis de seguridade dos datos, ao encargado do tratamento, ás prestacións de servizos sen acceso a datos persoais, á delegación de autorizacións, ao réxime de traballo fóra dos locais do responsable do ficheiro ou encargado do tratamento, ás copias de traballo de documentos, ao rexistro de incidencias, ao control de acceso e á xestión de soportes.

E de forma particular, aplicaranse as seguintes medidas de seguridade:

5.4.1 Almacenamento da documentación.

- Nivel básico:
  Os dispositivos de almacenamento dos documentos que conteñan datos de carácter persoal deberán dispoñer de mecanismos que obstaculicen a súa apertura. Cando as características físicas daqueles non permitan adoptar esta medida, o responsable do ficheiro ou tratamento adoptará medidas que impidan o acceso de persoas non autorizadas.

- Nivel alto:
  Os armarios, arquivadores ou outros elementos nos que se almacenen os ficheiros non automatizados con datos de carácter persoal deberán encontrarse en áreas nas que o acceso estea protexido con portas de acceso dotadas de sistemas de apertura mediante chave ou outro dispositivo equivalente. As devanditas áreas deberán permanecer pechadas cando non sexa preciso o acceso aos documentos incluídos no ficheiro.
  Se isto non fose posible debido ás características do local onde se encontran, o responsable adoptará medidas alternativas que se incluirán no documento de seguridade.

5.4.2 Custodia dos soportes.

- Nivel básico:
  Mentres a documentación con datos de carácter persoal non se encontre arquivada nos dispositivos de almacenamento establecidos no artigo anterior, por estar en proceso de revisión ou tramitación, xa sexa previo ou posterior ao seu arquivo, a persoa que se encontre o cargo desta deberá custodiala e impedir en todo momento que poida ser accedida por persoa non autorizada.

5.4.3 Copia ou reproducción.

- Nivel alto:
  A xeración de copias ou a reprodución dos documentos unicamente poderá ser realizada baixo o control do persoal autorizado no documento de seguridade. Unha vez desbotadas, debe procederse á súa destrución de forma que se evite o acceso á información contida nas copias ou a súa recuperación posterior.

5.4.4 Criterios de arquivo.

- Nivel básico:
  O arquivo que se efectúe dos soportes ou documentos deberá garantir a correcta conservación dos documentos, a localización e consulta da información e posibilitar o exercicio dos dereitos de oposición ao tratamento, acceso, rectificación e cancelación.

5.4.5 Control de accesos.

- Nivel alto:
  O acceso á documentación limitarase exclusivamente ao persoal autorizado. Estableceranse mecanismos que permitan identificar os accesos realizados no caso de documentos que poidan ser utilizados por múltiples usuarios. Se acceden ao documento persoas distintas ás autorizadas deberá quedar axeitadamente rexistrado.

5.4.6 Traslado de documentación.

- Nivel alto:
  Sempre que se proceda ao traslado físico da documentación contida nun ficheiro, deberán adoptarse medidas dirixidas a impedir o acceso ou a manipulación da información obxecto de traslado.

5.5 Funcións e obrigas do persoal

5.5.1 Dos usuarios.

- **Usuario:** suxeito ou proceso autorizado para acceder a datos ou recursos. Terán a consideración de usuarios os procesos que permitan acceder a datos ou recursos sen identificación dun usuario físico.

- **Nivel básico:** as funcións e obrigas de cada un dos usuarios ou perfís de usuarios con acceso aos datos de carácter persoal e aos sistemas de información estarán claramente definidas e documentadas no documento de seguridade.

- **A título de exemplo:** pechar ou bloquear as sesións ao termo da xornada laboral ou cando se ausente de forma temporal do seu posto de traballo, obter autorización do responsable de seguridade para copiar ficheiros con datos de carácter persoal nalgún soporte, gardar os documentos con datos de carácter persoal en lugar seguro, solicitar a autorización do responsable de seguridade para trasladar soportes ou documentos con datos de carácter persoal.

5.5.2 Dos responsables.

➲ Do responsable do ficheiro ou tratamento

- Responsable do ficheiro ou tratamento: persoa física ou xurídica, de natureza pública ou privada, ou órgano administrativo, que decida sobre a finalidade, contido e uso do tratamento.

- Obrigas do responsable do ficheiro: Notificar á AEPD os ficheiros que se creen, a súa modificación e a súa eliminación; solicitar o consentimento dos interesados para o tratamento de datos, verificar que se cumpre o deber de información, formar o persoal respecto ás medidas de seguridade que cómpre adoptar, etc…

➲ Do responsable de seguridade

- Cando existan datos aos que haxa de aplicar medidas de seguridade de nivel medio, no documento de seguridade deberán designarse un ou varios responsables de seguridade encargados de coordinar e controlar as medidas definidas neste. Esta designación pode ser única para todos os ficheiros ou tratamentos de datos de carácter persoal ou diferenciada segundo os sistemas de tratamento utilizados, circunstancia que deberá facerse constar claramente no documento de seguridade.

- Algunhas das funcións principais do responsable de seguridade:

  - Revisar que os datos que se traten sexan adecuados, pertinentes e non excesivos en relación coas finalidades para as que se obtivesen, que non se usen finalidades incompatibles con aquelas para as que se recollesen os datos e que os devanditos datos sexan exactos e estean ao día.

  - Comprobar que se cumpre co deber de información e que se conta co consentimento do titular dos datos.

  - Implantar o procedemento para atender o exercicio dos dereitos de acceso, rectificación, oposición e cancelación e atender as peticións ao respecto dos titulares dos datos.

  - Implantar controis periódicos para verificar o cumprimento do disposto no documento de seguridade e revisar os devanditos controis.

  - Definir e documentar as obrigas do persoal.

- Establecer mecanismos que permitan identificar os usuarios que acceden ao sistema, que limiten a posibilidade de intentos reiterados de acceso non autorizados e que os usuarios só poidan acceder aos datos necesarios para as súas funcións.

- Autorizar as recuperacións de datos e a saída de soportes fóra dos locais.

- Realizar copias de respaldo, polo menos semanalmente, e verificar cada seis meses o procedemento para a súa realización.

- Establecer un procedemento de notificación e xestión das incidencias.

5.6 Controis: auditoría e controis periódicos

Auditoría

A partir do nivel medio, os sistemas de información e instalacións de tratamento e almacenamento de datos someteranse, polo menos cada dous anos, a unha auditoría interna ou externa que verifique o cumprimento do presente título.

Con carácter extraordinario deberá realizarse a devandita auditoría sempre que se realicen modificacións substanciais no sistema de información que poidan repercutir no cumprimento das medidas de seguridade implantadas co obxecto de verificar a adaptación, adecuación e eficacia destas.

O informe de auditoría deberá ditaminar sobre a adecuación das medidas e controis á Lei e o seu desenvolvemento regulamentario, identificar as súas deficiencias e propoñer as medidas correctoras ou complementarias necesarias. Deberá, igualmente, incluír os datos, feitos e observacións en que se baseen os ditames alcanzados e as recomendacións propostas.

Os informes de auditoría serán analizados polo responsable de seguridade competente, que elevará as conclusións ao responsable do ficheiro ou tratamento para que adopte as medidas correctoras axeitadas e quedarán a disposición da Axencia Española de Protección de Datos ou, no seu caso, das autoridades de control das comunidades autónomas.

Controis periódicos

Os ficheiros aos que sexan de aplicación as medidas de seguridade de nivel medio ou as medidas de seguridade de nivel alto deben ser sometidos a controis periódicos para verificar que se cumpre o establecido no documento de seguridade.

5.7 Modelos de formulario

5.7.1 Formulario de rexistro de entrada e saída de soportes

REXISTRO DE ENTRADA E SAÍDA DE SOPORTES						
REXISTRO DE ENTRADA						
Tipo de documento ou soporte	Data Hora	Emisor	Núm. documentos ou soportes enviados	Tipo de información	Forma de envío	Responsable recepción
REXISTRO DE SAÍDA						
Tipo de documento ou soporte	Data Hora	Emisor	Núm. documentos ou soportes enviados	Tipo de información	Forma de envío	Responsable recepción

5.7.2 Formulario de registro de incidencias

REXISTRO DE INDICENCIAS		
Núm. incidencia:	Data/Hora:	Persoa que notifica:
Dirixido a:		
Tipo de incidencia: Observacións: Efectos derivados:		
Medidas correctoras aplicadas:		
SÓ PARA DATOS DE NIVEL MEDIO:		
Procedemento de recuperación de datos: SI NON Persoa que executou o proceso de recuperación de datos: Datos que foi necesario gravar manualmente:		

6 Dereitos dos titulares dos datos (A.R.C.O.)

6 Dereitos dos titulares dos datos (A.R.C.O.)

6.1 Disposicións comúns

A Lei orgánica 15/1999, do 13 de decembro, de protección de datos de carácter persoal recolle unha serie de dereitos fundamentais dos cidadáns que lle proporcionan ao titular da información persoal a posibilidade de efectuar un control material dos seus datos.

6.1.1 Condicións para o exercicio dos dereitos

Os dereitos de acceso, rectificación, cancelación e oposición son persoais e serán exercidos polo afectado, acreditando a súa identidade.

Como excepcións a esta indicación considéranse os seguintes casos:

- Cando o afectado se encontre en situación de incapacidade ou minoría de idade que imposibilite o exercicio persoal destes dereitos, poderán exercitarse polo seu representante legal, en cuxo caso será necesario que acredite tal condición.

- Os dereitos tamén poderán exercitarse a través de representante voluntario, expresamente designado para o exercicio do dereito. Nese caso, deberá constar claramente acreditada a identidade do representado, mediante a achega de copia do seu documento nacional de identidade ou documento equivalente, e a representación conferida por aquel.

Os dereitos serán denegados cando a solicitude sexa formulada por unha persoa distinta do afectado e non se acreditase que esta actúa en representación daquel.

6.1.2 Condicións xerais para o exercicio dos dereitos

- Os dereitos de acceso, rectificación, cancelación e oposición son dereitos independentes, de tal forma que non pode entenderse que o exercicio de ningún deles sexa requisito previo para o exercicio doutro.

- Deberáselle conceder ao interesado un medio sinxelo e gratuíto para o exercicio dos dereitos, e non poderá supoñer un ingreso adicional para o responsable do tratamento ante o que se exercitan.

- Non se consideran conformes coa normativa de protección de datos que se estableza como medio para o exercicio de dereitos o envío de cartas certificadas ou semellantes, a utilización de servizos de telecomunicacións que implique unha tarificación adicional ou calquera outro que implique un custo excesivo para o interesado.

- Se a empresa dispón de servizos para a atención ao público ou para o exercicio de reclamacións relacionadas co servizo prestado ou os produtos ofertados, estes poden utilizarse para que os interesados exerciten os seus dereitos. En tal caso, a identidade do interesado considerarase acreditada polos medios establecidos para a identificación dos clientes do responsable na prestación dos seus servizos ou contratación dos seus produtos.

- Deberá atenderse a solicitude de acceso, rectificación, cancelación ou oposición exercida por un afectado aínda cando este non utilizase o procedemento establecido especificamente para o efecto por aquel, sempre que o interesado utilizase un medio que permita acreditar o envío e a recepción da solicitude.

6.1.3 Solicitude e contestación

Solicitude

O exercicio dos dereitos deberá levarse a cabo mediante comunicación dirixida ao responsable do ficheiro, que conterá:

- Nome e apelidos do interesado; fotocopia do seu documento nacional de identidade, ou do seu pasaporte ou outro documento válido que o identifique e, no seu caso, da persoa que o represente, ou instrumentos electrónicos equivalentes; así como o documento ou instrumento electrónico acreditativo de tal representación. A utilización de firma electrónica identificativa do afectado eximirá da presentación das fotocopias do DNI ou documento equivalente.

- Petición en que se concreta a solicitude.

- Dirección para os efectos de notificacións, data e sinatura do solicitante.

- Documentos acreditativos da petición que formula, se é o caso.

Contestación

- O responsable do tratamento deberá contestar a solicitude que se lle dirixa en todo caso, con independencia de que figuren ou non datos persoais do afectado nos seus ficheiros.

- No caso de que a solicitude non reúna os requisitos especificados, deberá solicitarse a emenda destes.

- Corresponderá ao responsable do tratamento a proba do cumprimento do deber de resposta, e debe conservar a acreditación do cumprimento do mencionado deber.

- O responsable do ficheiro deberá adoptar as medidas oportunas para garantir que as persoas da súa organización que teñen acceso a datos de carácter persoal poidan informar do procedemento que debe seguir o afectado para o exercicio dos seus dereitos.

6.1.4 Dereitos ante o encargado do tratamento

Cando os afectados exercitasen os seus dereitos ante un encargado do tratamento e solicitasen o exercicio do seu dereito ante este, o encargado deberá dar traslado da solicitude ao responsable, co fin de que por este se resolva, a menos que na relación existente co responsable do tratamento se prevexa precisamente que o encargado atenderá, por conta do responsable, as solicitudes de exercicio polos afectados dos seus dereitos de acceso, rectificación, cancelación ou oposición.

6.2 Dereito de acceso

6.2.1 Concepto e exercicio

Concepto do dereito de acceso

O dereito de acceso é o dereito do afectado a obter información sobre se os seus propios datos de carácter persoal están a ser obxecto de tratamento; a finalidade do tratamento que, se é o caso, se estea a realizar; así como a información dispoñible sobre a orixe dos devanditos datos e as comunicacións realizadas ou previstas destes.

En virtude do dereito de acceso, o afectado poderá obter do responsable do tratamento información relativa a datos concretos, a datos incluídos nun determinado ficheiro, ou á totalidade dos seus datos sometidos a tratamento.

Non obstante, cando razóns de especial complexidade o xustifiquen, o responsable do ficheiro poderá solicitar do afectado a especificación dos ficheiros respecto dos cales queira exercitar o dereito de acceso, a cuxo efecto deberá facilitarlle unha relación de todos eles.

O dereito de acceso é independente do que outorgan aos afectados as leis especiais e, en particular, a Lei 30/1992, de 26 de noviembre, de réxime xurídico das Administracións públicas e do procedemento administrativo común.

Exercicio do dereito de acceso

Ao exercitar o dereito de acceso, o afectado poderá optar por recibir a información a través dun ou varios dos seguintes sistemas de consulta do ficheiro:

- visualización en pantalla;
- escrito, copia ou fotocopia remitida por correo, certificado ou non;
- telecopia;
- correo electrónico ou outros sistemas de comunicacións electrónicas;
- calquera outro sistema que sexa adecuado á configuración ou implantación material do ficheiro ou á natureza do tratamento, ofrecido polo responsable.

Os sistemas de consulta do ficheiro poderán restrinxirse en función da configuración ou implantación material do ficheiro ou da natureza do tratamento, sempre que o que se ofreza ao afectado sexa gratuíto e asegure a comunicación escrita se este así o esixe.

Se se ofrece un determinado sistema para facer efectivo o dereito de acceso e o afectado o rexeitase, o responsable do tratamento non responderá polos posibles riscos que para a seguridade da información puidesen derivarse da elección.

Se se ofrece un procedemento para facer efectivo o dereito de acceso e o afectado esixise que este se materializase a través dun procedemento que implique un custo desproporcionado, surtindo o mesmo efecto e garantindo a mesma seguridade o procedemento ofrecido polo responsable, serán de conta do afectado os gastos derivados da súa elección.

6.2.2 Contestación: outorgamento e denegación do acceso

Outorgamento do acceso

Debe resolverse sobre a solicitude de acceso no prazo máximo dun mes a contar dende a recepción da solicitude. Se nese prazo non se responde de forma expresa á petición, o interesado poderá interpoñer unha reclamación ante a AEPD.

Se non se teñen datos de carácter persoal de quen realiza a solicitude, débeselle comunicar no mesmo prazo dun mes.

Se a solicitude se estima pero non se acompaña á comunicación a información, o acceso farase efectivo durante os dez días seguintes á devandita comunicación.

A información que se proporcione, calquera que sexa o soporte en que for facilitada, darase en forma lexible e intelixible, sen utilizar claves ou códigos que requiran o uso de dispositivos mecánicos específicos.

A devandita información comprenderá todos os datos de base do afectado, os resultantes de calquera elaboración ou proceso informático, así como a información dispoñible sobre a orixe dos datos, os cesionarios destes e a especificación dos usos e finalidades concretos para os que se almacenaron os datos.

Denegación de acceso

Poderase denegar o acceso aos datos de carácter persoal cando o dereito xa se exercite nos doce meses anteriores á solicitude, salvo que se acredite un interese lexítimo para o efecto.

Tamén poderá denegarse o acceso nos supostos en que así o prevexa unha lei ou unha norma de dereito comunitario de aplicación directa ou cando estas impidan ao responsable do tratamento revelar aos afectados o tratamento dos datos aos que se refira o acceso.

En todo caso, informarase o afectado do seu dereito a solicitar a tutela da Axencia Española de Protección de Datos.

6.3 Dereitos de rectificación e cancelación

6.3.1 Concepto e exercicio

O **dereito de rectificación** é o dereito do afectado a que se modifiquen os datos que resulten ser inexactos ou incompletos.

O **dereito de cancelación** é o que dará lugar a que se supriman os datos que resulten ser inadecuados ou excesivos, sen prexuízo do deber de bloqueo dos devanditos datos..

Exercicio dos dereitos de rectificación e cancelación

A solicitude de rectificación deberá indicar a que datos se refire e a corrección que haxa de realizarse, e deberá ir acompañada da documentación xustificativa do solicitado.

Na solicitude de cancelación, o interesado deberá indicar a que datos se refire, e achegar ao efecto a documentación que o xustifique, se é o caso.

Contestación á solicitude

O responsable do ficheiro resolverá sobre a solicitude de rectificación ou cancelación no prazo máximo de dez días a contar dende a recepción da solicitude. Se nese prazo non se responde de forma expresa á petición, o interesado poderá interpoñer unha reclamación ante a AEPD.

Se non se teñen datos de carácter persoal de quen realiza a solicitude, debe comunicárselle no mesmo prazo de dez días.

6.3.2 Comunicación ao cesionario

Se os datos rectificados ou cancelados fosen cedidos previamente, o responsable do ficheiro deberá comunicar a rectificación ou cancelación efectuada ao cesionario, en idéntico prazo, para que este, tamén no prazo de dez días contados dende a recepción da devandita comunicación, proceda, así mesmo, a rectificar ou cancelar os datos.

A rectificación ou cancelación efectuada polo cesionario non requirirá comunicación ningunha ao interesado, sen prexuízo do exercicio dos dereitos por parte dos interesados recoñecidos na LOPD.

6.3.3 Denegación dos dereitos de rectificación e cancelación.

A cancelación non procederá cando os datos de carácter persoal deban ser conservados durante os prazos previstos nas disposicións aplicables ou, no seu caso, nas relacións contractuais entre a persoa ou entidade responsable do tratamento e o interesado que xustificaron o tratamento dos datos.

Poderá tamén denegarse os dereitos de rectificación ou cancelación nos supostos en que así o prevexa unha lei ou unha norma de dereito comunitario de aplicación directa ou cando estas impidan ao responsable do tratamento revelar aos afectados o tratamento dos datos aos que se refira o acceso.

En todo caso, informarase o afectado do seu dereito a solicitar a tutela da Axencia Española de Protección de Datos.

6.4 Dereito de oposición

6.4.1 Concepto e exercicio

Concepto do dereito de oposición

É o dereito do afectado a que non se leve a cabo o tratamento dos seus datos de carácter persoal ou se cese neste nos seguintes supostos:

- Cando non sexa necesario o seu consentimento para o tratamento, como consecuencia da concorrencia dun motivo lexítimo e fundado, referido á súa concreta situación persoal, que o xustifique, sempre que unha lei non dispoña o contrario.
- Cando se trate de ficheiros que teñan por finalidade a realización de actividades de publicidade e prospección comercial, calquera que sexa a empresa responsable da súa creación.
- Cando o tratamento teña por finalidade a adopción dunha decisión referida ao afectado e baseada unicamente nun tratamento automatizado dos seus datos de carácter persoal.

Exercicio do dereito de oposición

O dereito de oposición exercitarase mediante solicitude dirixida ao responsable do tratamento.

Cando a oposición se realice con base a que non foi necesario o seu consentimento para o tratamento, deberán facerse constar os motivos fundados e lexítimos, relativos a unha concreta situación persoal do afectado, que xustifican o exercicio deste dereito.

6.4.2 Contestación

O responsable do ficheiro resolverá sobre a solicitude de oposición no prazo máximo de dez días a contar dende a recepción da solicitude. Se nese prazo non se responde de forma expresa á petición, o interesado poderá interpoñer unha reclamación ante a AEPD.

No caso de que non dispoña de datos de carácter persoal dos afectados, deberá igualmente comunicárllelo no mesmo prazo.

6.4.3 Exclusión ou denegación

O responsable do ficheiro ou tratamento deberá excluír do tratamento os datos relativos ao afectado que exercite o seu dereito de oposición ou denegar motivadamente a solicitude do interesado no prazo de dez días.

6.4.4 Dereito de oposición ás decisións baseadas unicamente nun tratamento automatizado de datos.

Concepto

Os interesados teñen dereito a non se ver sometidos a unha decisión con efectos xurídicos sobre eles ou que lles afecte de xeito significativo, que se basee unicamente nun tratamento automatizado de datos destinado a avaliar determinados aspectos da súa personalidade, tales como o seu rendemento laboral, o seu crédito, a súa fiabilidade ou a súa conduta.

Excepcións

- Que se adoptase no marco da celebración ou execución dun contrato a petición do interesado, sempre que se lle outorgue a posibilidade de alegar o que considerara pertinente, co fin de defender o seu dereito ou interese. En todo caso, o responsable do ficheiro deberá informar previamente o afectado, de forma clara e precisa, de que se adoptarán decisións nas que se avaliarán aspectos da súa personalidade e cancelará os datos en caso de que non chegue a asinarse finalmente o contrato.

- Que a decisión baseada no tratamento automatizado estea autorizada por unha norma con rango de lei que estableza medidas que garantan o interese lexítimo do interesado.

6.5 Tutela dos dereitos e indemnización

Tutela dos dereitos

Cando a un interesado se lle denegue, total ou parcialmente, o exercicio dos dereitos de oposición, acceso, rectificación ou cancelación, poderá poñelo en coñecemento da AEPD, que deberá asegurarse da procedencia ou improcedencia da denegación e ditar resolución expresa de tutela de dereitos en seis meses.

Dereito a indemnización

Os interesados que sufran dano ou lesión nos seus bens ou dereitos a causa dun incumprimento do establecido na LOPD terán dereito a ser indemnizados.

Cando se trate de ficheiros de titularidade pública, a responsabilidade esixirase de acordo coa lexislación reguladora do réxime de responsabilidade das Administracións públicas.

No caso dos ficheiros de titularidade privada, a acción exercitarase ante os órganos da xurisdición ordinaria.

6.6 Modelo de formulario para o exercicio de dereitos ARCO

Formulario para o exercicio de dereitos de acceso, rectificación, cancelación ou oposición (A.R.C.O):
D/DNa._____, DNI_____,
Domicilio_____; CP_____,
Localidad_____, Provincia _____, Teléfono _____.
Solicita (sinalar que proceda):
Exercitar o dereito de acceso sobre os seus datos de carácter persoal, solicitando que se lle remita información por correo á dirección anteriormente indicada.
Exercitar o dereito de rectificación dos seguintes datos de carácter persoal, no sentido que se indica a continuación:
_____
_____
Exercitar o dereito de cancelación dos datos de todos os arquivos/ficheiros de _____ (datos do responsable do ficheiro)
Exercitar o dereito de oposición ao tratamento os seus datos para as seguintes finalidades:
_____
_____
Deberase entregar o formulario debidamente cuberto e achegando unha fotocopia de DNI ou documento equivalente que acredite a identidade do solicitante. Se actúa en representación dun terceiro deberá achegarse DNI do representante e documento acreditativo da representación do interesado.
O seguinte formulario deberá remitirse por correo a _____(nombre do responsable do ficheiro e dirección onde se pode remitir a solicitude).
Co envío do presente formulario, vostede presta o seu consentimento e dáse por informado de que os datos que voluntariamente facilite a través deste serán incorporados no ficheiro non automatizado denominado "Solicitudes de Exercicios ARCO", cuxo responsable é _____ (nome responsable do ficheiro), e con domicilio en _____(dirección do responsable do ficheiro). A recollida e tratamento dos seus datos terá como finalidade exclusiva a xestión axeitada do exercicio dos dereitos de acceso, rectificación, cancelación e oposición en relación cos seus datos tal e como se indica no presente formulario.

7 Acceso a datos conta de terceiros e prestación de servizos sen acceso a datos

7 Acceso a datos por conta de terceiros e prestación de servizos sen acceso a datos

7.1 Acceso a datos por conta de terceiros

Acceso en locais do responsable de tratamento ou acceso remoto

Cando o responsable do ficheiro ou tratamento facilite o acceso aos datos, aos soportes que os conteñan ou aos recursos do sistema de información que os trate a un encargado de tratamento que preste os seus servizos nos locais do primeiro, deberá facerse constar esta circunstancia no documento de seguridade do devandito responsable, e o persoal do encargado comprometerase ao cumprimento das medidas de seguridade previstas no citado documento.

Cando o devandito acceso sexa remoto, despois de prohibirse ao encargado incorporar tales datos a sistemas ou soportes distintos dos do responsable, este último deberá facer constar esta circunstancia no documento de seguridade do responsable, e o persoal do encargado comprometerase ao cumprimento das medidas de seguridade previstas no citado documento.

Acceso en locais do encargado

Se o servizo fose prestado polo encargado do tratamento nos seus propios locais, alleos aos do responsable do ficheiro, deberá elaborar un documento de seguridade ou completar o que xa tivese elaborado, se é o caso, identificando o ficheiro ou tratamento e o responsable deste, e incorporando as medidas de seguridade que cómpre implantar en relación co devandito tratamento.

O acceso aos datos polo encargado do tratamento estará sometido ás medidas de seguridade establecidas na normativa de protección de datos de carácter persoall.

Identificación de accesos por terceiros

Cando exista un tratamento de datos por conta de terceiros, o documento de seguridade deberá conter a identificación dos ficheiros ou tratamentos que se traten en concepto de encargado con referencia expresa ao contrato ou documento que regule as condicións do encargo, así como da identificación do responsable e do período de vixencia do encargo.

Delegación total do tratamento no encargado

Naqueles casos nos que datos persoais dun ficheiro ou tratamento se incorporen e traten de modo exclusivo nos sistemas do encargado, o responsable deberá anotalo no seu documento de seguridade. Cando tal circunstancia afectase a parte ou á totalidade dos ficheiros ou tratamentos do responsable, poderá delegarse no encargado a levanza do documento de seguridade, salvo no relativo a aqueles datos contidos en recursos propios.

Este feito indicarase de modo expreso no contrato asinado entre o responsable do ficheiro e o encargado do tratamento, con especificación dos ficheiros ou tratamentos afectados.

Nestes casos, atenderase ao documento de seguridade do encargado para o efecto do cumprimento do disposto pola normativa sobre protección de datos de carácter persoal.

7.2 Prestacións de servizos sen acceso a datos persoais

O responsable do ficheiro ou tratamento adoptará as medidas axeitadas para limitar o acceso do persoal a datos persoais, aos soportes que os conteñan ou aos recursos do sistema de información, para a realización de traballos que non impliquen o tratamento de datos persoais.

Cando se trate de persoal alleo, o contrato de prestación de servizos recollerá expresamente a prohibición de acceder aos datos persoais e a obriga de segredo respecto aos datos que o persoal puidese coñecer con motivo da prestación do servizo.

8 Particularidades de determinados tipos de ficheiros

8 Particularidades de determinados tipos de ficheiros

8.1 Ficheiros de información sobre solvencia patrimonial ou crédito

Procedencia dos datos

Os que se dediquen á prestación de servizos de información sobre a solvencia patrimonial e o crédito só poderán tratar datos de carácter persoal obtidos dos rexistros e as fontes accesibles ao público establecidos para o efecto ou procedentes de informacións facilitadas polo interesado ou co seu consentimento.

Exercicio dos dereitos de acceso, rectificación, cancelación e oposición

Réxese polo disposto de modo xeral para o resto dos ficheiros cos seguintes criterios:

- Cando a petición de exercicio dos dereitos se dirixise ao responsable do ficheiro, este estará obrigado a satisfacer, en calquera caso, os devanditos dereitos.
- Se a petición se dirixise ás persoas e entidades ás que se presta o servizo, estas unicamente deberán comunicar ao afectado aqueles datos relativos a el que lles fosen comunicados e a facilitar a identidade do responsable para que, se é o caso, poidan exercitar os seus dereitos ante este.

8.2 Tratamento de datos relativos ás obrigas monetarias

O tratamento de datos relativos ao cumprimento ou incumprimento de obrigas monetarias facilitados polo acredor ou por quen actúe pola súa conta ou interese, implica:

Requisitos para a inclusión dos datos

- Existencia previa dunha débeda certa, vencida, esixible, que resultase impagada.
- Que non transcorresen seis anos dende a data en que houbo de procederse ao pagamento da débeda ou do vencemento da obriga ou do prazo concreto se aquela fose de vencemento periódico.

- Requirimento previo de pagamento a quen corresponda o cumprimento da obriga.

Información previa á inclusión dos datos no ficheiro

- O acredor deberá informar o debedor, no momento en que se asine o contrato e, en todo caso, ao tempo de efectuar o requirimento, que en caso de non se producir o pagamento no termo previsto para iso e cumprirse os requisitos previstos, os datos relativos ao non pagamento poderán ser comunicados a ficheiros relativos ao cumprimento ou incumprimento de obrigas monetarias.

- O acredor ou quen actúe pola súa conta ou interese estará obrigado a conservar a disposición do responsable do ficheiro común e da Axencia Española de Protección de Datos documentación abonda que acredite o cumprimento dos requisitos establecidos para a inclusión dos datos e do requirimento previo.

Notificación da inclusión

- O responsable do ficheiro común deberá notificar aos interesados respecto dos que rexistrasen datos de carácter persoal, no prazo de trinta días dende o devandito rexistro, unha referencia dos que fosen incluídos, informándoo así mesmo da posibilidade de exercitar os seus dereitos de acceso, rectificación, cancelación e oposición, nos termos establecidos pola LOPD.

- Efectuarase unha notificación por cada débeda concreta e determinada con independencia de que esta se teña con este ou con distintos acredores.

- A notificación deberá efectuarse a través dun medio fiable, auditable e independente da entidade notificante, que lle permita acreditar a efectiva realización dos envíos.

- En todo caso, será necesario que o responsable do ficheiro poida coñecer se a notificación foi obxecto de devolución por calquera causa, en cuxo caso non poderá proceder ao tratamento dos datos referidos a ese interesado. Non se entenderán suficientes para que non se poida proceder ao tratamento dos datos referidos a un interesado as devolucións nas que o destinatario rexeitase recibir o envío.

- Se a notificación de inclusión fose devolta, o responsable do ficheiro común comprobará coa entidade acredora que a dirección utilizada para efectuar esta notificación se corresponde coa contractualmente pactada co cliente para os efectos de comunicacións e non procederá ao tratamento dos datos se a mencionada entidade non confirma a exactitude deste dato.

Conservación dos datos

- Só poderán ser obxecto de tratamento os datos que respondan con veracidade á situación da débeda en cada momento concreto. O pagamento ou cumprimento da débeda determinará a cancelación inmediata de todo dato relativo a esta.

- Nos restantes supostos, os datos deberán ser cancelados cando se cumprisen seis anos contados a partir do vencemento da obriga ou do prazo concreto se aquela fose de vencemento periódico.

Acceso á información contida no ficheiro

Os datos contidos no ficheiro común só poderán ser consultados por terceiros cando precisen axuizar a solvencia económica do afectado. En particular, considerarase que concorre a devandita circunstancia nos seguintes supostos:

- Que o afectado manteña co terceiro algún tipo de relación contractual que aínda non se encontre vencida.

- Que o afectado pretenda asinar co terceiro un contrato que implique o pagamento aprazado do prezo.

- Que o afectado pretenda contratar co terceiro a prestación dun servizo de facturación periódica.

Exercicio dos dereitos de acceso, rectificación, cancelación e oposición

Ademais de cumprir o previsto para a xeneralidade de ficheiros para o exercicio dos dereitos, teranse en conta as seguintes regras:

- Se a solicitude se dirixise ao titular do ficheiro común, este deberá comunicar ao afectado todos os datos relativos a este que obren no ficheiro.

- Neste caso, o titular do ficheiro común deberá, ademais de dar cumprimento ao establecido no presente regulamento, facilitar as avaliacións e apreciacións que sobre o afectado se comunicasen nos últimos seis meses e o nome e dirección dos cesionarios.

- Se a solicitude se dirixise a calquera outra entidade participante no sistema, deberá comunicar ao afectado todos os datos relativos a este aos que ela poida acceder, así como a identidade e dirección do titular do ficheiro común para que poida completar o exercicio do seu dereito de acceso.

8.3 Tratamento para actividades de publicidade e prospección comercial

Deben cumprir cos requisitos que se expoñerán a continuación as seguintes empresas:

- As que se dediquen á recompilación de direccións, repartición de documentos, publicidade, venda a distancia, prospección comercial e outras actividades análogas.

- As que realicen estas actividades co fin de comercializar os seus propios produtos ou servizos ou os de terceiros

8.3.1 Datos susceptibles de tratamento

Só poderán utilizar nomes e direccións ou outros datos de carácter persoal cando estes se encontren nun dos seguintes casos:

- Cando figuren nunha fonte accesible ao público e o interesado non manifestase a súa negativa ou oposición a que os seus datos sexan obxecto de tratamento para as actividades descritas neste apartado.

- Cando fosen facilitados polos propios interesados ou obtidos co seu consentimento para finalidades determinadas, explícitas e lexítimas relacionadas coa actividade de publicidade ou prospección comercial, despois de informar os interesados sobre os sectores específicos e concretos de actividade respecto dos que poderá recibir información ou publicidade.

Cales se consideran pola LOPD fontes accesibles ao público?

- O censo promocional.

- As guías de servizos de comunicacións electrónicas.

- As listaxes de persoas pertencentes a grupos de profesionais que conteñan unicamente os datos de nome, título, profesión, actividade, grao académico, dirección profesional e indicación da súa pertenza ao grupo. No caso de colexios profesionais, poderán indicarse como datos de pertenza ao grupo os de número de colexiado, data de incorporación e situación de exercicio profesional.

- Os diarios e boletíns oficiais.

- Os medios de comunicación social.

8.3.2 Deber de información ao interesado

Cando os datos procedan de fontes accesibles ao público e se destinen á actividade de publicidade ou prospección comercial, deberá informarse ao interesado en cada comunicación que se lle dirixa da orixe dos datos (que foron obtidos de fontes accesibles ao público e da entidade da que se obtivesen) e da identidade do responsable do tratamento así como dos dereitos que lle asisten, con indicación de ante quen poderán exercitarse.

8.3.3 Campañas de publicidade entre os clientes

Cando unha empresa queira realizar unha campaña de publicidade dos seus produtos ou servizos entre os seus clientes, poderá:

- Realizar por si mesma unha actividade publicitaria dos seus produtos ou servizos entre os seus clientes, para o cal deberá contar co consentimento inequívoco do cliente para que os seus datos sexan utilizados para tal fin.

- Contratar a terceiros para a realización da campaña publicitaria dos seus produtos ou servizos, encomendándolle o tratamento de determinados datos; nese caso aplicaranse as seguintes normas:

  - Cando os parámetros identificativos dos destinatarios da campaña sexan fixados pola entidade que contrate a campaña, esta será responsable do tratamento dos datos.

  - Cando os parámetros fosen determinados unicamente pola entidade ou entidades contratadas, as devanditas entidades serán as responsables do tratamento.

  - Cando na determinación dos parámetros interveñan ambas as dúas entidades, serán ambas as dúas responsables do tratamento.

Que se consideran parámetros identificativos?

As variables utilizadas para identificar o público obxectivo ou destinatario dunha campaña ou promoción comercial de produtos ou servizos que permitan acoutar os destinatarios individuais desta.

Ao encargar a campaña a un terceiro deberanse adoptar as medidas necesarias para asegurarse de que a entidade contratada solicitou os datos cumprindo as esixencias da normativa de protección de datos.

8.3.4 Ficheiros de exclusión do envío de comunicacións comerciais

Cando un afectado manifeste a súa negativa a recibir publicidade, poderanse conservar os mínimos datos imprescindibles para identificalo e adoptar as medidas necesarias que eviten o envío de publicidade.

É posible a creación de ficheiros comúns, de carácter xeral ou sectorial, nos que sexan obxecto de tratamento os datos de carácter persoal que resulten necesarios para evitar o envío de comunicacións comerciais aos interesados que manifesten a súa negativa ou oposición a recibir publicidade. Os citados ficheiros poderán conter os mínimos datos imprescindibles para identificar o afectado.

8.3.5 Exercicio dos dereitos de acceso, rectificación, cancelación e oposición

No caso de exercicio dos dereitos de acceso, rectificación e cancelación, ademais de cumprir o previsto para a xeneralidade de ficheiros para o exercicio dos dereitos, deberase:

- Se o dereito se exercitase ante unha entidade que encargase a un terceiro a realización dunha campaña publicitaria, aquela estará obrigada, no prazo de dez días dende a recepción da comunicación da solicitude de exercicio de dereitos do afectado, a comunicar a solicitude ao responsable do ficheiro co fin de que este outorgue ao afectado o seu dereito no prazo de dez días dende a recepción da comunicación, dando conta del ao afectado.

- No caso de exercicio do dereito de oposición, ademais dos requisitos previstos para o dito exercicio na normativa, deberá terse en conta que:

  - Se o dereito de oposición se exercitase ante unha entidade que encomendase a un terceiro a realización dunha campaña p ublicitaria, aquela estará obrigada, no prazo de dez días dende a recepción da comunicación da solicitude de exercicio de dereitos do afectado, a comunicar a solicitude ao responsable do ficheiro co fin de que este atenda o dereito do afectado no prazo de dez días dende a recepción da comunicación, dando conta del ao afectado.

9 Transferencias internacionais de datos

9 Transferencias internacionais de datos

9.1 Autorización e notificación

Para que a transferencia internacional de datos poida considerarse conforme á normativa de protección de datos, será necesaria a autorización do Director da Axencia Española de Protección de Datos.

A autorización non será necesaria:

- Cando o Estado no que se encontrase o importador ofreza un nivel axeitado de protección.
- Cando a transferencia se encontre nun dos seguintes supostos:
  - Resulte da aplicación de tratados ou convenios nos que sexa parte España.
  - Sexa feita para os efectos de prestar ou solicitar auxilio xudicial internacional.
  - Sexa necesaria para a prevención ou para o diagnóstico médico, a prestación de asistencia sanitaria ou tratamento médico, ou a xestión de servizos sanitarios.
  - Faga referencia a transferencias monetarias conforme á súa lexislación específica.
  - O afectado dese o seu consentimento inequívoco á transferencia prevista.
  - Sexa necesaria para a execución dun contrato entre o afectado e o responsable do ficheiro ou para a adopción de medidas precontractuais adoptadas a petición do afectado.
  - Sexa necesaria para a celebración ou execución dun contrato celebrado ou por celebrar, en interese do afectado, polo responsable do ficheiro e un terceiro.
  - Sexa esixida necesaria ou legalmente para a salvagarda dun interese público.
  - Sexa precisa para o recoñecemento, exercicio ou defensa dun dereito nun proceso xudicial.

- Sexa efectuada, a petición dunha persoa con interese lexítimo, dende un rexistro público e aquela sexa acorde coa finalidade deste.

- Teña como destino un Estado membro da Unión Europea, ou un Estado respecto do cal a Comisión das Comunidades Europeas, no exercicio das súas competencias, declarase que garante un nivel de protección axeitado.

En todo caso, a transferencia internacional de datos deberá ser notificada co fin de proceder á súa inscrición no Rexistro Xeral de Protección de Datos.

Transferencias a Estados que proporcionen un nivel axeitado de protección

Considéranse países cun nivel axeitado de protección:

- Suiza.
- as entidades estadounidenses adheridas aos principios de "Porto Seguro",
- Canadá respecto das entidades suxeitas ao ámbito de aplicación da lei canadense de protección de datos,
- Arxentina,
- Guernsey,
- Illa de Man,
- Jersey,
- Illas Faeroe,
- Andorra,
- Israel.

9.2 Transferencias a Estados que non proporcionen un nivel axeitado de protección

Cando a transferencia teña por destino un Estado respecto do que non se declarase pola Comisión Europea ou non se considerase polo Director da Axencia Española de Protección de Datos que existe un nivel axeitado de protección, será necesario solicitar a autorización do Director da Axencia Española de Protección de Datos.

A autorización poderá ser outorgada en caso de que o responsable do ficheiro ou tratamento achegue un contrato escrito, celebrado entre o exportador e o importador, no que consten as necesarias garan-

tías de respecto á protección da vida privada dos afectados e aos seus dereitos e liberdades fundamentais e se garanta o exercicio dos seus respectivos dereitos.

O director da Axencia Española de Protección de Datos poderá denegar ou suspender temporalmente, logo de audiencia do exportador, a transferencia cando concorra algunha das circunstancias seguintes:

- Que a situación de protección dos dereitos fundamentais e liberdades públicas no país de destino ou a súa lexislación impidan garantir o cumprimento íntegro do contrato e o exercicio polos afectados dos dereitos que o contrato garante.

- Que a entidade destinataria incumprise previamente as garantías establecidas en cláusulas contractuais deste tipo.

- Que existan indicios racionais de que as garantías ofrecidas polo contrato non están a ser ou non serán respectadas polo importador.

- Que existan indicios racionais de que os mecanismos de aplicación do contrato non son ou non serán efectivos.

- Que a transferencia, ou a súa continuación, en caso de iniciarse, puidese crear unha situación de risco de dano efectivo aos afectados.

9.3 Procedemento de autorización de transferencias internacionais de datos

O procedemento para a obtención da autorización para as transferencias internacionais de datos a países terceiros iniciarase sempre por solicitude do exportador que pretenda levar a cabo a transferencia.

Na súa solicitude, ademais dos requisitos legalmente esixidos, o exportador deberá consignar, en todo caso:

- A identificación do ficheiro ou ficheiros a cuxos datos se refira a transferencia internacional, con indicación da súa denominación e código de inscrición do ficheiro no Rexistro Xeral de Protección de Datos.

- A transferencia ou transferencias respecto das que se solicita a autorización, con indicación da finalidade que a xustifica.

- A documentación que incorpore as garantías esixibles para a obtención da autorización así como o cumprimento dos requisitos legais necesarios para a realización da transferencia, se é o caso.

- Cando a autorización se fundamente na existencia dun contrato entre o exportador e o importador dos datos, deberá achegarse copia deste, acreditándose así mesmo a concorrencia de poder abondo nos seus outorgantes.

Cando o director da Axencia Española de Protección de Datos resolva autorizar a transferencia internacional de datos, darase traslado da resolución de autorización ao Rexistro Xeral de Protección de Datos, co fin de proceder á súa inscrición.

O prazo máximo para ditar e notificar resolución será de tres meses, a contar dende a data de entrada na Axencia Española de Protección de Datos da solicitude. Se no devandito prazo non se ditase e se notificase resolución expresa, entenderase autorizada a transferencia internacional de datos.

10 Infraccións e sancións

10 Infraccións e sancións

Os responsables do tratamento de datos de carácter persoal e os encargados do seu tratamento están sometidos ao réxime sancionador da Lei orgánica de protección de datos (LOPD).

10.1 Infraccións en materia de protección de datos de carácter persoal

A LOPD cualifica as infraccións en leves, graves e moi graves.

10.1.1 Infraccións moi graves

- A recollida de datos en forma enganosa ou fraudulenta.
- Tratar ou ceder os datos de carácter persoal relativos á ideoloxía, afiliación sindical, relixión, crenzas, orixe racial, saúde, vida sexual e relativos á comisión de infraccións penais ou administrativas, se non se está nun dos supostos en que a lei o autoriza ou violentar a prohibición de crear ficheiros coa finalidade exclusiva de almacenar datos de carácter persoal que revelen a ideoloxía, afiliación sindical, relixión, crenzas, orixe racial ou étnica, ou vida sexual.
- Non cesar no tratamento ilícito de datos de carácter persoal cando existise un previo requirimento do director da Axencia Española de Protección de Datos para iso.
- A transferencia internacional de datos de carácter persoal con destino a países que non proporcionen un nivel de protección equiparable sen autorización do director da Axencia Española de Protección de Datos salvo nos supostos nos que conforme a esta Lei e as súas disposicións de desenvolvemento a devandita autorización non resulta necesaria.

10.1.2 Infraccións graves

- Proceder á creación de ficheiros de titularidade pública ou iniciar a recollida de datos de carácter persoal para estes, sen autorización de disposición xeral, publicada no Boletín Oficial do Estado ou diario oficial correspondente.

- Tratar datos de carácter persoal sen solicitar o consentimento das persoas afectadas, cando este sexa necesario conforme á normativa de protección de datos.

- Tratar datos de carácter persoal ou usalos posteriormente, cando os devanditos datos non sexan adecuados, pertinentes, exactos nin estean postos ao día ou se usen para finalidades incompatibles con aquelas para as que foron recollidos.

- A vulneración do deber de gardar segredo acerca do tratamento dos datos de carácter persoal.

- O impedimento ou o obstáculo do exercicio dos dereitos de acceso, rectificación, cancelación e oposición.

- O incumprimento do deber de información ao afectado acerca do tratamento dos seus datos de carácter persoal cando os datos non sexan solicitados do propio interesado.

- O incumprimento dos restantes deberes de notificación ou requirimento ao afectado impostos pola normativa de protección de datos de carácter persoal.

- Manter os ficheiros, locais, programas ou equipos que conteñan datos de carácter persoal sen as debidas condicións de seguridade.

- Non atender os requirimentos ou apercibimentos da Axencia Española de Protección de Datos ou non proporcionarlle cantos documentos e informacións sexan solicitados por esta.

- A obstrución ao exercicio da función inspectora.

- A comunicación ou cesión dos datos de carácter persoal sen contar con lexitimación para iso.

10.1.3 Infraccións leves

- Non remitir á AEPD as notificacións previstas na normativa de protección de datos.

- Non solicitar a inscrición do ficheiro de datos de carácter persoal no Rexistro Xeral de Protección de Datos.

- O incumprimento do deber de información ao afectado acerca do tratamento dos seus datos de carácter persoal cando os datos sexan solicitados do propio interesado.

- A transmisión dos datos a un encargado do tratamento sen asinar un contrato onde se regule a realización de tratamentos por conta do terceiro e as medidas de seguridade que este debe adoptar.

10.2 Sancións en materia de protección de datos de carácter persoal

A AEPD ten a potestade de impoñer sancións de conformidade coa gravidade da infracción.

10.2.1 Sancións

- As infraccións leves serán sancionadas con multa de 900 a 40.000 euros.
- As infraccións graves serán sancionadas con multa de 40.001 a 300.000 euros.
- As infraccións moi graves serán sancionadas con multa de 300.001 a 600.000 euros.

10.2.2 Gradación das sancións

Os tramos que establecen para as sancións son tan amplas que se establecen unha serie de criterios que a AEPD debe ter en conta para graduar a sanción:

- o carácter continuado da infracción;
- o volume dos tratamentos efectuados;
- a vinculación da actividade do infractor coa realización de tratamentos de datos de carácter persoal;
- o volume de negocio ou actividade do infractor;
- os beneficios obtidos como consecuencia da comisión da infracción;
- o grao de intencionalidade;
- a reincidencia por comisión de infraccións da mesma natureza;
- a natureza dos prexuízos causados ás persoas interesadas ou a terceiras persoas;
- a acreditación de que con anterioridade aos feitos constitutivos de infracción a entidade imputada tiña implantados procedementos axeitados de actuación na recollida e tratamento dos datos de carácter persoal, sendo a infracción consecuencia dunha anomalía no funcionamento dos devanditos procedementos non debida a unha falta de dilixencia esixible ao infractor;
- calquera outra circunstancia que sexa relevante para determinar o grao de antixuridicidade e de culpabilidade presentes na concreta actuación infractora.

10.2.3 Atenuantes

En caso de que se aprecie a existencia dalgunha das seguintes circunstancias, aplicarase a contía da sanción que se estableza para a infracción anterior en gravidade na escala (así, unha infracción moi grave sancionarase como leve se se aprecia a existencia dunha desas circunstancias):

- Cando se aprecie unha cualificada diminución da culpabilidade do imputado ou da antixuridicidade do feito como consecuencia da concorrencia significativa de varios dos criterios expostos para graduar a sanción, sempre que estes se aprecien en sentido positivo (que non se obtivese beneficio da infracción, que non existise intencionalidade, que o infractor puxese todos os medios ao seu alcance para paliar os efectos da infracción...).

- Cando a entidade infractora regularice a situación irregular de forma dilixente.

- Cando poida apreciarse que a conduta do afectado puido inducir á comisión da infracción.

- Cando o infractor recoñeza espontaneamente a súa culpabilidade.

- Cando se produza un proceso de fusión por absorción e a infracción fose anterior ao devandito proceso, non sendo imputable á entidade absorbente.

10.2.4 Apercibimento

A AEPD poderá non abrir expediente sancionador e limitarse a apercibir o infractor para que tome as medidas correctoras necesarias cando concorran os seguintes presupostos:

- Que os feitos fosen constitutivos de infracción leve ou grave conforme ao disposto nesta lei.

- Que o infractor non fose sancionado ou apercibido con anterioridade.

11 A páxina web da AEPD

11 A páxina web da AEPD

A través da páxina web da AEPD, www.agpd.es, podemos proceder aos seguintes trámites:

- Dar de alta os ficheiros de datos de carácter persoal dos que sexamos responsables; así mesmo, podemos notificar calquera modificación dos devanditos ficheiros ou proceder a dar de baixa un ficheiro, todo iso faise a través do formulario NOTA.

- Efectuar consultas tanto sobre o estado de tramitación das solicitudes que fixésemos a través do formulario NOTA, como do contido das inscricións que realizásemos no Rexistro Xeral de Protección de Datos.

Ademais de para realizar os devanditos trámites, a páxina web da AEPD pode ser unha ferramenta de apoio moi útil para adaptar a nosa empresa á normativa existente en protección de datos; a través das resolucións e informes que en materia de protección de datos emite a Axencia.

12 Consellos e recomendacións

12 Consellos e recomendacións

Cumprir coa normativa de protección de datos é de vital importancia para a nosa empresa, xa que tal e como vimos nesta guía as sancións poden chegar a ser de moi elevada contía; ademais, cada vez de forma máis xeneralizada, os clientes e usuarios son coñecedores dos dereitos que os asisten e da opción que teñen de denunciar ante a Axencia de Protección de Datos cando os devanditos dereitos non son respectados.

Algunhas recomendacións básicas en materia de protección de datos que poden evitar que se produzan denuncias contra a nosa empresa ante a AEPD ou que en caso de producirse atenúen as posibles sancións:

- Ter cláusulas tipo que deben incorporarse a toda a documentación que produza a empresa e que pode ter implicación no ámbito da protección de datos (facturas, correos electrónicos, fax etc.).
- Que todos aqueles terceiros que teñan acceso aos ficheiros con datos de carácter persoal asinen un contrato onde se responsabilicen do cumprimento de todas as obrigas relativas á protección de datos.
- Formación dos traballadores da empresa en materia de protección de datos.
- En caso de que exista algunha incidencia e a seguridade dos datos se vise comprometida, é fundamental reaccionar coa maior celeridade posible e tratar de minimizar os efectos da devandita incidencia.
- Rexistrar debidamente todo o referente aos ficheiros nos que consten datos de carácter persoal (entradas e saídas de ficheiros e soportes, incidencias, acceso de terceiros etc.).
- Realizar auditorías periódicas para verificar o cumprimento das obrigas establecidas pola normativa de protección de datos.

13 Bibliografía

13 Bibliografía

- *Manuales prácticos de xestión: Conceptos xurídicos básicos*. CEEI Galicia S.A. (2010)
- Fichas informativas. Protección de datos. CEEI Galicia S.A.
- Lei orgánica 15/1999, do 13 de decembro, de protección de datos de carácter persoal. BOE núm. 298 do 14 de decembro de 1999.

IGAPE

BIC GALICIA

galicia

UNIÓN EUROPEA
FONDO SOCIAL EUROPEO
"O FSE inviste no teu futuro"

XUNTA DE GALICIA