GOBIERNO DE ESPAÑA
MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO

INTECO
Instituto Nacional de Tecnologías de la Comunicación

Estudio sobre la protección de datos en las empresas españolas

INSTITUTO NACIONAL DE **TECNOLOGÍAS** DE LA **COMUNICACIÓN**

Edición: octubre 2012

El *Estudio sobre la protección de datos en las empresas españolas* ha sido elaborado por el Instituto Nacional de Tecnologías de la Comunicación (INTECO):

Pablo Pérez San-José (dirección)

Susana de la Fuente Rodríguez (coordinación)

Cristina Gutiérrez Borge

Eduardo Álvarez Alonso

INTECO quiere señalar el apoyo técnico en la realización del trabajo de campo e investigación de:

MADISON®

ÍNDICE

PUNTOS CLAVE

El *Estudio sobre la protección de datos en las empresas españolas* tiene por objetivo establecer un diagnóstico de la percepción de cumplimiento de la normativa vigente en materia de protección de datos personales por parte de la pequeña y mediana empresa española en 2012.

Para ello, se ha realizado una encuesta a los responsables de seguridad de 1.109 empresas españolas de menos de 250 empleados repartidas por todo el territorio nacional. Los resultados de la encuesta han sido sometidos a la consideración de un grupo de expertos, cuyas aportaciones han sido esenciales para la comprensión de la situación del sector empresarial español.

Se exponen a continuación los puntos clave del análisis.

I CONOCIMIENTO DE LA NORMATIVA SOBRE PROTECCIÓN DE DATOS

La práctica generalidad del colectivo de pequeñas y medianas empresas españolas conoce la LOPD y es consciente de su sujeción a la misma. Hay muchas más empresas conocedoras de la protección de datos en 2012 que en 2008, gracias a la intensa labor divulgativa de las autoridades de protección de datos.

- El 86,4% de empresas afirma conocer la LOPD; en 2008, el porcentaje era de un 34%.

- Además, el 80,4% de las pequeñas y medianas empresas españolas manifiesta ser conscientes de estar sujetas a la normativa sobre protección de datos.

II EXISTENCIA DE FICHEROS

Las pequeñas y medianas empresas españolas trabajan habitualmente con ficheros con datos personales, especialmente las de mayor tamaño. Los ficheros más frecuentes son los de clientes y proveedores, y los datos personales recogidos en ellos son datos de identificación y detalles de contacto.

- 3 de cada 4 empresas afirman disponer de ficheros con datos personales; entre las microempresas sin asalariados o con menos de 10 empleados el porcentaje es de 73,4%, mientras que en el segmento de medianas empresas de entre 50 y 249 empleados, el 94,3% de ellas manifiesta trabajar con ficheros que contienen datos de carácter personal.

- Los tipos de ficheros más habituales en el tráfico empresarial son los de clientes y proveedores, declarados por la práctica totalidad de las empresas que disponen de ficheros con datos personales (94,5% y 80,2%, respectivamente).

- Por detrás de ellos, con una frecuencia considerablemente inferior, se encuentran los ficheros de nóminas (42,4%), los archivos para la Seguridad Social (32,6%) y los currículos de candidatos (32,1%).

- Datos de contacto como dirección, teléfono y correo electrónico (97,2%), nombre y apellidos (96,1%) y DNI (91,1%) son los datos de carácter personal manejados en mayor medida por las empresas españolas.

III Percepción de adopción de las obligaciones sobre protección de datos

Solo la mitad de las pequeñas y medianas empresas españolas manifiesta cumplir con todas las obligaciones que contempla la normativa española sobre protección de datos. No obstante, el grupo de expertos considera que el nivel de cumplimiento real de la LOPD es, en la mayoría de los casos, inferior al manifestado en la encuesta.

- El 57,5% de las empresas españolas con ficheros con datos de carácter personal afirma haber realizado la inscripción de los mismos en el Registro General de Protección de Datos.

- No obstante, poniendo en relación el número de entidades de titularidad privada que han registrado ficheros ante la AEPD con el total de empresas existentes en España, la estimación de INTECO es que solo un 31,8% de las empresas españolas habría inscrito sus ficheros en la Agencia Española de Protección de Datos.

- La percepción de la pequeña y mediana empresa española en cuanto al cumplimiento normativo es optimista: un 72,7% declara cumplir con el deber de información, un 70,6% afirma solicitar el consentimiento del interesado, y un 51% manifiesta adoptar procedimientos para facilitar y garantizar el ejercicio de los derechos ARCO.

IV PERCEPCIÓN DE ADOPCIÓN DE MEDIDAS DE SEGURIDAD

La percepción de adopción de las medidas de seguridad previstas en el Reglamento de Desarrollo de la LOPD es irregular entre las empresas españolas. Así, coexisten medidas que han sido implantadas de manera generalizada (por ejemplo, el control de acceso a los datos de carácter personal), con otras adoptadas por una minoría de empresas (creación de un registro de incidencias o establecimiento de un protocolo de destrucción de ficheros, por ejemplo).

- Un 56,9% de las empresas españolas con ficheros con datos personales manifiesta disponer de un Documento de Seguridad.

- El personal de las pequeñas y medianas empresas españolas conoce las obligaciones respecto al tratamiento de datos y consecuencias de su incumplimiento. Así, el 48,6% de las empresas manifiesta haber organizado sesiones de formación específica sobre protección de datos personales.

- Por su parte, solo un 30,3% de las empresas participantes en la encuesta reconoce disponer de un registro de incidencias.

- El 77,7% de las entidades afirma que se ha definido quiénes pueden acceder a los datos de carácter personal y las tareas que pueden realizar al respecto.

- El 65,4% de las pequeñas y medianas empresas españolas manifiesta disponer de un sistema de identificación de los usuarios con acceso a los datos de carácter personal. El 77,2% de las empresas españolas afirma haber establecido un sistema de contraseñas para el acceso a los equipos y aplicaciones.

- Algo más de la mitad de las empresas españolas (el 53,9%) declara disponer de un inventario de todos los soportes, electrónicos y en papel, que contienen datos de carácter personal. Más infrecuente es el establecimiento de protocolos de actuación para la destrucción de ficheros, declarado solo por el 37% de las entidades.

- Un 61,8% de las pequeñas y medianas empresas españolas realiza copias de respaldo con periodicidad semanal.

1 INTRODUCCIÓN Y OBJETIVOS

1.1 PRESENTACIÓN

El Instituto Nacional de Tecnologías de la Comunicación, S.A. (INTECO), es una sociedad estatal adscrita al Ministerio de Industria, Energía y Turismo a través de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información.

INTECO es un centro de desarrollo de carácter innovador y de interés público de ámbito nacional que se orienta a la aportación de valor, a la industria y a los usuarios, y a la difusión de las nuevas tecnologías de la información y la comunicación (TIC) en España, en clara sintonía con Europa.

Su objetivo fundamental es servir como instrumento para desarrollar la Sociedad de la Información, con actividades propias en el ámbito de la innovación y el desarrollo de proyectos asociados a las TIC, basándose en tres pilares fundamentales: la investigación aplicada, la prestación de servicios y la formación.

La misión de INTECO es aportar valor e innovación a los ciudadanos, a las empresas, a las Administraciones Públicas y al sector de las tecnologías de la información, a través del desarrollo de proyectos que contribuyan a reforzar la confianza en los servicios de la Sociedad de la Información en nuestro país, promoviendo además una línea de participación internacional.

Para ello, INTECO desarrolla actuaciones en las siguientes líneas:

- **Seguridad tecnológica:** INTECO está comprometido con la promoción de servicios de la Sociedad de la Información cada vez más seguros, que protejan los datos personales de los interesados, su intimidad, la integridad de su información y eviten ataques que pongan en riesgo los servicios prestados. Y, por supuesto, que garanticen un cumplimiento estricto de la normativa legal en materia de TIC. Para ello coordina distintas iniciativas públicas en torno a la seguridad de las TIC, que se materializan en la prestación de servicios por parte del Observatorio de la Seguridad de la Información, el Centro de Respuesta a Incidentes de Seguridad en Tecnologías de la Información (INTECO-CERT), con su Catálogo de Empresas y Soluciones de Seguridad TIC, y la Oficina de Seguridad del Internauta (OSI), de los que se benefician ciudadanos, empresas, administraciones públicas y el sector tecnológico.

- **Accesibilidad:** INTECO promueve servicios de la Sociedad de la Información más accesibles, que supriman las barreras de exclusión, cualquiera que sea la dificultad o carencia técnica, formativa, etc., incluso discapacidad, que tengan sus usuarios. Y que faciliten la integración progresiva de todos los colectivos de

usuarios, de modo que todos ellos puedan beneficiarse de las oportunidades que ofrece la Sociedad de la Información. En particular, INTECO dispone de amplia experiencia en el desarrollo de proyectos en el ámbito de la accesibilidad para la televisión digital, así como de aquellos orientados a garantizar los derechos de los ciudadanos a relacionarse con las administraciones públicas por medios electrónicos, reconocidos en la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.

- **Calidad TIC**: INTECO promueve unos servicios de la Sociedad de la Información que cada vez sean de mayor calidad, que garanticen unos adecuados niveles de servicio, lo cual se traduce en una mayor robustez de aplicaciones y sistemas, un compromiso en la disponibilidad y los tiempos de respuesta, un adecuado soporte para los usuarios, una información precisa y clara sobre la evolución de las funcionalidades de los servicios, y en resumen, servicios cada vez mejores. En esta línea impulsa la competitividad de la industria del Software a través de la promoción de la mejora de la calidad y la certificación de las empresas y profesionales de la ingeniería del software, a través del Laboratorio Nacional de Calidad del Software.

- **Formación**: la formación es un factor determinante para la atracción de talento y para la mejora de la competitividad de las empresas. Por ello, INTECO impulsa la formación de universitarios y profesionales en las tecnologías más demandadas por la industria.

Es uno de los objetivos del Instituto describir de manera detallada y sistemática el nivel de seguridad, privacidad y confianza en la Sociedad de la Información y de generar conocimiento especializado en la materia. De este modo, se encuentra al servicio de los ciudadanos, las empresas y las administraciones públicas españolas para describir, analizar, asesorar y difundir la cultura de la seguridad de la información, la privacidad y la e-confianza.

INTECO ha diseñado un Plan de Actividades y Estudios con el objeto de producir conocimiento especializado y útil en materia de seguridad y privacidad, así como de elaborar recomendaciones y propuestas que definan tendencias válidas para la toma de decisiones futuras por parte de los poderes públicos.

Dentro de este plan de acción se realizan labores de investigación, análisis, estudio, asesoramiento y divulgación que atenderán, entre otras, a las siguientes estrategias:

- Elaboración de estudios e informes propios en materia de seguridad de las Tecnologías de la Información y la Comunicación, con especial énfasis en la Seguridad y privacidad en Internet.

- Seguimiento de los principales indicadores y políticas públicas relacionadas con la seguridad de la información y la confianza en el ámbito nacional e internacional.

- Generación de una base de datos que permita el análisis y evaluación de la seguridad y la confianza con una perspectiva temporal.

- Impulso de proyectos de investigación en materia de seguridad TIC.

- Difusión de estudios e informes publicados por otras entidades y organismos nacionales e internacionales, así como de información sobre la actualidad nacional y europea en materia de la seguridad y confianza en la Sociedad de la Información.

- Asesoramiento a las Administraciones Públicas en materia de seguridad de la información y confianza, así como el apoyo a la elaboración, seguimiento y evaluación de políticas públicas en este ámbito.

1.2 ESTUDIO SOBRE LA PROTECCIÓN DE DATOS EN LAS EMPRESAS ESPAÑOLAS: ANTECEDENTES Y OBJETIVO DE LA INVESTIGACIÓN

El pilar de la legislación española sobre protección de datos es la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD). En virtud de esta ley y de la normativa que la desarrolla (principalmente, reglamento de desarrollo de la LOPD, aprobado por el RD 1720/2007, de 21 de diciembre), se imponen toda una serie de obligaciones tendentes a *garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar*.

Las obligaciones previstas en la normativa sobre protección de datos recaen sobre las personas físicas o jurídicas, de naturaleza pública o privada, que efectivamente decidan sobre la finalidad, contenido y uso del tratamiento de datos personales. Las empresas, en su calidad de responsables de tratamiento, están incluidas en el ámbito de aplicación de la ley.

Los últimos datos del Instituto Nacional de Estadística (INE)[1] dibujan un mapa de 3.199.617 empresas en España, de las cuales 3.194.694 tienen menos de 199 asalariados. Más del 99% del tejido empresarial español está constituido por organizaciones que encajan en la definición de microempresas, pequeñas y medianas empresas, de acuerdo con lo dispuesto por la Comisión Europea.

[1] Directorio Central de Empresas (DIRCE), datos de 1 de enero de 2012. Consulta del directorio disponible en: http://www.ine.es/jaxi/menu.do?type=pcaxis&path=/t37/p201/&file=inebase.

Ilustración 1: Definición de microempresas, pequeñas y medianas empresas

Recomendación 2003/361/CE de la Comisión, de 6 de mayo de 2003, sobre la definición de microempresas, pequeñas y medianas empresas [Diario Oficial L 124 de 20.5.2003]

Las microempresas y las pequeñas y medianas empresas se definen en función de sus efectivos y de su volumen de negocios o de su balance general anual:

- **Se define a una mediana empresa como una empresa que ocupa a menos de 250 personas y cuyo volumen de negocios anual no excede de 50 millones de euros o cuyo balance general anual no excede de 43 millones de euros.**
- **Se define a una pequeña empresa como una empresa que ocupa a menos de 50 personas y cuyo volumen de negocios anual o cuyo balance general anual no supera los 10 millones de euros.**
- **Se define a una microempresa como una empresa que ocupa a menos de 10 personas y cuyo volumen de negocios anual o cuyo balance general anual no supera los 2 millones de euros.**

Fuente: Comisión Europea[2]

En este contexto, transcurridos más de diez años desde la entrada en vigor de la normativa sobre protección de datos en España, y considerada la relevancia numérica de las microempresas, pequeñas y medianas empresas en nuestro país, es oportuno realizar un diagnóstico del nivel de cumplimiento normativo en 2012.

INTECO, a través de su Observatorio de la Seguridad de la Información, ha abordado en el pasado proyectos de investigación dirigidos a evaluar el grado de adopción de la LOPD entre las empresas españolas. Así, en 2008 se publicó el *Estudio sobre el grado de adaptación de las Pequeñas y Medianas Empresas españolas a la Ley Orgánica de Protección de Datos (LOPD) y el nuevo Reglamento de Desarrollo (RDLOPD)*[3] y, fruto de sus resultados, en 2009 se editó la *Guía para empresas: cómo adaptarse a la normativa sobre protección de datos*[4].

El *Estudio sobre la protección de datos en las empresas españolas* que ahora presentamos tiene por objetivo establecer un diagnóstico de la percepción de cumplimiento de la normativa vigente en materia de protección de datos personales por parte de la pequeña y mediana empresa española en 2012, realizando un análisis evolutivo de los principales indicadores identificados en la lectura de 2008.

El objetivo general se desglosa, a su vez, en una serie de objetivos específicos, que sirven para articular la estructura del estudio:

[2] Recomendación 2003/361/CE de la Comisión, de 6 de mayo de 2003, sobre la definición de microempresas, pequeñas y medianas empresas [Diario Oficial L 124 de 20.5.2003]

[3] INTECO (2008). *Estudio sobre el grado de adaptación de las Pequeñas y Medianas Empresas españolas a la Ley Orgánica de Protección de Datos (LOPD) y el nuevo Reglamento de Desarrollo (RDLOPD)*. Disponible en: http://www.inteco.es/Seguridad/Observatorio/Estudios/estudio_lopd_pymes

[4] INTECO (2009). *Guía para empresas: cómo adaptarse a la normativa sobre protección de datos*. Disponible en: http://www.inteco.es/Seguridad/Observatorio/guias/GuiaManual_LOPD_pymes

- Conocer hasta qué punto las pequeñas y medianas empresas españolas están familiarizadas con la normativa sobre protección de datos.

- Identificar los hábitos de las empresas en cuanto a tratamiento de ficheros con datos personales, especialmente en lo referente a la tipología de ficheros que utilizan y los datos personales que tratan.

- Comprender cuál es su percepción subjetiva sobre el nivel de cumplimiento de la normativa sobre protección de datos y sobre la adopción de medidas de seguridad y, en los casos en los que es posible, realizar un contraste con la situación real de cumplimiento.

- Conocer cuáles son los perfiles de empresas en función de su conocimiento y cumplimiento de la Ley Orgánica de Protección de Datos.

2 METODOLOGÍA

Para la realización de este estudio se ha utilizado una combinación de técnicas de análisis, que han permitido estructurar el proyecto en las siguientes fases:

- Fase 1: Análisis documental.
- Fase 2: Encuesta a empresas.
- Fase 3: Entrevistas en profundidad a responsables de protección de datos.
- Fase 4: Grupo de expertos.

2.1 FASE 1: ANÁLISIS DOCUMENTAL

Se ha llevado a cabo una investigación exhaustiva de documentación sobre protección de datos, que ha servido para sentar las bases del estudio y enriquecer el análisis. Particularmente, se ha prestado especial atención a la legislación española y europea sobre privacidad, información procedente de la Agencia Española de Protección de Datos (AEPD), estudios previos elaborados por INTECO y consultas a los sitios web de la Agencia de Protección de Datos de la Comunidad de Madrid, la Agencia Vasca de Protección de Datos y la Autoridad Catalana de Protección de Datos.

La siguiente relación proporciona una visión de los documentos considerados en esta fase:

- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
  http://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/estatal/common/pdfs/Ley-15_99.pdf
- Real decreto por el que se aprueba el Reglamento de Desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre de Protección de Datos de Carácter Personal.
  http://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/estatal/common/pdfs/RD_1720_2007.pdf
- Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a su libre circulación
  http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:1995:281:0031:0050:ES:PDF

- Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos). http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:ES:PDF

- Agencia Española de Protección de Datos (2011). *El derecho fundamental a la protección de datos: Guía para el Ciudadano.* http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/GUIA_CIUDADANO_OK.pdf

- Agencia Española de Protección de Datos (2010). *Guía de Seguridad de Datos.* http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/pdfs/guia_seguridad_datos_2008.pdf

- Agencia Española de Protección de Datos (2008). *Guía del Responsable de Ficheros.* http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/pdfs/guia_responsable_ficheros.pdf

- Agencia Española de Protección de Datos. Consulta de inscripción de ficheros. http://www.agpd.es/portalwebAGPD/index-ides-idphp.php

- Agencia de Protección de Datos de la Comunidad de Madrid. www.madrid.org/apdcm/

- Agencia Vasca de Protección de Datos (2012). *Estudio cuantitativo sobre la protección de datos personales.* http://www.avpd.euskadi.net/s04-5273/es/contenidos/informacion/estudio/es_cuali/cuali.html

- Autoridad Catalana de Protección de Datos (APDCAT). http://www.apd.cat

- INTECO (2010). *Estudio sobre la privacidad y la seguridad de los datos personales en el sector sanitario español.* http://www.inteco.es/Seguridad/Observatorio/Estudios/estudio_LOPD_salud

- INTECO (2009). *Guía para empresas: cómo adaptarse a la normativa sobre protección de datos.* http://www.inteco.es/Seguridad/Observatorio/guias/GuiaManual_LOPD_pymes

- INTECO (2008). *Estudio sobre el grado de adaptación de las Pequeñas y Medianas Empresas españolas a la Ley Orgánica de Protección de Datos (LOPD) y el nuevo Reglamento de Desarrollo (RDLOPD).* http://www.inteco.es/Seguridad/Observatorio/Estudios/estudio_lopd_pymes

2.2 FASE 2: ENCUESTA A EMPRESAS

La finalidad de la investigación cuantitativa ha sido aportar información primaria que permitiera conocer la percepción de las empresas españolas en materia de protección de datos. Para ello, se ha elaborado un cuestionario que ha sido respondido por 1.109 responsables de microempresas, pequeñas y medianas empresas españolas, y cuyos resultados conforman la base del análisis estadístico llevado a cabo en el presente estudio.

2.2.1 Universo del estudio y sujeto de opinión

La población analizada está formada por las microempresas, pequeñas y medianas empresas establecidas en el territorio nacional. Para delimitar con mayor precisión el concepto de empresa participante, se ha tenido en cuenta a profesionales liberales y empresas de hasta 250 trabajadores con conexión a Internet.

Los datos de empresas con conexión a Internet se han extraído de la *Encuesta de uso de TIC y Comercio Electrónico (CE) en las empresas 2010-2011*[5] del Instituto Nacional de Estadística (INE), que proporciona las siguientes cifras a 1 de enero de 2011: 64,1% de conexión a Internet en microempresas de menos de 10 empleados, 97,0% en pequeñas empresas de 10 a 49, y el 99,4% en medianas empresas de 50 a 250 empleados. No se dispone de datos oficiales de conexión a Internet segmentados por sector de actividad y zona geográfica de la empresa. No obstante, debido a la amplitud del universo, pequeñas variaciones en su tamaño no afectan a la muestra seleccionada y a los errores muestrales alcanzados.

[5] Última encuesta publicada en la fecha de preparación del diseño metodológico de la encuesta.

Tabla 1: Universo del estudio

Número de empleados	Total empresas[6]	Total empresas con conexión a Internet[7]	%
Microempresas *(menos de 10 empleados)*	3.094.721	1.983.716	93,1%
Pequeñas empresas *(10-49 empleados)*	130.994	127.064	6,0%
Medianas empresas *(50-249 empleados)*	19.864	19.745	0,9%
Total	**3.245.579**	**2.130.525**	**100%**
Sector de actividad	**Total empresas**	**Total empresas con conexión a Internet**	**%**
Industrias extractivas, manufactura, construcción	706.643	s/d[8]	21,8%
Comercio y hostelería	1.068.649	s/d	32,9%
Transporte, logística, mensajería	216.802	s/d	6,7%
Informática, I+D+i y telecomunicaciones	60.032	s/d	1,8%
Servicios empresariales	739.664	s/d	22,8%
Otros servicios	453.789	s/d	14,0%
Total	**3.245.579**	**2.130.525**	**100%**
Zona geográfica	**Total empresas**	**Total empresas con conexión a Internet**	**%**
Andalucía, Ceuta, Melilla y Canarias	631.586	s/d	19,5%
Aragón, Castilla y León, Castilla-La Mancha, Extremadura	452.184	s/d	13,9%
Cataluña	600.698	s/d	18,5%
Comunidad Valenciana, Islas Baleares, Murcia	526.669	s/d	16,2%
Galicia, Asturias, Cantabria, País Vasco, Rioja, Navarra	534.352	s/d	16,5%
Comunidad de Madrid	500.090	s/d	15,4%
Total	**3.245.579**	**2.130.525**	**100%**

Fuente: INTECO

La unidad informante de la encuesta ha sido la persona responsable de la seguridad de la información de la empresa o, en su defecto, el responsable de informática. En caso de ausencia de las dos figuras anteriores, el sujeto de opinión ha sido el responsable de la empresa.

[6] A los efectos de cálculo de la muestra se han utilizado los datos del Directorio Central de Empresas del Instituto Nacional de Estadísticas (INE), que establece el límite del intervalo en 200 empleados. Esto no implica desviaciones significativas en el diseño muestral. Se han tomado los datos de 2011, últimos disponibles en la fecha de preparación del diseño muestral.

[7] Encuesta de uso de TIC y Comercio Electrónico (CE) en las empresas 2010-2011 del Instituto Nacional de Estadística (INE):

Datos para empresas de menos de 10 empleados disponibles en: http://www.ine.es/jaxi/tabla.do?path=/t09/e02/a2010-2011/l0/&file=01004.px&type=pcaxis&L=0

Datos para empresas de 10-49 y de 50-249 empleados disponibles en: http://www.ine.es/jaxi/tabla.do?path=/t09/e02/a2010-2011/l0/&file=01002.px&type=pcaxis&L=0

[8] s/d: Sin datos

2.2.2 Tamaño y distribución muestral

El tamaño de la muestra ha sido de 1.109 empresas de menos de 250 empleados, repartidas por todo el territorio nacional.

La muestra se ha distribuido por estratos, utilizando para ello una solución de compromiso entre afijación uniforme y proporcional, según los datos de empresas recogidos en el Directorio Central de Empresas (DIRCE) del Instituto Nacional de Estadística (INE) referidos a 2011, últimos disponibles en la fecha de preparación del diseño muestral.

Para realizar el muestreo se han tenido en cuenta tres variables de estratificación: tamaño de la empresa (número de empleados), sector de actividad y zona geográfica.

Tabla 2: Distribución de la muestra

Número de empleados	Muestra	%
Microempresas *(menos de 10 empleados)*	501	45,2%
Pequeñas empresas *(10-49 empleados)*	343	30,9%
Medianas empresas *(50-249 empleados)*	265	23,9%
Total	**1.109**	**100%**
Sector de actividad	**Muestra**	**%**
Industrias extractivas, manufactura, construcción	209	18,8%
Comercio y hostelería	172	15,5%
Transporte, logística, mensajería	147	13,3%
Informática, I+D+i y telecomunicaciones	153	13,8%
Servicios empresariales	202	18,2%
Otros servicios	226	20,4%
Total	**1.109**	**100%**
Zona geográfica	**Muestra**	**%**
Andalucía, Ceuta, Melilla y Canarias	184	16,6%
Aragón, Castilla y León, Castilla-La Mancha, Extremadura	172	15,5%
Cataluña	188	17,0%
Comunidad Valenciana, Islas Baleares, Murcia	188	17,0%
Galicia, Asturias, Cantabria, País Vasco, Rioja, Navarra	201	18,1%
Comunidad de Madrid	176	15,9%
Total	**1.109**	**100%**

Fuente: INTECO

La distribución de la muestra presenta diferencias respecto a la población real. Esto es así porque la afijación de la muestra por estratos se realizó de manera no proporcional, con el objeto de asegurar la representatividad de determinados estratos.

Por ello, ha sido necesario aplicar un factor de ponderación que permitiera guardar la proporcionalidad de cada uno de los estratos de la muestra respecto de la población real objeto de estudio. Es decir, el factor de ponderación cambia los pesos de los distintos estratos muestrales para que estos se ajusten a los poblacionales.

En este caso, la aplicación del factor de ponderación ha supuesto asignar más peso a las respuestas aportadas por las microempresas, y menos a las pequeñas y medianas empresas, ya que dentro del conjunto poblacional existe esta diferencia entre el número de organizaciones de cada tipo. Igualmente se ha incrementado el peso de las empresas pertenecientes a las actividades y de las zonas geográficas cuya representatividad efectiva en el conjunto de la población es mayor que la existente en la muestra.

Por tanto, esta ponderación se ha llevado a cabo en función de las siguientes variables: tamaño de la empresa (número de empleados), sector de actividad y zona geográfica.

Ilustración 2: Factor de ponderación

$$\left(\frac{N_i}{N_t}\right) \Big/ \left(\frac{n_i}{n_t}\right)$$

Ni= número de empresas que hay en cada estrato

Nt= número de empresas que hay en la población de referencia

ni= número de empresas que hay en cada estrato de la muestra

nt= número total de empresas que componen la muestra

Fuente: ONTSI[9]

Los datos poblacionales para la elaboración de este ponderador han sido obtenidos a partir de la información publicada por el Instituto Nacional de Estadística (INE) a través del Directorio Central de Empresas (DIRCE).

A lo largo del estudio, se describe al pie de cada gráfico la base de cálculo. Apréciese que se recogen los datos reales de la muestra, sin aplicar ningún factor de ponderación, con objeto de proporcionar una visión más realista del análisis.

2.2.3 Error muestral

Teniendo en cuenta los criterios anteriores y asumiendo un nivel de confianza del 95,0%, y en las condiciones más desfavorables del muestreo ($\sigma=2$, p=q=0,5), se garantiza en todo caso un error de muestreo para los datos globales del ±2,9%. Este nivel de error asegura la representatividad de los datos para poder extraer conclusiones a nivel

[9] El Observatorio Nacional de las Telecomunicaciones y de la Sociedad de la Información (ONTSI) es un órgano adscrito a Red.es cuyo principal objetivo es el estudio y análisis de la Sociedad de la Información en España.

nacional, así como por tamaño de la empresa (número de empleados), sector de actividad y zona geográfica.

Tabla 3: Error muestral[10]

Número de empleados	Muestra	Error muestral
Microempresas *(menos de 10 empleados)*	501	±4,4%
Pequeñas empresas *(10-49 empleados)*	343	±5,3%
Medianas empresas *(50-249 empleados)*	265	±6,0%
Total	**1.109**	**±2,9%**
Sector de actividad	**Muestra**	**Error muestral**
Industrias extractivas, manufactura, construcción	209	±6,8%
Comercio y hostelería	172	±7,5%
Transporte, logística, mensajería	147	±8,1%
Informática, I+D+i y telecomunicaciones	153	±7,9%
Servicios empresariales	202	±6,9%
Otros servicios	226	±6,5%
Total	**1.109**	**±2,9%**
Zona geográfica	**Muestra**	**Error muestral**
Andalucía, Ceuta, Melilla y Canarias	184	±7,2%
Aragón, Castilla y León, Castilla-La Mancha, Extremadura	172	±7,5%
Cataluña	188	±7,1%
Comunidad Valenciana, Islas Baleares, Murcia	188	±7,1%
Galicia, Asturias, Cantabria, País Vasco, Rioja, Navarra	201	±6,9%
Comunidad de Madrid	176	±7,4%
Total	**1.109**	**±2,9%**

Fuente: INTECO

[10] En el cálculo del error estadístico se ha considerado un universo infinito.

2.2.4 Realización del trabajo de campo y técnica de investigación

El trabajo de campo se ha realizado entre el 23 de enero y el 10 de febrero de 2012.

El cuestionario definitivo ha sido programado en aplicación CATI (*Computer Assisted Telephone Interview*), lo que ha permitido la recogida de la información por vía telefónica.

2.2.5 Tratamiento y análisis estadístico de los datos

A partir de la información recogida en la encuesta, se ha aplicado un plan de explotación estadística que ha permitido dar respuesta a los objetivos definidos.

El primer paso para el análisis consiste en la tabulación básica, que ofrece información general de la encuesta y permite medir la calidad de los datos. Tras analizar los listados de frecuencias, se ha procedido al diseño del protocolo de explotación de los datos y plan de tablas estadísticas y gráficos a obtener. Este proceso se ha llevado a cabo con el programa SPSS, a partir del protocolo de explotación.

Se han aplicado las siguientes técnicas estadísticas y de análisis:

- **Técnicas estadísticas descriptivas.** Distribución de frecuencias relativas de todas las variables categóricas del cuestionario y obtención de medias para las variables numéricas.

- **Test de inferencia estadística o tests estadísticos de significación.** Su objetivo es conocer si existen diferencias estadísticamente significativas entre las distintas categorías de una variable.

- **Análisis multivariante.** Estas técnicas realizan una explotación de los datos, tratándolos de forma que permiten una interpretación más profunda y otorgando valor añadido al estudio. Se ha realizado un análisis *cluster*, que consiste en clasificar una población amplia, compuesta por el total de población estudiada (empresas) en un pequeño número de grupos, mutuamente excluyentes y exhaustivos, basándose en las semejanzas de perfiles existentes entre los diferentes elementos componentes de dicha población respecto a un aspecto concreto, en este caso la protección de datos.

En algunas ocasiones se presentan datos de cumplimiento normativo de LOPD correspondientes a 2008. Estos datos han sido extraídos del *Estudio sobre el grado de adaptación de las Pequeñas y Medianas Empresas españolas a la Ley Orgánica de Protección de Datos (LOPD) y el nuevo Reglamento de Desarrollo (RDLOPD)*, elaborado por INTECO en 2008. En él se realizó una encuesta a 250 empresas españolas, con un error muestral de ±6,2%. La metodología del estudio incluía, además de la encuesta, la realización de entrevistas en profundidad a expertos y la comprobación online de la inscripción efectiva de ficheros ante el Registro General de Protección de Datos.

2.3 FASE 3: ENTREVISTAS EN PROFUNDIDAD A RESPONSABLES DE PROTECCIÓN DE DATOS

El propósito de esta fase ha sido identificar experiencias particulares, extraer patrones de comportamiento y necesidades de actuación para la mejora y el desarrollo de las materias objeto de la investigación en la empresa española. Para ello, se ha realizado una entrevista en profundidad a los responsables de seguridad de la información de cinco empresas participantes en la encuesta. Las entrevistas han tenido lugar entre los meses de febrero y marzo de 2012.

La identificación de cada uno de los cinco participantes en la fase de entrevistas en profundidad se ha hecho con el objetivo de cubrir la heterogénea realidad del tejido empresarial. Los criterios tenidos en cuenta para realizar la selección se han basado en las características que definen los perfiles detectados a partir del análisis *cluster*, que serán analizados en detalle en el capítulo 8: empresas despreocupadas o indiferentes, empresas desinformadas, empresas previsoras o estratégicas y empresas cumplidoras.

Los cinco perfiles finalmente seleccionados para la realización de entrevistas en profundidad las entrevistas han sido los siguientes.

Ilustración 3: Perfiles de empresas participantes en las entrevistas en profundidad

Empresa 1
- Número de empleados: 200.
- Sector de actividad: distribución informática.
- Ficheros registrados en la AEPD.
- Manifiesta estar al corriente en las obligaciones LOPD.
- Proporciona formación a los empleados sobre LOPD.
- Persona entrevistada: responsable del área de informática.
- Perfil asociado: *"Empresas previsoras o estratégicas"*.

Empresa 2
- Número de empleados: 50.
- Ficheros registrados en la AEPD.
- Manifiesta estar al corriente en las obligaciones LOPD.
- Reciben asesoramiento externo para el cumplimiento de LOPD.
- Persona entrevistada: responsable del área de informática.
- Perfil asociado: *"Empresas cumplidoras"*.

Empresa 3
- Número de empleados: 1.
- Sector de actividad: servicios veterinarios.
- Disponen de ficheros con datos de carácter personal.
- Persona entrevistada: gerente.
- Perfiles asociados: *"Empresas despreocupadas o indiferentes"* y *"Empresas desinformadas"*.

Empresa 4
- Número de empleados: 10.
- Sector de actividad: informática.
- Ficheros registrados en la AEPD.
- Manifiesta estar al corriente en las obligaciones LOPD.
- Persona entrevistada: responsable del área de informática.
- Perfil asociado: *"Empresas cumplidoras"*.

Empresa 5
- Número de empleados: 40 asalariados y 50 autónomos.
- Sector de actividad: transporte.
- Ficheros registrados en la AEPD.
- Manifiesta estar al corriente en las obligaciones LOPD.
- Persona entrevistada: responsable del área de informática.
- Perfil asociado: *"Empresas cumplidoras"*.

Fuente: INTECO

Los resultados de la fase de entrevistas en profundidad han sido considerados en la elaboración del presente informe, enriqueciendo el análisis y las conclusiones de cada apartado.

2.4 FASE 4: GRUPO DE EXPERTOS

Por último, se ha llevado a cabo un grupo de trabajo con expertos pertenecientes a diferentes ámbitos. Para la selección de la relación definitiva de expertos se han tenido en cuenta los siguientes factores:

- Experiencia y conocimiento en materia de seguridad de la información y protección de datos, así como reputación en el sector.
- Diversidad de perfiles en el grupo: empresas, asociaciones empresariales, autoridades de control en el ámbito de la protección de datos personales, organismos de certificación, proveedores de servicios legales y servicios de consultoría y apoyo relacionados con la protección de datos personales.

Con estos criterios, el grupo de expertos ha quedado conformado por los siguientes profesionales:

- Emilio Aced (*Agencia de Protección de Datos de la Comunidad de Madrid*).
- Adrián Agudo (*Indra Sistemas*).
- César Alonso (*AUDISEC Seguridad de la Información*).
- Antonio Cimorra (*Asociación Multisectorial de Empresas de la Electrónica, las Tecnologías de la Información y Comunicación, de las telecomunicaciones y de los contenidos digitales - AMETIC*).
- Luis Fuertes (*Symantec Ibérica*).
- Ricard Martínez (*Asociación Profesional Española de Privacidad – APEP, IRTIC-Universitat de València*).
- Oscar Pastor (*Ingeniería de Sistemas para la Defensa de España - ISDEFE*).
- Pablo Pérez (*Instituto Nacional de Tecnologías de la Comunicación - INTECO Observatorio de la Seguridad de la Información*).
- José Ángel Valderrama (*Asociación Española de Normalización y Certificación - AENOR*).

Se ha realizado una única sesión de debate por parte del grupo de expertos, celebrada el día 28 de marzo de 2012 a las 16:30 horas, con una duración de 2,5 horas.

El objetivo de esta sesión ha sido contrastar los resultados obtenidos en la investigación cuantitativa e identificar recomendaciones para impulsar la protección de la privacidad.

Para la consecución del objetivo, la metodología de trabajo durante la sesión ha consistido en la presentación de los resultados preliminares de la encuesta y la apertura de un turno de debate durante el que los expertos han aportado sus opiniones o consideraciones. Todo ello ha sido llevado a cabo con el control de un moderador.

Con posterioridad a la celebración de la sesión, el análisis se ha basado en el estudio de la transcripción literal de las deliberaciones, que han sido examinadas, filtradas e integradas en el presente estudio.

3 PROTECCIÓN DE DATOS

Con el nacimiento de la LOPD en 1999 se logra en España la adecuación de la legislación nacional a la normativa europea y se avanza en la protección de derechos fundamentales para los ciudadanos, tal y como indica la Ley en su artículo primero: *La presente Ley orgánica tiene por objeto garantizar y proteger en lo que concierne al tratamiento de los datos personales las libertades públicas y los derechos fundamentales de las personas físicas y especialmente su honor e intimidad personal y familiar.* Posteriormente, en 2007, el Reglamento de Desarrollo de la LOPD (RDLOPD) complementa y cohesiona la normativa en materia de protección de datos.

El derecho fundamental a la protección de datos es la capacidad que tiene el ciudadano para disponer y decidir sobre todas las informaciones que se refieran a él. Es un derecho reconocido en la Constitución Española y el Derecho Europeo, y protegido por la LOPD.

Pero el derecho fundamental a la protección de datos tiene implicaciones también desde un punto de vista activo para las empresas, para las que se traduce en una obligación. Las empresas, así como cualquier entidad de carácter público o privado que trate con datos de carácter personal, son las encargadas de garantizar el cumplimiento de la normativa sobre protección de datos. Así, la protección de datos se transforma de este modo en un elemento esencial a tener en cuenta en el ámbito de la seguridad jurídica de las empresas.

Ilustración 4: Glosario básico de términos de protección de datos

Datos de carácter personal
Cualquier información concerniente a personas físicas identificadas o identificables.

Fichero
Todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.

Tratamiento de datos
Operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.

Cualquier operación que consista en la recogida de datos personales (nombre, apellidos, fecha de nacimiento, etc.) es un tratamiento de datos.

Responsable de fichero o tratamiento
Es la entidad, persona u órgano administrativo que decide sobre la finalidad, el contenido y el uso del tratamiento de los datos personales.

Por ejemplo, una empresa será la responsable de los ficheros que contengan datos personales de empleados, proveedores o clientes.

Encargado del tratamiento
Es la persona física o jurídica que trate datos por cuenta del responsable del fichero o tratamiento. La realización de un tratamiento por cuenta de terceros deberá estar regulada en un contrato que establezca expresamente que el encargado tratará los datos conforme a las instrucciones del responsable.

Será encargado del tratamiento, por ejemplo, la empresa que preste servicios para la realización de envíos postales.

Fuente: INTECO, a partir de la LOPD

La LOPD establece las obligaciones que los responsables de los ficheros y los encargados de los tratamientos han de cumplir para garantizar la observancia del derecho a la protección de datos de carácter personal. En el tratamiento de datos, se debe respetar el principio de calidad, que presenta las siguientes manifestaciones:

- Los datos deben recogerse con fines determinados explícitos y legítimos. La empresa, por tanto, no podrá utilizarlos para fines diferentes de los que haya explicitado en el momento de registrar el fichero ante la AEPD.

- Los datos deben ser adecuados, pertinentes y no excesivos en relación con su finalidad.

- Los datos deben ser exactos y responder con veracidad a la situación del titular, lo que implica que la empresa debe mantener los datos actualizados.

- Los datos solo deben conservarse durante el tiempo necesario para las finalidades del tratamiento para las que han sido recogidos y, en consecuencia, cancelarlos en el momento en el que dejan de ser necesarios.

Las empresas, en calidad de responsables o encargadas del tratamiento de datos personales, deben cumplir una serie de obligaciones entre las que destacan el deber de información (los responsables deben informar al ciudadano cuando recojan datos personales que les afecten), consentimiento (el titular de los datos debe consentir el tratamiento de los mismos) e inscripción (los ficheros deben ser inscritos ante el Registro General de Protección de Datos de la AEPD).

La AEPD, en su Guía del Responsable de Ficheros y su Guía de Seguridad de Datos, ofrece un análisis detallado de las obligaciones previstas en la LOPD y RDLOPD. También INTECO, en la Guía para empresas: cómo adaptarse a la normativa sobre protección de datos, proporciona pautas de actuación. Remitimos al lector a estos documentos para una visión completa de las obligaciones que afectan a las empresas en relación con la normativa sobre protección de datos.

Las Autoridades de Protección de Datos en España son las siguientes: Agencia Española de Protección de Datos (AEPD), Agencia de Protección de Datos de la Comunidad de Madrid (APDCM), Autoridad Catalana de Protección de Datos y Agencia Vasca de Protección de Datos. Mientras que la AEPD tiene competencias en todo el territorio español sobre ficheros de titularidad pública y privada, el resto de Agencias, de ámbito autonómico, tiene competencia exclusivamente sobre los ficheros de titularidad pública en su área geográfica.

El 25 de enero de 2012, la Comisión Europea propuso una reforma generalizada de las normas de protección de datos de la UE de 1995 con el fin de afianzar los derechos a la

privacidad en Internet e impulsar la economía digital en Europa. Esta reforma se materializa en un borrador de reglamento general de protección de datos. La iniciativa es resultado de una amplia consulta de todas las partes interesadas sobre la revisión del actual marco jurídico y tiene por objeto lograr un equilibro entre la protección de los datos de las personas y la libre circulación de datos personales dentro de la Unión Europea.

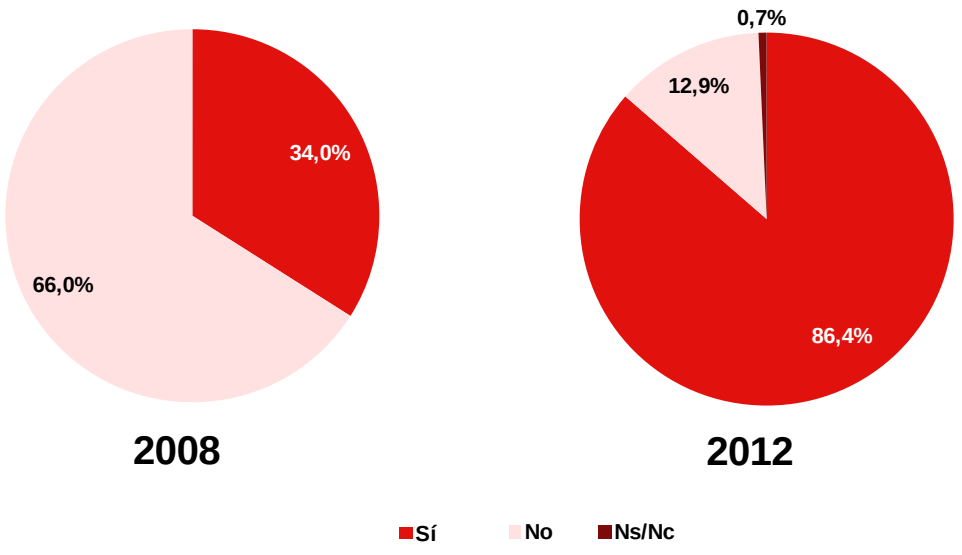
4 CONOCIMIENTO DE LA NORMATIVA SOBRE PROTECCIÓN DE DATOS

El análisis estadístico comienza con el grado de conocimiento que las empresas españolas muestran hacia la normativa sobre protección de datos. Este examen constituye un paso previo al estudio sobre su percepción de cumplimiento efectivo, y permite extraer conclusiones acerca de la familiaridad del sector empresarial hacia la protección de datos.

Si en 2008 la proporción de pequeñas y medianas empresas españolas que afirmaba conocer la LOPD era de un minoritario 34%, la encuesta de 2012 eleva hasta un 86,4% el porcentaje de empresas que manifiesta estar familiarizada con la ley.

El nivel de conocimiento es elevado entre microempresas (86,1%), pequeñas (91,5%) y medianas empresas (90,4%).

Gráfico 1: Empresas que declaran conocer la LOPD. Evolución 2008-2012 (%)



Base: empresas españolas (n=1.109 en 2012) *Fuente: INTECO*

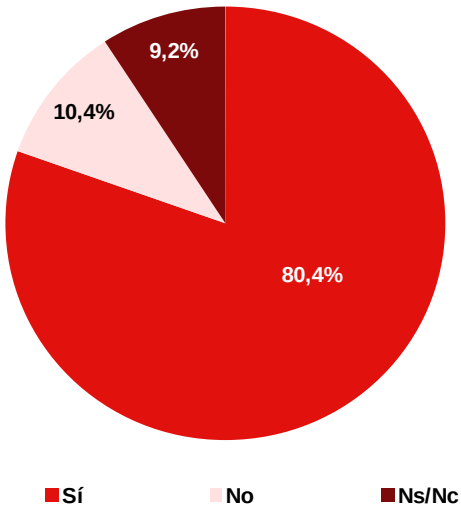
El análisis evolutivo refleja un crecimiento de más de 50 puntos porcentuales en cuatro años. ¿Qué factores pueden estar detrás del aumento? El grupo de expertos participantes en el estudio se muestra de acuerdo al enumerar las siguientes razones:

- Intensa labor divulgativa de las autoridades de protección de datos en España.
- Eco en los medios de comunicación de cuestiones como la privacidad y los derechos de los ciudadanos a la protección de sus datos personales.

- Difusión realizada por las consultorías o gestorías que prestan servicios de adecuación a la LOPD.
- Efecto tractor generado por las empresas más grandes, normalmente más sensibilizadas en el cumplimiento de la LOPD.
- Inclusión, por parte de las Administraciones Públicas, de requerimientos sobre protección de datos personales en las cláusulas de los pliegos para la contratación de servicios que incluyen el tratamiento de datos personales.
- Repercusión mediática de las inspecciones y sanciones derivadas del incumplimiento de la normativa sobre protección de datos.

Además de conocer de manera generalizada la LOPD, un 80,4% de las empresas españolas considera que esta norma les es de aplicación a título individual, tal y como muestra el gráfico siguiente.

Gráfico 2: Empresas que declaran ser conscientes de estar sujetas a la normativa sobre protección de datos (%)



Base: empresas españolas (n=1.109) *Fuente: INTECO*

En este caso, el tamaño de la empresa sí resulta determinante a la hora de apreciar diferencias. Entre las microempresas, el 79,9% afirma ser consciente de su sujeción a la LOPD, mientras que entre pequeñas empresas el porcentaje aumenta hasta el 87,9% y entre medianas empresas se generaliza, alcanzando a un 95,6%. (No está de más recordar que la normativa de protección de datos resulta de aplicación a toda entidad, de carácter público o privado, independiente de su tamaño, que disponga de ficheros con datos personales.)

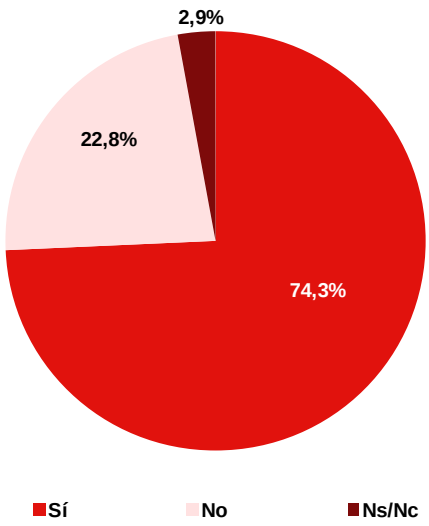
5 EXISTENCIA DE FICHEROS

A los efectos de la normativa sobre protección de datos, un fichero es un conjunto organizado de datos de carácter personal, cualquiera que sea su forma o modalidad de creación, almacenamiento, organización y acceso. Se trata, por ejemplo, de ficheros de clientes, proveedores, empleados, currículos, grabaciones de videovigilancia, etc.

El primer paso, por tanto, es identificar qué porcentaje de empresas trabaja con ficheros con datos personales, ya sean en soporte automatizado o en papel. En España, el 74,3% de las microempresas, pequeñas y medianas empresas afirma disponer de ficheros con datos personales, tal y como se aprecia en el gráfico siguiente.

Por tanto, una de cada cuatro empresas no trabaja con ficheros con información de carácter personal. ¿Es realista esta conclusión? El grupo de expertos participantes en el estudio coinciden en que la lógica empresarial actual haría razonable pensar que toda empresa trabaja, en mayor o menor medida, con datos personales. El análisis desglosado por tamaño de empresa proporciona pistas interesantes que pueden ayudar a extraer conclusiones. Así, la práctica totalidad de medianas empresas (94,3%) y buena parte de las pequeñas empresas (88,4%) declaran disponer de ficheros que contienen datos de carácter personal. Lo que ocurre es que, entre las microempresas de menos de 10 empleados, que precisamente representan más del 90% del universo del estudio, solo el 73,4% manifiestan trabajar con este tipo de activo. Es lógico pensar que las microempresas, entre las que se incluyen profesionales autónomos sin ningún empleado a su cargo, presenten menor predisposición a disponer de ficheros con datos personales o sean manejados por asesores fiscales y laborales que actuarían como encargados.

Gráfico 3: Empresas que declaran disponer de ficheros con datos de personales (%)

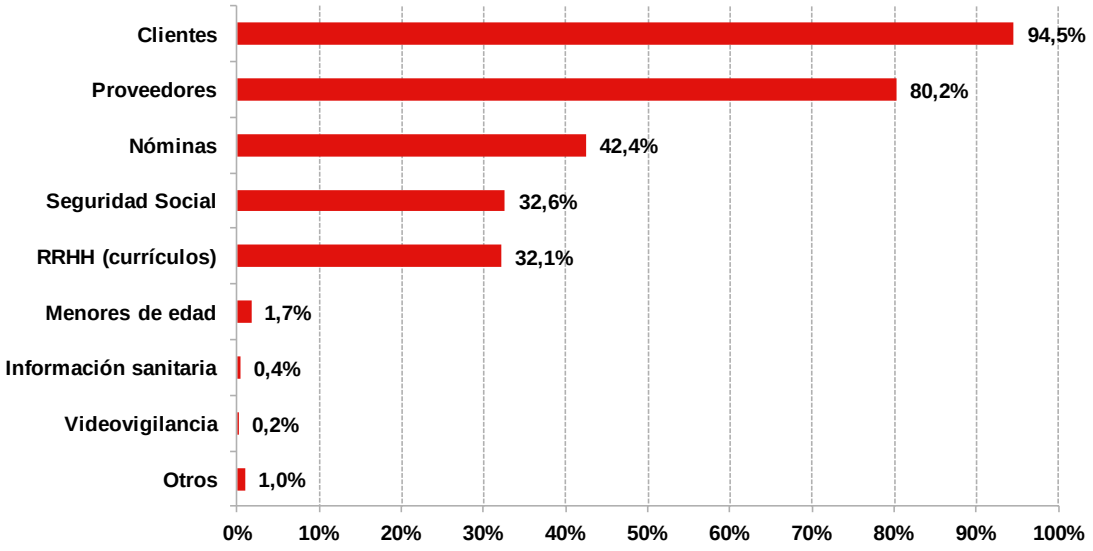


Base: empresas españolas (n=1.109) *Fuente: INTECO*

Los tipos de ficheros más habituales en el tráfico empresarial son los de clientes y proveedores, declarados por la práctica totalidad de las empresas que disponen de ficheros con datos personales (94,5% y 80,2%, respectivamente). Por detrás de ellos, con una frecuencia considerablemente inferior, se encuentran los ficheros de nóminas (42,4%), los archivos para la Seguridad Social (32,6%) y los currículos de candidatos (32,1%).

La presencia de ficheros con otro tipo de datos personales (menores de edad, información sanitaria, o videovigilancia) es ciertamente residual, tal y como refleja el gráfico.

Gráfico 4: Tipología de ficheros con datos personales (%)



Base: empresas españolas con ficheros con datos personales (n=919) *Fuente: INTECO*

El número de empleados influye en la tipología de ficheros con los que trabaja la empresa. Así, los datos de clientes y proveedores están ampliamente extendidos en las empresas, sea cual sea su tamaño. No ocurre así con los archivos de nóminas, seguridad social y currículos de candidatos. En la siguiente tabla se puede apreciar que estos tres tipos de ficheros son frecuentes en las empresas de tamaño mediano y pequeño, pero en cambio están muy poco representados en las microempresas de menos de diez empleados.

También se aprecian diferencias en los ficheros minoritarios. Así, aunque infrecuentes en general, los ficheros con datos de menores, información sanitaria o videovigilancia están presentes en mayor medida en empresas con mayor número de empleados que en microempresas con pocos o ningún asalariado.

Tabla 4: Tipología de ficheros con datos de carácter personal, segmentado por tamaño de empresa (%)

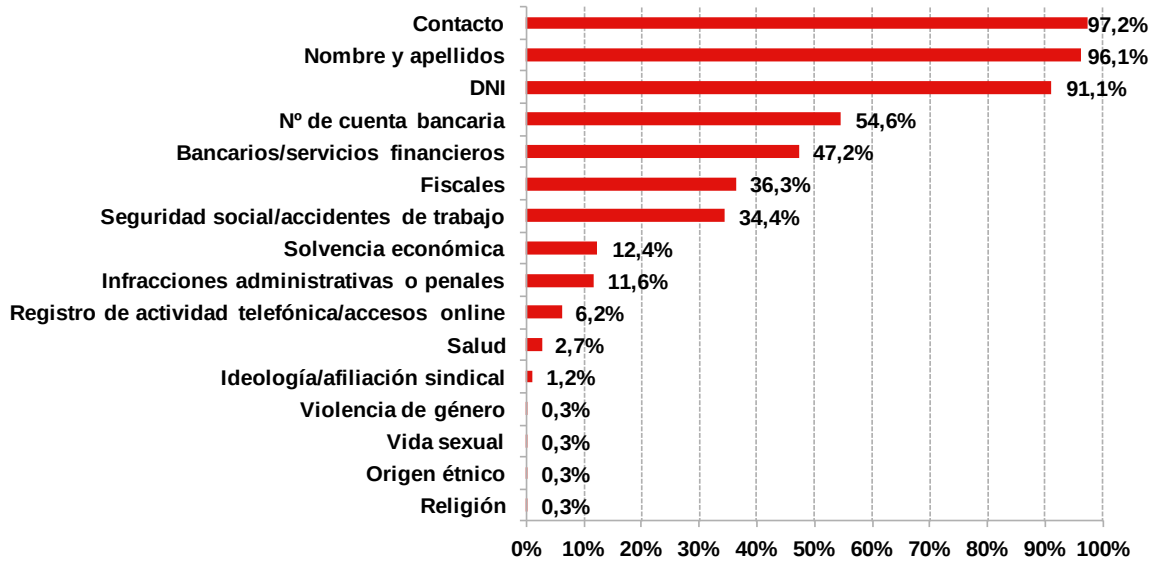
	Microempresa	Pequeña empresa	Mediana empresa
Clientes	94,8%	91,8%	89,8%
Proveedores	79,8%	84,6%	88,4%
Nóminas	39,8%	75,9%	81,7%
Seguridad Social	30,1%	64,1%	73,2%
RRHH (currículos)	29,1%	69,1%	84,3%
Menores de edad	1,7%	2,1%	3,5%
Información sanitaria	0,4%	0,2%	1,2%
Videovigilancia	0,1%	0,4%	1,8%
Otros	1,1%	0,3%	0,4%

Base: empresas españolas con ficheros con datos personales (micro n=373, pequeña n=300, mediana n=246)

Fuente: INTECO

Datos de contacto como dirección, teléfono y correo electrónico (97,2%), nombre y apellidos (96,1%) y DNI (91,1%) son los datos de carácter personal manejados en mayor medida por las empresas españolas. Por detrás de ellos, se encuentran el número de cuenta (54,6%), los datos financieros (47,2%), así como información fiscal (36,3%) y de la Seguridad Social (34,4%).

Gráfico 5: Tipología de datos de carácter personal manejados dentro de los ficheros (%)



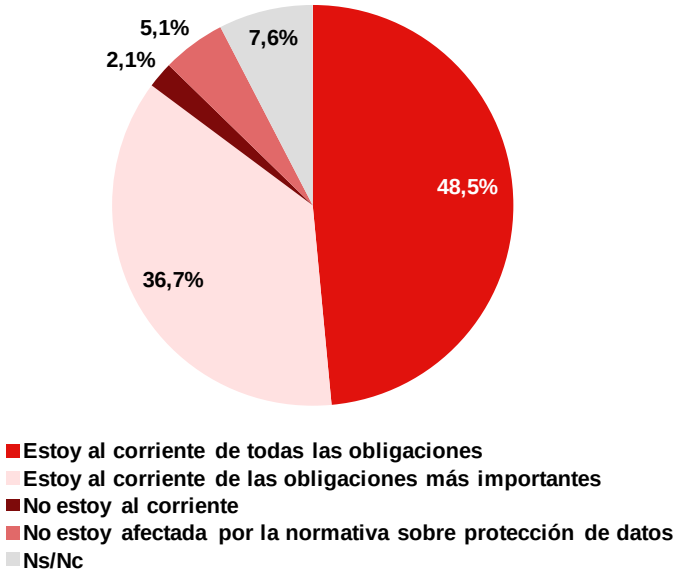
Base: empresas españolas con ficheros con datos personales (n=919) *Fuente: INTECO*

6 PERCEPCIÓN DE ADOPCIÓN DE LAS OBLIGACIONES SOBRE PROTECCIÓN DE DATOS

Confirmado el conocimiento de la normativa sobre protección de datos entre las empresas españolas, y el uso de ficheros con datos personales, es hora de avanzar en el análisis que motiva el estudio. Las pequeñas y medianas empresas españolas, ¿perciben que cumplen las obligaciones previstas en la LOPD?

Teniendo en cuenta las respuestas proporcionadas por las propias empresas, solo la mitad de ellas manifiesta cumplir con todas las obligaciones que contempla la normativa española sobre protección de datos.

Gráfico 6: Percepción de las empresas con ficheros con datos personales sobre su adecuación a la normativa sobre protección de datos (%)



Base: empresas españolas con ficheros con datos personales (n=919) *Fuente: INTECO*

En los siguientes epígrafes se lleva a cabo un análisis individualizado del nivel de adopción de la empresa española de algunas de las disposiciones que contempla la legislación española, en concreto:

- Declaración de ficheros.
- Deber de información.
- Deber de solicitud de consentimiento.
- Deber de gestión de los derechos ARCO.

- Tratamiento de datos personales por parte de terceros.
- Tratamiento de datos personales en caso de transferencias internacionales.

En el análisis del cumplimiento de la empresa española de estas obligaciones se tiene en cuenta las respuestas proporcionadas en la encuesta, lo que lleva implícito cierto sesgo derivado de la propia metodología. Parece lógico pensar que, tratándose del cumplimiento de una ley, las personas encuestadas tiendan a sobrevalorar su actuación en relación con las disposiciones normativas.

Por otro lado, también se da la circunstancia, identificada por los expertos, que muchas empresas tienen subcontratada la protección de datos con consultoras externas, lo que puede distanciar al entrevistado de la situación real y que este responda sin un total conocimiento del grado de cumplimiento de su empresa.

En este sentido, el grupo de expertos, al analizar los datos de la encuesta, está de acuerdo en que el nivel de cumplimiento real de la LOPD es, en la mayoría de los casos, inferior al manifestado por las empresas encuestadas. El lector debe tener en cuenta, en cada caso, que lo que se muestra aquí es el estudio sobre la *percepción* de las empresas españolas en materia de protección de datos, y por tanto conclusiones sobre nivel *real* de cumplimiento normativo deben ser extraídas con cautela.

6.1 INSCRIPCIÓN DE FICHEROS

El art. 26 de la LOPD establece que toda persona o entidad que proceda a la creación de ficheros de datos de carácter personal lo notificará previamente a la Agencia de Protección de Datos. El RDLOPD detalla el procedimiento y requisitos para llevar a cabo la notificación e inscripción de ficheros ante el Registro General de Protección de Datos (arts. 55 y siguientes).

Desde un punto de vista práctico, la Agencia Española de Protección de Datos pone a disposición de los responsables de ficheros el formulario electrónico NOTA[11], que permite la presentación de notificaciones a través de Internet. El trámite de la inscripción de ficheros en el Registro es gratuito.

La declaración de ficheros ante la AEPD, con carácter previo a la creación del propio fichero, constituye el punto de partida para el cumplimiento de las obligaciones que la ley impone a las entidades que traten ficheros con datos de carácter personal.

[11] Disponible en: https://www.agpd.es/portalwebAGPD/canalresponsable/inscripcion_ficheros/Notificaciones_tele/obtencion_formulario/index-ides-idphp.php .

La Agencia Española de Protección de Datos permite acceder a información básica relativa a los ficheros públicos y privados inscritos en el Registro General de Protección de Datos. El acceso al Registro es público y gratuito, y puede consultarse en la web de la Agencia.

En el momento de elaboración del presente informe[12], 1.017.725 entidades de titularidad privada han registrado un total de 2.737.848 ficheros. Teniendo en cuenta que, según los últimos datos publicados por el Instituto Nacional de Estadística[13], el 1 de enero de 2012 había en España 3.199.617 empresas, un cálculo simple nos permite concluir que, en el mejor de los casos, solo un 31,8% de las empresas españolas dispondrían de ficheros registrados ante la Agencia Española de Protección de Datos. Parece lógico que las empresas de mayor tamaño sean más propensas a inscribir sus ficheros que las de menor tamaño, aunque la AEPD no ofrece este tipo de información.

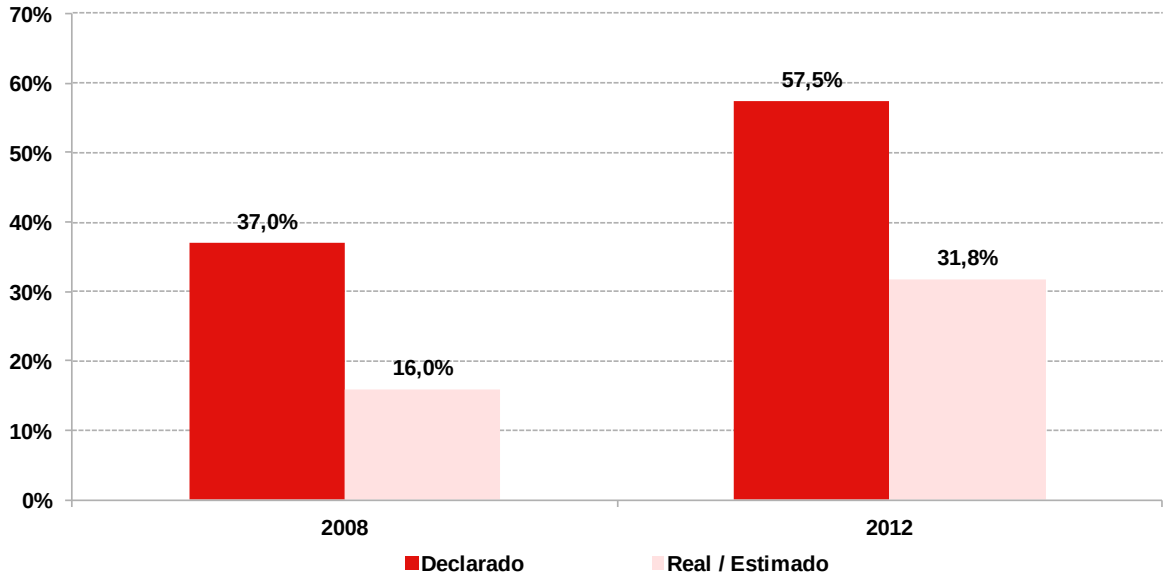
¿Qué declaran las empresas participantes en el estudio? Su percepción dista considerablemente de esta situación, tal y como confirma el siguiente gráfico. Así, el 57,5% de las empresas consultadas manifiesta haber inscrito sus ficheros en la AEPD. Se confirma, en este caso, la sospecha del Grupo de Expertos participante en el estudio, que mencionan que las empresas tienden a sobre-declarar su nivel de cumplimiento normativo.

Ya en 2008 se apuntaba un desfase entre lo declarado en encuesta y el dato real obtenido en el Registro: frente al 30,3% de las empresas que afirmaba haber inscrito sus ficheros en la AEPD, solo un 16% lo había hecho realmente. (En aquella ocasión, el dato de inscripción real permitía el contraste directo, ya que se realizó una consulta individual para cada una de las empresas participantes en el estudio.)

[12] Consulta realizada el 30 de agosto de 2012 (datos de julio de 2012): http://www.agpd.es/portalwebAGPD/ficheros_inscritos/index-ides-idphp.php

[13] Datos disponibles en: http://www.ine.es/jaxi/menu.do?type=pcaxis&path=%2Ft37%2Fp201&file=inebase&L=0

Gráfico 7: Empresas con ficheros con datos personales que declaran haber inscrito ficheros en la Agencia de Protección de Datos y contraste con el porcentaje real / estimado. Evolución 2008-2012 (%)



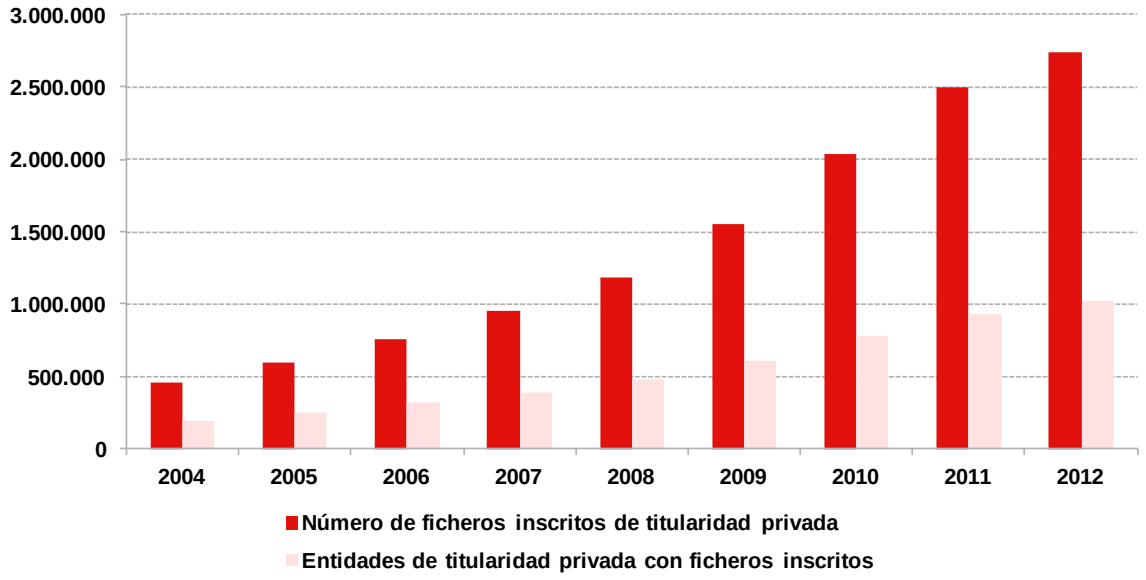
Base: empresas españolas con ficheros con datos personales (n=919 en 2012) *Fuente: INTECO*

En cualquier caso, desde el año 2000 (recordemos que la LOPD data de 1999) se ha producido un importantísimo y constante crecimiento en el número de ficheros inscritos de titularidad privada, así como en el total de entidades que registran sus ficheros ante la AEPD, tal y como se aprecia en el siguiente gráfico.

Así, en 2004, menos de 250.000 entidades habían inscrito poco más de 450.000 ficheros, mientras que en 2012, en el momento de elaboración del presente informe, como se ha indicado anteriormente, algo más de un millón de entidades de titularidad privada han registrado más de 2,7 millones de ficheros[14].

[14] Consulta realizada el 30 de agosto de 2012 (datos de julio de 2012): http://www.agpd.es/portalwebAGPD/ficheros_inscritos/index-ides-idphp.php

Gráfico 8: Evolución del número de inscripciones de ficheros en el Registro General de Protección de Datos



Fuente: Agencia Española de Protección de Datos[15]

6.2 DEBER DE INFORMACIÓN

El art. 5 de la LOPD regula el deber de información al afectado, previo al tratamiento de sus datos de carácter personal. Así, contempla que los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco de los siguientes aspectos:

De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.

Del carácter obligatorio o facultativo de su respuesta.

De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.

De la posibilidad de ejercitar los derechos ARCO.

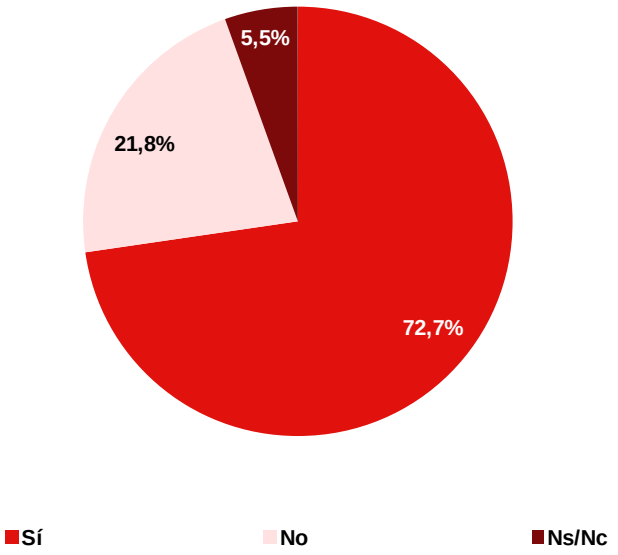
De la identidad y dirección del responsable del tratamiento o de su representante.

En cumplimiento de esta obligación, los responsables de ficheros incluirán una cláusula informativa en el propio impreso de captación de datos, en formularios de Internet, mediante carteles informativos, mediante una alocución telefónica[16], etc.

[15] Todos los datos se refieren al mes de diciembre, excepto los de 2012, que reflejan el último dato disponible en el momento de elaboración del estudio (consulta realizada el 30 de agosto de 2012, datos de julio de 2012).

Los resultados de la encuesta y la opinión de los expertos sobre la realidad de las pequeñas y medianas empresas, una vez más, es contrapuesta. Así, mientras que casi 3 de cada 4 empresas españolas dicen cumplir con el deber de información previsto en la ley, sin embargo los expertos indican que este porcentaje es menor. Y más aún si la cifra del 72,7% se pone en relación con el resultado obtenido por INTECO en 2008, cuando apenas el 29% de las empresas manifestaba estar al tanto de la obligación de informar a los usuarios sobre el tratamiento de sus datos personales. ¿A qué puede deberse esta divergencia?

Gráfico 9: Empresas con ficheros con datos personales que declaran cumplir con el deber de información a las personas físicas titulares de los datos (%)



Base: empresas españolas con ficheros con datos personales (n=919) *Fuente: INTECO*

Varios podrían ser los motivos que están detrás de esta disparidad. En primer lugar, no debemos olvidar que en la encuesta se interpela a las empresas sobre el cumplimiento de sus obligaciones legales y que, por tanto, existe un riesgo moral de cierto sesgo en la sinceridad de los responsables consultados. Por otro lado, del análisis global de las respuestas obtenidas se evidencia un cierto grado de desconocimiento de las obligaciones reales que tienen las empresas con respecto a la LOPD, que puede hacer que juzguen equivocadamente su grado de cumplimiento.

Más allá de esto, de acuerdo con la opinión de los expertos, detrás de este elevado porcentaje de cumplimiento declarado del deber de información se encuentra una

[16] En el caso de que el deber de información sea cumplido telefónicamente, el responsable del fichero debe conservar las grabaciones mientras dure el tratamiento de datos. La consideración de haber cumplido con el deber de informar según doctrina reiterada de la Audiencia Nacional corresponde al responsable del fichero la prueba del cumplimiento del deber de informar, y dicha prueba no podría obtenerse en caso de una mera información verbal.

realidad: en la práctica, resulta más sencillo incorporar en las comunicaciones con los usuarios una cláusula informativa que cumplir con otras obligaciones más exigentes en materia de protección de datos (por ejemplo, la inscripción del fichero en el registro). En muchas ocasiones dicha cláusula es tomada y copiada tal cual de un modelo existente o bien de las utilizadas por otra empresa o institución. En segundo lugar, las empresas tratan de adecuarse a aquellas obligaciones y aspectos de la ley que los usuarios o clientes de la empresa podrían advertir con mayor facilidad en caso de incumplimiento. Y este es el caso del deber de información.

Precisamente por ser una falta fácilmente evidenciable, las empresas son las primeras interesadas en el cumplimiento de esta obligación, con objeto de evitar las posibles denuncias de los titulares de los datos.

6.3 SOLICITUD DE CONSENTIMIENTO

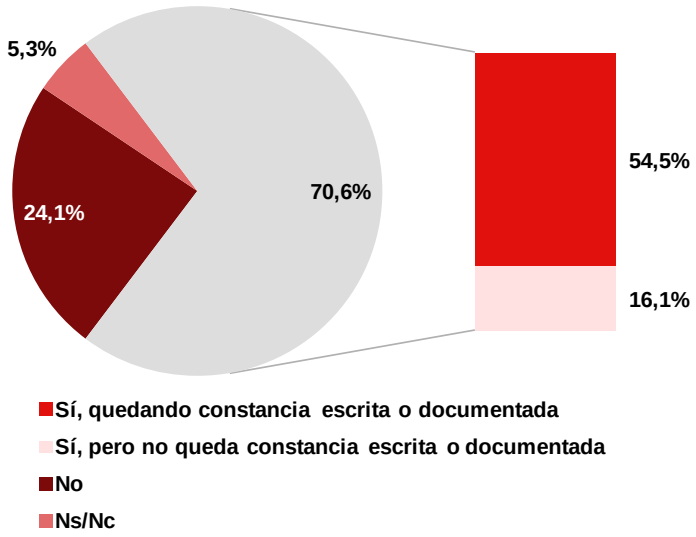
El art. 6 de la LOPD establece la normativa para recabar el consentimiento de los afectados en el tratamiento de sus datos de carácter personal: *el tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la ley disponga otra cosa*.

¿Qué se entiende por consentimiento del interesado? El art. 3 h) es claro en su definición: toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen. Por tanto, el consentimiento debe cumplir estos cuatro requisitos para ser considerado válido. Cuando el tratamiento en cuestión afecta a datos especialmente protegidos, el consentimiento deberá ser expreso y, en ciertos casos, por escrito.

El 70,6% de las empresas participantes en el estudio afirma solicitar el consentimiento, generalmente quedando constancia escrita o documentada del mismo (54,5% de los casos). Existe un 16,1% de empresas que requieren el consentimiento, pero no queda constancia escrita o documentada, al realizarse de forma verbal.

Por su parte, un 24,1% de entidades reconoce abiertamente no cumplir con el deber de solicitud de consentimiento. (En 2008, el porcentaje de empresas que afirmaba no solicitar el consentimiento de los afectados ascendía a un 70%.)

Gráfico 10: Empresas con ficheros con datos personales que declaran cumplir con el deber de solicitud de consentimiento a las personas físicas titulares de los datos (%)



Base: empresas españolas con ficheros con datos personales (n=919) *Fuente: INTECO*

Solicitud de consentimiento a menores de edad

La legislación española contempla de manera particular la casuística del consentimiento otorgado por las personas menores de edad. Así, el art. 13.1 RDLOPD distingue entre los mayores de catorce años, que pueden prestar consentimiento salvo en aquellos casos en los que la Ley exija para su prestación la asistencia de los titulares de la patria potestad o tutela, y los menores de catorce, caso que requerirá el consentimiento de los padres o tutores.

Las empresas que traten datos personales de menores de edad, por tanto, han de ser especialmente cautelosas.

Solamente el 1,7% de las pequeñas y medianas empresas españolas dispone de ficheros con datos personales de menores de edad, tal y como se veía en el Gráfico 4 al analizar la existencia de ficheros. De ellas, el 97,9% afirma que solicita el consentimiento de los padres o tutores al tratar datos de menores de 14 años, o de mayores de 14 (para un negocio que requiera la autorización de sus padres como por ejemplo comprar una motocicleta o disponer de una tarjeta de crédito). Se confirma, por tanto, una mayor prudencia de las empresas en el tratamiento de datos personales de menores de edad.

Dado lo reducido de la base de cálculo (29 empresas que trabajan con ficheros de menores), la extracción de conclusiones requiere cautela.

6.4 GESTIÓN DE DERECHOS ARCO

La LOPD reconoce los derechos de los titulares de los datos a acceder, rectificar, cancelar y oponerse al tratamiento de sus datos personales (arts. 15-17 LOPD). Los procedimientos para el ejercicio de los derechos de acceso, rectificación, cancelación y oposición (derechos ARCO) son detallados en el RDLOPD, que establece que deberá concederse al interesado un medio sencillo y gratuito para el ejercicio de los derechos ARCO (art. 24.2 RDLOPD).

Las empresas que traten derechos personales, por tanto, deberán atender las solicitudes de acceso, rectificación, cancelación y oposición de los titulares de los datos, de manera gratuita, y dentro de los plazos previstos legalmente.

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

Derecho de rectificación: derecho a dirigirse al responsable de un fichero o tratamiento para que rectifique sus datos personales, en el caso de que éstos sean inexactos o incompletos.

Derecho de cancelación: ofrece al interesado la posibilidad de dirigirse al responsable para solicitar la cancelación de sus datos personales.

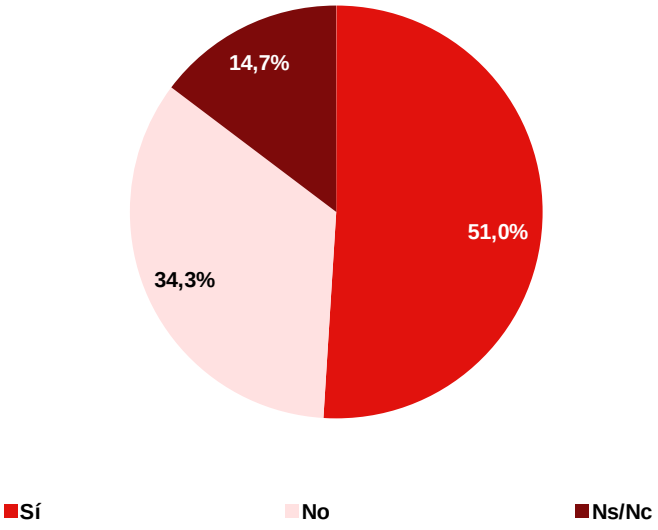
Derecho de oposición: el interesado puede oponerse, mediante su simple solicitud, a que sus datos sean tratados con fines de publicidad y de prospección comercial.

¿Cuál es la situación en la empresa española? Como muestra el siguiente gráfico, algo más de la mitad de las entidades consultadas declara adoptar procedimientos para facilitar y garantizar el ejercicio de los derechos ARCO.

Según los expertos, el grado declarado del cumplimiento normativo es mayor que el real.

Los derechos ARCO conforman la garantía esencial de la existencia efectiva del derecho fundamental a la protección de datos personales y constituyen las herramientas básicas e indispensables de que disponen las personas para controlar el uso que se hace de sus datos de carácter personal de una forma directa y proactiva. Tanto los resultados de la encuesta como la percepción de los expertos –incluso bastante menos positiva que los primeros- constatan el hecho de que aún queda mucho camino por recorrer y mucho trabajo por hacer para que las pequeñas y medianas empresas conozcan y reconozcan de forma adecuada el sentido, significado e importancia de los mismos.

Gráfico 11: Empresas con ficheros con datos personales que declaran adoptar procedimientos para facilitar y garantizar el ejercicio de los derechos ARCO (%)



Base: empresas españolas con ficheros con datos personales (n=919) *Fuente: INTECO*

6.5 TRATAMIENTO DE DATOS POR PARTE DE TERCEROS

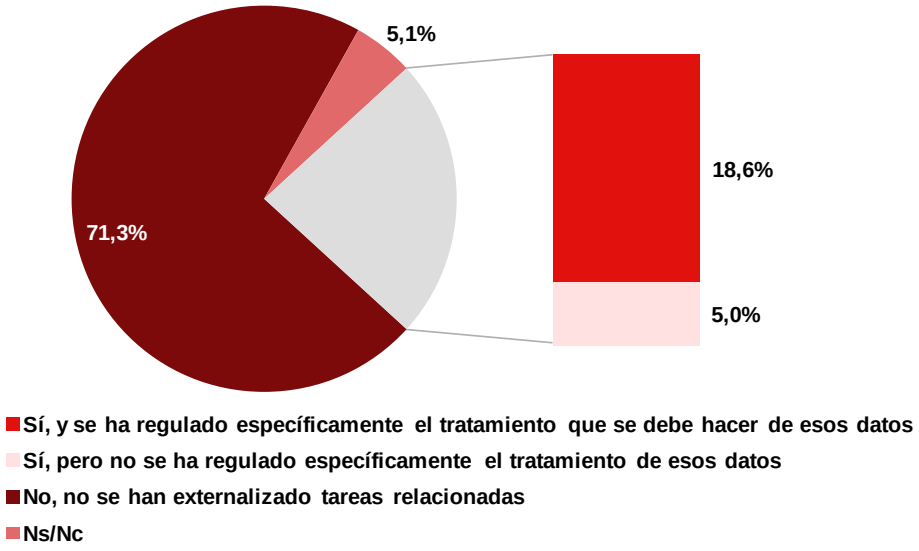
El art. 12.2 de la LOPD dispone lo siguiente: *La realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas.*

Se trataría de casos en los que el responsable del fichero externaliza algún servicio o tarea de la organización que requiere que un tercero realice algún tipo de tratamiento de datos de carácter personal (por ejemplo, una gestoría que se ocupa de las nóminas de los empleados).

Si bien la mayoría de los expertos coincide en que un número significativo de microempresas subcontrata en un tercero, bien servicios que implican algún tipo de tratamiento de datos (por ejemplo, gestión de nóminas, marketing, fiscalidad), o incluso la propia la gestión de las obligaciones en materia de protección de datos, sin embargo apenas el 23,6% de las pequeñas y medianas empresas españolas afirma haber externalizado o subcontratado servicios que exigen que un tercero realice algún tratamiento de datos de carácter personal, frente a un mayoritario 71,3% que no lo ha hecho.

Entre las empresas que sí lo han hecho (23,6%), es frecuente la regulación expresa del tratamiento prevista en el art. 12.2 LOPD. Tal y como se aprecia en el gráfico siguiente, el 18,6% de las empresas declara haberlo regulado específicamente, y solo un 5% señala haber subcontratado el servicio sin haberlo contemplado.

Gráfico 12: Empresas con ficheros con datos personales que declaran haber externalizado servicios que requieren un tratamiento de datos personales por parte de un tercero (%)



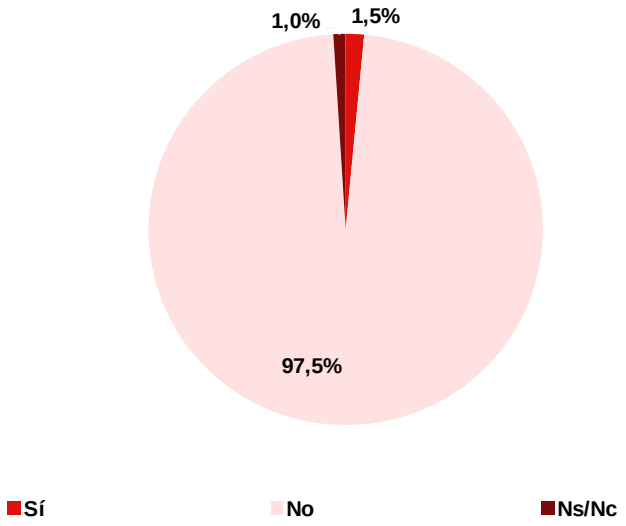
Base: empresas españolas con ficheros con datos personales (n=919) *Fuente: INTECO*

6.6 TRANSFERENCIAS DE DATOS INTERNACIONALES

El Título V de la LOPD regula el movimiento internacional de datos, estableciendo, como norma general, que *no podrán realizarse transferencias temporales ni definitivas de datos de carácter personal que hayan sido objeto de tratamiento o hayan sido recogidos para someterlos a dicho tratamiento con destino a países que no proporcionen un nivel de protección equiparable al que presta la presente Ley, salvo que, además de haberse observado lo dispuesto en ésta, se obtenga autorización previa del Director de la Agencia de Protección de Datos.*

La realización de transferencias internacionales de datos personales es ciertamente infrecuente entre las pequeñas y medianas empresas españolas. Solo un 1,5% de las empresas españolas con ficheros con datos personales declara llevar a cabo transferencias de datos internacionales (1,1% han respondido que hacen transferencia de datos a países UE/EEE y 0,4%, hacen transferencia indistintamente a países de dentro o fuera EEE).

Gráfico 13: Empresas con ficheros con datos personales que declaran realizar transferencias internacionales de datos de carácter personal (%)



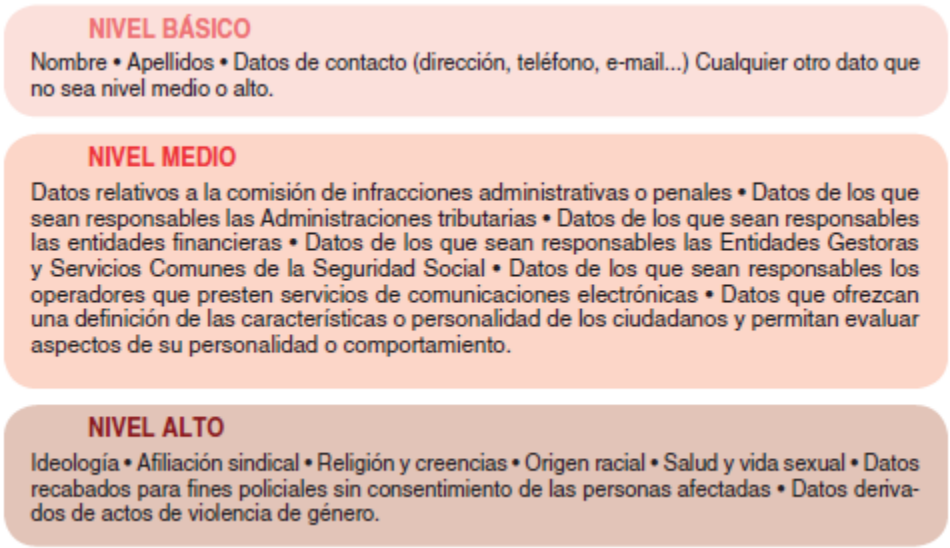
Base: empresas españolas con ficheros con datos personales (n=919) *Fuente: INTECO*

7 PERCEPCIÓN DE ADOPCIÓN DE MEDIDAS DE SEGURIDAD

El RDLOPD identifica una serie de medidas de seguridad que deben aplicarse a los ficheros y tratamientos de datos de carácter personal. Se trata de exigencias de carácter técnico, organizativo y/o jurídico que tienen por objetivo garantizar la seguridad de los datos de carácter personal y evitar su alteración, pérdida, tratamiento o acceso no autorizado.

Las medidas de seguridad a aplicar en cada caso dependerán, de un lado, del soporte del fichero (se exigen diferentes requisitos si el fichero es automatizado o no automatizado) y, de otro, del nivel de seguridad correspondiente al fichero. La siguiente ilustración resume los niveles de seguridad: básico, medio y alto previstos en el RDLOPD.

Ilustración 5: Niveles de seguridad



Fuente: INTECO, a partir del RDLOPD

A los efectos del estudio, se ha preguntado a las empresas sobre la adopción de algunas de las medidas de seguridad previstas en el RDLOPD exigibles a los ficheros con nivel de seguridad básico, en concreto las medidas de seguridad relativas a:

- Documento de seguridad.
- Divulgación de las normas sobre protección de datos entre el personal.
- Registro de incidencias.

- Control de acceso.
- Mecanismos de identificación y autenticación.
- Gestión de soportes.
- Copias de respaldo.

El análisis sobre la percepción de las empresas acerca de la adopción de estas medidas se realiza en los siguientes epígrafes. La relación completa de medidas de seguridad puede consultarse en el Título VIII del RDLOPD.

7.1 DOCUMENTO DE SEGURIDAD

El art. 88 del RDLOPD establece la necesidad de disponer de un documento de seguridad que recoja las medidas técnicas y organizativas que rijan la actuación del personal con acceso a los sistemas de información. Los apartados 3 y 4 detallan los aspectos que se deben contemplar en el documento de seguridad que, en cualquier caso, es un documento interno de la organización, que debe mantenerse actualizado en todo momento, y ser revisado siempre que se produzcan cambios relevantes.

El documento de seguridad es exigible con independencia del soporte de los ficheros (automatizados y no automatizados) y para cualquier nivel de seguridad (aunque para los ficheros de nivel medio y alto el documento debe cumplir requisitos adicionales, previstos en el art. 88.4 RDLOPD).

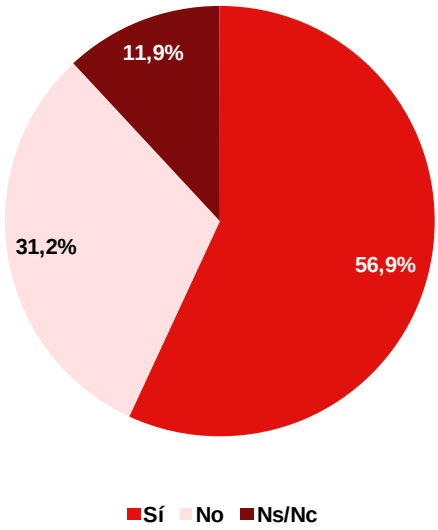
La Agencia Española de Protección de Datos en su *Guía de Seguridad de Datos*[17] proporciona una guía modelo del Documento de Seguridad, donde ofrece pautas de carácter práctico que pueden ayudar a las empresas interesadas en dar cumplimiento a las disposiciones previstas en el RDLOPD. También la Agencia de Protección de Datos de la Comunidad de Madrid proporciona un modelo genérico de Documento de Seguridad, para que el responsable del fichero lo adapte a las necesidades concretas de su organización[18].

Un 56,9% de las pequeñas y medianas empresas españolas con ficheros con datos personales manifiesta disponer de un Documento de Seguridad, tal y como puede apreciarse en el gráfico siguiente. El porcentaje de empresas que reconoce no disponer del documento es considerable, hasta un 31,2% de las encuestadas.

[17] Agencia Española de Protección de Datos (2010). *Guía de Seguridad de Datos.* Disponible en: http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/pdfs/guia_seguridad_datos_2008.pdf

[18] Agencia de Datos de la Comunidad de Madrid. *Documento de Seguridad*. Disponible en: http://www.madrid.org/cs/Satellite?c=CM_Texto_FA&cid=1109267626172&idPage=1109266885515&language=es&pagename=APDCM%2FCM_Texto_FA%2FmuestraTextoFA_APDCM

Gráfico 14: Empresas con ficheros con datos personales que declaran disponer de Documento de Seguridad (%)



Base: empresas españolas con ficheros con datos personales (n=919) *Fuente: INTECO*

7.2 DIVULGACIÓN DE LA NORMATIVA DE PROTECCIÓN DE DATOS AL PERSONAL DE LA EMPRESA

El art. 89 del RDLOPD regula las funciones y obligaciones del personal de la empresa. Así, establece en primer lugar que los usuarios con acceso a los datos de carácter personal deberán estar definidos y documentados en el documento de seguridad. Por otra parte, en el segundo apartado se dispone expresamente que *el responsable del fichero o tratamiento adoptará las medidas necesarias para que el personal conozca de una forma comprensible las normas de seguridad que afecten al desarrollo de sus funciones así como las consecuencias en caso de incumplimiento*.

Es interesante este punto, ya que exige que la normativa sobre protección de datos sea divulgada de manera clara entre el personal de la empresa. No se establece la forma concreta de difusión, por lo que la empresa podrá optar entre organizar jornadas de formación, difundir la normativa y procedimientos entre los empleados utilizando canales de comunicación interna, etc.

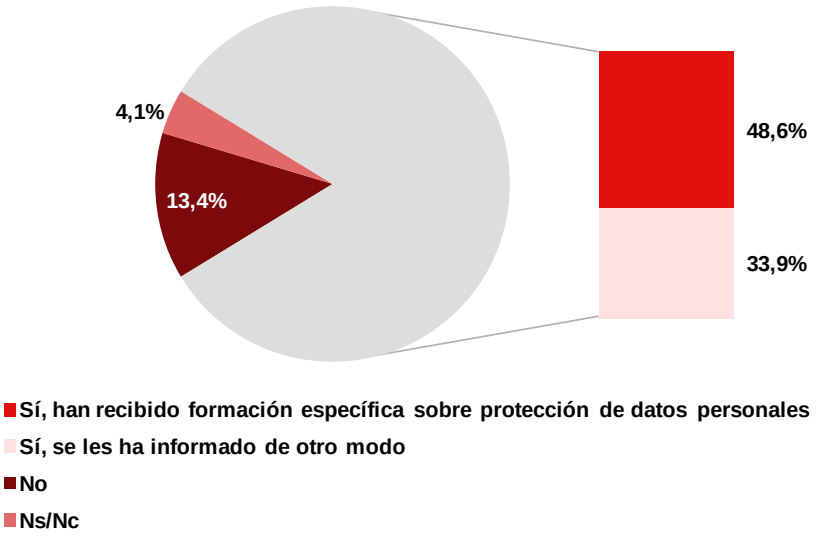
Esta medida es exigible con independencia del soporte de los ficheros (automatizados y no automatizados) y para ficheros de cualquier nivel de seguridad: básico, medio y alto.

El personal de las empresas españolas conoce las obligaciones respecto al tratamiento de datos y las consecuencias de su incumplimiento, de acuerdo con las respuestas proporcionadas en la encuesta y reflejadas en el gráfico siguiente.

Así, el 48,6% de las empresas manifiesta haber organizado sesiones de formación específica sobre protección de datos personales, y un 33,9% afirma haber difundido la normativa sobre protección de datos entre los empleados de otro modo. En total, un 82,5% de empresas estaría cumpliendo con la obligación prevista en el art. 89 del RDLOPD.

Por su parte, un minoritario 13,4% de entidades manifiesta no haber adoptado medidas para asegurar la formación de su personal en materia de protección de datos, y un 4,1% no se pronuncia al respecto.

Gráfico 15: Empresas con ficheros con datos personales que declaran haber difundido entre sus empleados las normas de protección de datos y las consecuencias de su incumplimiento (%)



Base: empresas españolas con ficheros con datos personales (n=919) *Fuente: INTECO*

7.3 REGISTRO DE INCIDENCIAS

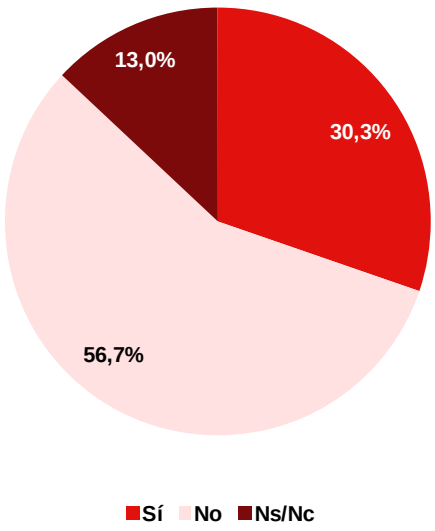
El art. 90 del RDLOPD dispone la existencia de un procedimiento de notificación y gestión de las incidencias que afecten a los datos de carácter personal, y de un registro de incidencias. Dicho registro debe reflejar: el tipo de incidencia, el momento en que se ha producido o detectado, la persona que realiza la notificación, a quién se le comunica, los efectos derivados de la incidencia y las medidas correctoras aplicadas.

La obligatoriedad de mantener un registro de incidencias permite disponer de un control completo, detallado y documentado de cualquier problema que pueda ocurrir dentro de los sistemas de información que traten con datos de carácter personal, con el fin de definir las responsabilidades y medidas correctivas a aplicar en caso de ocurrir dichas irregularidades.

El registro de incidencias es una medida de seguridad exigible a ficheros automatizados y no automatizados de nivel básico, medio y alto. (Para ficheros automatizados de nivel medio se exigen requisitos adicionales con respecto al registro de incidencias, contemplados en el art. 100 del RDLOPD.)

La disponibilidad de registro de incidencias entre las pequeñas y medianas empresas españolas es minoritaria. Solo un 30,3% de las empresas participantes en la encuesta reconoce disponer del registro.

Gráfico 16: Empresas con ficheros con datos personales que declaran tener registro de incidencias (%)



Base: empresas españolas con ficheros con datos personales (n=919) *Fuente: INTECO*

7.4 CONTROL DE ACCESO

Para asegurar la calidad en el tratamiento de los datos personales, es importante establecer un control de acceso a los mismos, de manera que puedan acceder a los datos personales aquellos empleados que lo necesiten para el ejercicio de sus funciones en la empresa, pero no los trabajadores que no lo requieran.

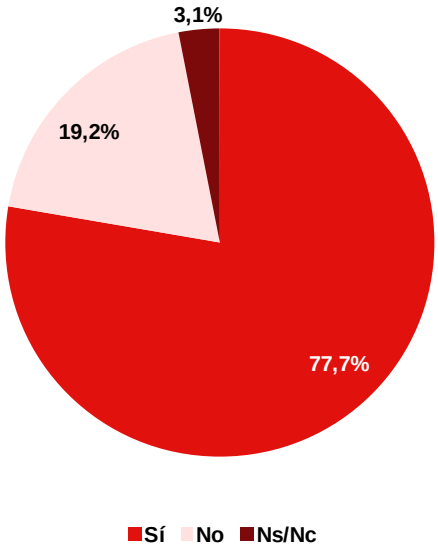
El art. 91 del RDLOPD regula el control de acceso, recogiendo una serie de obligaciones para el responsable del fichero. Así, debe existir una relación actualizada de usuarios y perfiles de usuarios, que contemple los accesos autorizados para cada uno de ellos. También es responsabilidad del responsable del fichero el establecimiento de mecanismos para evitar que un usuario pueda acceder a recursos con derechos distintos de los autorizados.

Es necesario, por tanto, que en el ámbito de la empresa se definan privilegios de acceso al sistema en función del puesto del empleado, de modo que los usuarios solo tengan acceso a los recursos que precisen el ejercicio de sus funciones.

Estas medidas de seguridad afectan a ficheros automatizados y no automatizados de todos los niveles, si bien los arts. 99, 103 y 113 establecen obligaciones adicionales para acceder a ficheros de niveles medio y alto.

De los resultados de la encuesta se desprende que existe un cumplimiento amplio de la normativa de control de acceso a datos personales entre las empresas españolas, tal y como refleja el siguiente gráfico. El 77,7% de las entidades afirma que se ha definido quiénes pueden acceder a los datos de carácter personal y las tareas que pueden realizar al respecto.

Gráfico 17: Empresas con ficheros con datos personales que declaran haber establecido control de acceso (%)



Base: empresas españolas con ficheros con datos personales (n=919) *Fuente: INTECO*

7.5 MECANISMOS DE IDENTIFICACIÓN Y AUTENTICACIÓN

El art. 93 del RDLOPD establece que el responsable del fichero o tratamiento deberá adoptar las medidas que garanticen la correcta identificación y autenticación de los usuarios.

La identificación es el procedimiento que permite *reconocer* la identidad de un usuario (quién es), mientras que la autenticación permite *comprobar* dicha identidad (si es quien dice ser). Por lo tanto el sistema deberá permitir leer los datos del usuario, compararlos con los almacenados en su base de datos y decidir si está o no autorizado para acceder.

Las contraseñas constituyen un mecanismo de autenticación muy utilizado en el entorno empresarial, ya que permiten comprobar la identidad del usuario a partir de algo que solo él conoce.

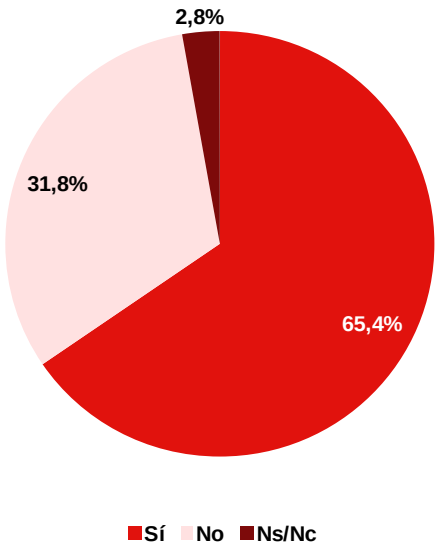
Con respecto a las contraseñas, el reglamento contempla que se debe establecer un procedimiento de asignación, distribución y almacenamiento de contraseñas, de manera que se garantice su confidencialidad e integridad. Asimismo, prevé la periodicidad de cambio de las contraseñas, que en ningún caso será superior a un año.

Estas medidas de seguridad afectan exclusivamente a ficheros automatizados de todos los niveles, si bien el art. 98 establece obligaciones adicionales los ficheros de nivel medio.

El 65,4% de las empresas españolas manifiesta disponer de un sistema de identificación de los usuarios con acceso a los datos de carácter personal, tal y como se observa en el siguiente gráfico. Por su parte, un 31,8% de las entidades con ficheros con datos personales no ha cumplido con esta obligación.

Es importante, de cara a garantizar la identificación de los usuarios, la utilización de identificadores de usuarios únicos y personales; no compartidos ni de carácter genérico.

Gráfico 18: Empresas con ficheros con datos personales que declaran haber establecido un sistema de identificación de los usuarios con acceso a los datos de carácter personal (%)



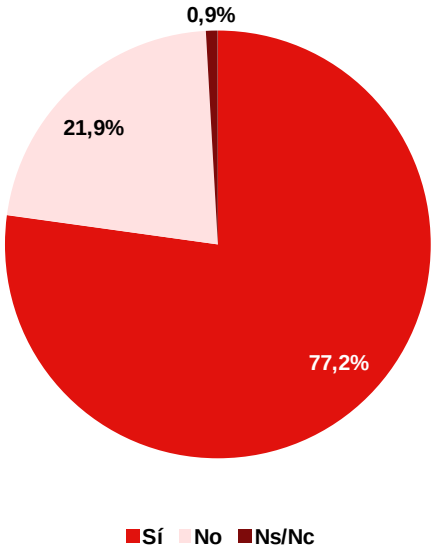
Base: empresas españolas con ficheros con datos personales (n=919) *Fuente: INTECO*

Más frecuente es el establecimiento de un mecanismo de autenticación basado en la utilización de contraseñas. El 77,2% de las empresas españolas afirma haber establecido un sistema de contraseñas para el acceso a los equipos y aplicaciones.

La importancia de establecer contraseñas robustas es clave, en tanto en cuanto constituyen el primer nivel para proteger el acceso a diferentes recursos personales. El artículo *Gestión de contraseñas*[19], elaborado por INTECO, proporciona pautas para crear y gestionar correctamente las contraseñas y analiza el funcionamiento de los programas de gestión de contraseñas.

[19] INTECO (2010). *Gestión de contraseñas.* Disponible en: http://www.inteco.es/Seguridad/Observatorio/Articulos/Gestion_contrasenas

Gráfico 19: Empresas con ficheros con datos personales que declaran haber establecido un sistema de contraseñas de los usuarios para el acceso a los equipos y aplicaciones (%)



Base: empresas españolas con ficheros con datos personales (n=919) *Fuente: INTECO*

7.6 GESTIÓN DE SOPORTES Y DOCUMENTOS

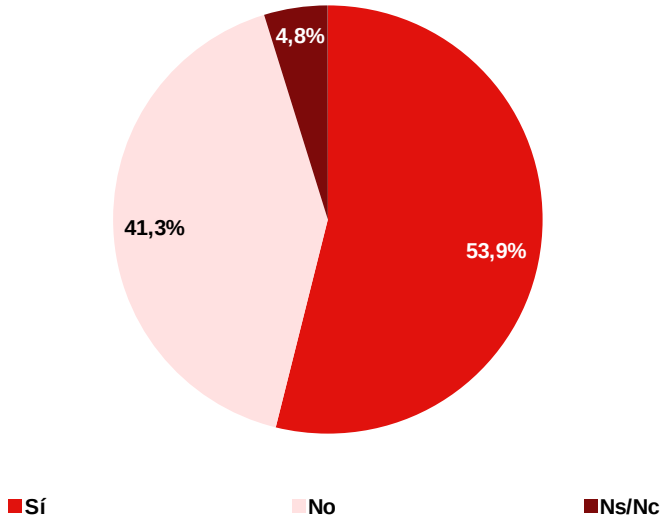
El art. 92 del RDLOPD recoge una serie de obligaciones que el responsable del fichero deberá tener en cuenta con respecto a la gestión de soportes.

En primer lugar, se exige que los soportes o documentos que contengan datos de carácter personal estén identificados e inventariados. Se recogen, asimismo, pautas de actuación a tener en cuenta en caso de salida, traslado y destrucción de soportes. Estas medidas van encaminadas a garantizar la seguridad de los datos y evitar la sustracción, pérdida, acceso indebido o recuperación posterior.

La normativa de gestión de soportes y documentos se refiere a ficheros automatizados y no automatizados de todos los niveles, si bien los arts. 97, 101, 108 y 114 establecen obligaciones adicionales para los ficheros de niveles medio y alto.

La primera obligación se refiere, pues, a la constitución de un inventario de todos los soportes, electrónicos y en papel, que contienen datos de carácter personal. Algo más de la mitad de las empresas españolas (el 53,9%) declara disponer de dicho inventario, frente a un importante 41,3% que responde en sentido contrario.

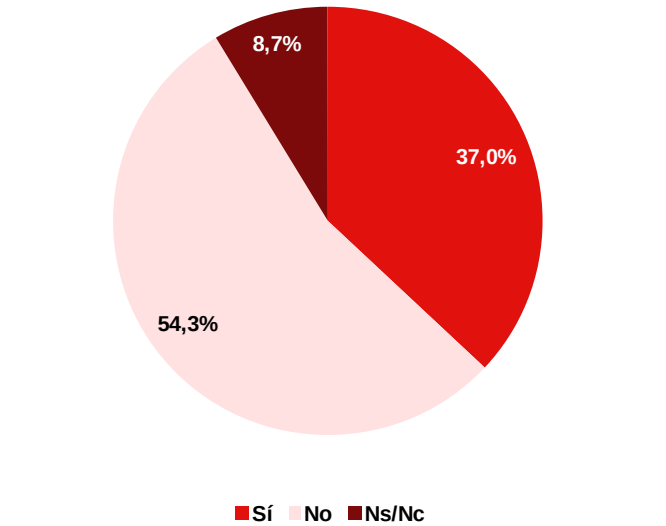
Gráfico 20: Empresas con ficheros con datos personales que declaran disponer de un inventario de los soportes que contienen datos de carácter personal (%)



Base: empresas españolas con ficheros con datos personales (n=919) *Fuente: INTECO*

Más infrecuente es el establecimiento de protocolos de actuación para la destrucción de ficheros, declarado solo por el 37% de las empresas españolas.

Gráfico 21: Empresas con ficheros con datos personales que declaran haber establecido un protocolo de actuación para la destrucción de ficheros (%)



Base: empresas españolas con ficheros con datos personales (n=919) *Fuente: INTECO*

7.7 COPIAS DE RESPALDO

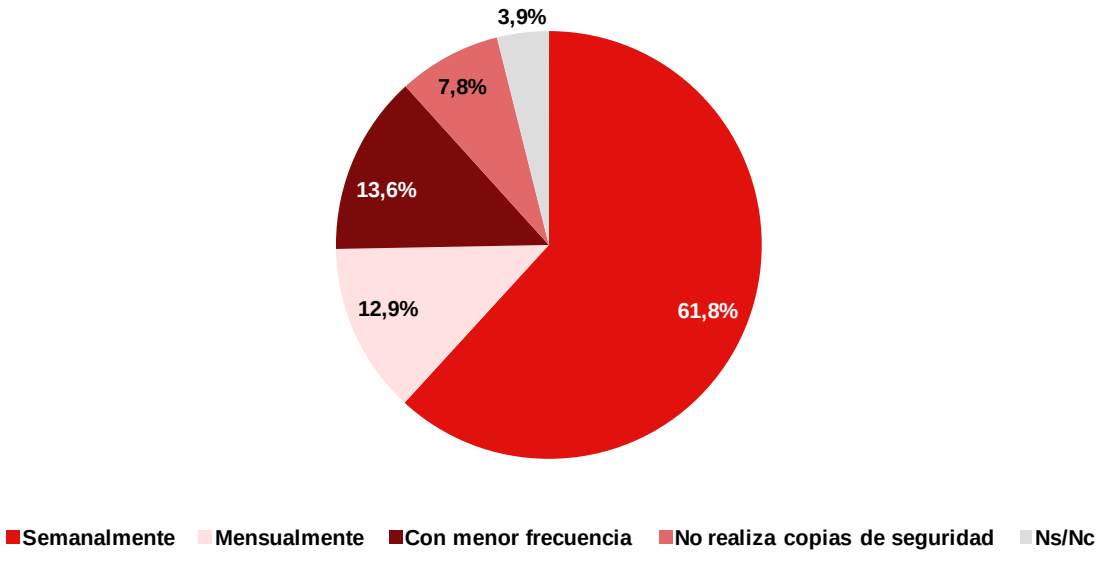
Las copias de respaldo o *backup* son las copias de datos de un fichero automatizado en un soporte que facilite su recuperación en caso de pérdida o destrucción.

El RDLOPD regula las copias de respaldo y recuperación en su artículo 94, estableciendo la obligatoriedad de realizar copias con una periodicidad, al menos, semanal, así como la necesidad de establecer procedimientos para la recuperación de los datos al estado en que se encontraban al tiempo de producirse la pérdida o destrucción.

Las medidas de seguridad sobre copias de respaldo afectan exclusivamente a ficheros automatizados, independientemente de su nivel, si bien el art. 102 establece obligaciones adicionales para realizar copias de respaldo de ficheros de nivel alto.

Un 61,8% de las empresas españolas cumpliría con lo previsto en el RDLOPD, al realizar copias de respaldo semanalmente. Por su parte, el 12,9% de las entidades declara hacer *backups* con una periodicidad mensual y un 13,6% reconoce hacerlo con una frecuencia menor.

Gráfico 22: Frecuencia con la que las empresas con ficheros con datos personales declaran realizar copias de respaldo (%)



Base: empresas españolas con ficheros con datos personales (n=919) *Fuente: INTECO*

La importancia de realizar copias de respaldo frecuentes va más allá del mero cumplimiento normativo del RDLOPD. La empresa debe ser consciente de que la información es una pieza clave para garantizar la continuidad del negocio ante un incidente de seguridad.

8 PERFILES DE EMPRESAS SEGÚN SU NIVEL DE CUMPLIMIENTO DE LA NORMATIVA SOBRE PROTECCIÓN DE DATOS

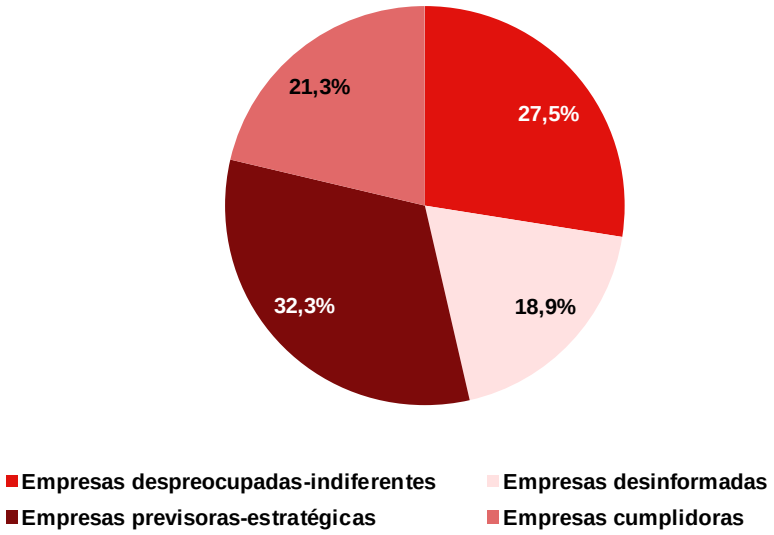
La utilización de *clusters*, una técnica estadística multivariante, permite clasificar una población amplia (las empresas participantes en el estudio) en grupos (*clusters* o perfiles), de forma que el grado de similitud entre los miembros de un mismo *cluster* es mayor que el grado de asociación entre miembros de grupos diferentes. Así, cada perfil se describe en función de las características de los miembros que lo componen.

En este estudio se ha realizado un análisis *cluster*, obteniendo 4 grupos diferenciados de empresas en función de su conocimiento y cumplimiento de la Ley Orgánica de Protección de Datos.

A los cuatro perfiles resultantes del análisis se les ha denominado, respectivamente, despreocupadas-indiferentes, desinformadas, previsoras-estratégicas y cumplidoras. Se ha utilizado estos apelativos porque son descriptivos de sus rasgos más característicos en cuanto a cumplimiento de la normativa sobre protección de datos.

La distribución en los cuatro grupos es relativamente homogénea, tal y como se aprecia en el gráfico siguiente.

Gráfico 23: *Clusters* de empresas



Fuente INTECO

8.1 PERFIL 1: EMPRESAS DESPREOCUPADAS-INDIFERENTES

Las empresas despreocupadas-indiferentes apenas conocen la LOPD y no consideran estar sujetas a ella. Entre las que sí realizan tratamientos de datos personales, un porcentaje importante indica que no está al corriente de las obligaciones de la LOPD.

Dentro de este grupo hay un elevado porcentaje de empresas cuya actividad es el comercio minorista y la hostelería. Se trata de microempresas que presentan niveles de facturación relativamente bajos.

Algunos de sus rasgos distintivos son:

- Cuatro de cada diez empresas pertenecientes a este perfil señalan no realizar tratamiento de datos de carácter personal.
- La mayoría, no obstante, dispone de ficheros, que son casi exclusivamente de proveedores y clientes. Solo dos de cada diez han indicado trabajar con ficheros relacionados con los recursos humanos.
- La mayoría de las empresas integrantes de este grupo no ha inscrito los ficheros en el Registro General de Protección de Datos de la Agencia Española de Protección de Datos. Solo el 10,2% dice haber cumplido con el deber de notificación de los ficheros ante la AEPD.
- Las empresas despreocupadas-indiferentes no suelen informar al interesado sobre la existencia de un fichero con datos personales ni la finalidad de la recogida. Un limitado 15,5% de ellas afirma cumplir con el deber de información.
- Solo una de cada cuatro empresas despreocupadas-indiferentes considera estar totalmente al corriente del cumplimiento de las obligaciones de la LOPD y su reglamento, mientras que poco más de un tercio señala que solo respecto a las más importantes.
- Un porcentaje importante de ellas no facilita formación a sus trabajadores sobre protección de datos.
- Solo el 13,9% ha establecido procedimientos para facilitar y garantizar el ejercicio de los derechos ARCO a los titulares de los datos personales.

8.2 PERFIL 2: EMPRESAS DESINFORMADAS

Estas empresas realizan tratamientos de datos de carácter personal, pero, en general, desconocen las obligaciones exigidas en la LOPD.

El *cluster* está integrado principalmente por empresas de la industria, siendo la mayoría de reducido tamaño.

En general, en este grupo se obtiene un mayor porcentaje de "no sabe / no contesta" a las distintas preguntas del cuestionario.

- Tres de cada cuatro empresas desinformadas indican que realizan tratamiento de datos de carácter personal.
- La mayoría de los ficheros tratados son de clientes y de proveedores, aunque existe una mayor presencia de ficheros de nóminas que en el grupo de las empresas despreocupadas-indiferentes.
- Poco más de un tercio de las empresas de este grupo considera estar totalmente al corriente del cumplimiento de las obligaciones de la LOPD y su reglamento.
- Cerca de la mitad declara haber inscrito los ficheros en el Registro General de Protección de Datos. No obstante, destaca el elevado porcentaje que no conoce si se ha cumplido con este trámite.
- La mayoría de las empresas, siete de cada diez, ha facilitado a sus empleados formación específica de protección de datos personales.

8.3 PERFIL 3: EMPRESAS PREVISORAS-ESTRATÉGICAS

Las empresas incluidas en el perfil 3 se denominan previsoras-estratégicas, ya que conocen la LOPD, están al tanto de sus obligaciones y observan su cumplimiento. A la vez se preocupan de mantener informados a sus empelados. Igualmente se trata de empresas previsoras, ya que existe un porcentaje relevante que cuenta con un protocolo de acción definido para la gestión de incidencias relacionadas con la protección de datos personales.

Este grupo está integrado principalmente por empresas de servicios, comercio y hostelería. Se trata del segmento que aglutina a las medianas empresas de mayor tamaño, ya que existe mayor presencia de empresas con más de 50 empleados que en el conjunto de la muestra.

- La práctica totalidad de empresas del perfil previsor-estratégico realiza tratamientos de datos de carácter personal.

- En este grupo todos los tipos de ficheros tienen mayor presencia que en el resto, especialmente los de Seguridad Social (47,0%), nóminas (55,4%) y RR.HH. (46,9%).

- Las empresas previsoras-estratégicas cumplen con la medida de seguridad que exige disponer de un inventario con todos los soportes, electrónicos y en papel, que contienen datos de carácter personal.

- La práctica totalidad de las empresas de este perfil ha inscrito los ficheros con datos personales ante el Registro General de Protección de Datos de la Agencia Española de Protección de Datos.

- En general, se observa la obligación de informar a los interesados de la existencia de un fichero, así como de la finalidad de la recogida de los datos. El 85,3% así lo manifiesta.

- La mayoría de las empresas previsoras-estratégicas (un 87%) dispone del documento de seguridad exigido por el art. 88 del RDLOPD.

- Nueve de cada diez empresas forman a sus empleados sobre las obligaciones respecto a la protección de datos personales y las consecuencias ante su incumplimiento.

- Tres cuartas partes de las empresas de este perfil han establecido procedimientos para garantizar el ejercicio de los derechos de oposición al tratamiento, acceso, rectificación y cancelación.

8.4 PERFIL 4: EMPRESAS CUMPLIDORAS

Las empresas incluidas en este perfil pertenecen al sector de los servicios empresariales. Se denominan cumplidoras porque presentan, en general, un grado de cumplimiento de la LOPD mayor que el resto de perfiles.

- La práctica totalidad realiza tratamiento de datos de carácter personal. Los ficheros de clientes están presentes en el 98,2% de las empresas, siendo los de proveedores (73,9%) los siguientes en importancia.

- Más de la mitad de las empresas considera estar totalmente al corriente del cumplimiento de las obligaciones de la LOPD y su reglamento.

- La mayoría de las empresas informa a los interesados de la existencia de un fichero, así como de la finalidad de la recogida de los datos.

- La mayoría ha establecido procedimientos para facilitar y garantizar el ejercicio de los derechos de oposición al tratamiento, acceso, rectificación y cancelación.

- Han divulgado entre sus empleados las obligaciones respecto a la protección de datos personales y las consecuencias de su incumplimiento.

9 CONCLUSIONES

El cumplimiento de la normativa sobre protección de datos en España no está extendido de manera generalizada entre las empresas, especialmente entre las pequeñas y medianas. La LOPD entró en vigor en 1999 y todavía hoy, más de diez años después, hay un importante número de empresas que ni siquiera han cumplido con la obligación de inscribir los ficheros con datos personales ante la Agencia de Protección de Datos.

No obstante, sí existe un conocimiento de la existencia de normativa sobre protección de datos. A este conocimiento han contribuido, sin duda, las acciones emprendidas por las autoridades españolas en materia de protección de datos, que han apoyado de manera decisiva la sensibilización empresarial.

Qué duda cabe que la ciudadanía está cada vez más concienciada en materia de protección de datos. El ciudadano de a pie reconoce su derecho fundamental a la protección de sus datos personales. Quizás las prácticas indiscriminadas y campañas masivas publicitarias y de telemarketing han sensibilizado al ciudadano, consciente de estar amparado por los derechos de acceso, rectificación, cancelación y oposición.

Es decir, ciudadanos y empresas saben de la existencia de la ley. Los primeros, conocen sus derechos, y las segundas se saben sujetas a una serie de obligaciones. En cambio, la situación de cumplimiento normativo entre el sector empresarial dista de ser generalizada. Los expertos participantes en el estudio insisten en que las empresas, sobre todo las de menor tamaño, ven con cierta distancia las implicaciones que la normativa de protección de datos tiene sobre sus negocios. En muchas ocasiones, las empresas han recurrido al soporte de un consultor externo para implantar la LOPD, y han delegado en ellos la responsabilidad de adecuarse a la normativa, por lo que no saben el alcance real de la implantación. También hay que reconocer que, en el sector de la consultoría, se han llevado a cabo algunas malas prácticas que han contribuido a ello (consultores poco cualificados que realizan adaptaciones meramente formales, con poca utilidad para la empresa u ofertas de servicios gratuitos vinculados a fondos de formación respecto de los cuales ha advertido la propia Fundación Tripartita)[20].

Los perfiles de empresas obtenidos mediante el análisis *cluster* dibujan la realidad española empresarial en cuanto a su aproximación a la normativa de protección de datos.

- Una cuarta parte de las pequeñas y medianas empresas españolas, las despreocupadas, desconocen la normativa sobre protección de datos y, en consecuencia, no se consideran sujetas a ella. Se trata de pequeños comercios y negocios de hostelería con una facturación reducida.

[20] http://www.fundaciontripartita.org/index.asp?MP=4&MS=105&TR=A&IDR=11&id=458

- En esta misma línea se encuentran las empresas desinformadas que, si bien reconocen disponer de ficheros con datos personales, no están al corriente de las obligaciones previstas en la legislación.

- Una de cada tres pequeñas y medianas empresas españolas se encuentra en el perfil de las previsoras, conocen la LOPD, están al tanto de sus obligaciones y observan su cumplimiento.

- Y por último, las empresas cumplidoras, pertenecientes sobre todo al sector de servicios empresariales. Esta tipología de empresa presenta, en general, un grado de cumplimiento de la LOPD mayor que el resto de perfiles.

En definitiva, a pesar de las plausibles iniciativas lanzadas por los sectores público y privado para generalizar la adopción de la normativa sobre protección de datos entre las empresas, los resultados no son todavía óptimos. Entre estas iniciativas destacan las emprendidas por las autoridades de protección de datos, tanto la Agencia Española de Protección de Datos como las autoridades autonómicas.

El siguiente epígrafe aborda una serie de recomendaciones encaminadas a mejorar el cumplimiento de la normativa española sobre protección de datos personales.

10 RECOMENDACIONES

A partir de las conclusiones obtenidas y de las aportaciones realizadas por los expertos que han colaborado en el estudio, a continuación se formulan algunas recomendaciones que buscan aumentar tanto el conocimiento como el cumplimiento normativo por parte de las pequeñas y medianas empresas en España.

10.1 PROPUESTAS EN MATERIA DE CONCIENCIACIÓN Y FORMACIÓN

10.1.1 Incrementar la intensidad de las acciones de sensibilización y adaptarlas a las necesidades del colectivo de pequeñas y medianas empresas

Para aumentar el nivel de conocimiento y el cumplimiento de la normativa sobre protección de datos, es necesario potenciar la formación y sensibilización dirigidas a las pequeñas y medianas empresas. Este esfuerzo no tiene por qué ser exclusivo de las administraciones, sino que también tienen que participar el resto de actores implicados: asociaciones sectoriales, cámaras de comercio, empresas prescriptoras y facilitadoras.

En este sentido, sería deseable la adaptación de las acciones a las particularidades de las pequeñas y medianas empresas. No se debe olvidar que este colectivo cuenta con unas circunstancias propias que las caracterizan y diferencian de las grandes empresas. Acciones formativas que tengan en cuenta y asuman estas particularidades (básicamente, limitación de recursos humanos, económicos y técnicos) pueden resultar más efectivas que acciones de tipo más genérico. Incluso, se pueden plantear acciones segmentadas por sectores concretos dentro del colectivo empresarial.

Como hemos visto a lo largo del estudio, de las discrepancias entre las respuestas de las empresas, los datos del registro de las autoridad reguladoras y la opinión de los expertos y profesionales de instituciones y empresas prescriptoras, implantadoras y auditoras, puede concluirse que entre las pequeñas y medianas empresas existe una falta de conocimiento de las obligaciones derivadas de la normativa de protección de datos.

En todo caso, el nivel de desconocimiento de las empresas no es homogéneo, existiendo empresas que nunca han oído hablar de la ley y otras que desconocen aspectos concretos de la misma. Por ello es clave articular programas de concienciación adaptado al grado de conocimiento de las empresas participantes.

Finalmente, la dispersión geográfica y el elevado número de usuarios potenciales aconsejan la utilización de la teleformación y de la formación de formadores. Estos cursos deberían considerar diferentes niveles de madurez y competencias, a saber: básico, intermedio y avanzado, respectivamente, de acuerdo con las responsabilidades asumidas por los directivos y personal laboral, es decir: responsable del fichero, responsable de seguridad, técnico informático y usuario.

A la hora de organizar este tipo de formación se ha de primar la orientación práctica y la posibilidad de realizar acciones continuadas que permitan a aquellos usuarios que ya son conocedores de la normativa la actualización de sus conceptos y nociones.

10.1.2 Abordar la concienciación desde un enfoque didáctico, no impositivo

En opinión de los expertos consultados, entre las pequeñas y medianas empresas existe una falta de cultura sobre la necesidad de proteger los datos personales. Además, varios de ellos coinciden en que, en muchos casos, las empresas que cumplen con la normativa lo hacen fundamentalmente por cubrirse ante el riesgo de una posible sanción de la AEPD, y no porque estén concienciadas sobre sus beneficios.

Sin embargo, debemos ser conscientes de cómo el cumplimiento de la legislación de protección de datos aporta valores que inciden positivamente en la empresa tanto desde el punto de vista organizativo como reputacional. El proceso de implantación de la LOPD, cuando es adecuado[21], sigue el ciclo de vida de los tratamientos de información personal y nos permite afinar nuestro modelo de gestión, comprometiendo a empleados y colaboradores y permitiendo un incremento de la eficiencia empresarial.

Por otra parte, desde el punto de vista de su reputación, las empresas deben ser conscientes de que el cliente aprecia cada vez el valor de su privacidad. Por ello, espera facilitar sus datos y recibir una información adecuada y poder confiar que se garantizará la seguridad de su información y se utilizará solo para la finalidad para la que se obtuvo. Cuando además se trate de un modelo de negocio que se desarrolle en el ámbito de internet el daño en su imagen y su buen nombre tendrá un mayor impacto que cualquier sanción.

Así pues, para formar a las empresas y generalizar el cumplimiento de la normativa es deseable que estas sean conscientes de las implicaciones que este derecho fundamental tiene para todos los ciudadanos, y de los beneficios que puede tener para su propio negocio.

Por ello, deberían desarrollarse acciones de formación y concienciación que destacaran aspectos tales como la necesidad de la protección de datos, su aportación a la ciudadanía y al propio negocio de las empresas.

10.1.3 Elaboración de las disposiciones normativas a un lenguaje adaptado a las empresas

Relacionado con las iniciativas en materia de formación, en opinión de las propias empresas resultaría muy útil la clarificación de la terminología empleada en las

[21] La Asociación Profesional Española de Privacidad ha documentado los pasos que debería seguir este proceso para ser adecuado en:, http://www.apep.es/claves-para-identificar-un-proyecto-adecuado-de-consultora-para-implementar-la-lopd-de-forma-integral

disposiciones previstas en la legislación, ya que les resulta excesivamente técnica, incluso tediosa y compleja. Así, la "traducción" de la normativa al idioma habitual de las pequeñas empresas puede ayudarles a comprender las implicaciones concretas.

Uno de los informes del Eurobarómetro[22] analizaba explícitamente este punto. Ante la pregunta a las empresas de si estas ven favorable una "clarificación de la aplicación práctica de las definiciones y conceptos clave de la directiva europea y de las leyes nacionales sobre protección de datos", un 76% de las empresas europeas consultadas respondía afirmativamente. En el caso de empresas españolas, el porcentaje asciende al 97%: casi la totalidad de las empresas españolas (cabe recordar en este punto que el Eurobarómetro no abarca exclusivamente a pequeñas y medianas empresas, sino a empresas de más de 20 empleados) agradecería una clarificación terminológica de la ley sobre protección de datos.

10.1.4 Poner en valor el papel de la AEPD

Actualmente, todavía hay empresas, especialmente pequeñas y medianas, que desconocen la existencia y/o la labor de la Agencia Española de Protección de Datos. Por ello, es clave reforzar la comunicación sobre la autoridad de control, sus funciones y responsabilidades en materia de protección de datos.

10.2 PROPUESTAS EN MATERIA DE DIAGNÓSTICO E INFORMACIÓN

10.2.1 Diagnóstico periódico del tratamiento y la seguridad de los datos de carácter personal en las empresas

La realización de un diagnóstico periódico sobre el estado y evolución del cumplimiento de la normativa de protección de datos en la empresa española ha de permitir a los poderes públicos, tanto diseñar adecuadamente las medidas oportunas de cara a conseguir el más alto grado de adaptación e implementación de las disposiciones, como realizar un seguimiento y evaluar el impacto que estas han tenido, así como ir adaptándolas a los factores endógenos y exógenos que se den en cada momento. El presente estudio es un ejemplo de ello.

10.2.2 Elaboración de un sistema de medición y seguimiento de indicadores sobre el estado de la protección de datos en la empresa

Esta acción permitiría elaborar estadísticas y dotar de información cuantitativa para poder dimensionar la situación real en cada momento. Así se podrían tomar decisiones de forma global sobre el grado de implantación y adecuación a la normativa vigente.

[22] Eurobarometro Comisión Europea (Feb. 2008): "Data Protection in the European Union. Data controllers percepctions"

10.3 PROPUESTAS EN MATERIA DEL PROCESO DE ADECUACIÓN Y LA GESTIÓN DEL TRATAMIENTO

10.3.1 Facilitar el proceso de adaptación, ofreciendo pautas y herramientas y asesorar a las empresas con mayores dificultades

Se propone asimismo facilitar información y asesorar a las empresas con mayores dificultades de implementación de la Ley, especialmente entre las empresas con menores recursos, que suelen coincidir con las de menor tamaño, proporcionando información y herramientas para su implantación y cumplimento de la manera más ágil posible.

Se propone informar a las empresas sobre los procedimientos necesarios para desempeñar los apartados de la normativa que desconocen y aplican en menor medida, como por ejemplo el registro de los ficheros de datos en el Registro General de Protección de Datos de la AEPD, la implantación de los inventarios que contengan, entre otros, los datos de carácter personal, la disposición de un protocolo de acción, así como la tenencia de un registro de incidencias, haciendo hincapié en los beneficios que conlleva como por ejemplo: mayor seguridad jurídica para la empresa, mejoras de calidad en los procesos, mayores garantías para trabajadores y clientes, etc.

Incrementar el nivel de cumplimiento normativo por parte de las empresas pasa, necesariamente, por simplificar y facilitar los trámites previstos para su adaptación.

Es destacable, en este punto, el esfuerzo constante de la Agencia Española de Protección de Datos. Así, el sistema de notificaciones telemáticas NOTA[23] permite la inscripción de ficheros en línea, de manera sencilla y gratuita. Recientemente ha puesto en marcha su sede electrónica, con objeto de facilitar la realización de trámites a través de Internet. Procedimientos como la presentación de una denuncia, o de una reclamación de tutela de derechos, por ejemplo, pueden ser realizados de manera electrónica.

A estas acciones se unen las iniciativas de carácter sensibilizador emprendidas por la AEPD, tales como la publicación y difusión de guías y la organización de seminarios y sesiones abiertas. También es destacable la herramienta Evalúa[24], consistente en una especie de diagnóstico sobre el cumplimiento de la normativa, basado en un auto-test en el que la empresa responde a una serie de preguntas con respuesta múltiple. Una vez cumplimentado el cuestionario, la Agencia Española de Protección de Datos facilita a la empresa un informe con indicaciones y recursos que le orientan, en su caso, para cumplir con lo dispuesto en la LOPD.

[23] Disponible en: https://www.agpd.es/portalwebAGPD/canalresponsable/inscripcion_ficheros/Notificaciones_tele/obtencion_formulario/index-ides-idphp.php.

[24] Disponible en: http://www.servicios.agpd.es/Evalua/home.seam.

También INTECO ha llevado a cabo acciones tendentes a facilitar el proceso de adaptación normativa a las pequeñas y medianas empresas. Así, INTECO ha elaborado una *Guía para empresas: cómo adaptarse a la normativa sobre protección de datos*[25], que pretende ser el punto de partida para que los encargados de estas empresas comiencen a formarse en la normativa y sienten una base inicial de partida para adaptarse a la misma.

El Catálogo de empresas y Soluciones de Seguridad TIC de INTECO-CERT, disponible online en http://cert.inteco.es/icdemoest/Catalogo_STIC/, permite realizar una búsqueda de empresas consultoras expertas en implantación y certificación de normativas establecidas en una provincia, lo que sirve de ayuda a las empresas interesadas en contar con la colaboración de una empresa externa para ayudarles a adecuar sus sistemas a la LOPD.

Por último, entre los cursos gratuitos de formación en seguridad que ofrece INTECO, se encuentra el *Curso de la LOPD: Adecuación y Cumplimiento*, al que se puede acceder a través de: https://formacion-online.inteco.es/inscripcion/.

10.3.2 Establecer requisitos y exigencias acordes al tamaño de la empresa y su actividad

Deben considerarse las particularidades de las pequeñas y medianas empresas (en dimensiones, sector de actividad, facturación, tipología de datos, disponibilidad de recursos humanos, económicos y técnicos…) para modular las exigencias normativas.

Se ha observado a lo largo del informe la estrecha relación entre el tamaño de la empresa y el grado de cumplimiento de la LOPD. Por ello, debido a la dificultad que tienen las empresas más pequeñas, tanto de conocer como de cumplir la normativa (bien sea por falta de recursos o por falta de cultura de protección de datos), se cree conveniente establecer exigencias diferentes en función del tipo de empresa y de su tamaño, especialmente atendiendo a las características específicas del negocio, puesto que no es igual la información que se maneja en un hospital que en una empresa manufacturera. Las empresas más pequeñas suelen tener una afluencia de datos menor y, en general, también es menor el nivel de protección de sus datos.

Salvo la reseñable modificación que recoge la Ley 2/2011, de 4 de marzo, de Economía Sostenible, introduciendo la figura del apercibimiento y graduando la cuantía de las sanciones ante determinadas circunstancias –el volumen de negocio, la actividad o el número de tratamientos efectuados, entre otros criterios– por regla general, la normativa en materia de protección de datos establece un marco general para todas las empresas, sin contemplar diferencias entre las grandes, medianas y pequeñas empresas.

[25] INTECO (2009). *Guía para empresas: cómo adaptarse a la normativa sobre protección de datos*. Disponible en: http://www.inteco.es/Seguridad/Observatorio/guias/GuiaManual_LOPD_pymes

Lo cierto es que se trata de realidades completamente diferentes. Muchas de las empresas pequeñas no tienen capacidad suficiente para poder asumir estas exigencias, puesto que carecen de recursos suficientes para poder abordarlas. Por ello, más allá del apartado de infracciones y sanciones, el legislador debería tener en cuenta estas diferencias para modular sus disposiciones. No se trata de establecer medidas de seguridad u obligaciones diferentes en función del tamaño de la empresa, pero sí de tener en cuenta las particularidades de cada colectivo para garantizar una aplicación eficaz.

10.3.3 Impulsar un mayor control y seguimiento del cumplimiento normativo

Se considera necesario realizar un mayor seguimiento a través de visitas de concienciación, recordatorio e información sobre la normativa, como paso previo a la sanción en caso de reincidir en esta práctica.

10.3.4 Poner mayor énfasis en los aspectos más relevantes, rebajando las exigencias de carácter formal

Actualmente, la Comisión Europea está definiendo nuevas propuestas sobre la protección de datos, por lo que se espera un cambio de filosofía importante. Las obligaciones se centran en lo sustantivo, suavizando las formalidades (inscripción del fichero, autorizaciones previas de transferencia, etc) haciendo mucho hincapié en la responsabilidad del control de los ficheros de datos y fomentando la autorresponsabilidad, plasmándose todo ello en una serie de documentación interna que podrá ser requerida llegado el caso para constatar que se ha hecho ese análisis previo de privacidad y que la protección de los datos se está gestionando adecuadamente.

Este cambio afectará especialmente a las pequeñas empresas quienes actualmente cumplen en menor medida la norma y tendrán que adaptarse de nuevo a otro tipo de procesos.

10.3.5 Contar con el apoyo de un tercero en el proceso de adecuación y tratamiento

Desde INTECO, la recomendación es recurrir a los profesionales para garantizar la calidad en el cumplimiento, basándonos en que un alto porcentaje de empresas que han tenido éxito en la implantación de la LOPD y RDLOPD se han apoyado en una empresa externa con experiencia en la materia.

En estos casos, es necesario asegurarse de que la empresa prescriptora está cualificada en la materia. INTECO ofrece un catálogo de empresas y profesionales que operan en el mercado español: http://cert.inteco.es/icdemoest/Catalogo_STIC.

10.3.6 Autorregulación de las empresas prescriptoras y facilitadoras

Asimismo, recordar la importancia de la autorregulación de las empresas dedicadas a prescribir y/o facilitar el proceso de adaptación a la normativa, al estilo de asociación o colegiación de los profesionales del sector, como es el caso de la Asociación Profesional Española de Privacidad (APEP) www.apep.es. Es especialmente importante su función de dotar de patrones de calidad al desarrollo profesional de las actividades vinculadas a la privacidad, mediante la elaboración de códigos éticos y certificaciones de competencias.

10.3.7 Apoyo económico a las empresas

Por un lado, se insta a las asociaciones empresariales a promover la firma de acuerdos sectoriales que abaraten la implantación y aplicación de SGSI y la LOPD, facilitando la renovación de equipos y la introducción de medios tecnológicos en la gestión de las empresas.

Por otro lado, incluso considerando la actual coyuntura económica restrictiva del sector público, se plantea tanto un posible apoyo presupuestario por la Administración, con ayudas o incentivos de carácter finalista para la adaptación continua en protección de datos; como un apoyo indirecto, a través del acceso a cursos de formación, herramientas, etc. que complementen los recursos propios de las empresas.

10.4 PROPUESTAS EN MATERIA DE NORMALIZACIÓN Y CERTIFICACIÓN

10.4.1 Establecer un sello ad hoc para las empresas cumplidoras con la LOPD

En España, los sistemas de certificación son valorados positivamente por los proveedores y clientes, y entre las empresas aumenta la necesidad de distinguirse del resto a través de la constatación de la calidad en la gestión para ganar así prestigio, especialmente en el desarrollo de los procesos.

Al igual que sucede con otro tipo de gestiones, se propone establecer un sistema de certificación para las empresas cumplidoras de la LOPD. Se trata de fijar un distintivo entre las empresas que protegen los ficheros de datos empleados de las que no lo hacen. Hasta ahora no existe ningún sistema para distinguir el cumplimiento normativo, más allá de las sanciones económicas en los casos de incumplimiento tras la inspección. El establecimiento de este tipo de sistemas puede animar y estimular a las empresas a ofrecer un servicio de calidad, sirviendo de reclamo para las empresas contratantes. Asimismo, las empresas que hasta ahora no cumplen con la norma, pueden sentirse presionadas a hacerlo, debido a los beneficios que conlleva, no solo los propios de la norma, sino también los adyacentes.

Adicionalmente, este sistema de certificación debería ampliarse a las empresas que prestan servicios a la pequeña y media empresa, como por ejemplo las gestorías, las que

mantienen sus sistemas de información, las que le proporcionan el *hosting*, y otros muchos ejemplos.

En la mayoría de los casos, dichas empresas se convierten para sus clientes, a efectos de la LOPD, en encargados del tratamiento. En bastantes ocasiones, en función del tamaño de la empresa y de los servicios que se prestan, se podría decir que la empresa prestadora del servicio soporta una gran parte de las medidas exigidas sobre todo por el RDLOPD.

De esta forma, con la aplicación de esta recomendación se lograrían dos objetivos:

- Para las empresas que contratan los servicios, este sello les aportaría mayores garantías de cumplimiento con la LOPD (o al menos la parte correspondiente al RDLOPD) puesto que, como este informe ha puesto de relieve, un número significativo de ellas desconoce o no tiene constancia de las obligaciones a las que hay que someterse para su cumplimiento. El conocimiento de que contratan servicios a empresas proveedores que poseyeran este sello, las haría más conscientes de esta realidad.

- Para las empresas que prestan los servicios, el poseer este sello les permitiría aportar valor añadido a su oferta, distinguiéndolas de aquellas que ofrecen los mismos servicios pero no lo tienen, lo que a su vez fomenta la competitividad sectorial. El hecho de que las empresas proveedoras tengan que publicitar y explicar a sus clientes lo que significa tener este sello, redundaría a su vez en fomentar la cultura de cumplimiento de la LOPD.

10.4.2 Certificación de la seguridad de la información y confianza digital

La implantación efectiva y la acreditación de las mejores prácticas identificadas de seguridad de la información, como evidencia interna y frente a terceros siguiendo los esquemas de certificación internacional como el ISO IEC 27001[26] y 27002[27], contribuirá a la implantación de controles de cumplimiento normativo, en general, y de protección de datos, en particular, así como a las auditorias y a las revisiones posteriores.

[26] ISO/IEC 27001 es el estándar para la seguridad de la información. Especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información en las organizaciones.

[27] ISO 27002 proporciona recomendaciones de las mejores prácticas en la gestión de la seguridad de la información, dividido en once secciones y por cada una de ellas se especifican los objetivos de los distintos controles.

ÍNDICE DE GRÁFICOS

ÍNDICE DE TABLAS

ÍNDICE DE ILUSTRACIONES

Síguenos a través de:

Web

Envíanos tus consultas y comentarios a:

observatorio@inteco.es

Instituto Nacional
de Tecnologías
de la Comunicación