INTECO

Instituto Nacional
de Tecnologías
de la Comunicación

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)

OBSERVATORIO DE LA SEGURIDAD DE LA INFORMACIÓN

Instituto Nacional
de Tecnologías
de la Comunicación

Edición: Julio 2008

La presente publicación pertenece a **Instituto Nacional de Tecnologías de la Comunicación (INTECO**) y está bajo una licencia Reconocimiento-No comercial 2.5 España de Creative Commons, y por ello esta permitido copiar, distribuir y comunicar públicamente esta obra bajo las condiciones siguientes:

- Reconocimiento: El contenido de este informe se puede reproducir total o parcialmente por terceros, citando su procedencia y haciendo referencia expresa tanto a INTECO como a su sitio web: www.inteco.es. Dicho reconocimiento no podrá en ningún caso sugerir que INTECO presta apoyo a dicho tercero o apoya el uso que hace de su obra.
- Uso No Comercial: El material original y los trabajos derivados pueden ser distribuidos, copiados y exhibidos mientras su uso no tenga fines comerciales.

Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra. Alguna de estas condiciones puede no aplicarse si se obtiene el permiso de INTECO como titular de los derechos de autor. Nada en esta licencia menoscaba o restringe los derechos morales de INTECO.

Texto completo de la licencia:
http://creativecommons.org/licenses/by-nc/2.5/es/

ÍNDICE

PUNTOS CLAVE

I El derecho a la protección de datos de carácter personal

El derecho a la protección de datos es el derecho fundamental de todo ciudadano a controlar sus datos personales y a disponer y decidir sobre los mismos.

La generalización de las tecnologías de información y comunicación (TIC) ha provocado la creación de mecanismos que facilitan el intercambio y tratamiento de datos. En este contexto, es necesario asegurar el equilibrio entre las posibilidades que ofrecen las TIC y la garantía del derecho fundamental a la protección de datos.

Implícito al reconocimiento de este derecho a todos los ciudadanos, la legislación impone a las organizaciones que disponen de ficheros con datos personales una serie de obligaciones tendentes a garantizar el derecho. Es en este contexto en el que se enmarca el presente estudio, que tiene como objetivo analizar el nivel de adecuación de la pequeña y mediana empresa española a las disposiciones derivadas de la normativa sobre protección de datos.

II Nivel de adopción de la normativa sobre protección de datos en la pyme

La pyme española muestra un bajo nivel de conocimiento de la normativa sobre protección de datos, tanto de la LOPD, vigente desde 1999 (34%) como del reciente reglamento de desarrollo (RDLOPD), en vigor desde abril de 2008 (14%). Dado que la ley lleva en vigor casi diez años, que su aplicación es de obligado cumplimiento para todas las empresas con ficheros de datos personales, y que se prevén sanciones ante su incumplimiento, preocupa el escaso conocimiento de la misma entre el colectivo pyme. De hecho, prácticamente la totalidad de empresas manejan datos personales: el 96% de las pymes españolas disponen de ficheros con datos de carácter personal (ya sea en sus sistemas informáticos o en sus archivos en papel) y están por tanto potencialmente sujetas a la normativa.

Las pymes trabajan principalmente con ficheros automatizados de clientes (72%), proveedores (51%) y nóminas (30%), que incorporan datos personales del tipo nombre (76%), dirección (71%) y teléfono (70%) del titular del derecho.

Se muestran a continuación algunos datos clave sobre el nivel de adopción de la normativa sobre protección de datos en el entorno pyme:

- Un 37% afirma haber declarado sus ficheros ante la AEPD; la verificación posterior confirma que sólo un 16% de las pymes ha notificado efectivamente los ficheros ante el Registro General de Protección de Datos. Este dato es coherente con la postura de la AEPD, que estima que el nivel de cumplimiento de la

obligación entre las pymes es de entre el 10 y el 15%. El desfase entre declaración y situación real confirma la existencia de un alto sesgo (motivado por el objeto del estudio: nivel de cumplimiento de una ley) y hace sospechar que el resto de resultados pueden verse afectados por este mismo sesgo.

- El nivel de cumplimiento declarado de las principales obligaciones previstas en la LOPD se mueve en torno al 20-30%. Si se asume un cierto sesgo en las respuestas, el nivel sería todavía más reducido. Algunos de los datos más relevantes son:
    - Empresas que cumplen con el deber de información: 29%
    - Empresas que cumplen con el deber de consentimiento: 29%
    - Empresas que disponen de datos personales completos y exactos: 28%
    - Empresas que han establecido procedimientos para garantizar el ejercicio de los derechos de acceso, rectificación, cancelación y oposición (derechos A.R.C.O.) por los particulares: 20%.
- El cumplimiento no es homogéneo entre las diferentes medidas de seguridad previstas en el reglamento. Éste se ha analizado sólo para las empresas que afirman haber declarado sus ficheros ante la AEPD, y oscila entre un 25% para las medidas menos implementadas y un 90% para las más exitosas. A continuación se enumera el nivel de cumplimiento de algunas de las medidas analizadas:
    - Empresas que disponen de documento de seguridad: 82%
    - Empresas que han divulgado la normativa de seguridad entre sus empleados: 72%
    - Empresas que cuentan con un registro de incidencias: 25%
    - Empresas que tienen implantado un control de acceso: 89%
    - Empresas con usuario y contraseña: 48%
- Por lo que respecta al comportamiento de las pymes con respecto a ficheros no automatizados, el 20% tiene establecidas medidas de seguridad equivalentes en el caso de ficheros automatizados y no automatizados, y el 23% afirma clasificar su documentación en papel en función de la confidencialidad del contenido. Aunque no se trata de una exigencia normativa, supone un indicio de que un 20% del tejido pyme español muestra una especial sensibilización hacia el tratamiento

de ficheros con datos personales en soporte papel, y por tanto parece que entre ellas la adaptación a las disposiciones del reglamento resultará, a priori, sencillo.

- A pesar de que los datos sobre nivel de cumplimiento son ciertamente mejorables, el mensaje final lanzado por las pymes es positivo: un 82% manifiesta estar concienciada sobre la necesidad de cumplimiento de la normativa, y un 79% afirma que destinará recursos (humanos y económicos) para su implementación.

III Frenos para la adopción y beneficios derivados de ella

La situación de la pyme española en lo que se refiere al nivel de conocimiento y adopción de la normativa sobre protección de datos no es especialmente positiva, en parte debido a la existencia de una serie de frenos o barreras con los que se encuentran las pymes en su proceso de adopción a la normativa:

- Falta de sensibilidad hacia la necesidad de proteger los datos personales y desconocimiento de la ley: en general, las pymes no son conscientes de la razón de ser de una normativa que proteja los datos de las personas por lo que, aún en el caso de que conozcan la existencia de la ley, la perciben como una imposición o carga y no como algo que pueda aportar un beneficio real para su negocio.

- Rechazo al cambio: quizás por las reducidas dimensiones de las pymes, éstas tienden a mostrar un carácter más conservador que las grandes empresas, y su actitud ante nuevos procesos de trabajo puede no resultar favorable.

- Limitación de recursos (económicos, humanos y de tiempo): éste, junto con el desconocimiento de la ley y la falta de concienciación, son los motivos más alegados por las pymes como causa para la no adopción. Perciben el coste y tiempo de implementación excesivos, y consideran que la necesidad de desviar recursos humanos del objeto principal del negocio para la implementación de la normativa es poco efectivo.

- Ámbito técnico de la normativa sobre protección de datos: tanto la ley como el reglamento adelantan conceptos que resultan excesivamente técnicos, teniendo en cuenta que el destinatario de la normativa no es un experto en normativa sobre protección de datos, sino una pyme cuyo objeto de negocio, en muchas ocasiones, no tiene nada que ver con ello. La excesiva complejidad de la norma supone un freno para su implementación.

- Errónea implementación de la normativa: incluso en los casos en que las empresas se muestran favorables a la implementación de la normativa, ésta se hace de forma incorrecta o incompleta. Así, algunas carencias detectadas son la falta de seguimiento posterior a la adecuación, o la adaptación sólo parcial.

Para contrarrestar estos posibles frenos que afectan en especial a las pequeñas empresas, es necesario concienciar al colectivo sobre los beneficios derivados de la implementación de la normativa sobre protección de datos. Se enumeran a continuación:

- El valor de los datos: los datos personales son, en sí mismos, un activo más de la empresa. Su valor reside en el hecho de tratarse de una información en muchos casos indispensable para continuar con la actividad de la empresa: datos sobre clientes, proveedores o empleados constituyen una información muy valiosa, y pocas veces la pyme se plantea las consecuencias negativas de una pérdida de esta información.

- Aumento de calidad en las operaciones: la normativa sobre protección de datos incorpora pautas que afectan a la sistematización de la información y calidad de la misma, y que implican establecer procesos que mejoran, a largo plazo, la calidad en las operaciones de la empresa.

- Mejora de la imagen corporativa: es cada vez más apreciado por proveedores, clientes, y resto de agentes empresariales, el hecho de que las empresas hayan adaptado su actuación a la normativa sobre protección de datos.

- Es un derecho fundamental, y por tanto se debe velar por su garantía y respeto. Además, el incumplimiento de la normativa por parte de las empresas conlleva la aplicación de posibles sanciones.

- Facilidad en la implementación: en este sentido, la AEPD está desarrollando herramientas tendentes a facilitar la adopción de la normativa por parte de las empresas.

- Creación de un entorno de seguridad: la normativa sobre protección de datos puede constituir el primer paso para que la pyme acceda a un entorno más ambicioso de seguridad, como puede ser por ejemplo la certificación en un Sistema de Gestión de la Seguridad de la Información (SGSI).

1 INTRODUCCIÓN Y OBJETIVOS

1.1 Presentación

1.1.1 Instituto Nacional de Tecnologías de la Comunicación.

El Instituto Nacional de Tecnologías de la Comunicación (INTECO), sociedad estatal promovida por el Ministerio de Industria, Turismo y Comercio, es una plataforma para el desarrollo de la Sociedad del Conocimiento a través de proyectos del ámbito de la innovación y la tecnología. Su objetivo es doble: por una parte, contribuir a la convergencia de España con Europa en la Sociedad de la Información y, de otra parte, promover el desarrollo regional, enraizando en León un proyecto con vocación global. La misión de INTECO es impulsar y desarrollar proyectos de innovación relacionados con el sector de las Tecnologías de la Información y la Comunicación (TIC) y en general, en el ámbito de la Sociedad de la Información, que mejoren la posición de España y aporten competitividad, extendiendo sus capacidades tanto al entorno europeo como al latinoamericano. Así, el Instituto tiene la vocación de ser un centro de desarrollo de carácter innovador y de interés público a nivel nacional que constituirá una iniciativa enriquecedora y difusora de las nuevas tecnologías en España en clara sintonía con Europa. El objeto social de INTECO es la gestión, asesoramiento, promoción y difusión de proyectos tecnológicos en el marco de la Sociedad de la Información. Para ello, INTECO desarrollará actuaciones, al menos, en líneas estratégicas de Seguridad Tecnológica, Accesibilidad, Innovación en soluciones TIC para la Pyme, e-Salud, e-Democracia.

1.1.2 Observatorio de la Seguridad de la Información

El Observatorio de la Seguridad de la Información se inserta dentro de la línea estratégica de actuación de INTECO en materia de Seguridad Tecnológica.

El Observatorio nace con el objetivo de describir de manera detallada y sistemática el nivel de seguridad 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 y la e-Confianza.

El Observatorio ha diseñado un Plan de Actividades y Estudios con el objeto de producir conocimiento especializado y útil en materia de seguridad por parte de INTECO, 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 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 Contexto y oportunidad del estudio

La protección de datos de carácter personal es un derecho fundamental reconocido en la Constitución Española que atribuye al titular del derecho la facultad de controlar sus datos. Las pymes, como agentes que manejan y tratan datos de carácter personal, están obligadas a asegurar el derecho fundamental a la protección de los datos personales de que disponen.

Concurren una serie de circunstancias que definen la realidad española en lo que se refiere a normativa sobre protección de datos y pymes:

- En primer lugar, el tejido empresarial español está constituido en más de un 99% por pequeñas empresas de menos de 50 empleados, y entre ellas tienen un peso especialmente notorio las empresas sin asalariados. Esta situación, diferente a la del resto de países industrializados, exige prestar una atención especial al colectivo pymes y micropymes, en tanto en cuanto son el motor principal de la economía y de la generación de empleo en España.

Tabla 1: Composición del tejido empresarial español por estrato de asalariados

Tipo de empresa por número de asalariados	Número de empresas	Porcentaje
Sin asalariados	1.706.140	51,13%
De 1 a 49 asalariados	1.600.927	47,98%
De 50 a 199 asalariados	23.517	0,70%
De 200 a 499 asalariados	4.218	0,13%
Más de 500 asalariados	1.855	0,06%
TOTAL	3.336.657	100,00%

Fuente: DIRCE (2007) INE

- El colectivo pyme en España presenta un atraso tecnológico con respecto a las empresas de mayor tamaño y un cierto escepticismo y falta de concienciación sobre la seguridad de la información. Son conclusiones del *Estudio sobre incidencias y necesidades de seguridad en las pequeñas y medianas empresas españolas*, elaborado por INTECO y publicado en enero de 2008[1].

- Se trata, además, de un colectivo caracterizado por la heterogeneidad de sectores de actividad, tal y como se mostrará más adelante en el estudio (ver Tabla 2). El común denominador de las pymes es su dimensión reducida, pero es difícil establecer un patrón de comportamiento común en protección de datos que se aplique por igual a tipologías de negocio tan diversas como la hostelería, el pequeño comercio, los profesionales liberales o las gestorías, por mencionar sólo unos ejemplos. A pesar de la heterogeneidad apuntada, en términos generales las pymes no cuentan con recursos específicos en seguridad (técnicos, formativos y humanos), lo cual supone una barrera para la adopción de medidas de seguridad de la información en general, y de protección de datos en particular.

- Además, el 19 de abril de 2008 entra en vigor el reglamento de desarrollo de la ley orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (RDLOPD). El reglamento nace con la vocación de resolver cuestiones interpretativas que existían en la LOPD, desarrollar los mandatos contenidos en ella, y dotar de coherencia a toda la regulación reglamentaria existente hasta entonces. El reglamento contiene nuevas implicaciones para las empresas, como son las extensiones de medidas de seguridad para los ficheros no automatizados, los cambios de niveles de seguridad aplicables a algunos tipos de datos o las transferencias de datos entre grupos internacionales de empresas, entre otras.

[1] Estudio completo disponible en:

http://www.inteco.es/Seguridad/Observatorio/Estudios_e_Informes/Estudios_e_Informes_1

- Por último, la población española muestra una creciente sensibilidad y preocupación sobre de la importancia de la información personal: qué tipo de datos sobre uno mismo están en poder de otras personas, qué uso se está dando de los mismos, etc. En este sentido, el barómetro del CIS correspondiente a febrero de 2008 refleja que a un 71% de la población española les preocupa mucho o bastante la protección de datos y el uso de información personal por otras personas[2].

En el contexto descrito, caracterizado por una creciente sensibilidad hacia la protección de los datos personales, un tejido empresarial español compuesto en más de un 99% por pequeñas empresas y un nuevo marco jurídico desde abril de 2008, se hace necesario un estudio que ofrezca un diagnóstico de la situación actual de las pymes españolas en cuanto a conocimiento y adaptación de la normativa referente a la protección de datos de carácter personal, con especial atención a las novedades previstas en el nuevo reglamento y que afectan a ficheros no automatizados.

1.3 Objetivos del estudio

El objetivo general del estudio es la elaboración de un análisis sobre la situación de la pyme española en lo que se refiere a normativa de protección de datos, con una doble vertiente:

- Diagnóstico, tanto del cumplimiento efectivo de la legislación vigente, como del nivel de preparación para la adecuación a las exigencias previstas en el RDLOPD (sobre todo en lo que se refiere al tratamiento de datos de carácter personal en soporte papel). En este sentido, es importante señalar que el RDLOPD establece plazos para la implantación de las medidas de seguridad previstas en el mismo. Estos plazos de adaptación, que afectan a los ficheros preexistentes a la fecha de entrada en vigor del reglamento, varían en función del tipo de fichero (automatizado o no automatizado) y el nivel de seguridad exigido (básico, medio o alto). Así, para los ficheros no automatizados, las medidas de seguridad de nivel básico serán exigibles en un año, mientras que las de nivel alto contemplan un plazo de dos años. Teniendo en cuenta la existencia de estos plazos, el objetivo del estudio se ha centrado no tanto en la implementación efectiva de las disposiciones del RDLOPD, sino en el nivel de preparación para su adecuación.

- Concienciación y sensibilización: además del objetivo de diagnóstico, existe el objetivo más ambicioso de modificar el comportamiento de la pyme, incrementando la tasa de cumplimiento de la normativa sobre protección de datos.

[2] CIS, Barómetro de Febrero de 2008, Estudio nº 2.754. Encuesta de ámbito nacional con una muestra de 2.470 sujetos (población española de ambos sexos de 18 años y más)

Por ello el proyecto abarca la publicación del presente informe y de una *Guía básica para la pyme de adaptación a la normativa de protección de datos*. La guía, elaborada en base a los resultados de la investigación cuantitativa y cualitativa, tiene como objetivo formar al colectivo pyme sobre la necesidad de la protección de datos, facilitar pautas para su adaptación a la normativa, concienciar acerca de los beneficios derivados de la implementación y remover las potenciales barreras que están frenando su adopción.

Este objetivo general de diagnóstico, concienciación y sensibilización se desglosa operativamente en los siguientes objetivos específicos:

- Identificar nivel de adecuación de la pequeña y mediana empresa española a la normativa en materia de protección de datos.

- Identificar qué frenos y barreras se están encontrando las pymes para su adopción. Del mismo modo, destacar cuáles son los beneficios y el valor añadido que la normativa sobre protección de datos aporta al negocio y aportar pautas para eliminar o minimizar los frenos.

- Valorar si la pyme española está preparada para hacer frente al RDLOPD, en vigor desde el 19 de abril de 2008.

- Formular recomendaciones al colectivo pyme y a la administración pública para incrementar el nivel de cumplimiento, en base a los resultados del estudio y a la propia experiencia de los agentes colaboradores.

1.4 Diseño metodológico

Cualquier estudio elaborado a partir de resultados obtenidos por medio de encuestas de opinión se encuentra con un sesgo implícito derivado de que las declaraciones se basan en la percepción del encuestado. En este caso, además, existen una serie de condicionantes añadidos que sesgan aún más las respuestas de las empresas, que se concretan en la especial sensibilidad del objeto de análisis (adaptación a una ley cuyo incumplimiento deriva en sanciones) y en el carácter técnico de la materia (que implica conocimientos que no se pueden presuponer a las pymes, que en ocasiones no son capaces de identificar sus necesidades ni de responder a preguntas técnicas). Las características inherentes a las organizaciones empresariales dificultan la realización de estudios de seguridad intrusivos, es decir, aquellos que implican una auditoría de protección de datos.

En vista de las dificultades identificadas se hace necesario definir una aproximación alternativa para contrarrestar y minimizar este posible sesgo, basada en una combinación de técnicas:

- Técnica cuantitativa, que contempla la realización de encuestas a 250 pymes españolas.

- Técnica cualitativa, con entrevistas en profundidad a agentes y expertos implicados en las distintas fases de implementación de la normativa: de un lado, a las propias pymes, actores principales del estudio; de otro, a gestorías y/o consultoras expertas en la implementación de soluciones de protección de datos al colectivo; por último, a la Agencia Española de Protección de Datos, organismo encargado de velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación.

- Contraste de resultados declarados con la AEPD, realizado a través de la comprobación online acerca de la inscripción efectiva de ficheros ante el Registro General de Protección de Datos.

El desarrollo del estudio, con las técnicas descritas, se ha llevado a cabo en una etapa de investigación y una etapa de formulación de recomendaciones, que se analizan a continuación.

1.4.1 Etapa de investigación

Esta etapa tiene como objetivo recopilar de las distintas fuentes, primarias y secundarias, toda la información necesaria para alcanzar los objetivos del proyecto. Consta, a su vez, de cuatro fases, que se tratarán en profundidad en los siguientes epígrafes:

- Fase I: Búsqueda y análisis documental

- Fase II: Investigación cuantitativa

- Fase III: Contraste de resultados

- Fase IV: Investigación cualitativa

Fase I: Búsqueda y análisis documental

Esta fase tiene como objetivo analizar exhaustivamente las disposiciones legales y otros contenidos, con el fin de sentar las bases de los criterios de búsqueda. Se han tenido en cuenta, principalmente, fuentes de carácter normativo, así como estudios e informes publicados en la materia que puedan enriquecer y orientar el proyecto de investigación.

Entre las referencias de carácter normativo y/o jurisprudencial destacan las siguientes:

- Constitución española de 1978.

- Ley Orgánica 5/92 de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal de 26 de Octubre (LORTAD) *(derogada)*

- Directiva Europea 95/46 CE del Parlamento Europeo y del Consejo de 24 de Octubre de 1995.

- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

- Reglamento de Medidas de Seguridad (Real Decreto 994/1999 de Medidas de Seguridad de los ficheros automatizados que contengan datos de carácter personal de 11 de Junio de 1999) *(derogado).*

- Sentencia 292/2000 del Tribunal Constitucional, de 30 de noviembre.

- Real Decreto 1720/2007, de 21 de Diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica de Protección de Datos de Carácter Personal.

Entre los estudios tenidos en cuenta para la identificación de hipótesis a contrastar y generación de contenido complementario destacan los siguientes:

- Barómetro de Febrero. Estudio nº 2.754. Centro de Investigaciones Sociológicas (CIS) (2008).

- Data Protection in the European Union. Citizens' perceptions. Flash Eurobarometer 225 – The Gallup Organization (2008).

- Data Protection in the European Union. Data controllers' perceptions. Flash Eurobarometer 226 – The Gallup Organization (2008).

- Datos en papel. Tratamiento de datos personales e información confidencial en soporte papel en la empresa española. Landwell (2006).

Por último, otras fuentes consultadas han sido las siguientes. Se relacionan a continuación artículos de revistas, guías prácticas y páginas web tenidas en cuenta en la elaboración del estudio:

- Agencia española de protección de datos. Guía de seguridad (abril 2008), Guía de Protección de Datos para Responsables de Ficheros (2008), Guía del derecho fundamental a la protección de datos de carácter personal (2004)

- De la Peña Muñoz, J. (2008). SIC. Nº 78. Pp. 68-72 (febrero 2008).

- García Rey, M. (2008). SIC. Nº 78. Pp. 74-75 (febrero 2008).
- Serrera Cobos, P. (2008). "¿Qué hacer con los ficheros en papel?". Protección de datos. Nº 21 (abril 2008).
- Tejeda, C. (2008). "Buenas prácticas en el desarrollo de un proyecto de protección de datos". Protección de datos. Nº 21 (abril 2008).
- Página web de la Agencia española de protección de datos: www.agpd.es
- Entrevista digital con Artemi Rallo (director de la AEPD): http://www.elmundo.es/encuentros/invitados/2008/04/3030/index.html
- http://www.derecho.com/legislacion/boe/33023
- http://www.derecho.com/legislacion/boe/735136
- Página Web de la Moncloa con las principales innovaciones del Nuevo Reglamento: http://www.la-moncloa.es

Fase II: Investigación cuantitativa

Esta fase incluye la realización de 250 encuestas telefónicas a pymes del territorio español peninsular, Baleares, Canarias, Ceuta y Melilla.

Universo

El universo objeto del estudio está constituido por toda empresa española de hasta 50 empleados, pertenecientes a los sectores señalados en la Tabla 2, con un rango de número de trabajadores. Se trata, por tanto, de micropymes (menos de 10 empleados) y pequeñas empresas (10-50 asalariados). Se excluyen del ámbito del estudio las medianas empresas (50-250 empleados) por el escaso peso que tienen dentro del panorama empresarial español (0,7% de los más de 3 millones de empresas) y por su tendencia a la asimilación con las grandes empresas en el cumplimiento de normativa.

Tabla 2: Universo pymes españolas de menos de 50 asalariados

CNAE	Sector de actividad	< 10 empleados	10 – 50 empleados	Total	Total (%)
CNAE 10 – 14	Industrias extractivas	2.148	722	2.870	0,1%
CNAE 15 – 40	Industria manufacturera	196.680	36.322	233.002	7,1%
CNAE 41	Producción y distribución de energía eléctrica, gas y agua	1.023	104	1.127	0,0%
CNAE 45	Construcción	443.548	39.948	483.496	14,6%
CNAE 50 – 52	Comercio, reparación de vehículos de motor, motocicletas y ciclomotores y artículos personales y de uso doméstico	808.426	32.509	840.935	25,4%
CNAE 55	Hostelería	275.429	10.001	285.430	8,6%
CNAE 60 – 64	Transporte, almacenamiento y comunicaciones	233.129	9.238	242.367	7,3%
CNAE 65 – 67	Intermediación financiera	59.602	803	60.405	1,8%
CNAE 70 – 74	Actividades inmobiliarias y de alquiler, servicios empresariales	739.283	21.035	760.318	23,0%
CNAE 80	Educación	57.240	5.189	62.429	1,9%
CNAE 85	Actividades sanitarias y veterinarias, servicio social	120.145	4.884	125.029	3,8%
CNAE 90 – 93	Otras actividades sociales y de servicios prestados a la comunidad, servicios personales	200.810	8.849	209.659	6,3%
TOTAL		3.137.463	169.604	3.307.067	100,0%

Fuente: INTECO

Tamaño y distribución muestral

Se ha extraído una muestra representativa de 250 empresas según un modelo aleatorio simple. Los datos de origen para la selección de la muestra han sido extraídos de la Base de Datos del Registro Mercantil, de un universo de pymes registradas. La muestra se ha distribuido entre los sectores pertenecientes al código CNAE 93 relacionados, habiéndose realizado el muestreo por cuotas de tamaño y representatividad de cada uno de los sectores.

Tabla 3: Distribución de la muestra por sector CNAE y número de asalariados (en valores absolutos y %)

CNAE	Sector de actividad	< 10 empleados	10 – 50 empleados	Total	Total (%)
CNAE 10 – 14	Industrias extractivas	20	5	25	10,0%
CNAE 15 – 40	Industria manufacturera	13	3	16	6,4%
CNAE 41	Producción y distribución de energía eléctrica, gas y agua	0	0	0	0,0%
CNAE 45	Construcción	30	3	33	13,2%
CNAE 50 – 52	Comercio, reparación de vehículos de motor, motocicletas y ciclomotores y artículos personales y de uso doméstico	55	2	57	22,8%
CNAE 55	Hostelería	19	1	20	8,0%
CNAE 60 – 64	Transporte, almacenamiento y comunicaciones	16	1	17	6,8%
CNAE 65 – 67	Intermediación financiera	4	0	4	1,6%
CNAE 70 – 74	Actividades inmobiliarias y de alquiler, servicios empresariales	50	1	51	20,4%
CNAE 80	Educación	4	0	4	1,6%
CNAE 85	Actividades sanitarias y veterinarias, servicio social	8	0	8	3,2%
CNAE 90 – 93	Otras actividades sociales y de servicios prestados a la comunidad, servicios personales	14	1	15	6,0%
TOTAL		233	17	250	100%

Fuente: INTECO

Captura de información

Encuestas telefónicas a los responsables de cada una de las empresas (gerentes, propietarios, responsables o delegados). El trabajo de campo fue realizado entre Diciembre de 2007 y Febrero de 2008.

Error muestral

De acuerdo con los criterios del muestreo aleatorio simple para variables dicotómicas en las que p=q=0,5 y para un nivel de confianza del 95%, se establece el siguiente cálculo del error muestral: muestra total n= 250, error muestral ±6,2%.

Fase III: Contraste de resultados

Dado que la técnica empleada en la fase cuantitativa (encuesta telefónica) cuenta con el sesgo implícito a cualquier herramienta basada en la percepción del sujeto, se ha incluido en la investigación un mecanismo objetivo que corrija esta posible desviación. De este

modo, se ha contrastado una parte de los resultados de las encuestas a empresarios con la información pública ofrecida por la AEPD a través de www.agpd.es. La información verificada es la relativa a la confirmación de declaración efectiva de ficheros ante el Registro.

El objetivo de esta fase es introducir un elemento objetivo y riguroso que permita, por una parte, mostrar la situación real en cuanto a implementación de determinados aspectos de la normativa sobre protección de datos por parte de las pymes españolas, y por otra, constatar la coincidencia o discrepancia entre las declaraciones o percepciones de las pymes encuestadas y el nivel real de cumplimiento.

La consulta fue realizada en febrero de 2008.

Fase IV: Investigación cualitativa: participantes

El objetivo de esta fase es la aportación de una visión integral y multidisciplinar al proyecto que, por un lado, profundice en los resultados obtenidos en la fase cuantitativa y, por otro, constituya un referente para la formulación de recomendaciones.

A través de entrevistas en profundidad, se ha recogido, documentado y analizado la opinión de 40 agentes pertenecientes a tres áreas de conocimiento o de negocio:

- Dentro del ámbito empresarial, se han analizado 25 casos de pymes (casos de éxito y casos de no éxito), con el objetivo de conocer las barreras más frecuentes en la implementación de la normativa y las necesidades particulares del colectivo, para poder identificar y activar los mecanismos de remoción de los frenos. Asimismo, los casos empresariales aportan la visión relativa al nivel de concienciación sobre la normativa, los beneficios detectados o esperados y otros aspectos que complementan los resultados de la fase cuantitativa.

- Se ha incluido en el análisis la visión del sector consultoría, aportando la visión de 13 consultoras especializadas en implementar la normativa LOPD en pequeñas y medianas empresas.

- Por último, un estudio de estas características no podía prescindir de la visión clave de la AEPD, organismo encargado de velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación. Se han realizado 2 entrevistas, al Director General de la Agencia y a la Subdirectora General del Registro General de Protección de Datos de la AEPD.

Las entrevistas fueron realizadas entre enero y abril de 2008, y se han seguido tres métodos diferentes para la obtención de la información, en función de la disponibilidad de la persona consultada:

- Entrevistas personales
- Entrevistas telefónicas
- Cuestionarios online

1.4.2 Etapa de análisis y elaboración de recomendaciones

Una vez finalizada la etapa de investigación y recabada toda la información disponible en la materia, se lleva a cabo un análisis de resultados que permite extraer conclusiones y formular recomendaciones a sector privado y público, que conforman la base del presente estudio.

Por otra parte, el proyecto contempla la elaboración de la *Guía básica para la pyme de adaptación a la normativa de protección de datos*, publicación autodidacta que tiene como objetivo iniciar al pequeño empresario en la necesidad de proteger los datos y facilitar unas pautas básicas sobre cómo iniciar el proceso.

1.4.3 Estructura de contenidos

El presente informe se estructura en torno a los siguientes puntos:

- Exposición de los puntos clave del proyecto, donde se detallan los principales resultados de la investigación.
- Presentación de INTECO y del Observatorio de la Seguridad de la Información, y explicación de los objetivos y metodología del estudio.
- Visión del derecho fundamental a la protección de datos, contextualizando la necesidad de una normativa específica en la materia y revisando la legislación española al respecto.
- Descripción de las obligaciones de las pymes en relación con la protección de datos derivadas de la normativa española.
- Análisis del nivel de adopción de la normativa de protección de datos de carácter personal entre las pymes españolas.
- Identificación de las barreras a las que se enfrentan las pymes en su proceso de adopción de la normativa, y enumeración de los beneficios y valores añadidos derivados de la misma.
- Resumen de las principales conclusiones que describen la situación analizada y formulación de recomendaciones a las pymes y a la administración pública, con el objetivo de asegurar la correcta implantación.

2 PROTECCIÓN DE DATOS

2.1 Necesidad de una normativa sobre protección de datos

El derecho a la protección de datos es el derecho que tiene todo ciudadano a controlar sus datos personales y a disponer y decidir sobre los mismos. Se trata de un derecho fundamental con entidad propia y diferente al derecho a la intimidad.

La normativa sobre protección de datos responde a la necesidad de proteger todos los datos de carácter personal, para que no sean utilizados de forma inadecuada, ni tratados o cedidos a terceros sin consentimiento inequívoco del titular.

En este contexto, se entiende por dato de carácter personal *"cualquier información concerniente a personas físicas identificadas o identificables*[3]*"* (art. 3 LOPD).

El entorno actual se caracteriza por un creciente protagonismo de las tecnologías de información y comunicación (TIC), que implica a su vez una mayor facilidad y rapidez en el intercambio de datos. Así, se han creado mecanismos eficaces de recogida y tratamiento de datos personales que, de un lado, permiten un mayor alcance en la recopilación y sistematización pero, de otro, pueden suponer un límite al control sobre los mismos. La extensión de estos mecanismos provoca que cada vez sean más las empresas que traten con datos personales. En este contexto, se hace necesario un equilibrio entre los beneficios derivados de la generalización en el uso de las TIC y la garantía de los derechos fundamentales de los ciudadanos, en concreto el derecho a la protección de datos objeto del presente estudio.

Este balance entre derecho del ciudadano a preservar el control sobre sus datos personales y la aplicación de las nuevas tecnologías de la Información es el contexto en el que se enmarca el derecho fundamental a la protección de datos de carácter personal en la legislación española. La regulación ofrece a los ciudadanos las garantías y mecanismos necesarios para proteger sus datos personales y controlar el uso que se realiza de los mismos.

De cara a garantizar la protección del derecho, se establecen obligaciones para toda persona física o jurídica que posea ficheros con datos personales. La mayor parte de las organizaciones (empresas, administraciones públicas), en mayor o menor medida, disponen de ficheros o bases de datos personales y están obligadas al cumplimiento de la normativa vigente en materia de protección de datos.

[3] La Directiva 95/46 CE define el término identificable como *"toda persona cuya identidad pueda determinarse directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social".*

2.2 Cronología de la protección de datos en España

La primera referencia sobre la necesidad de proteger la intimidad personal en el ámbito informático data del año 1978. El artículo 18.4 de la Constitución española dispone que "*la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos*". Con la inclusión de este apartado en el artículo 18, el constituyente ya era consciente de los riesgos que podría entrañar el uso de la informática, encomendando al legislador la aprobación de normas que garantizasen ciertos derechos fundamentales. Aunque no hace mención explícita a los datos de carácter personal, éstos forman parte de la intimidad de las personas, puesto que pertenecen al ámbito más privado de las mismas.

En 1992 aparece la primera Ley española que regula de forma específica la cuestión de los datos personales. Se trata de la Ley Orgánica 5/92 de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal de 26 de Octubre (LORTAD), y su objetivo es proporcionar cobertura a lo establecido en el artículo 18.4 de la Constitución española. De este modo, pretende delimitar una nueva frontera de la intimidad y del honor que proteja a las personas físicas de la utilización mecanizada, ordenada y discriminada de los datos a ellas referentes. Su ámbito de aplicación se circunscribe a los ficheros de carácter automatizado. La LORTAD constituyó el primer texto legal que en España regula la protección de datos de carácter personal.

El 24 de Octubre de 1995 se dicta la Directiva Europea 95/46 CE del Parlamento Europeo y del Consejo relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales. La directiva tiene como objetivo proteger los derechos y las libertades de las personas en lo que respecta al tratamiento de datos personales, estableciendo principios de orientación para determinar la licitud de dicho tratamiento.

Es a finales de 1999 cuando se publica en España la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD), que resuelve el vacío legal existente desde 1992 referente a los ficheros de carácter no automatizado, ampliando el ámbito de aplicación a todo tipo de ficheros, independientemente del soporte en el cuál sean tratados. Esta ley, que deroga la LORTAD, se adecua a lo establecido en la Directiva Europea 95/46 CE.

La LOPD tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente su honor e intimidad personal y familiar. Así, garantiza una serie de derechos a las personas físicas, titulares de los datos, tales como el derecho a ser informado de cuándo y porqué se tratan sus datos personales, el derecho a acceder a los datos y, en caso necesario, el derecho a la modificación o supresión de los datos o el derecho a la oposición al tratamiento de los mismos. Del mismo modo, establece las obligaciones relativas a la recogida de los datos, consentimiento, almacenaje,

conservación, uso, datos especialmente protegidos, comunicación o cesión de los mismos y transferencias internacionales de datos.

Esta ley marca el inicio de una nueva etapa del derecho de intimidad de las personas, más completa y ajustada a la realidad de cualquier presentación de información sobre la vida privada de un individuo.

La LOPD se apoya operativamente en el Reglamento de Medidas de Seguridad (RMS, Real Decreto 994/1999 de Medidas de Seguridad de los ficheros automatizados que contengan datos de carácter personal de 11 de Junio de 1999) como instrumento para facilitar los mecanismos prácticos para cumplir con las prescripciones establecidas en la LOPD. El RMS regula las medidas técnicas y organizativas que deben aplicarse a los sistemas de información en los cuales se traten datos de carácter personal de forma automatizada.

La Sentencia 292/2000 del Tribunal Constitucional, de 30 de noviembre, marca un hito en el ámbito de la protección de datos al recoger de manera expresa el derecho fundamental a la protección de datos como un derecho que se desprende del apartado 4 del artículo 18 de la Constitución Española que, si bien comparte con el derecho fundamental a la intimidad del artículo 18.1 el objetivo de ofrecer una eficaz protección constitucional de la vida privada personal y familiar, persigue una finalidad distinta como es garantizar a la persona un poder de control sobre sus datos personales, su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado. Es decir, en virtud de esta sentencia, el Tribunal Constitucional define el derecho fundamental a la protección de datos de carácter personal como autónomo e independiente.

Finalmente, aparece el Real Decreto 1720/2007, de 21 de Diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica de Protección de Datos de Carácter Personal (RDLOPD aprobado en Consejo de Ministros de 21/12/2007 y publicado en el Boletín Oficial del Estado (BOE) el 19 de Enero de 2008). Este reglamento deroga al RMS de 1999 y desarrolla de forma completa la Ley Orgánica 15/1999 de Protección de Datos de carácter personal. Nace con la vocación de, no sólo desarrollar los mandatos contenidos en la LOPD, en particular, en lo relativo a las medidas de seguridad y a los criterios aplicables a los ficheros y tratamientos de datos personales no automatizados, sino también de dotar de coherencia a toda la regulación reglamentaria existente hasta la fecha de su aprobación. También aporta seguridad jurídica gracias al desarrollo de aquellos aspectos en los que la experiencia práctica ha aconsejado un mayor grado de precisión. En general, el reglamento contribuye a conseguir una mayor claridad en la aplicación de la norma y a adaptar sus previsiones a la realidad existente en la actualidad. La LOPD es tan general, y pretende aplicarse a tal

universo de supuestos distintos, que necesitaba de un reglamento que la desarrollase y concretase al máximo, adaptándola a la realidad actual y a sectores muy diferentes.

El reglamento de desarrollo de la LOPD contiene nuevas implicaciones para las empresas, como son las extensiones de medidas de seguridad para los ficheros no automatizados, los cambios de niveles de seguridad aplicables a distintas tipologías de datos o las transferencias de datos entre grupos internacionales de empresas, entre otras. Así, establece las normas, medidas, procedimientos y mecanismos que se han de adoptar obligatoriamente para garantizar la seguridad respecto a los ficheros automatizados y no automatizados, los centros de tratamiento, locales, equipos, sistemas, programas y las personas que intervengan en el tratamiento de los datos de carácter personal.

El órgano de control del cumplimiento de la normativa de protección de datos dentro del territorio español es, con carácter general, la Agencia Española de Protección de Datos (AEPD), existiendo otras agencias de protección de datos de carácter autonómico para los ficheros de titularidad pública en la Comunidad de Madrid, Cataluña y País Vasco.

La Agencia Española de Protección de Datos es un ente de Derecho público, con personalidad jurídica propia y plena capacidad pública y privada, que actúa con plena independencia de las Administraciones Públicas en el ejercicio de sus funciones. Su misión es velar porque se garantice el derecho de la protección de datos, lo que significa recibir las denuncias de cualquier ciudadano, investigarlas y sancionarlas, si corresponde. Además, a la Agencia le corresponde asesorar a ciudadanos y al conjunto de las administraciones públicas sobre cómo garantizar el derecho. En concreto, las funciones más destacadas de la Agencia son:

- Informar sobre el contenido, los principios y las garantías del derecho fundamental a la protección de datos.
- Ayudar al ciudadano a ejercitar sus derechos, y a los responsables y encargados de tratamientos a cumplir las obligaciones que establece la LOPD.
- Tutelar al ciudadano en el ejercicio de los derechos de acceso, rectificación, cancelación y oposición cuando no han sido atendidos adecuadamente por los responsables de los ficheros.
- Garantizar el derecho a la protección de datos, investigando aquellas actuaciones de los responsables o encargados de ficheros que puedan ser contrarias a los principios y garantías contenidos en la LOPD, e imponer, en su caso, la correspondiente sanción.

2.3 Derecho comparado

El derecho a la protección de datos personales ha cobrado más fuerza en los últimos tiempos debido, de un lado, al incremento del uso y desarrollo de las tecnologías de la información y comunicación, y de otro lado, a la particular visión a nivel mundial de las empresas y organizaciones de considerar los datos personales como un activo más de las mismas, y por tanto, sujeto a las decisiones de negocio que estimen más beneficiosas, dando lugar a un aumento en la comercialización y tratamiento de los datos.

En la actualidad, Europa es el territorio más sensibilizado con la protección de datos, y en consecuencia, presenta un mayor grado de desarrollo regulatorio frente a otros territorios donde, bien existen iniciativas legislativas con vocación de ser implantadas en el corto o medio plazo, bien adolecen de una ausencia absoluta de regulación.

Con la promulgación de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, la Unión Europea ha intentado dar una solución a nivel comunitario para garantizar de manera el derecho a la protección de los datos de carácter personal y buscar el equilibrio entre la garantía del derecho y la libre circulación de los datos personales.

Sin embargo, dentro del ámbito comunitario, existen diferencias entre las distintas legislaciones en cuanto a aspectos tales como la necesidad de registrar los ficheros de datos personales, la existencia de organismos reguladores, el régimen sancionador, la necesidad de consentimiento de los titulares para el tratamiento y la cesión, la configuración de las obligaciones que, en materia de protección de datos, se derivan de las prestaciones de servicios que comportan un acceso a datos, etc.

Por ejemplo, los regímenes sancionadores conforman uno de los aspectos en los que se observan mayores diferencias entre los distintos estados miembros, de forma que se podría establecer una clasificación según la naturaleza de las sanciones. Existen, en este sentido, países en los que las respectivas legislaciones aplicables en materia de protección de datos de carácter personal, ante una eventual vulneración de las mismas, sólo contemplan sanciones económicas de carácter administrativo, como sería el caso de España, Bélgica, Reino Unido y Rumanía.

Dentro de este primer grupo de países las diferencias en relación con los importes de las sanciones resultan llamativas, existiendo países como España, con uno de los importes por sanciones más altos (que pueden alcanzar un máximo de 601.012,10 €) frente a países como Reino Unido, donde la sanción más alta es de 14.002 €.

Por otra parte, se puede distinguir un segundo grupo de países como Portugal, Austria, Polonia y Francia donde la vulneración de las legislaciones específicas de protección de

datos personales, además de sanciones económicas de carácter administrativo, puede llegar a comportar penas privativas de libertad, que van desde 1 año (Portugal, Austria) hasta 5 años (Francia). En Francia, además, es donde se observan las sanciones económicas más altas de todo el territorio de la Unión Europea (1.500.000 €).

En general, puede concluirse que, dentro de los países que conforman el territorio de la UE, existen legislaciones específicas en materia de protección de datos. Sin embargo, los estados difieren en cuanto al grado de desarrollo y alcance de las mismas, pudiendo destacarse países como Francia, Portugal o España, con una mayor presión regulatoria.

No obstante lo anterior, el alcance de la directiva va más allá del territorio que integran los estados miembros, ya que se recogen una serie de requisitos a la hora de transferir datos personales provenientes del territorio comunitario a terceros países, como constituye la exigencia de contar con un nivel de protección equiparable a la zona UE, pudiendo llegarse a cancelar la transferencia internacional de datos.

Las instituciones comunitarias, conscientes de su papel como potencia política y económica mundial y de la importancia que los flujos transfronterizos de datos personales tienen en el ámbito del comercio internacional, han llevado a cabo políticas de promoción de la colaboración con terceros países en los que no existe una verdadera cultura de respeto al derecho a la protección de datos de carácter personal.

En este sentido, se han suscrito acuerdos con países o grupos de países en los que se establecen disposiciones de cooperación en la protección de datos personales al objeto de elevar el nivel de protección y evitar obstáculos que dificulten operaciones comerciales con los mismos. Destaca, entre otras actuaciones, la creación por iniciativa de la Agencia Española de Protección de Datos de la Red Iberoamericana de Protección de Datos, en junio de 2003.

Dentro del continente americano, se encuentran casos tan dispares como el de Argentina, donde se han realizado importantes esfuerzos regulatorios, lo que le ha permitido convertirse en el primer país latinoamericano al que la Unión Europea le ha reconocido un nivel de protección adecuado, y los de Brasil o México, donde no hay una legislación específica en materia de protección de datos.

Por último, el Eurobarómetro[4] de la Comisión europea de febrero de 2008, elaborado a partir de opiniones de empresas europeas, analiza una serie de aspectos relativos a la protección de datos. De ellos se desprende que el 84% de las empresas europeas (el 98% de las españolas) son favorables a una mayor armonización en las medidas de

[4] Eurobarometer Comisión Europea – The Gallup Organization. Data Protection in the European Union. Data controllers' percepciones (February 2008). Encuesta de ámbito europeo realizada a 4.835 controladores de datos de empresas seleccionadas en base a dos criterios: país y número de empleados de la empresa (20-49, 50-249, 250+).

seguridad, y que el 80% (el 96% en el caso español) aboga por una mayor uniformidad entre las legislaciones de los estados miembros en lo que afecta a la normativa sobre protección de datos.

3 OBLIGACIONES PARA LAS PYMES EN MATERIA DE PROTECCIÓN DE DATOS

En virtud de los derechos que reconoce la normativa española a los titulares de los datos, las pymes están obligadas a cumplir con las disposiciones previstas en la LOPD y RDLOPD siempre que dispongan de ficheros con datos de carácter personal, con independencia del soporte en el que se encuentren (ficheros automatizados o no automatizados).

El tratamiento de datos de carácter personal ha de realizarse de acuerdo con los principios de información, calidad, finalidad, consentimiento y seguridad. Dichos principios se plasman en diversos preceptos de la LOPD.

Los principios de la LOPD pretenden proteger los datos personales de los interesados:

- Los datos deben tratarse de manera leal y lícita.
- Los datos deben recogerse con fines determinados, explícitos y legítimos. Los datos deben ser adecuados, pertinentes y no excesivos en relación con el ámbito y los fines para los que se han recogido.
- Los datos deben ser exactos y mantenerse actualizados de manera que respondan con veracidad a la situación actual de su titular.
- Los responsables deben atender a los interesados que soliciten el acceso a sus datos personales.
- Los datos personales sólo deben conservarse durante el tiempo necesario para las finalidades del tratamiento para el que han sido recogidos. Deben ser cancelados cuando hayan dejado de ser necesarios o pertinentes para el fin con que se obtuvieron.

Se enumeran en este apartado las principales implicaciones para las empresas que exige la normativa de protección de datos personales. Entre paréntesis se incluye la referencia normativa donde se recoge la obligación, para facilitar su consulta y contextualización. En el apartado 4.2 se explican en profundidad las implicaciones de cada obligación y su nivel de conocimiento y/o cumplimiento por parte de las empresas.

1. Declaración de los ficheros automatizados, no automatizados o mixtos en la Agencia de Protección de Datos. *(Art. 39 LOPD - Título V, Capítulo II, Art. 55 RDLOPD).*

2. Información al interesado sobre la recogida de datos. *(Art. 5 LOPD - Capítulo II sección 2ª RDLOPD).*

3. Solicitud de consentimiento del interesado para el tratamiento de sus datos. *(Art. 6 LOPD - Capítulo II sección 1ª RDLOPD).* Solicitud de consentimiento para tratar datos de menores de edad. *(Art. 13 LOPD).*

4. Determinación de la finalidad y definición de la calidad de los datos: clasificación, reclasificación (si fuese necesario), ordenación y agrupación de ficheros automatizados y no automatizados. *(Art. 8 LOPD - Título II Capítulo I RDLOPD).*

5. Información al interesado y gestión de la comunicación o cesión de datos de carácter personal. *(Art. 11 LOPD – Art. 10, 12, 16 RDLOPD).*

6. Gestión de derechos de acceso, rectificación, cancelación y oposición (derechos A.R.C.O.) *(Título III LOPD - Título III RDLOPD).*

7. Gestión del tratamiento de datos de carácter personal en transferencias internacionales. *(Título V LOPD – Título VI RDLOPD).*

8. Tratamiento de datos de carácter personal con fines publicitarios y prospección comercial. (*Art. 30 LOPD – Título IV, Sección 2ª, Capítulo II).*

9. Definición del encargado del tratamiento y el responsable del fichero. *(Art. 12 LOPD – Art. 5, 20, 82 RDLOPD).*

10. Gestión de medidas de seguridad aplicables a las distintas tipologías de datos. *(Disposición transitoria segunda, Título VIII RDLOPD).*

    - Desarrollo del documento de seguridad en el que consten las medidas tanto técnicas como organizativas que garanticen un adecuado tratamiento de los datos de carácter personal. *(Art. 88 RDLOPD).*

    - Divulgación de las normas de seguridad adoptadas a todo el personal de la empresa. *(Art. 89.2 RDLOPD).*

    - Control de acceso por parte de los usuarios a los datos de carácter personal. *(Art. 91, 99 RDLOPD).*

    - Definición del mecanismo de identificación/autenticación de los usuarios del sistema. *(Art. 93 RDLOPD).*

    - Gestión de copias de respaldo y recuperación de los ficheros con datos de carácter personal. *(Art. 94, 102 RDLOPD).*

- Desarrollo del registro de incidencias en el que conste fecha, posible motivo y responsable en el momento de ocurrir las incidencias relativas a datos de carácter personal. *(Art. 90, 100 RDLOPD).*
- Gestión de soportes y documentos. *(Art. 92, 97, 101 RDLOPD).*
- Definición del responsable de seguridad *(Art.95 RDLOPD)*.
- Auditoría bienal sobre los sistemas de información, instalaciones, personas y procesos cuyos ficheros sean declarados de nivel medio o alto. *(Art. 96, 110 RDLOPD)*.
- Criterios de archivo para la correcta conservación y localización de documentos que contengan datos de carácter personal. *(Art. 106 RDLOPD).*
- Gestión de accesos a la documentación sólo por personal autorizado. *(Art. 113 RDLOPD).*
- Definición del responsable de seguridad para los documentos que contengan datos de carácter personal. *(Art 109 RDLOPD).*
- Despliegue de medidas de protección física para los ficheros no automatizados con datos de carácter personal. (*Art. 107, 111 RDLOPD).*
- Definición de mecanismos contra la copia y reproducción no autorizada de ficheros no automatizados. *(Art. 112 RDLOPD).*

La mayor parte de las obligaciones contempladas en la normativa deben ser cumplidas por el **responsable del fichero o tratamiento de datos**.

El responsable de un fichero o tratamiento es la entidad que decide sobre la finalidad, el contenido y el uso del tratamiento de los datos personales. Es decir, la empresa será la responsable de los ficheros que contienen datos relativos a sus empleados y a sus clientes, y el resto de ficheros que manejen. Sobre el responsable del fichero recaen las principales obligaciones establecidas por la LOPD y le corresponde velar por el cumplimiento de la Ley en su organización.

Asociada a la figura del responsable está la figura del **encargado**, que es la persona o entidad, autoridad pública, servicio o cualquier otro organismo que, solo o con otros, trate datos por cuenta del responsable, como consecuencia de la existencia de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación para la prestación de un servicio.

Se trataría, por ejemplo, de una empresa que preste servicios para la realización de envíos postales; el informático ajeno a la organización del responsable que realiza tareas de mantenimiento de software o hardware; el gestor administrativo que confecciona nóminas y gestiona el fichero de personal… No se considera encargado del tratamiento a la persona física que tenga acceso a los datos personales en su condición de empleado dentro de la relación laboral que mantiene con el responsable del fichero.

Ambos, encargado y responsable del tratamiento, pueden ser sancionados de acuerdo a la LOPD si incumplen sus obligaciones.

4 NIVEL DE ADOPCIÓN DE LA NORMATIVA SOBRE LA PROTECCIÓN DE DATOS EN LAS PYMES

Se analiza a continuación la situación de la pyme española en cuanto a cumplimiento de las disposiciones legales previstas en la LOPD y RDLOPD.

Los resultados estadísticos sobre el cumplimiento de la normativa en materia de protección de datos que se muestran a continuación corresponden a la parte cuantitativa de los trabajos de investigación del estudio, complementados con información recabada en la fase cualitativa. Tal y como se ha explicado en el apartado 1.4, los resultados tienen su base en opiniones y percepciones de las empresas encuestadas, a excepción de la información contrastada a través del Registro General de Protección de Datos, que se indicará expresamente.

Con el objetivo de facilitar su comprensión este capítulo se ha dividido en 4 subapartados:

- Aproximación a la protección de datos en el entorno pyme.
- Cumplimiento de la normativa vigente.
- Concienciación de la necesidad de cumplir con la normativa de protección de datos de carácter personal.
- Inspecciones, denuncias y sanciones derivadas del incumplimiento de la normativa de protección de datos.

4.1 Aproximación a la protección de datos en el entorno pyme

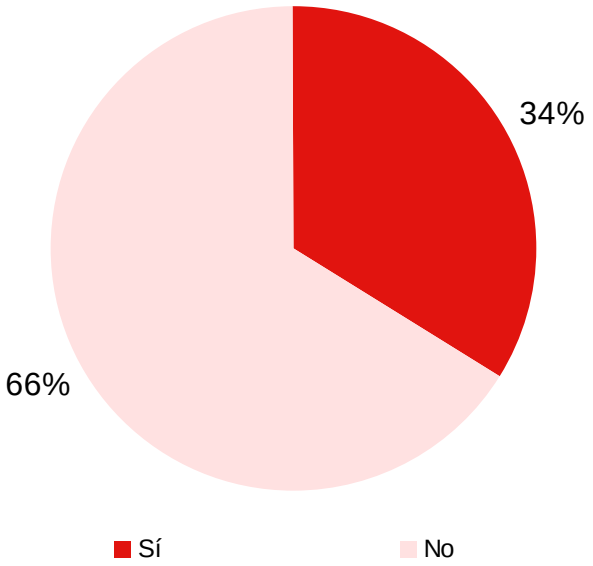
4.1.1 Conocimiento de la normativa sobre protección de datos

Este apartado muestra el nivel de consciencia que tienen las pymes españolas sobre la existencia de una normativa de protección de datos. A los efectos de este estudio, se ha considerado conocimiento como una noción básica de los aspectos que trata tanto la Ley como el Reglamento. El análisis de este punto no determina el nivel de cumplimiento, pero sí es un indicio de cuán extendido y generalizado está el conocimiento de la normativa sobre protección de datos entre las empresas españolas.

El Gráfico 1 recoge el nivel de conocimiento de la LOPD entre las pynes españolas: sólo un 34% declara conocer la existencia de la ley. Apreciaciones cualitativas de las empresas entrevistadas señalan que el conocimiento parte de información ofrecida por asociaciones sectoriales o Cámaras de Comercio, así como por gestorías. Un 66% dice desconocerla por completo, incluso después de haberles aclarado brevemente su origen

e implicaciones. El alto nivel de desconocimiento es síntoma de incumplimiento (parece lógico pensar que, si bien conocer no equivale a cumplir, no conocer sí es indicio de no cumplir), lo que preocupa teniendo en cuenta la fecha de entrada en vigor de la ley (desde 1999), el carácter obligatorio de sus disposiciones y la existencia de sanciones previstas ante su incumplimiento.

Gráfico 1: Empresas que conocen la LOPD (%)

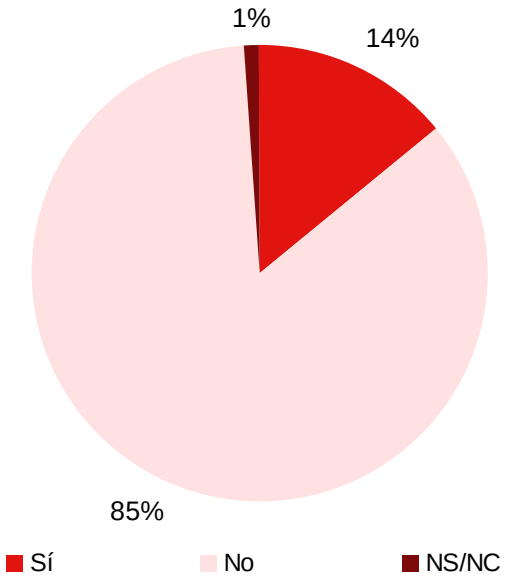


Fuente: INTECO

El Gráfico 2 muestra el nivel de conocimiento de las empresas sobre el RDLOPD, en vigor desde el 19 de abril de 2008: un 14% de las pymes declara conocer el reglamento, mientras que un 85% de los encuestados dice no conocer la existencia ni implicaciones del mismo. Un 1% muestra incertidumbre.

El alto porcentaje de desconocimiento, superior incluso al referido a la LOPD, puede deberse a la reciente entrada en vigor del reglamento, que podría no haber llegado aún a las empresas a través de ningún medio.

Gráfico 2: Empresas que conocen el RDLOPD (%)



Fuente: INTECO

A la vista de los resultados mostrados en los dos primeros gráficos, la conclusión es clara: la pyme española muestra un bajo nivel de conocimiento de la normativa sobre protección de datos, tanto de la LOPD (34%) como del reciente reglamento de desarrollo (14%).

En este punto, se ha considerado conveniente establecer una comparación entre el nivel de conocimiento mostrado por la pyme española (analizado anteriormente) y el declarado por la población española, de un lado, y la empresa europea, de otro. Así, tal y como se recoge en el Barómetro del CIS de febrero de 2008[5], a la pregunta *¿Sabe Ud. si existe alguna ley que proteja la intimidad personal y familiar de los ciudadanos contra los posibles abusos que puedan producirse con sus datos personales?* las respuestas fueron: 52,4% sí existe, 6,2% no existe y 41,0% no sabe (0.4% N.C.). La población española está más concienciada que el colectivo pyme acerca de la existencia de normativa sobre protección de datos.

Por lo que respecta a la empresa europea (no exclusivamente pyme), los datos del Eurobarómetro muestran que el 56% de las empresas declaran ser *"en cierto modo familiares"* con la normativa sobre protección de datos; sólo el 13% indica ser *"muy*

[5] CIS, Barómetro de Febrero de 2008, Estudio nº 2.754. Encuesta de ámbito nacional con una muestra de 2.470 sujetos (población española de ambos sexos de 18 años y más)

familiar"; y un 30% admite "*no ser en absoluto familiar*" con las provisiones de la ley.[6]. También en este caso la conclusión es clara: la pyme española muestra un menor conocimiento sobre la normativa que la empresa europea.

4.1.2 Conocimiento de la clasificación de datos

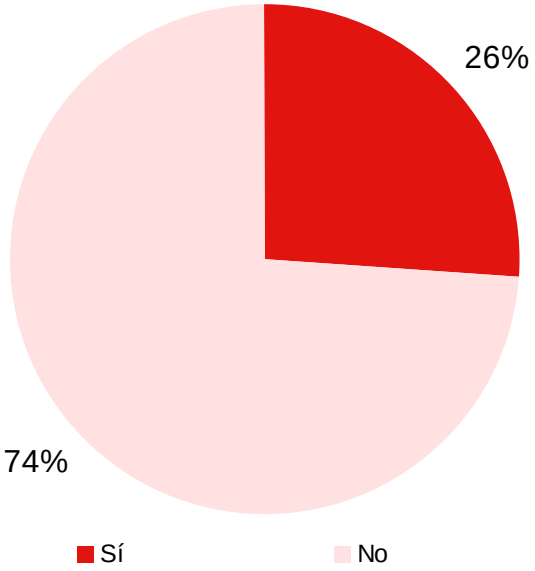
La normativa vigente sobre protección de datos descansa en la diferenciación de los datos y los requisitos de sensibilidad para su nivel de protección. En consecuencia se clasifican los ficheros que los contienen en ficheros de nivel básico, medio y alto. Esta clasificación implica el establecimiento de medidas de seguridad de carácter más o menos exigente en función de la sensibilidad de los datos. En el apartado 4.2.11 se profundiza sobre las características y medidas de seguridad a aplicar para cada uno de los ficheros de nivel básico, medio o alto.

En cualquier caso, se ha considerado que el conocimiento de esta clasificación constituye un síntoma de la concienciación y sensibilización de las PYME sobre la normativa, y por ello se ha incluido su análisis en el presente estudio.

Una cuarta parte de las PYME afirma conocer la clasificación de datos de nivel básico, medio y alto. El nivel de percepción de los encuestados, respecto de la clasificación de los datos de carácter personal es ciertamente bajo, pero coherente con lo esperado a la luz del conocimiento declarado de la normativa.

[6] Eurobarometer Comisión Europea – The Gallup Organization. Data Protection in the European Union. Data controllers' percepciones (February 2008). Encuesta de ámbito europeo realizada a 4.835 controladores de datos de empresas seleccionadas en base a dos criterios: país y número de empleados de la empresa (20-49, 50-249, 250+).

Gráfico 3: Empresas que conocen la clasificación de datos en nivel básico, medio y alto (%)



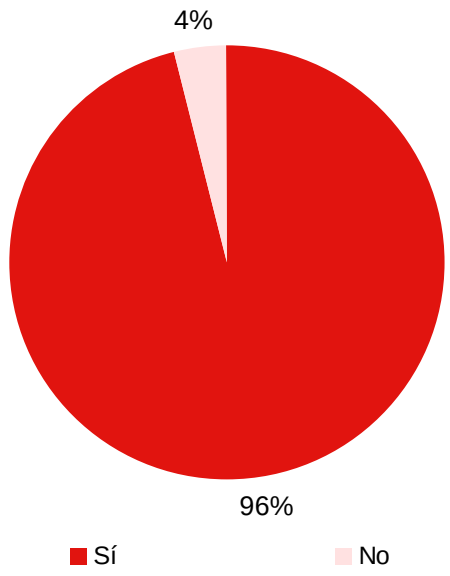
Fuente: INTECO

4.1.3 Existencia de ficheros

Una vez analizados los datos sobre el nivel de conocimiento de la ley y el reglamento, el estudio refleja en este apartado el porcentaje de empresas que manejan ficheros automatizados y/o no automatizados con datos de carácter personal. De esta forma, se ofrece una visión del porcentaje de pymes españolas afectadas (o potencialmente afectadas) por la normativa sobre protección de datos.

El Gráfico 4 muestra que del total de encuestados, el 96% dice tener datos de carácter personal en sus sistemas informáticos y/o en sus archivos de papel, mientras que por otro lado un 4% dice no tener ficheros con datos de carácter personal en ninguna de sus tipologías. Casi la totalidad de las pymes española dispone de ficheros con datos de carácter personal.

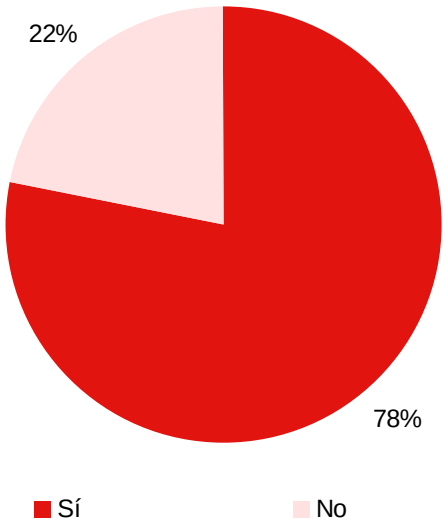
Gráfico 4: Empresas con ficheros automatizados y/o no automatizados que incluyan datos de carácter personal (%)



Fuente: INTECO

En el Gráfico 5 se analiza el nivel de pymes españolas que declaran disponer de ficheros automatizados con datos de carácter personal: un 78% del total de los encuestados trabaja con dichos ficheros.

Gráfico 5: Empresas con ficheros automatizados que incluyan datos de carácter personal (%)

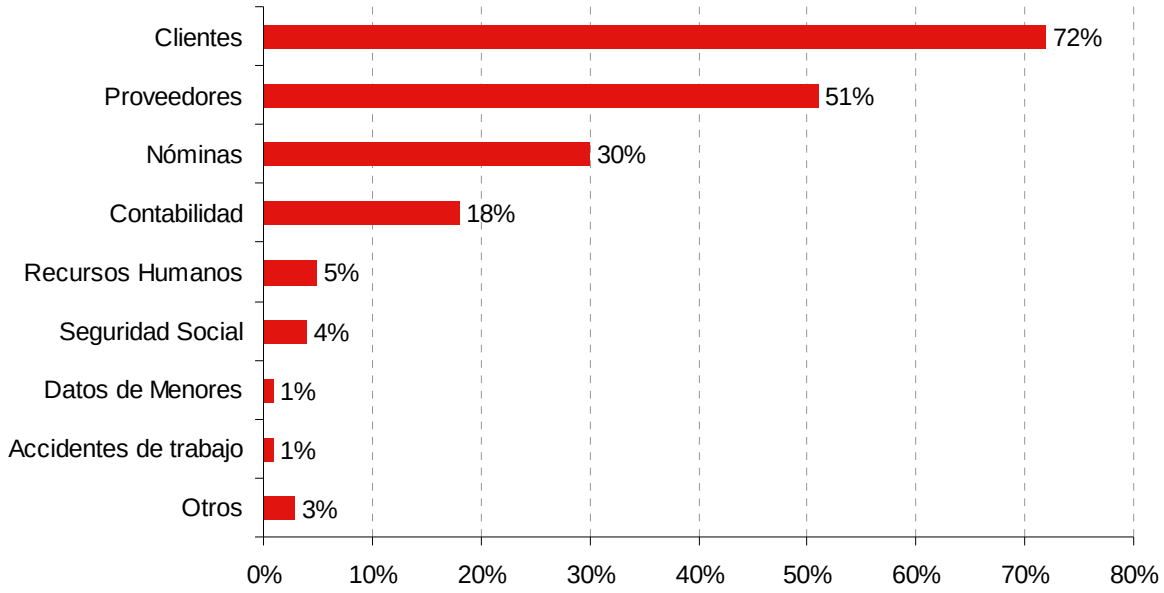


Fuente: INTECO

De la diferencia entre ambos gráficos, se puede concluir que existe un 18% de las pymes españolas que todavía trabaja exclusivamente con ficheros con datos de carácter personal en formato papel.

Se analiza en el Gráfico 6 la tipología de ficheros de los que dispone cada empresa. El tipo de fichero automatizado que más presencia tiene dentro de las empresas es el de clientes (72%), seguido de los ficheros de proveedores (51%) y nóminas (30%). Con mucha menor presencia, las pymes mencionan ficheros de contabilidad, seguridad social, menores, accidentes de trabajo y otros.

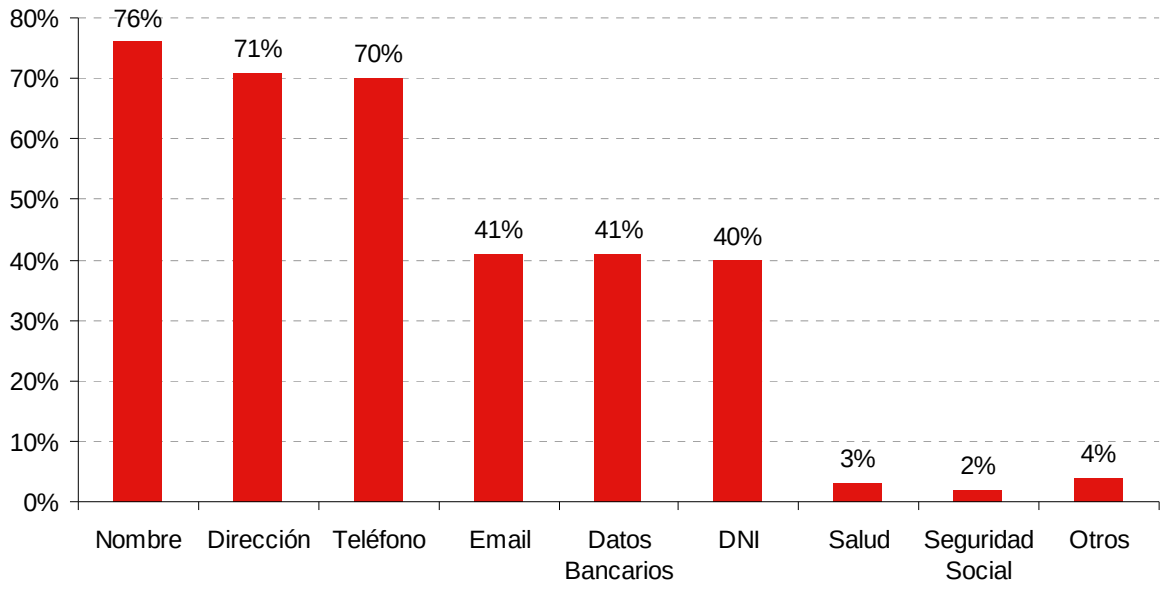
Gráfico 6: Tipología de ficheros automatizados con datos de carácter personal (%)



Fuente: INTECO

Dentro de estos ficheros se manejan datos del tipo: nombre (76%), dirección (71%) y teléfono (70%) así como: e-mail (41%), DNI (40%) y datos bancarios (41%). Se trata, en su mayoría, de datos con un nivel de seguridad básico, a excepción de los datos sobre salud (nivel de seguridad alto).

Gráfico 7: Tipología de datos de carácter personal manejados dentro de los ficheros automatizados (%)



Fuente: INTECO

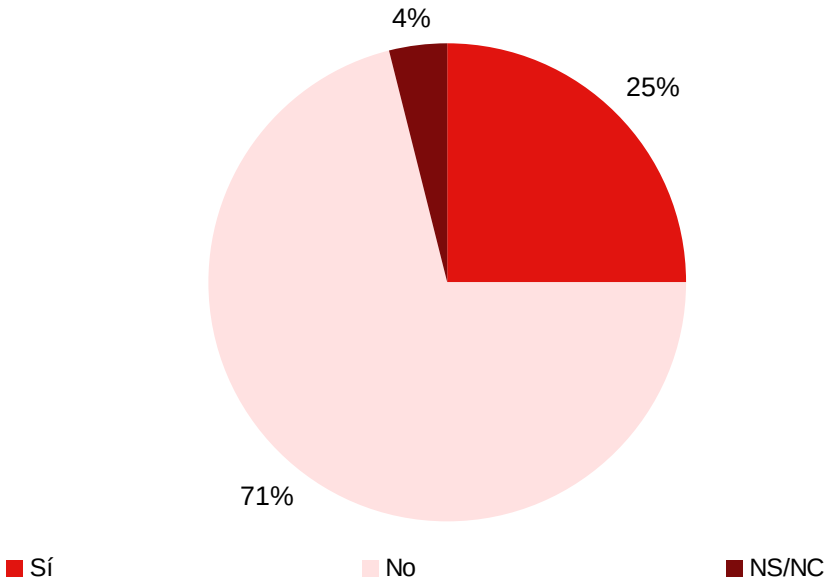
4.1.4 Aplicación de políticas de seguridad

Para el correcto tratamiento de los datos de carácter personal se deben tener en cuenta políticas específicas de seguridad que garanticen la privacidad de los mismos. Ejemplos de estas políticas son el establecimiento de un procedimiento de altas, bajas y modificaciones de usuarios, la realización de copias de seguridad, la gestión de incidentes, la elaboración de controles de acceso, etc. Todas estas políticas se traducen en una serie de procedimientos y controles que forman parte de los requerimientos para adaptarse a la normativa de protección de datos y que son recogidos dentro del RDLOPD como medidas de seguridad. Estas medidas deben estar englobadas dentro de una política que asegure que se cumplan y ser documentadas en el llamado Documento de Seguridad, del que se tratará en el apartado 4.2.10.

En cuanto a la aplicación de estas medidas de seguridad específicas para los datos de carácter personal que deberían tener tanto los ficheros automatizados como no automatizados, los resultados obtenidos se destacan en el Gráfico 8: La cuarta parte de las empresas dice aplicar políticas específicas de seguridad a los datos personales en soporte electrónico y en soporte papel. El resultado es acorde con el nivel de conocimiento de la normativa, considerando que no se ha preguntado por políticas de seguridad en los sistemas de información en general, sino más bien específicos del tratamiento de datos de carácter personal.

Conclusiones de la fase cualitativa muestran que las empresas que afirman tener implantada alguna política de seguridad, consideran que ésta puede consistir, por ejemplo, en tener definido un usuario y contraseña para acceder al equipo informático. El Gráfico 8 muestra, por tanto, el grado en que las pymes tienen la sensación de aplicar normas de seguridad específica a los ficheros con datos personales; el nivel efectivo de implementación de las medidas de seguridad será analizado en el apartado 4.2.11.

Gráfico 8: Aplicación de alguna política o norma de seguridad relativa específicamente a los datos personales en soporte electrónico y en papel (%)



Fuente: INTECO

4.2 Cumplimiento de la normativa vigente

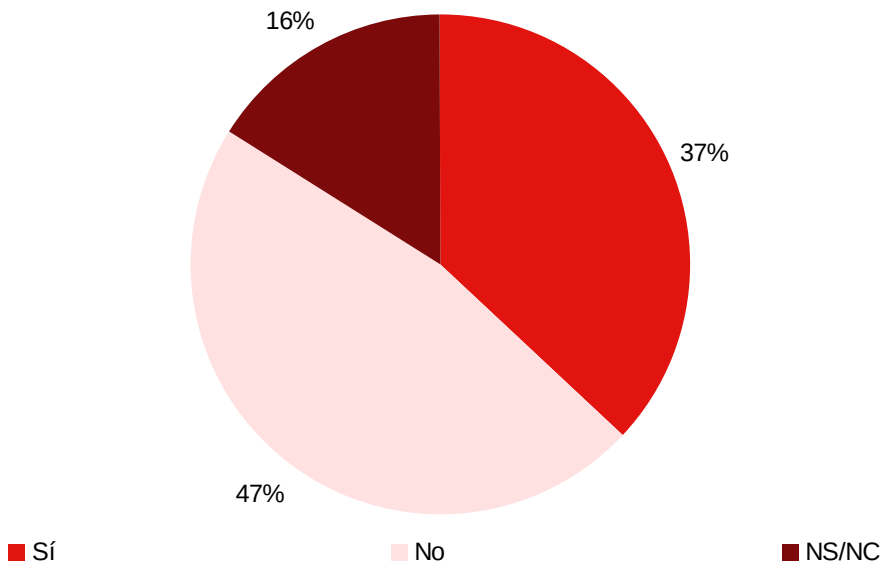
Este apartado muestra el nivel de adaptación de la pyme a las principales obligaciones previstas en la LOPD y el RDLOPD. Para cada una de ellas se explica brevemente en qué consiste la obligación y las implicaciones para la empresa, los artículos de la ley o reglamento donde se recoge, y los datos extraídos de la investigación cuantitativa y/o cualitativa que muestran el grado de cumplimiento por parte de las pymes.

4.2.1 Declaración de los ficheros en la Agencia de Protección de Datos.

La obligación principal y punto de partida para la correcta adecuación y cumplimiento de la normativa de protección de datos es la declaración ante el Registro General de Protección de Datos de todos los ficheros con datos personales susceptibles de tratamiento. Esta obligación viene recogida en el art. 26 de la LOPD y en el Título V, Capítulo II, Art. 55 del RDLOPD; artículos que disponen la forma de notificar e inscribir los ficheros en el registro.

El Gráfico 9 muestra que del total de pymes con ficheros automatizados, el 37% afirma haberlos declarado en el registro de la AEPD, frente a un 47% que confirma que no los ha declarado y un 16% que dice desconocer su situación al respecto. La investigación cualitativa ha permitido profundizar en los motivos para este elevado índice de desconocimiento, mostrando como posible razón el hecho de que la declaración de ficheros, al igual que otros procesos de carácter fiscal o contable, no se realiza directamente por la empresa, sino por un tercero (gestoría, consultora o similar). En cualquier caso, el alto nivel de desconocimiento constituye un indicio de la falta de concienciación con respecto al cumplimiento de la obligación básica de declarar los ficheros ante la AEPD.

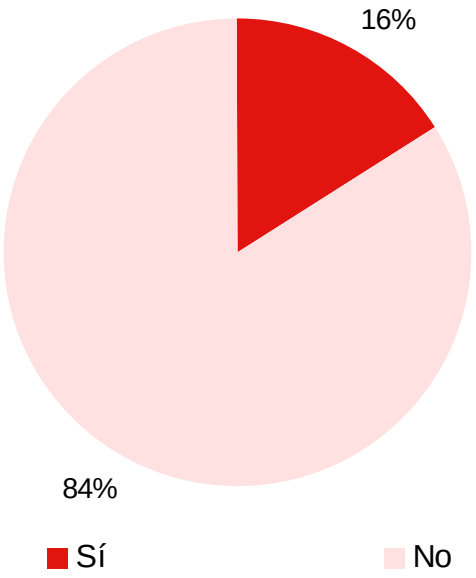
Gráfico 9: Empresas que afirman tener declarados los ficheros con datos de carácter personal en la Agencia de Protección de Datos (%)



Fuente: INTECO

En contraste con las respuestas de los encuestados en materia de declaración de ficheros de carácter personal, y con el objeto de mitigar el posible sesgo de las respuestas de las pymes, se ha verificado a través del portal web de la AEPD www.agpd.es el porcentaje real de aquellas empresas que han declarado sus ficheros con datos de carácter personal: sólo un 16% de las pymes con ficheros automatizados los tienen en realidad declarados, frente al 37% que afirma haberlo realizado.

Gráfico 10: Empresas que efectivamente tienen declarados los ficheros con datos de carácter personal en la Agencia de Protección de Datos (%)



Fuente: INTECO

La diferencia de 21 puntos porcentuales entre percepción (Gráfico 9) y realidad (Gráfico 10) puede deberse a:

- El lapso de tiempo que puede transcurrir entre el inicio de la solicitud de declaración y la fecha efectiva de registro. Podría darse el caso de empresas que han iniciado el proceso de declaración pero éste no se ha completado. No obstante, parece un desfase excesivo (21 puntos porcentuales) para justificar esta postura.

- Una respuesta condicionada del empresario ante un tema delicado: se trata de una pregunta sobre el cumplimiento de una disposición obligatoria prevista en la ley cuyo incumplimiento se puede traducir en una sanción. Es posible que exista cierto sesgo en las respuestas.

- Un desconocimiento de la normativa de protección de datos que puede estar provocando confusión en las respuestas de los encuestados.

El hecho de que un 84% de las empresas encuestadas no tenga declarados sus ficheros ante la AEPD, hace vislumbrar una cifra elevada de incumplimiento para el tejido empresarial más relevante del país.

Las cifras que maneja la Agencia Española de Protección de Datos sobre el porcentaje de pymes que han declarado sus ficheros son coherentes con los datos que se muestran

en el presente estudio; así, según la AEPD, el porcentaje de pymes que tiene sus ficheros declarados se sitúa entre el 10% y el 15%, con un nivel de declaración creciente cada año. La AEPD considera que el colectivo que realiza más inscripciones en la actualidad es el de pymes y micropymes dado que las grandes compañías fueron las primeras en adecuarse a la ley en años anteriores (la LOPD está vigente desde 1999). La evolución de ficheros inscritos es la siguiente:

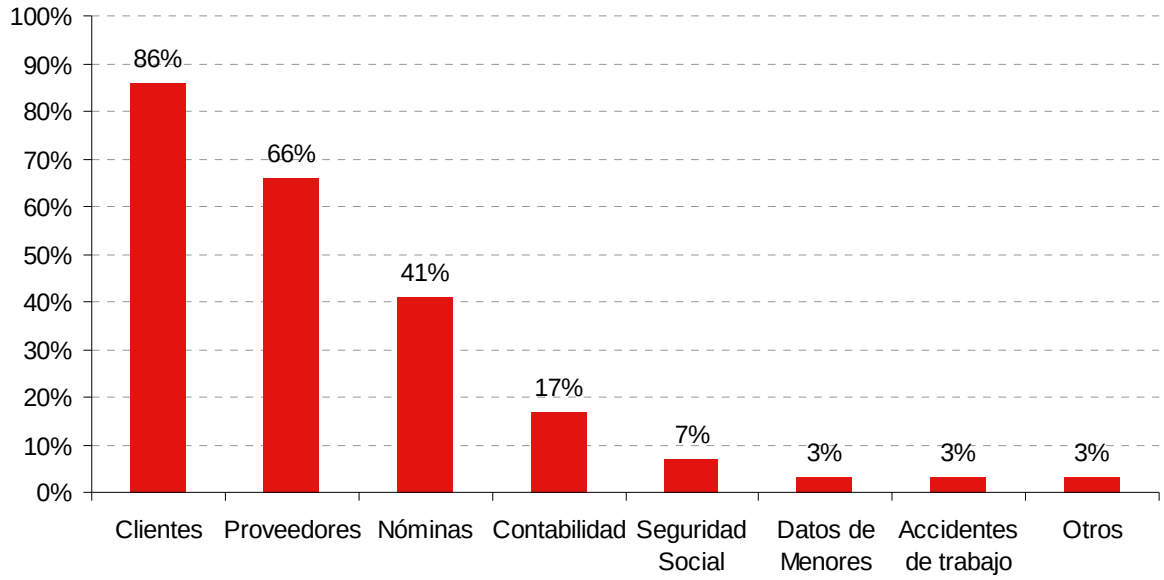
- Año 2000: 220.000 ficheros.
- Año 2006: 760.000 ficheros.
- Año 2007: 1.000.000 ficheros.

Según palabras de Artemi Rallo, Director de la AEPD*:"los resultados del estudio se ajustan bastante a los datos que manejamos en la AEPD. En cuanto al grado de cumplimiento estimamos que en torno a un 10% o un 15% de las pymes están cumpliendo con sus responsabilidades. En la actualidad tenemos inscritos en el Registro General de la Agencia de Protección de Datos un total de 1.085.731 ficheros y contabilizados 427.996 responsables. Son cifras que nos hacen ver con optimismo el futuro pero tenemos que seguir trabajando para que todas las compañías vayan adecuándose y cumpliendo con las obligaciones que establece la LOPD".*

Respecto a la tipología de ficheros declarados, el Gráfico 11 muestra la tipología de ficheros que los encuestados afirman haber declarado ante la AEPD. Los ficheros declarados con más frecuencia son los de clientes (86%), proveedores (66%) y nóminas (41%). Este resultado es consistente con los datos mostrados en el Gráfico 6, donde se analizaba la tipología de ficheros que manejan las pymes, y que mostraban que clientes, proveedores y nóminas son los ficheros que en mayor medida son manejados por las empresas.

Los datos recabados en este gráfico están basados en la percepción de los encuestados sobre el proceso de declaración, lo que puede implicar una desviación con la realidad.

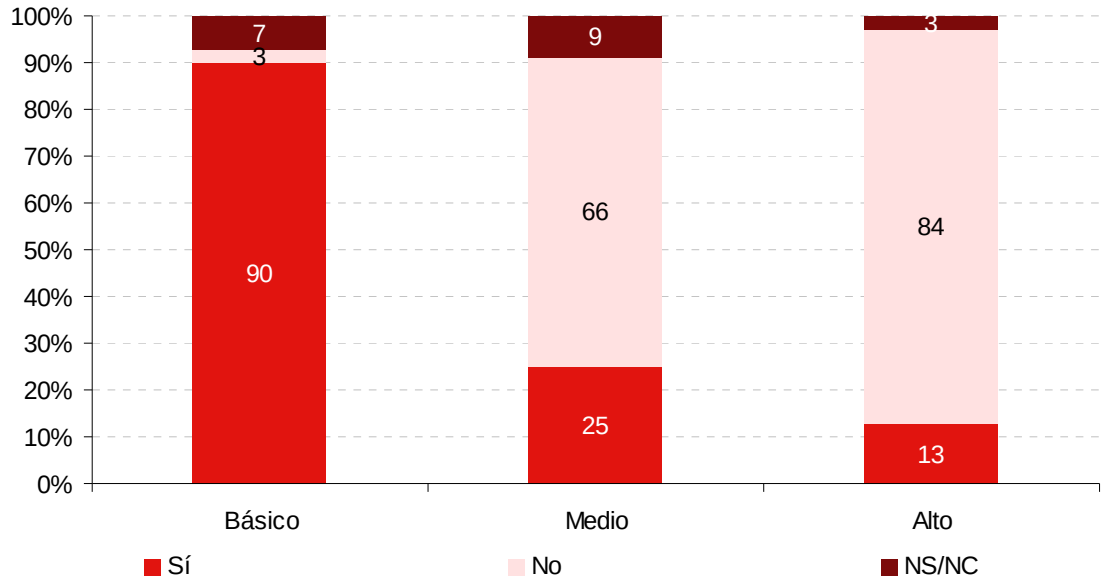
Gráfico 11: Tipología de ficheros declarados por la pyme ante la AEPD (%)



Fuente: INTECO

De las pymes que afirman tener declarados sus ficheros en la AEPD, el 90% dice haber declarado ficheros de nivel básico, un 25% de nivel medio y sólo un 13% ficheros de nivel alto. Estos resultados son consistentes con los mostrados en el Gráfico 7, donde se analizaban los datos personales que se encuentran en los ficheros de las empresas. Recordando las conclusiones de aquel gráfico, los datos más habituales en el entorno PYME son nombre, dirección, teléfono, e-mail, datos bancarios y DNI. Todos ellos son datos de nivel básico. Como se puede apreciar, existe un mínimo porcentaje de empresas que dicen haber declarado ficheros de nivel alto.

Gráfico 12: Nivel de seguridad de los ficheros declarados por las pymes ante la AEPD (%)



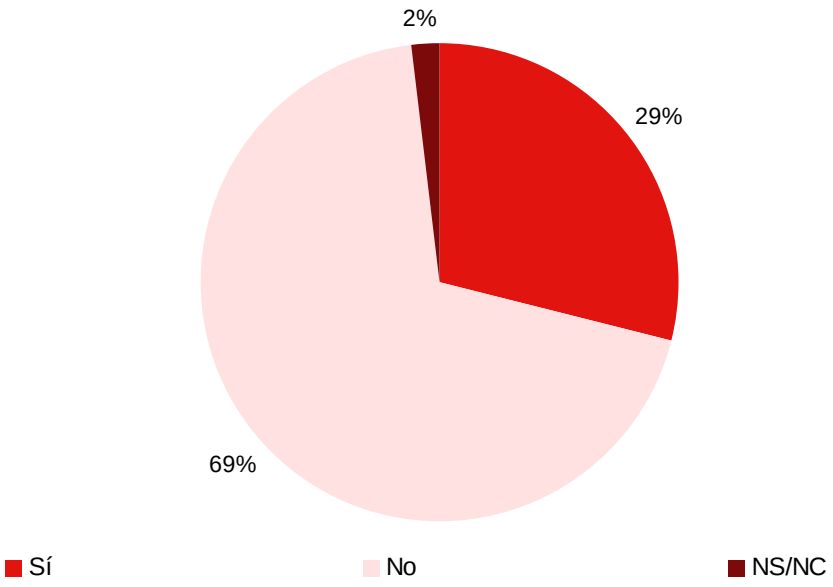
Fuente: INTECO

4.2.2 Información al interesado sobre la recogida de datos.

Cualquier persona tiene derecho a saber si sus datos personales van a ser incluidos en un fichero, y los tratamientos que se realizan con esos datos. La contrapartida de este derecho es la obligación, recogida en el art. 5 de la LOPD, que tienen los responsables de ficheros o tratamientos (las pymes, a los efectos del estudio) de informar a los ciudadanos de la incorporación de sus datos a un fichero, de la identidad y dirección del responsable, de la finalidad del fichero, de los destinatarios de la información, así como de la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.

El nivel de cumplimiento declarado del deber de información entre las pymes españolas que disponen de ficheros automatizados es, tal y como muestra el Gráfico 13, de un 29%.

Gráfico 13: Nivel de cumplimiento por las pymes con ficheros automatizados del deber de información a las personas físicas titulares de los datos (%)



Fuente: INTECO

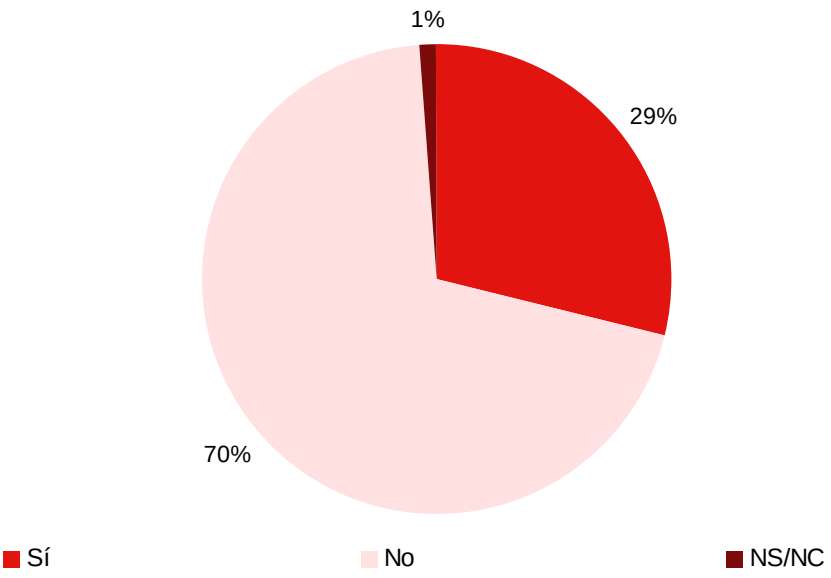
El porcentaje de cumplimiento es bajo, y más de dos terceras partes de las empresas declaran no cumplir con el deber de información a los ciudadanos. Entre los motivos alegados por las pymes para no informar a los titulares de los datos sobre la incorporación a los mismos a un fichero destaca la consideración de innecesario. Así, resultados de la fase cualitativa confirman que está extendida entre las pymes la creencia de dar por hecho que la persona que facilita sus datos de forma voluntaria está asumiendo implícitamente su incorporación a un fichero y uso posterior.

4.2.3 Consentimiento del interesado para el tratamiento de sus datos.

El deber de consentimiento implica la obligación de solicitar el consentimiento explícito de las personas físicas titulares de los datos - antes de la recogida de los mismos - para proceder al tratamiento. El consentimiento se debe establecer mediante un mecanismo claro cuya opción de recogida no esté validada por defecto.

El art. 6 de la LOPD y el capítulo II sección 1ª del RDLOPD establecen la normativa para recabar el consentimiento de los afectados para el tratamiento de sus datos de carácter personal. El Gráfico 14 expone el porcentaje de empresas que solicitan dicho consentimiento de acuerdo a la ley: De forma coherente con las empresas que cumplen el deber de información, poco más de la cuarta parte de las pymes dicen solicitar consentimiento, informando a los titulares de los datos sobre el tratamiento o serie de tratamientos concretos, con delimitación de la finalidad para los que se recaba, así como de las restantes condiciones que concurran en el tratamiento o serie de tratamientos.

Gráfico 14: Nivel de cumplimiento por las pymes con ficheros automatizados del deber de solicitud de consentimiento a las personas físicas titulares de los datos (%)



Fuente: INTECO

Además, con respecto a la recogida del consentimiento del interesado para el tratamiento de sus datos personales, el Artículo 13 del RDLOPD trata una serie de obligaciones y normativas referidas exclusivamente a los datos de menores de edad. La mención que se hace a este tipo de datos es una mejora introducida en el RDLOPD para el tratamiento de dichos datos respecto a la normativa anterior al reglamento.

Como regla general, se prohíbe recabar o tratar datos de menores de catorce años sin el consentimiento de sus padres. Si se trata de mayores de 14 años, podrá procederse al tratamiento de los datos sin necesidad del consentimiento paterno, pero sí con el consentimiento propio, salvo en aquellos casos en los que la ley exija para su prestación la asistencia de los titulares de la patria potestad o tutela.

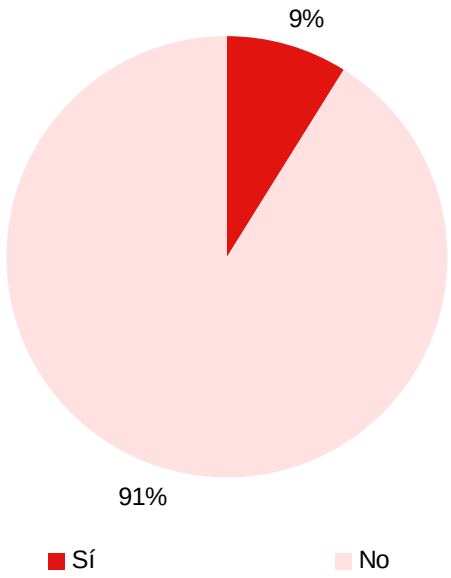
En ningún caso podrán recabarse de los menores datos que permitan obtener información sobre los demás miembros del grupo familiar, o sobre las características del mismo, como los datos relativos a la actividad profesional de los progenitores, información económica, datos sociológicos o cualesquiera otros, sin el consentimiento de los titulares de tales datos. No obstante, podrán recabarse los datos de identidad y dirección del padre, madre o tutor con la única finalidad de recabar la autorización prevista en el apartado anterior.

El Gráfico 15 muestra que un 9% de los encuestados recoge datos de menores de 14 años de edad. En la fase cualitativa, algunas de estas empresas mostraron, por lo general, una correcta recogida de los datos de menores. Estas pymes afirman solicitar la

autorización a los padres, a la vez que se les informa sobre la recogida de los mismos. Aseguran que sin consentimiento expreso y demostrable de los padres (p.e firma, copia DNI), los datos de menores no pueden ser recogidos por aquellas empresas que tratan con este tipo especial de datos.

En conclusión, existe un bajo nivel de empresas españolas afectadas por la obligación, ya que pocas recogen datos de menores de edad, no obstante, las empresas que dicen manejar este tipo de datos demuestran poseer mayor sensibilidad con respecto a la protección de datos.

Gráfico 15: Pymes con ficheros automatizados que recogen datos de menores de edad (%)



Fuente: INTECO

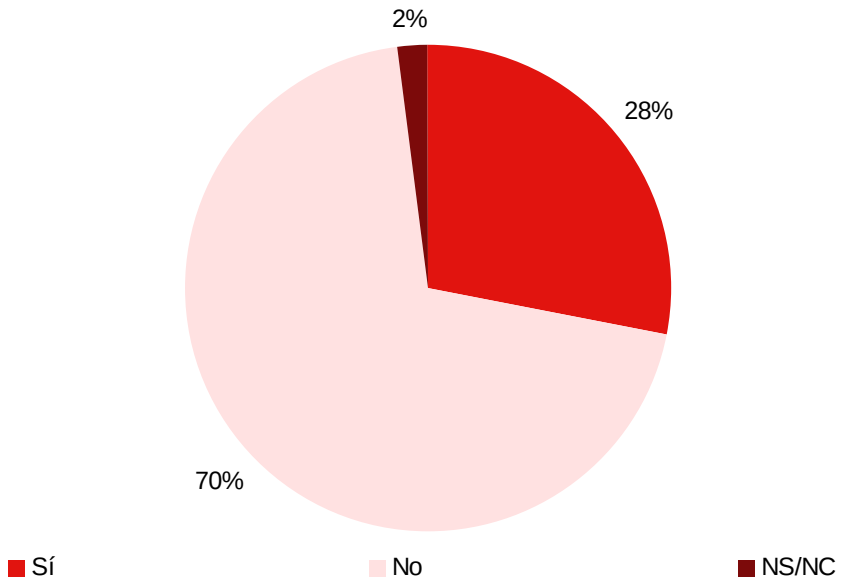
4.2.4 Calidad de los datos.

La normativa de protección de datos exige determinar la calidad de los mismos con el fin de clasificar, reclasificar (si fuese necesario), ordenar y agrupar los datos, ya sea en ficheros automatizados y/o no automatizados. La obligación de disponer de datos siempre actualizados se encuentra detallada en el art. 8 de la LOPD y en el Título II Capítulo I del RDLOPD.

Los datos de carácter personal serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado. Si los datos fueran recogidos directamente del afectado, se considerarán exactos los facilitados por éste.

El Gráfico 16 muestra que un 70% de las empresas con ficheros automatizados no dispone de procedimientos para tener los datos actualizados, ni controles exhaustivos para tenerlos completos y exactos.

Gráfico 16: Pymes con ficheros automatizados que mantienen los datos personales completos y exactos (%)



Fuente: INTECO

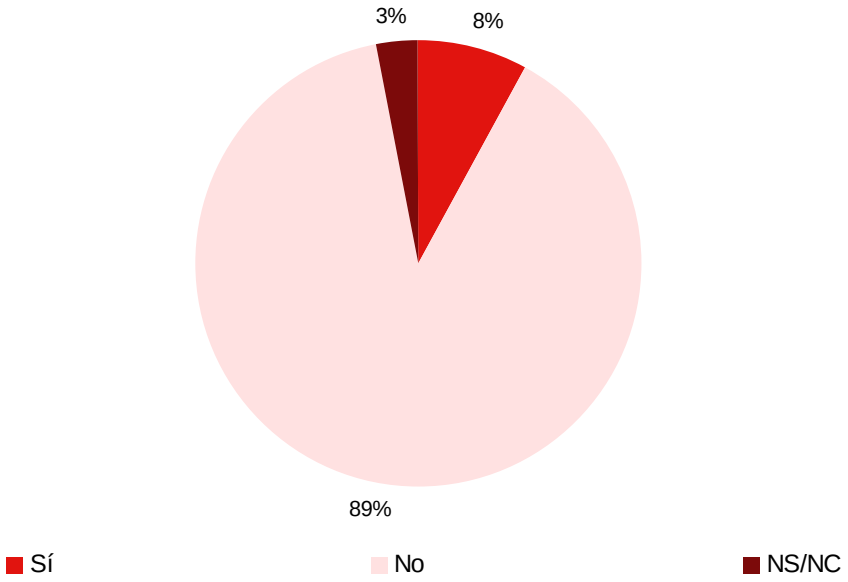
4.2.5 Cesión de datos de carácter personal.

Se entiende por cesión de datos toda revelación de datos realizada a una persona física o jurídica distinta del interesado. Los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario, y bajo el previo consentimiento del interesado. Esta disposición está recogida en el art. 11 de la LOPD y en el Art. 10 del RDLOPD.

El Gráfico 17 ofrece una perspectiva respecto de las cesiones o comunicaciones de datos que los encuestados afirman realizar: la mayoría de los encuestados (89%) no cede datos personales a terceros, mientras que un 8% sí lo hace.

En general, las empresas que afirman realizar cesión de datos a otras empresas han mostrado, en la fase cualitativa, una tendencia a informar a las personas físicas titulares de los datos sobre la finalidad del fichero, la naturaleza de los datos que han sido cedidos así como también el nombre y la dirección del cesionario. Se trata de un comportamiento similar al analizado en el Gráfico 15 referido a las empresas que recogen datos de menores. Parece que las empresas que llevan a cabo actuaciones especiales (recogida de datos de menores, cesión de datos a terceros) muestran una mayor sensibilidad al cumplimiento de la normativa sobre protección de datos.

Gráfico 17: Pymes con ficheros automatizados que ceden datos personales a otras empresas (%)



Fuente: INTECO

4.2.6 Tratamiento de datos cedidos por un tercero.

Es habitual en el entorno pyme que se subcontraten servicios con terceras empresas tales como externalización de gestión de las nóminas, impresión de trabajos en imprentas, procesos fiscales o contables, servicios de mantenimiento informático, etc.

Cuando la pyme subcontrata un servicio con un tercero, se debe valorar si este tercero puede considerarse encargado del tratamiento (tal y como se explicaba en el apartado 3 al analizar los sujetos afectados por las obligaciones). En este sentido, se tiene que garantizar que el encargado de tratamiento realice un tratamiento adecuado de los datos de carácter personal, utilizando los datos únicamente para la finalidad para la cual hayan sido designados y siendo únicamente él responsable de las consecuencias que podrían originarse en caso de destinar los datos a otra finalidad distinta a la inicialmente establecida.

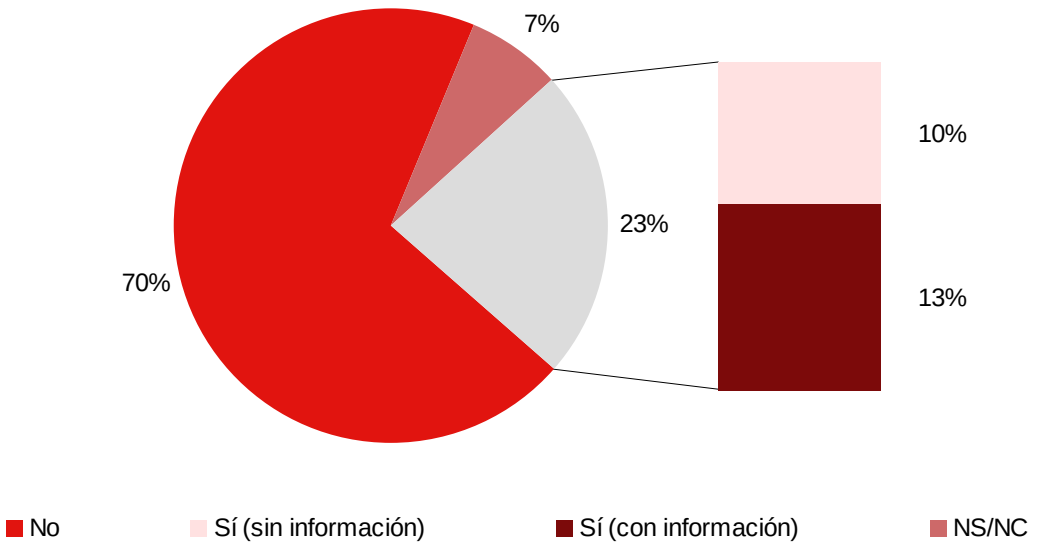
Por otra parte, para el correcto tratamiento de los datos cedidos por un tercero, es necesario informar a la persona física acerca de dónde se obtuvieron los mismos. Por ejemplo, en el caso de que se recojan datos de bases de datos públicas (registro mercantil, páginas blancas, páginas amarillas, etc.). Los artículos 6, 11, 12, y 20 de la LOPD entre otros y los artículos 10, 20, 21, 42, 45, 46 y 47 del RDLOPD entre otros, establecen la normativa en lo que respecta al manejo de datos de carácter personal por un tercero, y de manera específica en el artículo 20 y 21 del RDLOPD en lo concerniente

a las relaciones entre el encargado del tratamiento y el responsable del fichero, (de quien se hablará en el capítulo 4.2.11) si es que lo hubiera.

Esta acción de tratamiento por cuenta de terceros tiene que estar regulada por un contrato donde deberá constar por escrito la acreditación de su celebración y contenido, estableciéndose expresamente que el encargado del tratamiento 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.

El Gráfico 18 muestra el porcentaje de empresas que recaban datos de carácter personal por medio de terceros: un 70% de encuestados dice no recabar datos por medio de terceros. Por el contrario entre el 23% que sí recoge datos personales por medio de terceros, se distingue un 10% que no informa al titular y un 13% que sí informa al titular de esta acción.

Gráfico 18: Pymes que recaban datos de carácter personal por medio de terceros y realizan su posterior declaración de obtención al titular (%)

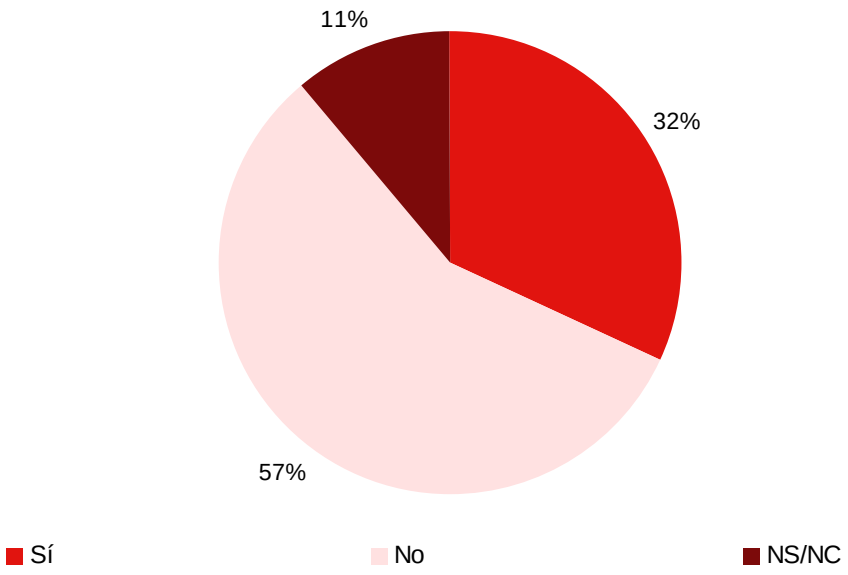


Fuente: INTECO

Continuando en esta línea, se ha identificado el porcentaje de empresas que han añadido en sus contratos de servicios con terceros cláusulas que manifiesten la privacidad y confidencialidad de los datos.

El Gráfico 19 muestra que un 32% de los encuestados incluyen cláusulas de confidencialidad y privacidad de los datos de carácter personal en sus contratos de servicios, mientras que un 57% no incorpora este tipo de cláusulas.

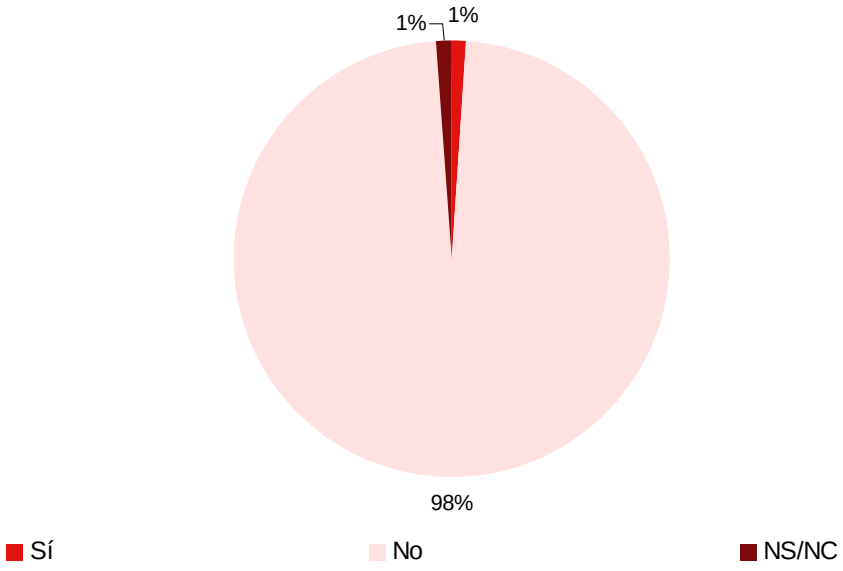
Gráfico 19: Pymes que incluyen en sus contratos escritos el carácter confidencial y privado de los datos (%)



Fuente: INTECO

El Gráfico 20 muestra que un 98% de los encuestados dice no acceder a ficheros con datos de carácter personal de otras empresas para realizar por cuenta de éstas la prestación de servicios, mientras que un 1% consultado sí accede a ficheros de otras empresas.

Gráfico 20: Pymes que acceden a ficheros de carácter personal de otras empresas para la prestación de servicios (%)



Fuente: INTECO

4.2.7 Derechos A.R.C.O.

Uno de los puntos clave de la LOPD viene constituido por los derechos de acceso, rectificación, cancelación y oposición (conocidos como derechos A.R.C.O.), reconocidos a los titulares de los datos. Como contrapartida de estos derechos, que se explicarán a continuación, la ley contempla la obligación del responsable del fichero o tratamiento de atender y facilitar el ejercicio de estos derechos a los titulares de los datos. La forma de exposición de los derechos contempla esta doble vertiente; de un lado se exponen los derechos que la ley concede a los ciudadanos titulares de los datos personales, y de otro, las obligaciones que los responsables del fichero (las pymes, a los efectos del estudio) deben cumplir.

Acceso

Derecho del titular de los datos: en virtud del derecho de acceso, regulado en el art. 15 de la LOPD, el ciudadano puede solicitar y obtener gratuitamente información sobre sus datos de carácter personal sometidos a tratamiento, así como el origen de dichos datos y las comunicaciones realizadas o que se prevean realizar.

Obligación para la pyme: por su parte, el responsable del fichero o tratamiento tiene que resolver la solicitud de acceso en el plazo máximo de un mes a contar desde la fecha en que haya recibido la solicitud. En caso de estimar la solicitud, el acceso debe hacerse efectivo en el plazo de los diez días siguientes a la notificación. La obligación de contestar a la solicitud ha de producirse con independencia de que figuren o no datos

personales del ciudadano en sus ficheros. La contestación al derecho de acceso ha de practicarse utilizando cualquier medio que permita acreditar el envío y la recepción de la misma.

Rectificación

Derecho del titular de los datos: el art. 16 de la LOPD reconoce al ciudadano el 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. La solicitud de rectificación debe indicar el dato que se estima erróneo y la corrección que debe realizarse y debe ir acompañada de la documentación justificativa de la rectificación solicitada.

Obligación para la pyme: El responsable del fichero o tratamiento tiene el deber de atender el derecho de rectificación en el plazo de diez días naturales. Deberá contestar de forma motivada a la solicitud que se le dirija, debiendo utilizar cualquier medio que permita acreditar el envío y la recepción de su respuesta. Asimismo, si los datos rectificados hubieran sido cedidos previamente a un tercero, el responsable del fichero tiene la obligación de notificar al cesionario la rectificación practicada.

Cancelación

Derecho del titular de los datos: este derecho, regulado en el art. 16 de la LOPD, ofrece al ciudadano la posibilidad de dirigirse al responsable para solicitar la cancelación de sus datos personales.

Obligación para la pyme: El responsable del fichero o tratamiento tiene la obligación de hacer efectivo el derecho de cancelación en el plazo de diez días naturales. Deberá contestar de forma motivada a la solicitud que se le dirija, debiendo utilizar cualquier medio que permita acreditar el envío y la recepción de su respuesta. Igualmente, si los datos cancelados hubieran sido cedidos previamente a un tercero, el responsable del fichero deberá notificar al cesionario la cancelación efectuada.

Oposición

Derecho del titular de los datos: el ciudadano puede oponerse, mediante su simple solicitud, a que sus datos sean tratados con fines de publicidad y de prospección comercial. Este derecho de oposición se encuentra regulado en los arts. 6.4, 17 y 30.4 de la LOPD. Se ejercita mediante una solicitud por escrito dirigida al responsable del fichero o tratamiento, en la que se hagan constar los motivos fundados y legítimos relativos a una concreta situación personal del afectado, que justifican el ejercicio de este derecho.

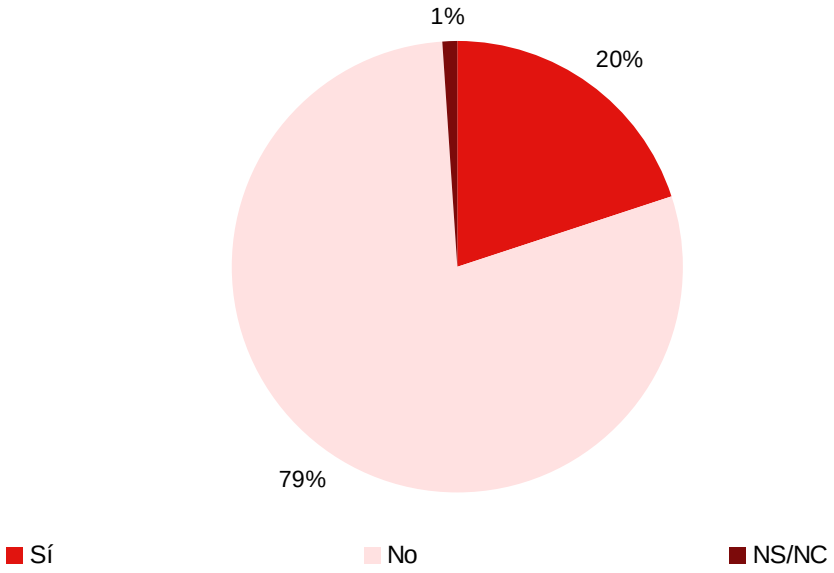
Obligación para la pyme: El responsable del fichero o tratamiento tiene un plazo máximo de un mes a contar desde la recepción de la petición, para resolver la solicitud de oposición. Si transcurrido este plazo no se ha recibido de forma expresa una respuesta a la petición de acceso, ésta puede entenderse desestimada a los efectos de presentar una reclamación de tutela de derechos ante la AEPD. En el caso de que sea procedente acceder a la oposición, el responsable del fichero ha de excluir del tratamiento los datos del ciudadano solicitante. En relación a los tratamientos de datos con fines de publicidad y de prospección comercial, los ciudadanos pueden ejercer el derecho de oposición y, a su simple solicitud, el responsable ha de dar de baja sus datos personales en el tratamiento, cancelando de este modo las informaciones que figuraban en el mismo.

En resumen, existe la obligación para las pymes de establecer algún mecanismo gratuito mediante el cual los afectados puedan ejercitar los derechos de acceso, rectificación, cancelación y oposición. En este sentido, se debe facilitar al interesado un medio sencillo y gratuito para manifestar su negativa al tratamiento de los datos. En particular se destacan los siguientes medios:

- Envío prefranqueado al responsable del tratamiento.
- Llamada a un número telefónico gratuito.
- Servicios de atención al público que se hayan establecido.

El Gráfico 21 muestra que sólo un 20% de las empresas han establecido procedimientos para garantizar el ejercicio de los derechos A.R.C.O. por los particulares.

Gráfico 21: Nivel de cumplimiento por las pymes con ficheros automatizados del deber de establecimiento de procedimientos para que las personas físicas titulares de los datos puedan ejercer los derechos A.R.C.O. (%)



Fuente: INTECO

Los procedimientos mencionados por el 20% que declara haberlos establecido son los siguientes (nótese que en este caso la base es muy pequeña, sólo 39 empresas, por lo que los datos que se muestran a continuación han de ser tomados con cautela):

- E-mail: 28%.
- Correo ordinario: 23%.
- Página web: en un 5%.
- Otros: 44%, incluyendo en algún caso procedimientos verbales no válidos, lo que podría suponer un indicio de que el nivel real de cumplimiento de la obligación de disponer de un procedimiento que permita a los interesados ejercitar los derechos A.R.C.O. es inferior al 20%.

En la fase de investigación cualitativa se profundizó en los casos de pymes con procedimientos para garantizar el ejercicio de los derechos A.R.C.O. a los ciudadanos y se detectó que, en general, estos procedimientos no suelen estar definidos documentalmente, y se suelen gestionar con un importante margen de improvisación.

El reducido nivel de adaptación a este punto muestra, una vez más, un limitado cumplimiento de la normativa sobre protección de datos entre la pyme española. En el caso particular de los derechos A.R.C.O., además, puede constituir motivo de denuncia.

Así, el ciudadano al que le haya sido denegado el ejercicio de los derechos de acceso, rectificación, cancelación u oposición, puede ponerlo en conocimiento de la AEPD para que ésta verifique la procedencia o improcedencia de la denegación, pudiendo dar lugar los hechos constatados a la iniciación de procedimientos sancionadores.

Comparando la realidad de la empresa con la de la sociedad en general, es relevante apuntar los datos del CIS correspondientes al Barómetro de febrero de 2008, donde se muestra sólo un 22,1% de la población española ha solicitado en alguna ocasión que borren o cancelen sus datos personales de algún registro (mediante el teléfono, Internet o correo). El 76,1% nunca lo ha solicitado. Además, el 52,7% de los que han cancelado alguna vez sus datos lo encontraron difícil o muy difícil[7].

Según el Eurobarómetro[8] casi la mitad de los entrevistados responsables de la protección de datos en su empresa (46%) indicaron que su compañía había recibido solicitudes de acceso a los datos personales durante el último año. Algo menos de cuatro de cada 10 encuestados (37%) informaron de que su empresa no recibió ninguna solicitud de acceso en el mismo período. Respecto a los que recibieron solicitudes (un total del 46%): el 28% declaró haber recibido menos de diez y un 12% entre diez y cincuenta solicitudes. Sólo el 6% de los entrevistados respondió que su empresa había recibido más de 50 solicitudes durante el último año.

La misma fuente ofrece los datos para España, que muestra un 44% de empresas que nunca han recibido una solicitud de acceso, un 24% de empresas que han recibido menos de 10 solicitudes, un 13% entre 10 y 50 y sólo un 6% que ha recibido más de 50 solicitudes.

Estos datos, si bien reflejan una realidad no idéntica a la mostrada en este estudio (la muestra del Eurobarómetro reúne a empresas de más de 20 empleados, mientras que aquí se analizan empresas de hasta 50, con un peso importante de las empresas sin asalariados y entre 1 y 9 empleados), muestran una todavía relativa penetración de la práctica de acceder a los datos personales por parte de la población europea. En buena lógica, cabe esperar que la creciente solicitud de acceso por parte de la población empujará a las empresas a establecer procedimientos en este sentido.

[7] CIS, Barómetro de Febrero de 2008, Estudio nº 2.754. Encuesta de ámbito nacional con una muestra de 2.470 sujetos (población española de ambos sexos de 18 años y más)

[8] Eurobarometer Comisión Europea – The Gallup Organization. Data Protection in the European Union. Data controllers' percepciones (February 2008). Encuesta de ámbito europeo realizada a 4.835 controladores de datos de empresas seleccionadas en base a dos criterios: país y número de empleados de la empresa (20-49, 50-249, 250+).

4.2.8 Gestión del tratamiento de datos de carácter personal en transferencias internacionales.

En las transferencias internacionales de datos de carácter personal se debe garantizar una protección equiparable a la que existe en territorio español. Los títulos V de la LOPD y VI del RDLOPD establecen la normativa para el tratamiento en estos casos. La obligación de la pyme que trate con datos personales en transferencias internacionales es trasladar a la empresa del país de destino la necesidad de proporcionar un nivel de protección equiparable al que presta la LOPD.

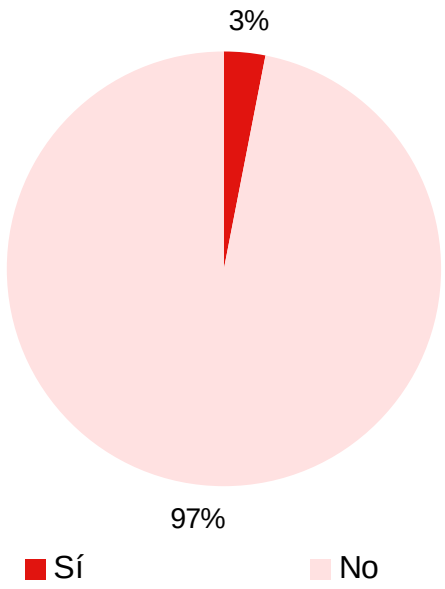
Si la comunicación de datos es a la Unión Europea o a un país considerado con un nivel adecuado de protección la empresa deberá:

- Notificarlo a la Agencia Española de Protección de Datos.
- Informar al afectado del destinatario de sus datos y de la finalidad para la cual se están cediendo los mismos. Igualmente, deberá obtener su consentimiento para realizar la transferencia.

Si la comunicación de datos es a un país considerado con un nivel no adecuado de protección deberá, además, solicitar la autorización del Director de la Agencia de Protección de Datos.

El Gráfico 22 muestra que un 97% de encuestados no realiza transferencias internacionales de datos de carácter personal. Las pymes tienen menor actividad internacional que las grandes empresas, y por tanto el dato es a priori coherente.

Gráfico 22: Pymes con ficheros automatizados que realizan transferencias internacionales de datos de carácter personal (%)



Fuente: INTECO

Comparando el dato con la realidad europea, el Eurobarómetro[9] muestra que el 10% de las empresas europeas realizan transferencias de datos personales a países externos a la Unión Europea, frente al 89% que no lo hacen. La realidad española, en base a la misma fuente, refleja un 7% de empresas que afirman realizar transferencias internacionales y un 93% que declaran no hacerlo. Estos datos se han extraído sobre una muestra de empresas de más de 20 empleados; parece lógico pensar que la diferencia de tamaño influye en el comportamiento internacional de las empresas, y por tanto justifica los 4 puntos porcentuales de diferencia entre los datos del presente informe y los ofrecidos por la Comisión Europea en el Eurobarómetro.

4.2.9 Tratamiento de datos de carácter personal con fines de publicidad y prospección comercial.

Merece especial atención el tratamiento de la publicidad y prospección comercial dentro de la ley, dado que históricamente han existido en España casos de sanción por este motivo.

Las sanciones mencionadas han tenido su origen en acciones promocionales realizadas por las empresas, a través de medios tradicionales (envío por correo, llamadas de teléfono) o electrónicos (e-mail), sin recabar el consentimiento previo al interesado para

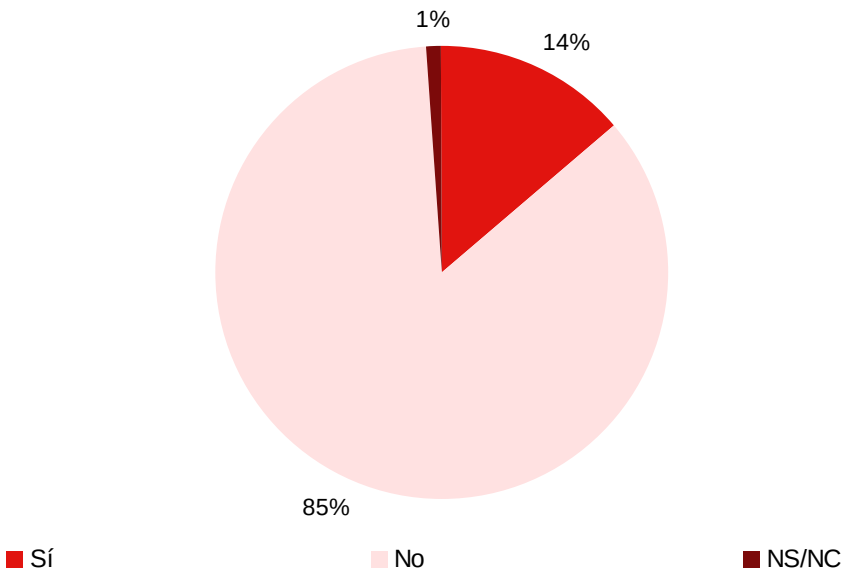
[9] Data Protection in the European Union – Data controllers' perception (European Commission – The Gallup Organization). Eurobarometer Febrero 2008. Muestra: empresas europeas de +20 empleados.

que sus datos formen parte de este proceso, y sin informarles de la posibilidad de que éste pueda ejercer sus derechos.

La LOPD obliga al establecimiento de mecanismos para ejercer los derechos de acceso y oposición de los interesados y su consentimiento para tratar sus datos. Dicho tratamiento y su cumplimiento se encuentran en el Art.30 de la LOPD.

.El Gráfico 23 muestra que un 14% de los encuestados dice realizar envíos promocionales por algún medio utilizando los datos personales de los que dispone, mientras que un 85% dice no hacerlo.

Gráfico 23: Pymes con ficheros automatizados que realizan envíos promocionales utilizando datos de carácter personal (%)



Fuente: INTECO

4.2.10 Documento de seguridad

El documento de seguridad recoge las medidas técnicas y organizativas de obligado cumplimiento para el personal con acceso a los sistemas de información (es decir, electrónicos y papel).

El responsable del fichero deberá elaborar e implantar la normativa de seguridad mediante un documento de seguridad de obligado cumplimiento para el personal. El documento deberá contener, atendiendo a la naturaleza de los datos, las medidas de índole técnica y organizativa necesaria que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, tal y como se establece en el título VII. Capítulo II, Art. 88 del RDLOPD.

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

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

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

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

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

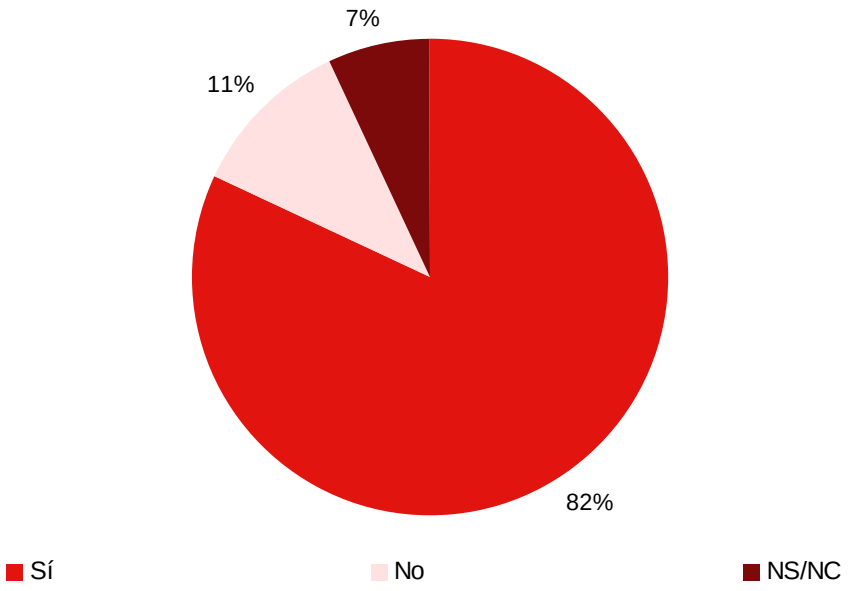
5) Procedimiento de notificación, gestión y respuesta ante las incidencias.

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

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

El Gráfico 24 ofrece la visión respecto de la existencia de documento de seguridad entre las pymes: sólo un 11% de las empresas que afirman haber registrado sus ficheros ante la AEPD no cuenta con documento de seguridad. Un alto porcentaje, el 82%, afirma tener un documento de seguridad. Parece, a primera vista, un resultado positivo; sin embargo es necesario puntualizar que los resultados se refieren sólo a las empresas que afirman haber registrado sus ficheros ante la Agencia, y no al total de pymes españolas. Es lógico pensar que las empresas suficientemente sensibilizadas como para registrar sus ficheros ante la AEPD también lo estén para elaborar un documento de seguridad (no se debe olvidar que ambos preceptos, inscripción y elaboración del documento, son obligatorios).

Gráfico 24: Pymes con ficheros declarados ante la AEPD que tienen un documento de seguridad (%)



Fuente: INTECO

4.2.11 Medidas de seguridad

En los siguientes apartados se detalla el nivel de cumplimiento de las pymes respecto a las medidas de seguridad previstas en el reglamento. Con el objetivo de facilitar la comprensión se incluye un cuadro resumen que muestra las medidas a implantar en función del nivel declarado (básico, medio o alto), y a la tipología de ficheros (soporte electrónico o papel).

Es importante aclarar las definiciones siguientes:

- Datos de nivel básico: nombre, apellidos, dirección, teléfono, e-mail, y cualquier otro dato que no sea de nivel medio o alto.

- Datos de nivel medio: comisión de infracciones penales, comisión de infracciones administrativas, información de Hacienda Pública, información de servicios financieros, datos de Seguridad Social, datos de mutuas, elaboración de perfiles (curricula), datos de tráfico y localización (telecomunicaciones).

- Datos de nivel alto: ideología, religión, creencias, origen racial, salud, vida sexual, afiliaciones sindicales, violencia de género.

Para cada una de las medidas de seguridad analizadas en los apartados sucesivos se realiza una breve descripción de las implicaciones de la medida para la empresa y un análisis estadístico del nivel efectivo de implementación entre las pymes españolas, en

base a resultados de la investigación cuantitativa. Nótese, en este punto, que las estadísticas están construidas sobre las empresas que han notificado sus ficheros a la AEPD. En los casos en que las medidas aplican exclusivamente a ficheros de nivel medio o alto las estadísticas se han elaborado a partir de las pymes que han notificado este tipo de ficheros, lo que hace que en ocasiones las bases consideradas sean reducidas, y por tanto las interpretaciones y conclusiones deben ser realizados con precaución.

Tabla 4: Medidas de seguridad obligatorias a implantar en los diferentes niveles de ficheros

Nivel básico	Nivel medio	Nivel alto
Responsable de seguridad		
	- El responsable del fichero tiene que designar a uno o varios responsables de seguridad (no es una delegación de responsabilidad). - El responsable de seguridad es el encargado de coordinar y controlar las medidas del documento	
Personal		
- Funciones y obligaciones de los diferentes usuarios o de los perfiles de usuarios claramente definidas y documentadas. - Definición de las funciones de control y las autorizaciones delegadas por el responsable - Difusión entre el personal, de las normas que les afecten y de las consecuencias por incumplimiento.		
Incidencias		
- Registro de incidencias: tipo, momento de su detección, persona que la notifica, efectos y medidas correctoras - Procedimiento de notificación y gestión de las incidencias	**Sólo ficheros automatizados** - Anotar los procedimientos de recuperación, persona que lo ejecuta, datos restaurados, y en su caso, datos grabados manualmente. - Autorización del responsable del fichero para la recuperación de datos.	

Nivel básico	Nivel medio	Nivel alto
Control de acceso		
- Relación actualizada de usuarios y accesos autorizados. - Control de accesos permitidos a cada usuario según las funciones asignadas. - Mecanismos que eviten el acceso a datos o recursos con derechos distintos de los autorizados. - Concesión de permisos de acceso sólo por personal autorizado. - Mismas condiciones para personal ajeno con acceso a los recursos de datos.	**Sólo ficheros automatizados** - Control de acceso físico a los locales donde se encuentren ubicados los sistemas de información.	**Sólo ficheros automatizados** - Registro de accesos: usuario, hora, fichero, tipo de acceso, autorizado o denegado. - Revisión mensual del registro por el responsable de seguridad - Conservación 2 años. - No es necesario este registro si el responsable del fichero es una persona física y es el único usuario **Sólo ficheros no automatizados** - Control de accesos autorizados - Identificación accesos para documentos accesibles por múltiples usuarios
Identificación y autenticación		
Sólo ficheros automatizados - Identificación y autenticación personalizada - Procedimiento de asignación y distribución de contraseñas - Almacenamiento ininteligible de las contraseñas - Periodicidad del cambio de contraseñas (>1 año)	**Sólo ficheros automatizados** - Limite de intentos reiterados de acceso no autorizado	
Gestión de soportes		
- Inventario de soportes - Identificación del tipo de información que contienen, o sistema de etiquetado - Acceso restringido al lugar de almacenamiento - Autorización de las salidas de soportes (incluidas a través de e-mail) - Medidas para el transporte y el desecho de soportes	**Sólo ficheros automatizados** - Registro de entrada y salida de soportes: documento o soporte, fecha, emisor/destinatario, número, tipo de información, forma de envío, responsable autorizada para recepción/entrega.	**Sólo ficheros automatizados** - Sistema de etiquetado confidencial - Cifrado de datos en la distribución de soportes. - Cifrado de información en dispositivos portátiles fuera de las instalaciones (evitar el uso de dispositivos que no permitan cifrado, o adoptar medidas alternativas)

Nivel básico		
	Nivel medio	
		Nivel alto
Copias de respaldo		
Sólo ficheros automatizados - Copia de respaldo semanal - Procedimientos de generación de copias de respaldo y recuperación de datos. - Verificación semestral de los procedimientos. - Reconstrucción de los datos a partir de la última copia. Grabación manual en su caso, si existe documentación que lo permita. - Pruebas con datos reales. Copia de seguridad y aplicación del nivel de seguridad correspondiente.		**Sólo ficheros automatizados** - Copia de respaldo y procedimientos de recuperación en lugar diferente del que se encuentren los equipos.
Criterios de archivo		
Sólo ficheros no automatizados - El archivo de los documentos debe realizarse según criterios que faciliten su consulta y localización para garantizar el ejercicio de los derechos ARCO		
Almacenamiento		
Sólo ficheros no automatizados - Dispositivos de almacenamiento dotados de mecanismos que obstaculicen su apertura		**Sólo ficheros no automatizados** - Armarios, archivadores e documentos en áreas con acceso protegido con puertas con llave.
Custodia de soportes		
Sólo ficheros no automatizados - Durante la revisión o tramitación de los documentos, la persona a cargo de los mismos debe ser diligente y custodiarla para evitar accesos no autorizados		

Nivel básico		
	Nivel medio	
		Nivel alto
Copia o reproducción		
		Sólo ficheros no automatizados - Sólo puede realizarse por los usuarios autorizados - Destrucción de copias desechadas
Auditoría		
	- Al menos cada dos años, interna o externa. - Debe realizarse ante modificaciones sustanciales en los sistemas de información con repercusiones en seguridad. - Verificación y control de la adecuación de las medidas. - Informe de detección de deficiencias y propuestas correctoras. - Análisis del responsable de seguridad y conclusiones al responsable del fichero	
Telecomunicaciones		
		Sólo ficheros automatizados - Transmisión de datos a través de redes electrónicas cifrada.
Traslado de documentación		
		Sólo ficheros no automatizados - Medidas que impidan el acceso o manipulación

Fuente: INTECO en base a información de la AEPD (Guía de Seguridad, abril 2008)

Responsable de Seguridad

Una de las medidas que se deben adoptar cuando se tienen datos personales de nivel medio o superior es la de asignar un responsable de seguridad. El art. 95 del RDLOPD recoge esta obligación.

En el documento de seguridad deberán designarse uno o varios responsables de seguridad encargados de coordinar y controlar las medidas definidas en el mismo. Esta designación puede ser única para todos los ficheros o tratamientos de datos de carácter personal o diferenciada según los sistemas de tratamiento utilizados, circunstancia que deberá hacerse constar claramente en el documento de seguridad.

Para distinguir las figuras de responsables y encargados se ofrece a continuación un repaso de sus responsabilidades:

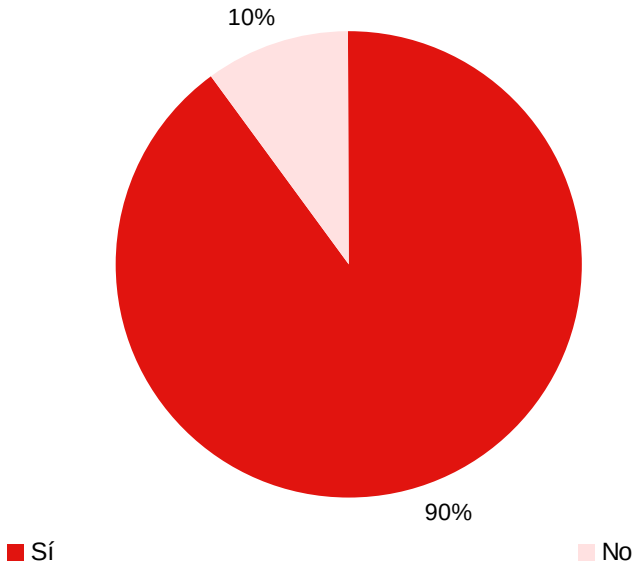
- Responsable de seguridad: Persona o personas a las que el responsable del fichero ha asignado formalmente la función de coordinar y controlar las medidas de seguridad. Su función es proteger y salvaguardar la información sensible dentro de la empresa.

- Responsable del fichero o responsable del tratamiento: Persona que decide sobre la finalidad, contenido y uso del tratamiento. El responsable del fichero o tratamiento es la persona jurídica o física, privada o pública, que decide sobre el tratamiento de los datos, es decir, toma decisiones sobre qué hacer con los mismos. Es el responsable durante toda la vida del dato, desde que entra a formar parte del sistema de información hasta la eliminación del mismo.

- Encargado del tratamiento: Persona jurídica o física, privada o pública, que accede a datos de la empresa a la que se le está prestando un determinado servicio. Es decir la persona que trate datos personales por cuenta del responsable del fichero o responsable de tratamiento.

Un 90% de las empresas que manifiestan haber declarado ficheros de nivel medio dice tener un responsable de seguridad asignado. El índice de cumplimiento es muy alto, pero ha de tenerse en cuenta que la base de análisis está constituida por las empresas que han notificado ficheros de nivel medio.

Gráfico 25: Pymes con ficheros de nivel medio declarados ante la AEPD que han designado un responsable de seguridad (%)



Fuente: INTECO

Divulgación de la normativa de seguridad al personal

El responsable del fichero o tratamiento, ya se trate de ficheros de nivel básico, medio o alto, debe adoptar las medidas necesarias para que el personal conozca las normas de seguridad que afecten al desarrollo de sus funciones, así como las consecuencias en que pudiera incurrir en caso de incumplimiento. La obligación de esta divulgación se encuentra recogida en el art. 89.2 del RDLOPD.

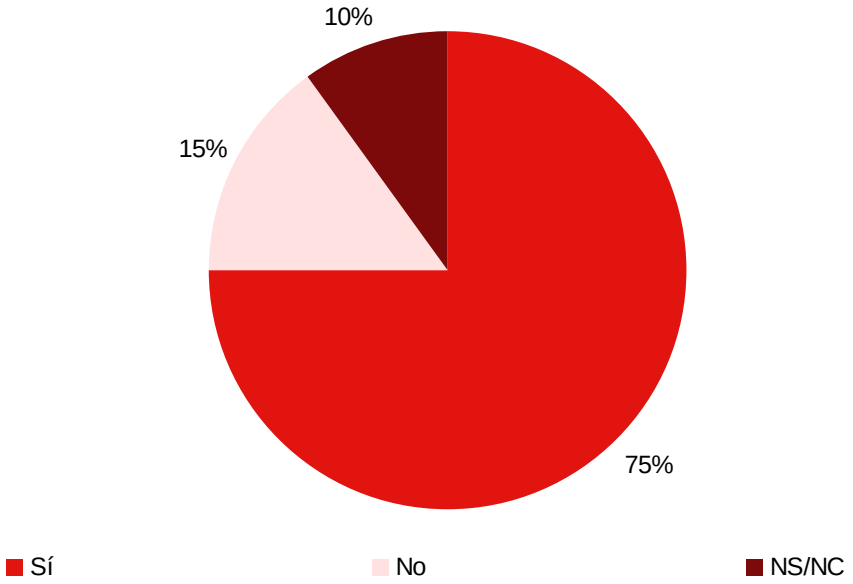
Entre las normas de seguridad más significativas del personal de la empresa se destacan las siguientes:

- Guardar secreto profesional sobre todos los datos de carácter personal que trate la compañía (p.e. firmando una cláusula de confidencialidad en el contrato).
- Cambiar la contraseña de acceso con la periodicidad establecida.
- No escribir o guardar referencia de los datos de la contraseña de acceso al sistema de información (p.e. no apuntar la contraseña en un papel).
- No dejar información visible en la pantalla del ordenador cuando se abandone el puesto (p.e. bloquear la pantalla cuando no se esté en el puesto de trabajo).

El Gráfico 26 muestra en qué medida se han divulgado las normas de seguridad al personal de la empresa. Así, tres cuartas partes de las pymes que afirman haber

declarado sus ficheros ante la AEPD confirman además haber divulgado las normas de seguridad al personal de la empresa.

Gráfico 26: Pymes con ficheros declarados ante la AEPD que han divulgado normas de seguridad entre sus empleados (%)

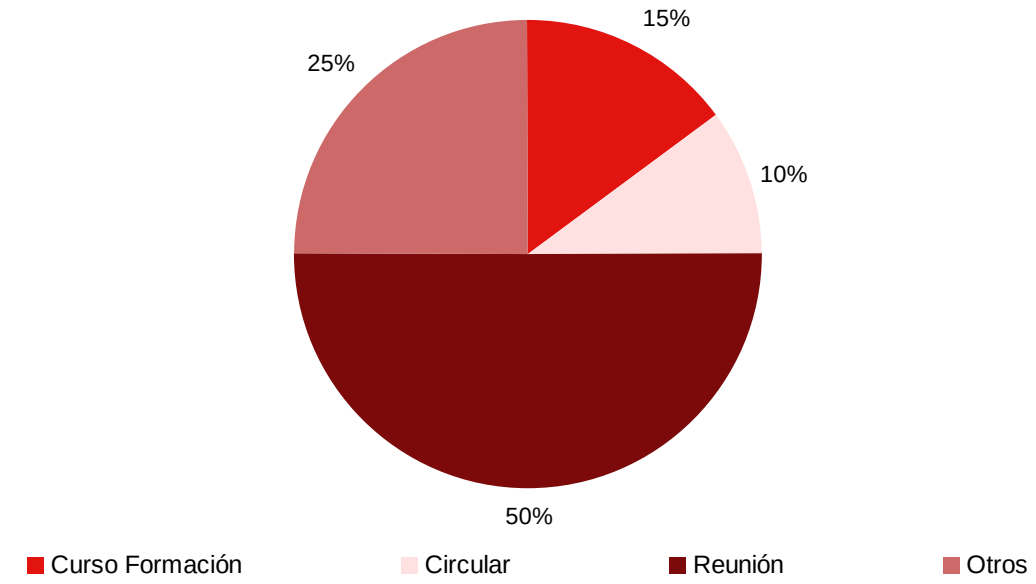


Fuente: INTECO

Respecto al modo empleado para la difusión de la normativa de seguridad, el Gráfico 27 muestra las formas más habituales:

- En una reunión en el 50% de los casos.
- Mediante curso de formación, en un 15%.
- A través de una circular (carta, e-mail, memorando…), en un 10%.
- Otros medios, en un 25% de las ocasiones.

Gráfico 27: Formas de divulgación de las normas de seguridad (%)



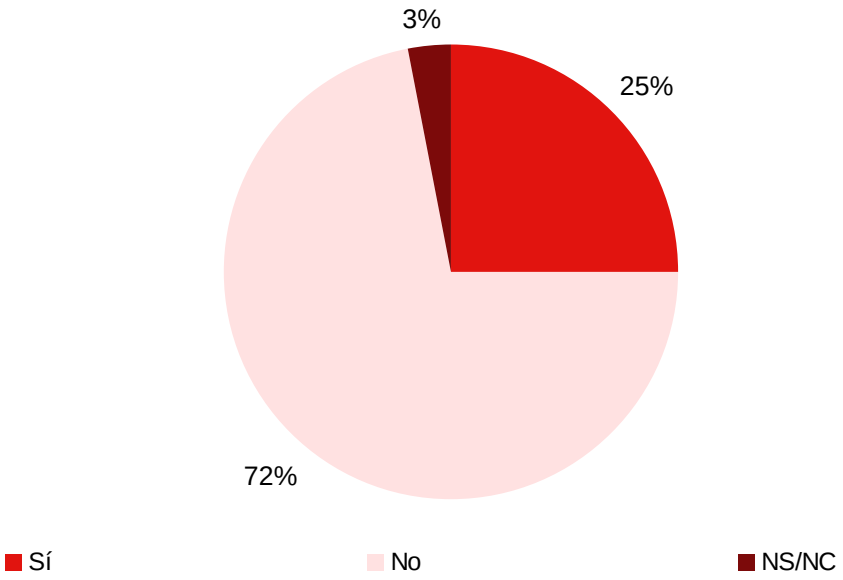
Fuente: INTECO

Registro de incidencias

El registro de incidencias permite disponer de un control completo, exacto y detallado de cualquier incidencia 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 ejecutar en caso de ocurrir dichas incidencias. Esta obligación se encuentra recogida en los artículos 90 y 100 del RDLOPD.

La pyme debe crear un procedimiento de notificación y gestión de las incidencias que afecten a los datos de carácter personal y establecer un registro en el que se haga constar el tipo de incidencia, el momento en que se ha producido, la persona que realiza la notificación, a quién se le comunica, los efectos que se hubieran derivado de la misma y las medidas correctivas aplicadas. Esta obligación afecta a las empresas con ficheros de nivel básico, medio y alto. De las empresas que afirman haber declarado sus ficheros ante la AEPD, sólo un 25% dispone de un registro de incidencias. Obsérvese que el nivel de cumplimiento de esta medida es muy inferior al resto de medidas de nivel básico analizadas hasta ahora: un 82% dispone de documento de seguridad, y un 72% han divulgado la normativa de seguridad entre sus empleados. En todos los casos, el porcentaje está calculado sobre las empresas que afirman tener sus ficheros registrados.

Gráfico 28: Pymes con ficheros declarados ante la AEPD que tienen registro de incidencias (%)



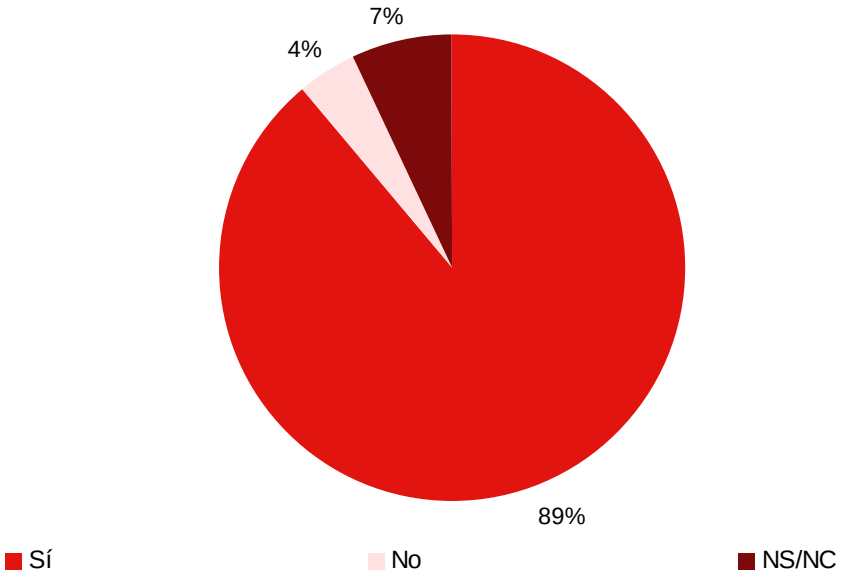
Fuente: INTECO

Control de acceso

Según el artículo 5 del RDLOPD, un acceso autorizado es una autorización concedida a un usuario para la utilización de los recursos. En cada caso, se incluirán las autorizaciones o funciones que tenga atribuidas cada usuario por delegación del responsable del fichero o tratamiento o del responsable de seguridad. Esta autorización se construye mediante una definición de privilegios de acceso, que atribuyen permisos de lectura, escritura, etc, sobre los ficheros asignados a cada persona y los accesos mínimos que requiera para cumplimiento de sus funciones. El art. 91 del RDLOPD recoge esta obligación, que afecta a todo tipo de ficheros (nivel básico, medio y alto).

El Gráfico 29 muestra el nivel de control de accesos a los ficheros digitales en el que las pymes españolas se encuentran: un 89% de las empresas con ficheros registrados dice tener un procedimiento de control de acceso a los ordenadores que contienen datos de carácter personal. Un 4% de los encuestados no tiene definido el acceso mediante ningún procedimiento y un 7% ns/nc.

Gráfico 29: Pymes con ficheros declarados ante la AEPD que han establecido un control de acceso a los ficheros digitales con datos de carácter personal (%)

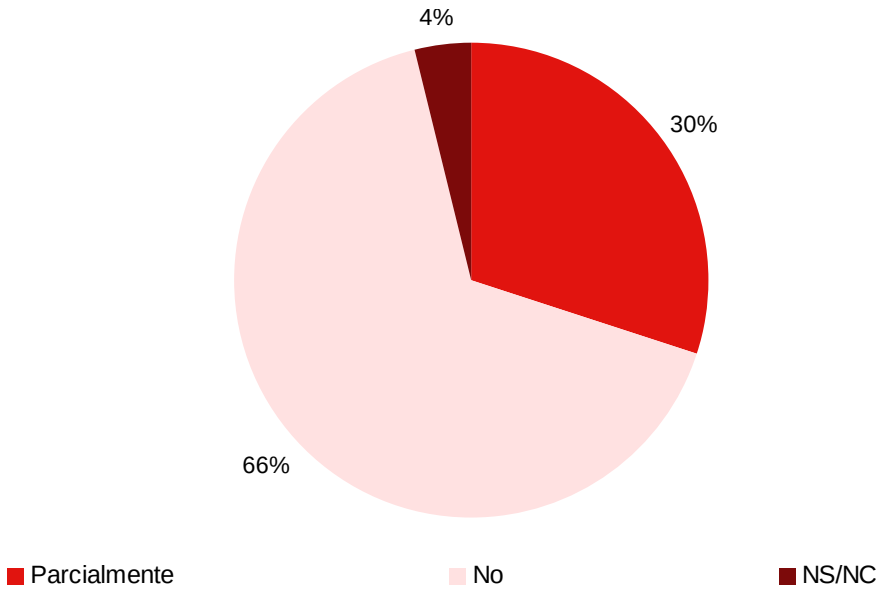


Fuente: INTECO

Con el fin de garantizar que los datos de carácter personal de nivel medio se encuentren protegidos contra cualquier amenaza medioambiental, de robo o pérdida de información, el art. 99 del RDLOPD plantea la obligación para limitar el acceso físico al lugar por parte de personal no autorizado al lugar donde se encuentren los sistemas de información y los datos. En este sentido, exclusivamente el personal autorizado para ello en el documento de seguridad podrá conceder, alterar o anular el acceso autorizado sobre los recursos, conforme a los criterios establecidos por el responsable del fichero.

El 30% de las empresas con ficheros registrados cuentan con medidas de seguridad física para los sistemas de información, frente al 66% que no las han implementado. Entre las medidas más frecuentemente declaradas se encuentran los sistemas contra incendios y el cierre con llave de los despachos donde se encuentran los archivos. También se han identificado mecanismos físicos de seguridad que no son suficientes (por ejemplo, la propia puerta de entrada a la empresa cerrada bajo llave).

Gráfico 30: Pymes con ficheros declarados ante la AEPD que cuentan con medidas de seguridad física para los sistemas de información (%)

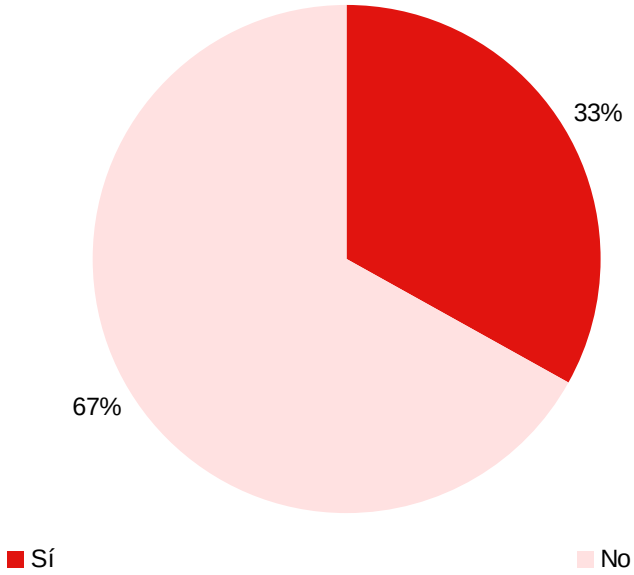


Fuente: INTECO

La normativa exige que, para los ficheros de nivel alto, además de implantar los controles adecuados, se registren los intentos de acceso y los accesos autorizados a las instalaciones donde se almacenan datos de carácter personal. Dicha obligación está recogida en el art. 103 del RDLOPD.

El Gráfico 31 muestra el porcentaje de empresas que han registrado ficheros de nivel medio que disponen de un registro para el acceso a estos ficheros: un 33% dice tener implantado dicho registro, mientras que un 67% no dispone de él.

Gráfico 31: Porcentaje de empresas que han declarado ficheros de nivel medio ante la AEPD que disponen de seguridad física en las instalaciones donde se almacenan ficheros automatizados (%)

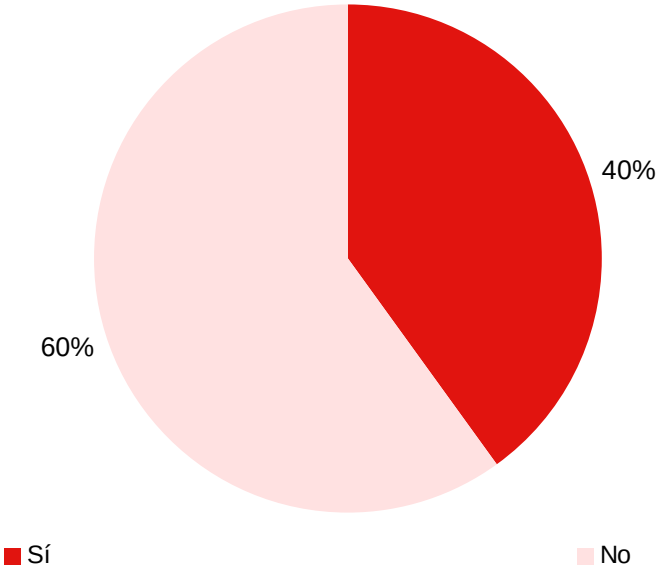


Fuente: INTECO

Además de los controles que se deben tener en cuenta para los sistemas de información que contengan datos de carácter personal, la normativa de protección de datos recoge obligaciones específicas para la documentación en papel que contenga datos personales. Dichas obligaciones están recogidas en los art.107, 108 y 113 del RDLOPD.

El Gráfico 32 muestra el porcentaje de empresas que cuentan con mecanismos para asegurar que sólo el personal autorizado pueda consultar los documentos con datos personales: un 40% afirma disponer de algún mecanismo de este tipo, frente a un 60% que dice lo contrario.

Gráfico 32: Pymes con mecanismos para asegurar que sólo el personal autorizado pueda consultar la documentación con datos de carácter personal (%)



Fuente: INTECO

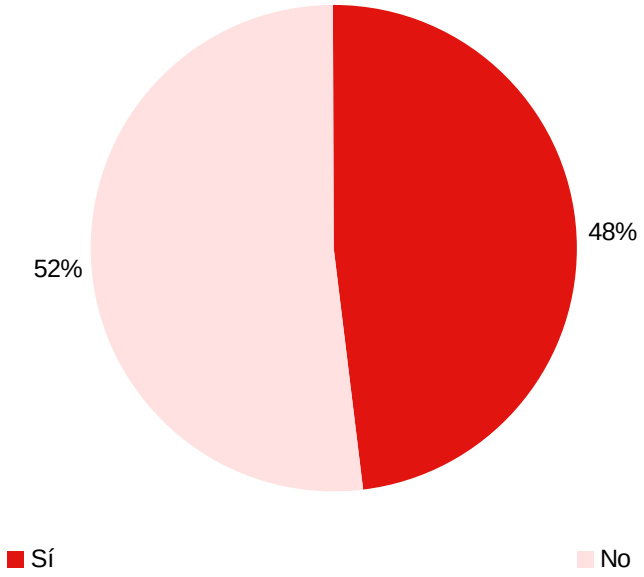
Como última reflexión, se podría decir que, dadas las características de la pyme, resultaría complicado y costoso establecer un nivel robusto de seguridad física en general, ya que estas empresas no cuentan, en la mayoría de los casos, con un espacio de trabajo que puedan aislar físicamente para destinar de forma exclusiva a los sistemas de información.

Identificación y Autenticación

La identificación es el procedimiento por el cual un usuario es reconocido dentro del sistema de información que trata con datos de carácter personal (nombre del usuario), mientras que la autenticación es el procedimiento de comprobación de la identidad en el sistema (la contraseña de acceso asociada al nombre de usuario). Esta obligación se encuentra recogida en el art. 93 del RDLOPD.

El 48% de las empresas con ficheros registrados controlan el acceso a ficheros automatizados con datos de carácter personal basándose en usuario y contraseña, frente al 52% que no lo hace. Cabe destacar que, en general, y basándose en los resultados de las entrevistas de la fase cualitativa, es habitual la implementación de la seguridad basada en un usuario y *password* en las empresas, principalmente debido a que los sistemas operativos implementan esta configuración por defecto. No obstante, no ocurre lo mismo en el caso de establecimiento de privilegios y permisos entre los diferentes usuarios que acceden al sistema.

Gráfico 33: Pymes con ficheros declarados ante la AEPD que controlan el acceso a los ficheros automatizados con datos de carácter personal basándose en usuario y contraseña (%)

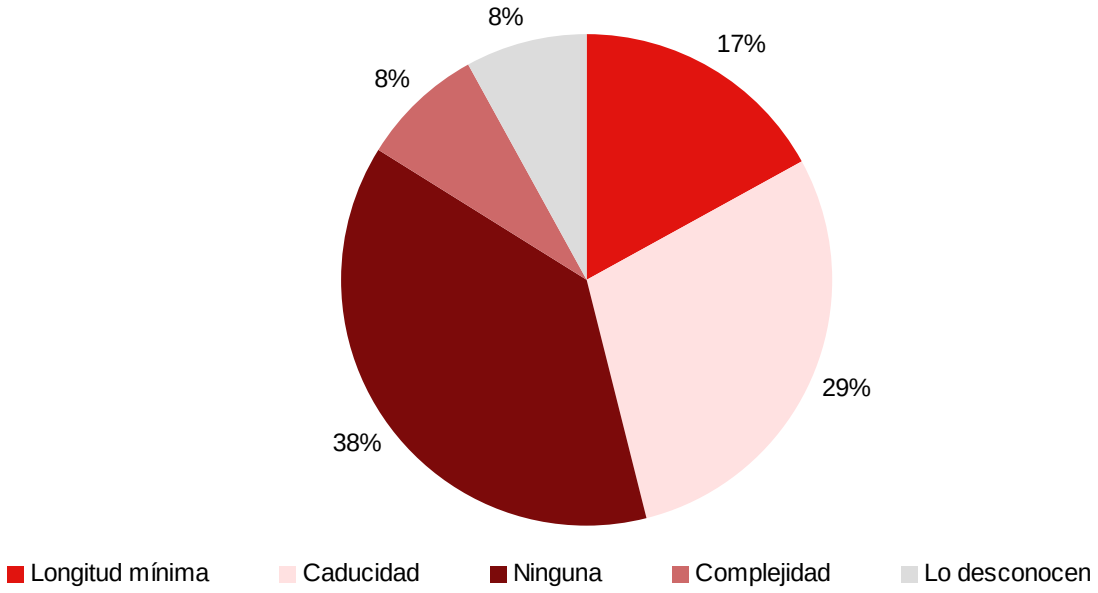


Fuente: INTECO

Por lo que respecta a las características de la contraseña, en los casos en que se utiliza, éstas se muestran en el Gráfico 34:

- Contraseña con fecha de caducidad, que obliga a renovarla periódicamente (29%).
- Contraseña a la que se exige una longitud mínima (17%).
- Contraseña con algún mecanismo que implica complejidad en la misma (por ejemplo, exigencia de combinar mayúsculas, minúsculas y caracteres alfanuméricos) (8%).
- Lo más frecuente, en cualquier caso, es no utilizar ningún mecanismo especial de seguridad en las contraseñas (38%).

Gráfico 34: Características de la contraseña utilizada para el control de acceso a los ficheros que contienen datos de carácter personal (%)



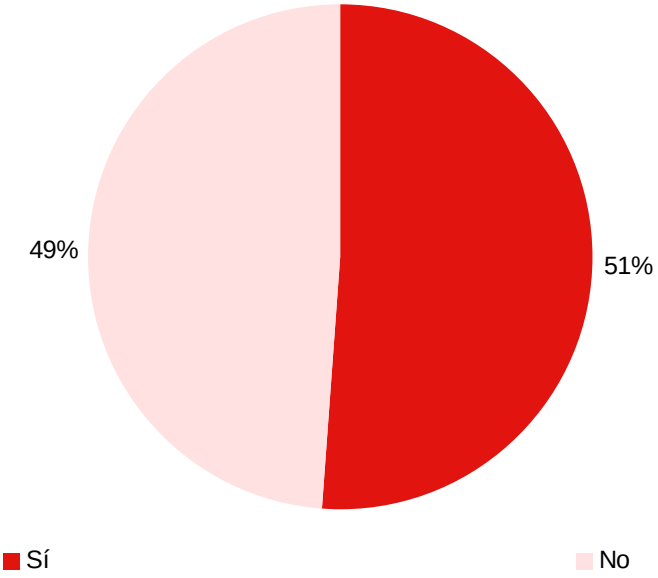
Fuente: INTECO

Gestión de Soportes

Con el fin de preservar y asegurar la información durante su transporte y manipulación, y en particular los datos de carácter personal, la normativa exige tener dicha información protegida mediante la gestión de los soportes que los contienen o almacenan. Esta información puede almacenarse en cualquier soporte electrónico (CDs, cintas magnéticas, memorias, discos duros externos, etc) o papel. Para su correcta manipulación, los art. 92, 97, 101 RDLOPD recogen las obligaciones en relación con la gestión de soportes.

Se ha preguntado a las pymes que han declarado datos de nivel medio acerca de si se ha hecho una valoración interna en materia de tratamiento y destrucción de los soportes electrónicos que contienen datos de carácter personal. El Gráfico 35 muestra que un 51% de ellas dice haber valorado internamente el tratamiento de soportes electrónicos (CD,s, DVD,s, Cintas, Discos duros, etc) y tenerlo procedimentado, mientras que un 49% dice no haber valorado dichos procedimientos.

Gráfico 35: Porcentaje de empresas que tienen definido y procedimentado el tratamiento de los soportes electrónicos que contienen datos de carácter personal (%)



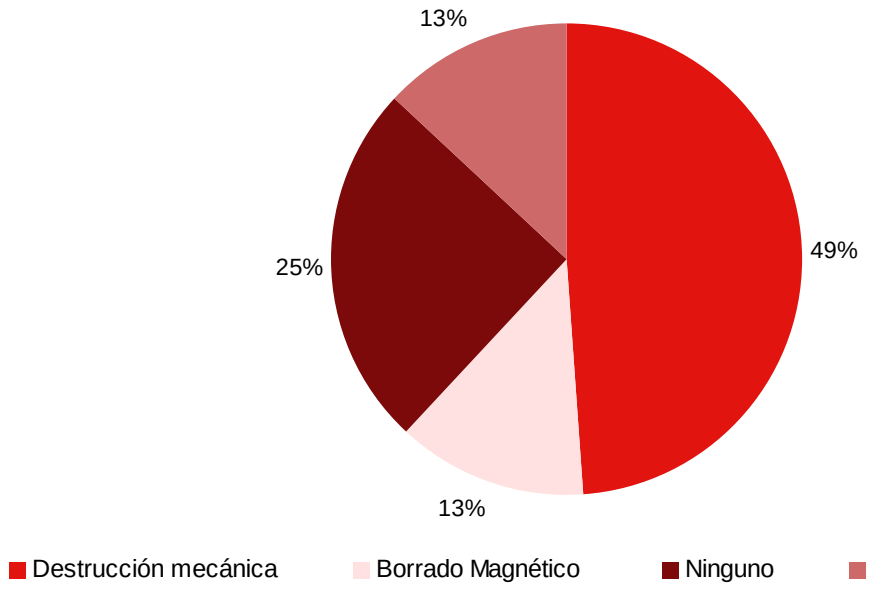
Fuente: INTECO

Del total de los encuestados que respondieron tener definido y procedimentado el tratamiento de los soportes electrónicos con datos de carácter personal (51%), el Gráfico 36 muestra que:

- La destrucción mecánica es el método más recurrente (49%), seguida del borrado magnético (13%) y la destrucción manual (13%).
- Un 25% de los encuestados dice no destruir los soportes electrónicos que almacenan datos de carácter personal.

La obligación para el tratamiento de los soportes y documentos se encuentra recogida en el art. 92.4 del RDLOPD. Siempre que vaya a desecharse cualquier documento electrónico o soporte que contenga datos de carácter personal deberá procederse a su destrucción o borrado, mediante la adopción de medidas dirigidas a evitar el acceso a la información contenida en el mismo o su recuperación posterior.

Gráfico 36: Métodos de destrucción de los soportes electrónicos que almacenan datos de carácter personal (%)

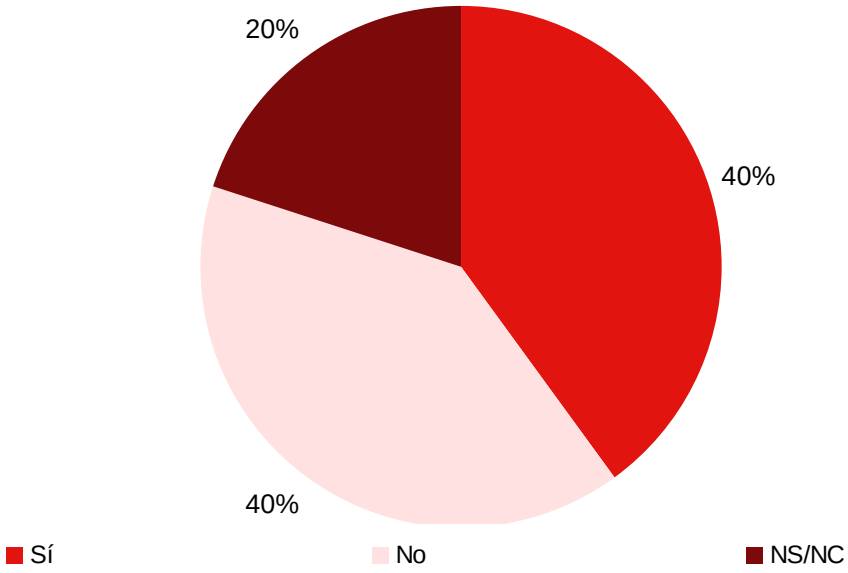


Fuente: INTECO

Continuando con las obligaciones en materia de soportes y documentación de datos personales, la normativa exige que para los ficheros declarados de nivel medio exista un registro de entrada y salida de soportes que contengan datos de carácter personal. La obligación recogida en el art. 97 del RDLOPD es la de controlar y establecer responsabilidades a la hora de manejar los soportes. En dicho registro se podrá conocer: el tipo de soporte, la fecha y hora, el emisor, el número de soportes incluidos en el envío, el tipo de información que contienen, la forma de envío y la persona responsable de la recepción que deberá estar debidamente autorizada.

El Gráfico 37 muestra que un 40% de las empresas que han declarado ficheros de nivel medio disponen de este registro, frente al 40% que declaran no tenerlo. Una quinta parte de las empresas desconocen la situación en cuanto a si se utiliza o no este tipo de registros.

Gráfico 37: Pymes con ficheros de nivel medio declarados ante la AEPD que han adoptado el registro de entrada/salida de soportes digitales que contienen datos de carácter personal (%)



Fuente: INTECO

Dentro de las medidas de seguridad que la normativa exige para los ficheros declarados de nivel alto, la gestión y distribución de soportes tiene especial importancia, particularmente en lo que se refiere a la confidencialidad de los datos.

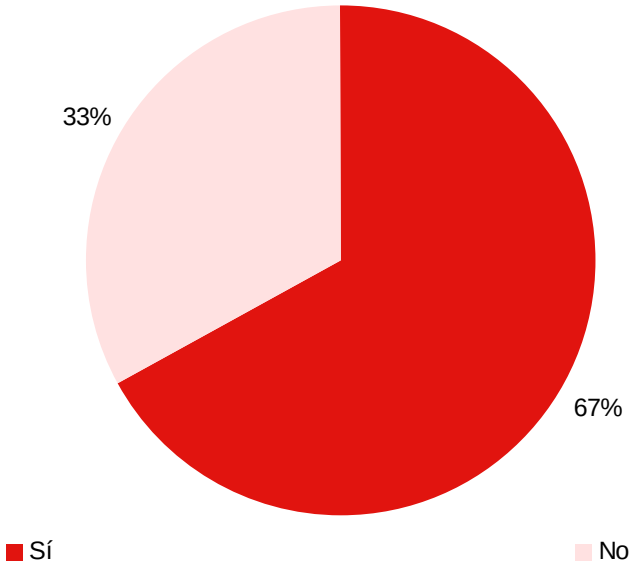
Estas obligaciones se encuentran recogidas en el art. 101 del RDLOPD, que establece:

- Utilizar un sistema de etiquetado en los soportes físicos.
- Distribuir los soportes cifrando los datos que contengan, incluyendo los datos que estén almacenados en ordenadores portátiles.

Un 67% de las pymes con ficheros de nivel alto declarados ante la AEPD etiquetan los soportes físicos para su salida fuera de las instalaciones de la empresa.

A pesar de etiquetarlos, resultados obtenidos en la entrevista cualitativa muestran en general las pymes dicen no cifrar los soportes para el almacenamiento de ficheros con datos de carácter personal.

Gráfico 38: Pymes con ficheros de nivel alto declarados ante la AEPD que etiquetan los soportes donde se almacenan datos de carácter personal (%)



Fuente: INTECO

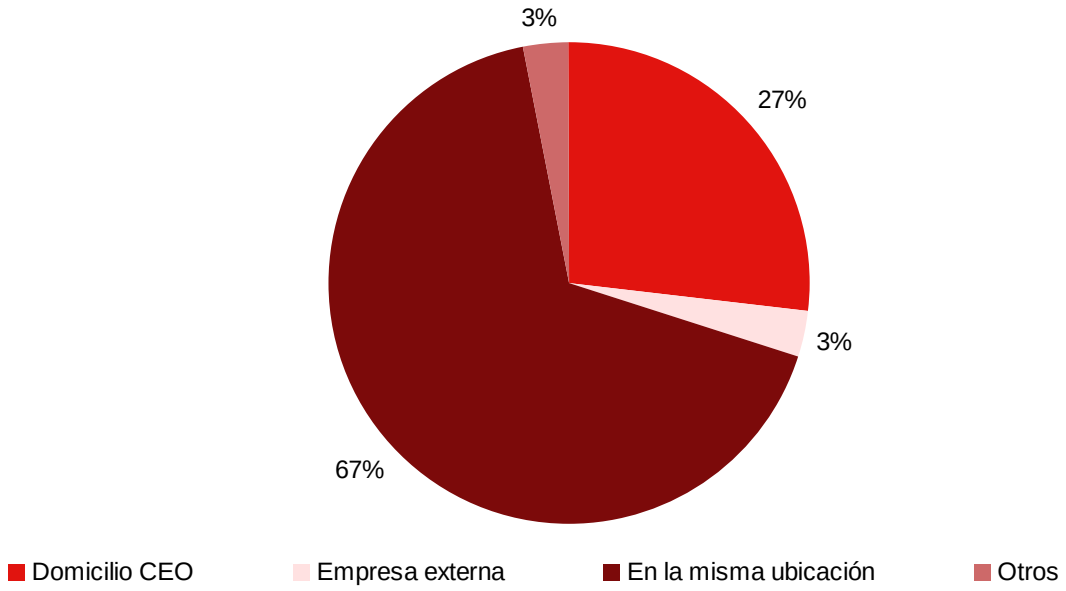
Copias de Respaldo

La normativa obliga a realizar al menos una copia de respaldo por semana de los ficheros con datos de carácter personal, al igual que los procedimientos pertinentes para su recuperación y prueba. Esta obligación está recogida en el art. 94 del RDLOPD y afecta a todo tipo de ficheros (básico, medio y alto).

Declaraciones de las pymes en la fase cualitativa del estudio muestran que, si bien es frecuente disponer de copias de seguridad de los ficheros con datos de carácter personal, éstas no se realizan con la periodicidad semanal que exige el reglamento. Lo más habitual es que las copias sean realizadas sin seguir un procedimiento preestablecido, y con una periodicidad intermitente (que en ocasiones supera al mes).

Con relación al lugar donde se depositan las copias de seguridad de los ficheros, el Gráfico 39 muestra cómo el 67% de las pymes que han declarado sus ficheros ante la AEPD manifiestan almacenarlos en la misma ubicación donde se encuentra el archivo origen. Esta práctica no es recomendable ya que en caso de un desastre, por ejemplo un incendio, existiría una alta probabilidad de que las copias se vieran dañadas y no existirá un respaldo a la hora de continuar con el proceso de negocio.

Gráfico 39: Lugares en donde almacenan las copias de seguridad las pymes con ficheros declarados ante la AEPD (%)

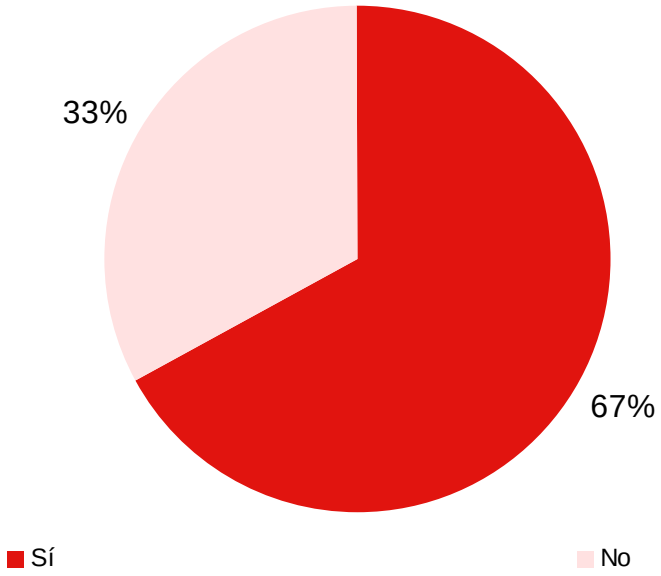


Fuente: INTECO

Dentro de las medidas de seguridad que la normativa exige para los ficheros declarados de nivel alto se encuentra la de almacenar las copias de seguridad en un lugar diferente al del tratamiento. Esta obligación viene recogida en el art. 102 del RDLOPD.

Dos tercios de las empresas que han registrado ficheros de nivel alto ante la AEPD almacenan las copias de seguridad en un lugar distinto a la ubicación de la empresa.

Gráfico 40: Pymes con ficheros de nivel alto declarados ante la AEPD que almacenan las copias de seguridad en un lugar distinto de la ubicación donde se tratan los datos (%)



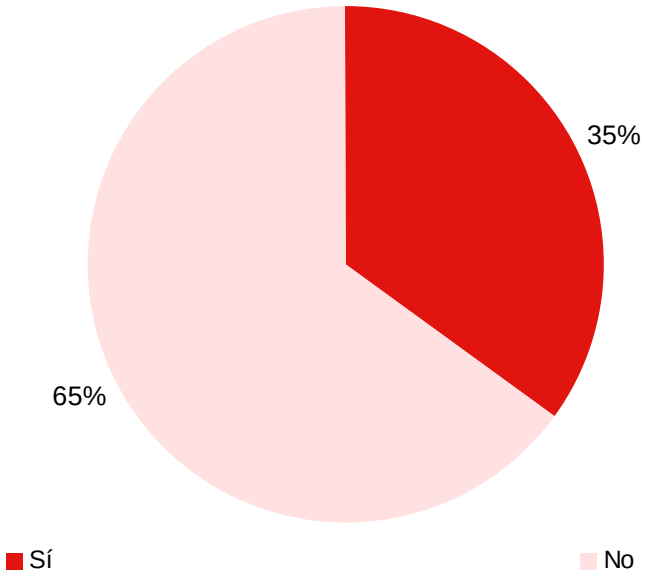
Fuente: INTECO

Criterios de Archivo

Con el fin de mantener la correcta conservación de los documentos, la localización y consulta de la información y posibilitar a los interesados el ejercicio de los derechos de oposición al tratamiento, acceso, rectificación y cancelación, la normativa de protección de datos obliga a los responsables del fichero a establecer unos criterios de archivo.

El Gráfico 41 muestra que un 35% de los encuestados dice contar con mecanismos que aseguran la conservación y localización de documentos que almacenan datos de carácter personal. Entre los mecanismos y dispositivos mencionados destacan armarios, archivadores, carpetas clasificadoras, etc. La mayoría (65%), en cambio, no tiene implementado ningún mecanismo para asegurar la conservación y localización de sus documentos con datos personales; una consecuencia de ello podría ser un retraso o dificultad en dar respuesta a una solicitud de derechos A.R.C.O.

Gráfico 41: Pymes que cuentan con mecanismos para asegurar la conservación y localización de documentos que almacenan datos de carácter personal (%)



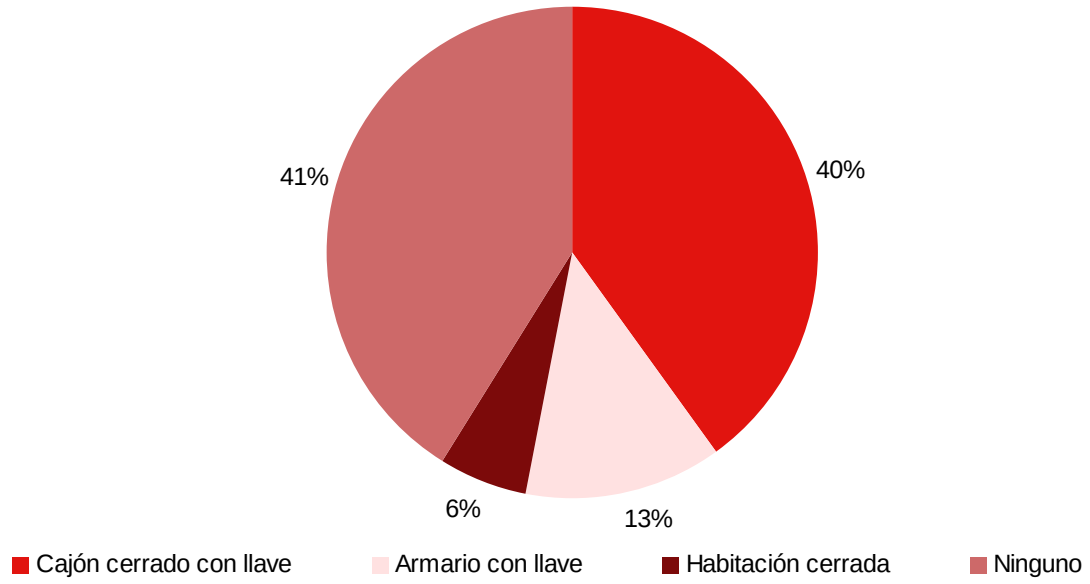
Fuente: INTECO

Almacenamiento

Dentro de las medidas referentes a la protección de ficheros no automatizados con datos de carácter personal, se encuentra la del establecimiento de requisitos que impidan el acceso físico a personal no autorizado a las instalaciones donde estén almacenados los documentos en papel. Esta obligación está recogida en el art. 107 y 111 del RDLOPD, donde se establece que se debe contar con medios de protección física para los documentos en papel que contengan datos personales.

Un 41% de las pymes española no contempla ninguna medida de protección física de sus documentos de papel. La medida más ampliamente implementada es la de guardar los ficheros en un cajón cerrado con llave (40%), seguida de un armario con llave (13%) y una habitación o despacho cerrado (6%).

Gráfico 42: Medidas de protección física para los documentos de papel con que cuentan las pymes (%)



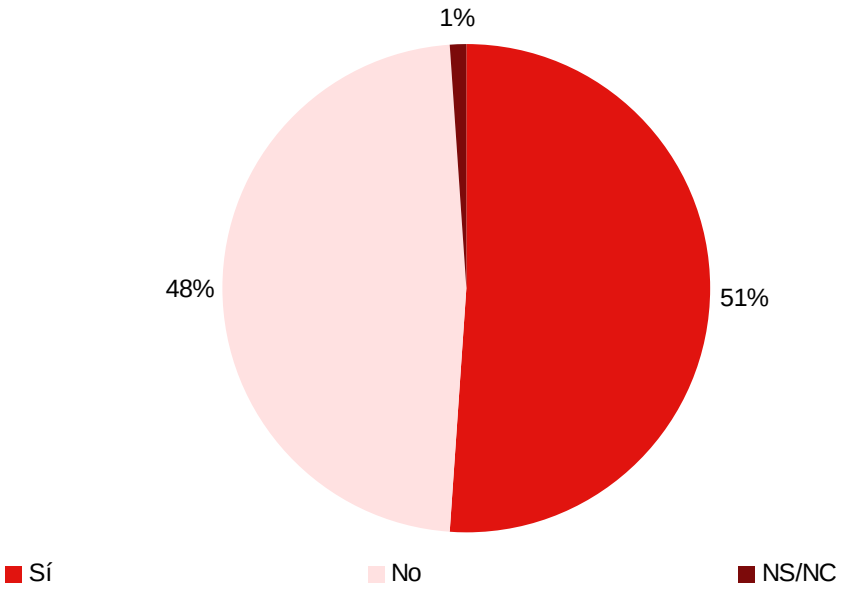
Fuente: INTECO

Custodia de Soportes

El responsable de seguridad es el encargado de proteger y salvaguardar la información sensible dentro de una empresa. En este caso en particular, el responsable de seguridad puede ser el encargado de salvaguardar la documentación que contenga datos de carácter personal o en su caso delegarla. Esta obligación está recogida en el art. 109 del RDLOPD.

El Gráfico 43 muestra que el 51% de los encuestados dice tener delegado un responsable de seguridad para estos documentos, mientras que un 48% dice no tener un delegado de seguridad específico para este tipo de documentación.

Gráfico 43: Porcentaje de empresas que tienen delegado un Responsable de Seguridad para los documentos que contienen datos de carácter personal (%)



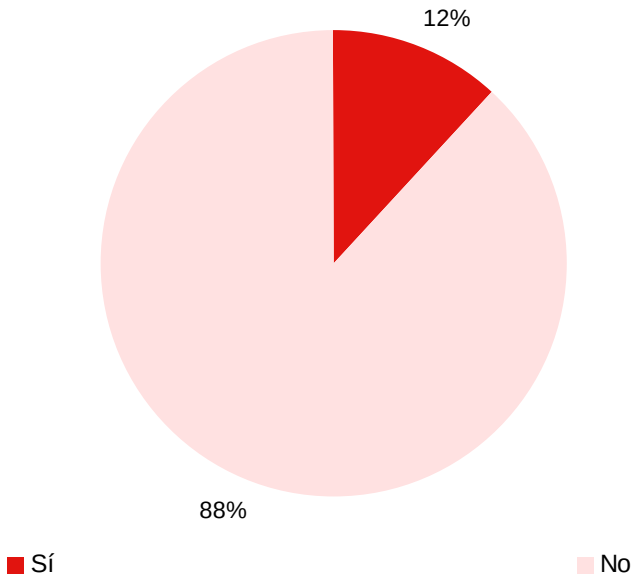
Fuente: INTECO

Copia o Reproducción

El art. 113 RDLOPD establece que se deben establecer mecanismos contra la copia y reproducción de ficheros no automatizados de nivel alto, lo que implica que sólo el personal autorizado podrá reproducir este tipo de archivos.

El Gráfico 44 muestra que sólo un 12% de los encuestados dice contar con mecanismos contra la copia y reproducción de documentos que contienen datos de carácter personal. Algunos de los dispositivos mencionados son impresoras y fotocopiadoras controladas, escáneres lejos de los emplazamientos de consulta, etc.

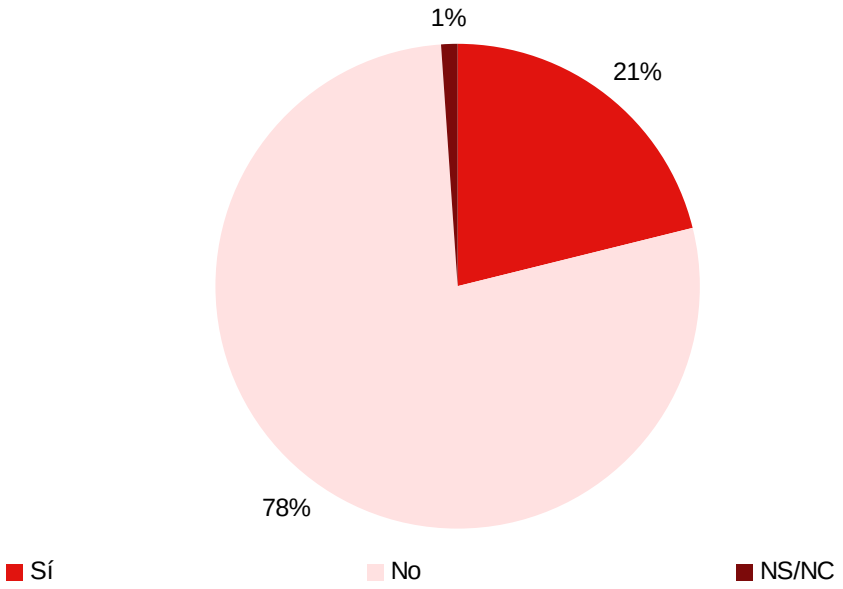
Gráfico 44: Empresas que cuentan con mecanismos contra la reproducción y copia de documentos de carácter personal (%)



Fuente: INTECO

Se analiza a continuación la predisposición de las empresas para adaptarse a la normativa que afecta a ficheros en soporte papel. Así, el Gráfico 45 muestra que el 21% de los encuestados han valorado internamente el tratamiento y destrucción de los documentos de papel que contienen datos de carácter personal, mientras que un 78% dice no tener procedimientos probados de destrucción de estos documentos. No se trata de una imposición o medida de seguridad que tenga cobertura legal ni reglamentaria, sino más bien una "declaración de intenciones" de las empresas.

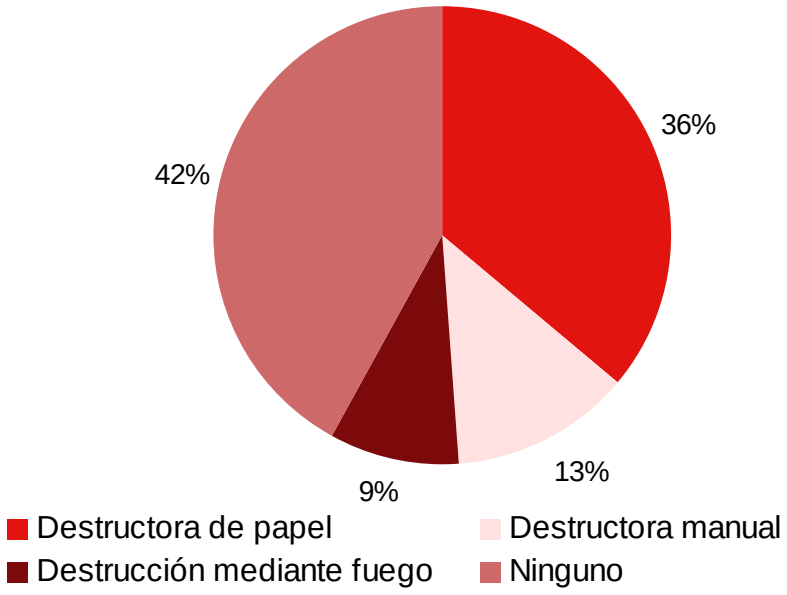
Gráfico 45: Empresas que han valorado internamente el tratamiento y destrucción de los documentos de papel que contienen datos de carácter personal (%)



Fuente: INTECO

El 21% de los encuestados que han valorado internamente el tratamiento y destrucción de los documentos en papel que contienen datos de carácter personal, fue interrogado sobre los métodos de destrucción utilizados. A continuación se presentan los resultados, donde se confirma que el método más ampliamente es la destructora de papel en un 36%. A destacar que un importante 42% de ellas no utiliza ningún método.

Gráfico 46: Métodos de destrucción de ficheros no automatizados (%)



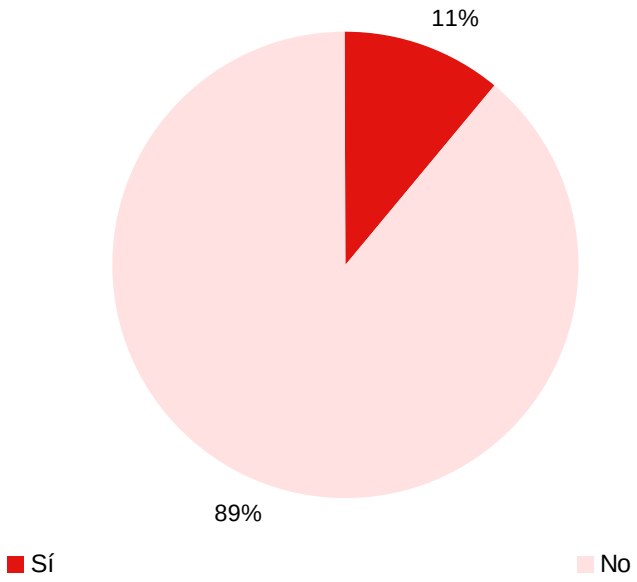
Fuente: INTECO

Auditoría

Los sistemas de información e instalaciones de tratamiento y almacenamiento de datos de ficheros de nivel medio se someterán, al menos cada dos años, a una auditoría interna o externa que verifique el cumplimiento de las medidas de seguridad. Esta obligación está recogida en el art. 96 del RDLOPD.

El Gráfico 47 muestra el porcentaje de las empresas que han registrado ficheros de nivel medio que afirman haber pasado por una auditoría bienal de sus sistemas de información, procesos, personas e instalaciones: sólo un 11% lo ha hecho, frente a un mayoritario 89% que dice no haber pasado nunca por una auditoría bienal.

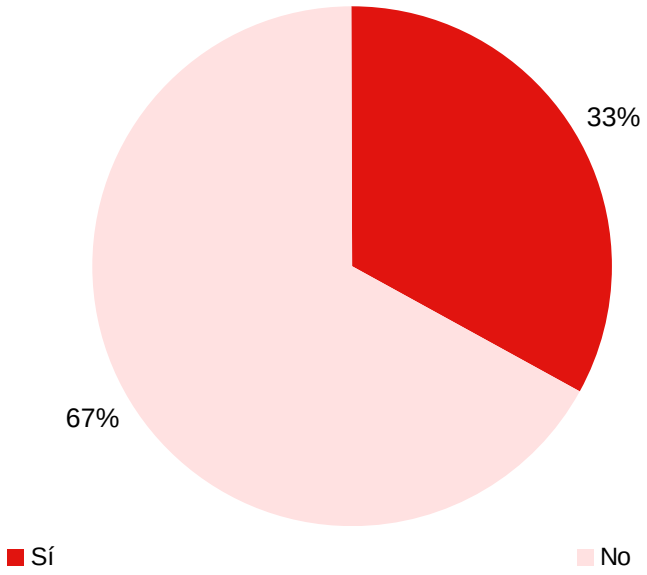
Gráfico 47 Pymes con ficheros de nivel medio declarados ante la AEPD que han tenido una auditoría bienal sobre los sistemas de información, procesos, personas e instalaciones donde se tratan datos de carácter personal de nivel medio (%)



Fuente: INTECO

El mismo análisis realizado entre las empresas que han declarado ficheros de nivel alto ante el Registro General de Protección de Datos muestra que un 33% de ellas ha realizado la auditoría bienal obligatoria, frente a un 67% que no lo ha hecho, tal y como muestra el Gráfico 48.

Gráfico 48: Pymes con ficheros de nivel alto declarados ante la AEPD que han tenido una auditoría bienal sobre los sistemas de información, procesos, personas e instalaciones donde se tratan datos de carácter personal de nivel alto (%)

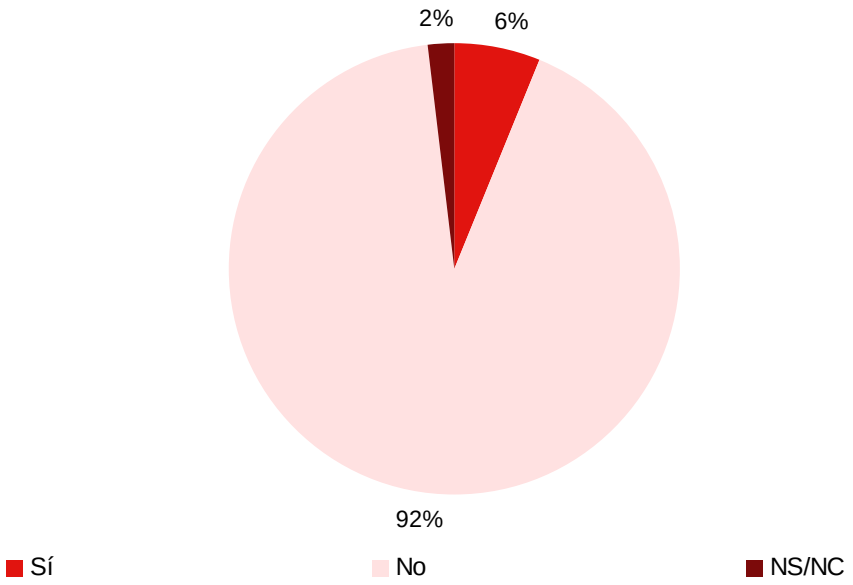


Fuente: INTECO

Del mismo modo que los ficheros declarados de nivel medio y alto deben cumplir con la obligación de realizar una auditoría bienal obligatoria, la misma medida debe aplicarse a los ficheros en soporte papel que contengan datos de carácter personal. Esta obligación se encuentra recogida en el art. 110 del RDLOPD.

Tan sólo un 6% de los encuestados dice haber cumplido una auditoría bienal para los ficheros no automatizados que contienen datos de carácter personal.

Gráfico 49: Pymes que han realizado una auditoria bienal para los documentos que contienen datos de carácter personal (%)



Fuente: INTECO

Telecomunicaciones

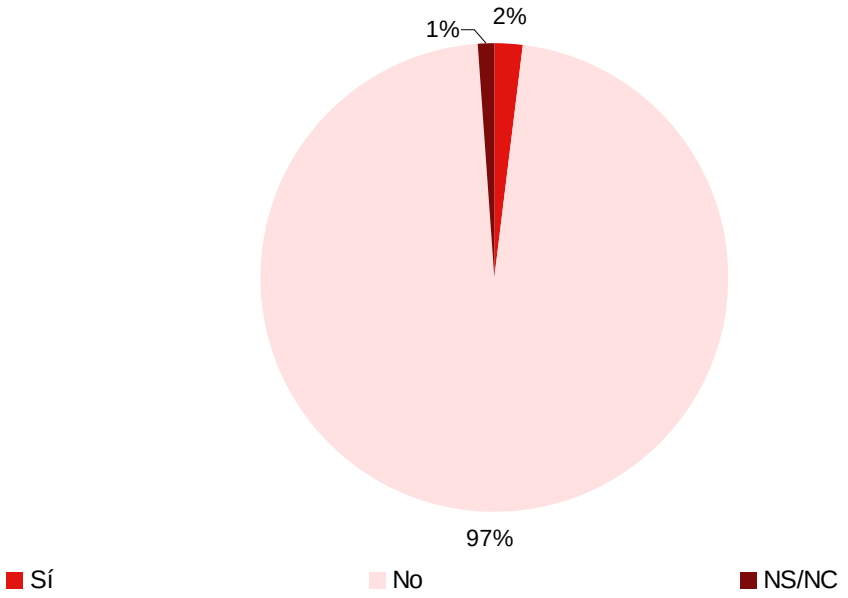
Del total de los encuestados que dicen haber declarado ficheros de nivel alto ante la AEPD, ninguno dice cifrar las comunicaciones electrónicas en el envío de ficheros al exterior de su empresa. Esta obligación se encuentra recogida en el art. 104 del RDLOPD.

Traslado de documentación

La normativa de protección de datos en el art. 114 recoge la obligación para establecer mecanismos de control sobre la documentación con datos de carácter personal para que ésta no sea accedida en su transporte.

El Gráfico 50 muestra que un 97% de los encuestados no ha establecido mecanismos para que sus ficheros no puedan ser accedidos o manipulados durante su transporte.

Gráfico 50: Empresas que han implementado mecanismos para asegurar que los ficheros no automatizados no son accedidos o manipulados durante su transporte (%)



Fuente: INTECO

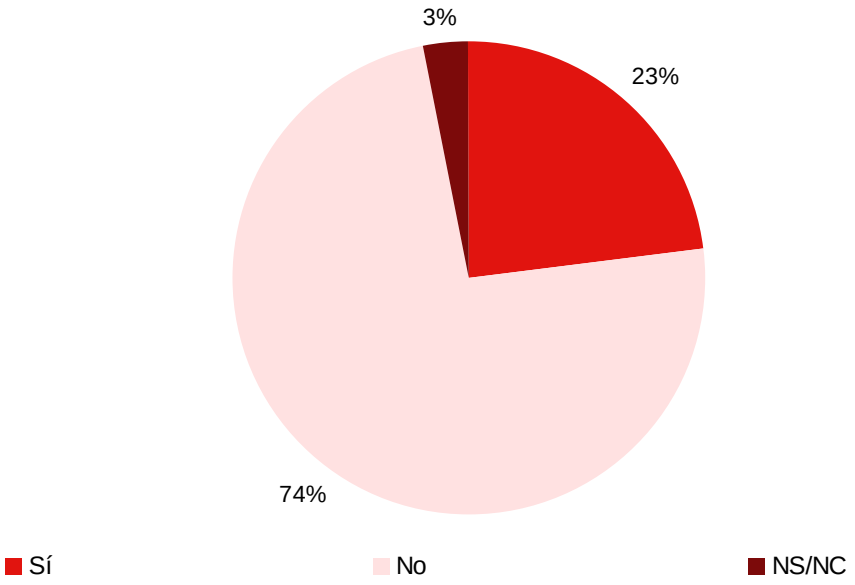
4.2.12 Ficheros no automatizados en soporte papel.

La existencia de documentación con datos personales en soporte papel se extiende a la práctica totalidad de las pymes españolas (96%, tal y como muestra el Gráfico 4). Siempre que la documentación esté ordenada en base a un criterio, constituye un fichero no automatizado y por tanto sujeto a la normativa sobre protección de datos.

El presente apartado ofrece una visión acerca del nivel de preparación de las pymes para la aplicación del RDLOPD en su operativa diaria sobre los ficheros no automatizados.

El Gráfico 51 muestra que un 23% de los encuestados dice clasificar sus documentos por nivel de confidencialidad, (pública, confidencial, reservada). Esta cuestión no responde a una obligación recogida expresamente en la ley o en el reglamento; no obstante, se trata de un indicio que muestra la mayor sensibilidad y atención de las empresas en el manejo de documentación. Es de suponer que las empresas que ya vienen implementado un tipo de clasificación de su documentación en papel, como es, en el caso analizado, el nivel de confidencialidad, podrán adaptarse con mayor facilidad a las disposiciones generales del reglamento que afectan a la seguridad de los ficheros no automatizados.

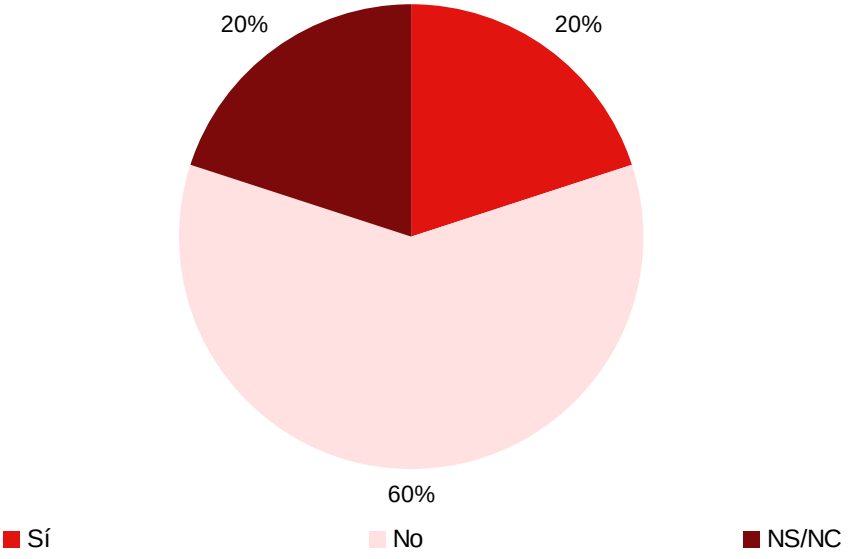
Gráfico 51: Pymes que clasifican sus documentos por nivel de confidencialidad (%)



Fuente: INTECO

El Gráfico 52 muestra el porcentaje de empresas que afirma haber implementado medidas de seguridad en sus ficheros en papel similares a las medidas que adoptan para los ficheros automatizados. En él se aprecia que un 20% manifiesta seguir medidas de seguridad equivalentes, con independencia del soporte en el que se encuentre el fichero.

Gráfico 52: Balance de cumplimiento entre medidas de seguridad de documentos y ficheros automatizados (%)



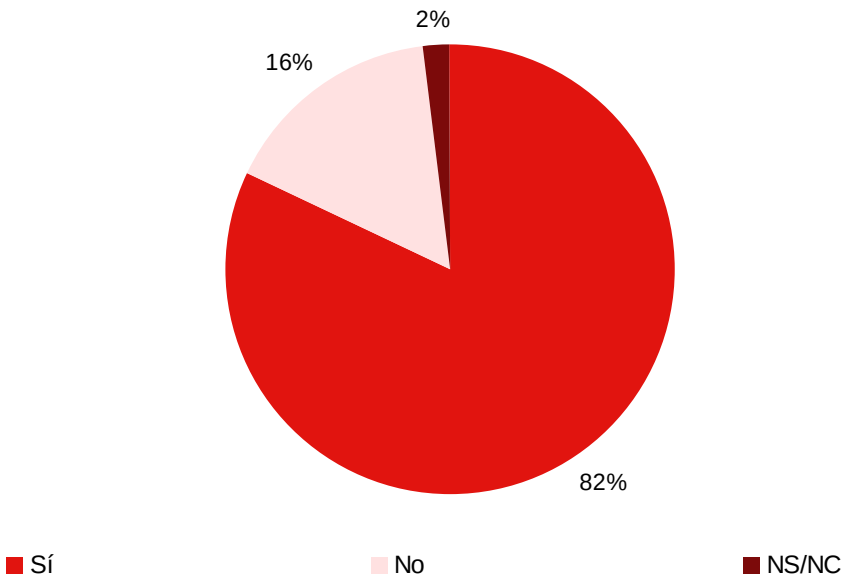
Fuente: INTECO

4.3 Concienciación de la necesidad de cumplir con la normativa de protección de datos de carácter personal

A pesar de que los resultados mostrados hasta ahora dejan ver un reducido nivel de cumplimiento de la normativa sobre protección de datos, es esperanzador el nivel de concienciación que muestran los encuestados. Así, este apartado pretende evaluar el nivel de conciencia respecto de la necesidad de cumplir con la normativa de protección de datos.

El Gráfico 53 muestra que el 82% de los encuestados dice estar concienciado con la necesidad de cumplir con la LOPD y el RDLOPD.

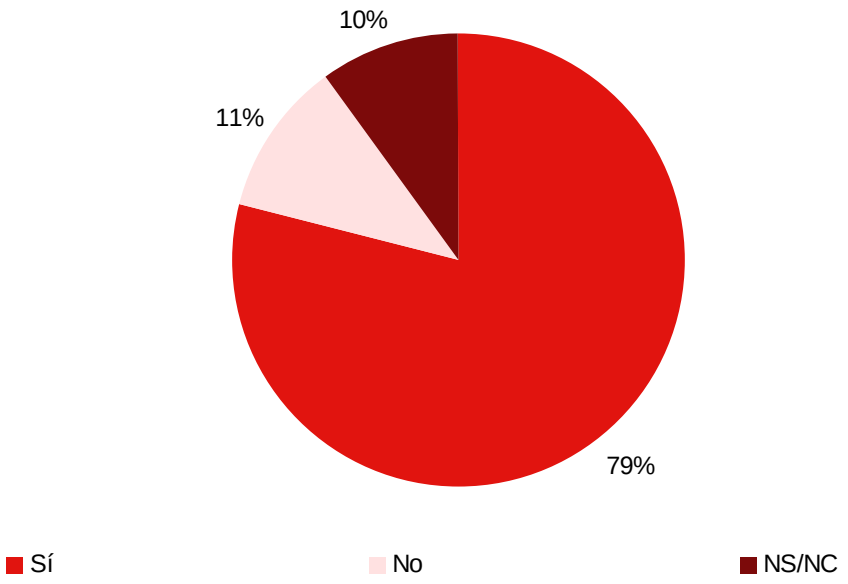
Gráfico 53: Pymes concienciadas de la necesidad de cumplimiento de la normativa sobre protección de datos (%)



Fuente: INTECO

Además, el 79% de los encuestados confirman su intención de destinar medios (económicos y/o humanos) para adaptarse a la normativa sobre protección de datos.

Gráfico 54: Pymes que van a destinar medios para adaptarse a la normativa sobre protección de datos (%)



Fuente: INTECO

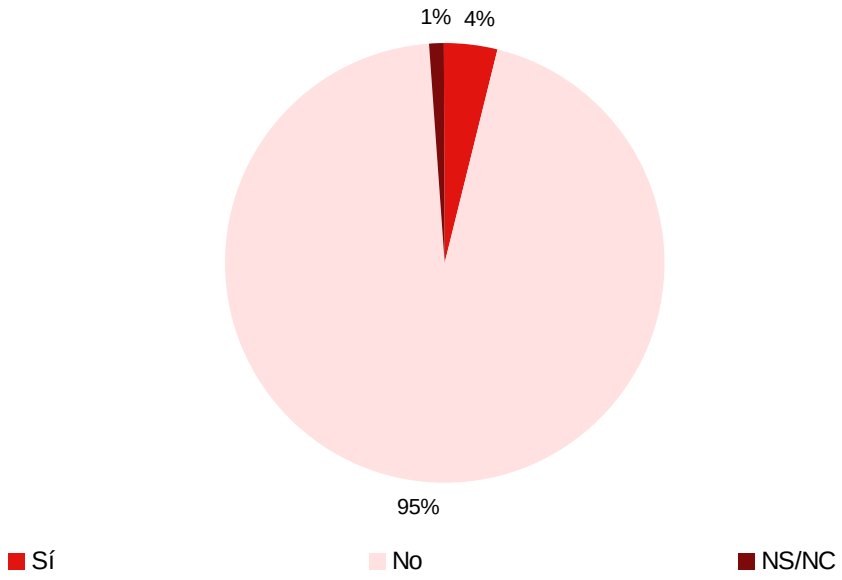
4.4 Inspecciones, denuncias y sanciones derivadas del incumplimiento de la normativa de protección de datos

Los arts. 43 a 49 de la LOPD regulan el procedimiento sancionador que podrá tramitar la AEPD. El procedimiento se inicia contra los responsables de ficheros cuando existan pruebas razonables de que se ha producido alguna infracción de los principios y garantías contenidos en la LOPD.

Este apartado analiza, por un lado, el volumen de empresas que se han visto afectadas por una inspección de la AEPD, y por otro, el nivel de conocimiento respecto a las sanciones a las que pueden verse sometidas las empresas como consecuencia de un incumplimiento de la normativa de protección de datos.

El Gráfico 55 muestra el porcentaje de empresas que han sufrido alguna inspección por parte de la Agencia. Un 95% de los encuestados dice no haber recibido nunca una inspección relativa a la protección de los datos de carácter personal. Parece que, hasta ahora, la actividad de la AEPD se ha venido centrando en la inspección a empresas de mayor tamaño.

Gráfico 55: Pymes que han sufrido alguna inspección por parte de la AEPD (%)

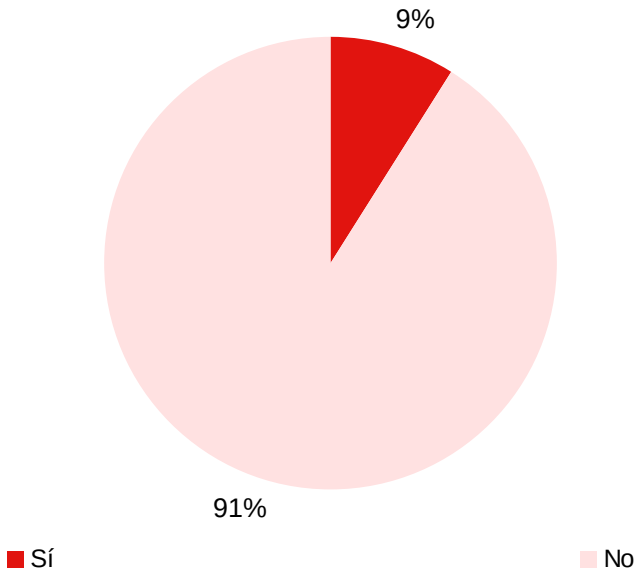


Fuente: INTECO

El Gráfico 56 analiza el nivel de conocimiento de la cuantía de las sanciones por parte de las empresas entrevistadas. Estas sanciones pueden ir desde los 600 euros en caso de infracción leve (por ejemplo, desatender la solicitud del interesado de cancelar sus datos personales, no solicitar la inscripción de los ficheros a la AEPD, o no cumplir el deber de información al recabar los datos personales) hasta los 600.000 euros si la infracción es muy grave (por ejemplo, recoger datos de forma fraudulenta y engañosa, comunicar o ceder datos fuera de los supuestos permitidos, o recabar y tratar los datos sin el consentimiento del afectado). Así viene establecido en el art. 45 RDLOPD.

Sólo el 9% de las pymes españolas declaran conocer a cuánto ascienden las sanciones en caso de incumplimiento de la normativa sobre protección de datos.

Gráfico 56: Nivel de conocimiento de la cuantía de las sanciones de la Agencia de Protección de Datos por incumplimiento de la LOPD (%)



Fuente: INTECO

5 FRENOS PARA LA ADOPCIÓN Y BENEFICIOS DERIVADOS DE ELLA

Tal y como se ha mostrado en el apartado 4, la situación de la pyme española en lo que se refiere al nivel de conocimiento y adopción de la normativa sobre protección de datos no es especialmente positiva: un 66% afirma desconocer la normativa, y sólo un 16% de las pymes participantes en el estudio tienen sus ficheros declarados ante la AEPD.

En el presente epígrafe se analizan los frenos o barreras con los que se encuentran las pymes en su proceso de adopción a la normativa, así como los beneficios y valor añadido que la implementación aporta al negocio.

Si bien en análisis de los beneficios es genérico y común a todo tipo de empresas, los frenos analizados afectan en especial a las pymes, ya que tienen que ver con sus circunstancias particulares de reducidas dimensiones y limitación de recursos (económicos, humanos, técnicos) que no afecta a las grandes empresas.

5.1 Frenos a la adopción

Falta de sensibilidad hacia la necesidad de proteger los datos personales y desconocimiento de la ley

Las pymes no conocen la importancia y necesidad de proteger los datos de carácter personal y no entienden el porqué de una normativa sobre protección de datos. Este hecho hace que desconozcan en gran medida la LOPD y el RDLOPD.

En ocasiones, es posible que la pyme tenga conocimiento de la existencia de una ley, pero desconocen la obligatoriedad de la misma y/o las consecuencias de su incumplimiento. En este sentido, existen empresas que no se consideran sujetas a la ley, ya que entienden que se trata de disposiciones que afectan exclusivamente a empresas de mayor tamaño.

Este desconocimiento y falta de sensibilización afecta incluso a la consideración de qué son datos personales y/o ficheros con datos personales, existiendo pymes que, por no conocer el ámbito objetivo de aplicación de la normativa, no se consideran afectadas.

La Administración, la propia Agencia de Protección de datos, organizaciones y patronales empresariales, así como entidades prescriptoras, han realizado labores formativas y de sensibilización. Parece que se hace necesario seguir profundizando en este esfuerzo informativo.

Rechazo al cambio

Incluso en el caso de conocer la normativa, existe entre las pymes un rechazo a las novedades. La adaptación a la legislación sobre protección de datos supone un cambio en la organización de la información que afecta a tareas, conceptos, procesos y mecánicas de trabajo. El colectivo pyme, a priori más conservador en su forma de trabajar, puede mostrar una predisposición reacia a todo lo que implique cambio sustancial en su forma de organizar el trabajo, si de ello no se desprende un beneficio percibido para su negocio. En general, las empresas que se encuentran en proceso de adaptación a la normativa sobre protección de datos lo perciben como una imposición o una carga y no como algo que aporta valor a su negocio.

Por ello, las medidas de sensibilización a implementar deben tener en cuenta esta circunstancia, haciendo énfasis en el valor añadido que la normativa aporta al negocio y que la adaptación al cambio requiere un esfuerzo inicial que a medio y largo plazo es sencillo de manejar.

Limitación de recursos (económicos, humanos y tiempo)

Puede darse el caso de empresas que conocen la normativa y no muestran un rechazo frontal al cambio que supone, pero no obstante reconocen una limitación de recursos necesarios para su correcta implementación. Se podría decir que, junto con el desconocimiento de la normativa, éste es el motivo que en mayor medida frena a las pymes a la hora de la adaptación.

Las pymes, por lo general, consideran que el gasto que supone la labor de adaptación (consultoría, si optan por esta opción, y medios materiales como soportes de almacenamiento, control de acceso lógico, cifrado, etc.), es excesivo e innecesario, en tanto en cuanto no les reporta un valor añadido inmediato.

Del mismo modo, al tratarse de algo que consideran complejo, consideran que no disponen de personal con suficientes conocimientos técnicos en la materia, y por tanto se plantean la necesidad de contratar a alguien específico.

Al excesivo coste percibido y la falta de recursos humanos cualificados se une el tiempo de adecuación, que en toda lógica, se desvía de la actividad principal del negocio para destinarse al cumplimiento de la normativa sobre protección de datos. En general, se percibe como una tarea tediosa que exige desviar recursos de la actividad principal del negocio.

Por ello, es necesario que en la labor difusora de la Administración se tenga en cuenta esta circunstancia, para instruir de forma objetiva acerca del coste, tiempo y recursos

humanos necesarios para la adopción de la normativa, y facilitar pautas para maximizar la efectividad.

Ámbito técnico de la normativa sobre protección de datos

Relacionado con lo anterior, se encuentra el freno derivado del ámbito excesivamente técnico de la normativa sobre protección de datos. Las medidas de seguridad informática que se deben implantar son temas que pueden resultar complejos para las pymes, no disponiendo de recursos técnicos (tanto materiales como humanos) capaces de hacerles frente.

Algunas consultoras especializadas en facilitar la adopción de la normativa entre las pymes critican que, precisamente por el carácter técnico de la norma, en ocasiones las implantaciones no se hacen con un nivel de efectividad del 100% ya que pueden descuidar aspectos de tipo informático – técnico, o legal, en función del perfil del implementador.

Errónea implementación de la normativa

Incluso en los casos en los que se la pyme implanta la normativa, ésta se hace de forma errónea. A lo largo del informe se han presentado numerosos ejemplos de situaciones en las que las empresas, invirtiendo medios para asegurar la implantación, no están en situación completamente ajustada a la ley. Se trata de conceptos y requisitos complicados (perfiles de usuario, permisos…), y de situaciones que las empresas pueden estar considerando ajustadas a la ley cuando realmente no es así (involucración de todo el personal de la empresa, realización de auditorías, registros de entrada y salida de datos…).

5.2 Beneficios derivados de la implantación

Reconociendo la existencia de los frenos anteriormente descritos, e insistiendo en la necesidad de implementar medidas para minimizarlos, es necesario puntualizar que la adopción de la normativa sobre protección de datos aporta una serie de beneficios que se traducen en un valor añadido para la empresa. Por ello, las acciones de concienciación y formación deben ir encaminadas a la exposición de las ventajas derivadas de la adopción de la normativa sobre protección de datos.

El valor de los datos

Los datos personales son valiosos en sí mismos. La tendencia actual es a considerarlos un activo más de la empresa. Los datos son información, y la información es valiosa. Por ello, es necesario hacer un esfuerzo por proteger los datos para garantizar su confidencialidad (interna y externa) y evitar posibles incidencias de seguridad: pérdida, fuga o robo de información que puede hacer llegar los datos a personas inadecuadas

(empresas de la competencia, medios de comunicación, empleados malintencionados…). Una incidencia de este tipo puede tener consecuencias muy negativas para la empresa, y en ocasiones los empresarios no se han planteado las consecuencias ante la pérdida de una base de datos de clientes, proveedores o empleados.

Aumento de calidad en las operaciones

La adaptación de la pyme para el cumplimiento de la LOPD contribuye a mejorar los procesos de manejo de la información, ya que proporciona una cultura de calidad en el tratamiento de los datos y la gestión del negocio que puede trasladarse a otros procesos de la empresa. Una cuestión tan básica como poner en orden la información contribuye en ocasiones a detectar problemas o carencias del negocio.

Mejora de la imagen corporativa

El cumplimiento de la normativa sobre protección de datos garantiza la confidencialidad y el derecho a la intimidad de los titulares de los datos cedidos. En este sentido, es una referencia y garantía de seriedad y confianza para los actores que se relacionan con las pymes en su tráfico diario, principalmente clientes y proveedores, pero también empresas de la competencia. Así, algunas pymes reconocen haber iniciado el proceso de adaptación a la ley ante una solicitud de alguno de sus clientes, o ante la generalización de la cultura de protección de datos entre empresas pertenecientes a su sector de actividad. En general, lo consideran beneficioso para la propia imagen y una manifestación de la responsabilidad social corporativa.

Es un derecho fundamental

La protección de datos es un derecho fundamental que ampara a todos los ciudadanos, y para su garantía efectiva las empresas han de cumplir las disposiciones previstas en la ley. De lo contrario, pueden verse afectadas por denuncias o sanciones. La Agencia Española de Protección de Datos, como órgano competente declarado en la Ley, tiene las atribuciones necesarias para realizar inspecciones y sancionar a los que incumplen la normativa. Las empresas que disponen de datos de carácter personal pueden verse involucradas en sanciones realizadas bajo denuncias de los diferentes agentes que participan en el negocio ya sea por parte de sus clientes, colaboradores o empleados. Cumplir con la normativa es una obligación cada día más latente debido en mayor medida a las sanciones y, en opinión de las empresas prescriptoras participantes en el estudio, es el miedo a las sanciones el motivo principal que empuja a las pymes a cumplir la normativa.

Facilidad en la implementación

La Agencia Española de Protección de Datos insiste en que el cumplimiento es más sencillo y ágil de lo que inicialmente pueden considerar las pymes. Así, desde la AEPD se han puesto en marcha numerosas acciones facilitadoras para simplificar los trámites formales de los responsables de los ficheros: sesiones abiertas de difusión, guías con pautas para el correcto cumplimiento (recientemente la AEPD ha publicado la *Guía del Responsable de ficheros*), implementación del sistema NOTA, modelos de notificación precumplimentados para inscribir los ficheros, gratuidad de la inscripción… Estas iniciativas se ha complementado en septiembre de 2007 con la firma de un Convenio entre la AEPD y el Ministerio de Industria para facilitar la inscripción de los ficheros de las pymes constituidas telemáticamente a través de los PAIT (Puntos de Asesoramiento e inicio de tramitación). En este mismo sentido, INTECO ha elaborado la *Guía básica para la pyme de adaptación a la normativa de protección de datos,* con información de interés para aquellas empresas que estén implementando la normativa sobre protección de datos.

Además, en las pymes concurren una serie de circunstancias que, hablando en términos generales, pueden facilitar la organización de la información. Así, parece lógico pensar que el menor tamaño y flujo de negocio que maneja una pyme, en comparación con una gran empresa, puede implicar un menor volumen de información manejada y por tanto facilitar su ordenación y control.

Creación de un entorno de seguridad

La adopción de la normativa sobre protección de datos puede constituir el primer paso para orientar a la empresa hacia un entorno de seguridad más ambicioso. Así, existen en la actualidad sistemas de gestión de seguridad de la información (SGSI) que persiguen, por un lado, incorporar la seguridad en los sistemas de información de las empresas como elemento de la mejora de la gestión y de la competitividad y, por otro, ofrecer protección contra los riesgos y pérdidas asociados al creciente uso de tecnologías de la información y de la comunicación en las empresas. INTECO está desarrollando un proyecto piloto en este sentido, facilitando, conjuntamente con las Cámaras de Comercio, la implementación de SGSI en las pymes.

6 CONCLUSIONES

La conclusión principal del estudio es clara: la normativa sobre protección de datos es escasamente conocida y no suficientemente implantada en el entorno pyme, por lo que no parece que las pequeñas empresas se encuentren preparadas para hacer frente a las nuevas medidas de seguridad previstas en el RDLOPD que afectan a ficheros no automatizados en los plazos que contempla el reglamento.

El desconocimiento de la normativa se manifiesta tanto a través de la respuesta de las empresas ante la pregunta directa sobre el conocimiento de la legislación (un 66% afirma abiertamente no conocer la LOPD, y un 85% manifiesta lo propio con respecto al RDLOPD), como mediante los indicios analizados a lo largo del estudio y derivados de las investigaciones cuantitativa y cualitativa. No se puede afirmar, en cambio, que todas las empresas se encuentren en un estadio similar de ignorancia de la normativa; así, existe un amplio abanico de circunstancias entre las pymes que abarcan desde empresas que ni siquiera han oído hablar de la ley, hasta casos que conocen la existencia de la misma, pero desconocen la obligatoriedad de su cumplimiento, su ámbito de aplicación, las implicaciones concretas para su negocio, las sanciones a las que se pueden enfrentar en caso de incumplimiento o los plazos de adecuación, por poner sólo ejemplos.

El nivel de desconocimiento es más acusado en lo que afecta al RDLOPD (lógico, por otra parte, teniendo en cuenta la reciente fecha de entrada en vigor del mismo).

Parece que las acciones formativas e informativas llevadas a cabo por las administraciones, AEPD, asociaciones empresariales y sectoriales, cámaras de comercio, empresas prescriptoras, etc., no han alcanzado la efectividad deseada, o no han tenido suficientemente en cuenta las particularidades del colectivo a la hora de elaborar acciones específicamente dirigidas a ellas.

En cualquier caso, el nivel de conocimiento declarado es muy inferior al declarado por el resto de la población. Así, el barómetro del CIS de febrero de 2008 incluía cuestiones relativas a la protección de datos, y en él se mostraba cómo un 52% de la población española afirma ser consciente de la existencia de una normativa sobre protección de datos, frente a sólo un 34% en el caso del colectivo pyme. El esfuerzo sensibilizador ha de estar orientado específicamente al entorno pyme, que, hablando en términos generales, presentan unas circunstancias comunes que las caracterizan y diferencian de las empresas de mayor tamaño.

En parte consecuencia del escaso conocimiento, el nivel de implementación de la normativa entre las pymes españolas es deficiente. La AEPD considera que no más de un 10-15% de las pymes españolas tienen sus ficheros con datos personales declarados ante el registro de la Agencia.

El nivel de cumplimiento entre las empresas no es homogéneo, existiendo empresas que incumplen completamente las disposiciones de la ley, y otras que están parcialmente adaptadas a la normativa (porque tienen registrados los ficheros, porque se han adaptado aunque no han hecho seguimientos, actualizaciones y/o auditorías posteriores…). Por tanto, es necesario que el esfuerzo en este sentido sea continuado y sostenido.

Detrás del limitado nivel de adopción se encuentra, aparte de una escasa cultura y concienciación sobre la necesidad de proteger los datos, la consideración por las pymes de que se trata de una obligación legal que implica tareas tediosas y complejas y que no aporta ningún valor añadido a su negocio, el desconocimiento de las consecuencias de incumplimiento, y la limitación de recursos humanos, económicos y técnicos para hacer frente a la adopción. Se trata, en su mayoría, de barreras declaradas por las propias pymes que en muchas ocasiones pueden ser fácilmente solventadas con acciones formativas concretas y efectivas.

Por todo ello, parece que la pyme española está aún alejada de estar en condiciones de afrontar el cumplimiento de las obligaciones de protección de datos de carácter personal en soporte papel: no conoce las obligaciones y todavía no ha valorado la situación e implicaciones internas del negocio.

En este contexto, es necesario un esfuerzo de concienciación y difusión por parte de todos los agentes implicados: las administraciones y autoridades competentes, que han de concienciar a las empresas sobre la necesidad de adaptarse a la normativa sobre protección de datos; el propio tejido empresarial (cámaras de comercio, patronales, asociaciones), que, como conocedor de primera mano de la realidad empresarial, puede ofrecer las soluciones de formación e información que mejor responden a las particularidades de las pymes; las empresas prescriptoras y facilitadoras (gestorías, consultoras), que están en condiciones de realizar un correcto diagnóstico sobre la situación de las empresas y planificar de forma eficiente su implantación; por último, la propia inercia del mercado contribuirá a generalizar el cumplimiento de la normativa sobre protección de datos entre el tejido pyme: a medida que se difunda entre la población el ejercicio de los derechos que la ley otorga a todo ciudadano, las empresas se adaptarán a lo dispuesto en la legislación sobre protección de datos.

7 RECOMENDACIONES DE ACTUACIÓN

Consecuencia del diagnóstico realizado en el presente estudio, se formulan a continuación una serie de recomendaciones, que afectan tanto al sector público como al privado, y que tienen como objetivo incrementar la tasa de cumplimiento de la normativa sobre protección de datos por parte de las pymes españolas. Las medidas de actuación recomendadas pasan por seguir realizando acciones de concienciación al colectivo, tanto por parte de las administraciones como por parte del resto de actores implicados: asociaciones sectoriales, cámaras de comercio, empresas prescriptoras y facilitadoras…

7.1 Recomendaciones a las administraciones públicas

Incrementar la intensidad de las acciones de sensibilización y adaptarlas a las necesidades del colectivo pyme

Para mitigar el bajo nivel de conocimiento y aplicación de la normativa sobre protección de datos, es necesario potenciar la formación y sensibilización dirigidas a las pymes. Este esfuerzo no tiene por qué de ser exclusivo de las administraciones, como se ha mencionado anteriormente.

Sería deseable que las medidas de sensibilización cumpliesen con las siguientes características:

- En primer lugar, respecto al ámbito objetivo, puede resultar positivo la adaptación de las acciones a las particularidades de las pymes. No se debe olvidar que el colectivo de pequeñas empresas 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 pyme.

- Por lo que respecta al enfoque, éste debería ser didáctico, no impositivo. Se detecta entre el colectivo pyme una falta de cultura sobre la necesidad de proteger los datos personales; así, en opinión de la mayoría de las empresas prescriptoras participantes en el estudio, las pymes que cumplen con la normativa lo hacen en gran medida por cubrirse ante el riesgo de una posible sanción de la AEPD, y no porque estén concienciadas sobre sus beneficios. Para formar a las empresas y generalizar el cumplimiento de la normativa es deseable que éstas 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 último, respecto al contenido de la formación, éste debe cubrir diferentes partes de la normativa. Como se ha mostrado anteriormente, el nivel de desconocimiento de las empresas no es homogéneo, existiendo pymes que nunca han oído hablar de la ley y otras que desconocen aspectos concretos de la misma. Por ello es clave articular un programa de concienciación adaptado al estadio de conocimiento de la/s empresa/s participante/s. Se enumeran a continuación una serie de aspectos en los que valdría la pena profundizar en las acciones de formación:

    - Necesidad de la protección de datos, qué aporta a la ciudadanía y qué aporta al negocio.

    - Ámbito de aplicación de la normativa en España. Se trata de recordar que la norma es obligatoria con independencia de las dimensiones y/o facturación de la empresa.

    - Información sobre la Agencia Española de Protección de Datos: buena parte de la sociedad española todavía no está familiarizada con la AEPD. De este modo, el barómetro del CIS de febrero de 2008[10] muestra que un 54,4% de la población española afirma no conocer la AEPD. Ante la pregunta *¿a través de qué medio denunciaría la utilización de sus datos personales sin su consentimiento?* sólo un 15,5% manifiesta que lo haría a través del "organismo público encargado de tutelar a los ciudadanos en esta materia". Un 12,8% lo haría a través de una asociación de consumidores y usuarios y un 8,1% en los ayuntamientos. Un 12,3% reconoce no saber dónde dirigirse. Todo ello parece confirmar que el conocimiento de la AEPD no es, entre la población española, universal. En base a los datos del barómetro, y a los presentados en este estudio, cabe esperar que entre las pymes españolas la situación no sea diferente. Se hace por ello necesario reforzar la comunicación sobre la AEPD, sus funciones y responsabilidades en materia de protección de datos.

    - Clarificación sobre las disposiciones previstas en la legislación: la terminología empleada tanto en la ley como en el reglamento es excesivamente técnica, y puede resultar a pymes no familiarizadas una información tediosa y compleja. La "traducción" de la normativa al idioma habitual de las pequeñas empresas puede ayudarles a comprender las

[10] CIS, Barómetro de Febrero de 2008, Estudio nº 2.754. Encuesta de ámbito nacional con una muestra de 2.470 sujetos (población española de ambos sexos de 18 años y más)

implicaciones concretas. El Eurobarómetro[11] analiza explícitamente este punto. Ante la pregunta a las empresas de si favorecerían un "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 responde 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 pymes, sino a empresas de más de 20 empleados) agradecería una clarificación terminológica de la ley sobre protección de datos.

Tener en cuenta las particularidades de las pymes (en dimensiones, sector de actividad, facturación, tipología de datos, disponibilidad de recursos humanos, económicos y técnicos…) para modular las exigencias normativas

La legislación actual no contempla diferencias entre las Grandes Empresas y las pymes en lo que respecta a obligaciones, nivel de exigencia ni cuantía de sanciones. La LOPD establece un marco general para todas las empresas, y debe ser cumplida por todos. La filosofía de la normativa española de protección de datos es tener en cuenta la gravedad de la infracción, siendo irrelevante las dimensiones.

Lo cierto es que se trata de dos realidades completamente diferentes, y 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. A título de ejemplo:

- Mayor esfuerzo formativo dirigido a las pymes: este punto ya se ha comentado anteriormente. Dado que, según declaraciones de la propia AEPD, las grandes empresas han sido las que primero han implantado la normativa, es lógico pensar que las empresas que todavía no se han adaptado a la LOPD son pymes, y por tanto el esfuerzo ha de ir focalizado a estas empresas.

- Elaboración de recomendaciones específicamente dirigidas a las pymes: hasta ahora la AEPD está elaborando recomendaciones por sector de actividad, sin tener en cuenta el tamaño de la empresa. Se podría considerar a la pyme como un colectivo, aunque transversal a muchos sectores, que merecería la pena ser considerado en su conjunto.

[11] Eurobarometer Comisión Europea – The Gallup Organization. Data Protection in the European Union. Data controllers' percepciones (February 2008). Encuesta de ámbito europeo realizada a 4.835 controladores de datos de empresas seleccionadas en base a dos criterios: país y número de empleados de la empresa (20-49, 50-249, 250+).

- Modular la cuantía de las sanciones teniendo en cuenta parámetros internos de la empresa (por ejemplo, un porcentaje de su facturación). La cuantía de las sanciones es alta (hasta 600.000 euros) e inafrontable para muchas pymes.

- Otras medidas podrían ser la ampliación de los períodos transitorios (estableciendo más amplios para las pymes que para las grandes empresas), el establecimiento de servicios públicos telefónicos u online de ayuda a la implementación…

- Por último, una parte de la población aboga por una legislación específica para cada sector de actividad. No se trata de una solución sencilla ni aplicable en el corto plazo, pero el 67% de las empresas españolas (y el 56% de las europeas)[12] favorecerían una iniciativa de este tipo.

Facilitar el proceso de adaptación, ofreciendo a las pymes pautas y herramientas para una implementación ágil y sencilla.

En este sentido, la AEPD ha puesto en marcha herramientas para simplificar y agilizar los trámites de inscripción de ficheros. También ha publicado guías, disponibles a través de www.agpd.es, y organizado seminarios y sesiones abiertas. Del mismo modo, INTECO ha elaborado una *Guía básica para la pyme de adaptación a la normativa de protección de datos*, 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. También ofrece en www.inteco.es un catálogo de consultores expertos en auditar e implementar la normativa LOPD entre las pymes. Desde INTECO, la recomendación es recurrir a los profesionales para garantizar la calidad en el cumplimiento.

Medidas facilitadoras más agresivas podrían ser ofrecer subvenciones y/o incentivos a las pymes que se adapten a la normativa.

7.2 Recomendaciones al sector privado

- Para la implementación, recurrir si es necesario a un tercero. 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. En www.inteco.es se ofrece un catálogo de consultores.

[12] Eurobarometer Comisión Europea – The Gallup Organization. Data Protection in the European Union. Data controllers' percepciones (February 2008). Encuesta de ámbito europeo realizada a 4.835 controladores de datos de empresas seleccionadas en base a dos criterios: país y número de empleados de la empresa (20-49, 50-249, 250+).

- Evaluar periódicamente el nivel de cumplimiento, a través de auditorías y medidas de seguimiento.

- Instar 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.

- 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.

ÍNDICE DE GRÁFICOS

ÍNDICE DE TABLAS

Instituto Nacional
de Tecnologías
de la Comunicación

http://www.inteco.es

http://observatorio.inteco.es