



Instituto Nacional
de Tecnologías
de la Comunicación

Estudio sobre la seguridad de los datos de carácter personal en el ámbito de las Entidades Locales

Diagnóstico sobre el grado de adaptación a la Ley Orgánica de Protección de Datos (LOPD) y al nuevo Reglamento de Desarrollo (RDLOPD)



Edición: Diciembre 2008

**INTECO quiere agradecer especialmente su colaboración en la elaboración
de este estudio a:**



La presente publicación pertenece al **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

ÍNDICE.....	3
PUNTOS CLAVE	8
I Adaptación a la Ley Orgánica de Protección de Datos (LOPD) y al nuevo Reglamento de Desarrollo (RDLOPD) por las Entidades Locales.....	8
II Niveles de madurez y análisis de mejores practicas	9
III Recomendaciones	10
1 INTRODUCCIÓN Y OBJETIVOS	12
1.1 Contexto y oportunidad del estudio	12
1.2 Objetivos del estudio.....	13
1.3 Ámbito normativo y marco de referencia	15
1.4 Entidades participantes.....	18
1.4.1 Instituto Nacional de Tecnologías de la Comunicación	18
1.4.2 Federación Española de Municipios y Provincias.....	20
2 DISEÑO METODOLÓGICO	21
2.1 Descripción	21
2.2 Ficha técnica de la fase cualitativa: entrevistas a expertos	21
2.3 Ficha técnica de la fase cuantitativa: entrevistas a personal laboral, funcionarios, responsables políticos y colaboradores en las Entidades Locales.....	22
2.3.1 Tamaño y distribución muestral	23
2.3.2 Método de recogida de información.....	29
2.3.3 Trabajo de campo	29
2.3.4 Error de muestreo	29
3 CONOCIMIENTO, CONCIENCIACIÓN Y ASIGNACIÓN DE RECURSOS CONFORME A LA NORMATIVA VIGENTE	30

3.1	Nivel de conocimiento del RDLOPD en las EELL.....	30
3.2	Nivel de concienciación respecto del cumplimiento de la normativa de protección de datos.....	33
3.3	Asignación de recursos.....	35
3.4	Grado de adaptación e implantación de la normativa.....	37
4	CLASIFICACIÓN DE LOS FICHEROS POR NIVELES DE SEGURIDAD Y TRATAMIENTO DE FICHEROS ESPECIALMENTE SENSIBLES	40
4.1	Clasificación de los ficheros por niveles de seguridad	40
4.2	Tratamiento de datos habituales por parte de las entidades locales.....	43
4.2.1	Padrón de habitantes.....	43
4.2.2	Padrón de vehículos	44
4.2.3	Servicios sociales.....	45
4.2.4	Licencia de actividad de locales comerciales	46
4.2.5	Videovigilancia	46
5	INSCRIPCIÓN DE FICHEROS DE DATOS DE CARÁCTER PERSONAL, RESPONSABLE DE SEGURIDAD Y DOCUMENTO DE SEGURIDAD	48
5.1	Inscripción de ficheros	48
5.2	Responsable de Seguridad.....	51
5.3	Documento de Seguridad	54
5.3.1	Ámbito de aplicación del documento con especificación detallada de los recursos protegidos.....	54
5.3.2	Medidas, normas, procedimientos de actuación, reglas y estándares encaminados a garantizar el nivel de seguridad exigido en el RDLOPD.....	55
5.3.3	Funciones y obligaciones del personal en relación con el tratamiento de los datos de carácter personal incluidos en los ficheros inscritos.....	56
5.3.4	Estructura de los ficheros y la descripción de los sistemas de información que los tratan.....	57

5.3.5	Procedimientos de notificación, gestión y respuesta ante las incidencias que pudieran devenir.....	57
5.3.6	Procedimientos de realización de copias de respaldo y de recuperación de los datos en los ficheros o tratamientos automatizados.....	58
5.3.7	Medidas necesarias a adoptar para el transporte de soportes u documentos, así como para la destrucción de los documentos y soportes, o en su caso, la reutilización de estos últimos.....	59
6	LEGITIMACIÓN DE DATOS: INFORMACION, CONSENTIMIENTO, CESIÓN Y CONFIDENCIALIDAD	61
6.1	Deber de información sobre la finalidad del tratamiento del interesado	61
6.2	Deber de consentimiento del interesado para el tratamiento de los datos	62
6.3	Gestión de la cesión de datos.....	63
6.4	Confidencialidad de los datos	64
7	DERECHOS ARCO.....	66
7.1	Derecho de Acceso.....	66
7.2	Derecho de Rectificación	66
7.3	Derecho de Cancelación.....	67
7.4	Derecho de Oposición	67
8	MEDIDAS DE SEGURIDAD.....	69
8.1	Medidas de seguridad con controles de carácter técnico	69
8.1.1	Registro de incidencias.....	69
8.1.2	Identificación y autenticación	70
8.1.3	Control de acceso	75
8.1.4	Registro de accesos.....	78
8.1.5	Telecomunicaciones	81
8.2	Medidas de seguridad con controles de gestión.....	82

8.2.1	Gestión de soportes y documentos.....	82
8.2.2	Copias de respaldo y recuperación.....	87
8.2.3	Pruebas con datos reales	92
8.2.4	Auditoría.....	94
9	SUPERVISIÓN, INSPECCIONES, DENUNCIAS Y SANCIONES DERIVADAS DEL INCUMPLIMIENTO DE LA NORMATIVA DE PROTECCIÓN DE DATOS	97
9.1	Inspecciones	97
9.2	Denuncias y sanciones	98
10	LA OPINIÓN DE LOS EXPERTOS RESPECTO AL GRADO DE ADAPTACIÓN E IMPLANTACIÓN DE LA NORMATIVA	102
10.1	Niveles de madurez	103
10.1.1	Nivel 1 de madurez	104
10.1.2	Nivel 2 de madurez	107
10.1.3	Nivel 3 de madurez	109
10.2	Mejores Prácticas	112
10.2.1	Desde el punto de vista organizativo	112
10.2.2	Desde el punto de vista técnico	112
10.3	Ejemplos de casos de éxito en la aplicación de las buenas prácticas.....	113
10.3.1	Estructura, modelo de gestión y actuaciones específicas en materia de protección de datos: el Excmo. Ayuntamiento de Santa Cruz de Tenerife	114
10.3.2	Auditoría: el área de Coordinación de Auditoría y Seguridad de la Información de la Agencia Catalana de Protección de Datos	116
10.3.3	Consultoría: la Subdirección General de Registro de Ficheros y Consultoría de la Agencia de Protección de Datos de la Comunidad de Madrid.....	119
10.3.4	Estructura, modelo de gestión y actuaciones específicas en materia de protección de datos: el Instituto Municipal de Informática del Excmo. Ayuntamiento de Barcelona	124

11	CONCLUSIONES DEL ESTUDIO	127
12	PROPUESTAS Y RECOMENDACIONES DIRIGIDAS A LOS PODERES PÚBLICOS.....	133
12.1	Propuestas y recomendaciones en materia de concienciación y formación....	133
12.2	Propuestas y recomendaciones en materia de diagnóstico e información	134
12.3	Propuestas y recomendaciones en materia de financiación.....	135
12.4	Propuestas y recomendaciones en materia de normalización y certificación..	135
12.5	Propuestas y recomendaciones en materia de promoción e incentivación de los niveles de madurez y buenas prácticas	136
13	ANEXOS	138
13.1	Expertos participantes	138
13.2	Entidades participantes.....	140
13.2.1	Relación de Ayuntamientos	140
	ÍNDICE DE GRÁFICOS.....	147
	ÍNDICE DE TABLAS.....	150

PUNTOS CLAVE

I **Adaptación a la Ley Orgánica de Protección de Datos (LOPD) y al nuevo Reglamento de Desarrollo (RDLOPD) por las Entidades Locales**

La conclusión más relevante del estudio es el **mayor nivel de adaptación** a la LOPD y la RDLOPD que, en general, presentan las Entidades Locales (en adelante, EELL) en comparación con el tejido empresarial español, y en concreto, las pequeñas y medianas empresas¹.

Así, el nivel de cumplimiento de una de las principales obligaciones de la LOPD, como es la **declaración de ficheros** ante el Registro de la Agencia Española de Protección de Datos (AEPD), es del **46,4% en el caso de las EELL frente a un 16% en el caso de las PYME**.

Por otro lado, el **grado de conocimiento** del recientemente aprobado **RDLOPD** (Real Decreto 1720/2007) es de un **28% en los ayuntamientos frente a un 14% en las PYME españolas**. Analizando en detalle este aspecto es del **76%** en los **ayuntamientos de grandes municipios** frente a un 48% en los medianos y un 20% en los pequeños. En las **Diputaciones, Consells y Cabildos Insulares el porcentaje alcanza el 66,7%**.

Complementariamente, y a pesar del comportamiento heterogéneo de los gobiernos locales en función del tamaño del municipio, éstos cumplen un papel fundamental en la **difusión en la adaptación en la materia de protección de datos** entre los ciudadanos y sus trabajadores. Prueba de ello es que, a nivel global **un 74,8% de las EELL tienen un nivel elevado de concienciación**, para adecuarse a la planificación que exige la normativa. Este dato se traduce en un 75,9% para los ayuntamientos con grandes municipios tengan planificado la formación de sus trabajadores, frente a un 75,6% de los ayuntamientos de medianos municipios y un 74,5% de los de menor tamaño.

Otros aspectos que evidencian el nivel de adaptación y cumplimiento por las EELL en materia de protección de datos son los referidos al grado de asignación de recursos, a la legitimación de los datos y al procedimiento para el ejercicio de los derechos ARCO.

Respecto al **grado de asignación de recursos**, donde más del 21%, a nivel global, lo ha llevado a cabo. Reflejo de este esfuerzo económico y de recursos humanos, esta el hecho de que un 56,5% de los ayuntamientos con grandes municipios, un 31,1% de los ayuntamientos de medianos municipios y un 16,8% de los de menor tamaño tienen planificado esta asignación.

¹ En España, las PYME representan el 99,3% del total de empresas españolas (DIRCE 2006 Instituto Nacional de Estadística)

Por lo que respecta a la **legitimación de los datos**, el celo en su cumplimiento queda de manifiesto en el hecho de que, en relación con el deber de información, un 67,5% de los ayuntamientos a nivel global y un 72,2% de las Diputaciones, Consells y Cabildos Insulares afirman cumplir con este compromiso de información previo y expreso de la existencia del fichero, de su finalidad y de destinatarios de los datos. Sin embargo, este nivel de cumplimiento se puede ver solapado con el deber de recogida del consentimiento de los interesados, donde esta exigencia varía para cada estrato: 67% ayuntamientos con grandes municipios, un 43,4% de tamaño medio y un 33% para los organismos de pequeños municipios.

Por último la voluntad en el establecimiento de un **procedimiento para el ejercicio de los derechos** de acceso, rectificación, cancelación y oposición (**ARCO**) de las EELL, es determinante. Un 79% de los ayuntamientos con grandes municipios, un 58,1% de los ayuntamientos de medianos municipios y un 45,4% de los de menor tamaño lo tienen establecido. Para el caso de las Diputaciones, Consells y Cabildos Insulares la cifra se sitúa en un 52,8%.

Dos capítulos de especial importancia dentro de la normativa hacen referencia a las **medidas de seguridad**, que el RDLOPD establece como políticas específicas de seguridad y garantía de la privacidad, y a la potestad inspectora y sancionadora que se atribuye a las Agencias de Protección de Datos, tanto estatal como autonómicas.

El control de accesos se constituye como la medida de seguridad más extendida e implantada dentro de las EELL, alcanzando a nivel global un 70,4% de los ayuntamientos y el 91,7% de las Diputaciones, Consells y Cabildos Insulares. En todo caso, cabe señalar que la complejidad de las medidas hace que su cumplimiento por las Entidades sea diferente en función del tamaño de las mismas, percibiéndose para el conjunto de las medidas, un mayor grado de implantación en los ayuntamientos de mayor tamaño frente al potencial de crecimiento futuro en los de menor tamaño.

En último extremo, por lo que respecta al capítulo de **inspecciones, denuncias y sanciones**. Cabe señalar que a nivel global un 32,1% de los ayuntamientos afirman conocer las sanciones, mientras que un 95,7% declaran no haberlas sufrido. Por lo que respecta a las actividades de inspección hasta ahora el trabajo de las Agencias se ha venido centrando en las grandes entidades, de ahí la asimetría que el presente estudio demuestra respecto a las inspecciones sufridas entre las EELL de los distintos estratos.

II Niveles de madurez y análisis de mejores practicas

Los expertos participantes en el estudio clasifican las medidas de seguridad recogidas en el RDLOPD conforme a tres **niveles de madurez** que conducen, de manera progresiva, a la completa adaptación e implementación de la normativa. Estos niveles son:

- **Nivel 1:** Nivel incompleto de cumplimiento, que comprende las medidas más prioritarias a ejecutar por las EELL. Entre ellas se encuentran: la comunicación de las funciones y obligaciones del personal (37,5%), la realización de auditorías (34,8%) o la gestión de soportes y el registro de incidencias (ambas con un 33,3%).
- **Nivel 2:** Nivel legal de cumplimiento, que comprende todas las medidas de seguridad para conseguir la implantación de los requisitos del RDLOPD. Cabe señalar: el documento de seguridad (con el 62,5% de las valoraciones de los expertos), las telecomunicaciones (60,9%) y el registro de acceso (58,3%)
- **Nivel 3:** Nivel avanzado de cumplimiento, que comprende la gestión y mejora continúa de todas las medidas definidas en el RDLOPD y las buenas prácticas de su gestión. Se señalan como prioritarias: la identificación y autenticación (29,2%), las copias de respaldo (27,3%) y el control de acceso (25%).

Este modelo de madurez de los procesos de protección de datos personales debería solventar una de las principales dificultades de las Entidades como es la selección de prioridades para su adaptación a la Ley.

En relación con el **análisis de mejores prácticas**, los expertos consideran de gran interés y relevancia, trabajar en dos líneas de actuación: a) desde el punto de vista organizativo (por ejemplo, impartiendo sesiones de formación y concienciación a los funcionarios, personal laboral y colaboradores), y b) desde el punto de vista técnico (por ejemplo, facilitación del ejercicio de derechos a los ciudadanos y de capacitación de los trabajadores de la EELL).

III Recomendaciones

Las **líneas de actuación**, propuestas, son las siguientes:

- **Concienciación y formación.** La implantación efectiva de una cultura de protección de datos debería contar con programas estructurados de formación, particularizados y adaptados a las necesidades y peculiaridades de los empleados de las Entidades Locales, con una gran orientación práctica y con acciones continuadas de actualización.
- **Diagnóstico e información.** La implementación de las disposiciones normativas en materia de protección de datos de las Entidades debería contar con estadísticas e indicadores sobre el grado de adaptación a la normativa, a fin de que las entidades y Administraciones dispongan de información actualizada para poder poner en marcha acciones complementarias que permitan a las EELL alcanzar los plazos establecidos por la normativa vigente.

- Apoyo presupuestario. La insuficiencia financiera de las Entidades, que se puede ver agudizada por la pérdida de ingresos provenientes del desarrollo urbanístico, deberá apoyarse dando soporte a las necesidades derivadas de la implantación de nuevas medidas del RDLOPD, con ayudas y subvenciones directas de carácter finalista.
- Normalización y certificación. La implantación y utilización generalizada de la firma digital y sus certificados de atributos como sistema de identificación y autenticación segura es el medio idóneo para el control y verificación por el responsable del fichero de los accesos de los usuarios a los datos personales en las Entidades.
- Promoción e incentivación de los niveles de madurez y buenas prácticas. La implantación efectiva y acreditación de las mejores prácticas identificadas de seguridad de la información, como evidencia interna y frente a terceros siguiendo los esquemas de certificación internacional como el ISO IEC 27001 y 27002, contribuirán a la implantación de controles de cumplimiento normativo, en general, y de protección de datos, en particular, así como a las auditorias y revisiones por la Dirección.

El **papel de las Administraciones Públicas** será decisivo a la hora de destinar financiación, coordinando, armonizando y consolidando economías de escala, para las siguientes iniciativas sugeridas:

- Relativas a la concienciación y formación:
 - Realización de programas de difusión, divulgación y comunicación del nuevo RDLOPD.
 - Curso de formación y teleformación sobre medidas de protección de datos del nuevo RDLOPD.
- Relativas a la promoción e incentivación de los niveles de madurez y las mejores prácticas de protección de datos en las Entidades Públicas Locales:
 - Diagnóstico periódico realizado por alguna entidad independiente, del estado de la seguridad de datos en las Administraciones Locales.
 - La cobertura de los servicios de alguna entidad independiente a la que se le puedan plantear problemas, dudas o peticiones, que surgen a la hora de implantar las medidas de seguridad exigidas por la normativa.

1 INTRODUCCIÓN Y OBJETIVOS

1.1 Contexto y oportunidad del estudio

El presente informe, elaborado por el Instituto Nacional de Tecnologías de la Comunicación (en adelante, INTECO), tiene como objetivo principal la realización de un análisis, hasta hoy inédito en su extensión y profundidad, acerca de la situación actual de la protección de datos personales en las Entidades Públicas Locales en España.

Este trabajo proporciona un diagnóstico, completo y especializado, del grado de adopción de la legislación vigente, así como ofrece un conjunto de recomendaciones que han de permitir a las Administraciones la puesta en marcha de planes de regularización y adaptación a la normativa de protección de datos de carácter personal.

Para la elaboración del estudio se ha contado con la imprescindible colaboración de la Federación Española de Municipios y Provincias (en adelante, FEMP) y la participación de todos los responsables que intervienen en el ámbito de la seguridad de los datos de los Gobiernos Locales; es decir cargos políticos, responsables técnicos y personal administrativo de los Ayuntamientos, Diputaciones, Consells y Cabildos Insulares.

De particular interés y utilidad para alcanzar los objetivos perseguidos por el presente trabajo ha resultado la participación de las Agencias de Protección de Datos del Estado Español, representadas por la Agencia Española de Protección de Datos, como por las agencias con competencia autonómica como es el caso de la Agencia Catalana, la Agencia Vasca y la Agencia de Protección de Datos de la Comunidad de Madrid.

Por último, se ha contado con la opinión de un grupo de expertos en el ámbito de la industria, que han aportado su experiencia acerca de las mejores prácticas relacionadas con las medidas de seguridad exigidas, las prioridades en cuanto al cumplimiento de la normativa, así como las recomendaciones para una mejor adaptación de la normativa a la operativa y estructura de las EELL.

Los resultados del Estudio sobre la Seguridad de la Información y e-Confianza en el ámbito de las Entidades Locales², han puesto de manifiesto las dificultades para dar cumplimiento a la Ley 11/2007 de Acceso electrónico de los ciudadanos a los Servicios Públicos³.

² Estudio elaborado por el Observatorio de la Seguridad de la Información de INTECO en colaboración con la FEMP (www.inteco.es). Septiembre 2007.

³ LEY 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos. Disponible en http://www.map.es/iniciativas/mejora_de_la_administracion_general_del_estado/moderniza/Administracion_Electronica/parr_afo/05/document_es/A27150-27166.pdf

Esta norma, como es sabido, tiene entre sus finalidades la creación de las condiciones de confianza en el uso de las tecnologías, estableciendo las medidas necesarias para la preservación de la integridad de los derechos fundamentales y, en especial, los relacionados con la intimidad por medio de la garantía de seguridad de los sistemas, datos y comunicaciones.

Las Administraciones Públicas Locales, en consecuencia, deberán garantizar, a partir de 2010, el principio de igualdad y accesibilidad a los servicios prestados de manera electrónica, pero también la seguridad y la privacidad de los datos y de las comunicaciones con los ciudadanos y empresas.

De esta forma, el respeto a la normativa vigente de protección de datos se convierte en un asunto crítico para la aplicación efectiva de la Ley 11/2007 por los Gobiernos Locales, debido, fundamentalmente, a lo siguiente:

- Falta de realización de auditorías de cumplimiento.
- Ausencia de un documento de seguridad actualizado.
- Dificultades para la correcta gestión de los derechos de los propietarios de los datos.

Tal y como se puso de manifiesto en el estudio elaborado en el 2007:

- Estas prácticas de obligado cumplimiento, no se encuentran completamente implantadas en más del 50% de las Entidades Locales que fueron encuestadas, con especial incidencia, en los Ayuntamientos de municipios de tamaño más pequeño.
- Sólo uno de cada cuatro entes de los grandes municipios grandes cumplen las normas y prácticamente ninguno de ellos realiza auditorías sobre seguridad.

Parece oportuno, pues en este contexto, profundizar en el conocimiento detallado del estado actual de la protección de datos personales en las Entidades Locales españolas (en adelante EELL), completando este análisis global con la situación de protección y control del acceso a sus ficheros no automatizados con datos de carácter personal de los ciudadanos y las empresas.

1.2 Objetivos del estudio

El **objetivo general** del estudio es la elaboración de un análisis sobre la situación actual de las Entidades Locales Públicas en España en relación con la normativa de protección de datos de carácter personal, en una doble vertiente:

- Diagnóstico, tanto del estado actual de cumplimiento efectivo de la legislación como del nivel de preparación para la adecuación a las exigencias previstas en el RDLOPD por las EELL en España.
- Concienciación y sensibilización a las EELL para que estas incrementen la tasa de cumplimiento de la normativa sobre protección de datos. Para ello el proyecto abarca la publicación del presente informe y de una Guía básica para la adaptación de las Entidades Locales a la normativa sobre protección de datos. La guía elaborada en base a los resultados de la investigación cuantitativa y cualitativa, tiene como objetivo formar a los responsables que intervienen en el ámbito de la seguridad de los datos de los Gobiernos Locales (cargos políticos, responsables técnicos y personal administrativo de los Ayuntamientos, Diputaciones, Consells y Cabildos Insulares), sobre la necesidad de la protección de datos, facilitar pautas para la adaptación a la normativa, concienciar acerca de los beneficios derivados de la implementación y remover las potenciales barreras que están frenando su adopción.

Esta Guía, además, pretende servir de herramienta para:

- Mejorar la comprensión de la LOPD y el nuevo Reglamento de aplicación de Medidas de Seguridad utilizando un lenguaje cercano al destinatario, la pequeña y mediana Entidad Local.
- Facilitar la adopción tanto de la LOPD como del RDLOPD.
- Difundir los beneficios derivados de su implantación.

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

- Evaluar el grado de implantación de las medidas legales y operativas de seguridad de los datos personales en las EELL.
- Analizar los recursos organizativos y su disponibilidad dado que actualmente intervienen en los procedimientos de seguridad legal y su posible evolución futura.
- Conocer la previsión de actuaciones de implantación de medidas para el cumplimiento de las disposiciones actuales y futuras del RDLOPD.
- Definir y proponer las mejores prácticas para la adaptación a la LOPD, tanto de carácter técnico como organizativo, con el enfoque de ser útiles para impulsar una mejora relevante de las medidas de seguridad en las Entidades Locales de manera independiente a su tamaño y situación actual.

- Definir y proponer niveles de madurez de cumplimiento a partir de la clasificación de las medidas de seguridad, para facilitar la identificación de prioridades y la preparación de “hojas de ruta” por parte de las Entidades Locales como ayuda para alcanzar la adaptación plena a la normativa.
- Identificar y describir ejemplos de experiencias exitosas en la aplicación de las buenas prácticas respecto de actividades o medidas concretas reguladas por la normativa de protección de datos de carácter personal.
- Establecer recomendaciones que permitan a las Entidades Locales Públicas y a aquellas Administraciones Públicas que tutelan o que puedan contribuir a la adopción de las medidas de seguridad, la puesta en marcha de planes de regularización y adaptación a la normativa.

1.3 **Ámbito normativo y marco de referencia**

La protección de datos es una exigencia legal que se define en España a través de:

- La **Ley Orgánica 15/1999 de protección de datos de carácter personal**⁴ (en adelante, LOPD), al tener por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor, intimidad y privacidad personal y familiar. Esta ley adoptó el ordenamiento español a lo dispuesto por la Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995, relativa a la protección de las personal físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de los mismos.
- El **Reglamento de Medidas de Seguridad de los ficheros automatizados** aprobado mediante el Real Decreto 994/1999⁵ (en adelante, RMS). Este reglamento a pesar de haber sido sustituido por el RDLOPD se ha tomado como referencia al ser la normativa que a priori todas las EELL tenían que tener asumida e implantada. De esta forma el análisis del cumplimiento de los parámetros que establecía esta norma sirve de auditoria para evaluar el grado de cumplimiento de a las medidas de seguridad para la protección de los ficheros automatizados que contengan datos de carácter personal.

⁴ LEY ORGÁNICA 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Disponible en <http://www.boe.es/boe/dias/1999/12/14/pdfs/A43088-43099.pdf>

⁵ REAL DECRETO 994/1999, de 11 de junio, por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal. Disponible en <http://www.boe.es/boe/dias/1999/06/25/pdfs/A24241-24245.pdf>

- El Real Decreto 1720/2007 por el que se aprueba el **Reglamento de Desarrollo de la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal**⁶ (en adelante, RDLOPD) cuya entrada en vigor fue el 19 de abril de 2008. Permite determinar el estado actual de preparación de las EELL para dar respuesta a las nuevas medidas y su extensión a los ficheros no automatizados.

El fin de la LOPD es proteger la intimidad y la privacidad de las personas físicas, constituyéndose en un derecho fundamental, frente a la vulneración de tales derechos por parte de las EELL en la recogida y el tratamiento de sus datos personales.

Derivados de dicho derecho, se reconoce a las personas una serie de facultades en relación con sus datos personales que toda organización que los trate debe respetar, y se imponen una serie de obligaciones formales y sustantivas que las Entidades Públicas Locales, así como el sector privado, deben cumplir.

En caso contrario dichas acciones, derivadas de una incorrecta interpretación o implantación de la Ley, pueden llegar a suponer una sanción económica impuesta por las Agencias de Protección de Datos del Estado Español, representadas por la Agencia Española de Protección de Datos, como por las agencias con competencia autonómica como es el caso de la Agencia Catalana, la Agencia Vasca y la Agencia de Protección de Datos de la Comunidad de Madrid.

No obstante el cumplimiento de la ley por parte de las EELL a pesar de ser una obligación para las mismas, genera también beneficios asociados a la implantación y adecuación a la normativa como son:

- La formalización de unas medidas de seguridad que benefician, no sólo al interesado, sino al encargado del tratamiento.
- La implantación de protocolos de actuación que ante diversas situaciones habituales en el devenir cotidiano, contribuyen a la mejora y rapidez en la respuesta ante las mismas, lo que genera una fortaleza de las EELL.
- El cumplimiento de la normativa de protección de datos personales supone ofrecer una imagen de control, eficacia y orden de los documentos y datos que son tratados en las EELL.

En relación con el RDLOPD, éste nace con la vocación de resolver cuestiones interpretativas que existían en la LOPD, desarrollar los mandatos contenidos en ella,

⁶ REAL DECRETO 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. Disponible en <http://www.boe.es/boe/dias/2008/01/19/pdfs/A04103-04136.pdf>

dotar de coherencia a toda la regulación reglamentaria existente hasta entonces, actualizar la aplicación de esta norma de alto rango, adecuando su desarrollo a las prácticas y riesgos actuales y para sustituir el RMS. El RDLOPD presenta importantes novedades, entre las que destacan las siguientes:

- Afecta tanto al tratamiento automatizado, como al no automatizado de los datos personales.
- Fija el criterio en materia de cómputo de plazos, evitando distinciones que suponen diferencias de trato de los ficheros públicos respecto de los privados.
- Establece la regulación del modo de captación del consentimiento.
- Determina el cambio de nivel de protección de determinados datos personales.
- Deja fuera de su aplicación los tratamientos referidos a las personas jurídicas y a los datos de personas físicas que presten sus servicios en aquellas.
- Amplía los datos objeto de tratamiento como Fuentes Accesibles al Público.
- Establece la figura del encargado de tratamiento.
- Desarrolla la forma de ejercitar los derechos de los afectados: acceso, rectificación, cancelación y oposición.
- Fija un procedimiento a seguir en las transferencias internacionales de datos.
- Se aplica también a los ficheros y tratamientos no automatizados (papel) y se fijan criterios específicos sobre las medidas de seguridad de los mismos.
- Se garantiza que las personas, antes de consentir que sus datos sean recogidos y tratados, puedan tener un pleno conocimiento de la utilización que se vaya a hacer de estos datos.
- Permite al interesado disponer de un medio sencillo y gratuito para ejercitar su derecho de acceso, rectificación, cancelación y oposición, sin tener que usar correo certificado ni otros medios que le supongan un gasto adicional.
- Cambian el nivel de seguridad de los datos derivados de la violencia de género que pasan del nivel básico a tener un nivel alto.

Respecto al **periodo de adaptación** establecido en la normativa depende del nivel de seguridad de los datos y del tipo de ficheros. Así para los ficheros automatizados que

existieran en la fecha de entrada en vigor del reglamento (recordemos el 19 de abril de 2008):

- Un año para las medidas de seguridad de nivel medio de los siguientes ficheros: los que sean responsables las entidades gestoras y servicios comunes de la Seguridad Social y se relacionen con el ejercicio de sus competencias; los que sean responsables las mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social; aquellos que contengan un conjunto de datos de carácter personal que ofrezcan una definición de las características o de la personalidad de los ciudadanos y que permitan evaluar determinados aspectos de la personalidad o del comportamiento de los mismos, respecto de las medidas de este nivel que no fueran exigibles conforme a lo previsto en el artículo 4.4 del RMS.
- Un año desde el 19 de abril de 2008 para las medidas de seguridad de nivel medio de los siguiente ficheros: los que contengan datos derivados de la violencia de género; los que sean responsables los operadores que presten servicios de comunicaciones electrónicas disponibles al público o exploten redes públicas de comunicaciones electrónicas respecto a los datos de tráfico y a los datos de localización.
- Un año y medio desde el 19 de abril de 2008 para las medidas de seguridad de nivel alto de los mismos ficheros que en el epígrafe anterior.
- Un año para todas aquellas medidas no previstas en el RMS de los ficheros automatizados de datos de carácter personal pero que con el RDLOPD se exijan.

Para los ficheros no automatizados:

- Los plazos de adaptación son de 1 año para los ficheros de nivel básico, 18 meses para los de nivel medio y de 2 años para los de nivel alto.

Y por último, los ficheros, tanto automatizados como no automatizados, creados con posterioridad a la fecha de entrada en vigor del RDLOPD deberán tener implantadas, desde el momento de su creación la totalidad de las medidas de seguridad reguladas en el mismo.

1.4 Entidades participantes

1.4.1 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 con un doble objetivo: 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 y Calidad de Software.

Más Información: <http://www.inteco.es>

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 tiene por objetivo 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.

Más información: <http://observatorio.inteco.es>

1.4.2 Federación Española de Municipios y Provincias

La Federación Española de Municipios y Provincias (FEMP), es una asociación de gobiernos locales que agrupa Ayuntamientos, Diputaciones, Consells y Cabildos Insulares, en total más de 7.200 municipios. Tiene como objetivos, fines fundacionales y estatutarios los siguientes:

- El fomento y la defensa de la autonomía de las Entidades Locales.
- La representación y defensa de los intereses generales de los Ayuntamientos, Diputaciones, Consells y Cabildos Insulares ante otras Administraciones públicas.
- La prestación de toda clase de servicios a las Entidades Locales.
- El desarrollo y consolidación del espíritu europeo en el ámbito local, basado en la autonomía y solidaridad entre todos las Entidades Locales.
- La promoción y fomento de las relaciones de amistad y cooperación con los Ayuntamientos, Diputaciones, Consells y Cabildos Insulares y sus organizaciones en el ámbito internacional, especialmente el europeo, el iberoamericano y el árabe.
- La gestión de programas del Gobierno destinados al área local.

Más información: <http://www.femp.es>

2 DISEÑO METODOLÓGICO

2.1 Descripción

La ejecución del proyecto ha combinado diferentes metodologías, con el propósito de alcanzar los objetivos establecidos para el presente proyecto, abordadas de forma secuencial:

- **Búsqueda de fuentes de información** de carácter totalmente primario basado en la obtención de una visión completa del estado actual de la protección de datos personales en el ámbito de las Entidades Públicas Locales.
- **Entrevistas a expertos** procedentes de las EELL, de la industria y de otras Administraciones Públicas. Para ello, se ha contado con la colaboración de las agencias de protección de datos, tanto la estatal como las autonómicas.
- **Encuestas a personal laboral, funcionarios, responsables políticos y colaboradores en las Entidades Locales**, centradas en todos los aspectos de la seguridad de datos de carácter personal.
- **Elaboración del presente informe** donde se recogen el análisis y conclusiones de las fases anteriores, junto con las propuestas y recomendaciones de actuación.

2.2 Ficha técnica de la fase cualitativa: entrevistas a expertos

El objetivo de esta fase es doble: por un lado, el enriquecimiento de los cuestionarios, aportando información de interés sobre los niveles de madurez que las entidades tienen, en opinión de estos profesionales, con las medidas de seguridad que para la gestión de los procesos de cumplimiento de la LOPD y del RDLOPD han de tener en cuenta; por otro, la importancia que le otorgan a diez buenas prácticas relacionadas con la implantación efectiva de las medidas de seguridad establecidas en la normativa.

En esta fase se ha contado con la participación de **25 expertos** (profesionales y representantes de instituciones) pertenecientes a **diversas áreas de conocimiento**. Para la recogida de información se han realizado 13 entrevistas semiestructuradas⁷ presenciales y 12 cuestionarios autoaplicados. La selección de los expertos⁸ se realizó a partir de unos ámbitos de representatividad y de unos perfiles profesionales que permitiera garantizar el enfoque integral y la cobertura de diferentes puntos de vista:

⁷ Consiste en un proceso de comunicación dinámica entre dos personas, entrevistador y entrevistado, bajo el control del primero. El objetivo que persigue es obtener información lo más implicadora posible sobre el objeto de análisis que se plantea.

⁸ En el Anexo 13.1 se incluye un listado con los profesionales que han participado en el estudio

- Experiencia de gestión y/o técnica en el ámbito de las entidades públicas.
- Especialización en protección de datos.
- Responsabilidad en la planificación y gestión de los sistemas de información y comunicaciones.
- Representatividad en los distintos niveles de las Entidades Públicas Locales, ya sean Ayuntamientos, Diputaciones o Consells y Cabildos Insulares.

Las entrevistas fueron realizadas entre los días 14 de marzo de 2008 y el 2 de abril de 2008.

2.3 Ficha técnica de la fase cuantitativa: entrevistas a personal laboral, funcionarios, responsables políticos y colaboradores en las Entidades Locales

Para llevar a cabo esta fase del trabajo de campo se ha elaborado un marco estadístico de referencia de la encuesta que ha servido como fuente de información para el resto del estudio. Este marco se ha enfocado principalmente a:

- El Ayuntamiento, Diputación, Consell y Cabildo Insular como elemento estadístico individual. Para ello, se ha obtenido la muestra para la realización de las encuestas a partir de la Relación de Municipios del Instituto Nacional de Estadística (INE)⁹ sobre la base de 17 Comunidades y 2 Autónomas, 8.112 Ayuntamientos y 63 Diputaciones, Consells y Cabildos Insulares.
- El otro elemento individual afectado en el marco del estudio ha sido el individuo profesional de las Entidades Locales.

A continuación y una vez seleccionada la muestra, se han trazado los objetos de análisis cualitativos, complementados con variables provenientes del análisis cuantitativo que se ha aplicado a cada una de las Entidades. Posteriormente se ha realizado una segmentación por Comunidades Autónomas, por Provincias y por número de habitantes del municipio en el caso de los Ayuntamientos.

La elaboración de los cuestionarios se ha realizado con carácter previo al trabajo de campo, tanto para los expertos como para los responsables de las EELL. Y por ese motivo se han elaborado dos tipos de cuestionarios diferentes:

⁹ Instituto Nacional de Estadística. Relación de municipios y códigos por provincias. Disponible en <http://www.ine.es/inebase/cji/um?M=%2Ft20%2Fe245%2Fcodmun%2F&O=inebase&N=&L=0>

- Un cuestionario dirigido a los **Ayuntamientos de municipios de más de 5.000 habitantes**, así como a las **Diputaciones, Consells y Cabildos Insulares**, con un total de 45 preguntas.
- Un cuestionario simplificado para **Ayuntamientos de municipios de menos de 5.000 habitantes** con 25 preguntas. La elaboración de este cuestionario simplificado ha fomentado la participación de EELL que, por su menor tamaño, no tienen la misma disponibilidad que una entidad mayor.

2.3.1 Tamaño y distribución muestral

El estudio ha contado con la **participación de 601 Entidades Públicas Locales**, del conjunto de encuestas 91 son de procedencia anónima¹⁰, 474 corresponden a Ayuntamientos y 36 son Diputaciones, Consells y Cabildos Insulares, y de 24 expertos.

Procedimiento de muestreo para Ayuntamientos

La muestra de Ayuntamientos se ha definido de manera segmentada de acuerdo con el número de habitantes del municipio, estableciéndose 9 estratos¹¹ tal y como aparece en la Tabla 1.

Tabla 1: Estratificación poblacional

Estrato	Nº Habitantes	Nº Habitantes (tablas de resultados)	Tipo de Municipio
A	Mas de 500.000 habitantes	Mas de 500	Grandes Municipios
B	De 100.000 a 500.000 habitantes	De 100 a 500	
C	De 50.000 a 100.000 habitantes	De 50 a 100	
D	De 10.000 a 50.000 habitantes	De 10 a 50	Medianos Municipios
E	De 5.000 a 10.000 habitantes	De 5 a 10	
F	De 2.000 a 5.000 habitantes	De 2 a 5	
G	De 1.000 a 2.000 habitantes	De 1 a 2	Pequeños Municipios
H	De 500 a 1.000 habitantes	De 0'5 a 1	
I	Menos de 500 habitantes	Menos de 0'5	

Fuente: INTECO

Análisis de participación

Tras la toma de contacto con las muestras representativas seleccionadas, el envío de cuestionarios a las distintas Entidades Públicas Locales, las entrevistas a expertos y su

¹⁰ Los cuestionarios anónimos no se han tenido en cuenta para el presente diagnóstico y análisis de la situación, dado que no se pueden estratificar.

¹¹ El tamaño muestral correspondiente a los estratos de los municipios de mayor tamaño (estratos A y B: aquellos de más de 100.000 hab.) determina un mayor error muestral en los datos resultantes del estudio de estos grupos en particular. Por ello, se puede apreciar una mayor variabilidad en los resultados porcentuales del análisis de conceptos de estos estratos que en el resto.

posterior análisis, los resultados arrojan una participación muy satisfactoria por parte de todos ellos.

La **participación por Comunidades Autónomas** cuyos municipios han colaborado en la encuesta, ofrecen algunos datos significativos en cuanto a la segmentación por municipios. Así la tasa de respuesta media ha sido de un 43,6% (474) sobre los municipios del premuestro seleccionado (1.086), lo que supone una **cobertura absoluta del 5,8% del total de municipios españoles** (8.112). Los índices más significativos de respuesta, según refleja la Tabla 2, se distribuyen de la siguiente manera:

- La más alta cobertura sobre el conjunto de la población de la provincia se sitúa en Murcia (26,7%), Canarias (18,2%), Madrid (15,1%) y Asturias (con 14,1%).
- La participación de Castilla y León es relevante pues el 69,8% de los participantes han participado en el estudio. Esta tasa de respuesta es también elevada para Navarra (60,9%) y Aragón con el 58,3%.

Tabla 2: Participación de entidades locales por Comunidades Autónomas sobre la premuestra y la cobertura poblacional

Comunidad Autónoma	Nº Municipios	Premuestra: Nº Municipios	Muestra: Nº Municipios	Participación sobre premuestra	Cobertura sobre población
Andalucía	770	183	71	38,8%	9,2%
Aragón	730	36	21	58,3%	2,9%
Asturias	78	25	11	44,0 %	14,1%
Baleares	67	22	5	22,7%	7,5%
Canarias	88	50	16	32,0%	18,2%
Cantabria	102	19	9	47,4%	8,8%
Castilla y León	2.249	96	67	69,8%	2,9%
Castilla-La Mancha	919	69	33	47,8%	3,6%
Cataluña	946	161	64	39,8%	6,8%
C. Valenciana	542	140	54	38,6%	9,9%
Extremadura	383	28	15	53,6%	3,9%
Galicia	315	82	32	39,0%	10,2%
Madrid	179	60	27	45,5%	15,1%
Murcia	45	31	12	38,7%	26,7%
Navarra	272	23	14	60,9%	5,1%
P. Vasco	251	46	16	34,8%	6,4%
La Rioja	174	13	7	53,8%	4,0%
Ceuta y Melilla	2	2	0	0,0%	0,0%
TOTAL	8.112	1.086	474	43,6%	5,8%

Fuente: INTECO

La **participación por estratos** ha sido también muy significativa (véase Tabla 3), lo que ha permitido obtener información sobre el grado de aplicación de la Ley Orgánica de Protección de Datos (LOPD) según la densidad poblacional de los Ayuntamientos.

La cobertura sobre todo el conjunto de población es más alta en los municipios con mayor población, como resultado de la composición de número de habitantes por municipio en España. Como se aprecia, el número de municipios en España con menos de 50.000 habitantes es 7.945; 137 de ellos tienen más de 50.000 habitantes y 61 de los municipios, 100.000 habitantes o más. En cuanto al reparto de la población, del total nacional (45.200.737 habitantes), 17.927.461 personas vienen en los 61 municipios con más de 100.000 habitantes, lo que representa que un 39,7% de la población vive en el 0,8% de los municipios. Esto indica una gran concentración de la población en núcleos grandes, lo que se confirma por el dato de que 6.800 Ayuntamientos (el 83,8%) pertenecen a municipios de menos de 5.000 habitantes. Esta estructura facilita y confirma que la participación de las grandes entidades poblacionales es muy alta., dado que los Ayuntamientos participantes de municipios de más de 50.000 habitantes cubren más del 51,7% de la población total, y en el caso de los de 50.000 a 100.000 habitantes la cobertura sobre la población de los participantes es de hasta un 12%.

Tabla 3: Participación de entidades por estratos sobre la premuestra de municipios y la cobertura poblacional

Estr	Nº habitantes (miles)	Nº municipios	Premuestra: Nº Municipios	Muestra: Nº Municipios	Participación sobre la premuestra	Cobertura poblacional
A	Más de 500	6	6	3	50,0%	50,0%
B	De 100 a 500	55	53	25	47,2%	45,5%
C	De 50 a 100	76	75	39	52,0%	51,3%
D	De 10 a 50	648	584	137	23,5%	21,1%
E	De 5 a 10	527	58	33	56,9%	6,3%
F	De 2 a 5	1.016	86	67	77,9%	6,6%
G	De 1 a 2	923	80	59	73,8%	6,4%
H	De 0'5 a 1	1.054	57	38	66,7%	3,6%
I	Menos de 0,5	3.807	87	73	83,9%	1,9%
	TOTAL	8.112	1.086	474	43,6%	5,8%

Fuente: INTECO

La **participación por Diputaciones, Consells y Cabildos Insulares** ha sido relevante, siendo 36 las entidades participantes sobre un total de 57, lo que representa una participación del 63,2% de esta tipología de gobiernos locales en el estudio.

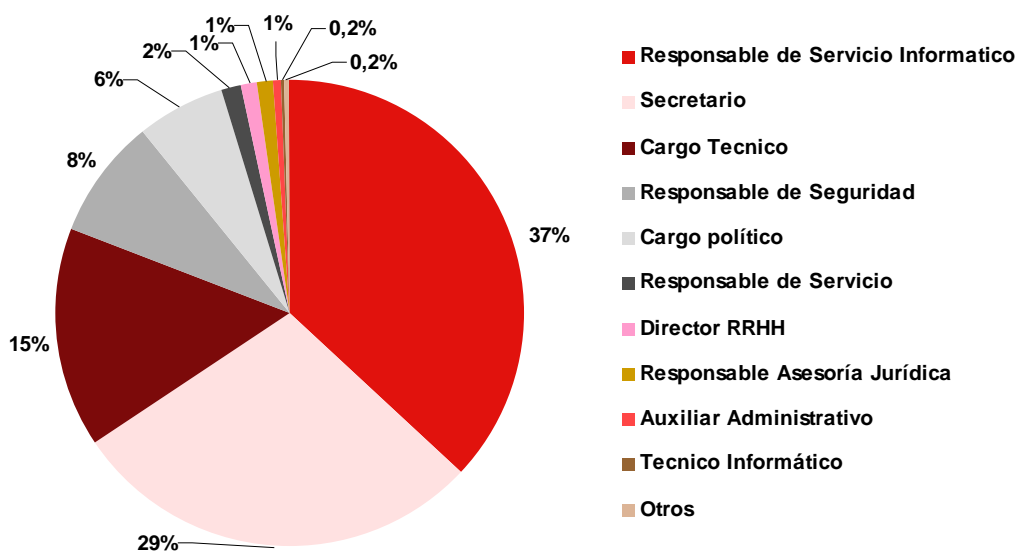
La **participación por perfil del profesional participante** que ha respondido al cuestionario en las Entidades Públicas Locales ha sido diverso, tal y como representa como el Gráfico 1, en lo referente a: la categoría o perfil profesional de la persona entrevistada y al porcentaje de participantes activos por perfil.

De acuerdo con los resultados obtenidos el perfil profesional del participante que ha contestado mayoritariamente al cuestionario es un responsable informático, con un 42,8% de participación, debido a que habitualmente resultan ser los expertos a los que se

encomienda implantar las medidas de seguridad. En segundo lugar, los cuestionarios han sido completados por los Secretarios de las Entidades, con un 25%, como responsables técnicos de los asuntos legales. Los cargos políticos y los concejales o diputados delegados han tenido una participación menor con un 4,3% y 1,6% respectivamente.

Sin embargo, el porcentaje de respuestas obtenidas por parte de la figura del Responsable de Seguridad de las entidades, ha sido de un 7%, factor este indicativo de la falta de nombramiento específico de esta importante figura en las entidades.

Gráfico 1: Perfil de los profesionales participantes en las encuesta como representantes de las EELL participantes (%)



Fuente: INTECO

Ponderación

Se ha realizado una ponderación estratificada por el número de habitantes de los municipios de acuerdo con los datos poblacionales antes mencionados del INE.

Asimismo y debido a las desviaciones entre la muestra obtenida y la teórica, la muestra total se ha tenido que equilibrar hasta cuatro veces:

- Sobre el total de la muestra y para cada uno de los estratos, se ha realizado dos tipos de ponderaciones en función de la muestra total de municipios que participan en cada uno de los cuestionarios antes mencionados.
 - Por un lado sobre una muestra obtenida de 474 municipios para la muestra teórica basada en las respuestas a los dos cuestionarios antes mencionados (Tabla 4).

Tabla 4: Distribución muestral por estrato, y coeficiente de ponderación para las entidades locales que han contestado el cuestionario ampliado sobre el total de la muestra participante (%)

Estr	Nº habitantes (miles)	Nº municipios	Distribución porcentual por municipio	Muestra: Nº Municipios	Distribución porcentual sobre la muestra	Coeficiente ponderación
A	Más de 500	6	0,07%	3	0,6%	11,7%
B	De 100 a 500	55	0,68%	25	5,3%	12,9%
C	De 50 a 100	76	0,94%	39	8,2%	11,4%
D	De 10 a 50	648	7,99%	137	28,9%	27,6%
E	De 5 a 10	527	6,50%	33	7,0%	93,3%
F	De 2 a 5	1.016	12,52%	67	14,1%	88,6%
G	De 1 a 2	923	11,38%	59	12,4%	91,4%
H	De 0'5 a 1	1.054	12,99%	38	8,0%	162,1%
I	Menos de 0,5	3.807	46,93%	73	15,4%	304,7%
TOTAL		8.112	100,00%	474	100,0%	

Fuente: INTECO

- Por otro, sobre una muestra obtenida de 226 municipios para la muestra teórica basada en el cuestionario simplificado (Tabla 5).

Tabla 5: Distribución muestral por estrato, y coeficiente de ponderación para las entidades locales que han contestado el cuestionario simplificado sobre el total de la muestra participante (%)

Estr	Nº habitantes (miles)	Nº municipios	Distribución porcentual por municipio	Muestra: Nº Municipios	Distribución porcentual sobre la muestra	Coeficiente ponderación
A	Más de 500	6	0.26%	3	1,3%	19,4%
B	De 100 a 500	55	2.36%	25	11,1%	21,4%
C	De 50 a 100	76	3.26%	39	17,3%	18,9%
D	De 10 a 50	648	27.84%	126	55,8%	49,9%
E	De 5 a 10	527	22.64%	25	11,1%	204,6%
F	De 2 a 5	1.016	43.64%	8	3,5%	1232,9%
TOTALES		2.328	100,00%	226	100,0%	

Fuente: INTECO

- Sobre el tamaño de los estratos y para el tipo de municipio, es decir para los ayuntamientos de los grandes, medianos y pequeños municipios. En este caso también se han realizado dos tipos de ponderaciones en función del tamaño de la muestra.
 - Sobre tres muestras independientes que representan a los ayuntamientos por estrato (137, 237 y 170) para la muestra teórica basada en las respuestas al cuestionario ampliado (Tabla 6).

Tabla 6: Distribución muestral por estrato, y coeficiente de ponderación para las entidades locales que han contestado el cuestionario ampliado sobre el tamaño (%)

Estr	Nº habitantes (miles)	Nº municipios	Distribución porcentual por municipio	Muestra: Nº Municipios	Distribución porcentual sobre la muestra	Coeficiente ponderación
A	Más de 500	6	0,04%	3	0,04%	0,9%
B	De 100 a 500	55	0,40%	25	0,37%	1,1%
C	De 50 a 100	76	0,55%	39	0,58%	0,9%
TOTAL		137		67		
D	De 10 a 50	648	0,29%	137	0,57%	0,5%
E	De 5 a 10	527	0,24%	33	0,13%	1,7%
F	De 2 a 5	1.016	0,46%	67	0,28%	1,6%
TOTAL		2.191		237		
G	De 1 a 2	923	0,16%	59	0,35%	0,5%
H	De 0'5 a 1	1.054	0,18%	38	0,22%	0,8%
I	Menos de 0,5	3.807	0,66%	73	0,43%	1,5%
TOTAL		5.784		170		

Fuente: INTECO

- o Sobre dos muestras independientes correspondiente a los ayuntamientos de grandes y medianos municipios (67 y 159) basada en las respuestas al cuestionario simplificado (Tabla 7).

Tabla 7: Distribución muestral por estrato, y coeficiente de ponderación para las entidades locales que han contestado el cuestionario simplificado sobre el tamaño (%)

Estr	Nº habitantes (miles)	Nº municipios	Distribución porcentual por municipio	Muestra: Nº Municipios	Distribución porcentual sobre la muestra	Coeficiente ponderación
A	Más de 500	6	0,04%	3	0,04%	0,9%
B	De 100 a 500	55	0,40%	25	0,37%	1,1%
C	De 50 a 100	76	0,55%	39	0,58%	0,9%
TOTAL		137		67		
D	De 10 a 50	648	0,29%	26	0,79%	0,4%
E	De 5 a 10	527	0,24%	25	0,16%	1,5%
F	De 2 a 5	1.016	0,46%	8	0,05%	9,2%
TOTAL		2.191		159		

Fuente: INTECO

En ambos casos y con el objetivo de alcanzar un ajuste más perfecto, las variables que se han tenido en cuenta para elaborar estas ponderaciones han sido el número de encuestas por municipios por CCAA y las variables de cuota (es decir al tipo de municipio). Las muestras obtenidas presentan los coeficientes de ponderación asignados como subgrupo de la muestra total. No obstante, las dos muestras representan el grupo de entidades locales analizadas y participantes en la fase cuantitativa.

En definitiva, los datos que se analizan a lo largo del presente estudio a nivel global y por tamaño de los mismos (grandes, medianos y pequeños municipios) hay que interpretarlos como resultado de la ponderación anteriormente descrita.

2.3.2 Método de recogida de información

Para facilitar la accesibilidad y respuesta de los cuestionarios, se han realizado las siguientes acciones:

- Envío por correo electrónico, con el cuestionario adjunto, para su remisión vía fax, correo electrónico u ordinario.
- Habilitación de los cuestionarios en Internet, con certificado seguro tipo SSL, para su respuesta en línea.
- Colaboración de la Federación Española de Municipios y Provincias, la cual realizó una invitación masiva de participación a los Ayuntamientos de municipios de menos de 50.000 habitantes.

Por otra parte, los ficheros de los datos de contacto de los Gobiernos y expertos se han confeccionado y tratado conforme a la legislación vigente de protección de datos personales. Procediéndose al registro de ficheros en la Agencia Española de Protección de Datos, la inclusión del aviso legal en todas las comunicaciones efectuadas y la facilitación de los derechos a los usuarios para acceder, rectificar, cancelar u oponerse al registro de los mismos.

A partir de la información recopilada en las encuestas realizadas se procedió al tratamiento de los datos recibidos, tanto cuantitativos como cualitativos, y se han presentado bajo tres criterios de segmentación:

- Geográfica: Comunidades Autónomas y Provincias.
- Densidad poblacional de los municipios, para los Ayuntamientos.
- Grupo de análisis: expertos y encuestas.

2.3.3 Trabajo de campo

Ha sido realizado entre el **6 de febrero y el 30 de mayo de 2008**.

2.3.4 Error de muestreo

El método de selección muestral se ha realizado de manera estratificada, determinándose el tamaño de la misma mediante la fórmula correspondiente a una población finita, en la que se ha estimado un **margen de error de $\pm 4,42\%$ para un nivel de confianza del 95%**.

3 CONOCIMIENTO, CONCIENCIACIÓN Y ASIGNACIÓN DE RECURSOS CONFORME A LA NORMATIVA VIGENTE

Este apartado muestra el nivel de conocimiento, concienciación y asignación de recursos que conforme a la normativa vigente de protección de datos tienen las entidades locales. A los efectos del 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 EELL.

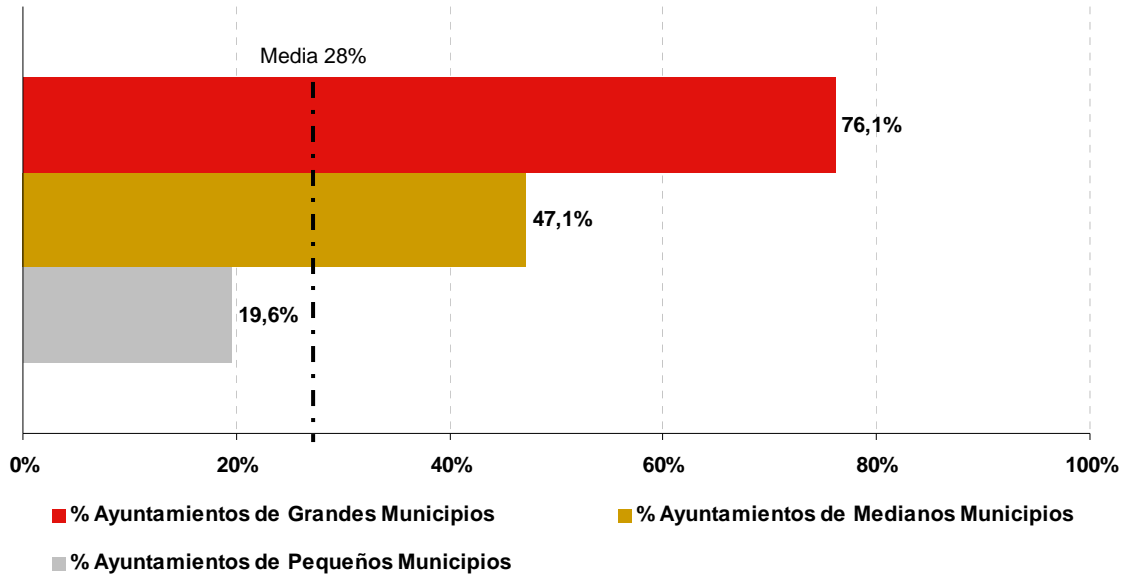
3.1 Nivel de conocimiento del RDLOPD en las EELL

El primer paso que las entidades tienen que tener para adecuarse a lo estipulado por la ley ha de ser realizar un completo y detallado inventario de todos los ficheros con datos de carácter personal con los que cuenten en el uso de sus funciones. Es decir, los que recabe, gestione, almacene y puedan ser objeto de cesión por parte de la Entidad, comprendiendo tanto a ficheros automatizados como no automatizados, independientemente del soporte físico en el que sean almacenados dichos datos.

Entre las EELL que han participado en este estudio, un 66,7% de las Diputaciones, Consells y Cabildos Insulares y sólo un 28% de las mismas afirman conocer el RDLOPD frente a un 61% de los ayuntamientos que manifiestan desconocerlo. La explicación de tan elevado desconocimiento puede deberse a que un 11,7% de los participantes afirmen ser responsables de seguridad en sus entidades y por consiguiente las EELL no tengan convenientemente adaptada la normativa.

Por estratos la situación como se puede ver en el Gráfico 2 varía. Así mientras que el 76,1% de los ayuntamientos de grandes municipios responden afirmativamente, en el resto de los ayuntamientos considerados –medianos y pequeños– el nivel de conocimiento es inferior a un 48% y a un 20% respectivamente.

Gráfico 2: Nivel de conocimiento del alcance, la entrada en vigor y los plazos de implantación disponibles en la normativa de protección de datos por tamaño (%)



Fuente: INTECO

Un análisis en profundidad para cada uno de los municipios muestra que, los que tienen más de 500.000 habitantes poseen un conocimiento pleno de la publicación del RDLOPD. Así como en los que se encuentran por debajo del estrato de los Ayuntamientos de 10.000 a 50.000 habitantes se supera el 55,5% de municipios con conocimiento suficiente de esta normativa. Y los municipios de pequeño tamaño en especial en aquellos de menos de 500 habitantes, un 21,9% afirma conocerlo.

Tabla 8: Conocimiento del nuevo reglamento (RDLOPD), por tamaño (%)

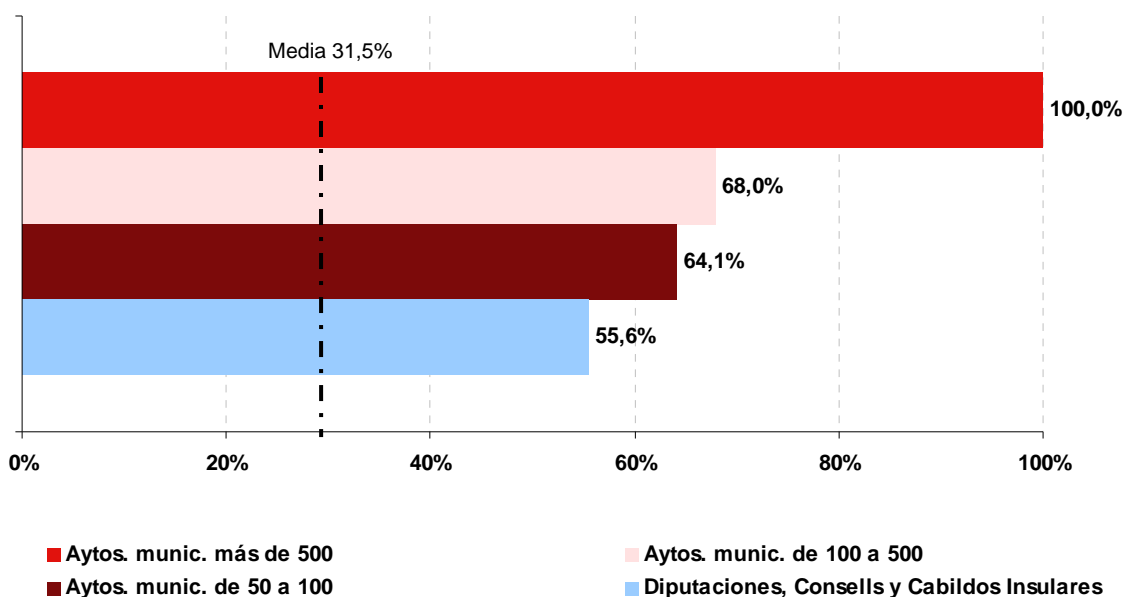
Población (en miles)	Distribución porcentual			Distribución media ponderada			
	SI	NO	NS/NC	SI	NO	NS/NC	
Grandes	Más de 500	100,0%	0,0%	0,0%			
	De 100 a 500	68,0%	32,0%	0,0%	67,2%	28,5%	4,3%
	De 50 a 100	64,1%	28,2%	7,7%			
Medianos	De 10 a 50	55,5%	32,1%	12,4%			
	De 5 a 10	39,4%	51,5%	9,1%	44,6%	43,3%	12,1%
	De 2 a 5	40,3%	46,3%	13,4%			
Pequeños	De 1 a 2	37,3%	57,6%	5,1%			
	De 0,5 a 1	28,9%	55,3%	15,8%	25,7%	63,4%	10,9%
	Ayts. munic. menos 0,5	21,9%	67,1%	11,0%			
Diputaciones, Consells y Cabildos Insulares		55,6%	30,6%	13,9%			

Fuente: INTECO

Además de conocer en qué consiste toda la normativa, las entidades locales deben afrontar las medidas específicas para los ficheros no automatizados. Por este motivo se les ha preguntado sobre el conocimiento de las referentes al tratamiento, almacenamiento, destrucción y acceso de los ficheros de archivos en papel.

Dicho conocimiento en los ayuntamientos de los grandes municipios es diverso aunque puede ser considerado como positivo. Se puede comprobar, en el Gráfico 3, que en los Ayuntamientos de municipios de más de 500.000 habitantes el conocimiento es pleno, mientras que en el resto está bastante extendido. Así, en aquellos núcleos de 100.000 a 500.000 habitantes afirman conocerlo el 66,7% de sus gobiernos, seguidos por lo de poblaciones de 50.000 a 100.000 habitantes (64,1%). Las Diputaciones, Consells y Cabildos Insulares presentan también un conocimiento elevado sobre las medidas de seguridad establecidas en el nuevo reglamento (55,6%).

Gráfico 3: Conocimiento de las nuevas medidas de seguridad para ficheros no automatizados del RDLOPD en Ayuntamientos de grandes municipios y en Diputaciones, Consells y Cabildos Insulares (%)



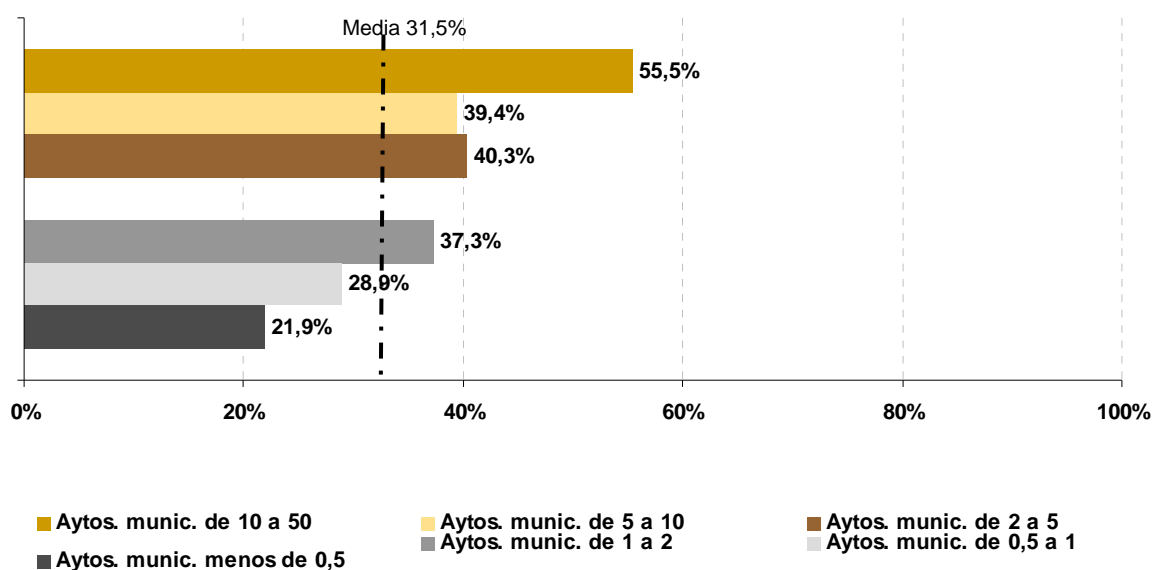
Fuente: INTECO

Por otro lado, en los Ayuntamientos de municipios de tamaño reducido, el grado de conocimiento se va reduciendo en función del tamaño del municipio, como se aprecia en el Gráfico 4, salvo en el caso de los gobiernos de localidades de 2.000 a 5.000 habitantes (40,3%) donde el número de municipios que afirman conocer la nueva normativa no sigue esta evolución.

Además en los gobiernos de todos los núcleos de entre 10.000 a 50.000 habitantes se dan indicadores de conocimiento superior al 50% (en concreto un 55,5%). Es en los

Ayuntamientos más pequeños, aquellos de menos de 2.000 habitantes, donde las medidas de seguridad para los ficheros no automatizados son menos conocidas, con datos de entre el 21,9% y el 37,3% para cualquier estrato de estos municipios. Esto supone que por ejemplo, en el caso de los municipios de menos de 500 habitantes, el 78,1% no tiene conocimiento de que el nuevo Reglamento defina medidas de seguridad para los ficheros de datos personales en papel.

Gráfico 4: Conocimiento de las medidas de seguridad para ficheros no automatizados del RDLOPD en pequeños y medianos municipios (%)



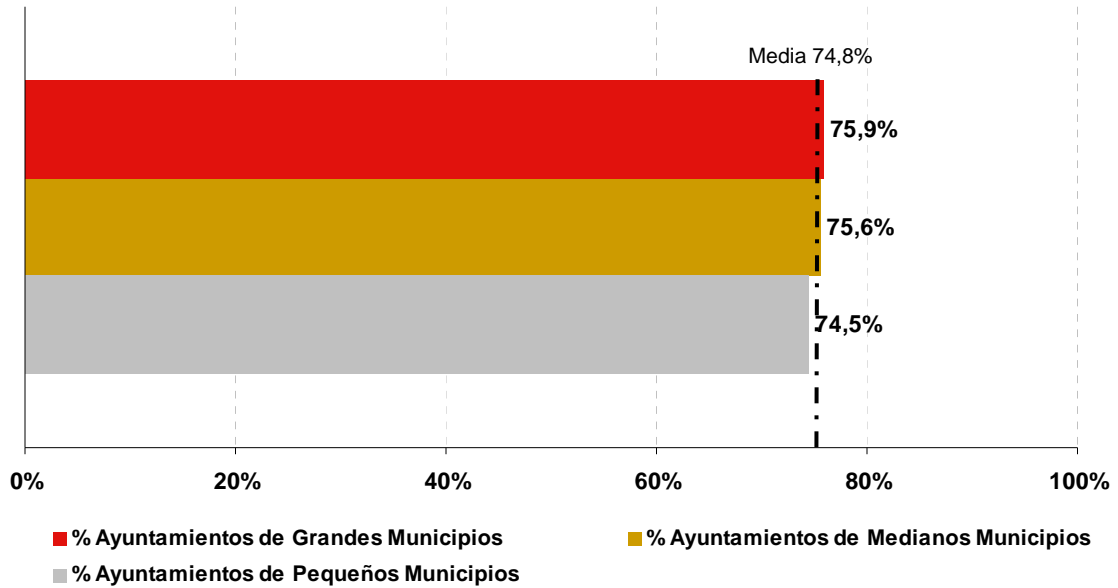
Fuente: INTECO

3.2 Nivel de concienciación respecto del cumplimiento de la normativa de protección de datos

Cualquier persona que trabaje en una EELL, con independencia de su puesto, debe conocer las normas de seguridad que afecten al desarrollo de sus funciones, en particular al tratamiento de datos personales que pueda realizar, siendo el responsable del fichero la persona que garantice esta medida, utilizando el modo de difusión que considere más adecuado.

A nivel global un 74,8% de las EELL cumple con esta labor, porcentaje similar al que presentan los ayuntamientos de los grandes, medianos y pequeños municipios si nos fijamos en el Gráfico 5.

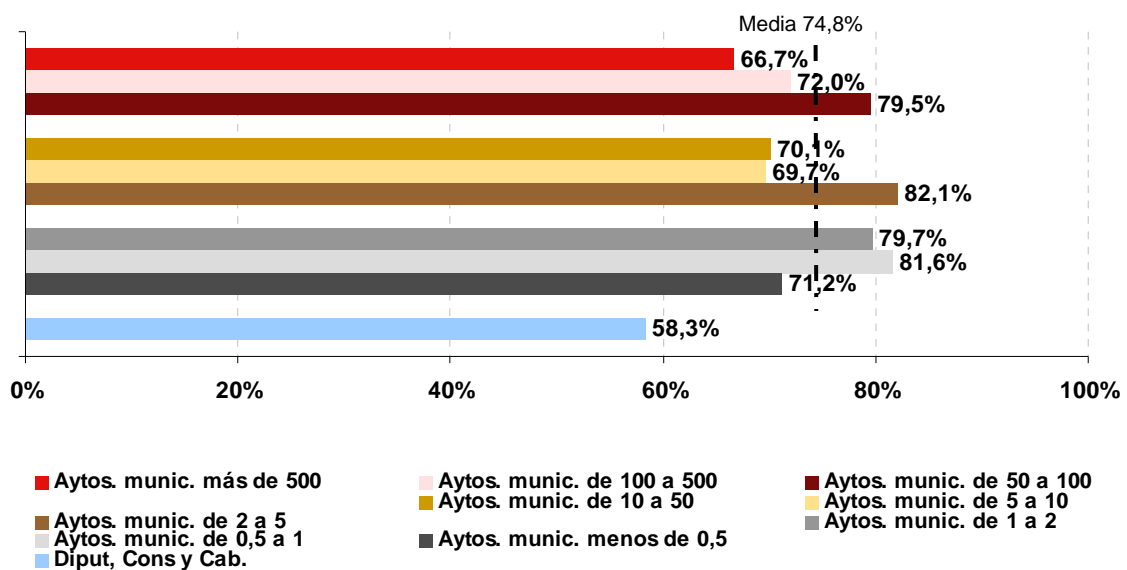
Gráfico 5: Difusión a los trabajadores de las funciones y obligaciones respecto al tratamiento de los datos personales entre los ayuntamientos por tamaño (%)



Fuente: INTECO

Adicionalmente y si se realiza un análisis en profundidad de las respuestas de las entidades (Gráfico 6), se observa que el tamaño del municipio no influye.

Gráfico 6: Difusión a los trabajadores de las funciones y obligaciones respecto al tratamiento de los datos personales por tamaño del municipio (%)



Fuente: INTECO

Como se muestra en el Gráfico 6, los municipios que más cobertura le otorgan son los de 2.000 a 5.000 donde el 82,1% de municipios lo realizan. En el otro extremo se encuentran los de más de 500.000 habitantes con tan sólo el 66,7% y el 58,3% de las Diputaciones, Consells y Cabildos Insulares.

En este sentido, es importante que las Entidades Públicas Locales dispongan de un calendario de cumplimiento para la adaptación al RDLOPD en los plazos establecidos (ver epígrafe 1.3), por lo que se ha preguntado sobre la asignación de recursos como indicador de su adecuada planificación.

3.3 Asignación de recursos

El hecho de que sólo un 21,4% de las entidades locales participantes en el estudio hayan realizado la asignación, constituye una prueba del esfuerzo que estos organismos han de llevar a cabo para poder adecuarse a la planificación. Un análisis por estrato y tamaño del mismo, nos muestra un irregular grado de cumplimiento de esta obligación. Así el 56,5% de los ayuntamientos con grandes municipios tienen planificado dicha asignación, frente a un 31,1% de los ayuntamientos de medianos municipios y un 16,8% de los de menor tamaño (Tabla 9).

Por otra parte, un análisis en detalle sobre el grado de respuesta por tamaño de los municipios, nos muestra tal y como se puede comprobar en la siguiente tabla que los estratos con menor número de habitantes son los que menos preparados están, debido a que solamente un 12,3% de municipios de menos de 500 habitantes tienen ya planificado su proceso de adaptación al nuevo Reglamento.

La planificación de la adaptación al nuevo Reglamento está establecida en los Ayuntamientos de municipios de entre 50.000 y 500.000 habitantes (entre el 54,2% y el 61,5%), mientras que sólo 1 de cada 3 Gobiernos Locales de núcleos de más de 500.000 habitantes lo realiza.

Ahora bien, es una práctica de adaptación desigual por Entidades Locales de municipios entre 2.000 y 50.000 habitantes (22,4%-44%) y disminuye sensiblemente en el caso de los Ayuntamientos más pequeños (12,3%-30%).

Evidentemente estos resultados están condicionados por el conocimiento del RDLOPD analizado al principio de este epígrafe (ver 3.1).

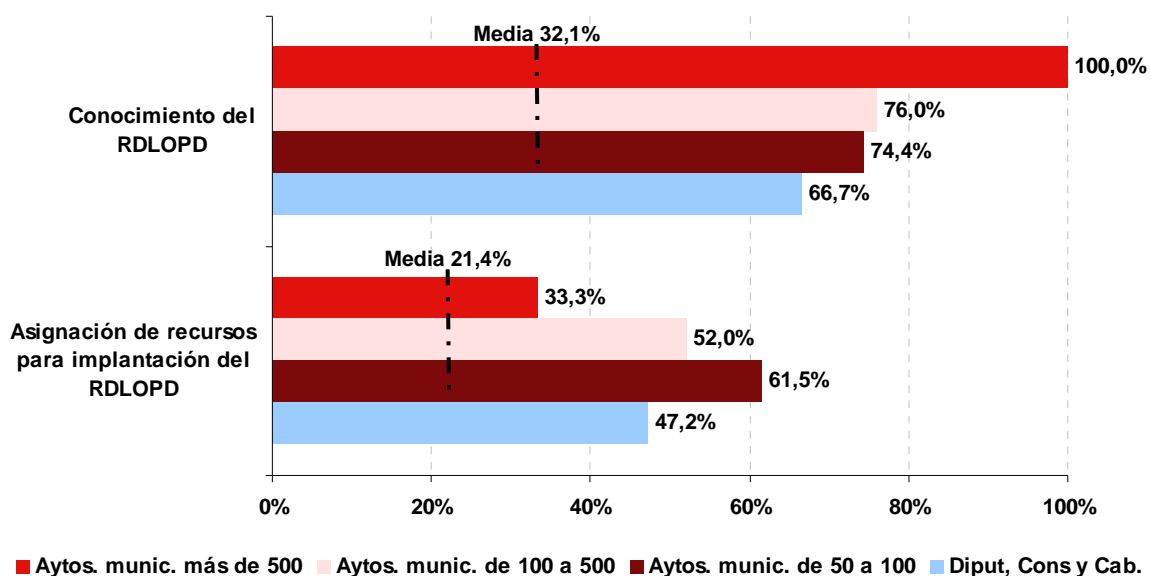
Tabla 9: Nivel de planificación en la asignación de recursos para la adecuación a las medidas definidas en el RDLOPD por tamaño (%)

Población (en miles)		Distribución porcentual			Distribución media ponderada		
		SI	NO	NS/NC	SI	NO	NS/NC
Grandes	Más de 500	33,3%	33,3%	33,3%	56,5%	34,6%	8,9%
	De 100 a 500	52,0%	40,0%	8,0%			
	De 50 a 100	61,5%	30,8%	7,7%			
Medianos	De 10 a 50	43,1%	38,7%	18,2%	31,1%	48,7%	20,2%
	De 5 a 10	33,3%	45,5%	21,2%			
	De 2 a 5	22,4%	56,7%	20,9%			
Pequeños	De 1 a 2	30,5%	55,9%	13,6%	16,8%	71,4%	11,8%
	De 0,5 a 1	21,1%	65,7%	13,2%			
	Aytos. Munic. menos 0,5	12,3%	76,7%	11,0%			
Diputaciones, Consells y Cabildos Insulares		47,2%	30,6%	22,2%			

Fuente: INTECO

Comparando los resultados (ver Gráfico 7 y Gráfico 8) se comprueba que aquellos municipios que declaran conocer el RDLOPD, tienen un elevado porcentaje de planificación para su adaptación.

Gráfico 7: Conocimiento del RDLOPD vs, nivel de la planificación de recursos para la adecuación en grandes ayuntamientos y Diputaciones, Consells y Cabildos Insulares (%)



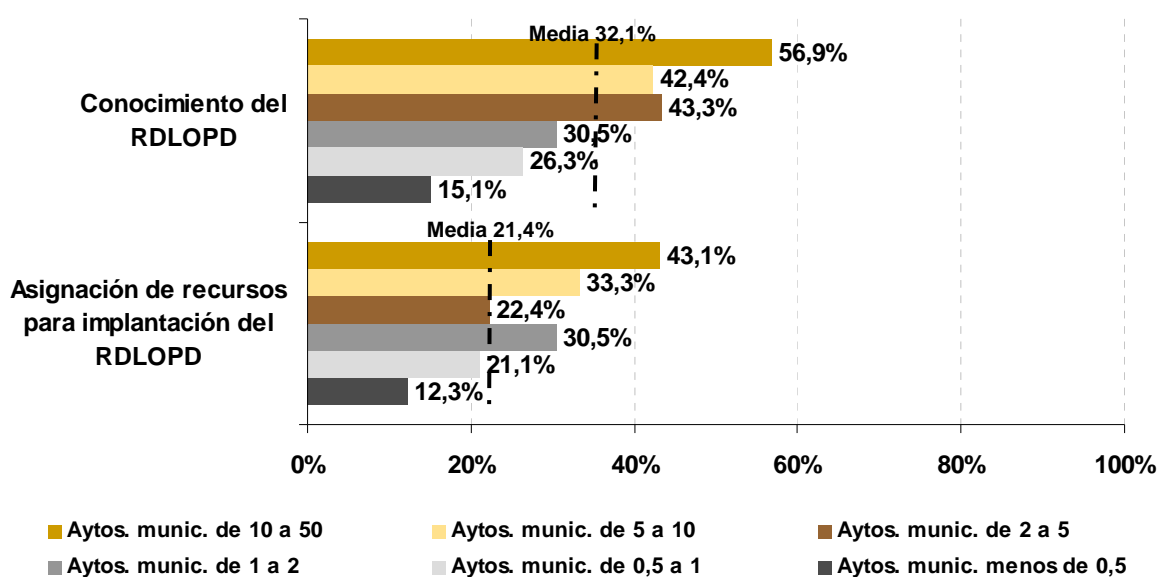
Fuente: INTECO

Por ejemplo, los estratos de 100.000 a 500.000 y de 50.000 a 100.000 habitantes tienen un 76% y un 74,4% de conocimiento, respectivamente, y un 52% y 61,5% de asignación

de recursos. Sin embargo los municipios de más de 500.000 habitantes tienen un 100% de conocimiento y tan solo un 33,3% de asignación de recursos.

Para los municipios con menor número de habitantes la situación se mantiene estable entre los que conocen la normativa y asignan recursos para su adecuación (Gráfico 8). Salvo en el caso del estrato 1.000 a 2.000 habitantes, donde los municipios que afirman conocerlo y haberlo planificado es idéntico (30,5%).

Gráfico 8: Conocimiento del RDLOPD vs, nivel de la planificación de recursos para la adecuación en pequeños y medianos municipios (%)



Fuente: INTECO

3.4 Grado de adaptación e implantación de la normativa

Una vez analizados los datos sobre el nivel de conocimiento y concienciación de la ley y el reglamento y el nivel de planificación para la asignación de recursos en las entidades locales, el estudio refleja en este apartado el porcentaje de organismos que han implementado medidas técnicas u organizativas para proteger los datos de carácter personal. De esta forma, se ofrece una visión de los porcentajes de EELL que cuentan con políticas y procedimientos de seguridad. Estos procedimientos son:

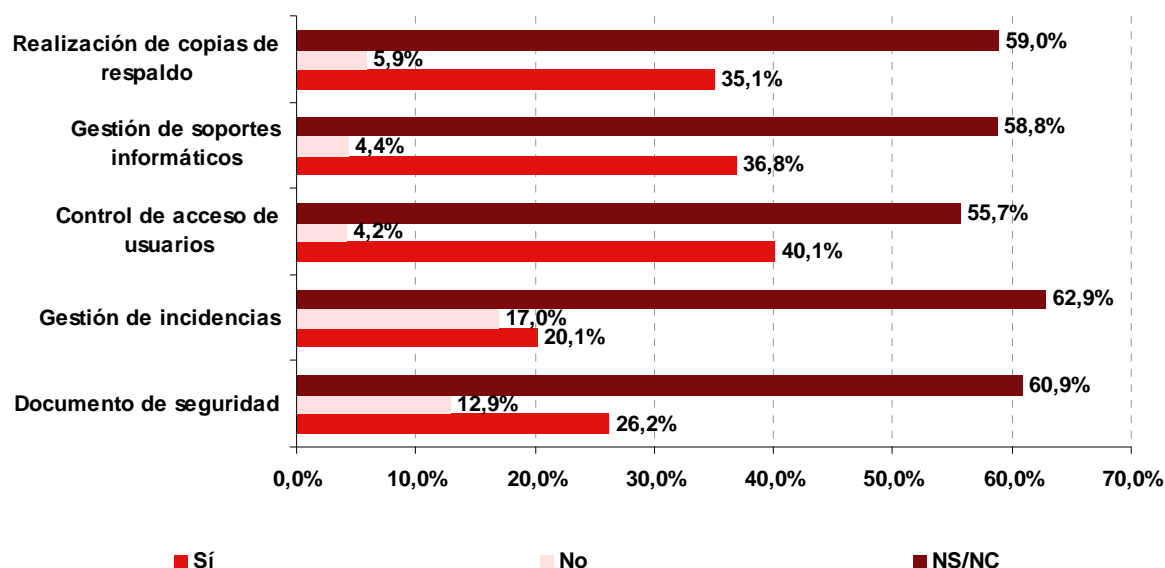
- Existencia del documento de seguridad.
- Gestión de incidencias.
- Control de acceso de usuarios.
- Gestión de soportes informáticos.

- Realización de copias de respaldo.

Como se puede ver en el siguiente gráfico (Gráfico 9) la mayoría de entidades no ha respondido a esta pregunta o desconocen su situación, con porcentajes superiores al 55%, por lo que los niveles de adaptación pudieran no ser un fiel reflejo de la situación.

En el lado opuesto, entre los que han respondido, destaca el establecimiento por el 40,1% de los ayuntamientos de un control de acceso de usuarios seguido por la gestión de soportes informáticos y la realización de copias de respaldo (ambas desarrolladas respectivamente por el 36,6% y el 35,1% de las entidades locales).

Gráfico 9: Tipología de medidas técnicas u organizativas adoptadas por los ayuntamientos para proteger los datos de carácter personal (%)



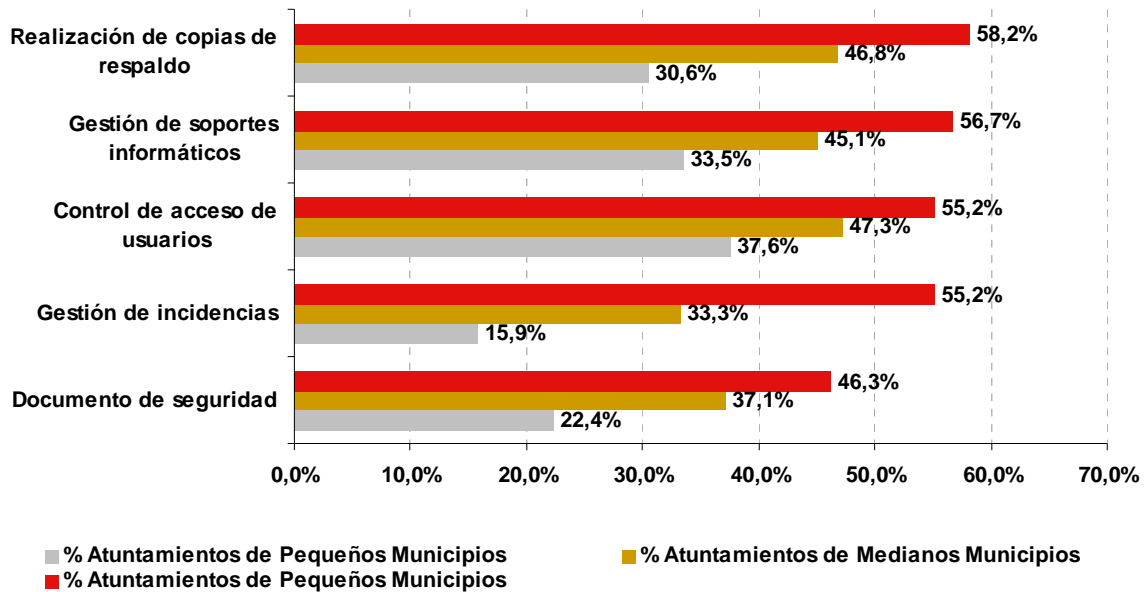
Fuente: INTECO

A pesar del bajo porcentaje de participación, se puede ver en el siguiente Gráfico 10 como se reparte la realización efectiva de estas políticas por tamaño del estrato. Del total de participantes en el estudio son los grandes municipios los que más llevan a la práctica el establecimiento de estos procedimientos de seguridad especificados en la normativa (entre un 58,2% y un 46,3%). Esto puede ser posible dado que este tipo de ayuntamientos son los que cuentan con mayor volumen de ficheros y de recursos técnicos u organizativos que permitan el desarrollo de estas políticas.

Entre los pequeños municipios, el porcentaje de entidades que llevan a cabo el establecimiento de los procedimientos varía entre un 47,3% de ayuntamientos que tienen un sistema de control de acceso de usuarios y un 33,3% de organismos que realizan una gestión de incidencias.

Por último, el volumen de municipios pequeños que realiza estas políticas es más variable y escaso. Así un 37,6% de los mismos realiza el control de acceso de usuarios y por el contrario sólo un 15,9% lleva a cabo la gestión de incidencias.

Gráfico 10: Tipología de medidas técnicas u organizativas adoptadas por las entidades para proteger los datos de carácter personal por tamaño (%)



Fuente: INTECO

4 CLASIFICACIÓN DE LOS FICHEROS POR NIVELES DE SEGURIDAD Y TRATAMIENTO DE FICHEROS ESPECIALMENTE SENSIBLES

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.

4.1 Clasificación de los ficheros por niveles de seguridad

Esta clasificación implica el establecimiento de medidas de seguridad de forma acumulativa atendiendo al tipo de dato de carácter personal a proteger y teniendo la consideración de mínimos legales exigibles. Así, en caso del tratamiento de ficheros de nivel medio, deberán implantarse todas y cada una de las medidas de seguridad descritas para el nivel básico y las del nivel medio. Igualmente sucederá con los ficheros de nivel alto, que deberán implantar las medidas descritas para el nivel básico, el medio y el alto.

Tabla 10: Niveles de Seguridad

NIVEL BÁSICO	NIVEL MEDIO	NIVEL ALTO
<ul style="list-style-type: none"> • Nombre, apellidos, DNI, teléfono, domicilio, nº cta bancaria. • Los referidos a ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual, cuando los datos se utilicen únicamente con la finalidad de realizar una transferencia dineraria a las entidades de las que los afectados sean miembros. • Los ficheros no automatizados que de forma incidental contengan datos especialmente protegidos • Los ficheros cuyo tratamiento tenga como finalidad el cumplimiento de deberes públicos, en el caso de datos como el grado de minusvalía o la declaración de la condición de invalidez. 	<ul style="list-style-type: none"> • Comisión de infracciones administrativas o penales. • Aquello de los que sean responsables Administraciones tributarias y se relacionen con el ejercicio de sus potestades tributarias. • Ficheros de entidades gestoras, servicios comunes de la Seguridad Social, mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social. • Hacienda pública (datos relativos a tributos u otras obligaciones fiscales que trata la administración –no los relativos a los impuestos que declaran las empresas-). • Datos que permitan deducir el comportamiento de los ciudadanos. 	<ul style="list-style-type: none"> • Ideología o afiliación sindical. • Religión o creencias. • Origen racial o étnico. • Salud (servicios sociales, necesidad de atención médica especial). • Vida sexual. • Recogidos para fines policiales sin consentimiento del interesado. • Violencia de género.

Fuente: INTECO

En cualquier caso, se ha considerado que la clasificación de los ficheros de datos personales constituye, sin duda alguna, un indicador de una adecuada concienciación y aplicación de la normativa por las Entidades Locales. Por ese motivo y a modo de

evaluación del conocimiento de la adecuada clasificación por niveles en las Entidades, se han seleccionado seis tipos de ficheros con datos personales, que habitualmente tratan, a saber:

- Actividades culturales, educativas y deportivas.
- Gestión de expedientes administrativos.
- Cementerio.
- Ayudas y subvenciones.
- Archivo histórico.
- Biblioteca municipal.

Respecto a los que en opinión de las entidades participantes, predomina el uso de datos con un nivel de seguridad básico con porcentajes superiores al 68% (ver Tabla 11). No obstante, se evidencia una heterogeneidad en las respuestas según los niveles de seguridad asignados para cada tipo de fichero, para los casos de cultura, cementerio, archivo y biblioteca, pero la respuesta no es unánime para el resto. Así existen algunas entidades clasifican estos ficheros como de nivel alto. El resto de tipos de datos, expedientes y ayudas, tienen un porcentaje de clasificación de nivel bajo del 68 y 68,8% respectivamente. Siendo los porcentajes de clasificación de nivel medio, 24,6% y 24% para este tipo de archivos.

Tabla 11: Clasificación de niveles de seguridad definidos en el RDLOPD de los datos que contienen los ficheros de carácter personal que los Ayuntamientos disponen (%)

Tipo de ficheros	Nivel Básico	Nivel Medio	Nivel Alto	No sabe
Actividades culturales, educativas y deportivas	89,8%	6,6%	0,9%	2,7%
Gestión de expedientes administrativos	68,0%	24,6%	5,8%	1,7%
Cementerio	81,7%	10,8%	0,6%	6,9%
Ayudas y subvenciones	68,8%	24,0%	3,4%	3,8%
Archivo histórico	79,5%	12,2%	3,7%	4,6%
Biblioteca municipal	86,9%	5,0%	0,3%	7,8%

Fuente: INTECO

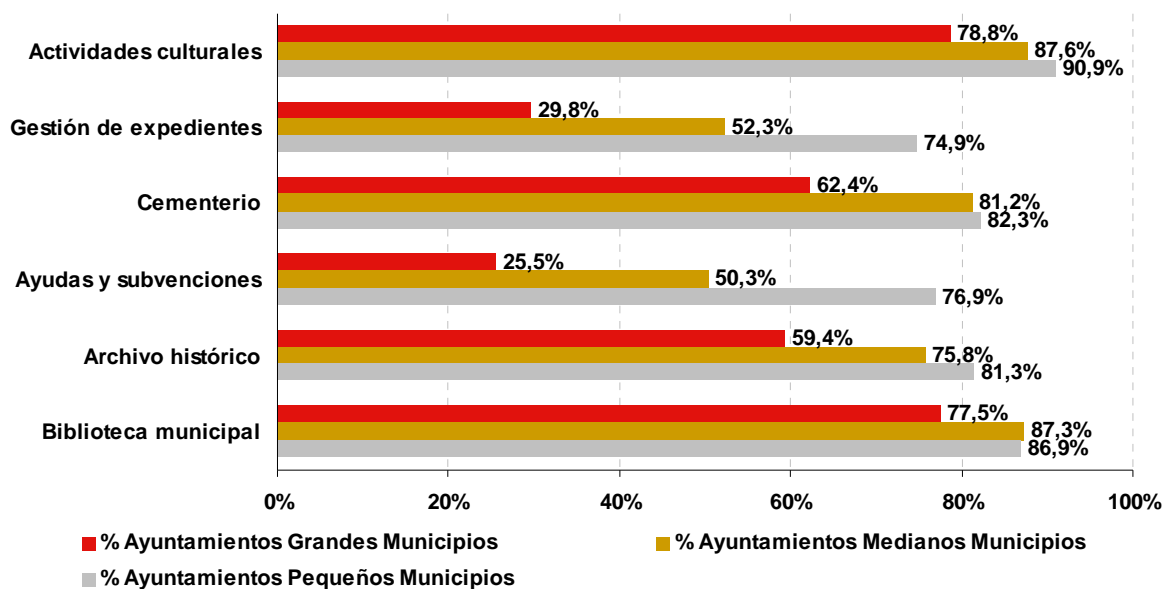
Un análisis en profundidad de los tipos de datos que tienen un nivel alto de seguridad sobre el grado de respuesta en función del tamaño del estrato (Gráfico 11), nos muestra que son los ayuntamientos de pequeños municipios los que les otorgan un mayor nivel con porcentajes de entidades que varían entre un 90,9% de organismos que se lo dan a los ficheros de actividades culturales, educativas y deportivas y un 74,9% de ayuntamientos que se lo conceden a los de gestión de expedientes.

Entre los ayuntamientos de medianos municipios los porcentajes de entidades que les confieren un nivel alto de protección a los ficheros identificados es similar. La excepción está en el hecho de que el número de entidades que proporcionan este nivel es inferior en el caso de los ficheros de gestión de expedientes y el de ayudas y subvenciones (con un 52,3% y un 50,3% respectivamente).

Por último las entidades de grandes municipios son los que dan un menor nivel de protección a los datos de carácter personal que contienen estos dos tipos de ficheros (29,8% y un 25,5%).

Es preciso matizar, llegados a este punto, que cuando se les preguntaba a los encuestados por los expedientes administrativos no se puntualizaba en ninguno específico, por lo que este motivo podría explicar el escaso porcentaje de ayuntamientos, con independencia del tamaño del estrato aunque sea inferior la categorización, que otorgan una clasificación alta. No obstante, estos son de aplicación general a cualquier servicio que se preste.

Gráfico 11: Tipología de datos clasificados de nivel alto que contienen los ficheros de de carácter personal que las Entidades disponen, por tamaño (%)



Fuente: INTECO

En el caso de las Diputaciones, Consells y Cabildos Insulares la clasificación de niveles de seguridad para estos ficheros es más heterogénea a pesar de que el número de estas entidades es inferior con respecto al de los ayuntamientos. La excepción nuevamente está en los casos de los ficheros de gestión de expedientes administrativos y de ayudas y subvenciones donde la valoración de nivel alto es superior que en el resto de archivos.

Tabla 12: Clasificación de niveles de seguridad definidos en el RDLOPD de los datos que contienen los ficheros de carácter personal que las Diputaciones, Consells y Cabildos Insulares disponen (%)

Tipo de ficheros	Nivel Básico	Nivel Medio	Nivel Alto	No sabe
Actividades culturales, educativas y deportivas	80,6%	13,9%	2,8%	2,8%
Gestión de expedientes administrativos	38,9%	44,4%	11,1%	5,6%
Cementerio	63,9%	0%	5,6%	30,6%
Ayudas y subvenciones	47,2%	36,1%	13,9%	2,8%
Archivo histórico	66,7%	5,6%	5,6%	22,2%
Biblioteca municipal	72,2%	0%	5,6%	22,2%

Fuente: INTECO

4.2 Tratamiento de datos habituales por parte de las entidades locales

Para finalizar el análisis de la clasificación por niveles, se ha considerado oportuno y de interés, evaluar aquellos ficheros de datos personales susceptibles de un tratamiento más común, por contener datos que requieren medidas de seguridad de nivel alto o tratarse de datos de gran relevancia para los interesados.

Se han identificado los siguientes ficheros, todos ellos de alta probabilidad de existencia en las EELL, como ficheros especialmente sensibles:

- Padrón de habitantes.
- Padrón de vehículos.
- Servicios sociales
- Licencia de actividad de locales comerciales.
- Videovigilancia.

Para este conjunto de ficheros se va a realizar un análisis de su utilización en las Entidades Públicas Locales y a proponer una serie de buenas prácticas para que su tratamiento sea el más adecuado posible.

4.2.1 Padrón de habitantes

Todas las personas que viven en España tienen la obligación de inscribirse en el padrón municipal de habitantes del lugar donde tengan su residencia habitual, según la Ley 7/1985, de 2 de abril, Reguladora de las Bases de Régimen Local¹² (en adelante, LBRL).

¹² Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local. Disponible en http://www.boe.es/g/es/bases_datos/doc.php?coleccion=iberlex&id=1985/05392

Las EELL no tienen el deber de recabar el consentimiento del interesado para el tratamiento de los datos del padrón, ya que, como indica el artículo 6.2 de la LOPD, el padrón forma parte de las funciones administrativas que son competencia de los Ayuntamientos.

Según el artículo 16.3 de la LBRL: *“Los datos del Padrón municipal se cederán a otras Administraciones Públicas que lo soliciten sin consentimiento previo del afectado solamente cuando les sean necesarios para el ejercicio de sus respectivas competencias, y exclusivamente para asuntos en los que la residencia o el domicilio sean datos relevantes. También pueden servir para elaborar estadísticas oficiales sometidas al secreto estadístico, en los términos previstos en la Ley 12/1989, de 9 de mayo, de la Función Estadística Pública¹³”.*

Por lo tanto, la Administración que solicite los datos al Ayuntamiento debe justificar que son para alguna de las competencias que le reconoce el ordenamiento jurídico, además de argumentar la relevancia de la residencia o el domicilio para este tratamiento.

Por otro lado, respecto a los fines estadísticos, los Ayuntamientos están obligados a facilitar la información de los datos del padrón al Instituto Nacional de Estadística, siempre que se justifique su petición dentro de las competencias que le otorga la Ley de Función Estadística Pública.

Por lo que respecta a la cesión de estos datos a las Fuerzas y Cuerpos de Seguridad del Estado, cuando los datos sean solicitados dentro de una investigación policial, el responsable del fichero del padrón únicamente debe comprobar que el solicitante acredita que pertenece como miembro a las Fuerzas y Cuerpos de Seguridad del Estado. Esta situación viene regulada por el artículo 22.2 de la LOPD en el que se indica que la recogida y tratamiento de datos personales por las Fuerzas y Cuerpos de Seguridad se puede realizar sin consentimiento del afectado cuando se trate de la prevención de un peligro real para la seguridad pública o para la represión de infracciones reales.

Respecto a las medidas de seguridad a aplicar a este tipo de ficheros, debe tenerse en cuenta que se trata de datos clasificados como nivel básico.

4.2.2 Padrón de vehículos

La finalidad del tratamiento de los datos de este fichero es la recaudación del impuesto municipal de circulación, además de mantener un registro de propietarios de vehículos (por ejemplo, para la gestión de transferencias).

¹³ Ley 12/1989, de 9 de mayo, de la Función Estadística Pública. Disponible en <http://www.boe.es/boe/dias/1989/05/11/pdfs/A14026-14035.pdf>

Si en el momento en el que se establezca este tipo de fichero se incorporasen únicamente datos de salud de los propietarios de los vehículos –referentes exclusivamente al grado de discapacidad o a la simple declaración de la condición de discapacidad o invalidez del afectado– el fichero pasaría a ser clasificado de nivel básico, entrando, de esta forma, a ser considerado en la exclusión contemplada en el artículo 81.6 del RDLOPD sobre la aplicación de los niveles de seguridad.

En el caso de tener contratada la gestión de algún servicio relacionado con los vehículos, por el que se tenga que acceder a este fichero para poder realizar las funciones encomendadas, hay que prestar especial atención al artículo 12 de la LOPD, que hace referencia al acceso a los datos por cuenta de terceros.

La LOPD permite que el responsable del fichero habilite el acceso material a datos de carácter personal por parte de la entidad que va a prestarle un servicio, que se constituirá como encargado del tratamiento, sin que, por mandato expreso de la Ley, pueda considerarse dicho acceso como una cesión de datos. Si bien se exige que en el contrato deban constar una serie de requisitos, tales como seguir las instrucciones del responsable del fichero, no utilizar los datos para un fin distinto, no comunicarlos a otras personas, estipular las medidas de seguridad del artículo 9 y, cumplida la prestación, destruir los datos o proceder a su devolución al responsable del fichero.

4.2.3 Servicios sociales

Los Servicios Sociales están disponibles y son accesibles para todos los ciudadanos sin discriminación por algún motivo personal. Los ficheros de datos personales gestionados por los Servicios Sociales de las Entidades Públicas Locales se clasifican con nivel de seguridad alto.

La LOPD, en su artículo 7, considera como datos especialmente protegidos los relativos a la ideología, afiliación sindical, religión y creencias, así como los datos personales que hagan referencia al origen racial, a la salud y a la vida sexual. Si bien, respecto a los primeros únicamente se puede llevar a cabo el tratamiento con el consentimiento expreso y por escrito del interesado. Respecto a los segundos, solo podrán ser recabados cuando así lo disponga una Ley o cuando el afectado consienta expresamente.

Por lo tanto, cuando una EELL recabe datos deberá manifestar una *adecuada justificación de la finalidad de la propia prestación social*.

En este sentido, a modo de ejemplo, cabe señalar la Resolución R/00431/2008 de la AEPD en la que figuran como *hechos probados*, la remisión de felicitaciones navideñas por parte de una EELL, en cantidad aproximada de quinientas, utilizando para ello datos obtenidos de los participantes en actividades de las Escuelas de Padres y de la Escuela de Verano, en este caso menores, así como de los beneficiarios de ayudas sociales, de

los servicios de Telesistencia y Ayudas a domicilio. Dichos datos habían sido recopilados, en base a las entrevistas personales realizadas por el Teniente de “Cargo 3” y, en otros casos, de los formularios de participación en las actividades citadas”.

Ante estos hechos, entre los *fundamentos de derecho* empleados en la citada Resolución se encuentra el apartado 2 del artículo 4 LOPD -principio de calidad de datos- aplicable al supuesto de hecho que se analiza al disponer que: *“Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos. No se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos”*.

En definitiva, las EELL deben tener siempre presente el deber de informar al interesado cuando, en relación a los ficheros de datos personales gestionados por los Servicios Sociales de las Entidades Públicas Locales, se pretenda recabar el consentimiento, ya que los datos no pueden ser tratados para fines distintos a los que motivaron su recogida, pues esto supondría un nuevo uso que requiere el consentimiento del interesado.

4.2.4 Licencia de actividad de locales comerciales

La solicitud de una licencia de actividad es un acto obligatorio y previo al inicio de cualquier actividad empresarial que necesite ubicarse en un local.

El nivel de clasificación de los datos de estos ficheros es básico, por lo que deben aplicarse las medidas de seguridad correspondientes indicadas en el RDLOPD.

Es habitual en las EELL que esta solicitud sea en formato papel, por lo que se debe incorporar a la misma un texto explicativo en el que se indiquen claramente los siguientes puntos:

- Existencia de un fichero, declarado en la Agencia de Protección de Datos, donde se van a incorporar los datos de la solicitud indicando quien es el responsable del fichero.
- Finalidad del tratamiento de los datos.
- Cesiones a terceros en el caso de que las haya.
- Forma de ejercer los derechos del interesado: acceso, rectificación, cancelación y oposición, ofreciendo un medio de contacto con la entidad para poder contactar.

4.2.5 Videovigilancia

La captación y grabación de imágenes de personas físicas identificadas o identificables por medio de sistemas de videocámaras, es considerado por la LOPD, según su artículo 3.a, como dato de carácter personal.

Un número cada vez mayor de EELL instalan dispositivos de este tipo. Hay que tener en cuenta que se considera tratamiento de datos personales: la captación, grabación, conservación, elaboración, modificación, bloqueo, cancelación y cesión de imágenes.

La Agencia Española de Protección de Datos, en virtud de la competencia que la LOPD le otorga, dictó la Instrucción 1/ 2006, de 8 de noviembre de 2006, por la que se regula el tratamiento de imágenes, con el objeto de regular y garantizar los derechos de las personas cuyas imágenes son tratadas por videocámaras con fines de vigilancia.

Se excluyen las imágenes grabadas para uso doméstico y el tratamiento de imágenes por parte de las Fuerzas y Cuerpos de Seguridad del Estado, que está regulado por la Ley Orgánica 4/97, de 4 de agosto.

Las principales exigencias a implantar son las siguientes:

- Para cumplir con el deber de información, se deben colocar, en las zonas videovigiladas, al menos un distintivo informativo ubicado en lugar suficientemente visible, tanto en espacios abiertos como cerrados.

Este distintivo deberá de incluir una referencia a la “Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal”, incluirá una mención a la finalidad para la que se tratan los datos (“ZONA VIDEOVIGILADA”), y una mención expresa a la identificación del responsable ante quien puedan ejercitarse los derechos de las personas en materia de Protección de Datos.

- Sólo se considerará admisible la instalación de cámaras cuando la finalidad de vigilancia no pueda obtenerse mediante otros medios que resulten menos intrusivos para la intimidad de las personas.
- Las imágenes sólo serán tratadas cuando sean adecuadas, pertinentes y no excesivas en relación con el ámbito y las finalidades determinadas, que hayan justificado la instalación de las cámaras.
- La creación de un fichero de imágenes de videovigilancia exige su previa notificación a la Agencia Española de Protección de Datos, para la inscripción en su Registro General.

5 INSCRIPCIÓN DE FICHEROS DE DATOS DE CARÁCTER PERSONAL, RESPONSABLE DE SEGURIDAD Y DOCUMENTO DE SEGURIDAD

Este apartado muestra el nivel de conocimiento en relación con la inscripción de ficheros de datos de carácter personal, la obligación de designar a un responsable de seguridad y la definición del alcance del documento de seguridad en grandes Ayuntamientos y Diputaciones, Consells y Cabildos Insulares. Para cada una de ellas se explica brevemente en qué consiste la obligación y las implicaciones para las EELL, los artículos de la ley o reglamento donde se recoge, y los datos extraídos de la investigación cuantitativa que muestran el grado de cumplimiento por parte de las administraciones.

5.1 Inscripción de ficheros

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.

La disposición de creación de ficheros de las administraciones públicas se regula en el art. 20 de la LOPD y se matiza en el 54 del Reglamento.

Así, el art. 20 de la LOPD establece que la creación, modificación o supresión de los ficheros de las Administraciones Públicas sólo podrá hacerse por medio de disposición general publicada en el Boletín Oficial del Estado o diario oficial correspondiente, como paso previo obligatorio para la posterior notificación de los ficheros ante la correspondiente Agencia de Protección de Datos. Asimismo en dichas disposiciones se deberá indicar:

- La finalidad del fichero y los usos previstos para el mismo.
- Las personas o colectivos sobre los que se pretenda obtener datos de carácter personal o que resulten obligados a suministrarlos.
- El procedimiento de recogida de los datos de carácter personal.
- La estructura básica del fichero y la descripción de los tipos de datos de carácter personal incluidos en el mismo.
- Las cesiones de datos de carácter personal y, en su caso, las transferencias de datos que se prevean a países terceros.
- Los órganos de las Administraciones responsables del fichero.

- Los servicios o unidades ante los que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición.
- Las medidas de seguridad con indicación del nivel básico, medio o alto exigible.

En cuanto al contenido el art. 54 del RDLOPD se describen todos los apartados que debe contener la disposición:

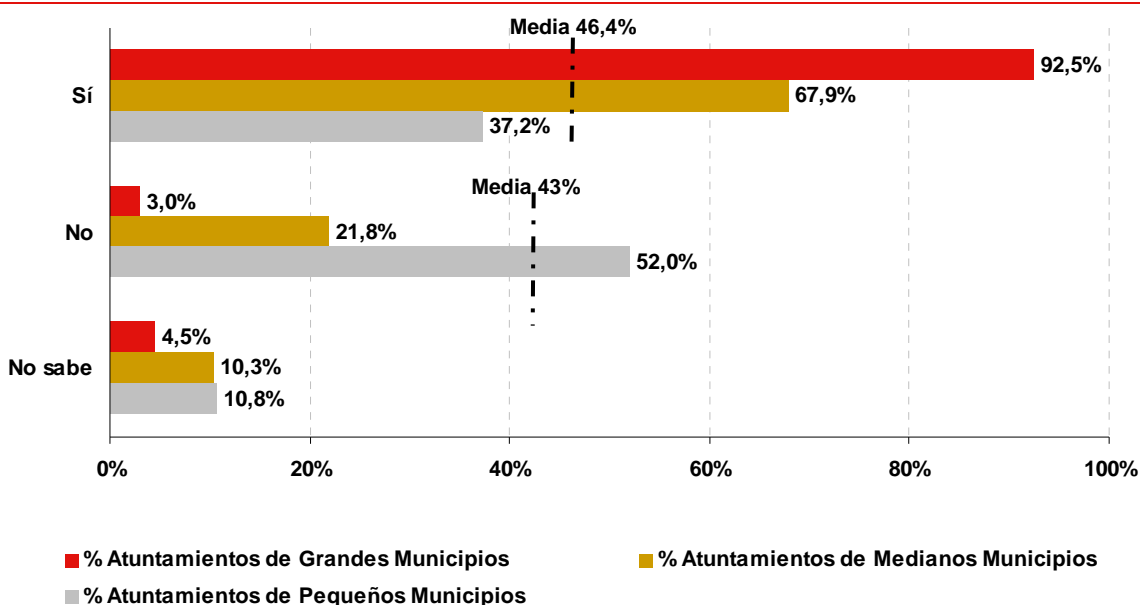
- La identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos.
- El origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia.
- La estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización.
- Las comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios.
- Las transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos.
- Los órganos responsables del fichero.
- Los servicios o unidades ante los que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición.
- El nivel básico, medio o alto de seguridad que resulte exigible, de acuerdo con lo establecido en el título VIII del presente reglamento.

Respecto a las disposiciones que se dicten para la supresión de los ficheros (reguladas en el art. 20.3 de la LOPD) se establecerá el destino de los mismos o, en su caso, las previsiones que se adopten para su destrucción.

Del total de ayuntamientos, el 46,4% afirma haberlos declarado en el registro de la AEPD, frente a un 43% que confirma que no los ha declarado y un 10,5% que dice desconocer su situación al respecto. Respecto a las Diputaciones, Consells y Cabildos Insulares, un 88,9% afirma haberlo realizado frente a sólo un 8,3% que no lo ha hecho.

El análisis por tamaño del estrato permite comprobar que el nivel de cumplimiento se da en el caso de los ayuntamientos de grandes municipios donde un 92,5% de los mismos realizan esta acción y en los de mediano tamaño (67,9%). En cambio sólo un 37,2% de los ayuntamientos de pequeños municipios inscriben los ficheros.

Gráfico 12: Inscripción de ficheros de datos de carácter personal en el registro general de ficheros de la Agencia de Protección de Datos estatal o autonómica correspondientes, por tamaño (%)



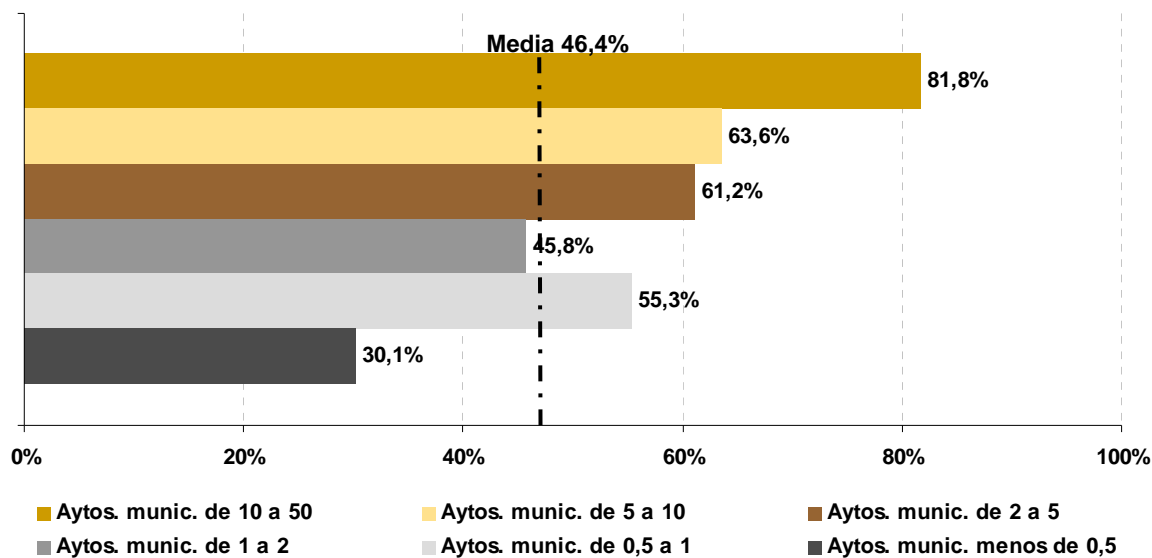
Fuente: INTECO

Ahora bien, si se analiza a fondo el grado de respuesta de los municipios de menor tamaño se puede observar, ver Gráfico 13, que en los ayuntamientos con menos de 500 habitantes es donde el porcentaje de estos respecto a la inscripción de archivos es menor; sólo un 30,1% de los ayuntamientos de este estrato realizan este trámite ante la Agencia de Protección de Datos estatal o autonómica.

Sin embargo, el volumen de municipios que llevan a cabo la inscripción de ficheros se va reduciendo en función del tamaño del municipio, salvo en el caso de los gobiernos de localidades de 500 a 1.000 habitantes (55,3%). Además en los gobiernos de todos los núcleos de entre 2.000 a 50.000 habitantes el número de municipios que cumplen con lo establecido en la norma es superior al 60% (entre el 61,2% y el 80,8%).

La falta de recursos para dar cumplimiento a esta obligación podría inferirse como la causa objetiva principal de esta situación, no obstante, la inscripción es gratuita y su procedimiento simplificado y estandarizado.

Gráfico 13: Inscripción de ficheros de datos de carácter personal en el registro general de ficheros de la Agencia de Protección de Datos estatal o autonómica correspondientes, en pequeños y medianos municipios (%)



Fuente: INTECO

5.2 Responsable de Seguridad

Con independencia de que las entidades deben asignar un responsable como medida de seguridad cuando se tienen datos personales de nivel medio o superior tal y como establece el art. 95 del RDLOPD, es una figura que debe existir con antelación.

Las entidades deben nombrar un responsable de seguridad para que haya una figura, conocida por todos, encargada de velar por el cumplimiento de la normativa definida en el documento de seguridad.

Esta persona será designada por el responsable del fichero, que podrá delegar en él, el cumplimiento de la Ley y la implementación de las medidas del reglamento, pero en ningún caso podrá delegar su responsabilidad final sobre el tratamiento de los datos de carácter personal.

Para distinguir las figuras de responsables y encargado 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.

A nivel global un 28,7% de los ayuntamientos manifiestan haber nombrado un responsable de seguridad frente al 52,8% de las Diputaciones, Consells y Cabildos Insulares. La cobertura por nivel de estrato y tamaño de la población muestra que únicamente 3 estratos superan el 50% y los dos estratos de menos de 1.000 habitantes no alcanzan ni siquiera el 20% de municipios (Tabla 13).

Cabe destacar el caso de los municipios de más de 500.000 habitantes, habitualmente los de mayor grado de cumplimiento, con un 33,3% de cobertura para el nombramiento de un responsable de seguridad.

A nivel de estrato destaca que el 73,2% de los ayuntamientos con pequeños municipios no ha nombrado a su responsable de seguridad. Y solo el 48,4% de las entidades con medianos municipios lo han realizado. En el lado opuesto están los ayuntamientos de grandes municipios donde el 61,1% de los mismos afirman haberlo designado. Esta situación justificaría que sólo un 8,3% de los que han contestado la encuesta sean en su entidad los responsables (ver Gráfico 1).

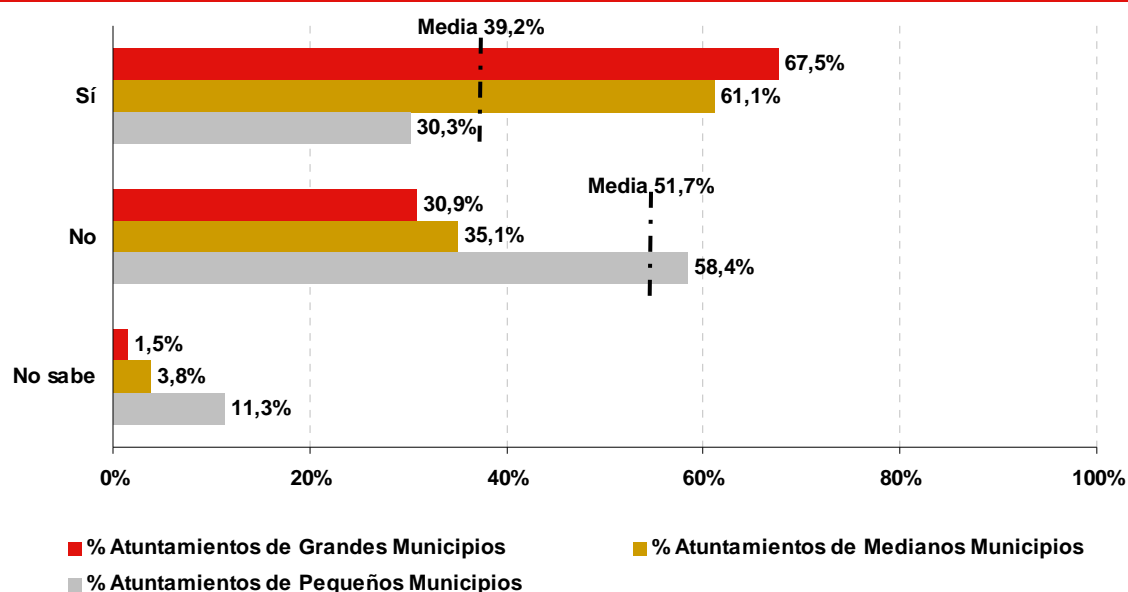
Tabla 13: Distribución de las entidades locales donde se ha procedido a nombrar un responsable de seguridad, por tamaño (%)

Población (en miles)	Distribución porcentual			Distribución media ponderada			
	SI	NO	NS/NC	SI	NO	NS/NC	
Grandes	Más de 500	33,3%	33,3%	33,3%	61,1%	34,6%	4,3%
	De 100 a 500	60,0%	40,0%	0,0%			
	De 50 a 100	64,1%	30,8%	5,1%			
Medianos	De 10 a 50	54,0%	36,5%	9,5%	48,4%	43,9%	7,7%
	De 5 a 10	48,5%	45,5%	6,1%			
	De 2 a 5	44,8%	47,8%	7,5%			
Pequeños	De 1 a 2	33,9%	61,0%	5,1%	20,5%	73,2%	6,3%
	De 0,5 a 1	18,4%	76,3%	5,3%			
	Ayts. Munic. menos 0,5	17,8%	75,3%	6,8%			
Diputaciones, Consells y Cabildos Insulares		52,8%	41,7%	5,6%			

Fuente: INTECO

No obstante, lo interesante es conocer que entre los que manifiestan haber declarado ficheros sólo un 39,2% de las entidades locales afirman haber asignado un responsable de seguridad (Gráfico 14). El índice de cumplimiento entre los grandes (67,5%) y medianos municipios, un 61,1%, 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 14: Distribución de las entidades locales donde se ha procedido a nombrar un responsable de seguridad entre los que tienen inscritos ficheros, por tamaño (%)



Fuente: INTECO

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

Además se establece la necesidad de mantener dicho instrumento actualizado y revisarse de forma periódica de manera que esté siempre adecuado a los cambios que se produzcan en la Entidad en materia de protección de datos de carácter personal. Así deberá contener, como mínimo, los siguientes aspectos:

- Ámbito de aplicación del documento con especificación detallada de los recursos protegidos.
- Medidas, normas, procedimientos de actuación, reglas y estándares encaminados a garantizar el nivel de seguridad exigido en el RDLOPD.
- Funciones y obligaciones del personal en relación con el tratamiento de los datos de carácter personal incluidos en los ficheros inscritos.
- Estructura de los ficheros y la descripción de los sistemas de información que los tratan.
- Procedimientos de notificación, gestión y respuesta ante las incidencias que pudieran devenir.
- Procedimientos de realización de copias de respaldo y de recuperación de los datos en los ficheros o tratamientos automatizados.
- Medidas necesarias a adoptar para el transporte de soportes u documentos, así como para la destrucción de los documentos y soportes, o en su caso, la reutilización de estos últimos.

5.3.1 Ámbito de aplicación del documento con especificación detallada de los recursos protegidos

A pesar de lo establecido por la norma, en las Entidades Locales no es una práctica común la definición del alcance en el documento de seguridad ya que sólo el 35,3% de

las mismas lo ha realizado. No obstante, sólo los ayuntamientos de menor tamaño incumplen con dicha obligación tal y como muestra la Tabla 14.

Entre los Ayuntamientos de tamaño medio está definido el alcance en los gobiernos locales de 2.000 a 5.000 habitantes (50,7%) y en los de 10.000 a 50.000 habitantes (58,5%), mientras que 4 de cada 10 núcleos de 5.000 a 10.000 realizan esta definición del alcance del documento de seguridad. Por último, está ampliamente establecida en los Ayuntamientos de municipios de entre 50.000 y 500.000 habitantes (79,2%-100%).

Tabla 14: Definición del alcance de aplicación del documento de seguridad, por tamaño (%)

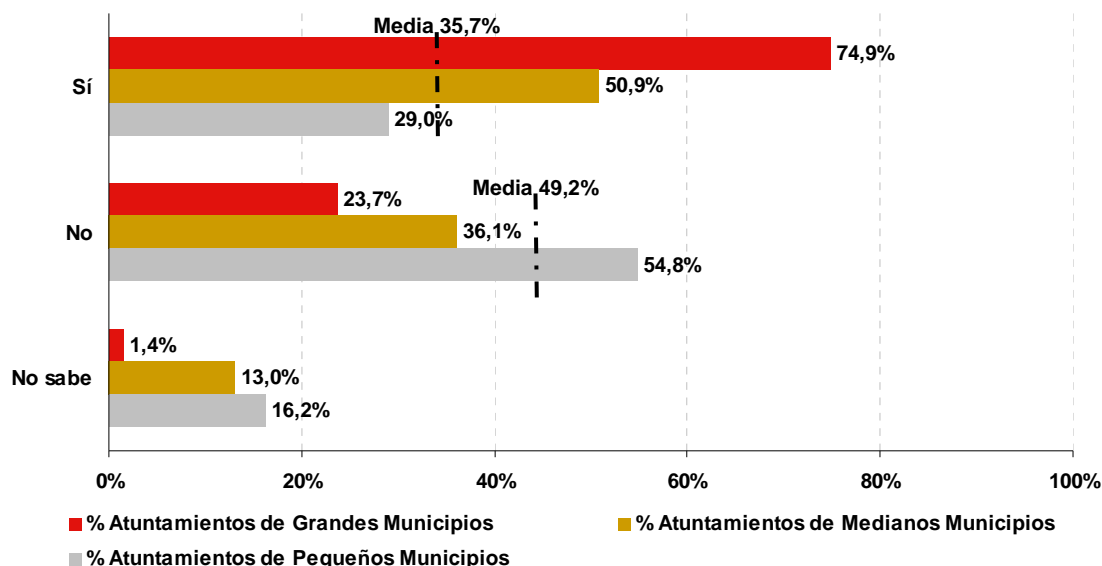
Población (en miles)		Distribución porcentual			Distribución media ponderada		
		SI	NO	NS/NC	SI	NO	NS/NC
Grandes	Más de 500	100,0%	0,0%	0,0%			
	De 100 a 500	80,0%	20,0%	0,0%	80,6%	19,4%	0,0%
	De 50 a 100	79,5%	20,5%	0,0%			
Medianos	De 10 a 50	58,4%	29,2%	12,4%			
	De 5 a 10	42,4%	48,5%	9,1%	51,0%	32,8%	16,2%
	De 2 a 5	50,7%	26,9%	22,4%			
Pequeños	De 1 a 2	33,9%	49,2%	16,9%			
	De 0,5 a 1	21,1%	63,2%	15,8%	24,6%	54,5%	20,9%
	Ayts. Munic. menos 0,5	23,3%	53,4%	23,3%			
Diputaciones, Consells y Cabildos Insulares		58,3%	36,1%	5,6%			

Fuente: INTECO

5.3.2 Medidas, normas, procedimientos de actuación, reglas y estándares encaminados a garantizar el nivel de seguridad exigido en el RDLOPD

Estas son también obligatorias de estar en el documento de seguridad por lo que resulta lógico que el porcentaje de entidades locales que las han implementado sea parecido; en este caso, un 35,7% para los ayuntamientos y un 61,1% para las Diputaciones, Consells y Cabildos Insulares frente al 49,2% y al 33,3% que no lo han realizado. Por estrato y tamaño del mismo, el grado de cumplimiento de los ayuntamientos de menor tamaño ha aumentado con respecto a la medida anterior; un 29% de los organismos de pequeños municipios lo lleva a cabo tal y como se muestra en el Gráfico 15.

Gráfico 15: Establecimiento de medidas, normas y procedimientos de seguridad por tamaño (%)



Fuente: INTECO

5.3.3 Funciones y obligaciones del personal en relación con el tratamiento de los datos de carácter personal incluidos en los ficheros inscritos

En la Tabla 15 se puede comprobar que más de 4 de cada 10 ayuntamientos de pequeños municipios incorporan este tipo de información en los ficheros. A nivel global un 46,1% de los ayuntamientos y un 56,8% de las Diputaciones, Consells y Cabildos Insulares afirman haberlo realizado y cumplen por consiguiente con lo establecido en el RDLOPD.

Tabla 15: Definición de las funciones y obligaciones del personal, por tamaño (%)

Población (en miles)		Distribución porcentual			Distribución media ponderada		
		SI	NO	NS/NC	SI	NO	NS/NC
Grandes	Más de 500	66,7%	0,0%	0,0%	70,4%	28,1%	1,5%
	De 100 a 500	76,0%	24,0%	0,0%			
	De 50 a 100	66,7%	33,3%	0,0%			
Medianos	De 10 a 50	54,7%	35,8%	9,5%	53,4%	38,2%	8,4%
	De 5 a 10	42,4%	51,5%	6,1%			
	De 2 a 5	58,2%	32,8%	9,0%			
Pequeños	De 1 a 2	47,5%	44,1%	8,5%	42,7%	49,6%	7,7%
	De 0,5 a 1	39,5%	55,3%	5,3%			
	Aytos. Munic. menos 0,5	42,5%	49,3%	8,2%			
Diputaciones, Consells y Cabildos Insulares		56,8%	35,1%	8,1%			

Fuente: INTECO

5.3.4 Estructura de los ficheros y la descripción de los sistemas de información que los tratan

El documento de seguridad debe incluir una descripción detallada de la estructura de los ficheros con datos personales notificados a la Agencia, así como, la descripción de los sistemas de información que soportan estos ficheros.

Un 38,1% de los ayuntamientos llevan a cabo esta función frente a un 75% de Diputaciones, Consells y Cabildos Insulares, siendo el estrato de más de 500.000 habitantes el que más cobertura tiene para este punto, con un 100%. En el lado opuesto, entre los ayuntamientos de menor tamaño, sólo el 24,7% de los ayuntamientos de menos de 500 habitantes cumplen con lo establecido por la normativa (Tabla 16).

Tabla 16: Inclusión en el documento de seguridad de la descripción de los ficheros declarados y el sistema de información que los trata, por tamaño (%)

Población (en miles)		Distribución porcentual			Distribución media ponderada		
		SI	NO	NS/NC	SI	NO	NS/NC
Grandes	Más de 500	100,0%	0,0%	0,0%	83,6%	16,4%	0,0%
	De 100 a 500	84,0%	16,0%	0,0%			
	De 50 a 100	82,1%	17,9%	0,0%			
Medianos	De 10 a 50	64,2%	26,3%	9,5%	59,8%	29,0%	11,2%
	De 5 a 10	51,5%	42,4%	6,1%			
	De 2 a 5	61,2%	23,9%	14,9%			
Pequeños	De 1 a 2	42,4%	45,8%	11,9%	28,7%	57,0%	14,2%
	De 0,5 a 1	31,6%	55,3%	13,2%			
	Aytos. Munic. menos 0,5	24,7%	60,3%	15,1%			
Diputaciones, Consells y Cabildos Insulares		75,0%	19,4%	5,6%			

Fuente: INTECO

5.3.5 Procedimientos de notificación, gestión y respuesta ante las incidencias que pudieran devenir

Este aspecto es también de obligado cumplimiento por lo que todos los documentos de seguridad que elaboran las entidades locales deben contenerlo. Sin embargo sólo un 27,6% de los ayuntamientos afirma realizarlo y un 36,1% de las Diputaciones, Consells y Cabildos Insulares.

Por estratos la situación, salvo en el caso de los ayuntamientos de más de 500.000 habitantes donde es un 100% de cobertura, varía entre el 68%-59% para los de mayor número de habitantes (entre 50.000 y 500.000 habitantes). Los de tamaño intermedio y por consiguiente categorizados como medianos en el presente estudio, varían entre un 33,3% y un 46,7%. Por último entre los de menor tamaño, ayuntamientos de municipios de menos de 500 habitantes, el porcentaje de ayuntamientos que cumplen con lo

establecido en la normativa es de un 17,8% tal y como se puede comprobar en la Tabla 17.

Tabla 17: Inclusión en el documento de seguridad de los procedimientos de notificación, gestión y respuesta ante las incidencias que pudieran devenir, por tamaño (%)

Población (en miles)		Distribución porcentual			Distribución media ponderada		
		SI	NO	NS/NC	SI	NO	NS/NC
Grandes	Más de 500	100,0%	0,0%	0,0%	64,4%	32,8%	2,8%
	De 100 a 500	68,0%	32,0%	0,0%			
	De 50 a 100	59,0%	35,9%	5,1%			
Medianos	De 10 a 50	46,7%	40,1%	13,1%	40,5%	49,3%	10,2%
	De 5 a 10	33,3%	60,6%	6,1%			
	De 2 a 5	40,3%	49,3%	10,4%			
Pequeños	De 1 a 2	27,1%	62,7%	10,2%	21,8%	67,0%	11,2%
	De 0,5 a 1	31,6%	60,5%	7,9%			
	Aytos. Munic. menos 0,5	17,8%	69,9%	12,3%			
Diputaciones, Consells y Cabildos Insulares		36,1%	44,4%	19,4%			

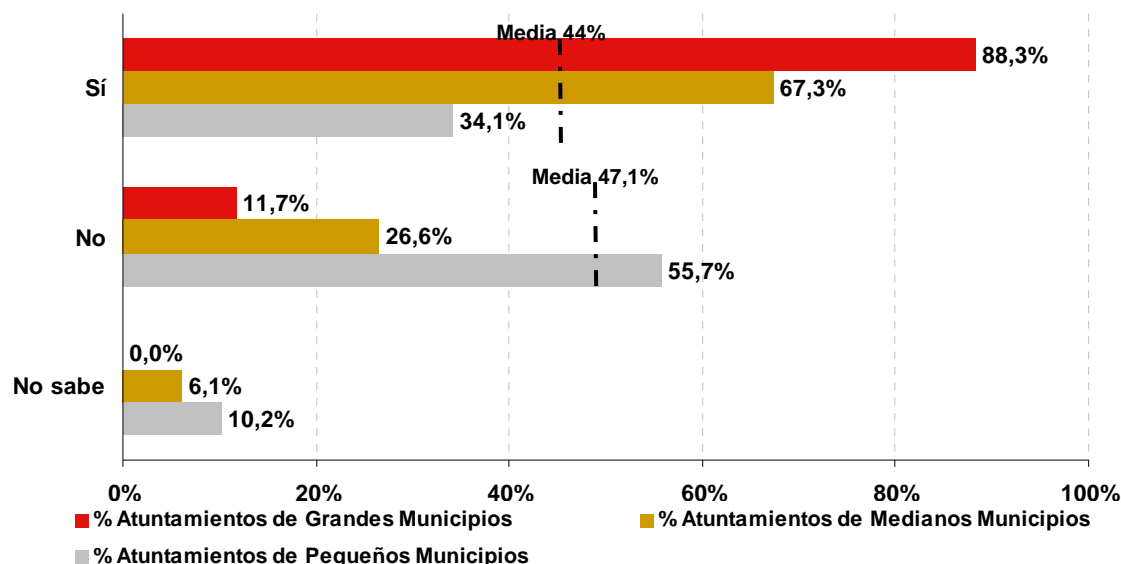
Fuente: INTECO

5.3.6 Procedimientos de realización de copias de respaldo y de recuperación de los datos en los ficheros o tratamientos automatizados

A nivel global el 44% de los ayuntamientos y un 72% de las Diputaciones, Consells y Cabildos Insulares establecen procedimientos de realización de copias de respaldo y de recuperación. Estos resultados indican que es más común en los municipios la práctica de la realización de las copias de respaldo frente a una gestión formal de incidencias, sin tener procedimiento ni registro formalizado.

Un análisis por estrato muestra que sólo un 34,1% de los ayuntamientos de pequeños municipios detallen estos procedimientos en sus documentos de seguridad. Una posible explicación puede ser que para este estrato el número de ficheros y datos que generen sea inferior al de los otros estratos. En el resto de estratos porcentajes superiores a un 67% de los ayuntamientos efectúan las copias de respaldo y recuperación.

Gráfico 16: Inclusión en el documento de seguridad de los procedimientos de realización de copias de respaldo y de recuperación de los datos, por tamaño (%)



Fuente: INTECO

5.3.7 Medidas necesarias a adoptar para el transporte de soportes u documentos, así como para la destrucción de los documentos y soportes, o en su caso, la reutilización de estos últimos

En relación a la gestión de soportes, el RDLOPD indica que el documento de seguridad debe incluir una descripción de los controles que la Entidad ha decidido implantar para impedir la recuperación de la información que vaya a ser desechada o sea reutilizada para otra finalidad.

Esta práctica no es de difícil de cumplimiento, ya que existen medios sencillos para llevarla a cabo, sin embargo, a nivel global un 28,3% de los ayuntamientos y un 44,4% de las Diputaciones, Consells y Cabildos Insulares afirman realizarlo. Además y como se muestra en la Tabla 18 sólo en los ayuntamientos de entre 50.000 y más de 500.000 habitantes se supera el 64% de cobertura. En los municipios pequeños de menos de 2.000 habitantes no se supera el 35% de cobertura, destacando los de menos de 500 habitantes, en los que únicamente un 16,4% de municipios tienen implantada esta práctica.

Tabla 18: Inutilización de soportes desechados o reutilizados, por tamaño (%)

Población (en miles)		Distribución porcentual			Distribución media ponderada		
		SI	NO	NS/NC	SI	NO	NS/NC
Grandes	Más de 500	66,7%	33,3%	0,0%	65,8%	32,6%	1,6%
	De 100 a 500	68,0%	28,0%	4,0%			
	De 50 a 100	64,1%	35,9%	0,0%			
Medianos	De 10 a 50	46,7%	43,8%	9,5%	42,0%	44,8%	13,3%
	De 5 a 10	39,4%	54,5%	6,1%			
	De 2 a 5	40,3%	40,3%	19,4%			
Pequeños	De 1 a 2	35,6%	57,6%	6,8%	22,3%	61,2%	16,5%
	De 0,5 a 1	31,6%	57,9%	10,5%			
	Aytos. Munic. menos 0,5	16,4%	63,0%	20,5%			
Diputaciones, Consells y Cabildos Insulares		44,4%	47,2%	8,3%			

Fuente: INTECO

6 LEGITIMACIÓN DE DATOS: INFORMACION, CONSENTIMIENTO, CESIÓN Y CONFIDENCIALIDAD

El tratamiento de los datos personales por una Entidad Local, ha de cumplir con la normativa vigente, desde la recogida de la información (art. 5 de la LOPD), su mantenimiento y actualización (art. 4 de la LOPD), hasta la cesión y tratamiento a terceros (art. 11 y 12 de la LOPD), y la facilitación de los derechos de los ciudadanos (Titulo III de la LOPD).

6.1 Deber de información sobre la finalidad del tratamiento del interesado

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 entidades locales a los efectos de este estudio) de informar a los ciudadanos sobre distintos aspectos:

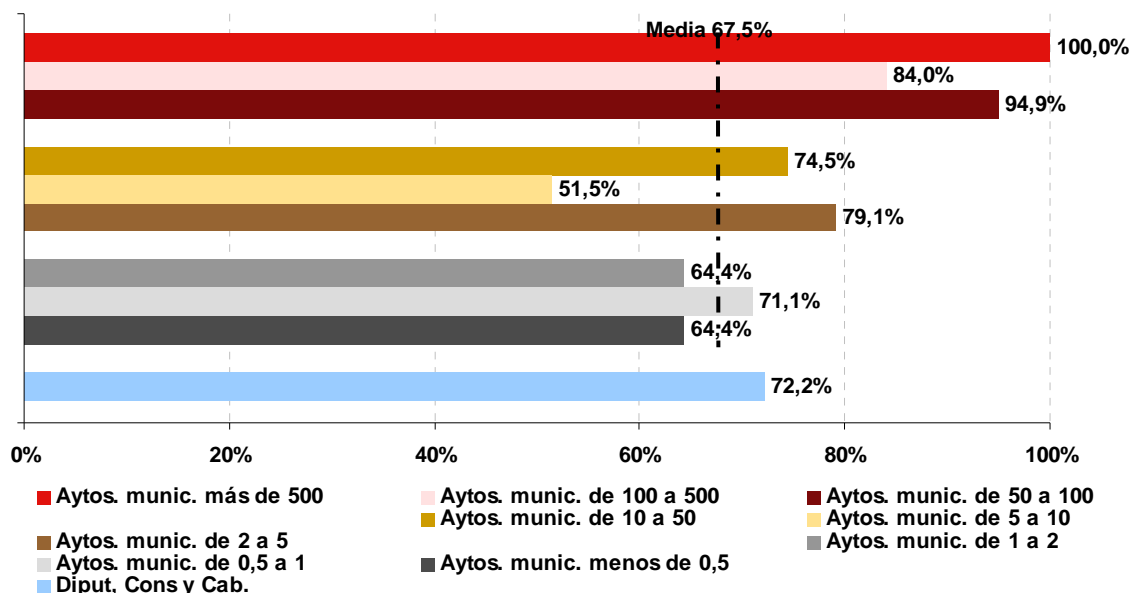
- De la incorporación de sus datos a un fichero.
- De la identidad y dirección del responsable.
- De la finalidad del fichero.
- De los destinatarios de la información.
- Así como de la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.

Un 67,5% de los ayuntamientos y un 72,2% de las Diputaciones, Consells y Cabildos Insulares declaran cumplir con el deber de información entre las entidades locales que disponen de ficheros automatizados. A nivel de estratos, el cumplimiento se da en gran parte de los organismos y varía entre un 90,7%, un 71,1% y un 65,6% de los ayuntamientos de grandes, medianos y pequeños municipios respectivamente.

En cambio, si se comprueba este deber por tamaño de municipio, la situación difiere un poco como es lógico al no ser resultados ponderados. Por un lado estarían los municipios con más de 500.000 habitantes que lo realizan con un 100% de cobertura y los de 50.000 a 100.000 habitantes con un 94,9%.

En los municipios de menor tamaño el grado de cobertura es también elevado (entorno a un 64,4%-79,1%), resultando los Ayuntamientos de 5.000 a 10.000 habitantes los que menos realizan esta práctica, con un 51,5%.

Gráfico 17: Información al interesado sobre la finalidad de la recopilación de los datos, en función del tamaño de los municipios (%)



Fuente: INTECO

6.2 Deber de consentimiento del interesado para el tratamiento de los datos

Este deber 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 posteriormente a su 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 el marco normativo para recabar el consentimiento de los afectados para el tratamiento de sus datos de carácter personal. No obstante, el art. 10.3 del RDLOPD señala que los datos de carácter personal podrán tratarse sin necesidad del consentimiento del interesado cuando se recojan para el ejercicio de las funciones propias de las Administraciones públicas en el ámbito de las competencias que les atribuya una norma con rango de Ley o una norma de derecho comunitario.

Para el supuesto en el que los responsables de ficheros necesiten realizar un tratamiento de datos considerados como protegidos (afiliación sindical, religión o creencias, salud, vida sexual u origen racial), se requerirá autorización expresa por parte del interesado, así como un documento por escrito que lo acredite (art.7.2 de la LOPD). Y además cuando los datos vayan a ser cedidos a un tercero para su tratamiento, se deberá recabar, igualmente, el consentimiento del interesado. El responsable del tratamiento deberá tener pruebas de la existencia de este consentimiento, habitualmente mediante la firma manuscrita en el formulario correspondiente.

La falta de obtención del consentimiento y posterior cesión a un tercero de los datos, es fuente habitual de reclamaciones de los ciudadanos cuando se contacta con ellos conociendo sus datos, sin ser consciente el interesado de habérselos facilitado.

La Tabla 19 muestra el porcentaje de entidades que solicitan dicho consentimiento de acuerdo a la Ley, no obstante a nivel global el 36,4% de ayuntamientos obtienen el consentimiento. Como se puede observar los municipios de mayor número de habitantes son los que más cumplen con este requisito, siendo los de 50.000 a 100.000 habitantes, con un 69,2%, los que mayor porcentaje acumulan. No obstante, los pequeños Ayuntamientos no superan el 40% de cumplimiento, y los de menos de 500 habitantes, con un 30,1%, los que menos formalizan el consentimiento.

Tabla 19: Entidades que solicitan el consentimiento de los interesados, por tamaño (%)

Población (en miles)		Distribución porcentual			Distribución media ponderada		
		SI	NO	NS/NC	SI	NO	NS/NC
Grandes	Más de 500	66,7%	33,3%	0,0%			
	De 100 a 500	64,0%	28,0%	8,0%	67,0%	25,5%	7,5%
	De 50 a 100	69,2%	23,1%	7,7%			
Medianos	De 10 a 50	51,8%	32,1%	16,1%			
	De 5 a 10	33,3%	42,4%	24,2%	43,4%	42,5%	14,0%
	De 2 a 5	43,3%	49,3%	7,5%			
Pequeños	De 1 a 2	37,3%	54,2%	8,5%			
	De 0,5 a 1	39,5%	55,3%	5,3%	33,0%	62,0%	5,0%
	Aytos. Munic. menos 0,5	30,1%	65,8%	4,1%			
Diputaciones, Consells y Cabildos Insulares		41,7%	41,7%	16,7%			

Fuente: INTECO

6.3 Gestión de la cesión de datos

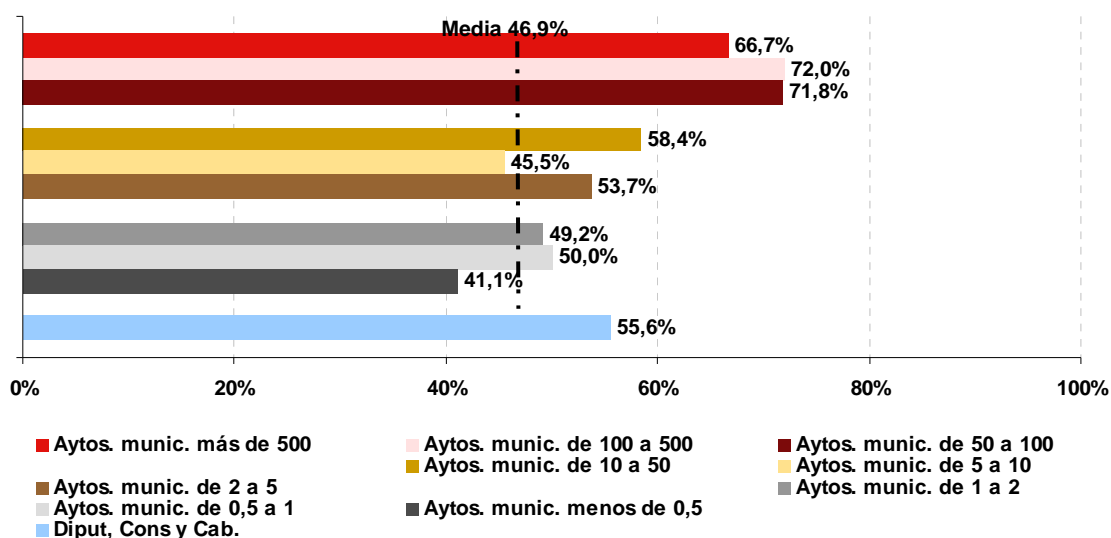
Se entiende por cesión de datos toda revelación de datos realizada a una persona física o jurídica distinta al interesado. Los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas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

Se trata de una medida que no está lo suficientemente extendida entre los Ayuntamientos ya que sólo lo realizan el 46,9% de ellos por un 55,6% de las Diputaciones, Consells y Cabildos Insulares. Sin embargo si lo está para los ayuntamientos de grandes municipios donde un 71,7% de ellos lo lleva a cabo frente a un 53,1% y un 44% de los ayuntamientos de medianos y pequeños municipios.

Tomando en consideración los datos que aporta el análisis por tamaño del municipio tal y como se muestra en el Gráfico 18 en aquellos núcleos de 50.000 a 100.000 habitantes lo implementa el 71,8% de los gobiernos, seguidos por los de poblaciones de 100.000 a 500.000 habitantes (70,8%). Más de 6 cada 10 Gobiernos de municipios de más de 500.000 habitantes y más de la mitad de las Diputaciones, Consells y Cabildos Insulares siguen dicha práctica. Ahora bien, el hecho de que no sea más extendida esta práctica puede ocasionar graves sanciones por parte de la Agencia Española de Protección de Datos por lo que debería ser tenido en cuenta por las propias entidades.

En los Ayuntamientos de menos de 50.000 habitantes la asunción de esta medida es bastante heterogénea. Así entre los gobiernos que los implementan el 50% o más (56,7%-58,6%) se encuentran los núcleos de entre 500 a 1.000 habitantes, seguidos por las poblaciones de 2.000 a 5.000 habitantes y en los de 10.000 a 50.000 habitantes respectivamente. Entre los gobiernos que menos informan al interesado sobre la cesión de datos a otras organizaciones se encuentran los de menos de 500 habitantes (41,1%).

Gráfico 18: Información al interesado sobre la cesión de los datos a otras organizaciones, en función del tamaño de los municipios (%)



Fuente: INTECO

6.4 Confidencialidad de los datos

Es habitual entre las Entidades de mayor tamaño que se subcontraten servicios con empresas de servicios (por ejemplo de limpieza y basuras, el servicio de mantenimiento de equipos informáticos, el servicio de expedir las tarjetas de aparcamiento, de gestorías, auditores o abogados, etc.). Por este motivo y desde el punto de vista de la normativa sobre protección de datos, cuando las entidades subcontratan un servicio con un tercero, éstas deben valorar si este tercero puede considerarse encargado del tratamiento,

garantizando que el mismo se realice adecuándolo a los datos de carácter personal. Es decir, utilizando los datos únicamente para la finalidad para la cual hayan sido designados y siendo únicamente éste el responsable de las consecuencias que podrán originarse en caso de destinar los datos a otra finalidad distintas a la inicialmente establecida.

No obstante el responsable de los ficheros de la entidad debe garantizar mediante el establecimiento de cláusulas de confidencialidad el deber de guardar secreto sobre la información tratada. Estas deben ser firmadas por el personal de la entidad que tenga acceso a los ficheros y afectan tanto al personal de la entidad como sobre los terceros con los que se tenga algún tipo de acuerdo.

A nivel global la situación el cumplimiento de este deber es insuficiente como lo muestra el hecho de que a nivel global un 28,9% de los ayuntamientos lo lleve a cabo. En el caso de la Diputaciones, Consells y Cabildos Insulares la situación es mejor ya que un 44,4% lo realiza. Sin embargo, está situación es más óptima en los gobiernos de todos los núcleos de entre 50.000 y 500.000 habitantes donde más de un 74% de las entidades realizan esta práctica (ver Tabla 20).

En las entidades de tamaño mediano la firma de las cláusulas de confidencialidad se realiza por menos de la mitad de los gobiernos. Así, en aquellos núcleos de 10.000 a 50.000 habitantes lo implementa el 48,9% de los municipios y entorno a 4 de cada 10 gobiernos de 2.000 a 10.000 habitantes siguen dicha práctica. Por último, es en los Ayuntamientos más pequeños, aquellos de menos de 2.000 habitantes, donde la firma de las cláusulas tiene menor implantación, con datos entre el 15% y 24%.

Tabla 20: Firma de cláusulas de confidencialidad por lo trabajadores y terceras personas que prestan servicios a las Entidades, por tamaño (%)

Población (en miles)		Distribución porcentual			Distribución media ponderada		
		SI	NO	NS/NC	SI	NO	NS/NC
Grandes	Más de 500	100,0%	0,0%	0,0%	76,1%	18,0%	5,9%
	De 100 a 500	76,0%	20,0%	4,0%			
	De 50 a 100	74,4%	17,9%	7,7%			
Medianos	De 10 a 50	48,2%	31,4%	20,4%	43,1%	43,1%	13,8%
	De 5 a 10	39,4%	51,5%	9,1%			
	De 2 a 5	41,8%	46,3%	11,9%			
Pequeños	De 1 a 2	20,3%	66,1%	13,6%	22,4%	67,7%	10,0%
	De 0,5 a 1	15,8%	71,1%	13,2%			
	Ayts. Munic. menos 0,5	24,7%	67,1%	8,2%			
Diputaciones, Consells y Cabildos Insulares		44,4%	30,6%	25,0%			

Fuente: INTECO

7 DERECHOS ARCO

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 deben cumplir.

No obstante y según recoge el art. 23 de la LOPD, los responsables de los ficheros que contengan datos utilizados para fines policiales podrán denegar el acceso, la rectificación o cancelación en función de los peligros que pudieran derivarse para la defensa del Estado o la seguridad pública, la protección de los derechos y libertades de terceros o las necesidades de las investigaciones que se estén realizando.

7.1 Derecho de Acceso

Los derechos del titular de los datos aparecen recogidos en el art. 15 de la LOPD y el art. 27 del RDLOPD, que reconocen 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.

Complementariamente las entidades tienen la obligación de informar gratuitamente de todos aquellos datos que posee sobre un ciudadano. El art. 29 del RDLOPD establece que el responsable del fichero resolverá sobre la solicitud de acceso en el plazo máximo de un mes a contar desde la recepción de la solicitud y el 25 del RDLOPD, señala que el responsable del tratamiento deberá contestar la solicitud que se le dirija en todo caso, con independencia de que figuren o no datos personales del afectado en sus ficheros. Asimismo, si los datos rectificadas hubieran sido cedidos previamente a un tercero, el responsable del fichero tiene la obligación de notificar al cesionario la rectificación practicada.

7.2 Derecho de Rectificación

Los art. 16 de la LOPD y el 31 y 32 del RDLOPD reconocen 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.

Estos artículos también señalan que el responsable del fichero o tratamiento tiene el deber de atender el derecho de rectificación en el plazo de diez días naturales. Debiendo contestar de forma motivada a la solicitud que se le dirija, para lo cual utilizará cualquier medio que permita acreditar el envío y la recepción de su respuesta. Asimismo, si los datos rectificadas hubieran sido cedidos previamente a un tercero, el responsable del fichero tiene la obligación de notificar al cesionario la rectificación practicada en el mismo plazo.

7.3 Derecho de Cancelación

Este derecho, regulado en el art. 16 de la LOPD y el 31 y 32 del RDLOP, ofrece al ciudadano la posibilidad de dirigirse al responsable para solicitar la cancelación de sus datos personales. La cancelación dará lugar al bloqueo de los datos, conservándose únicamente a disposición de las administraciones públicas, jueces y tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas; cumplido dicho plazo deberá procederse a la supresión.

Adicionalmente el art. 16 de la LOPD y el art. 32 del RDLOPD reconocen que 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.

7.4 Derecho de Oposición

El ciudadano puede oponerse a que no se lleve a cabo el tratamiento de sus datos de carácter personal o se cese en el mismo en tres casos según se recoge en el art. 34 del RDLOPD: cuando no sea necesario su consentimiento para el tratamiento, cuando se trate de ficheros que tengan por finalidad la realización de actividades de publicidad y prospección comercial y cuando el tratamiento tenga por finalidad la adopción de una decisión referida al afectado y basada únicamente en un tratamiento automatizado de sus datos de carácter personal. También 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.

El art. 35 del RDLOPD establece que el responsable del fichero o tratamiento tiene un plazo máximo de diez días 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

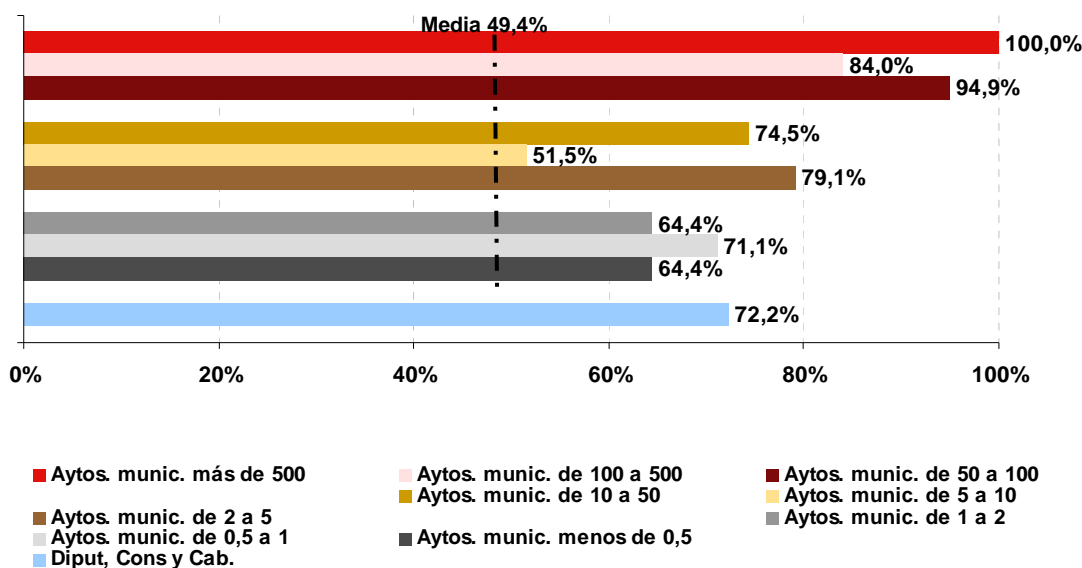
respuesta a la petición de acceso, el interesado podrá interponer la reclamación prevista. El responsable del fichero o tratamiento deberá excluir del tratamiento los datos relativos al afectado que ejercite su derecho de oposición o denegar motivadamente la solicitud del interesado en el plazo antes mencionado.

En resumen, existe la obligación para las Entidades de dar información a los ciudadanos sobre cómo estos deben ejercer sus derechos ARCO. En este sentido, se debe facilitar al interesado un medio sencillo y gratuito para manifestar su negativa al tratamiento de los datos tal y como se recoge de forma más amplia en los art. 25 y 26 del RDLOPD.

Se trata de una medida que está bastante extendida entre los Ayuntamientos y las Diputaciones, Consells y Cabildos Insulares donde en un 49,4% y un 52,8% se lo otorgan a sus interesados. Por tamaño del estrato son tanto los ayuntamientos de municipios grandes como los medianos los que cumplen con esta obligación (un 79% y un 58,1% respectivamente). En el caso de los de menor tamaño un 45,4% de los ayuntamientos de municipios pequeños informan a los interesados de cómo proceder.

La implantación de este deber se realiza de forma heterogénea (Gráfico 19), donde el 100% de los núcleos de más 500.000 habitantes lo realizan, seguidos por los de poblaciones de 50.000 a 100.000 habitantes y los de 100.000 a 500.000 habitantes donde más del 70% de sus gobiernos lo efectúan (79,5% y 75% respectivamente). El menor nivel de cobertura se da en los ayuntamientos de 5.000 a 10.000 habitantes donde es realizada por más del 50% de los gobiernos.

Gráfico 19: Información al interesado de cómo proceder para ejercer los derechos ARCO, en función del tamaño de los municipios (%)



Fuente: INTECO

8 MEDIDAS 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 ha tratado en el epígrafe 5.3.

A continuación, se analiza el nivel de cumplimiento de las medidas de seguridad exigidas en el RDLOPD, comprendiendo los controles tanto de gestión como de carácter técnico, y clasificadas en niveles de seguridad.

8.1 Medidas de seguridad con controles de carácter técnico

8.1.1 Registro de incidencias

Una incidencia es cualquier anomalía que afecte o pudiera afectar a la seguridad, integridad, confidencialidad o disponibilidad de los datos de carácter personal.

El responsable de seguridad debe según el art. 100 del RDLOPD, mantener un registro de incidencias, para poder realizar un seguimiento a la resolución de las mismas. Para cada incidente se deben registrar los siguientes datos:

- Tipo de la incidencia.
- Fecha y hora en la que se produjo o en la que se detectó.
- Persona que la notifica.
- Persona a quien se le comunica.
- Descripción de la incidencia.
- Causas y efectos derivados de la incidencia.
- Medidas correctoras aplicadas para su resolución.

Este registro debe ser útil al responsable de seguridad para controlar que no haya ninguna incidencia sin resolver en el tiempo adecuado. Así mismo, la evaluación de las

causas puede dar lugar a la implantación de acciones preventivas para evitar repeticiones del mismo problema.

A pesar de lo establecido en la normativa la realidad muestra que son pocos los ayuntamientos y las Diputaciones, Consells y Cabildos Insulares que lo realizan (un 21,1% y un 38,9% respectivamente). A nivel de estrato es realizado por 6 de cada 10 ayuntamientos de grandes municipios (61,5%), por 3 de cada 10 ayuntamientos de mediano municipio (33,4%) y por un 15,5% de los gobiernos de pequeños organismos.

La Tabla 21 muestra que únicamente los Ayuntamientos grandes disponen de un registro de incidencias en un porcentaje superior a 50%, entendidas estas como cualquier problema que afecte a la seguridad de los datos.

Los Ayuntamientos más pequeños, de entre 500 a 1.000 y menos de 500 están por debajo del 14%, siendo insuficiente la implantación de esta medida. Mientras que el 52,8% de las Diputaciones, Consells y Cabildos Insulares no registran sus incidencias. Como consecuencia existe una pobre gestión de la seguridad de los datos personales y una supervisión de los problemas improvisada.

Tabla 21: Realización de un registro de la incidencia, el momento en que se ha producido, la persona que la notifica, la persona a la que se le comunica y los efectos derivados en los sistemas de información, por tamaño (%)

Población (en miles)		Distribución porcentual			Distribución media ponderada		
		SI	NO	NS/NC	SI	NO	NS/NC
Grandes	Más de 500	100,0%	0,0%	0,0%			
	De 100 a 500	68,0%	32,0%	0,0%	61,5%	37,0%	1,4%
	De 50 a 100	53,8%	43,6%	2,6%			
Medianos	De 10 a 50	41,6%	46,0%	12,4%			
	De 5 a 10	27,3%	63,6%	9,1%	33,4%	53,1%	13,5%
	De 2 a 5	31,3%	52,2%	16,4%			
Pequeños	De 1 a 2	28,8%	59,3%	11,9%			
	De 0,5 a 1	10,5%	76,3%	13,2%	15,5%	71,2%	13,3%
	Aytos. Munic. menos 0,5	13,7%	72,6%	13,7%			
Diputaciones, Consells y Cabildos Insulares		38,9%	52,8%	8,3%			

Fuente: INTECO

8.1.2 Identificación y autenticación

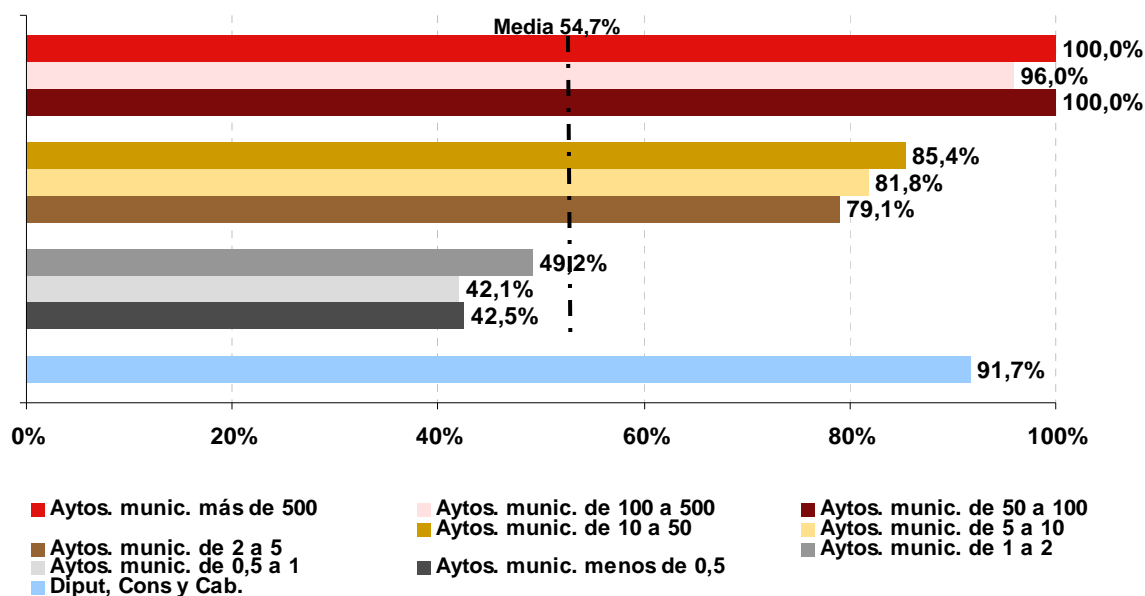
Las entidades deben establecer conforme al art. 93 del RDLOPD criterios para asignar derechos de acceso de los trabajadores a los sistemas de información en función de su desempeño. Siendo importante que las revisen periódicamente y actualicen los derechos, en caso de bajas o cambios.

El 54,7% de los ayuntamientos y el 91,7% de las Diputaciones, Consells y Cabildos Insulares lo llevan a cabo. Por nivel de estrato, más de 9 de cada 10 ayuntamientos de grandes municipios lo realizan (un 98,4%) y más del 81,6% de organismos de medianos municipios, mientras que los que lo realizan entre las entidades de menor tamaño son un 43,5%.

La cobertura de los municipios que han definido criterios de acceso para los usuarios de sus sistemas de información es superior al 80% entre los municipios de 2.000 y los de más de 500.000 habitantes.

Sin embargo los municipios de menos de 2.000 habitantes están por debajo del 50%, por lo que al no definir sus criterios de acceso, los usuarios no se rigen por ninguna política y no se controlará de forma adecuada quien accede a cada sistema de información.

Gráfico 20: Establecimiento de criterios de acceso de los usuarios a los sistemas de información, en función del tamaño de los municipios (%)



Fuente: INTECO

En cualquier caso el RDLOPD, en su artículo 91 referido al control de acceso, ya señala que “el responsable del fichero se encargará de que exista una relación actualizada de usuarios y perfiles de usuarios, y los accesos autorizados para cada uno de ellos”.

A nivel global la obligatoriedad de tener en sus entidades una lista o relación de usuarios es realizada por un 36,2% de los ayuntamientos y un 77,8% de las Diputaciones, Consells y Cabildos Insulares. Por tamaño de estrato un elevado porcentaje de ayuntamientos de grandes y medianos municipios también cumplen como se muestra en la Tabla 22.

Tabla 22: Existencia de una lista actualizada de usuarios, incluyendo los derechos de acceso que tiene autorizados, por tamaño (%)

Población (en miles)		Distribución porcentual			Distribución media ponderada		
		SI	NO	NS/NC	SI	NO	NS/NC
Grandes	Más de 500	66,7%	33,3%	0,0%	86,6%	13,4%	0,0%
	De 100 a 500	88,0%	12,0%	0,0%			
	De 50 a 100	87,2%	12,8%	0,0%			
Medianos	De 10 a 50	77,4%	18,2%	4,4%	64,5%	30,8%	4,8%
	De 5 a 10	60,6%	36,4%	3,0%			
	De 2 a 5	58,2%	35,8%	6,0%			
Pequeños	De 1 a 2	35,6%	62,7%	1,7%	24,4%	69,9%	5,7%
	De 0,5 a 1	18,4%	76,3%	5,3%			
	Aytos. Munic. menos 0,5	23,3%	69,9%	6,8%			
Diputaciones, Consells y Cabildos Insulares		77,8%	19,4%	2,8%			

Fuente: INTECO

Por otra parte las EELL tienen también la obligatoriedad de establecer algún proceso de autenticación o comprobación de la identidad del usuario. El uso de contraseñas, de tarjetas inteligentes o controles biométricos son medios disponibles para tal fin siempre que se gestionen correctamente,¹⁴ evitando por ejemplo que se utilicen de forma individual o que se creen grupos de usuarios que aunque facilitan la administración de identidades no permiten responsabilizar de los posibles incidentes de seguridad que pudieran ocasionarse.

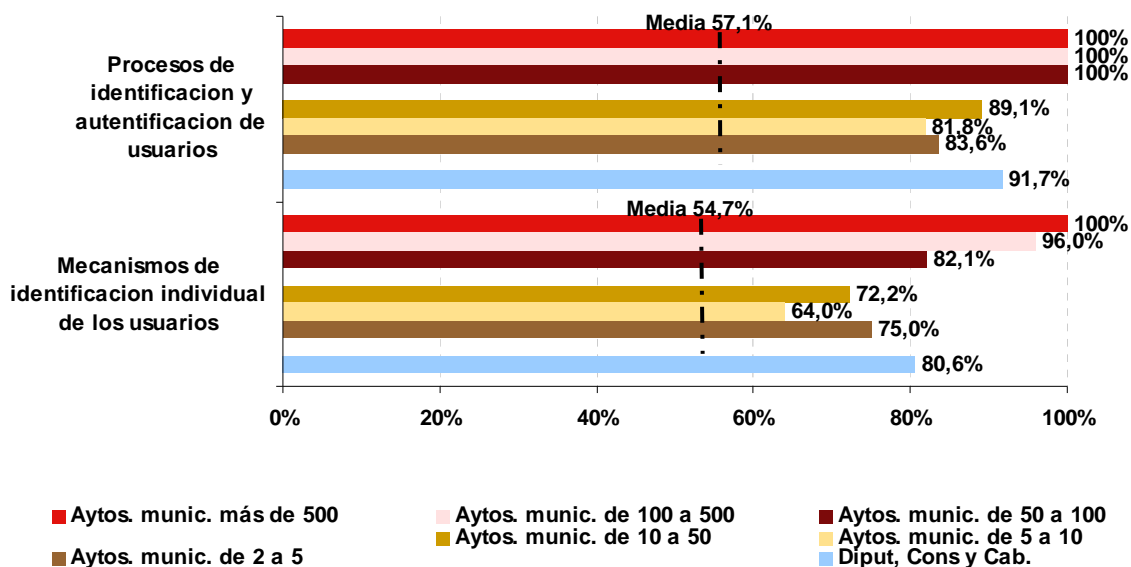
Por ese motivo, lo interesante es contrastar la opinión de las EELL en relación con la definición de procesos, para la identificación y autenticación de los usuarios y la existencia de mecanismos que permitan la identificación de forma individual e incuestionable de todo usuario y la verificación de que está autorizado. A nivel global la definición de los procesos se realiza por 57,1% de los Ayuntamientos y un 91,7% de las Diputaciones y en un 72,5% de los Ayuntamientos existen dichos mecanismos frente a un 80,6% de Diputaciones, Consells y Cabildos Insulares (Gráfico 21).

Se muestra en el gráfico que las entidades dan más importancia a los procesos de identificación, que facilita el reconocimiento de la identidad de los usuarios, y autenticación (con porcentajes superiores al 81%) que, a la existencia de mecanismos. Los cuales a pesar de la alta cobertura no son utilizados por la totalidad de las entidades

¹⁴ INTECO. Recomendaciones para la creación y uso de contraseñas seguras. Disponible en http://www.inteco.es/Seguridad/Observatorio/Estudios_e_Informes/Notas_y_Articulos/recomendaciones_creacion_uso_cont_rasenas

lo que hace creer que no es posible la identificación de forma individual de los usuarios que acceden a los ficheros con daos de carácter personal.

Gráfico 21: Definición de procesos para la identificación y autenticación vs. existencia de mecanismos que permitan la identificación de forma individualizada de los usuarios y la verificación de que está autorizado, en función del tamaño de los municipios (%)



Fuente: INTECO

No obstante, las EELL deben en el caso de que se haya elegido un método de autenticación por contraseñas, establecer una política que defina la forma de asignar y comunicar, la primera vez que se le otorgue a un usuario su acceso al sistema, así como su renovación periódica.

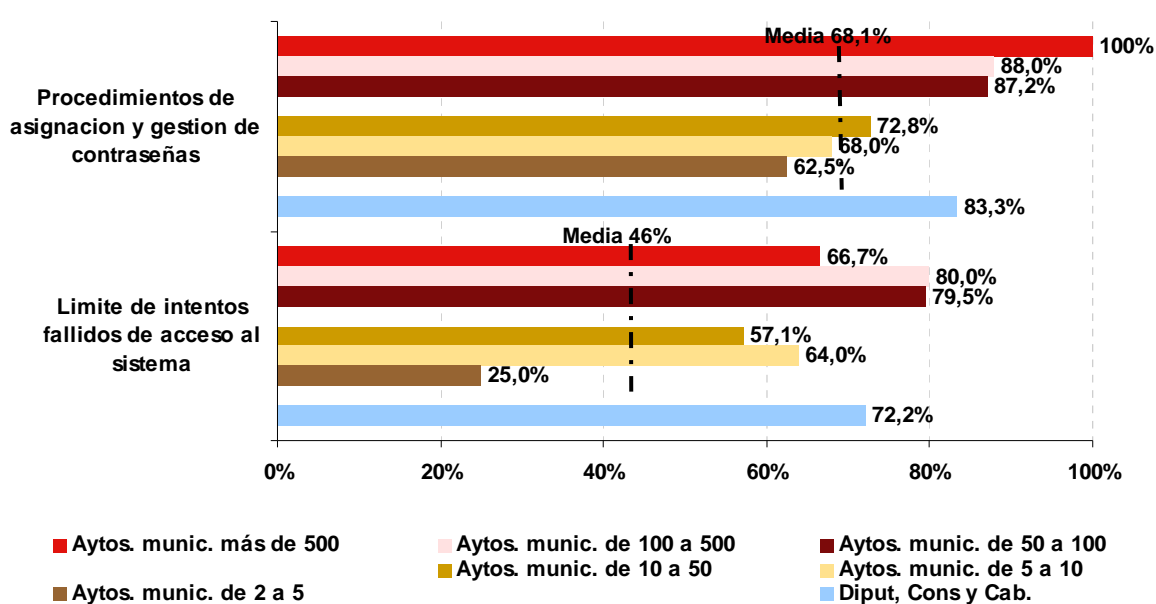
A nivel global un 68,1% y un 83,3% de los Ayuntamientos y las Diputaciones, Consells y Cabildos Insulares respectivamente han establecido procedimientos de asignación y gestión de las contraseñas. Además un análisis por tamaño del estrato muestra que la implantación de procedimientos de asignación y gestión de contraseñas tiene una cobertura elevada. Así los municipios de más de 50.000 habitantes están por encima del 87%, incluso las Diputaciones, Consells y Cabildos Insulares tienen un 83,3% de cobertura para este control de seguridad (Gráfico 22).

Además existe otra medida de seguridad como es el control de los intentos fallidos de acceso por parte de los usuarios, exigida por el RDLOPD en su art. 103 donde establece “de cada intento de acceso se guardarán, como mínimo, la identificación del usuario, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado”.

Esta práctica no es utilizada masivamente por los ayuntamientos donde el 46% de los mismos afirma haberla puesto en marcha por un 72,2% de las Diputaciones, Consells y Cabildos Insulares, En el Gráfico 22 se comprueba que a nivel del tamaño de los ayuntamientos esta práctica se realiza de forma heterogénea por las entidades, dado que entorno al 80% de los organismos de entre 50.000 y 500.000 si lo llevan a cabo frente al 66,7% de los municipios de más de 500.000 habitantes.

Además destaca que el 25% de los municipios de 2.000 a 5.000 habitantes no hayan implantado este control, posibilitando ataques de fuerza bruta que prueban masivamente posibles contraseñas hasta obtener la clave de acceso.

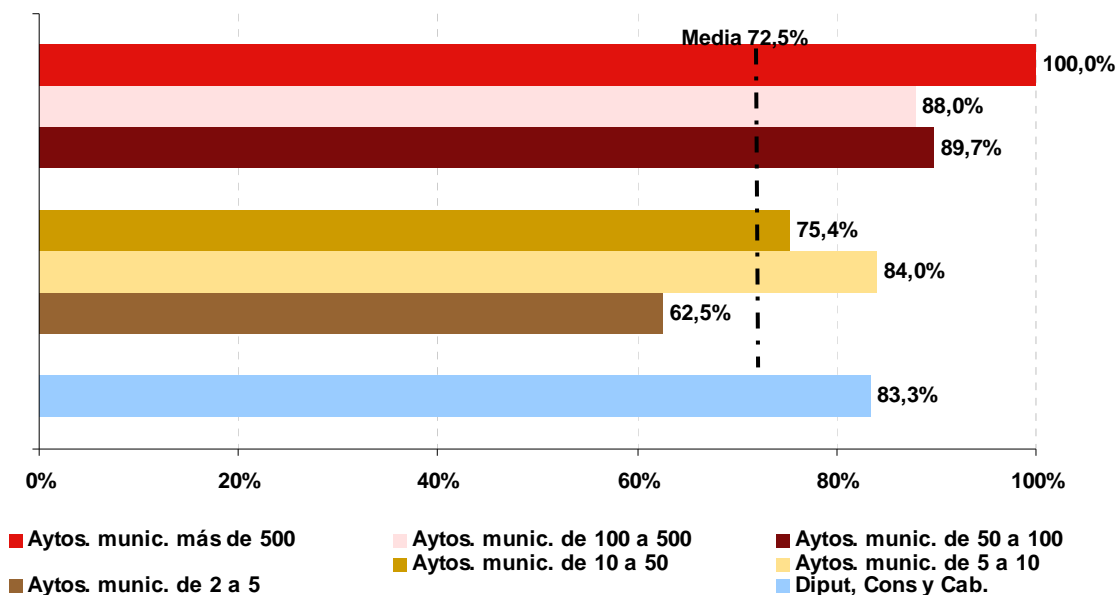
Gráfico 22: Establecimiento de procedimientos de asignación y gestión de contraseñas vs. establecimiento de un límite para los intentos reiterados fallidos de acceso al sistema, en función del tamaño de los municipios (%)



Fuente: INTECO

En caso de que las contraseñas se guarden, debe hacerse de forma que no sean legibles para evitar que una persona no autorizada tenga acceso a ellas de forma fraudulenta. El 72,5% de los Ayuntamientos y el 83,3% de las Diputaciones, Consells y Cabildos Insulares almacenan las contraseñas de forma ininteligible. El análisis por tamaño de los municipios muestra también una alta cobertura para esta medida de seguridad, con porcentajes superiores al valor medio de los ayuntamientos, salvo en los 2.000 a 5.000 habitantes donde el 62,5% de los organismos realiza esta medida.

Gráfico 23: Almacenamiento de contraseñas de forma ininteligible, en función del tamaño de los municipios (%)



Fuente: INTECO

8.1.3 Control de acceso

Los derechos de acceso, como se han indicado anteriormente, deben ser concedidos en función a la necesidad de saber o el desempeño que tengan los usuarios en el sistema, estando el responsable de seguridad obligado a garantizar este control tal y como se establece en el art. 91 del RDLOPD.

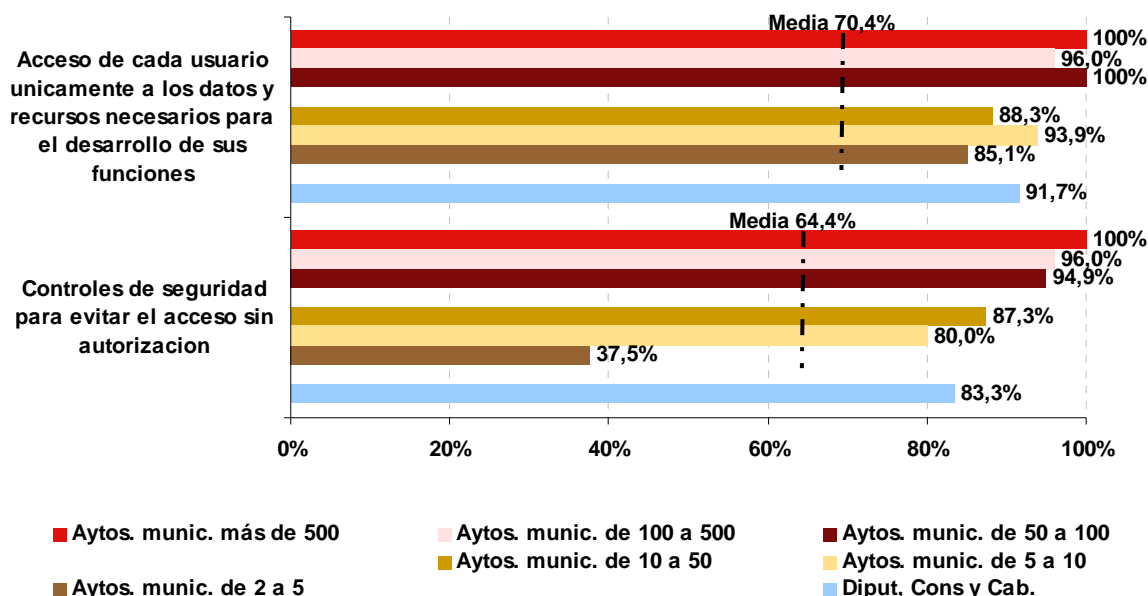
Para facilitar la comprensión de la importancia en la asunción de este control por las Entidades, se ha realizado una comparativa de la asignación para cada usuario únicamente a los datos y recursos necesarios en el desarrollo de sus funciones, en relación, con la existencia de controles de seguridad para evitar el acceso a datos o recursos por usuarios, sin estar previamente autorizados.

El análisis a nivel global muestra que el 70,4% de los ayuntamientos y el 91,7% de las Diputaciones, Consells y Cabildos Insulares afirman que cada usuario accede a los datos necesarios conforme al puesto que desempeñan en estas entidades. En relación con la existencia de los controles estos son realizados por un 64,4% de los ayuntamientos y 83,3% de las Diputaciones.

El Gráfico 24 muestra el nivel de cumplimiento de estas medidas por tamaño del estrato y número de habitantes donde existe una cobertura superior a la media para estos dos controles, salvo en el caso del 37,5% de los ayuntamientos de 2.000 a 5.000 habitantes que afirman no establecer controles de seguridad a pesar de que un 85,1% los ayuntamientos con esta población si regula los accesos.

Las Diputaciones, Consells y Cabildos Insulares están en la misma situación, con un 91,7% de cobertura para el establecimiento de los accesos, pero sólo un 83,3% de implantación de controles para asegurar que se cumplen estos derechos.

Gráfico 24: Establecimientos de controles de acceso mediante la asignación de los permisos para cada usuario de forma individualizada vs. establecimiento de controles de seguridad para evitar el acceso sin autorización, en función del tamaño de los municipios (%)



Fuente: INTECO

Los derechos de acceso deben ser concedidos sólo por quien haya designado el responsable del fichero, siendo habitualmente el administrador o administradores de sistemas los que materializan los permisos de accesos a los sistemas de los usuarios. Las entidades deben establecer un mecanismo de autorizaciones para que el administrador tenga la garantía suficiente de que debe otorgar el acceso al usuario que lo haya solicitado.

El 78% de los ayuntamientos y el 94,4% de las Diputaciones, Consells y Cabildos Insulares han establecido algún procedimiento para asegurar que los derechos de acceso son autorizados únicamente por el personal designado.

En la Tabla 23 se muestra el alto grado de cobertura de las Entidades para el cumplimiento de esta medida de seguridad. Los estratos de municipios grandes, con más de 50.000 habitantes, tienen el 100% de cumplimiento y los estratos medianos de más de 2.000 habitantes alcanzan el 80,6% de cobertura. Mientras que en los municipios pequeños, que suelen tener porcentajes más bajos para el cumplimiento de medidas de seguridad, hay más de un 68% de cumplimiento.

Tabla 23: Concesión de permisos de acceso para los usuarios realizada solamente por personal autorizado, por tamaño (%)

Población (en miles)		Distribución porcentual			Distribución media ponderada		
		SI	NO	NS/NC	SI	NO	NS/NC
Grandes	Más de 500	100,0%	0,0%	0,0%	100,0%	0,0%	0,0%
	De 100 a 500	100,0%	0,0%	0,0%			
	De 50 a 100	100,0%	0,0%	0,0%			
Medianos	De 10 a 50	92,7%	2,2%	5,1%	86,7%	8,3%	5,0%
	De 5 a 10	90,9%	6,1%	3,0%			
	De 2 a 5	80,6%	13,4%	6,0%			
Pequeños	De 1 a 2	76,3%	22,0%	1,7%	74,2%	20,0%	5,7%
	De 0,5 a 1	68,4%	26,3%	5,3%			
	Aytos. Munic. menos 0,5	75,3%	17,8%	6,8%			
Diputaciones, Consells y Cabildos Insulares		94,4%	5,6%	0,0%			

Fuente: INTECO

Por último a la hora de establecer el control de acceso, es importante que la ubicación de los sistemas de información de las entidades deba contar con un control de acceso físico. Esto impedirá que cualquier persona no autorizada tenga acceso y pueda realizar cualquier manipulación fraudulenta.

A nivel global se puede comprobar que el control de acceso físico no tiene tanta implantación como el acceso lógico, si lo realizan el 55,6% de los ayuntamientos y el 69,4% de las Diputaciones, Consells y Cabildos Insulares.

Tabla 24: Acceso físico a los sistemas de información, por tamaño (%)

Población (en miles)		Distribución porcentual			Distribución media ponderada		
		SI	NO	NS/NC	SI	NO	NS/NC
Grandes	Más de 500	100,0%	0,0%	0,0%	78,8%	21,2%	0,0%
	De 100 a 500	72,0%	28,0%	0,0%			
	De 50 a 100	82,1%	17,9%	0,0%			
Medianos	De 10 a 50	76,6%	21,9%	1,5%	64,3%	33,8%	1,9%
	De 5 a 10	63,6%	30,3%	6,1%			
	De 2 a 5	56,7%	43,3%	0%			
Pequeños	De 1 a 2	52,5%	45,8%	1,7%	51,8%	44,8%	3,5%
	De 0,5 a 1	50,0%	47,4%	2,6%			
	Aytos. Munic. menos 0,5	52,1%	43,8%	4,1%			
Diputaciones, Consells y Cabildos Insulares		69,4%	27,8%	2,8%			

Fuente: INTECO

Por tamaño del municipio la Tabla 24 muestra que los municipios de menos de 2.000 habitantes tienen alrededor de un 50% de cobertura, por lo que la mitad de estos Ayuntamientos no tienen implantado ningún control de acceso físico.

8.1.4 Registro de accesos

Entre las medidas requeridas para los ficheros clasificados como nivel alto, está el registro de accesos, que implica un control exhaustivo para cada uno de ellos, de acuerdo a lo que establece el art 103 del RDLOPD, capturando la siguiente información de cada intento de acceso:

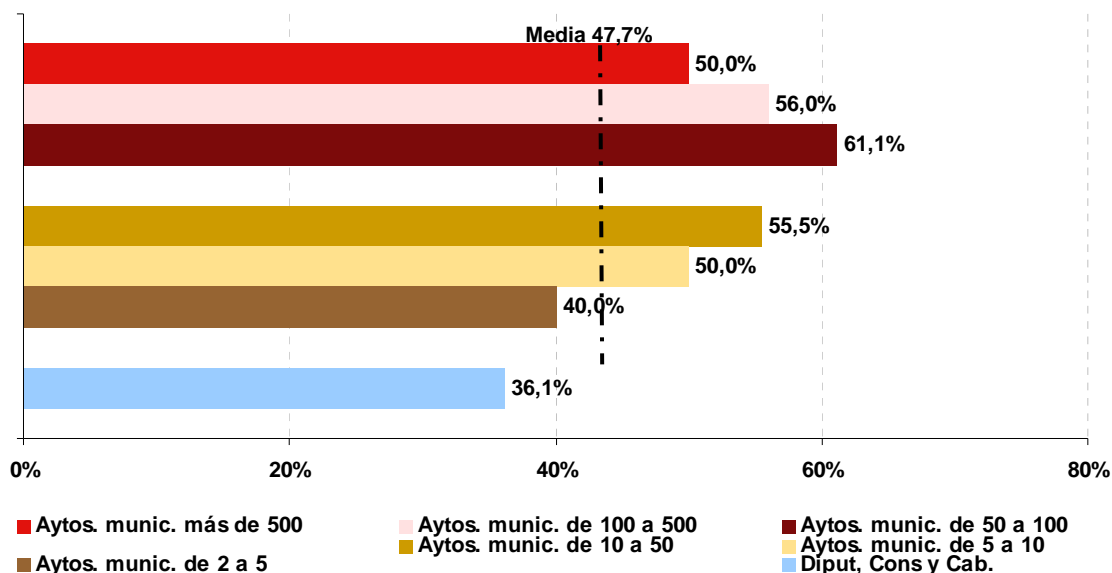
- Identificación del usuario.
- Fecha y hora en la que se realizó.
- Fichero accedido.
- Tipo de acceso: consulta, modificación, borrado, etc.
- Si ha sido autorizado o denegado el acceso.
- Registro concreto accedido: en el caso de que el acceso hubiese sido autorizado.

A nivel global un 47,7% de los ayuntamientos y un 36,1% de las Diputaciones, Consells y Cabildos Insulares llevan a cabo un registro de acceso por cual se guardan, de cada acceso a los datos la información antes mencionada.

A nivel de estratos las entidades de menor tamaño no han respondido a esta pregunta pero si el resto, así el 58,6% de los ayuntamientos de grande tamaño y el 47% de los medianos disponen de dicho registro.

En el Gráfico 25 se puede comprobar cuál es el grado de cumplimiento en las entidades clasificadas por el número de habitantes que tienen. Se puede comprobar en que al menos, un 40% de los Ayuntamientos tiene implantado este control, siendo el estrato de 50.000 a 100.000 habitantes el que mayor cobertura presenta con un 61,1% de cumplimiento.

Gráfico 25: Registro de los accesos a los datos, en función del tamaño de los municipios (%)



Fuente: INTECO

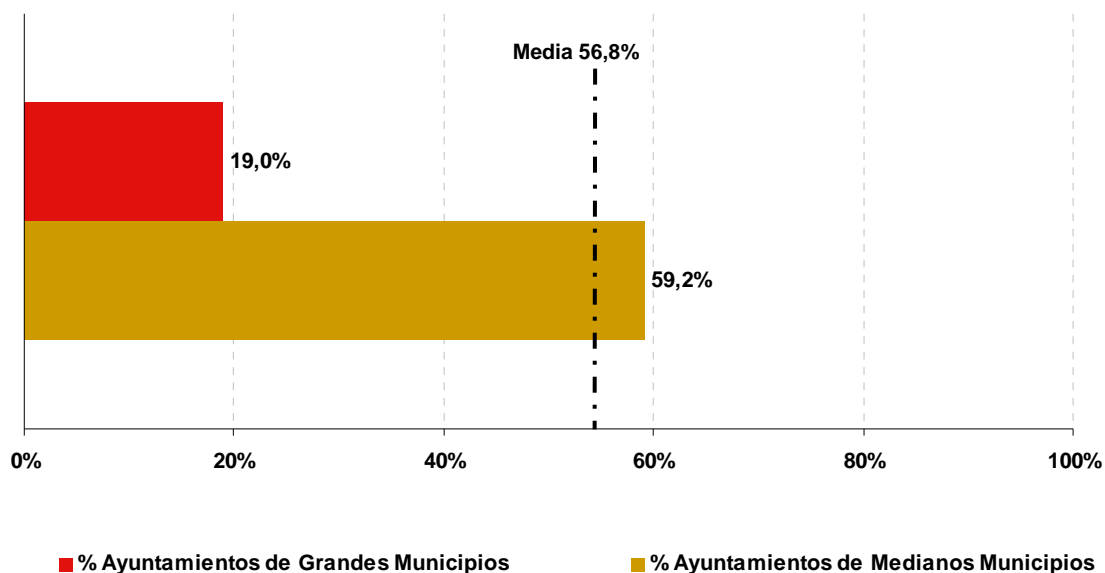
Otros elementos que las entidades han de tener en cuenta respecto a los registros de acceso son el periodo de conservación y el control de los registros mediante la emisión de un informe mensual tal y como establece la normativa.

Respecto al primero de ellos, el art. 103.4 establece que el periodo mínimo de conservación de los datos registrados será de dos años. El nivel de cumplimiento a nivel global es de un 62,1% en los ayuntamientos y de un 47,2% en las Diputaciones, Consells y Cabildos Insulares. Por tamaño de las entidades el porcentaje de ayuntamientos varía entre un 67% y un 61,8% para los de mayor y los de mediano tamaño respectivamente.

Por otro lado, el art. 103.5 del RDLOPD establece que el responsable de seguridad se encargará de revisar al menos una vez al mes la información de control registrada y elaborará un informe de las revisiones realizadas y los problemas detectados. Esto es cumplido por el 26,6% de los ayuntamientos y el 13,9% de las Diputaciones, Consells y Cabildos Insulares a nivel global.

Ahora bien lo interesante es conocer el motivo del bajo cumplimiento en las entidades. Para ello se debe conocer cuál es el grado de respuesta ante la realización del informe mensual en aquellas entidades que afirmaron haber nombrado un responsable de seguridad. El Gráfico 26 muestra como a nivel global el 56,8% de las entidades cumplen con dicha función; respecto a este valor medio, el comportamiento por estratos muestra que el porcentaje de ayuntamientos de mediano tamaño es de 59,2% entidades mientras que los de gran tamaño está en un 19%.

Gráfico 26: Realización por los responsables de seguridad de un control de los registros emitiendo un informe mensual en aquellas EELL que han nombrado a éste, por tamaño (%)

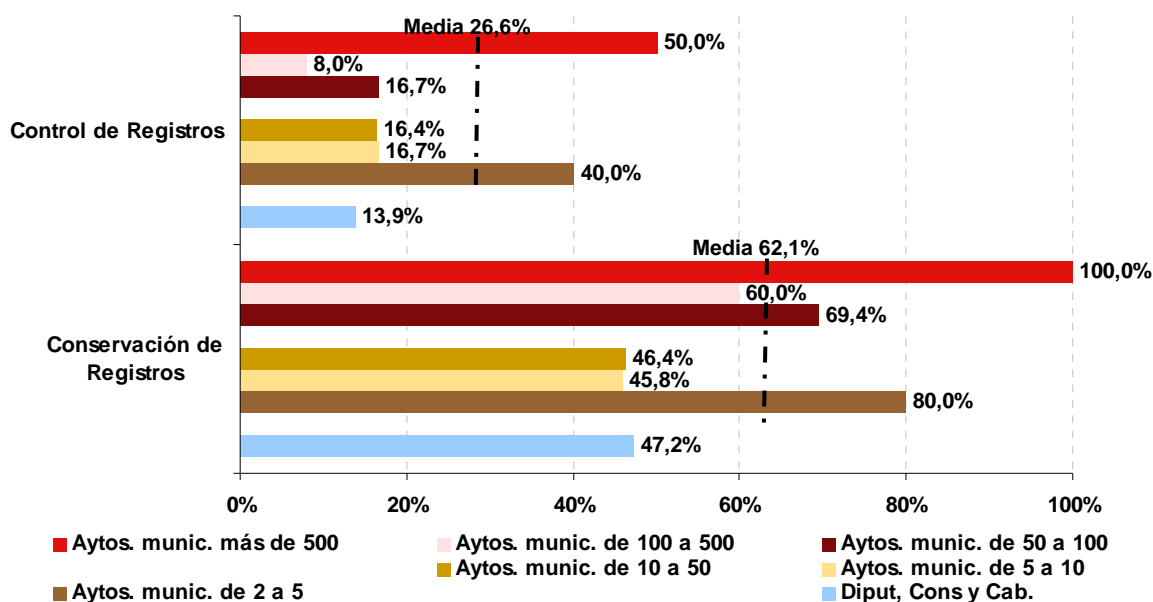


Fuente: INTECO

Un análisis por tamaño de los municipios muestra como es el comportamiento de las entidades en relación con la conservación y el control de registros. Respecto a este último, el control y revisión de los registros por parte del responsable de seguridad, se realiza por un 50%-40% respectivamente en los municipios de más de 500.000 habitantes y en los de 2.000 a 5.000, mientras que en el resto incluidas las Diputaciones, Consells y Cabildos Insulares no supera el 17% de cobertura.

No obstante, la conservación de los registros, como se observa en el Gráfico 27, es una medida con mayor grado de cumplimiento, de modo que su cumplimiento supera el 60% en los ayuntamientos grandes. Un caso excepcional es el de los organismos de 2.000 a 5.000 habitantes donde el 80% de los municipios con está población cumplen con lo establecido en la normativa. El resto de municipios incluidas las Diputaciones, Consells y Cabildos Insulares están entorno a un 45,8%-47,2% de entidades que conservan durante dos años los registros de los datos.

Gráfico 27: Realización del control de los registros de acceso y conservación de los mismos por las EELL, en función del tamaño de los municipios (%)



Fuente: INTECO

8.1.5 Telecomunicaciones

El RDLOPD exige en su art. 104, para datos personales clasificados como nivel alto, la implantación de controles que garanticen la confidencialidad y la integridad en las transmisiones a través de redes públicas o redes inalámbricas de comunicaciones electrónicas. Además se presenta como mecanismo más habitual para cumplir este control, el cifrado de los datos, dado que garantiza que la información no será inteligible ni manipulada por terceros.

A nivel global el 46,8% de los ayuntamientos y el 58,3% de las Diputaciones, Consells y Cabildos Insulares afirman cifrar los datos en las transmisiones. Un análisis en profundidad del grado de respuesta por tamaño del municipio se puede ver en la Tabla 25, donde el 100% de las Entidades de más de 500.000 habitantes tienen implantada esta medida, en el lado opuesto están el 40% de los municipios de 2.000 a 5.000 habitantes.

Tabla 25: Cifrado de los datos en las transmisiones a través de redes de telecomunicaciones, por tamaño (%)

Población (en miles)		Distribución porcentual			Distribución media ponderada		
		SI	NO	NS/NC	SI	NO	NS/NC
Grandes	Más de 500	100,0%	0,0%	0,0%	60,7%	34,6%	4,7%
	De 100 a 500	52,0%	44,0%	4,0%			
	De 50 a 100	63,9%	30,6%	5,6%			
Medianos	De 10 a 50	55,5%	33,6%	10,9%	46,0%	28,2%	25,8%
	De 5 a 10	45,8%	37,5%	16,7%			
	De 2 a 5	40,0%	20,0%	40,0%			
Diputaciones, Consells y Cabildos Insulares		58,3%	13,9%	27,8%			

Fuente: INTECO

8.2 Medidas de seguridad con controles de gestión

8.2.1 Gestión de soportes y documentos

El responsable de seguridad tiene obligación de realizar una gestión efectiva de los soportes que existan en la Entidad, conforme a lo establecido en el art. 92 del RDLOPD.

Así el art. 92.1, señala que los soportes y documentos que contengan datos de carácter personal deberán permitir identificar el tipo de información que contiene, ser inventariados y sólo deberán ser accesibles por el personal autorizado para ello en el documento de seguridad. La excepción viene establecida cuando las características físicas del soporte imposibiliten su cumplimiento, quedando constancia motivada de ello en el documento de seguridad.

En relación con la identificación de la información contenida en los soportes, el 58,3% de los ayuntamientos y el 72,2% de las Diputaciones, Consells y Cabildos Insulares lo realizan evitando de esta forma que estos puedan ser confundidos, extraviados o sobrescritos al no estar adecuadamente identificados. El resultado por tamaño de los municipios no difiere de estos datos globales (ver Tabla 26), mejorando incluso el grado de cumplimiento para la práctica totalidad de los estratos de los ayuntamientos salvo en el caso de los de 500 a 1.000 habitantes donde el porcentaje es del 55,3% y para los de menos de 500 habitantes (54,8%).

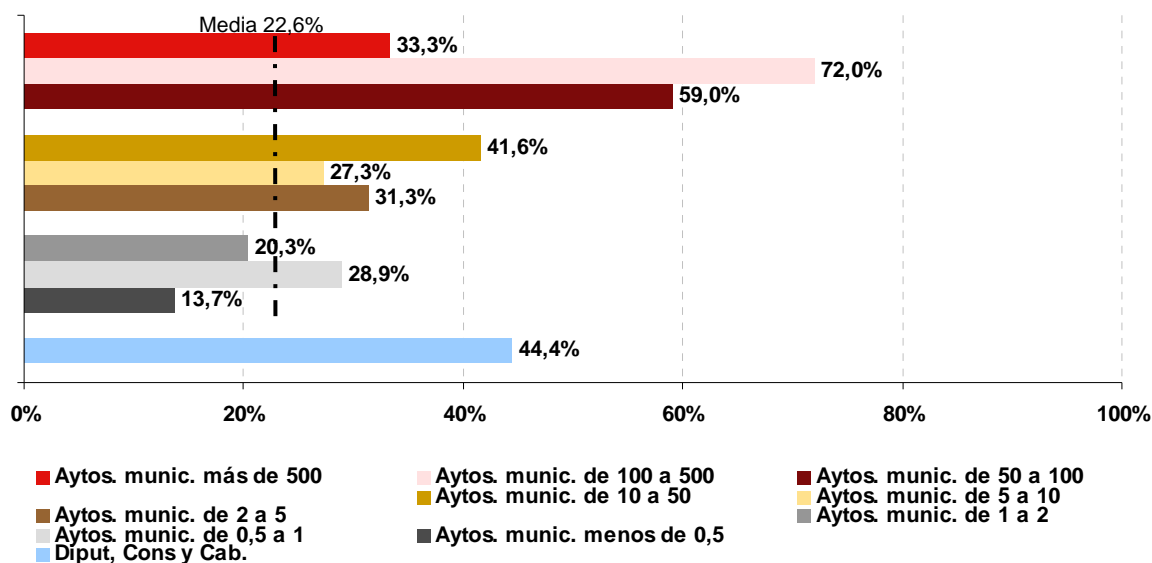
Tabla 26: Identificación de la información contenida en los soportes, por tamaño (%)

Población (en miles)	Distribución porcentual			Distribución media ponderada			
	SI	NO	NS/NC	SI	NO	NS/NC	
Grandes	Más de 500	100,0%	0,0%	0,0%	71,5%	27,1%	1,4%
	De 100 a 500	68,0%	32,0%	0,0%			
	De 50 a 100	71,8%	25,6%	2,6%			
Medianos	De 10 a 50	64,2%	24,8%	10,9%	64,8%	20,8%	14,5%
	De 5 a 10	63,6%	24,2%	12,1%			
	De 2 a 5	65,7%	16,4%	17,9%			
Pequeños	De 1 a 2	59,3%	30,5%	10,2%	55,6%	25,5%	18,9%
	De 0,5 a 1	55,3%	34,2%	10,5%			
	Ayts. Munic. menos 0,5	54,8%	21,9%	23,3%			
Diputaciones, Consells y Cabildos Insulares		72,2%	16,7%	11,1%			

Fuente: INTECO

Además para una gestión eficaz, la normativa establece que el responsable de seguridad debe mantener un inventario en el que se registren todos los soportes destinados a contener datos personales que hayan sido autorizados en la Entidad. A nivel global el 22,6% de los ayuntamientos y el 44,4% de las Diputaciones, Consells y Cabildos Insulares afirman que en sus entidades existe un inventario de los soportes.

Gráfico 28: Inventario de soportes, en función del tamaño de los municipios (%)



Fuente: INTECO

Por tamaño del municipio el 72% de los ayuntamientos de 100.000 a 500.000 habitantes y el 59% de los de 50.000 a 100.000 afirman disponer del mismo. El resto de los estratos

tiene un grado de cumplimiento desigual, destacando los estratos pequeños en los que a priori se supone que tendrían menos dificultad dado el volumen de ficheros de los que disponen (Gráfico 28).

Respecto a la accesibilidad de los soportes y documentos está en relación con el acceso restringido al sitio donde se almacenan. Dicha restricción afirman realizarla a nivel global el 64,8% de los ayuntamientos y el 69,4% de las Diputaciones, Consells y Cabildos Insulares.

A nivel municipal se puede comprobar en la Tabla 27 que este control tiene un grado de implantación aceptable, así un 81,8% de los municipios de entre 5.000 y 50.000 habitantes lo realizan, mientras que en los ayuntamientos de menor tamaño el porcentaje de municipios es entorno al 60%.

Tabla 27: Control de acceso físico a los soportes, por tamaño (%)

Población (en miles)		Distribución porcentual			Distribución media ponderada		
		SI	NO	NS/NC	SI	NO	NS/NC
Grandes	Más de 500	66,7%	33,3%	0,0%	83,4%	16,6%	0,0%
	De 100 a 500	80,0%	20,0%	0,0%			
	De 50 a 100	87,2%	12,8%	0,0%			
Medianos	De 10 a 50	81,8%	16,1%	2,2%	75,0%	20,9%	4,1%
	De 5 a 10	81,8%	15,2%	3,0%			
	De 2 a 5	67,2%	26,9%	6,0%			
Pequeños	De 1 a 2	61,0%	37,3%	1,7%	60,5%	32,0%	7,5%
	De 0,5 a 1	65,8%	28,9%	5,3%			
	Aytos. Munic. menos 0,5	58,9%	31,5%	9,6%			
Diputaciones, Consells y Cabildos Insulares		69,4%	25,0%	5,6%			

Fuente: INTECO

Por otra parte el art. 92.2 del RDLOPD estipula que la salida de soportes y documentos que contengan datos de carácter personal, incluidos los comprendidos y/o ajenos a un correo electrónico, fuera de los locales bajo el control del responsable del fichero o tratamiento deberá ser autorizada por el responsable del fichero o encontrarse debidamente autorizada en el documento de seguridad.

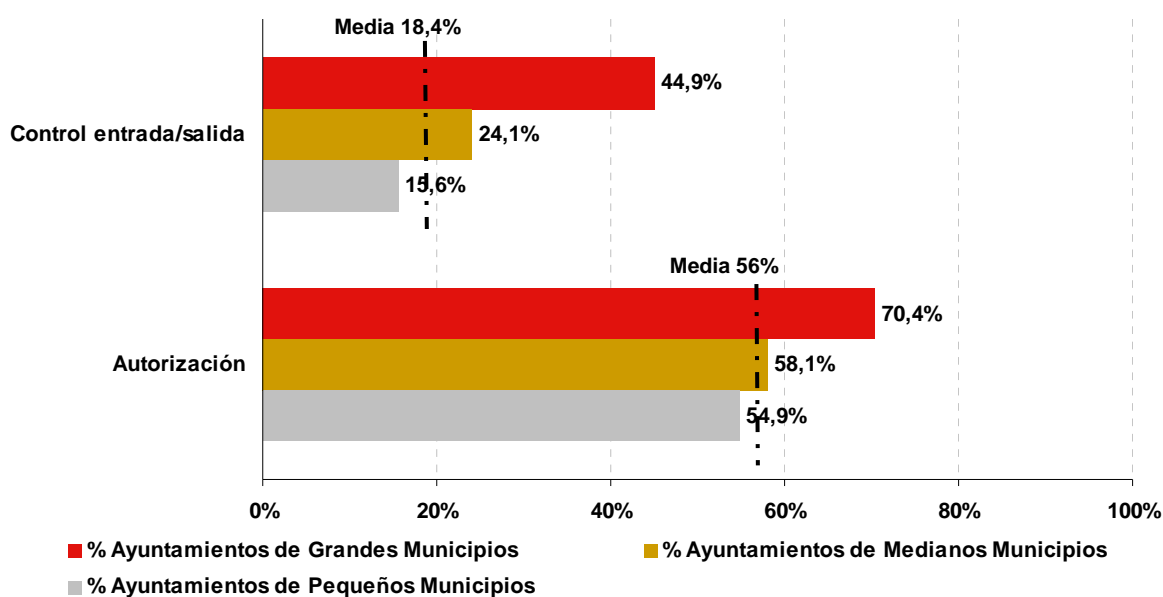
Siendo además necesario establecer cuando se vaya a proceder al traslado de la documentación lo establecido en el art. 92.3 del RDLOPD en relación con las medidas a adoptar para evitar la sustracción, pérdida o acceso indebido a la información durante su transporte.

A nivel global el control de la salida y entrada de soportes es realizado por el 18,4% de los ayuntamientos y por un 30,6% de las Diputaciones, Consells y Cabildos Insulares.

Mientras que la autorización por parte del responsable de seguridad es efectuado por el 56% de los ayuntamientos y el 52,8% de las Diputaciones, Consells y Cabildos Insulares.

A nivel de tamaño del estrato existe una disparidad en la asunción de estas obligaciones, mientras que el porcentaje de ayuntamientos de grandes municipios es superior al 44% en el control y al 70% en la autorización, en el caso de los organismos de mediano y pequeño tamaño el porcentaje de los que cumplen se aproxima al valor global.

Gráfico 29: Gestión de salida y entrada de soportes vs. autorización, por tamaño (%)



Fuente: INTECO

Asimismo el art. 92.4 establece otra serie de medidas a poner en marcha siempre que vaya a desecharse cualquier documento o soporte que contengan datos de carácter personal consistente en la destrucción o borrado a fin de evitar el acceso a la información contenida en el mismo o su recuperación posterior. El problema de fondo es que está las entidades tienden a deshacerse de los dispositivos sin haberse asegurado de haber eliminado toda la información. Incluso estiman que el borrado es suficiente para garantizar el acceso a la información almacenada. La solución pasa por realizar un análisis previo de las necesidades y tener claro el fin del soporte, es decir si debe reutilizarse o no¹⁵.

¹⁵ INTECO. Reutilización y sustitución segura de dispositivos de almacenamiento. Disponible en http://www.inteco.es/Seguridad/Observatorio/Estudios_e_Informes/Notas_y_Articulos/Reutilizacion_y_sustitucion_segura_de_dispositivos_11

Preguntadas las entidades al efecto, la respuesta a nivel global la respuesta ha sido que el 39,6% de los ayuntamientos y el 36,1% de las Diputaciones, Consells y Cabildos Insulares ejecutan medidas para impedir la recuperación indebida de la información.

La Tabla 28 muestra como es la respuesta por tamaño del municipio, donde destaca que el 66,7% de los ayuntamientos de más de 500.000 habitantes cumplen con esta obligación y entre los de menor tamaño destacan el 40% de los de 5.000 a 10.000 habitantes.

Tabla 28: Existencia de medidas para impedir la recuperación indebida de información, por tamaño (%)

Población (en miles)		Distribución porcentual			Distribución media ponderada		
		SI	NO	NS/NC	SI	NO	NS/NC
Grandes	Más de 500	66,7%	33,3%	0,0%			
	De 100 a 500	48,0%	52,0%	0,0%	50,6%	46,5%	2,8%
	De 50 a 100	51,3%	43,6%	5,1%			
Medianos	De 10 a 50	39,7%	46,8%	13,5%			
	De 5 a 10	40,0%	52,0%	8,0%	38,2%	46,3%	15,5%
	De 2 a 5	25,0%	25,0%	50,0%			
Diputaciones, Consells y Cabildos Insulares		36,1%	44,4%	19,4%			

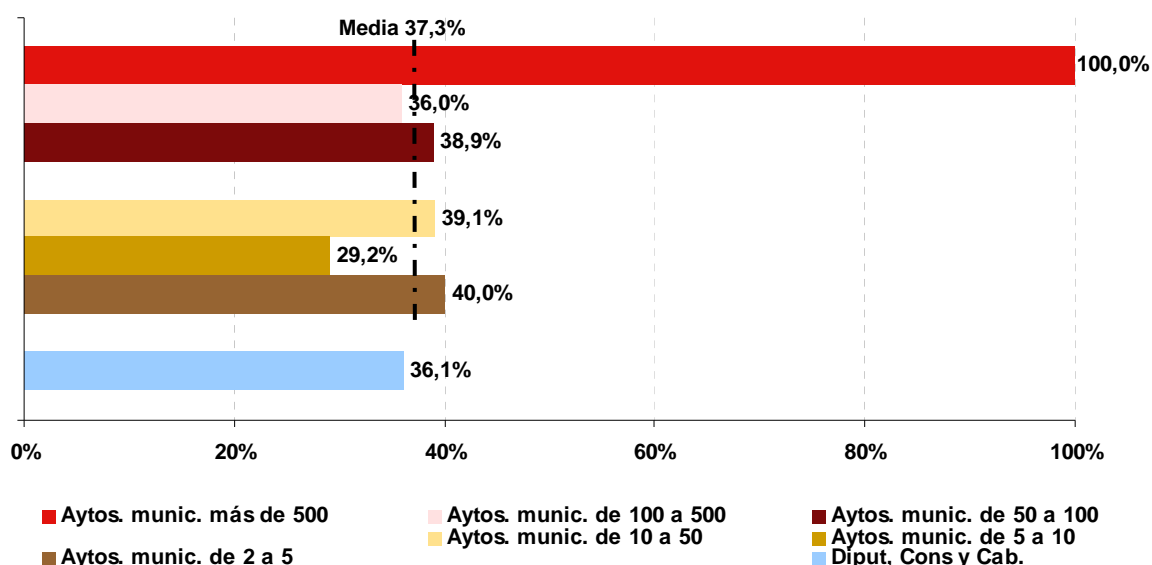
Fuente: INTECO

Por último, existen unas medidas de seguridad de nivel alto relativas a la gestión y distribución de soportes como son la identificación, la distribución de los soportes y el tratamiento en dispositivos portátiles. Respecto a la identificación, el art. 101.1 del RDLOPD indica que se deberá realizar utilizando sistemas de etiquetado comprensibles y con significado que permitan a los usuarios con acceso autorizado a los citados soportes y documentos identificar su contenido, y que dificulten la identificación para el resto de personas.

En relación con la distribución de los soportes, el art. 101.2 establece que se realizará cifrando dichos datos o bien utilizando otro mecanismo que garantice que dicha información no sea accesible o manipulada durante su transporte. Asimismo, se cifrarán los datos que contengan los dispositivos portátiles cuando éstos se encuentren fuera de las instalaciones que están bajo el control del responsable del fichero. Complementariamente el art. 101.3 recoge que deberá evitarse el tratamiento de datos en dispositivos portátiles que no permitan su cifrado. En caso de que sea estrictamente necesario se hará constar, motivadamente, en el documento de seguridad y se adoptarán medidas que tengan en cuenta los riesgos de realizar tratamientos en entornos desprotegidos.

El cumplimiento de estas prerrogativas por las entidades a nivel global es similar dado que el 37,3% de los ayuntamientos y el 36,1% de las Diputaciones, Consells y Cabildos Insulares afirman cifrar los datos contenidos en los soportes que salen de las instalaciones de la entidad. En cambio un análisis por tamaño de municipio nos muestra que el cumplimiento es homogéneo entre los ayuntamientos de entre 500.000 y 10.000 habitantes con porcentajes de entidades entorno al 37%. Por encima están los ayuntamientos de más de 500.000 donde la totalidad de los mismos cifran los datos y por debajo los ayuntamientos de entre 5.000 y 10.000 habitantes donde lo realizan casi 3 de cada 10 entidades (Gráfico 30).

Gráfico 30: Distribución de EELL que llevan a cabo el cifrado de datos contenidos en soportes que salen de las instalaciones de la entidad, en función del tamaño de los municipios (%)



Fuente: INTECO

8.2.2 Copias de respaldo y recuperación

Es crítico garantizar la continuidad de las actividades de la EELL, para lo que se debe asegurar la disponibilidad de los datos que se tratan. Las copias de seguridad o de respaldo, procuran este objetivo, empleándose para la recuperación de los datos originales en caso de pérdida o alteración indebida.

El RDLOPD en su art. 94.1 obliga a establecer procedimientos de actuación para la realización, como mínimo semanal, de copias de respaldo, salvo que en dicho período no se hubiera producido ninguna actualización de los datos. A nivel global entre las entidades participantes el 55,2% de los ayuntamientos y el 94,4% de las Diputaciones,

Consells y Cabildos Insulares realizan una copia completa de todos los datos al menos una vez a la semana.

Preguntados los municipios por la implantación de la copia semanal, se obtuvo un alto grado de cumplimiento, como se puede observar en la Tabla 29. Los municipios de más de 10.000 habitantes están por encima del 94% de cobertura, mientras que los municipios más pequeños, de menos de 500 habitantes, alcanzan el 39,7%.

Es decir, casi la mitad de los Ayuntamientos realizan sus copias de seguridad con la suficiente frecuencia como para que los datos no se queden obsoletos.

Tabla 29: Entidades que llevan a cabo la realización de una copia de respaldo completa de todos los datos al menos una vez a la semana (salvo que en dicho periodo no se hayan producido ningún cambio en los datos), por tamaño (%)

Población (en miles)		Distribución porcentual			Distribución media ponderada		
		SI	NO	NS/NC	SI	NO	NS/NC
Grandes	Más de 500	100,0%	0,0%	0,0%			
	De 100 a 500	96,0%	4,0%	0,0%	97,0%	3,0%	0,0%
	De 50 a 100	97,4%	2,6%	0,0%			
Medianos	De 10 a 50	94,2%	4,4%	1,5%			
	De 5 a 10	84,8%	12,1%	3,0%	80,1%	15,3%	4,6%
	De 2 a 5	68,7%	23,9%	7,5%			
Pequeños	De 1 a 2	62,7%	32,2%	5,1%			
	De 0,5 a 1	47,4%	44,7%	7,9%	44,8%	47,6%	7,7%
	Ayts. Munic. menos 0,5	39,7%	52,1%	8,2%			
Diputaciones, Consells y Cabildos Insulares		94,4%	2,8%	2,8%			

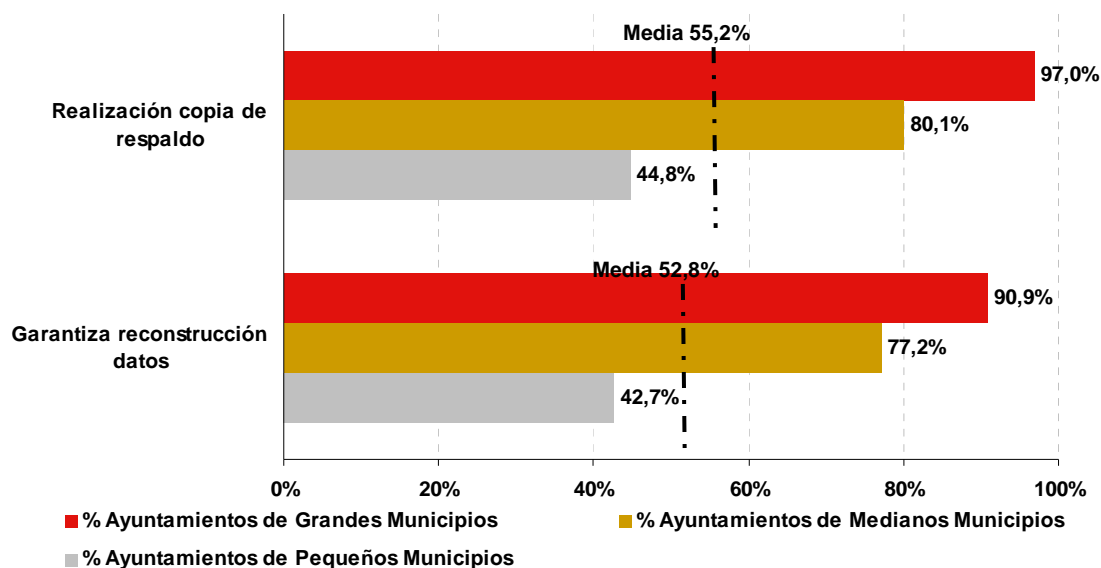
Fuente: INTECO

Asimismo la normativa establece en el art. 94.2, que han de realizarse los procedimientos para la recuperación de los datos que garanticen en todo momento su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción. Con la excepción, en el caso de que la pérdida o destrucción afectase a ficheros o tratamientos parcialmente automatizados, y siempre que la existencia de documentación permita alcanzar el objetivo al que se refiere el párrafo anterior, se deberá proceder a grabar manualmente los datos quedando constancia motivada de este hecho en el documento de seguridad.

El comportamiento a nivel global es que el 52,8% de los ayuntamientos y el 88,9% de las Diputaciones, Consells y Cabildos Insulares garantizan la reconstrucción de los datos.

Un análisis comparado de estas obligaciones por nivel de estrato muestra parecidos niveles de cumplimiento para los ayuntamientos de pequeños municipios, aunque inferiores al valor medio (Gráfico 31).

Gráfico 31: Realización por las EELL de copia de respaldo completa vs. garantiza la reconstrucción de los datos, por tamaño (%)



Fuente: INTECO

También y con el fin de asegurar que la copia y la recuperación se realizan de forma eficaz, el responsable del fichero se encargará de verificar cada seis meses la correcta definición, funcionamiento y aplicación de los procedimientos de realización de copias de respaldo y de recuperación de datos según lo dispuesto en el art. 94.3 del RDLOPD.

En general dicha medida se realiza por la mayoría de los municipios con independencia de su tamaño, salvo en el caso de los ayuntamientos de 5.000 a 10.000 habitantes donde el porcentaje de entidades se aproxima al de las Diputaciones, Consells y Cabildos Insulares (68%) (Tabla 30).

Tabla 30: Comprobación de la definición y aplicación de los procedimientos de copia y restauración de datos, por tamaño (%)

Población (en miles)		Distribución porcentual			Distribución media ponderada		
		SI	NO	NS/NC	SI	NO	NS/NC
Grandes	Más de 500	100,0%	0,0%	0,0%	86,6%	10,5%	2,8%
	De 100 a 500	88,0%	12,0%	0,0%			
	De 50 a 100	84,6%	10,3%	5,1%			
Medianos	De 10 a 50	79,4%	13,5%	7,1%	74,6%	8,8%	16,6%
	De 5 a 10	68,0%	20,0%	12,0%			
	De 2 a 5	75,0%	0,0%	25,0%			
Diputaciones, Consells y Cabildos Insulares		69,4%	19,4%	11,1%			

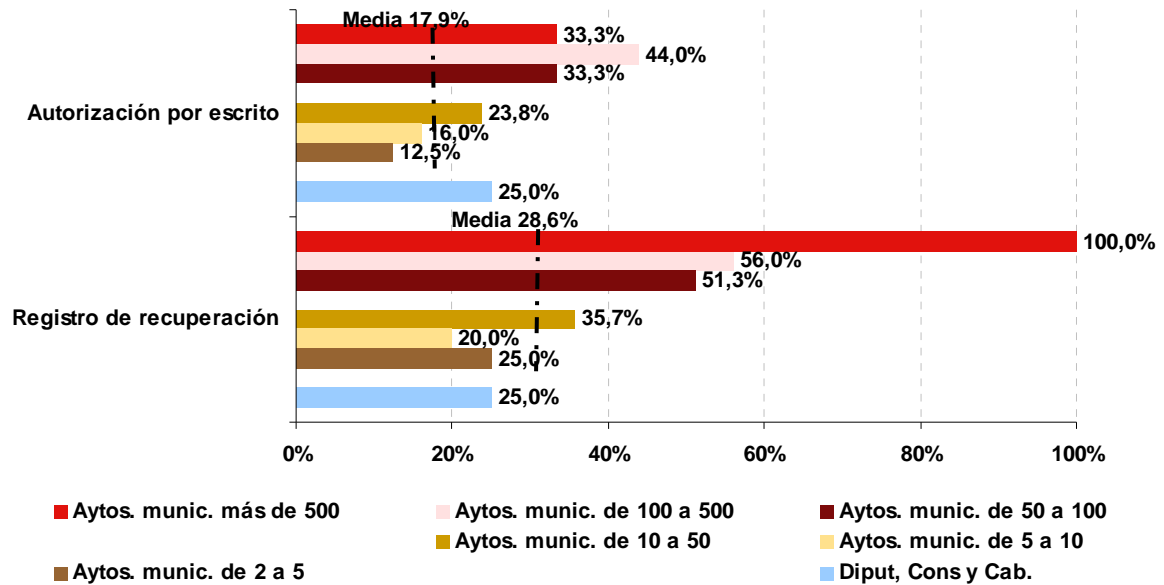
Fuente: INTECO

El responsable del fichero debe autorizar por escrito la recuperación de datos, además de mantener un registro con todas las restauraciones que se realicen con la siguiente información: fecha y hora, persona que realiza la restauración y los datos que se restauran de forma manual (por no estar incluidos en la copia de respaldo).

El Gráfico 32 muestra que los municipios no tienen mayoritariamente implantado el control de la autorización por escrito del responsable, al presentarse el mayor grado de cobertura en el 44% para los municipios de 100.000 a 500.000 habitantes. El resto de estratos está por debajo del 33,3%, incluida las Diputaciones, Consells y Cabildos Insulares que llegan al 25% de cobertura.

Sin embargo el registro de las recuperaciones tiene un grado de implantación mayor, con un 100% de los municipios de más de 500.000 habitantes por encima del 51% para los de más de 50.000 habitantes. El resto de estratos varían entorno al 25% de organismos que cumplen con lo establecido en la normativa, menos en el caso de los municipios de entre 10.000 y 50.000 habitantes (35,7%).

Gráfico 32: Autorización por escrito del responsable de los procesos vs. registro de las restauraciones de datos, en función del tamaño de los municipios (%)



Fuente: INTECO

Por último, para aquellos datos personales de nivel alto, el RDLOPD en su art. 102 exige la conservación de una copia de respaldo de los datos y de los procedimientos de recuperación de los mismos en un lugar diferente de aquel en que se encuentren los equipos informáticos que los tratan, utilizando elementos que garanticen la integridad y recuperación de la información, de forma que sea posible su recuperación.

Esta obligación es cumplida por el 64,5% de los ayuntamientos y el 66,7% de las Diputaciones, Consells y Cabildos Insulares. No obstante, a nivel del tamaño de los municipios el cumplimiento es superior a estos porcentajes en los de de más de 10.000 habitantes (Tabla 31).

Tabla 31: Entidades que guardan las copias de respaldo y una copia del procedimiento de recuperación de los datos en un lugar diferente de aquel en el que se encuentran los equipos informáticos que los tratan, por tamaño (%)

Población (en miles)	Distribución porcentual			Distribución media ponderada			
	SI	NO	NS/NC	SI	NO	NS/NC	
Grandes	Más de 500	100,0%	0,0%	0,0%			
	De 100 a 500	84,0%	8,0%	8,0%	85,9%	7,8%	6,3%
	De 50 a 100	86,1%	8,3%	5,6%			
Medianos	De 10 a 50	75,5%	21,8%	2,7%			
	De 5 a 10	54,2%	37,5%	12,5%	63,2%	24,0%	2,8%
	De 2 a 5	60,0%	40,0%	0,0%			
Diputaciones, Consells y Cabildos Insulares		66,7%	11,1%	22,2%			

Fuente: INTECO

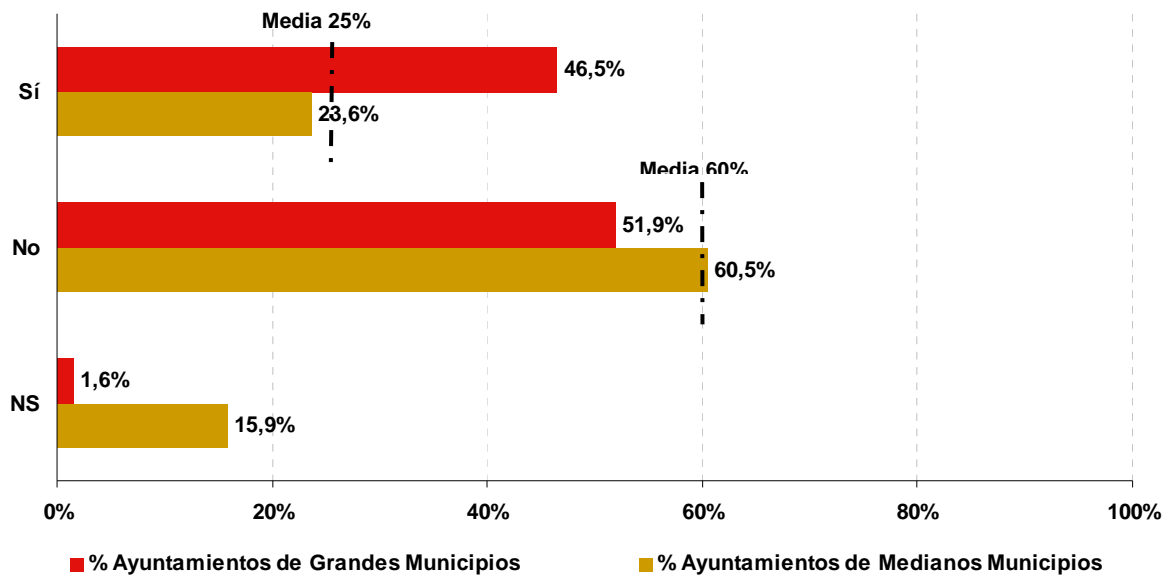
8.2.3 Pruebas con datos reales

El artículo 94.4 del RDLOPD recoge que las pruebas anteriores a la implantación o modificación de los sistemas de información que traten ficheros con datos de carácter personal no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente al tratamiento realizado y se anote su realización en el documento de seguridad. Si las entidades tienen previsto realizar pruebas con datos reales, previamente deberá haberse realizado una copia de seguridad. En cualquier caso, se recomienda el uso de datos ficticios para no tener que adoptar controles de seguridad adicionales.

La respuesta de las entidades participantes en el estudio muestra que a nivel global el 60% de los ayuntamientos y el 58,3% de las Diputaciones, Consells y Cabildos Insulares afirman que las pruebas no se realizan con datos reales frente a un 25% y a un 27,8% respectivamente que si los utilizan.

Este uso de los datos reales es más realizado por los ayuntamientos de mayor tamaño que por los medianos municipios, donde el 60,5% de los mismos no lo realizan. Frente a ellos 5 de cada 10 ayuntamientos de gran tamaño cumplen con lo establecido en la normativa. Destaca el 15,9% de las entidades de mediano tamaño que afirman desconocer con qué datos se realizan las pruebas de las nuevas aplicaciones (Gráfico 33).

Gráfico 33: Realización por las EELL de pruebas de las nuevas aplicaciones con datos reales, por tamaño (%)



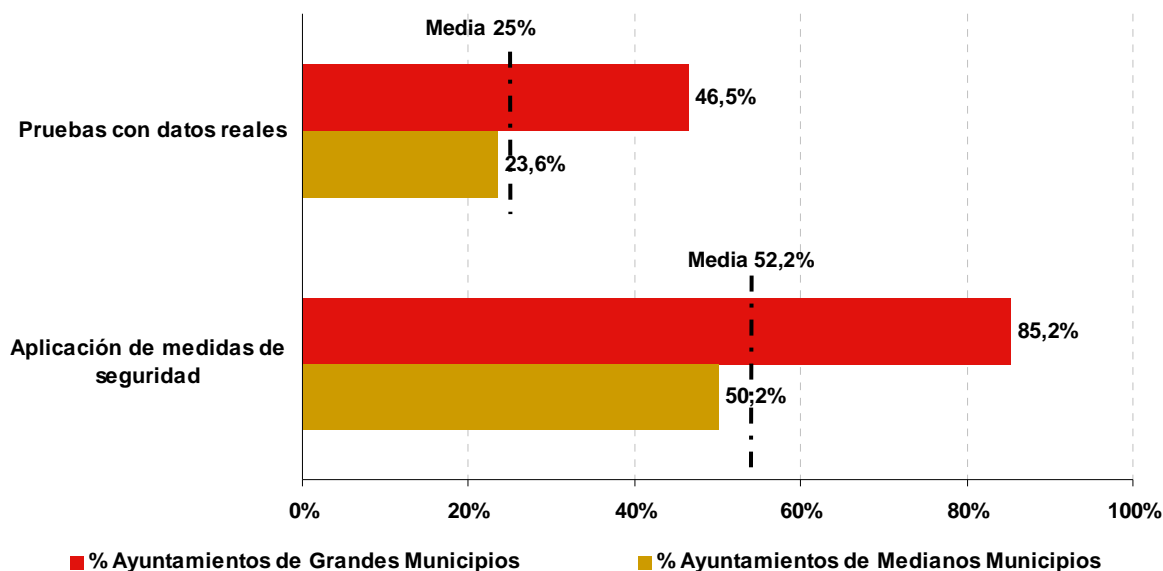
Fuente: INTECO

Tomando en consideración estos datos es necesario comprobar si en el caso de utilizar datos reales se aseguran que las medidas de seguridad aplicadas son las mismas que para los datos originales.

Así un 52,2% de los ayuntamientos y un 52,8% de las Diputaciones, Consells y Cabildos Insulares las toman en consideración.

A nivel de estrato el uso de datos reales ya se ha comentado en el gráfico anterior pero aún así como se comprueba en el Gráfico 34, los ayuntamientos de grandes municipios que son los que realizan en general pruebas con datos reales estables ponen en práctica dichas medidas; en concreto el 85,2% de los organismos de lo grandes municipios.

Gráfico 34: Realización por las EELL de pruebas de aplicaciones con datos reales vs. aplicación de medidas de seguridad, por tamaño (%)



Fuente: INTECO

8.2.4 Auditoría

Según el art. 96 del RDLOPD a partir del nivel medio de seguridad, los sistemas de información e instalaciones de tratamiento y almacenamiento de datos se someterán, al menos cada dos años, a una auditoría interna o externa que verifique el cumplimiento de las medidas de seguridad aplicables a ficheros y tratamientos automatizados.

Además con carácter extraordinario deberá realizarse dicha auditoría siempre que se realicen modificaciones sustanciales en el sistema de información que puedan repercutir en el cumplimiento de las medidas de seguridad implantadas con el objetivo de verificar la adaptación, adecuación y eficacia de las mismas.

El 10,9% de los ayuntamientos y el 19,4% de las Diputaciones, Consells y Cabildos Insulares a nivel global afirman que en sus entidades se realizan las auditorías con la periodicidad que establece la norma.

El análisis por tamaño de los municipios (Tabla 32) muestra que el cumplimiento más elevado, un 48%, se realiza por los ayuntamientos de entre 100.000 y 500.000 habitantes, mientras que el menor grado de obediencia se realiza por un 4,1% de los municipios de menos de 500 habitantes.

Tabla 32: Realización auditoría bianual, por tamaño (%)

Población (en miles)		Distribución porcentual			Distribución media ponderada		
		SI	NO	NS/NC	SI	NO	NS/NC
Grandes	Más de 500	33,3%	33,3%	33,3%	44,9%	39%	16,1%
	De 100 a 500	48,0%	44,0%	8,0%			
	De 50 a 100	43,6%	35,9%	20,5%			
Medianos	De 10 a 50	32,4%	35,3%	32,4%	24,2%	49,4%	25,9%
	De 5 a 10	12,1%	51,5%	36,4%			
	De 2 a 5	25,4%	58,2%	16,4%			
Pequeños	De 1 a 2	8,5%	76,3%	15,3%	5,0%	84,4%	10,6%
	De 0,5 a 1	5,3%	89,5%	5,3%			
	Ayts. Munic. menos 0,5	4,1%	84,9%	11,0%			
Diputaciones, Consells y Cabildos Insulares		19,4%	50,0%	30,6%			

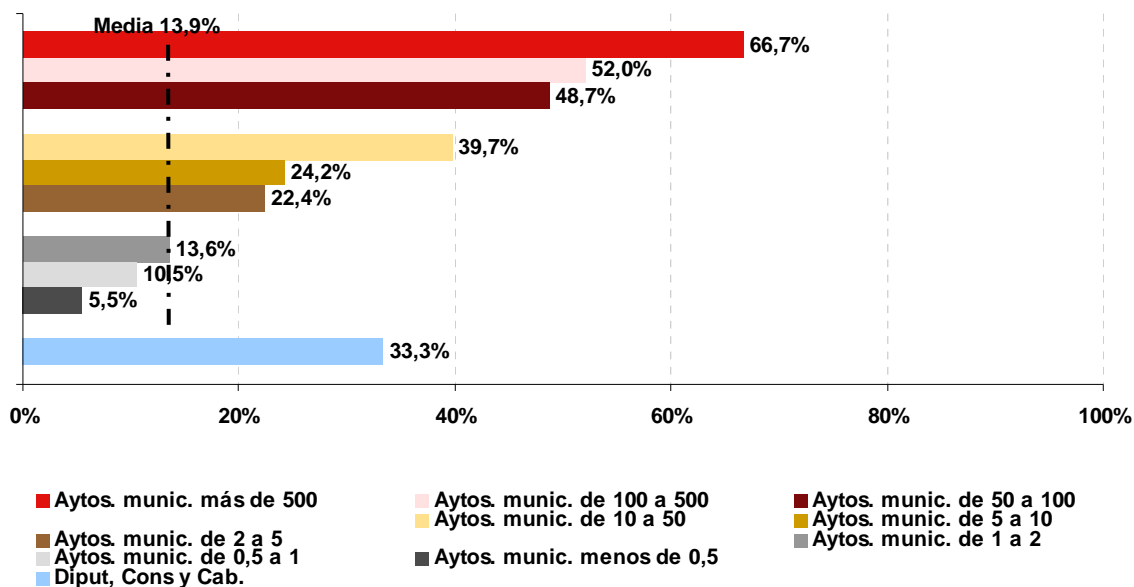
Fuente: INTECO

El informe de auditoría deberá dictaminar sobre la adecuación de las medidas y controles a la Ley y su desarrollo reglamentario, identificar sus deficiencias y proponer las medidas correctoras o complementarias necesarias. Deberá, igualmente, incluir los datos, hechos y observaciones en que se basen los dictámenes alcanzados y las recomendaciones propuestas.

El establecimiento es realizado a nivel global por el 13,9% de los ayuntamientos y el 33,3% de las Diputaciones, Consells y Cabildos Insulares. Por tamaño del estrato se ha cumplido por el 50,8% de los ayuntamientos de grandes municipios, el 27,9% de los de medianos municipios y 7,7% de los de menor tamaño.

En el Gráfico 35 se muestra la realidad a nivel del tamaño del municipio la respuesta de la exigencia de las entidades en su informe de auditoría. Los Ayuntamientos de más de 500.000 habitantes, con un 66,7%, son los que más requieren que se incluya desviaciones y recomendaciones, mientras que el resto no supera el 52%.

Gráfico 35: Establecimiento de deficiencias y propuestas correctoras en el informe de la auditoría, en función del tamaño de los municipios (%)



Fuente: INTECO

Los informes de auditoría serán analizados por el responsable de seguridad competente, que elevará las conclusiones al responsable del fichero o tratamiento para que adopte las medidas correctoras adecuadas y quedarán a disposición de la Agencia Española de Protección de Datos o, en su caso, de las autoridades de control de las comunidades autónomas.

A nivel global un 21,6% por los ayuntamientos y un 19,4% de las Diputaciones, Consells y Cabildos Insulares lo llevan a cabo; aunque a nivel de estrato es realizado por el 39% de los ayuntamientos de grandes municipios y por el 20,5% de los de mediano tamaño.

Tabla 33: Realización por el responsable de seguridad del análisis de los informes, compartiendo las conclusiones con el responsable del fichero, por tamaño (%)

Población (en miles)		Distribución porcentual			Distribución media ponderada		
		SI	NO	NS/NC	SI	NO	NS/NC
Grandes	Más de 500	33,3%	33,3%	33,3%	39,0%	43,3%	17,7%
	De 100 a 500	44,0%	44,0%	12,0%			
	De 50 a 100	35,9%	43,6%	20,5%			
Medianos	De 10 a 50	33,6%	31,2%	35,2%	20,5%	30,4%	49,0%
	De 5 a 10	20,0%	40,0%	40,0%			
	De 2 a 5	12,5%	25,0%	62,5%			
Diputaciones, Consells y Cabildos Insulares		19,4%	36,1%	44,4%			

Fuente: INTECO

9 SUPERVISIÓN, INSPECCIONES, DENUNCIAS Y SANCIONES DERIVADAS DEL INCUMPLIMIENTO DE LA NORMATIVA DE PROTECCIÓN DE DATOS

Las Agencias de protección de datos, tanto la estatal como las autonómicas, tienen atribuidas, por ley, competencias en materia sancionadora.

El procedimiento sancionador, de conformidad con lo previsto en el artículo 48.1 de la LOPD, está regulado en el Real Decreto 1332/1994, de 20 de junio, que detalla el cauce a seguir para la determinación de las infracciones y la imposición de sanciones.

En el caso de las Administraciones Públicas, según el art. 43.2 de la LOPD, se estará, en cuanto al procedimiento y a las sanciones, a lo dispuesto en el art. 46 que establece las infracciones de estas entidades.

Este apartado analiza, el volumen de EELL que se han visto afectadas por una inspección de la AEPD, el nivel de conocimiento respecto a las sanciones a las que pueden verse sometidas los organismos como consecuencia de un incumplimiento de la normativa de protección de datos y si han sufrido alguna sanción.

9.1 Inspecciones

El art 40.1 de la LOPD establece que las autoridades de control podrán inspeccionar los ficheros que contengan datos de carácter personal, recabando cuantas informaciones precisen para el cumplimiento de sus cometidos. A tal efecto, podrán solicitar la exhibición o el envío de documentos y datos, y, examinarlos en el lugar en que se encuentren depositados, así como inspeccionar los equipos físicos y lógicos utilizados para el tratamiento de los datos, accediendo a los locales donde se hallen instalados.

El 89,2% de los ayuntamientos y el 80,6% de las Diputaciones, Consells y Cabildos Insulares no han sufrido ninguna inspección por parte de la Agencia de Protección de Datos. Un análisis por tamaño del municipio y del estrato nos muestra en la Tabla 34 que todos los ayuntamientos de más 500.000 habitantes participantes en el estudio han sufrido alguna inspección; circunstancia esta que es explicable dado el elevado volumen de datos y ficheros que gestionan. Destaca que los ayuntamientos de 5.000 a 10.000 afirmen que no han recibido ninguna inspección. Esta es en cualquier caso, la situación de la mayoría de los estratos donde predomina la no inspección.

En el caso de las Diputaciones, Consells y Cabildos Insulares el 80,6% de las mismas no ha recibido ninguna inspección.

Tabla 34: Sufrimiento de alguna inspección por parte de la Agencia de Protección de Datos, por tamaño (%)

Población (en miles)		Distribución porcentual			Distribución media ponderada		
		SI	NO	NS/NC	SI	NO	NS/NC
Grandes	Más de 500	100,0%	0,0%	0,0%	42,1%	53,6%	4,3%
	De 100 a 500	48,0%	52,0%	0,0%			
	De 50 a 100	33,3%	59,0%	7,7%			
Medianos	De 10 a 50	9,5%	80,3%	10,2%	7,7%	83,7%	8,7%
	De 5 a 10	0,0%	90,9%	9,1%			
	De 2 a 5	10,4%	82,1%	7,5%			
Pequeños	De 1 a 2	5,1%	88,1%	8,8%	4,1%	92,1%	3,8%
	De 0,5 a 1	13,2%	86,8%	0,0%			
	Aytos. Munic. menos 0,5	1,4%	94,5%	4,1%			
Diputaciones, Consells y Cabildos Insulares		16,7%	80,6%	2,8%			

Fuente: INTECO

9.2 Denuncias y sanciones

Las entidades participantes en el presente estudio han sido preguntadas acerca de si tienen conocimiento de las sanciones que puede imponer la Agencia de Protección de Datos y si han sufrido alguna sanción.

El 32,1% de los ayuntamientos y el 69,4% de las Diputaciones, Consells y Cabildos Insulares afirman conocerla. Por tamaño del estrato este conocimiento es de un 80,8% para los ayuntamientos de los grandes municipios, un 50,3% para los medianos y un 24,1% para los de menor tamaño.

En la Tabla 35 se puede observar que hasta el estrato de 10.000 a 50.000 el conocimiento de las posibles sanciones ejercidas por la Agencia supera el 50% de organismos, mientras que aquellos de menos de 500 habitantes están por debajo del 20% de conocimiento.

El conocimiento de las posibles sanciones suele ser una motivación para acelerar la adaptación a la LOPD, por lo que un bajo grado de respuesta afirmativa puede indicar un bajo interés de adopción por algunas entidades.

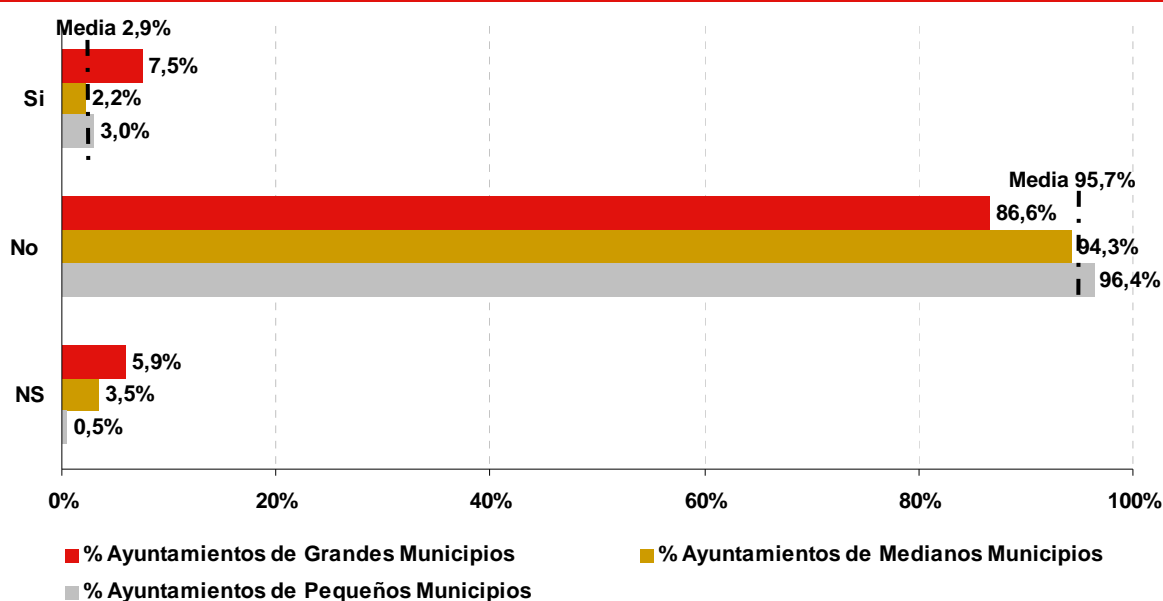
Tabla 35: Conocimiento de las sanciones que puede imponer la Agencia Española de Protección de Datos, por tamaño (%)

Población (en miles)		Distribución porcentual			Distribución media ponderada		
		SI	NO	NS/NC	SI	NO	NS/NC
Grandes	Más de 500	100,0%	0,0%	0,0%	80,8%	17,8%	1,4%
	De 100 a 500	84,0%	16,0%	0,0%			
	De 50 a 100	76,9%	20,5%	2,6%			
Medianos	De 10 a 50	62,8%	29,9%	7,3%	50,3%	39,8%	9,9%
	De 5 a 10	48,5%	39,4%	12,1%			
	De 2 a 5	43,3%	46,3%	10,4%			
Pequeños	De 1 a 2	35,6%	59,3%	5,1%	24,1%	66%	9,9%
	De 0,5 a 1	31,6%	57,9%	10,5%			
	Aytos. Munic. menos 0,5	19,2%	69,9%	11,0%			
Diputaciones, Consells y Cabildos Insulares		69,4%	22,2%	8,3%			

Fuente: INTECO

En relación con la otra pregunta, el sufrimiento de alguna sanción, el 2,9% de los ayuntamientos a nivel global afirma haberla sufrido frente a un 95,7% que no lo ha hecho. En el caso de las Diputaciones, Consells y Cabildos Insulares un 91,7% de ellas no ha sufrido sanción y el resto afirma desconocerlo. Por estrato como muestra el Gráfico 36, destaca que el 7,5% de los ayuntamientos de grandes municipios han sufrido alguna.

Gráfico 36: Sufrimiento de alguna sanción por parte de la Agencia de Protección de Datos, por tamaño (%)



Fuente: INTECO

El importe de las sanciones es variable, así pueden ir desde los 600 hasta los 60.000€ en el caso de las infracciones leves, pasando por las graves cuya cuantía varía entre los 60.101,21€ y los 180.101,21€ puede llegar a hasta las muy graves (300.506,05€-602.214,12€). Algunos ejemplos que identifica la normativa para cada una de las sanciones son:

- Infracciones leves: desatender la solicitud del interesado de cancelar sus datos personales, no solicitar la inscripción del fichero de datos de carácter personal en el Registro General de Protección de Datos, o no cumplir el deber de información al recabar los datos personales que establece el art. 5 de la LOPD.
- Infracciones graves: crear ficheros de titularidad pública o iniciar la recogida de datos de carácter personal sin autorización de disposición general publicada en el “Boletín Oficial del Estado” o diario oficial correspondiente.
- Infracciones muy graves: comunicar o ceder datos fuera de los supuestos permitidos, o recabar y tratar los datos sin el consentimiento del afectado tal y como viene establecido en el art. 45 RDLOPD.

Entre las entidades participantes todas menos los ayuntamientos de más de 500.000 habitantes, señalan cuál es tipo de sanción recibida (Tabla 36). A nivel global entorno al 38% de entidades afirman haber sufrido alguna de las sanciones que la normativa establece; en concreto el 38,6% sanciones leves, 38,1% de EELL con sanciones graves y muy graves. En el caso de las Diputaciones, Consells y Cabildos Insulares el porcentaje de entidades para todas las sanciones es el mismo (38,9%).

Tabla 36: Tipo de sanción impuesta a las EELL que afirman haber sufrido alguna, por tamaño (%)

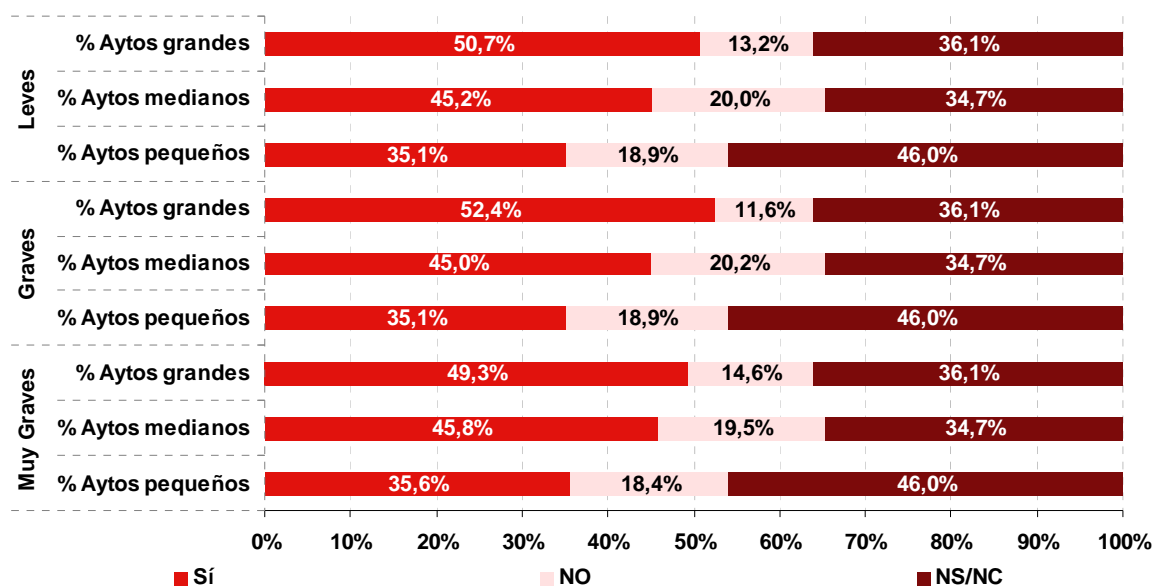
Población (en miles)		Distribución porcentual			Distribución media ponderada		
		Leve	Grave	Muy Grave	Leve	Grave	Muy Grave
Grandes	Más de 500	0,0%	0,0%	0,0%	49,3%	52,4%	50,7%
	De 100 a 500	52,0%	56,0%	52,0%			
	De 50 a 100	51,3%	53,8%	53,8%			
Medianas	De 10 a 50	40,1%	40,1%	40,9%	45,8%	45,0%	45,2%
	De 5 a 10	54,5%	51,5%	51,5%			
	De 2 a 5	44,8%	44,8%	44,8%			
Pequeños	De 1 a 2	49,2%	49,2%	49,2%	35,6%	35,1%	35,1%
	De 0,5 a 1	23,7%	21,1%	21,1%			
	Ayts. Munic. menos 0,5	35,6%	35,6%	35,6%			
Diputaciones, Consells y Cabildos Insulares		38,9%	38,9%	38,9%			

Fuente: INTECO

Por último y en relación con el conocimiento de las sanciones por parte de las entidades este es progresivo según el tamaño de la misma, tal y como se muestra en el Gráfico 37. De esta forma se puede comprobar que las sanciones más predominantes entre los ayuntamientos de municipios grandes son las graves (52,4%), seguidas de las leves (50,7%) y por último de las muy graves (49,3%). Entre los ayuntamientos de los medianos municipios, las sanciones más impuestas son las muy graves (45,8%), posteriormente las leves (45,2%) y por último las graves (45% de los municipios así lo afirman).

Entre los organismos de los municipios de menor tamaño apenas varían entre el 35% de los municipios que afirman tener algún tipo de las sanciones indicadas. No obstante entre éstos destaca que un 46% más o menos no señala sus respuesta a estas preguntas por lo que no se puede afirmar donde se ubican.

Gráfico 37: Tipos de sanciones impuestas a las EELL que han sufrido alguna por parte de la Agencia de Protección de Datos, por tamaño (%)



Fuente: INTECO

10 LA OPINIÓN DE LOS EXPERTOS RESPECTO AL GRADO DE ADAPTACIÓN E IMPLANTACIÓN DE LA NORMATIVA

Hasta el momento se ha descrito de manera exhaustiva el nivel actual de adopción de la normativa en materia de protección de datos de carácter personal - LOPD y RDLOPD - por parte de las Entidades Locales españolas.

En este capítulo del Estudio se recoge la opinión de expertos en la materia con el fin de establecer un marco de análisis que aporte nuevas perspectivas y señale nuevas tendencias de actuación respecto del grado de adaptación e implantación de la normativa en protección de datos por parte de las EELL.

La selección de los expertos se realizó a partir de unos ámbitos de representatividad y de unos perfiles profesionales que permitiera garantizar el enfoque integral y la cobertura de diferentes puntos de vista:

- Experiencia de gestión y/o técnica en el ámbito de las entidades públicas.
- Especialización en protección de datos.
- Responsabilidad en la planificación y gestión de los sistemas de información y comunicaciones.
- Representatividad en los distintos niveles de las Entidades Públicas Locales, ya sean Ayuntamientos, Diputaciones o Consells y Cabildos Insulares.

En este sentido, el grupo de expertos ha estado compuesto por responsables de las áreas descritas de 24 Entidades Públicas Locales que representan Ayuntamientos de distinto tamaño y geografía, así como Diputaciones y Cabildos Insulares. Se ha solicitado también la colaboración de la Agencia Española de Protección de Datos y de las tres Agencias Autonómicas que existen actualmente: Comunidad de Madrid, Cataluña y País Vasco, así como la colaboración de profesionales independientes.

Con la información recogida de esta opinión cualificada se elabora el presente epígrafe conteniendo el análisis detallado de:

- La definición de los **niveles de madurez** en la implantación de las medidas de seguridad, como herramienta de selección de prioridades en la fase inicial de adaptación a la Ley. Así, se han definido tres niveles de madurez para las medidas de seguridad descritas en el reglamento y con el propósito de ayudar así, a las Entidades que inicien su adaptación o regularicen, a seleccionar prioridades.

- El conjunto de **buenas prácticas** que sirvan a las Entidades para iniciar o mejorar su adaptación a la Ley. Identificando las buenas prácticas, tanto de carácter organizativo como técnico, para lograr una adecuada y eficaz implantación de las medidas de seguridad exigidas.
- Los **ejemplos de casos de éxito en la aplicación de buenas prácticas**. Se han seleccionado cuatro experiencias que destacan por algún aspecto relativo a la LOPD, bien sea por la implantación de forma exitosa de alguna medida de seguridad o por la labor de ayuda a otras entidades que puedan estar prestando en la actualidad.

10.1 Niveles de madurez

Una de las principales dificultades con las que se encuentran las EELL en su proceso de adopción a la normativa, es la selección de prioridades en la fase inicial de adaptación a la Ley. Por ello, la definición de niveles de madurez en la implantación facilitada por los expertos pretende solucionar este problema, de forma que cada nivel acometa unas determinadas medidas de seguridad de la reglamentación a las que ir dando cumplimiento por fases.

La implantación progresiva de estos niveles proporcionará como resultado una completa adaptación a los requisitos definidos en la normativa, así como la optimización de los controles implantados.

Los niveles de madurez, que son acumulativos, pueden clasificarse de la siguiente forma:

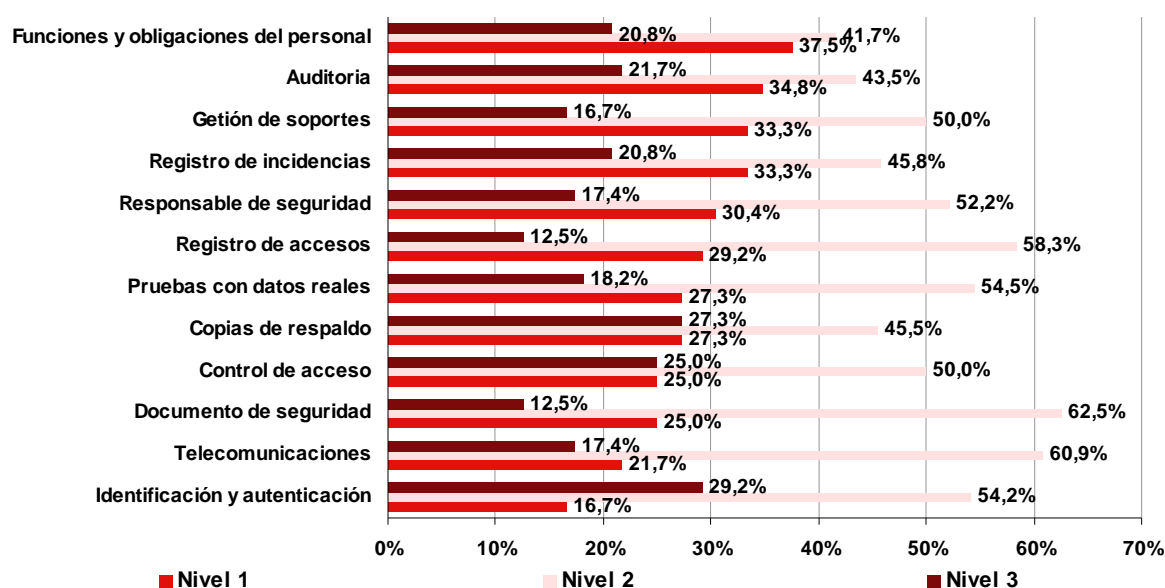
- Nivel 1 o nivel incompleto de cumplimiento: comprende las medidas de seguridad elementales, aunque no incluyen todas las necesarias de acuerdo con la legislación.
- Nivel 2 o nivel legal de cumplimiento: comprende todas las medidas de seguridad para conseguir la implantación de los requisitos recogidos en el RDLOPD.
- Nivel 3 o nivel avanzado de cumplimiento: comprende la gestión y mejora continua de todas las medidas definidas en el RDLOPD y las buenas prácticas de su gestión.

El Gráfico 38 muestra la opinión de los expertos para el conjunto de las medidas en relación con estos niveles. El conjunto de medidas identificadas son consideradas preferentemente en un nivel 2 como era lógico prever por la propia implicación que su cumplimiento tiene. Entre las disposiciones destaca el documento de seguridad (62,5% de menciones), las telecomunicaciones (60,9%) y el registro de acceso (58,3%). No obstante y a pesar de esta priorización efectuada no se debe perder de vista las medidas

urgentes a desarrollar para el nivel 1 como por ejemplo la comunicación de las funciones y obligaciones del personal (37,5%), la realización de auditorías (34,8%) o la gestión de soportes y el registro de incidencias (ambas con un 33,3%).

Como nivel 3 se señalan como prioritarias la identificación y autenticación (29,2%), las copias de respaldo (27,3%) y el control de acceso (25%).

Gráfico 38: Establecimiento de niveles de madurez para la implantación de las medidas de seguridad en las EELL (%)



Fuente: INTECO

Para poder profundizar en las valoraciones que se realizan, a continuación se recoge la clasificación realizada por los expertos consultados respecto de las medidas concretas que se recogen en el RDLOPD según los tres niveles de madurez definidos. Por ese motivo no sólo se identifican las actividades sino que además se identifican los artículos a los que hacen referencia y las medidas.

10.1.1 Nivel 1 de madurez

El Gráfico 39 muestra las once medidas de seguridad más importantes identificadas por los expertos como principales acciones a implantar en una fase preliminar o de inicio de adaptación a la LOPD. Las medidas básicas identificadas por los expertos como las más prioritarias son las asociadas a las siguientes actividades:

- 1) Registro de accesos: El responsable de seguridad debe llevar un control del registro de acceso, emitiendo un informe mensual de incidencias relacionadas (Art. 103.5 RDLOPD).

- 2) Delegación de autorizaciones: El responsable de fichero no puede delegar en otra persona su responsabilidad última de cara al cumplimiento de la Ley (Art. 84 RDLOPD).
- 3) Gestión y distribución de soportes: La distribución de los soportes que contengan datos de carácter personal se realizará cifrando dichos datos o bien utilizando otro mecanismo que garantice que dicha información no sea accesible o manipulada durante su transporte (Art. 101.2 RDLOPD).
- 4) Gestión de soportes y documentos: La salida de soportes y documentos que contengan datos de carácter personal, fuera de los locales bajo el control del responsable del fichero o tratamiento deberá ser autorizada por el responsable del fichero o encontrarse debidamente autorizada en el documento de seguridad (Art. 92.2 RDLOPD).
- 5) Control periódico: El responsable de seguridad se encargará de realizar un control periódico de la correcta aplicación del documento (Art. 88.4b RDLOPD).
- 6) Funciones y obligaciones del personal: El personal de la Entidad Local debe conocer las normas de seguridad que afecten al desarrollo de sus funciones, así como las consecuencias en que pudiera incurrir en caso de incumplimiento. Para ello, el responsable del fichero o tratamiento adoptará las medidas necesarias para que el personal conozca de una forma comprensible dichas normas de seguridad (Art. 89 RDLOPD).
- 7) Registro de incidencias: Será necesaria la autorización por escrito del responsable del fichero para la ejecución de los procedimientos de recuperación de los datos (Art. 100 RDLOPD).
- 8) Auditoría: Los informes de auditoría deben ser analizados por el responsable de seguridad y deben ser elevados al responsable del fichero para adoptar las medidas correctivas correspondientes (Art. 96.3 RDLOPD).
- 9) El documento de seguridad:
 - a. Se deben definir las medidas, normas, procedimientos, reglas y estándares de seguridad para garantizar el nivel de seguridad exigido (Art. 88.3b RDLOPD).
 - b. Se debe identificar al responsable de seguridad (Art. 88.4a RDLOPD).
- 10) Registro de acceso: El período mínimo de conservación de los datos registrados será de dos años (Art. 103.4 RDLOPD).

En el primer nivel de madurez, se sitúa de forma destacada -con un 70,8% de menciones-, la realización del informe mensual de incidencias correspondiente a la medida de seguridad de registro de accesos, como la medida prioritaria que los expertos consideran a la hora de iniciar un proceso de implantación de la normativa en materia de protección de datos, a pesar de tratarse de una medida de seguridad de nivel alto.

En segundo lugar -con un 52,4% de menciones -, se sitúan la delegación de funciones de coordinación y gestión por parte del responsable del fichero en uno o varios responsables de seguridad, sin que proceda en ningún caso la delegación de su responsabilidad última de cara al cumplimiento de la Ley.

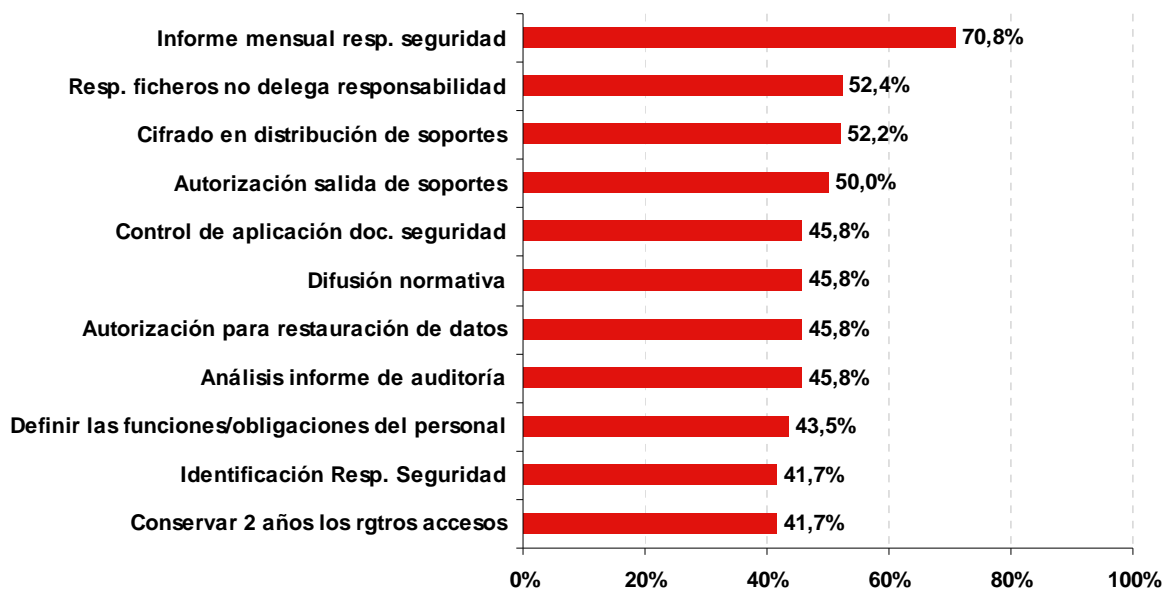
Asimismo con un 52,2% de las menciones figura en tercer lugar el cifrado en distribución de soportes. Esta actividad tiene relación con el cifrado de la información de soportes que contengan datos de carácter personal cuando se distribuyen fuera de los locales bajo el control del responsable del fichero o tratamiento.

Complementariamente a la medida anterior está, con un 50% de menciones, la actividad en la que el responsable del fichero, o la persona en quien haya delegado, deben autorizar toda salida de soporte de las instalaciones de la Entidad.

Las demás medidas seleccionadas –con porcentajes inferiores al 46% de menciones– hacen referencia a las funciones del responsable de seguridad, como coordinador de las medidas de seguridad implantadas, como difusor de la normativa a cumplir por los trabajadores de la Entidad, con la autorización para la recuperación de datos que se soliciten, como encargado del análisis de las recomendaciones que debe contener el informe de auditoría.

Por último también los expertos identifican medidas específicas relativas al documento de seguridad, como la definición de las funciones y obligaciones del personal, la identificación del responsable de seguridad y la conservación durante dos años de los registros de acceso.

Gráfico 39: Identificación por los expertos de las medidas de nivel 1 de madurez a implantar por las EELL



Fuente: INTECO

10.1.2 Nivel 2 de madurez

Este nivel incluye todas las medidas de seguridad para conseguir la implantación de todos los requisitos identificados en la normativa. En el Gráfico 40 se indican las nueve medidas del reglamento más referenciadas para este nivel. Por orden de prioridad, son las que se indican a continuación:

- 1) El documento de seguridad: Este debe tener establecido su ámbito de aplicación, incluyendo una especificación detallada de los recursos protegidos (Art. 88 RDLOPD).
- 2) Registro de accesos: De cada intento de acceso a los ficheros de datos se guardarán como mínimo, el identificador del usuario, hora, fichero, tipo de acceso y registro concreto accedido (Art. 103 RDLOPD).
- 3) Telecomunicaciones: La transmisión de datos de carácter personal a través de redes públicas o redes inalámbricas de comunicaciones electrónicas se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros (Art. 104 RDLOPD).
- 4) Auditoría: El informe de auditoría debe reflejar las deficiencias halladas en cuanto al cumplimiento del reglamento, así como proponer medidas correctivas (Art. 96 RDLOPD).

- 5) Control de acceso: El responsable del fichero debe establecer procedimientos de identificación y autenticación para tener control de acceso a los ficheros (Art. 91 RDLOPD).
- 6) Identificación y autenticación: La identificación de usuarios debe ser de forma inequívoca y personalizada para todos los trabajadores que tengan que acceder a los datos (Art. 93 RDLOPD).
- 7) Control de acceso físico: Exclusivamente el personal autorizado podrá tener acceso a los locales donde se encuentren ubicados los sistemas de información que albergan los datos de carácter personal (Art. 99 RDLOPD).
- 8) Copias de respaldo y recuperación: Las pruebas anteriores a la instalación o modificación de los sistemas de información no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente al nivel del fichero tratado (Art. 94 RDLOPD).
- 9) El documento de seguridad: Se debe identificar al responsable de seguridad (Art. 88.4a RDLOPD).

En el segundo nivel de madurez, se posiciona la definición del ámbito de aplicación del documento de seguridad, como principal medida con un 62,5% de menciones, correspondiente a la medida de seguridad del documento de seguridad. Es importante detallar en el documento una especificación general de los sistemas de información que soportan e intervienen en el tratamiento de los datos personales.

De igual manera, con un 58,3% de las menciones se sitúan el registro de accesos, haciendo referencia a los realizados por los usuarios. En dicho registro es obligatorio que se incluya el identificador del usuario, la hora, el fichero al que se accede, el tipo de acceso (consulta, borrado, modificación, alta) y el registro específico al que se accede. Y el cifrado de datos de carácter personal cuando estos son enviados a través de redes de comunicaciones como actividad correspondiente a la medida de seguridad referida a las telecomunicaciones.

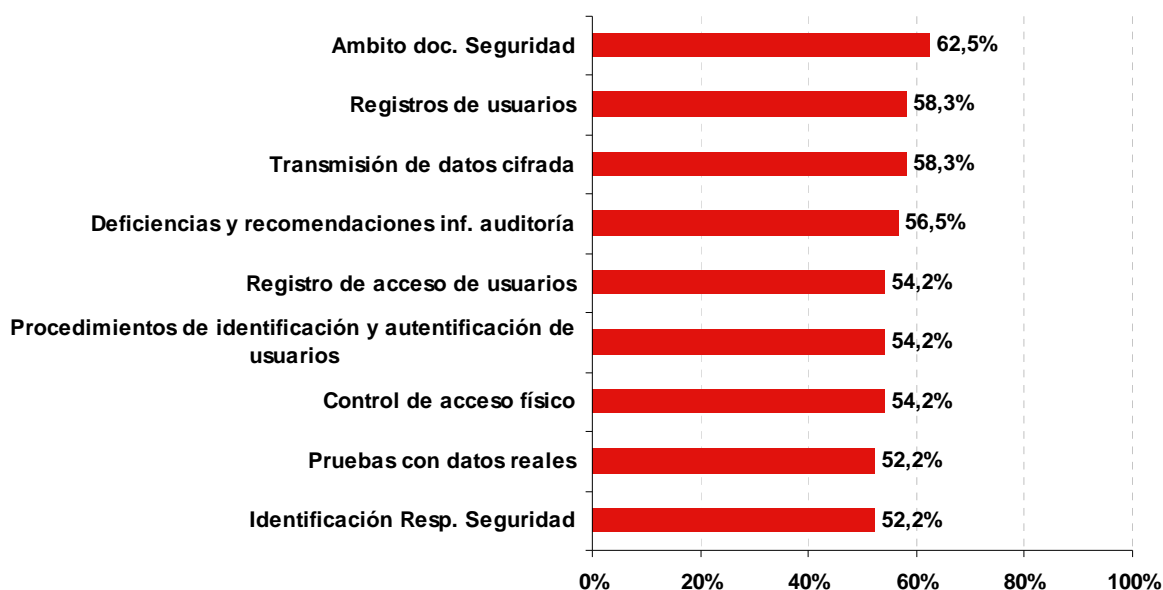
En cuarta posición -con un 56,5% de menciones – se encuentra la exigencia referida a que el informe de auditoría no contenga sólo las desviaciones halladas, sino también recomendaciones de mejora, correspondiente con la medida de seguridad de auditoría.

Las siguientes medidas, con un 54,2% de mención, hacen referencia a las siguientes actividades: a) el registro de accesos, b) el responsable de fichero debe establecer un procedimiento donde se detalle la forma en la que se va a realizar la identificación y autenticación de los usuarios y c) el control de acceso físico, señalándose que únicamente el personal autorizado, debe tener acceso a las salas donde se ubican los

sistemas de información, actividad referida a la medida de seguridad de control de acceso físico.

En el siguiente escalón se sitúan las pruebas con datos reales correspondientes a la medida de seguridad copias de respaldo y recuperación y la identificación del responsable de seguridad, ambas con un 52,2% de menciones. La primera medida hace referencia a cuando se tiene una aplicación desarrollada a medida, las pruebas de sistema que se realizan antes de su paso a producción con datos ficticios, evitando utilizar datos reales. Únicamente en caso de poder garantizar las condiciones de seguridad exigidas por el reglamento, en el entorno de pruebas, se podrán realizar las pruebas con datos reales.

Gráfico 40: Identificación por los expertos de las medidas de nivel 2 de madurez implantar por las EELL



Fuente: INTECO

10.1.3 Nivel 3 de madurez

Comprende las diez medidas de seguridad en las que las EELL deben aplicar mejoras continuas que les permitan la gestión con total eficacia y eficiencia. El Gráfico 41 muestra las medidas seleccionadas por los expertos para este nivel de madurez:

- 1) Copias de respaldo y recuperación:
 - a. Debe realizarse copias de los datos al menos una vez a la semana, salvo que en dicho periodo no se haya producido ningún cambio en los datos (Art. 94 RDLOPD).

- b. Debe conservarse una copia de respaldo y de los procedimientos de recuperación, en un lugar diferente de aquél, en el que se encuentran los sistemas de información que los tratan (Art. 102 RDLOPD).
 - c. Se establecerán procedimientos para la recuperación de los datos que garanticen en todo momento su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción (Art. 94. 2 RDLOPD).
- 2) Identificación y autenticación: Si se almacenan las contraseñas de los usuarios, debe hacerse de forma ininteligible (Art. 93 RDLOPD).
 - 3) Gestión de soportes: Debe mantenerse un inventario de soportes actualizado (Art. 92 RDLOPD).
 - 4) Copias de respaldo y recuperación: Establecer y documentar un procedimiento de copias de respaldo y restauración de los datos (Art. 94.1 RDLOPD).
 - 5) Identificación y autenticación:
 - a. Establecer y documentar un procedimiento de gestión de contraseñas, incluyendo la periodicidad con la que se cambian (Art. 93.4 RDLOPD).
 - b. Establecer un procedimiento de asignación y gestión de contraseñas, incluyendo la periodicidad con la que se cambian (Art. 93.3 RDLOPD).
 - 6) Control de acceso: Concesión de permisos de acceso para los usuarios realizada solamente por personal autorizado (Art. 91 RDLOPD).
 - 7) Control de acceso físico: Exclusivamente el personal autorizado podrá tener acceso a los locales donde se encuentren ubicados los sistemas de información que albergan los datos de carácter personal (Art. 99 RDLOPD).

Este tercer nivel de madurez comprende las medidas de fácil automatización o de mejora continua a partir del cumplimiento legal, necesarias si se pretende conseguir un cumplimiento eficiente a largo plazo.

La medida de seguridad con mayor porcentaje de mención, un 47,8%, son las referidas a las copias de respaldo y recuperación. Entre las actividades que alcanzan este porcentaje están: a) la obligación de almacenamiento en lugar diferente del tratamiento para poder garantizar la continuidad del servicio, en caso de producirse algún tipo de incidente grave en el lugar original, b) realización semanal de la copia de seguridad, de manera que, en caso de producirse una pérdida de datos, tan sólo se produzca una pérdida eventual de la semana de trabajo.

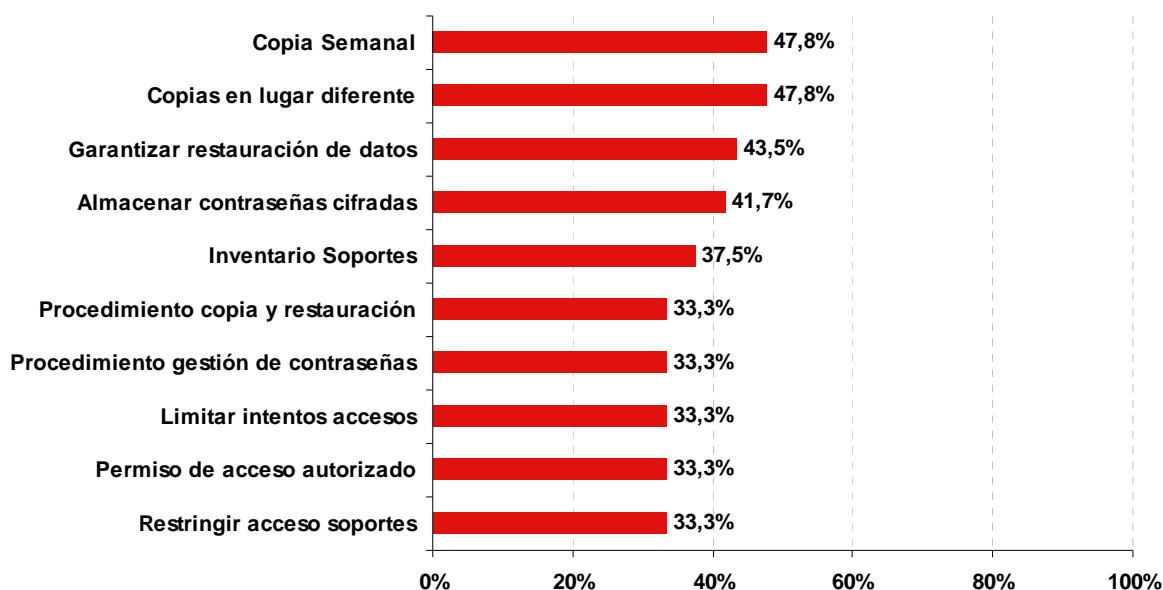
Dentro de la medida anterior, con un 43,5% de menciones, se identifica la necesidad de garantizar que la restauración de la información proporcione los datos en el mismo estado en que se encontraban, antes de producirse una incidencia. Es necesario realizar pruebas de restauración de los datos para asegurar este requisito.

En cuarta posición -con un 41,7% de menciones – se señala la exigencia referida al hecho de que el almacenamiento de las contraseñas de acceso de los usuarios, debe hacerse de forma que no sean inteligibles por alguien que, de forma irregular, tenga acceso a ellas, correspondiente con la medida de seguridad de identificación y autenticación.

De igual manera, con un 37,5% de las menciones se sitúa la automatización del inventario de soportes que nos permitirán su actualización y conseguir una gestión sencilla y ágil.

El resto de actuaciones seleccionadas –con porcentajes inferiores al 34% de menciones– hacen referencia: a) establecer y documentar un procedimiento de gestión de contraseñas, b) establecer un procedimiento de asignación y gestión de contraseñas, incluyendo la periodicidad con la que se cambian, c) concesión de permisos de acceso para los usuarios realizada solamente por personal autorizado y d) restringir el acceso al lugar de almacenamiento de los soportes físicos, ya que éstos por su tamaño, son fáciles de ocultar y pueden contener gran cantidad de información, se corresponden con la medida de seguridad de control de acceso.

Gráfico 41: Identificación por los expertos de las medidas de nivel 3 de madurez implantar por las EELL



Fuente: INTECO

10.2 Mejores Prácticas

El presente estudio, además de ofrecer un análisis de la situación de las Entidades Públicas Locales en la adaptación a la exigencia normativa en materia de protección de datos de carácter personal, propone como valor añadido un conjunto de buenas prácticas que pretenden servir a las propias Entidades para iniciar o mejorar su adaptación a la Ley.

Los expertos consideran de gran interés y relevancia, en la adaptación e implementación de la LOPD y el RDLOPD, trabajar en relación a las siguientes líneas identificadas por orden de prioridad:

10.2.1 Desde el punto de vista organizativo

- Impartir sesiones de formación y concienciación a los funcionarios, personal laboral y colaboradores, sobre las medidas de seguridad en las que están implicados.
- Promover la información a los ciudadanos y empresas sobre el tratamiento de sus propios datos cuando estos acceden en línea a un servicio público.
- Promover la toma de conciencia de los ciudadanos y empresas sobre su derecho fundamental a la protección de datos personales.
- Distribuir el documento de seguridad entre los funcionarios, personal laboral y colaboradores, con acuse de recibo de leído y comprendido, de forma individualizada.

10.2.2 Desde el punto de vista técnico

- Facilitar el ejercicio de los derechos de los interesados sobre sus datos, por diferentes canales de comunicación telemáticos (teléfono, fax, página Web, correo electrónico) y presencial, evitando la exclusión digital, y capacitando a los funcionarios, personal laboral y colaboradores para identificar y atender las solicitudes con eficiencia.
- Contratar a un servicio externo para la realización de la auditoría interna y, de este modo, garantizar su independencia y objetividad.
- Automatizar el proceso de gestión de incidencias, independientemente de su origen, para facilitar su resolución.
- Automatizar el proceso de implantación de las medidas del RDLOPD con una herramienta de gestión que facilite el seguimiento del proceso y pueda generar la documentación requerida.

- Combinar más de un método de identificación y autenticación para el control de acceso a los ficheros de datos personales.
- Contratar a un servicio externo para la custodia y destrucción segura de los soportes (automatizados o en papel) que contengan datos de carácter personal.

Los expertos han valorado estas prácticas de menor a mayor importancia en una escala numérica de valor de 1 a 10. No obstante las valoraciones tienen carácter orientativo y deben considerarse que las prácticas a las que hacen referencia pretenden la optimización en la implantación de medidas de seguridad de carácter organizativo, que pueden incidir de forma positiva en una mejora en la gestión del control técnico.

En este sentido, han otorgado la más alta valoración a la buena práctica de *carácter organizativo* sobre la impartición de sesiones de formación y concienciación a los trabajadores y a la buena práctica de *carácter técnico* de facilitación del ejercicio de derechos a los ciudadanos y de capacitación de los trabajadores de la EELL, ambas con una valoración global de 188 puntos de valoración.

En segundo y tercer lugar con una valoración de 176 y 175 puntos respectivamente están las buenas prácticas de *carácter organizativo* sobre promover la información sobre el tratamiento de sus datos y la toma de conciencia a los ciudadanos y empresas sobre su derecho fundamental a la protección de datos personales.

De igual manera, con una valoración de 162 puntos está la buena práctica de *carácter técnico* de contratar un servicio externo para la realización de la auditoría externa.

En las posiciones menos valoradas con valoraciones que varían entre los 157 y los 144 puntos se encuentran: a) la automatización de la gestión de incidencias, b) la automatización del proceso de implantación de las medidas con una herramienta de gestión, c) la distribución del documento de seguridad entre los funcionarios con acuse de recibo y d) combinar más de un método de identificación y autenticación para el control de acceso a ficheros. Por último está la práctica de contratación de servicios externos para la gestión de soportes con una valoración de 107 puntos.

Del análisis de las mejores prácticas resulta que la implantación de aquellas relacionadas con actividades organizativas, y por ende, de carácter formativo son las más valoradas por los expertos. Así, mediante la materialización de las mismas se consigue la base para realizar una implantación efectiva del resto de medidas y cumplir de esta forma, con los requisitos que establece la Ley.

10.3 Ejemplos de casos de éxito en la aplicación de las buenas prácticas

Analizado el conjunto de buenas prácticas que sirvan de herramienta de trabajo a las Entidades Locales para iniciar o mejorar su adaptación a la Ley, se describen a

continuación tres ejemplos de experiencias exitosas en la aplicación de dichas prácticas. Las cuales tienen relación con las actividades o medidas concretas reguladas por la normativa de protección de datos de carácter personal y llevadas a cabo por organismos, que por su grado de concienciación y enfoque práctico sirven como ejemplo de adaptación y cumplimiento.

La información que figura a continuación, se centra en la actividad específica por la que se ha querido destacar a la Entidad como caso de estudio. Además, se ha desarrollado a partir de la información facilitada por los responsables de protección de datos personales en el caso de los Ayuntamientos y con los directores de área en el caso de las Agencias.

10.3.1 Estructura, modelo de gestión y actuaciones específicas en materia de protección de datos: el Excmo. Ayuntamiento de Santa Cruz de Tenerife

En el año 2005 se inició el proceso de adaptación a la LOPD en el Excmo. Ayuntamiento de Santa Cruz de Tenerife¹⁶. Siendo dos las prioridades en la implementación de las medidas de adecuación de la estructura administrativa municipal:

- La redacción y aprobación del documento de seguridad.
- Completar un catálogo de ficheros municipales con datos de carácter personal para su posterior inscripción en el Registro Público de la Agencia Española de Protección de Datos.

Estructura

El Ayuntamiento crea en el año 2005 una Oficina de Protección de Datos y nombrándose un responsable a cargo de la Dirección General de Seguridad y de Protección de Datos dependiente a su vez de la Concejalía de Recursos Humanos, Calidad, Tecnología y Protección de Datos Personales. El puesto de Director de Seguridad y Protección de Datos en el Excmo. Ayuntamiento de Santa Cruz de Tenerife tenía como base de la convocatoria los siguientes requisitos: a) ser funcionario de carrera, b) licenciado en derecho y c) acreditar una experiencia de 5 años en la Administración Pública.

Esta Dirección General de Seguridad y de Protección de Datos se complementó con la colaboración del departamento de informática y telecomunicaciones del Ayuntamiento. Además, a medio plazo, se estimó una dotación de personal con perfil de auxiliar administrativo para reforzar las labores de gestión de todos los trámites que generasen los procedimientos implementados para dar cumplimiento a las medidas de seguridad exigidas por la LOPD.

¹⁶ Más información disponible en <http://www.sctfe.es/>

Dentro del Ayuntamiento, e incluido en el documento de seguridad, existe un Comité de Protección de Datos como órgano colegiado de asesoramiento en materia de protección de datos, formado por representantes permanente de:

- Concejalía de Protección de Datos.
- Dirección General de Protección de Datos.
- Sección Informática.
- Responsables internos de los ficheros de datos.

Pudiendo participar adicionalmente, según los asuntos tratados y siempre que sean convocados, el departamento de asesoría jurídica u otros órganos directivos.

Sin embargo, la Dirección General de Seguridad y de Protección de Datos actúa como máximo órgano administrativo en la coordinación de medidas de seguridad, así como de desarrollo de los principios de la LOPD, por lo que sus decisiones son de obligado cumplimiento para el resto de órganos municipales y en general, para todos los trabajadores del Ayuntamiento.

Modelo de gestión

En el Ayuntamiento se ha optado por un modelo centralizado de gestión, por lo que cualquier actividad conexas con la materia de protección de datos se canaliza a través de la Dirección General como órgano directivo. Así mismo, todas las decisiones a nivel resolutivo son adoptadas, de igual manera, por la Dirección General.

El ámbito de competencia de la Dirección General de Seguridad y de Protección de Datos comprende todos los órganos y departamentos del Ayuntamiento y los 4 organismos autónomos existentes: Deportes, Cultura, Urbanismo y Fiestas y Actividades Recreativas. Se excluyen, por su mayor autonomía de derecho privado, las sociedades municipales.

El seguimiento, mantenimiento y actualización de las medidas de seguridad implantadas en el Ayuntamiento es dirigido desde la Dirección General de Seguridad y de Protección de Datos, con plena autonomía, por lo que el nivel de supervisión es de carácter técnico; excluyéndose de este ámbito el carácter político.

Actuaciones específicas en materia de protección de datos de carácter personal

Uno de los pilares en los que se fundamenta la eficacia de las medidas de seguridad implantadas radica en la difusión y formación impartida por la Dirección General de Seguridad y de Protección de Datos. Así, como señala el Director de Seguridad y

Protección de Datos del Ayuntamiento: “La formación es fundamental porque son los propios funcionarios los verdaderos usuarios que proceden al tratamiento de los datos”.

El Plan Municipal de Formación incluye, todos los años, un Curso de Protección de Datos. Las acciones de difusión realizadas incluyen la edición de un díptico: “Protege tus Datos”, así como información disponible en la página Web externa del Ayuntamiento y en la Intranet corporativa.

De igual manera, se han venido realizando entre enero de 2007 y 2008 varias Jornadas de difusión al ciudadano con la intervención de diversos ponentes especializados en materia de protección de datos de carácter personal.

En relación al Nuevo Reglamento de Desarrollo de la LOPD, el 18 de abril se aprobó una nueva versión del documento de seguridad cuya redacción se adapta a las nuevas indicaciones del Reglamento. El Pleno Municipal aprobó, en sesión ordinaria de 16 de mayo de 2008, el Reglamento de Aprobación de Ficheros de Datos Personales con las modificaciones oportunas para adaptarse al nuevo Reglamento.

La Dirección General de Seguridad y de Protección de Datos ha publicado varias modificaciones de procedimientos y diversas instrucciones para irse posicionando en la misma línea del RDLOPD, como por ejemplo, la cláusula de confidencialidad para usuarios y contratistas, nuevos modelos normalizados de solicitud, etc. Además y fruto de la implicación de su modelo de gestión, presta su colaboración a otras Direcciones y departamentos del Ayuntamiento en la emisión de dictámenes jurídicos y asesoramiento en materia de protección y seguridad.

10.3.2 Auditoría: el área de Coordinación de Auditoría y Seguridad de la Información de la Agencia Catalana de Protección de Datos

La Agencia Catalana de Protección de Datos¹⁷ tiene, respecto de su ámbito de actuación, las competencias de registro, control, inspección, sanción y resolución, y también la adopción de propuestas e instrucciones.

Como caso de éxito, se desarrolla la labor de auditoría que se realiza por parte del área de Coordinación de Auditoría y Seguridad de la Información, la cual presta su apoyo de carácter tecnológico a la Dirección y a las áreas, proyectos e iniciativas de la Agencia, con especial dedicación a las actividades vinculadas a las funciones de inspección, dado que requieren de forma directa apoyo especializado en auditoría de sistemas de la información y seguridad de las TIC.

¹⁷ Más información disponible en www.apdcat.net

De forma específica, también se responsabiliza del diseño y ejecución de los programas de auditoría y control de oficio. Estos programas tienen por objetivo la verificación sectorial de tratamientos de datos de carácter personal, con la finalidad de valorar el nivel de adecuación a la normativa y, en su caso, recomendar y orientar sobre las medidas correctoras adecuadas.

Los Planes de Auditoría y Control de Oficio de la Agencia Catalana de Protección de Datos se desarrollan en el ejercicio de la función y competencias de supervisión de la aplicación de la legislación, en materia de protección de datos, que le atribuye a la propia Agencia la Ley 5/2002, de 19 de abril, de la Agencia Catalana de Protección de Datos por la que fue creada.

Su actuación es de carácter eminentemente preventivo. Tiene como objetivo revisar la situación de cumplimiento y recomendar las acciones necesarias para la adecuación a la LOPD según el tratamiento de datos personales que realice la entidad auditada.

Las labores de auditoría se iniciaron obedeciendo a la necesidad de dar un mayor apoyo a las Entidades bajo control de la Agencia y especialmente con la intención de adelantarse a los posibles incidentes derivados del incumplimiento de las normas.

El Plan de Auditoría

La auditoría se realiza de oficio, lo que no es óbice para que cualquier Entidad, respecto de la que sea competente la Agencia, pueda solicitar de forma voluntaria ser incluida en el Plan de Auditoría. Normalmente estas solicitudes son atendidas, salvo que desvíen de forma considerable los objetivos y planificación de las auditorías.

El Plan de Auditoría no comprende a todas las entidades de Cataluña, principalmente por el número de localizaciones que lo imposibilita. Para los Ayuntamientos y Consejos Comarcales se procede a realizar un muestreo que resulte significativo en función del objetivo específico de cada plan de auditoría, completado con un proceso de selección aleatoria.

El mecanismo de selección de la muestra se define para cada Plan de Auditoría. La selección se realiza por una entidad externa a la Agencia. De este modo, sirva de ejemplo, que para el Plan de Auditoría para la verificación del cumplimiento del artículo 5 de la LOPD, la selección fue realizada con la colaboración de un equipo de administración pública del departamento de Ciencias Políticas y Sociales de la Universidad Pompeu Fabra. Los criterios que debía cumplir la muestra eran los siguientes: a) cubrir un 80% de la población, b) equilibrio territorial y de dimensión de los municipios y c) con un número de municipios en torno a 130.

En cuanto al contenido de la auditoría, éste se determina en función de diferentes criterios que pueden ser tanto de tipo coyuntural como de oportunidad. No realizándose nunca sobre el cumplimiento total de la normativa, sino sobre un aspecto concreto de adecuación. De esta forma se consigue que tanto el propio proceso de auditoría, como la posterior adaptación de las recomendaciones puedan ser llevados a cabo en tiempos reales y sin que lleguen a suponer un impacto que no pudiera ser asumido por las entidades auditadas.

El modelo adoptado se basa en la evaluación continua ya que cada 6 meses aproximadamente, está previsto lanzar un nuevo plan de auditoría siguiendo las directrices anteriormente descritas.

La forma de proceder es común para todas las entidades a las que auditan; es decir, la Agencia asigna un auditor, que de forma personalizada interacciona con cada entidad. Regulando las fases y plazos y adaptando los contenidos a la situación concreta de cada entidad y a sus posibilidades reales. De esta forma facilita a los ayuntamientos de pequeños municipios su organización dada la escasez de recursos humanos que presumiblemente tienen.

A cada entidad, de forma individualizada se le entrega un informe de auditoría, en el que se indica la descripción detallada de la situación de cumplimiento, las recomendaciones necesarias para la adecuación y el plazo de adaptación para implementarlas.

Una vez terminado el Plan de Auditoría se hace un informe global final, de carácter público, donde se indican recomendaciones de ámbito general. Este informe está destinado, principalmente, a las entidades no auditadas, de modo que estas tengan una referencia a la hora de verificar su cumplimiento y puedan actuar en consecuencia.

La respuesta de las Entidades Locales es muy positiva, prestando total colaboración con el auditor. La adaptación de las recomendaciones también es muy positiva, si bien siempre existen algunas excepciones, por falta de recursos, que, en algunos casos, determina que la Entidad contrate una asesoría externa para la ejecución de los trabajos de adaptación.

Todos los recursos que participan en la ejecución de las auditorías son propios de la Agencia, no previendo realizar en ningún momento la subcontratación de los trabajos principalmente por los posibles conflictos de intereses que se puedan generar, al disponer de información privilegiada de las entidades. Asimismo, la Agencia tampoco recomienda ninguna consultora, dejándose en manos del mercado y sus reglas.

En relación al Nuevo Reglamento de Desarrollo de la LOPD ya en vigor desde abril de 2008, tenía previsto incorporarse a los nuevos planes de auditoría que se fuesen a realizar en 2008.

El resultado final de estas pequeñas acciones de auditoría se refleja en el impacto que causan en la entidad, haciendo que haya una concienciación general y se dispongan a alcanzar el cumplimiento global de todas las medidas de seguridad que exige la normativa.

Nuevas iniciativas

En estos momentos la Agencia tiene el compromiso de focalizarse en la prevención de forma efectiva y eficaz. Para ello, está diseñando dos futuras acciones:

- *Implantación de Evaluaciones de Impacto de Privacidad (Privacy Impact Assessment)*: Es una metodología consistente en la valoración de los tipos de impacto que los nuevos proyectos de una Entidad vayan a ocasionar sobre la privacidad de los ciudadanos, para poder así minimizarlos en la medida de lo posible. Estos nuevos proyectos pueden ser de cualquier ámbito, desde iniciar la gestión de nuevos servicios, a su externalización o hasta la adquisición de nuevas tecnologías para los sistemas de información.
- Búsqueda de mejores modelos organizativos en las Entidades que sean capaces de dar respuesta a la problemática de la gestión de los datos de carácter personal. Para lo cual se pretende que sean las circunstancias y posibilidades de cada entidad las que determinen el modelo a utilizar. Con esta acción se pretende promover la figura del encargado o responsable de protección de datos en cada organización, lo que se conoce en el mundo anglosajón como los “Data Protection Officer”.

10.3.3 Consultoría: la Subdirección General de Registro de Ficheros y Consultoría de la Agencia de Protección de Datos de la Comunidad de Madrid

La Agencia de Protección de Datos de la Comunidad de Madrid¹⁸ (APDCM), tiene como finalidad garantizar y proteger los derechos fundamentales de las personas físicas respecto al honor e intimidad familiar y personal, en lo relativo al tratamiento de sus datos personales.

Sus competencias versan sobre los ficheros de titularidad pública creados o gestionados por la Comunidad Autónoma de Madrid, los Entes que integran la Administración Local de su ámbito territorial, las Universidades Públicas y las Corporaciones de Derecho Público representativas de intereses económicos y profesionales de la comunidad.

Como caso de éxito, se desarrolla la labor de consultoría que se realiza por parte de la Subdirección General de Registro de Ficheros y Consultoría encargada del registro de los

¹⁸ Más información disponible en www.madrid.org/apdcm

ficheros de datos de carácter personal de titularidad pública de la Comunidad de Madrid y realizando también labores de consultoría y asesoramiento para responsables de los ficheros.

Las funciones del departamento de consultoría son las siguientes:

- Elaborar y poner a disposición de los responsables de ficheros, y de sus usuarios, los recursos técnicos para apoyar la inscripción en el Registro de Ficheros de Datos Personales, así como en general la gestión de dichos ficheros conforme a lo establecido por la Ley 8/2001 de Protección de Datos de Carácter Personal en la Comunidad de Madrid¹⁹ y sus disposiciones complementarias. Los recursos que establecen podrán incluir, entre otros, metodologías, aplicaciones informáticas de apoyo, esquemas de homologación de productos o servicios, materiales para la formación, modelos de documentación y guías de preguntas frecuentes.
- Colaborar con los responsables de ficheros, sin perjuicio de las competencias que éstos tienen atribuidas, al objeto de que los ficheros se ajusten a las previsiones contenidas en la Ley 8/2001, mediante la prestación de servicios que podrán incluir, entre otros, difusión y formación, ayuda para la utilización de los recursos técnicos, identificación de tratamientos de datos de carácter personal, apoyo a la inscripción de ficheros en el Registro de Ficheros de Datos Personales, asesoramiento sobre la implantación y adecuación de las medidas de seguridad que establece la LOPD y el RDLOPD.
- Atender las consultas planteadas por los responsables de ficheros en materia de protección de datos.
- Analizar los proyectos de disposiciones generales que incidan en la materia de la Ley 8/2001, sin perjuicio de lo dispuesto en el Estatuto de la Agencia²⁰.
- En general, actuar como interlocutor de la Agencia de Protección de Datos de la Comunidad de Madrid ante los responsables de ficheros en todas las materias, con excepción de lo dispuesto en el Estatuto de la Agencia, y sin perjuicio de las funciones definidas para el resto de órganos y unidades de la misma.

¹⁹ LEY 8/2001, de 13 de julio, de Protección de Datos de Carácter Personal en la Comunidad de Madrid. Disponible en <https://www.agpd.es/portalweb/canaldocumentacion/legislacion/autonomica/common/pdfs/A.19-cp--Ley-8-2001.pdf>

²⁰ Decreto 22/1998, de 12 de febrero, por el que se aprueba el Estatuto de la Agencia de Protección de Datos de la Comunidad de Madrid. Disponible en http://www.uicm.org/Documentos/ProteccionDatos/Legislacion/Estatuto_APD_CAM_1998.pdf

- Asesorar al Director de la Agencia y al resto de órganos y unidades de la misma en materias de especialización técnica y de gestión relevantes para la protección de datos personales, como pueden ser la e-Administración, Internet, tecnologías y procedimientos de identificación electrónica individual, tales como certificados y firma electrónica, o cualesquiera otras análogas.

Función de consultoría

La motivación de esta labor de consultoría parte de los propios estatutos de la APDCM, pero se basa en el convencimiento de que esta labor es básica para conseguir sus objetivos. Por este motivo y en relación a las Entidades Públicas Locales, la APDCM, se ha puesto en contacto con los 179 Municipios, Mancomunidades y Organismos Autónomos de la Comunidad de Madrid ofreciéndoles su ayuda.

El objetivo inicial principal de las labores de consultoría fue conseguir que el 100% de los municipios tuviesen sus ficheros inscritos. No sólo es importante el número de ficheros inscritos sino la calidad de la inscripción, es decir, que se hayan inscritos todos de forma correcta.

Este requisito hay que situarlo en el contexto del tamaño de cada municipio, por lo que las actuaciones de consultoría se planificaron y se han llevado a cabo de forma escalonada, cubriendo en primer lugar aquellos municipios con mayor número de habitantes para ir extendiendo las actuaciones al resto de los municipios. De forma paralela a la inscripción de ficheros se ha realizado el trabajo de revisión de los ya inscritos para conseguir una completa actualización.

En los Municipios de mayor tamaño la consultoría se centra en indicar directrices de gestión ya que, normalmente tienen los recursos adecuados para tener un conocimiento suficiente sobre la LOPD y su desarrollo reglamentario, así como para su implantación. Sin embargo en las Entidades de pequeño tamaño este conocimiento es difícil que exista, por lo que la ayuda y el apoyo que reciben del consultor responsable de la Agencia son mucho más intensos y abarcan un abanico más amplio de actuaciones.

En relación con las medidas de seguridad, un buen punto de partida es la petición del informe de la última auditoría de seguridad realizada por aplicación de la normativa de protección de datos. En el caso de que dicho informe no exista, se abordan las necesidades de seguridad mediante el diálogo con la Entidad Local y se concientia sobre la necesidad de su adopción.

La labor de consultoría proporciona ayuda en todos los campos de la LOPD y el RDLOPD, tanto en medidas de carácter organizativo, como jurídico, e incluso de procedimiento para las medidas de seguridad de carácter más técnico.

No se revisa todo el reglamento en cada Entidad, sino que se hace hincapié en la parte de cada una que se determina como más débil o necesitada. La revisión completa se puede llevar a cabo a través de la Inspección, que siempre puede actuar de oficio y solicitar a cualquier entidad la realización de una completa revisión de su situación.

Una preocupación importante por parte de los consultores de la APDCM es el documento de seguridad. No sólo por ser el referente normativo para todos los trabajadores de la entidad, sino también por ser el documento que describe la situación actual de la entidad con respecto a la LOPD. De esta forma se garantiza una continuidad de políticas y procedimientos ante, por ejemplo, un cambio de gobierno en un Ayuntamiento. El equipo gestor entrante puede continuar la labor a partir de un documento de seguridad preciso y actualizado.

En relación a las medidas de seguridad de carácter más técnico, los consultores, para garantizar el grado de total independencia de la APDCM, no pueden realizar ninguna recomendación de algún tipo de tecnología, herramienta o aplicación comercial concreta. Por la misma razón, tampoco se recomienda ninguna empresa externa que pueda realizar la consultoría de adaptación a la LOPD.

La APDCM tiene a disposición de las Entidades Públicas Locales 2 herramientas para facilitar la adaptación a la LOPD:

- DEPD: Aplicación para el ejercicio telemático de los derechos protección de datos. Está implantada en la administración regional de la Comunidad de Madrid.
- CUMPLE: Sistema de Ayuda al Responsable de Ficheros de Titularidad Pública para el Cumplimiento de sus Obligaciones en Materia de Protección de Datos.

La realización de las labores de consultoría se realiza con recursos propios de la Agencia, no está externalizado ni se va a externalizar por dos motivos fundamentales: por convencimiento, ya que se piensa que esta labor debe realizarla directamente personal de la Agencia para garantizar una imagen de competencia e independencia, y en segundo lugar, por carecer de una partida presupuestaria que pudiera cubrir esta eventualidad.

Otras funciones de la APDCM

En junio de 2008 la Agencia ha publicado el libro “Protección de datos personales para Administraciones Locales” que continúa la línea iniciada con la “Guía de Protección de Datos para Ayuntamientos”. En el se hace una revisión y actualización completa de la guía teniendo en cuenta la experiencia de la APDCM en los últimos cuatro años así como la publicación del RDLOPD. Para lo cual incluye ejemplos de buenas prácticas, herramientas de ayuda al responsable y la adaptación a las medidas de seguridad

descritas en el nuevo Reglamento que entró en vigor el pasado 19 de abril con especial hincapié en las que afectan a los ficheros manuales.

Además la Agencia realiza labores de formación continua, fruto de la cual se han beneficiado más de 40.000 personas llevando a cabo 5 ediciones del curso de LOPD con una duración y dirigida a secretarios de servicio de los Ayuntamientos y a directores de centros de enseñanza.

Asimismo se realizan charlas de concienciación con alto grado de asistencia de responsables de Entidades Locales que tienen como objetivo la motivación de la puesta en marcha o refuerzo del proceso de cumplimiento.

Como actividades paralelas que realiza la Agencia se pueden destacar las siguientes:

- Página Web corporativa: página sectorializada con una sección para las Entidades Públicas Locales.
- Memoria anual y publicación de indicadores semestrales: incluye información sobre la inscripción de ficheros, inspecciones realizadas, informes solicitados y sesiones formativas realizadas.
- Premio a las mejores prácticas de protección de datos de Administraciones Europeas: con el objetivo de servir de referencia como caso de éxito a otras entidades. Cada edición se organiza una jornada en la que todas las candidaturas presentadas ponen en valor las buenas prácticas que han implementado.
- Otras publicaciones de la Agencia:
 - www.datospersonales.org: revista dirigida al responsable de ficheros orientada a recomendaciones de gestión. Edición bimensual.
 - www.dataprotectionreview.eu: con un enfoque internacional más global. Artículos de opinión y legislación. Edición cuatrimestral.
 - Revista Española de Protección de Datos: orientada al mundo profesional y universitario. Edición semestral.

10.3.4 Estructura, modelo de gestión y actuaciones específicas en materia de protección de datos: el Instituto Municipal de Informática del Excmo. Ayuntamiento de Barcelona

El Instituto Municipal de Informática (en adelante, IMI) del Excmo. Ayuntamiento de Barcelona²¹ es un organismo autónomo local, cuyo objetivo es gestionar eficazmente todos aquellos aspectos relacionados con la informática interna del Ayuntamiento de Barcelona y otros entes públicos de servicio al ciudadano como la policía local o el servicio de bomberos. Da servicio a más de 6.500 usuarios entre funcionarios y empleados de servicios públicos en más de 300 edificios.

Como caso de éxito se va a desarrollar la organización de la gestión de la protección de datos dentro de una Entidad tan amplia como es el Ayuntamiento de Barcelona.

Estructura

La coordinación general corre a cargo de la Subdirección de Información de Base del IMI y el soporte jurídico lo realiza la Dirección de Servicios Jurídicos. En los Sectores, Distritos, Institutos y Patronatos, así como en las Sociedades Privadas Municipales la responsabilidad en la aplicación de la LOPD es desempeñada por los responsables de ficheros, cargos con un perfil de gerente o director de servicios, y los responsables operativos de ficheros, con un perfil de secretarios delegados.

Las políticas en la aplicación de la LOPD son comunes para toda la organización municipal. En el caso de los organismos autónomos como Institutos, Patronatos y Sociedades Privadas Municipales, los procedimientos y controles son adaptados a sus características específicas por sus equipos de gestión.

El equipo gestor de la LOPD en el Ayuntamiento tiene dos perfiles diferenciados: a) Licenciados en Derecho para la organización y la formalización de procedimientos y b) Informáticos para la gestión de información.

La Subdirección de Información de Base coordina ambos grupos funcionales. Esta Subdirección pertenece al IMI. A su cargo, o como soporte funcional, tiene especialistas en seguridad informática, metodologías de desarrollo y en gestión de la información. También tiene a su cargo a especialistas en procedimientos administrativos y conocimiento de la legislación básica, específica de protección de datos. El soporte legal adicional se cubre con el trabajo de los abogados de los Servicios Jurídicos Centrales.

Modelo de gestión

²¹ Más información disponible en <http://www.bcn.es/>

A la hora de adecuarse a la LOPD la prioridad principal consistió en la creación de la Comisión Técnica de Seguridad en Protección de Datos de Carácter Personal del Ayuntamiento de Barcelona²², llamada CSPD, con las siguientes funciones:

- Establecer las directrices generales en materia de protección de datos personales en el conjunto de la organización municipal.
- Establecer criterios de aplicación de la normativa reguladora de protección de datos personales.
- Autorizar la publicación en la intranet municipal de buenas prácticas, procedimientos internos u otros documentos de interés en materia de protección de datos personales.
- Autorizar los planes de formación municipal en materia de protección de datos personales.

La gestión diaria de todo lo relacionado con la LOPD se realiza en el IMI, no obstante la gestión de incidencias es revisada semanalmente por la Subdirección de Información de Base y por el responsable de seguridad tecnológica del IMI. Además, de forma trimestral se reúne la CSPD (Comisión Técnica de Seguridad en Protección de Datos de Carácter Personal del Ayuntamiento de Barcelona) que está presidida por un Teniente de Alcalde.

Se realizan tres tipos de control y revisión generales:

- Auditorias bienales exigidas por la normativa.
- Auditorías interanuales internas a cargo de la Subdirección de Información de Base.
- Control interno permanente para supervisar y controlar el cumplimiento de la LOPD.

El IMI dispone de herramientas parciales de gestión desarrolladas de forma interna. El próximo paso será la interconexión con los aplicativos y los flujos de trabajo²³ correspondientes.

A medio plazo el IMI tiene previsto valorar la implantación de:

²² Comisión creada mediante Decret d'Alcaldia 21/7/2006.

²³ También conocidos como workflows, se encarga de plasmar cómo se estructuran las tareas realizadas en un Organismo Público o empresa privada, cuál es su orden correlativo, cómo se sincronizan, cómo fluye la información que soporta las tareas y cómo se le hace seguimiento al cumplimiento de las tareas.

- Herramienta de gestión y soporte para la documentación de seguridad.
- Mejora de las herramientas de gestión de los derechos ARCO.
- Herramienta de soporte y seguimiento de las auditorías que incluya la supervisión de la implantación de acciones correctivas correspondientes.

Actuaciones específicas en materia de protección de datos de carácter personal

La formación en el Ayuntamiento se realiza de forma sectorial, según el perfil y cargo de los trabajadores. En relación a la LOPD se pueden distinguir los siguientes tipos:

- Personal de asesoría legal: se imparte formación de nivel superior relativa a sentencias, expedientes, actividades de las agencias, etc.
- Personal de jefaturas de las oficinas de atención al ciudadano: se forma en introducción a la LOPD, con especial énfasis en derechos ARCO y circuitos municipales.
- Personal responsable y gestores operativos de ficheros: se imparte formación legal intensiva relativa a LOPD, Reglamento Protección de Datos, recomendaciones de la Agencia catalana y española de Protección de Datos, etc.
- Personal en general: está en preparación una introducción a la LOPD online.

En relación a la entrada en vigor del RDLOPD, se ha constituido un grupo de trabajo de la CSPD. La adaptación del Ayuntamiento se encuentra en fase de estudio.

Respecto a la Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos, se está estudiando en el seno de la Comisión de Administración Electrónica del Ayuntamiento, donde también participa la Subdirección de Información de Base y Cartografía.

11 CONCLUSIONES DEL ESTUDIO

Analizada la situación actual de las Entidades Locales españolas respecto del nivel de adopción de la normativa de protección de datos personales, se observa que a nivel global **el 28% de los ayuntamientos declara conocer el RDLOPD y un 46,4% afirma tener sus ficheros declarados en el Registro de la Agencia Española de Protección de Datos**; y si se compara con la situación extraída para la PYME española en el “*Estudio sobre el grado de adaptación de las Pequeñas y Medianas Empresas españolas a la Ley Orgánica de Protección de Datos (LOPD) y el nuevo Reglamento de Desarrollo (RDLOPD)*”²⁴ donde, en base a los datos, el nivel de conocimiento y adopción de la normativa sobre protección de datos no resultaba especialmente positivo –un 14% de la PYME declara conocer el RDLOPD, y sólo un 16% de las PYME participantes en el estudio tenían sus ficheros declarados ante la AEPD– se puede concluir que **el posicionamiento de las EELL respecto de la protección de datos de carácter personal se encuentran en un mayor nivel de madurez que el tejido empresarial español**.

Sin embargo el **nivel de conocimiento por estrato** muestra importantes diferencias, así **el porcentaje de ayuntamientos de grandes municipios es de un 76% frente al 48% en los medianos y un 20% en los pequeños. En el caso de las Diputaciones, Consells y Cabildos Insulares un 66,7% afirman conocer el nuevo reglamento de desarrollo**.

Complementariamente y a pesar de las diferencias existentes por estratos, las entidades cumplen un papel esencial tanto en la difusión de la información de la normativa entre el personal laboral, funcionarios, responsables políticos y colaboradores en las Entidades Locales, como en el cumplimiento de la misma garantizando a los ciudadanos el acceso a sus derechos.

Preguntadas las EELL sobre el nivel de concienciación respecto al cumplimiento de la normativa de protección de datos, el nivel de respuesta (un 74,8% a nivel global entre los ayuntamientos y un 58,3% para las Diputaciones, Consells y Cabildos Insulares) constituye una prueba del esfuerzo que estos organismos llevan a cabo para poder adecuarse a la normativa. El análisis por estrato y tamaño del mismo muestra un homogéneo grado de cumplimiento de esta obligación estando todos próximos a la media global.

No obstante, las EELL deben seguir trabajando y mejorando su adaptación a la normativa a través de por ejemplo el incremento de la planificación y asignación de recursos donde

²⁴ Estudio elaborado por el Observatorio de la Seguridad de la Información de INTECO (www.inteco.es). Julio 2008.

1 de cada 5 (21,4%) ayuntamientos y un 47,5 de las Diputaciones, Consells y Cabildos Insulares participantes afirman haberlo ya realizado. Detrás de este esfuerzo están:

- Los costes económicos directos e indirectos que suponen la adaptación.
- La complejidad técnico-jurídica que en algunos casos, como en los ayuntamientos de menor tamaño, implica conceptos y procesos con los que no están familiarizados.
- La necesidad de documentar las medidas, normas, procedimientos, reglas y estándares de seguridad necesarios para garantizar el nivel de seguridad establecido en la norma.
- El coste organizacional, dado que internamente exige instaurar o modificar roles, responsabilidades y procedimientos.

A todos ellos las EELL ya están haciendo frente. Así, **un 46,1% de las EELL y un 56,8% de las Diputaciones, Consells y Cabildos Insulares han definido las obligaciones y funcionales del personal responsable del tratamiento de datos personales**. Ahora bien, un análisis por estrato y tamaño del mismo muestra un irregular grado de cumplimiento de esta obligación; así el 56,5% de los ayuntamientos de grandes municipios tienen planificado dicha asignación, frente a un 31,1% de los ayuntamientos de medianos municipios y un 16,8% de los de menor tamaño.

Por otro lado, **el esfuerzo que las Entidades están realizando se encuentra en algunos casos evidenciado por el grado de implantación de algunas medidas de seguridad** esenciales. Entre las que caben destacar:

- Entidades que disponen de documento de seguridad: un 26,2% de los ayuntamientos y 50% de las Diputaciones, Consells y Cabildos Insulares.
- Entidades que cuentan con un registro de incidencias: un 20,1% de los ayuntamientos frente a un 44,4% de las Diputaciones, Consells y Cabildos Insulares.
- Entidades que tienen implantado un control de acceso de usuarios: un 40,1% de ayuntamientos y un 58,3% de las Diputaciones, Consells y Cabildos Insulares.
- Entidades que gestionan los soportes informáticos: un 36,8% de los ayuntamientos y un 50% de las Diputaciones, Consells y Cabildos Insulares.
- Entidades que realizan copias de respaldo: un 35,1% de los ayuntamientos y un 55,6% de las Diputaciones, Consells y Cabildos Insulares.

Respecto a la **inscripción de los ficheros y a la legitimación de los datos** las EELL muestran un comportamiento heterogéneo tanto a nivel global como por estrato donde los ayuntamientos de los pequeños municipios tienen un menor nivel de participación.

En relación con la inscripción, del total de ayuntamientos, el 46,4% afirma haberlos declarado en el registro de la Agencia Española de Protección de Datos (AEPD) frente a un 43% que confirma que no los ha declarado y un 10,5% que desconoce su situación. La situación por estrato y tamaño muestra que mientras el número de organismos de los grandes y medianos municipios es elevado (un 92,5% y un 67,9% respectivamente), el 37,2% de los de menor tamaño ha realizado la inscripción de los ficheros. En el caso de las Diputaciones, Consells y Cabildos Insulares, un 88,9% afirma haberlo realizado frente a sólo un 8,3% que no lo ha hecho.

En cuanto a la legitimación de los datos esta compuesta por cuatro aspectos: el deber de información, el deber de consentimiento, la gestión en la cesión y la confidencialidad de los datos. El comportamiento de los ayuntamientos presenta algunas diferencias por lo que algunas medidas presentan índices de implantación mejorables, a saber:

- Deber de información al interesado sobre la finalidad del tratamiento: a nivel global un 67,5% de los ayuntamientos y un 72,2% de las Diputaciones, Consells y Cabildos Insulares afirman cumplir con este deber. A nivel de estratos, el acatamiento se da en gran parte de ellos y varía entre un 90,7%, un 71,1% y un 65,6% de los ayuntamientos de grandes, medianos y pequeños municipios respectivamente.
- Deber de consentimiento del interesado: es una medida bastante extendida a nivel global entre los ayuntamientos y las Diputaciones, Consells y Cabildos Insulares donde en un 36,4% y un 41,7% se lo otorgan a sus ciudadanos. A nivel de estratos el cumplimiento se da en gran parte de ellos y varía entre un 67%, un 43,4% y un 33% de los ayuntamientos de grandes, medianos y pequeños municipios respectivamente.
- Gestión de la cesión de datos: un 46,9% de los ayuntamientos y un 55,6% de las Diputaciones, Consells y Cabildos Insulares a nivel global lo realizan. El cumplimiento a nivel de estratos se da en gran parte de ellos y varía entre un 71,1%, un 53,1% y un 44% de los ayuntamientos de grandes, medianos y pequeños municipios respectivamente.
- Confidencialidad de los datos: es una medida bastante extendida a nivel global entre los ayuntamientos y las Diputaciones, Consells y Cabildos Insulares donde en un 28,9% y un 44,4% se lo otorgan a sus interesados. Por estrato la situación no difiere a la del resto de medidas, dado que el 22,4% de los ayuntamientos de

los pequeños municipios la llevan a cabo, frente a un 76,1% de los de grandes municipios y a un 43,1% de los organismos de los medianos municipios.

Junto a la legitimación, uno de los puntos clave de la LOPD viene constituido por el **procedimiento de ejercicio de los derechos de acceso, rectificación, cancelación y oposición** (conocidos como derechos A.R.C.O.), reconocidos a los titulares de los datos. Esta práctica, es realizada a nivel global por el 49,4% de los ayuntamientos y el 52,8% de las Diputaciones, Consells y Cabildos Insulares. Por tamaño de estrato el grado de cumplimiento es superior a la media para los ayuntamientos de grandes y medianos municipios (79% y 58,1% respectivamente), que en el caso de los de pequeños municipios (45,4% de los ayuntamientos).

Otro elemento clave en la gestión de la normativa de protección de datos personales en las EELL es el **documento de seguridad**, cuya existencia es obligatoria. Sin embargo como antes se ha mencionado no existe a nivel global en todas las entidades participantes en el estudio. Además, y con respecto al propio documento, no es una práctica común entre las EELL la definición del alcance en el documento de seguridad, dado que a nivel global lo han realizado el 35,3% de los ayuntamientos y el 58,3% de las Diputaciones, Consells y Cabildos Insulares.

Además del alcance el documento de seguridad debe contener otra serie de aspectos que no son tenidos en cuenta por la totalidad de las entidades, así por destacar alguno están:

- La definición de las funciones y obligaciones del personal: se ha realizado por el 46,1% de los ayuntamientos y el 56,8% de las Diputaciones, Consells y Cabildos Insulares a nivel global.
- La definición de las medidas, normas, procedimientos, reglas y estándares de seguridad necesarios para garantizar el nivel de seguridad exigido: lo han hecho a nivel global el 27,6% de los ayuntamientos y el 36,1% de las Diputaciones, Consells y Cabildos Insulares.
- La descripción de los ficheros declarados y el sistema de información que los trata: frente a un 75% de las Diputaciones, Consells y Cabildos Insulares los ayuntamientos que lo han realizado a nivel global son un 38,1%.

A pesar de este nivel de desarrollo del documento de seguridad en las entidades, la normativa establece una serie de medidas que han de estar englobadas dentro de la política interna de las organizaciones. Dichas medidas exigen el cumplimiento de controles de carácter técnico y de gestión entre las que figuran:

- Registro de incidencias: un 21,1% de los ayuntamientos y un 38,9% de las Diputaciones, Consells y Cabildos Insulares realizan una gestión de incidencias.
- Identificación y autenticación: el 54,7% de los ayuntamientos y el 91,7% de las Diputaciones, Consells y Cabildos Insulares lo llevan a cabo a nivel global.
- Control de acceso: el análisis a nivel global muestra que el 70,4% de los ayuntamientos y el 91,7% de las Diputaciones, Consells y Cabildos Insulares afirman que cada usuario accede a los datos necesarios conforme al puesto que desempeñan en estas entidades.
- Registro de accesos: a nivel global un 47,7% de los ayuntamientos y un 36,1% de las Diputaciones, Consells y Cabildos Insulares llevan a cabo un registro de acceso por cual se guardan, de cada acceso a los datos la información
- Telecomunicaciones: el cifrado de datos personales en las transmisiones a través de redes de comunicaciones muestra que a nivel global el 46,8% de los ayuntamientos y el 58,3% de las Diputaciones, Consells y Cabildos Insulares lo realiza.
- Gestión de soportes: realizado a nivel global por el 58,3% de los ayuntamientos y el 72,2% de las Diputaciones, Consells y Cabildos Insulares.
- Copias de respaldo: a nivel global entre las entidades participantes el 55,2% de los ayuntamientos y el 94,4% de las Diputaciones, Consells y Cabildos Insulares realizan una copia completa de todos los datos al menos una vez a la semana
- Pruebas con datos reales: la respuesta de las entidades participantes en el estudio muestra que a nivel global el 60% de los ayuntamientos y el 58,3% de las Diputaciones, Consells y Cabildos Insulares afirman que las pruebas no se realizan con datos reales frente a un 25% y a un 27,8% respectivamente que si los utilizan
- Auditoría: el 10,9% de los ayuntamientos y el 19,4% de las Diputaciones, Consells y Cabildos Insulares a nivel global afirman que en sus entidades se realizan las auditorías con la periodicidad que establece la norma.

El último aspecto sobre el que se les ha preguntado a las EELL es sobre el **conocimiento de las sanciones por el incumplimiento de la normativa** y si han sufrido alguna inspección o sanción. Destaca el desconocimiento de la existencia de sanciones entre los ayuntamientos de municipios pequeños (menos de una cuarta parte las conoce, en concreto un 24,1%). A nivel global el 32,1% de los ayuntamientos conoce

las sanciones recogidas en la normativa y el 5,7% ha sido objeto de inspección por la AEPD; por un 42,1% de los ayuntamientos de grandes municipios que si lo ha sufrido.

Como conclusión, existe entre las entidades una alta concienciación para el cumplimiento de la normativa y razonable nivel de inscripción de ficheros frente a las PYME, un 46% de media en las Entidades frente al 16%. Este hecho se caracteriza por la vocación pública de las entidades, por el conocimiento y sensibilidad hacia la importancia de preservar la confidencialidad e integridad de los datos personales que se manejan de los ciudadanos y empresas y por la percepción de su impacto en imagen pública y posibles sanciones de las Agencias de Protección de Datos de Carácter Personal, ya sea del ámbito estatal o autonómicas.

En el lado contrario, las entidades se enfrentan a la insuficiencia presupuestaria sobre todo en el caso de los ayuntamientos de pequeños municipios, para la implantación de los debidos controles, y a la falta de personal especializado y la necesidad de planes formativos continuos, principalmente en las pequeñas y medianas Entidades Locales, donde sólo un 20% de los ayuntamientos pequeños tiene un responsable de seguridad.

Esta oportunidad de mejora, al mismo tiempo que obligación legal, en las organizaciones, así como las recomendaciones de los expertos para abordar progresivamente la madurez de sus procesos, debe primero ponerse en el contexto más amplio del impulso a la administración electrónica que supone el enorme reto de implantar la Ley 11/2007 y, segundo, una actuación coordinada y decidida de todas las Administraciones y Agencias que deberán actuar como agentes y facilitadoras de las Entidades mas pequeñas.

12 PROPUESTAS Y RECOMENDACIONES DIRIGIDAS A LOS PODERES PÚBLICOS

Este capítulo recoge las propuestas y recomendaciones señaladas por los expertos consultados en base a su experiencia así como las extraídas de las conclusiones del Estudio, identificadas como generadoras de valor en la adopción e implantación de la normativa en materia de protección de datos por parte de las EELL.

Las recomendaciones que se recogen en este capítulo deben tener la consideración de acciones de orientación en el diseño de programas de mejora, para la adaptación e implementación de las medidas de seguridad establecidas en la LOPD y en el RDLOPD, para acometer, tanto por parte de las propias Entidades Públicas Locales como por el resto de actores que intervienen en los procesos de evaluación, definición e implantación de dichas medidas en el ámbito de la protección de datos de carácter personal.

En particular, se describen aquellas iniciativas que pueden contribuir a la expansión de las mejores prácticas propuestas por los expertos y resultantes de las conclusiones del informe, cuyo escaso grado de implantación por las Administraciones Locales se ha evidenciado a partir de los resultados de la encuesta realizada.

Las recomendaciones propuestas se han elaborado a partir de la premisa de progresividad de niveles de madurez que pretenden ayudar a las Administraciones Públicas a marcar las prioridades, asignar los recursos y focalizar los resultados para obtener la mejor relación coste-beneficio que exige toda gestión de programas de financiación pública.

12.1 Propuestas y recomendaciones en materia de concienciación y formación

Realización de programas de concienciación, difusión, divulgación y comunicación del nuevo RDLOPD

La implantación efectiva de una cultura de protección de datos debe contar con acciones de concienciación, difusión, divulgación y comunicación.

En esta línea, la AEPD ha publicado distintas 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 adaptación de las Entidades Locales a la normativa sobre protección de datos” que pretende acercar a las Entidades Locales el contenido de la normativa en materia de protección de datos de carácter personal, para establecer los principales objetivos, destinatarios y procesos de adaptación a la LOPD y a su nuevo RDLOPD.

Además la existencia de dichas acciones debe permitir aumentar el grado de conocimiento de funcionarios, laborales y colaboradores en materia de seguridad de los datos y de las medidas exigidas para los datos de carácter personal, por lo que el despliegue de esta iniciativa debe darse tanto en el ámbito estatal como en las Comunidades Autónomas.

Cursos de formación y teleformación adaptados a las necesidades y particularidades de los empleados de las EELL

La dispersión geográfica de las EELL y el elevado número de usuarios potenciales aconseja la utilización de la teleformación y de la formación de formadores.

Estos cursos deberían considerar diferentes niveles de madurez y competencias, a saber: incompleto, cumplimiento y mejora continua; y básico, intermedio y avanzado, respectivamente, de acuerdo con las responsabilidades asumidas por los funcionarios, personal laboral y colaboradores de la Administración Local, es decir: responsable del fichero, responsable de seguridad, técnico informático y usuario.

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

Es conveniente por otro lado, que el reconocimiento de las acciones formativas se realice por los organismos oficiales pertinentes (Agencias de Protección de Datos, Instituto Nacional de Administración Pública²⁵ –INAP–, etc.), contribuyendo con ello a incrementar la percepción de su importancia y necesidad por parte de todos los usuarios.

Así los cursos deberán tener una currícula homologada por las Agencias de Protección de Datos y los organismos oficiales competentes (INAP, CCAA) e impartirse en las diferentes lenguas cooficiales del Estado español.

Por último, se debe primar la creación de una red de alta capilaridad de tutores e instructores para el apoyo a las acciones formativas virtuales y presenciales dado que su presencia será decisiva para el éxito de esta actuación.

12.2 Propuestas y recomendaciones en materia de diagnóstico e información

Diagnóstico periódico del estado de la seguridad de los datos de carácter personal en las Administraciones Locales

La realización de un diagnóstico sobre el estado de seguridad de los datos de carácter personal en las Administraciones Locales, ha de permitir a estas tomar las medidas

²⁵ Más información disponible en www.inap.map.es

oportunas de cara a conseguir el más alto grado de adaptación e implementación de las disposiciones normativas en materia de protección de datos.

Dichas acciones deberían extenderse también a las páginas Web de las entidades, con el objetivo de evitar que por ejemplo los listados con datos personales se constituyan en una fuente de datos pública.

Elaboración de un sistema de medición y seguimiento de indicadores sobre el estado de seguridad de los datos

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

12.3 Propuestas y recomendaciones en materia de financiación

Apoyo presupuestario directo

Las Entidades Locales son actores claves para lograr el acceso electrónico de los ciudadanos a los Servicios Públicos, lo que plantea un tratamiento riguroso en relación con la privacidad y seguridad de los datos de los ciudadanos y empresas para asegurar el éxito de esta iniciativa legislativa.

En situaciones de insuficiencia financiera de las Entidades, que por ende puedan repercutir en la asignación de recursos específicos para el ámbito de actuación y competencia en materia de protección de datos, aquellas deberán verse apoyadas con ayudas y subvenciones directas de carácter finalista para la adaptación continua en protección de datos.

Apoyo presupuestario indirecto

La ausencia de personal en el seno de las Entidades que puedan desarrollar la adaptación a la normativa no debe ser el justificante del retraso, por este motivo los propios organismos han de poder acceder a cursos de formación o campañas de difusión que complementen los recursos propios de las EELL.

También otra posibilidad es la creación de grupos de trabajo entre las entidades para la puesta en común de sus problemáticas o el establecimiento de convenios de colaboración con las Agencias de Protección de Datos.

12.4 Propuestas y recomendaciones en materia de normalización y certificación

Identificación y autenticación mediante firma digital

La implantación y utilización generalizada de la firma digital y sus certificados de atributos como sistema de identificación y autenticación segura, es el medio idóneo para el control y verificación por el Responsable del Fichero de los accesos de los usuarios a los datos personales en las Entidades.

Certificación de la seguridad de la información y confianza digital

La implantación efectiva y la acreditación de las mejores prácticas identificadas de seguridad de la información, como evidencia interna y frente a terceros siguiendo los esquemas de certificación internacional como el ISO IEC 27001 y 27002²⁶, contribuirá a la implantación de controles de cumplimiento normativo, en general, y de protección de datos, en particular, así como a las auditorías y a las revisiones posteriores.

12.5 Propuestas y recomendaciones en materia de promoción e incentivación de los niveles de madurez y buenas prácticas

Creación de algún tipo de Entidad de ayuda y soporte para favorecer la implantación de la normativa

Esta propuesta se considera especialmente indicada para las Entidades de reducido tamaño por las dificultades añadidas puesta de manifiesto a lo largo del estudio.

La nueva entidad que se cree podría formalizarse a través por ejemplo de la FEMP y facilitaría la adaptación a la norma en los ayuntamientos y a las Diputaciones, Consells y Cabildos Insulares. Esta labor la conseguiría mediante la identificación de los niveles de madurez y buenas prácticas por tamaño de estrato o por ejemplo en la constitución de equipos de trabajo para el conjunto de entidades.

Además esta nueva entidad podría servir como nexo entre los responsables de protección de datos de las Entidades Locales, para:

- Poder disponer de un foro común donde plantear problemas, dudas o peticiones, que surgen a la hora de implantar las medidas de seguridad exigidas por la normativa.
- Realizar convenios con entidades que puedan garantizar el acceso seguro a los datos, dando además un servicio de gestión automatizada de las incidencias.

²⁶ ISO/IEC 27001 es el estándar para la seguridad de la información. Especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información en las organizaciones. ISO 27002 proporciona recomendaciones de las mejores prácticas en la gestión de la seguridad de la información, dividido en once secciones y por cada una de ellas se especifican los objetivos de los distintos controles. En total 133 controles que cada organización debe considerar según sus propias necesidades.

Apoyo en la adaptación e implementación de las disposiciones del nuevo Reglamento

Debido al gran volumen de archivos de que disponen las EELL, este apoyo se hace especialmente necesario para el supuesto en el cual se almacenan y tratan ficheros de nivel alto y, por lo tanto, se deben implantar controles relativos al registro de acceso.

Por este motivo, sería conveniente que las entidades antes de poner en marcha nuevos servicios o áreas, sean capaces de diseñar e implementar controles cuyo fin último sea la realización de evaluaciones de impacto sobre la privacidad vaya a tener dichas iniciativas. Cubriendo aspectos no sólo de cumplimiento normativo, si no también de incidencia sobre la privacidad en sentido amplio y teniendo en cuenta el factor de la opinión pública.

13 ANEXOS

13.1 Expertos participantes

- Adrián García Campos. Director General de Hacienda. Ayuntamiento de Palma de Mallorca.
- Alberto Bernardez Jiménez. Departamento de Informática. Ayuntamiento de Alcalá de Guadaíra.
- Alberto Virto. Jefe de Proyectos de Sistemas de Información. Ayuntamiento de Zaragoza.
- Ana M^a Colas. Jefa de Desarrollo y Aplicaciones. Cabildo de Gran Canaria.
- Ana Novoa. Responsable de Seguridad de Datos de Carácter Personal. Ayuntamiento de Vitoria.
- Antonio Marín Pérez. Jefe del Servicio de Protección de Datos. Ayuntamiento de Madrid.
- Blanca Eulalia Sánchez Rabanal. Técnico del Observatorio de la Seguridad de la Información. Instituto Nacional de Tecnologías de la Comunicación.
- David Quirós. Área de Gobernación del Ayuntamiento de Hospitalet.
- Eduardo Risco. Jefe de Informática. Ayuntamiento de Lugo.
- Emilio Aced Felez. Subdirector General del Registro de Ficheros y Consultoría. Agencia de Protección de Datos de la Comunidad de Madrid.
- Jaume Taulats. Jefe del Servicio de Información y Comunicación. Ayuntamiento de Granollers.
- Javier Rey Perille. Técnico del Observatorio de la Seguridad de la Información. Instituto Nacional de Tecnologías de la Comunicación.
- José Antonio Díaz Sosa. Jefe de Informática. Cabildo de la Isla de La Palma.
- José Damián Ferrer Quintana. Jefe del Servicio de Telecomunicaciones y Sistemas. Gobierno de Canarias.
- José Félix Muñoz Soro. Director del Observatorio Aragonés. Gobierno de Aragón.

- José Ramón Ferri. Jefe del Servicio de Tecnologías de la Información y Comunicación. Ayuntamiento de Valencia.
- Josep Clotet Sopena. Gerente del Ayuntamiento de Lleida.
- Juan Manuel Serrano. Dirección de Organización y Recursos. Federación Española de Municipios y Provincias.
- Luis Sanz Marco. Subdirector de Informática de Base y Cartografía del Instituto Municipal de Informática. Ayuntamiento de Barcelona.
- Manuel Bellido Mengual. Socio Director de Caveat Abogados.
- María José Blanco Antón. Subdirectora General del Registro de Protección de Datos. Agencia Española de Protección de Datos.
- Mario Pons Botella. Concejal de Modernización, Fomento y Calidad. Ayuntamiento de Alcoy.
- Monika Serrano. Directora de Servicios Jurídicos. Federación Española de Municipios y Provincias.
- Juan Pablo Peñarubia y Eusebio Moya López. Servicio de Gestión Informática y Organización. Diputación de Valencia.
- Pablo Pérez San-José. Gerente del Observatorio de la Seguridad de la Información. Instituto Nacional de Tecnologías de la Comunicación.
- Patricia Fernández. Concejala del Régimen Interior Personal y Asuntos Jurídicos. Ayuntamiento de San Andrés de Rabanedo.
- Pedro Alberto González. Responsable de Registro y Nuevas Tecnologías. Agencia Vasca de Protección de Datos.
- Ramón Martín Miralles López. Coordinador de Auditoría y Seguridad de la Información. Agencia Catalana de Protección de Datos.
- Valentín Pérez Martínez. Gerente Organismo Autónomo de Gestión Económica y Recaudación (OAGER). Ayuntamiento de Salamanca.

13.2 Entidades participantes

13.2.1 Relación de Ayuntamientos

Comunidad Autónoma	Provincia	Nº	Municipio
Andalucía	Almería	1	Albox
Andalucía	Almería	2	Antas
Andalucía	Almería	3	El Ejido
Andalucía	Almería	4	Gádor
Andalucía	Almería	5	Nijar
Andalucía	Almería	6	Roquetas de Mar
Andalucía	Almería	7	Vera
Andalucía	Almería	8	Vícar
Andalucía	Cádiz	9	Barbate
Andalucía	Cádiz	10	Bornos
Comunidad Autónoma	Provincia	Nº	Municipio
Andalucía	Cádiz	11	Chiclana de la Frontera
Andalucía	Cádiz	12	Jerez de la Frontera
Andalucía	Cádiz	13	La Línea
Andalucía	Cádiz	14	Puerto Real
Andalucía	Cádiz	15	Rota
Andalucía	Cádiz	16	San Fernando
Andalucía	Córdoba	17	Benamejí
Andalucía	Córdoba	18	Córdoba
Andalucía	Córdoba	19	Montilla
Andalucía	Córdoba	20	Pedro Abad
Andalucía	Córdoba	21	Villanueva de Córdoba
Andalucía	Córdoba	22	Zuheros
Andalucía	Granada	23	Granada
Andalucía	Granada	24	Guadix
Andalucía	Granada	25	Huétor Santillán
Andalucía	Granada	26	Jayena
Andalucía	Granada	27	La Taha
Andalucía	Granada	28	Las Gabias
Andalucía	Granada	29	Lecrín
Andalucía	Granada	30	Morelabor
Andalucía	Granada	31	Ogijares
Andalucía	Granada	32	Pinos Puente
Andalucía	Huelva	33	Aracena
Andalucía	Huelva	34	Cala
Andalucía	Huelva	35	Cartaya
Andalucía	Huelva	36	Galaroza
Andalucía	Huelva	37	Gibraleón
Andalucía	Huelva	38	Huelva
Andalucía	Huelva	39	Lepe
Andalucía	Huelva	40	Punta Umbría
Andalucía	Jaén	41	Montizón
Andalucía	Jaén	42	Villacarrillo
Andalucía	Málaga	43	Alhaurín de la Torre
Andalucía	Málaga	44	Alpandeire
Andalucía	Málaga	45	Antequera
Andalucía	Málaga	46	Benalmadena
Andalucía	Málaga	47	Cártama
Andalucía	Málaga	48	Casares
Andalucía	Málaga	49	Cortes de la Frontera
Andalucía	Málaga	50	Estepona
Andalucía	Málaga	51	Fuengirola
Andalucía	Málaga	52	Istán
Andalucía	Málaga	53	Júzcar
Andalucía	Málaga	54	Manilva
Andalucía	Málaga	55	Marbella
Andalucía	Málaga	56	Mijas
Andalucía	Málaga	57	Montejaque
Andalucía	Málaga	58	Nerja
Andalucía	Málaga	59	Rincón de la Victoria
Andalucía	Málaga	60	Riogordo
Andalucía	Málaga	61	Ronda
Andalucía	Málaga	62	Torrox
Andalucía	Sevilla	63	Alcalá de Guadaíra
Andalucía	Sevilla	64	Alcolea del Río
Andalucía	Sevilla	65	Carrión de los Cespedes
Andalucía	Sevilla	66	Castilleja del Campo

Andalucía	Sevilla	67	Coria del Río
Andalucía	Sevilla	68	Dos Hermanas
Andalucía	Sevilla	69	La Algaba
Andalucía	Sevilla	70	Pilas
Andalucía	Sevilla	71	Rinconada
Aragón	Huesca	72	Agrupación secretarial Lascuarre
Aragón	Huesca	73	Alcubierre
Aragón	Huesca	74	Angües
Aragón	Huesca	75	Castejon de Sos
Aragón	Huesca	76	Castiello de Jaca
Aragón	Huesca	77	El Grado
Aragón	Huesca	78	Panticosa
Aragón	Huesca	79	Posan de Vero
Aragón	Teruel	80	Allepuz
Aragón	Teruel	81	Miravete de la Sierra
Aragón	Teruel	82	Mora de Rubielos
Comunidad Autónoma	Provincia	Nº	Municipio
Aragón	Teruel	83	Villanueva del Rebollar de la Sierra
Aragón	Teruel	84	Villarroya de los Pinares
Aragón	Zaragoza	85	Alhama de Aragón
Aragón	Zaragoza	86	Figueroelas
Aragón	Zaragoza	87	Jaraba
Aragón	Zaragoza	88	La Puebla de Alfinden
Aragón	Zaragoza	89	Leciñena
Aragón	Zaragoza	90	Monegrillo
Aragón	Zaragoza	91	Tarazona
Aragón	Zaragoza	92	Zaragoza
Comunidad Valenciana	Alicante	93	Alcoy
Comunidad Valenciana	Alicante	94	Almoradi
Comunidad Valenciana	Alicante	95	Beneixama
Comunidad Valenciana	Alicante	96	Benferri
Comunidad Valenciana	Alicante	97	Beniarbeig
Comunidad Valenciana	Alicante	98	Benidorm
Comunidad Valenciana	Alicante	99	Crevillent
Comunidad Valenciana	Alicante	100	Dolores
Comunidad Valenciana	Alicante	101	Gaianes
Comunidad Valenciana	Alicante	102	Javea
Comunidad Valenciana	Alicante	103	Los Montesinos
Comunidad Valenciana	Alicante	104	Monóvar
Comunidad Valenciana	Alicante	105	Novelda
Comunidad Valenciana	Alicante	106	Orihuela
Comunidad Valenciana	Alicante	107	Pego
Comunidad Valenciana	Alicante	108	Torrevieja
Comunidad Valenciana	Castellón	109	Betxí
Comunidad Valenciana	Castellón	110	Cabanes
Comunidad Valenciana	Castellón	111	Castellón de la Plana
Comunidad Valenciana	Castellón	112	Forcall
Comunidad Valenciana	Castellón	113	Jerica
Comunidad Valenciana	Castellón	114	L'Alcora
Comunidad Valenciana	Castellón	115	Matet
Comunidad Valenciana	Castellón	116	Moncofa
Comunidad Valenciana	Castellón	117	Todolella
Comunidad Valenciana	Castellón	118	Vall d'Alba
Comunidad Valenciana	Castellón	119	Vall d'Uixó
Comunidad Valenciana	Castellón	120	Vilafamés
Comunidad Valenciana	Castellón	121	Vila-real
Comunidad Valenciana	Valencia	122	Albaida
Comunidad Valenciana	Valencia	123	Alboraya
Comunidad Valenciana	Valencia	124	Aldaia
Comunidad Valenciana	Valencia	125	Alfajar
Comunidad Valenciana	Valencia	126	Algemesi
Comunidad Valenciana	Valencia	127	Alginet
Comunidad Valenciana	Valencia	128	Benageber
Comunidad Valenciana	Valencia	129	Bonrepòs i Mirambell
Comunidad Valenciana	Valencia	130	Camporrobles
Comunidad Valenciana	Valencia	131	Cerda
Comunidad Valenciana	Valencia	132	Emperador
Comunidad Valenciana	Valencia	133	Fois
Comunidad Valenciana	Valencia	134	Gandia
Comunidad Valenciana	Valencia	135	Gilet
Comunidad Valenciana	Valencia	136	Godella
Comunidad Valenciana	Valencia	137	Llíria
Comunidad Valenciana	Valencia	138	Llocnou de Sant Jeroni
Comunidad Valenciana	Valencia	139	Ontinyent

Comunidad Valenciana	Valencia	140	Picassent
Comunidad Valenciana	Valencia	141	Rafelguaraf
Comunidad Valenciana	Valencia	142	Sedaví
Comunidad Valenciana	Valencia	143	Sueca
Comunidad Valenciana	Valencia	144	Utiel
Comunidad Valenciana	Valencia	145	Valencia
Comunidad Valenciana	Valencia	146	Villar del Arzobispo
Canarias	Las Palmas	147	Agüimes
Canarias	Las Palmas	148	Las Palmas de Gran Canaria
Canarias	Las Palmas	149	Mogán
Canarias	Las Palmas	150	Santa Lucía de Tirajana
Canarias	Las Palmas	151	Valsequillo de Gran Canaria
Canarias	Las Palmas	152	Yaiza
Canarias	Santa Cruz de Tenerife	153	Arona
Canarias	Santa Cruz de Tenerife	154	Garachico
Canarias	Santa Cruz de Tenerife	155	Granadilla de Abona
Comunidad Autónoma	Provincia	Nº	Municipio
Canarias	Santa Cruz de Tenerife	156	Güímar
Canarias	Santa Cruz de Tenerife	157	La Matanza de Acentejo
Canarias	Santa Cruz de Tenerife	158	Los Llanos de Aridane
Canarias	Santa Cruz de Tenerife	159	Puerto de la Cruz
Canarias	Santa Cruz de Tenerife	160	Santa Cruz de Tenerife
Canarias	Santa Cruz de Tenerife	161	Tijarafe
Canarias	Santa Cruz de Tenerife	162	Vallehermoso
Cantabria	Cantabria	163	Arenas de Iguña
Cantabria	Cantabria	164	Cabezón de la Sal
Cantabria	Cantabria	165	Campoo de Yuso
Cantabria	Cantabria	166	Comillas
Cantabria	Cantabria	167	Pesquera
Cantabria	Cantabria	168	Rasines
Cantabria	Cantabria	169	Santa Cruz de Bezana
Cantabria	Cantabria	170	Santander
Cantabria	Cantabria	171	Valdeolea
Castilla - La Mancha	Albacete	172	Casas de Juan Núñez
Castilla - La Mancha	Albacete	173	Ferez
Castilla - La Mancha	Albacete	174	Golosalvo
Castilla - La Mancha	Albacete	175	Tobarra
Castilla - La Mancha	Albacete	176	Villaverde de Guadalimar
Castilla - La Mancha	Ciudad Real	177	Ciudad Real
Castilla - La Mancha	Ciudad Real	178	Cózar
Castilla - La Mancha	Ciudad Real	179	Daimiel
Castilla - La Mancha	Ciudad Real	180	Torre Nueva
Castilla - La Mancha	Ciudad Real	181	Villanueva de la Fuente
Castilla - La Mancha	Ciudad Real	182	Villarrubia de los Ojos
Castilla - La Mancha	Cuenca	183	Cañete
Castilla - La Mancha	Cuenca	184	Cuenca
Castilla - La Mancha	Cuenca	185	Iniesta
Castilla - La Mancha	Cuenca	186	Olmeda del Rey
Castilla - La Mancha	Cuenca	187	Pozoamargo
Castilla - La Mancha	Cuenca	188	Sisante
Castilla - La Mancha	Cuenca	189	Ucles
Castilla - La Mancha	Guadalajara	190	Alcolea del Pinar
Castilla - La Mancha	Guadalajara	191	Alovera
Castilla - La Mancha	Guadalajara	192	Condemios de Arriba
Castilla - La Mancha	Guadalajara	193	Checa
Castilla - La Mancha	Guadalajara	194	Hijos
Castilla - La Mancha	Guadalajara	195	Orea
Castilla - La Mancha	Guadalajara	196	Tórtola de Henares
Castilla - La Mancha	Toledo	197	Alcaudete de la Jara
Castilla - La Mancha	Toledo	198	Arcicóllar
Castilla - La Mancha	Toledo	199	Los Yébenes
Castilla - La Mancha	Toledo	200	Mora
Castilla - La Mancha	Toledo	201	Seseña
Castilla - La Mancha	Toledo	202	Toledo
Castilla - La Mancha	Toledo	203	Villatobas
Castilla - La Mancha	Toledo	204	Yuncler
Castilla y León	Burgos	205	Aranda de Duero
Castilla y León	Burgos	206	Atapuerca
Castilla y León	Ávila	207	Cebreros
Castilla y León	Burgos	208	Miranda de Ebro
Castilla y León	Ávila	209	Navahondilla
Castilla y León	Burgos	210	Oña
Castilla y León	Burgos	211	Pancorbo
Castilla y León	Burgos	212	Regumiel de la Sierra

Castilla y León	Burgos	213	Rubena
Castilla y León	León	214	Bembibre
Castilla y León	León	215	Cea
Castilla y León	León	216	La Bañeza
Castilla y León	León	217	León
Castilla y León	León	218	Ponferrada
Castilla y León	León	219	San Andrés del Rabanedo
Castilla y León	León	220	Valderrey
Castilla y León	León	221	Valencia de Don Juan
Castilla y León	León	222	Villablino
Castilla y León	León	223	Villaquejida
Castilla y León	León	224	Villaselán
Castilla y León	Palencia	225	Brañosera
Castilla y León	Palencia	226	Reinoso de Cerrato
Castilla y León	Palencia	227	Venta de Baños
Castilla y León	Palencia	228	Villaviudas
Comunidad Autónoma	Provincia	Nº	Municipio
Castilla y León	Salamanca	229	Alconada
Castilla y León	Salamanca	230	Calvarrasa de Arriba
Castilla y León	Salamanca	231	Castellanos de Moriscos
Castilla y León	Salamanca	232	Ciudad Rodrigo
Castilla y León	Salamanca	233	Cordovilla
Castilla y León	Salamanca	234	Espeja
Castilla y León	Salamanca	235	Galinduste
Castilla y León	Salamanca	236	Hinojosa de Duero
Castilla y León	Salamanca	237	Mieza
Castilla y León	Salamanca	238	Moriñigo
Castilla y León	Salamanca	239	Parada de Rubiales
Castilla y León	Salamanca	240	San Felices de los Gallegos
Castilla y León	Salamanca	241	San Martín del Castañar
Castilla y León	Salamanca	242	Sancti-Spiritus
Castilla y León	Salamanca	243	Terradillos
Castilla y León	Salamanca	244	Vitigudino
Castilla y León	Segovia	245	Cerezo de Abajo
Castilla y León	Segovia	246	La Losa
Castilla y León	Segovia	247	Mozoncillo
Castilla y León	Segovia	248	Samboal
Castilla y León	Segovia	249	Segovia
Castilla y León	Segovia	250	Turégano
Castilla y León	Soria	251	Berlanga de Duero
Castilla y León	Soria	252	Covalada
Castilla y León	Soria	253	Ólvega
Castilla y León	Soria	254	San Leonardo de Yagüe
Castilla y León	Valladolid	255	Aldeamayor de San Martín
Castilla y León	Valladolid	256	Arroyo de la Encomienda
Castilla y León	Valladolid	257	Castrejón de Trabanca
Castilla y León	Valladolid	258	Medina de Rioseco
Castilla y León	Valladolid	259	Medina del Campo
Castilla y León	Valladolid	260	Mucientes
Castilla y León	Valladolid	261	Olmedo
Castilla y León	Valladolid	262	Tordehumos
Castilla y León	Valladolid	263	Torre de la Orden
Castilla y León	Valladolid	264	Valoria la Buena
Castilla y León	Valladolid	265	Viana de Cega
Castilla y León	Valladolid	266	Villanueva de Duero
Castilla y León	Valladolid	267	Zaratan
Castilla y León	Zamora	268	Benavente
Castilla y León	Zamora	269	Pedralba de Pradería
Castilla y León	Zamora	270	Puebla de Sanabria
Castilla y León	Zamora	271	Requejo
Cataluña	Barcelona	272	Badalona
Cataluña	Barcelona	273	Caldes de Montbui
Cataluña	Barcelona	274	Calella
Cataluña	Barcelona	275	Capolat
Cataluña	Barcelona	276	Cardedeu
Cataluña	Barcelona	277	Castellar del Vallès
Cataluña	Barcelona	278	Cerdanyola del Vallès
Cataluña	Barcelona	279	Cornellà de Llobregat
Cataluña	Barcelona	280	D'Avinyó
Cataluña	Barcelona	281	Esplugues de Llobregat
Cataluña	Barcelona	282	Font-Rubí
Cataluña	Barcelona	283	Granollers
Cataluña	Barcelona	284	Hospitalet
Cataluña	Barcelona	285	Masquefa

Cataluña	Barcelona	286	Monistrol de Calders
Cataluña	Barcelona	287	Pont de Vilomara i Rocafort (El)
Cataluña	Barcelona	288	Pontons
Cataluña	Barcelona	289	Prat de Llobregat (El)
Cataluña	Barcelona	290	Premià de Mar
Cataluña	Barcelona	291	Ripollet
Cataluña	Barcelona	292	Saldes
Cataluña	Barcelona	293	Sant Adrià de Besòs
Cataluña	Barcelona	294	Sant Just Desvern
Cataluña	Barcelona	295	Sant Martí Sesgueioles
Cataluña	Barcelona	296	Santa Maria de Miralles
Cataluña	Barcelona	297	Santa Susana
Cataluña	Barcelona	298	Santpedor
Cataluña	Barcelona	299	Sora
Cataluña	Barcelona	300	Ullastrell
Cataluña	Barcelona	301	Vic
Comunidad Autónoma	Provincia	Nº	Municipio
Cataluña	Barcelona	302	Vilanova del Camí
Cataluña	Barcelona	303	Vilanova i la Geltrú
Cataluña	Girona	304	Begur
Cataluña	Girona	305	Brunyola
Cataluña	Girona	306	Calonge
Cataluña	Girona	307	D'Hostalric
Cataluña	Girona	308	Girona
Cataluña	Girona	309	Palafrugell
Cataluña	Girona	310	Sant Feliu de Guíxols
Cataluña	Girona	311	Sant Joan de les Abadesses
Cataluña	Girona	312	Santa Pau
Cataluña	Girona	313	Vall de Bianya (La)
Cataluña	Girona	314	Vilabertran
Cataluña	Girona	315	Vilablareix
Cataluña	Lleida	316	Alcoletge
Cataluña	Lleida	317	D'Aspa
Cataluña	Lleida	318	Juncosa
Cataluña	Lleida	319	Lleida
Cataluña	Lleida	320	Maldà
Cataluña	Lleida	321	Mollerussa
Cataluña	Lleida	322	Montferrer i Castellbò
Cataluña	Lleida	323	Palau d'Anglesola (El)
Cataluña	Lleida	324	Roselló
Cataluña	Lleida	325	Vilagrassa
Cataluña	Tarragona	326	Alcover
Cataluña	Tarragona	327	Borges del Camp, Les
Cataluña	Tarragona	328	Flix
Cataluña	Tarragona	329	Horta de Sant Joan
Cataluña	Tarragona	330	Riudecanyes
Cataluña	Tarragona	331	Santa Bàrbara
Cataluña	Tarragona	332	Tarragona
Cataluña	Tarragona	333	Torredembarra
Cataluña	Tarragona	334	Tortosa
Cataluña	Tarragona	335	Vendrell (El)
Comunidad de Madrid	Madrid	336	Arroyomolinos
Comunidad de Madrid	Madrid	337	Brunete
Comunidad de Madrid	Madrid	338	Buitrago del Lozoya
Comunidad de Madrid	Madrid	339	Ciempozuelos
Comunidad de Madrid	Madrid	340	Cobeña
Comunidad de Madrid	Madrid	341	Colmenar Viejo
Comunidad de Madrid	Madrid	342	Colmenarejo
Comunidad de Madrid	Madrid	343	Collado Villalba
Comunidad de Madrid	Madrid	344	Corpa
Comunidad de Madrid	Madrid	345	Chapinería
Comunidad de Madrid	Madrid	346	El Berrueco
Comunidad de Madrid	Madrid	347	Fuenlabrada
Comunidad de Madrid	Madrid	348	Guadarrama
Comunidad de Madrid	Madrid	349	Madrid
Comunidad de Madrid	Madrid	350	Meco
Comunidad de Madrid	Madrid	351	Navacerrada
Comunidad de Madrid	Madrid	352	Parla
Comunidad de Madrid	Madrid	353	Pozuelo del Rey
Comunidad de Madrid	Madrid	354	Puebla de la Sierra
Comunidad de Madrid	Madrid	355	San Martín de la Vega
Comunidad de Madrid	Madrid	356	San Sebastián de los Reyes
Comunidad de Madrid	Madrid	357	Serranillos del Valle
Comunidad de Madrid	Madrid	358	Torrejón de Velasco

Comunidad de Madrid	Madrid	359	Tres Cantos
Comunidad de Madrid	Madrid	360	Valdemoro
Comunidad de Madrid	Madrid	361	Velilla de San Antonio
Comunidad de Madrid	Madrid	362	Villanueva de la Cañada
Comunidad Foral de Navarra	Navarra	363	Ayegui
Comunidad Foral de Navarra	Navarra	364	Barañain
Comunidad Foral de Navarra	Navarra	365	Burlada / Burlata
Comunidad Foral de Navarra	Navarra	366	Cabanillas
Comunidad Foral de Navarra	Navarra	367	Esteribar
Comunidad Foral de Navarra	Navarra	368	Lodosa
Comunidad Foral de Navarra	Navarra	369	Mendigorría
Comunidad Foral de Navarra	Navarra	370	Murchante
Comunidad Foral de Navarra	Navarra	371	Pamplona / Iruña
Comunidad Foral de Navarra	Navarra	372	Puente La Reina / Gares
Comunidad Foral de Navarra	Navarra	373	Tudela
Comunidad Foral de Navarra	Navarra	374	Urdazubi / Urdax
Comunidad Autónoma	Provincia	Nº	Municipio
Comunidad Foral de Navarra	Navarra	375	Villava / Atarrabia
Comunidad Foral de Navarra	Navarra	376	Zugarramurdi
Extremadura	Badajoz	377	Badajoz
Extremadura	Badajoz	378	Olivenza
Extremadura	Badajoz	379	Peñalsordo
Extremadura	Badajoz	380	Valdetorres
Extremadura	Badajoz	381	Valverde de Leganés
Extremadura	Badajoz	382	Villagonzalo
Extremadura	Badajoz	383	Zafra
Extremadura	Badajoz	384	Zalamea de la Serena
Extremadura	Cáceres	385	Bohonal de Ibor
Extremadura	Cáceres	386	Cañaveral
Extremadura	Cáceres	387	El Gordo
Extremadura	Cáceres	388	Holguera
Extremadura	Cáceres	389	Majadas
Extremadura	Cáceres	390	Plasencia
Extremadura	Cáceres	391	Puerto de Santa Cruz
Galicia	A Coruña	392	A Coruña
Galicia	A Coruña	393	Arteixo
Galicia	A Coruña	394	Carballo
Galicia	A Coruña	395	Cerceda
Galicia	A Coruña	396	Fene
Galicia	A Coruña	397	Ferrol
Galicia	A Coruña	398	Miño
Galicia	A Coruña	399	Moeche
Galicia	A Coruña	400	O Pino
Galicia	A Coruña	401	Ribeira
Galicia	A Coruña	402	Sada
Galicia	A Coruña	403	Santiago de Compostela
Galicia	Lugo	404	Baralla
Galicia	Lugo	405	Lugo
Galicia	Lugo	406	Meira
Galicia	Lugo	407	Sarria
Galicia	Ourense	408	Amoeiro
Galicia	Ourense	409	Avión
Galicia	Ourense	410	Oímbra
Galicia	Ourense	411	Ourense
Galicia	Ourense	412	Petín
Galicia	Ourense	413	Quintela de Leirado
Galicia	Ourense	414	Taboadela
Galicia	Ourense	415	Verín
Galicia	Pontevedra	416	Cangas
Galicia	Pontevedra	417	Cerdedo
Galicia	Pontevedra	418	Lalín
Galicia	Pontevedra	419	Mondariz-Balneario
Galicia	Pontevedra	420	Salceda de Caselas
Galicia	Pontevedra	421	Tomiño
Galicia	Pontevedra	422	Vigo
Galicia	Pontevedra	423	Vilanova de Arousa
Illes Balears	Illes Balears	424	Calvià
Illes Balears	Illes Balears	425	Ciutadella de Menorca
Illes Balears	Illes Balears	426	Muro
Illes Balears	Illes Balears	427	Palma de Mallorca
Illes Balears	Illes Balears	428	Sant Joan de Labritja
La Rioja	La Rioja	429	Alfaro
La Rioja	La Rioja	430	Arnedo
La Rioja	La Rioja	431	Briones

La Rioja	La Rioja	432	Calahorra
La Rioja	La Rioja	433	Haro
La Rioja	La Rioja	434	Nájera
La Rioja	La Rioja	435	San Millán de la Cogolla
País Vasco	Álava	436	Lapuebla de Labarca
País Vasco	Álava	437	Laudio / Llodio
País Vasco	Guipúzcoa	438	Errenteria
País Vasco	Guipúzcoa	439	Hernani
País Vasco	Guipúzcoa	440	Irun
País Vasco	Guipúzcoa	441	Mendaro
País Vasco	Guipúzcoa	442	Tolosa
País Vasco	Guipúzcoa	443	Zestoa
País Vasco	Guipúzcoa	444	Zumarraga
País Vasco	Vizcaya	445	Barakaldo
País Vasco	Vizcaya	446	Basauri
País Vasco	Vizcaya	447	Bilbao
Comunidad Autónoma	Provincia	Nº	Municipio
País Vasco	Vizcaya	448	Ermua
País Vasco	Vizcaya	449	Getxo
País Vasco	Vizcaya	450	Ondarroa
País Vasco	Vizcaya	451	Portugalete
Principado de Asturias	Asturias	452	Aller
Principado de Asturias	Asturias	453	Avilés
Principado de Asturias	Asturias	454	Bimenes
Principado de Asturias	Asturias	455	Castropol
Principado de Asturias	Asturias	456	Colunga
Principado de Asturias	Asturias	457	Peñamellera Baja
Principado de Asturias	Asturias	458	Ribadedeva
Principado de Asturias	Asturias	459	San Martín del Rey Aurelio
Principado de Asturias	Asturias	460	Santo Adriano
Principado de Asturias	Asturias	461	Tineo
Principado de Asturias	Asturias	462	Villayón
Región de Murcia	Murcia	463	Albudeite
Región de Murcia	Murcia	464	Cartagena
Región de Murcia	Murcia	465	Cieza
Región de Murcia	Murcia	466	Fuente Álamo de Murcia
Región de Murcia	Murcia	467	Jumilla
Región de Murcia	Murcia	468	Molina de Segura
Región de Murcia	Murcia	469	Murcia
Región de Murcia	Murcia	470	Pliego
Región de Murcia	Murcia	471	San Javier
Región de Murcia	Murcia	472	Santomera
Región de Murcia	Murcia	473	Torre-Pacheco
Región de Murcia	Murcia	474	Totana

ÍNDICE DE GRÁFICOS

Gráfico 1: Perfil de los profesionales participantes en las encuesta como representantes de las EELL participantes (%)	26
Gráfico 2: Nivel de conocimiento del alcance, la entrada en vigor y los plazos de implantación disponibles en la normativa de protección de datos por tamaño (%).....	31
Gráfico 3: Conocimiento de las nuevas medidas de seguridad para ficheros no automatizados del RDLOPD en Ayuntamientos de grandes municipios y en Diputaciones, Consells y Cabildos Insulares (%)	32
Gráfico 4: Conocimiento de las medidas de seguridad para ficheros no automatizados del RDLOPD en pequeños y medianos municipios (%)	33
Gráfico 5: Difusión a los trabajadores de las funciones y obligaciones respecto al tratamiento de los datos personales entre los ayuntamientos por tamaño (%).....	34
Gráfico 6: Difusión a los trabajadores de las funciones y obligaciones respecto al tratamiento de los datos personales por tamaño del municipio (%)	34
Gráfico 7: Conocimiento del RDLOPD vs, nivel de la planificación de recursos para la adecuación en grandes ayuntamientos y Diputaciones, Consells y Cabildos Insulares (%)	36
Gráfico 8: Conocimiento del RDLOPD vs, nivel de la planificación de recursos para la adecuación en pequeños y medianos municipios (%).....	37
Gráfico 9: Tipología de medidas técnicas u organizativas adoptadas por los ayuntamientos para proteger los datos de carácter personal (%)	38
Gráfico 10: Tipología de medidas técnicas u organizativas adoptadas por las entidades para proteger los datos de carácter personal por tamaño (%)	39
Gráfico 11: Tipología de datos clasificados de nivel alto que contienen los ficheros de de carácter personal que las Entidades disponen, por tamaño (%)	42
Gráfico 12: Inscripción de ficheros de datos de carácter personal en el registro general de ficheros de la Agencia de Protección de Datos estatal o autonómica correspondientes, por tamaño (%).....	50
Gráfico 13: Inscripción de ficheros de datos de carácter personal en el registro general de ficheros de la Agencia de Protección de Datos estatal o autonómica correspondientes, en pequeños y medianos municipios (%)	51

Gráfico 14: Distribución de las entidades locales donde se ha procedido a nombrar un responsable de seguridad entre los que tienen inscritos ficheros, por tamaño (%)	53
Gráfico 15: Establecimiento de medidas, normas y procedimientos de seguridad por tamaño (%)	56
Gráfico 16: Inclusión en el documento de seguridad de los procedimientos de realización de copias de respaldo y de recuperación de los datos, por tamaño (%)	59
Gráfico 17: Información al interesado sobre la finalidad de la recopilación de los datos, en función del tamaño de los municipios (%)	62
Gráfico 18: Información al interesado sobre la cesión de los datos a otras organizaciones, en función del tamaño de los municipios (%)	64
Gráfico 19: Información al interesado de cómo proceder para ejercer los derechos ARCO, en función del tamaño de los municipios (%)	68
Gráfico 20: Establecimiento de criterios de acceso de los usuarios a los sistemas de información, en función del tamaño de los municipios (%)	71
Gráfico 21: Definición de procesos para la identificación y autenticación vs. existencia de mecanismos que permitan la identificación de forma individualizada de los usuarios y la verificación de que está autorizado, en función del tamaño de los municipios (%)	73
Gráfico 22: Establecimiento de procedimientos de asignación y gestión de contraseñas vs. establecimiento de un límite para los intentos reiterados fallidos de acceso al sistema, en función del tamaño de los municipios (%)	74
Gráfico 23: Almacenamiento de contraseñas de forma ininteligible, en función del tamaño de los municipios (%)	75
Gráfico 24: Establecimientos de controles de acceso mediante la asignación de los permisos para cada usuario de forma individualizada vs. establecimiento de controles de seguridad para evitar el acceso sin autorización, en función del tamaño de los municipios (%)	76
Gráfico 25: Registro de los accesos a los datos, en función del tamaño de los municipios (%)	79
Gráfico 26: Realización por los responsables de seguridad de un control de los registros emitiendo un informe mensual en aquellas EELL que han nombrado a éste, por tamaño (%)	80

Gráfico 27: Realización del control de los registros de acceso y conservación de los mismos por las EELL, en función del tamaño de los municipios (%)	81
Gráfico 28: Inventario de soportes, en función del tamaño de los municipios (%)	83
Gráfico 29: Gestión de salida y entrada de soportes vs. autorización, por tamaño (%)	85
Gráfico 30: Distribución de EELL que llevan a cabo el cifrado de datos contenidos en soportes que salen de las instalaciones de la entidad, en función del tamaño de los municipios (%)	87
Gráfico 31: Realización por las EELL de copia de respaldo completa vs. garantiza la reconstrucción de los datos, por tamaño (%)	89
Gráfico 32: Autorización por escrito del responsable de los procesos vs. registro de las restauraciones de datos, en función del tamaño de los municipios (%)	91
Gráfico 33: Realización por las EELL de pruebas de las nuevas aplicaciones con datos reales, por tamaño (%)	93
Gráfico 34: Realización por las EELL de pruebas de aplicaciones con datos reales vs. aplicación de medidas de seguridad, por tamaño (%)	94
Gráfico 35: Establecimiento de deficiencias y propuestas correctoras en el informe de la auditoria, en función del tamaño de los municipios (%)	96
Gráfico 36: Sufrimiento de alguna sanción por parte de la Agencia de Protección de Datos, por tamaño (%)	99
Gráfico 37: Tipos de sanciones impuestas a las EELL que han sufrido alguna por parte de la Agencia de Protección de Datos, por tamaño (%)	101
Gráfico 38: Establecimiento de niveles de madurez para la implantación de las medidas de seguridad en las EELL (%)	104
Gráfico 39: Identificación por los expertos de las medidas de nivel 1 de madurez a implantar por las EELL	107
Gráfico 40: Identificación por los expertos de las medidas de nivel 2 de madurez a implantar por las EELL	109
Gráfico 41: Identificación por los expertos de las medidas de nivel 3 de madurez a implantar por las EELL	111

ÍNDICE DE TABLAS

Tabla 1: Estratificación poblacional	23
Tabla 2: Participación de entidades locales por Comunidades Autónomas sobre la muestra y la cobertura poblacional.....	24
Tabla 3: Participación de entidades por estratos sobre la muestra de municipios y la cobertura poblacional	25
Tabla 4: Distribución muestral por estrato, y coeficiente de ponderación para las entidades locales que han contestado el cuestionario ampliado sobre el total de la muestra participante (%).	27
Tabla 5: Distribución muestral por estrato, y coeficiente de ponderación para las entidades locales que han contestado el cuestionario simplificado sobre el total de la muestra participante (%).	27
Tabla 6: Distribución muestral por estrato, y coeficiente de ponderación para las entidades locales que han contestado el cuestionario ampliado sobre el tamaño (%)	28
Tabla 7: Distribución muestral por estrato, y coeficiente de ponderación para las entidades locales que han contestado el cuestionario simplificado sobre el tamaño (%) .	28
Tabla 8: Conocimiento del nuevo reglamento (RDLOPD), por tamaño (%)	31
Tabla 9: Nivel de planificación en la asignación de recursos para la adecuación a las medidas definidas en el RDLOPD por tamaño (%)	36
Tabla 10: Niveles de Seguridad.....	40
Tabla 11: Clasificación de niveles de seguridad definidos en el RDLOPD de los datos que contienen los ficheros de carácter personal que los Ayuntamientos disponen (%).	41
Tabla 12: Clasificación de niveles de seguridad definidos en el RDLOPD de los datos que contienen los ficheros de carácter personal que las Diputaciones, Consells y Cabildos Insulares disponen (%)	43
Tabla 13: Distribución de las entidades locales donde se ha procedido a nombrar un responsable de seguridad, por tamaño (%).	53
Tabla 14: Definición del alcance de aplicación del documento de seguridad, por tamaño (%)	55

Tabla 15: Definición de las funciones y obligaciones del personal, por tamaño (%).....	56
Tabla 16: Inclusión en el documento de seguridad de la descripción de los ficheros declarados y el sistema de información que los trata, por tamaño (%)	57
Tabla 17: Inclusión en el documento de seguridad de los procedimientos de notificación, gestión y respuesta ante las incidencias que pudieran devenir, por tamaño (%).....	58
Tabla 18: Inutilización de soportes desechados o reutilizados, por tamaño (%).....	60
Tabla 19: Entidades que solicitan el consentimiento de los interesados, por tamaño (%)	63
Tabla 20: Firma de cláusulas de confidencialidad por lo trabajadores y terceras personas que prestan servicios a las Entidades, por tamaño (%)	65
Tabla 21: Realización de un registro de la incidencia, el momento en que se ha producido, la persona que la notifica, la persona a la que se le comunica y los efectos derivados en los sistemas de información, por tamaño (%)	70
Tabla 22: Existencia de una lista actualizada de usuarios, incluyendo los derechos de acceso que tiene autorizados, por tamaño (%)	72
Tabla 23: Concesión de permisos de acceso para los usuarios realizada solamente por personal autorizado, por tamaño (%)	77
Tabla 24: Acceso físico a los sistemas de información, por tamaño (%)	77
Tabla 25: Cifrado de los datos en las transmisiones a través de redes de telecomunicaciones, por tamaño (%)	82
Tabla 26: Identificación de la información contenida en los soportes, por tamaño (%).....	83
Tabla 27: Control de acceso físico a los soportes, por tamaño (%)	84
Tabla 28: Existencia de medidas para impedir la recuperación indebida de información, por tamaño (%).....	86
Tabla 29: Entidades que llevan a cabo la realización de una copia de respaldo completa de todos los datos al menos una vez a la semana (salvo que en dicho periodo no se hayan producido ningún cambio en los datos), por tamaño (%)	88
Tabla 30: Comprobación de la definición y aplicación de los procedimientos de copia y restauración de datos, por tamaño (%)	90

Tabla 31: Entidades que guardan las copias de respaldo y una copia del procedimiento de recuperación de los datos en un lugar diferente de aquel en el que se encuentran los equipos informáticos que los tratan, por tamaño (%)92

Tabla 32: Realización auditoría bianual, por tamaño (%).....95

Tabla 33: Realización por el responsable de seguridad del análisis de los informes, compartiendo las conclusiones con el responsable del fichero, por tamaño (%)96

Tabla 34: Sufrimiento de alguna inspección por parte de la Agencia de Protección de Datos, por tamaño (%).....98

Tabla 35: Conocimiento de las sanciones que puede imponer la Agencia Española de Protección de Datos, por tamaño (%).....99

Tabla 36: Tipo de sanción impuesta a las EELL que afirman haber sufrido alguna, por tamaño (%) 100



Instituto Nacional
de Tecnologías
de la Comunicación

<http://www.inteco.es>

<http://observatorio.inteco.es>