La seguridad en la Administración electrónica

PID_00238293

Agustí Cerrillo i Martínez
Sandra González
Ascen Moro

Tiempo mínimo de dedicación recomendado: 3 horas

Universitat Oberta de Catalunya

Índice

Introducción

Las tecnologías de la información y la comunicación están suponiendo nuevas amenazas para la seguridad de las transacciones y de los datos. Estas amenazas tienen una incidencia especial en relación con los datos personales.

En este módulo, se presentarán las medidas que el derecho está adoptando para poder garantizar la seguridad de las transacciones electrónicas. Asimismo, se analizarán los instrumentos para proteger los datos de las personas frente a los ataques que pueden provenir de Internet.

Objetivos

1. Conocer los instrumentos para garantizar la seguridad de las transacciones electrónicas.

2. Conocer la regulación de la protección de datos personales.

3. Analizar los distintos usos de los medios electrónicos en la Administración pública desde la perspectiva de la protección de los datos personales.

4. Valorar el impacto de la protección de datos personales en el desarrollo de la Administración electrónica.

1. La seguridad en las transacciones electrónicas

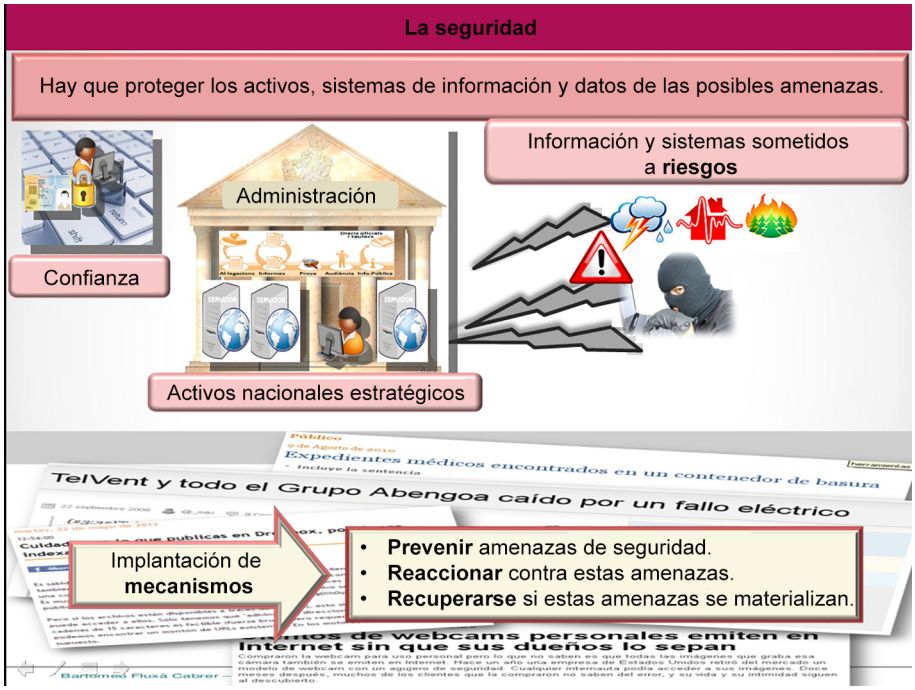
El uso de los medios electrónicos en las administraciones públicas comporta una serie de riesgos inherentes a la seguridad de estas transacciones. La información y los servicios que las administraciones públicas prestan están sometidos a riesgos que pueden provenir de una pluralidad de situaciones: acciones ilícitas, accidentes de seguridad, errores, desastres naturales, etc., que amenazan, entre otras informaciones, a activos considerados como estratégicos nacionales. No es difícil imaginar la importancia de los datos que la Administración maneja, y entender que deben protegerse de todas estas acciones que pueden amenazar su integridad.

De hecho, la seguridad de los sistemas de información y telecomunicaciones que soportan las administraciones públicas forma parte de una de las 8 líneas de acción que se incluyen en la estrategia de ciberseguridad nacional, cuyo contenido se materializa en garantizar la implantación del esquema nacional de seguridad, reforzar las capacidades de detección y mejorar la defensa de los sistemas[1].

(1)Ver http://www.lamoncloa.gob.es/documents/20131332estrategiadeciberseguridadx.pdf.

En este contexto, el reconocimiento del derecho a comunicarse con las administraciones públicas a través de medios electrónicos comporta una obligación correlativa de estas, consistente en la promoción de las condiciones necesarias para que estas transacciones se produzcan en un contexto adecuado, donde la libertad y la igualdad sean reales y efectivas, y se actúe en la superación de los obstáculos que puedan aparecer y que dificultan su pleno reconocimiento.

La ciudadanía, de manera legítima, ha de poder confiar en que los servicios disponibles electrónicamente se prestan en unas condiciones de seguridad equivalentes a los servicios prestados en los puntos de atención presencial, que es la relación tradicional con la Administración. En muchas ocasiones, la infrautilización de los servicios públicos digitales se debe al recelo que muestra la ciudadanía basado en la percepción injustificada de una mayor vulnerabilidad de la información en soporte electrónico, que puede provocarles riesgos de pérdida de privacidad.



Por todos estos motivos, la LAECSP fijó el concepto de seguridad a lo largo de todo su articulado. La preocupación de la Ley por la seguridad se materializa de manera transversal, aunque cabe destacar las manifestaciones en:

- **Objeto de la ley**: la LAECSP puntualizó que las administraciones públicas han de utilizar las TIC de acuerdo con lo que dispone la ley y asegurar la disponibilidad, el acceso, la autenticidad, la confidencialidad y la conservación de datos, las informaciones y los servicios que gestionen en el ejercicio de sus competencias[2].

(2)Art. 1.2 LAECSP.

- **Finalidades de la ley**: la LAECSP indica que han de crearse las condiciones de confianza en el uso de los medios electrónicos y establecer las medidas necesarias para la preservación de la integridad de los derechos fundamentales y, en especial, las relaciones con la intimidad y la protección de datos de carácter personal por medio de la garantía de la seguridad de los sistemas, los datos, las comunicaciones y los servicios electrónicos. Así, este artículo dota el concepto de seguridad y de las dimensiones de integridad, autenticidad, confidencialidad y disponibilidad, de un indiscutible protagonismo legal[3].

(3)Art. 3 LAECSP.

- **Principios generales en relación con la seguridad**: la LAECSP incluye diferentes principios como el principio de protección de datos de carácter personal, el principio de accesibilidad o el principio de seguridad. En particular, el principio de seguridad en la implantación y el uso de los medios electrónicos constituye el límite inferior de seguridad que hay que aportar, de manera que no resultaría razonable que el procedimiento tramitado electrónicamente sea menos seguro que el tramitado en soporte papel. Y por último, el principio de proporcionalidad en virtud del cual solo se exigen las garantías y medidas de seguridad adecuadas a la natu-

(4)Art. 4 LAECSP.

raleza y circunstancias de los diferentes trámites y actuaciones. Este principio constituye el límite superior de seguridad, en el sentido de que no resultaría razonable exigir un nivel de seguridad superior al necesario, en tanto que constituiría una barrera en el acceso de los ciudadanos a los servicios electrónicos[4].

Por otro lado, la LAECSP también estableció otras medidas de seguridad adicionales en la regulación de alguna de las instituciones más destacadas en el ámbito de la Administración electrónica como, por ejemplo, en la sede electrónica[5], en la transmisión de datos entre las diferentes administraciones[6]. Estas son aplicables, por conexión, a la publicación de diarios oficiales[7], el tablón de anuncios electrónico[8] y el registro electrónico[9].

(5)Arts. 10 y 17 LAECSP.

(6)Arts. 9 y 20 LAECSP.

(7)Art. 11 LAECSP.

(8)Art. 12 LAECSP.

(9)Art. 24 y ss. LAECSP.

Finalmente, otras manifestaciones de seguridad las encontramos con referencia a la identificación de los ciudadanos en la relación electrónica[10], en la identificación de la Administración pública[11], en las comunicaciones electrónicas[12] y en el archivo electrónico[13].

(10)Arts. 13 a 16 y 21 LAECSP.

(11)Arts. 17 a 19 LAECSP.

(12)Arts. 27 y 28 LAECSP.

(13)Art. 31 LAECSP.

En paralelo a estos principios, la LAECSP asentó definitivamente este concepto regulando verdaderos derechos de los ciudadanos en relación con la seguridad: el derecho a la garantía de la seguridad y confidencialidad de los datos que figurarán en los ficheros, sistemas y aplicaciones de la administraciones públicas, el derecho a obtener los medios de identificación electrónica necesarios y el derecho al uso de otros sistemas de firma electrónica admitidos en el ámbito de las administraciones públicas[14].

(14)Art. 6.2 LAECSP.

Con la aprobación de la LPACAP y la LRJSP, estos principios y derechos referidos a la seguridad han sido incorporados en su articulado, de manera más o menos explícita. Concretamente, la LPACAP recoge en sede de los derechos de las personas en sus relaciones con las administraciones públicas el derecho a la obtención y utilización de los medios de identificación y firma electrónica[15] y el derecho a la protección de datos de carácter personal (en particular, la seguridad y confidencialidad de los datos que figuren en los ficheros, sistemas y aplicaciones de las administraciones públicas[16]).

(15)Art.13.g) LPACAP.

(16)Art.13.h) LPACAP.

Por otro lado, la Ley hace constantes referencias al esquema nacional de seguridad. Así se puede observar en la regulación de los registros[17], el archivo electrónico[18] y en la validez y eficacia de las copias efectuadas por las administraciones públicas[19].

(17)Art. 16 LPACAP.

(18)Art. 17 LPACAP.

(19)Art. 27 LPACAP.

L 11/2007 LAECSP	L 39/2015 LPACAP	L 40/2015 LRJSP
Transmisión de datos (arts. 9 y 20) Sede electrónica (arts. 10 y 17)	Derecho de las personas en sus relaciones con la Administración pública (art. 13.h)	Las administraciones públicas se relacionarán entre sí a través de medios electrónicos que aseguren la integridad y la seguridad de los sistemas y soluciones, garantizarán LOPD (art. 3.2).
Publicación diarios oficiales (art. 11)	Registros (art. 16.1)	Intercambio electrónico de datos en entornos cerrados de comunicaciones (art. 44).
Registro electrónico (art. 24 a 26)	Archivo documentos (art. 17.3)	La sede electrónica (art. 38) Archivo electrónico de documentos (art. 46).
Comunicaciones (arts. 27 y 28) Archivo electrónico (art. 31) Tablón de anuncios (art. 12)	Validez y eficacia de las copias (art. 27.3) Cómputo plazos registros (art. 31)	Transmisiones de datos entre admini. públicas (art. 155). Remisión al ENS y al ENI (art. 156) Reutilización sistemas y aplicaciones (art. 157) Transferencia tecnología entre administraciones (art. 158)
Art. 42 LAECSP → Creación del ENS / Art. 156 LRJSP → Reconoce ENS.		

De la misma manera, la LRJSP también se encuentra impregnada de referencias al concepto de seguridad. En este sentido, cuando se regulan los principios generales, la Ley dispone que en la relación electrónica entre las administraciones públicas los medios que la posibiliten deberán asegurar la interoperabilidad y la seguridad de los sistemas y soluciones adoptados por cada una de ellas, y garantizarán la protección de los datos de carácter personal[20]. Asimismo, de manera similar a la regulación que hacía la LAECSP, la LRJSP establece previsiones de seguridad para otros instrumentos esenciales que posibilitan la tramitación electrónica: la sede electrónica[21], el intercambio electrónico de datos en entornos cerrados de comunicación[22], en el archivo electrónico[23], en la transferencia de tecnología entre administraciones públicas[24] y en la reutilización de sistemas y aplicaciones[25].

[20] Art. 3.2 LRJSP.

[21] Art. 38 LRJSP.

[22] Art. 44 LRJSP.

[23] Art. 46 LRJSP.

[24] Art. 158 LRJSP.

[25] Art. 157 LRJSP.

En este escenario, para garantizar el cumplimiento de todas estas disposiciones por parte de las administraciones públicas, la LAESCP previó la creación del esquema nacional de seguridad, que posteriormente fue desarrollado por el Real Decreto 3/2010 ENS, y que ha sido recientemente modificado por el Real Decreto 951/2015, de 23 octubre[26].

[26] Art. 42.2 LAESCP.

Más tarde, con la aprobación de las leyes vigentes de procedimiento administrativo común y régimen jurídico (LPACAP y LRJSP), la referencia concreta al ENS la encontramos en la LRJSP[27].

El ENS constituye normativa básica, y por tanto es de obligado cumplimiento para el conjunto de administraciones públicas.

(27)Art. 156 LRJSP.

2. El esquema nacional de seguridad. El Plan de adecuación

La finalidad del ENS es la creación de las condiciones necesarias de confianza en el uso de los medios electrónicos, a través de medidas que han de garantizar la seguridad de los sistemas, los datos, las comunicaciones y los servicios electrónicos, de modo que permita a los ciudadanos y a las administraciones públicas el ejercicio de derechos y el cumplimiento de deberes a través de estos medios, y está constituido por los principios básicos[28] y requisitos mínimos requeridos[29] para una protección adecuada de la información.

(28)Capítulo 2 RD 3/2010, de 8 de enero, por el que se regula el ENS.

(29)Capítulo 3 RD 3/2010, de 8 de enero, por el que se regula el ENS.

Los principios básicos del ENS establecen unos puntos de referencia para la toma de decisiones con referencia a las medidas de seguridad que hay que tomar; es decir, en las propias palabras del ENS son:

> «Los fundamentos que deben regir toda acción orientada a asegurar la información y los servicios.»

A diferencia de los principios básicos, los requisitos mínimos deben cumplirse siempre. Generalmente, se implementan con la aplicación de las medidas de seguridad establecidas en el anexo II del ENS, incluso en el caso de que estas medidas sean sustituidas por otras medidas compensatorias.

El ámbito objetivo de aplicación del ENS gira en torno al concepto básico de **sistema de información**, definido en la misma norma[30] como:

(30)Anexo IV.

> «El conjunto organizado de recursos para que la información se pueda recoger, almacenar, procesar o tratar, mantener, usar, compartir, distribuir, poner a disposición, presentar o transmitir.»

A pesar de complejidad del concepto, se puede considerar que los sistemas de información incluidos dentro del alcance del ENS son:

- Sistemas de información accesibles electrónicamente por los ciudadanos.
- Sistemas de información para el ejercicio de derechos.
- Sistemas de información para el cumplimiento de deberes.
- Sistemas de información para recabar información y estado del procedimiento administrativo.

Y todo esto independientemente del sistema de acceso por parte de la ciudadanía. Es decir, estarán incluidos dentro del ámbito de protección del ENS tanto los sistemas de información que dan soporte a la tramitación en línea, a los cuales se accede a través de las sedes electrónicas, como aquellos en los que se soporta la tramitación ofrecida en los puntos de tramitación presencial.

Como ejemplo práctico, se puede afirmar que entrarían dentro del ámbito de aplicación del ENS las sedes electrónicas, los registros electrónicos, las carpetas electrónicas o espacios que permitan recabar información y estado del procedimiento administrativo, así como un sistema de *back-office* utilizado para la gestión de procedimientos administrativos o el sistema de telefonía, en tanto incidan directamente en el normal desenvolvimiento del procedimiento administrativo y que prive a la ciudadanía del ejercicio de sus derechos o cumplimiento de obligaciones.

Así, con la aplicación de estas medidas de seguridad se busca, en esencia, minimizar el impacto que tendrían los incidentes de seguridad en los sistemas que permiten a la ciudadanía ejercer derechos y cumplir obligaciones.

Es lógico, por tanto, que los ayuntamientos hayan adquirido un papel protagonista en la aplicación de las medidas de seguridad que establece el ENS, dado el amplio catálogo de servicios que ofrecen a la ciudadanía. En la práctica, son muy pocos los sistemas de información municipales que serían excluidos del ámbito objetivo del ENS.

En cambio, cabe señalar que están excluidos del ámbito de aplicación del ENS los sistemas que tratan información clasificada regulada por Ley 9/1968 de 5 de abril, de secretos oficiales y sus normas de desarrollo.

De acuerdo con el texto normativo, con la aplicación del ENS se persiguen los siguientes objetivos:

1) Crear las condiciones necesarias de confianza en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de la información y los servicios electrónicos, que permita a los ciudadanos y las administraciones públicas el ejercicio de derechos y el cumplimiento de deberes a través de estos medios.

2) Establecer la política de seguridad en la utilización de medios electrónicos en el ámbito de la Ley 11/2007, que estará constituida por los principios básicos y requisitos mínimos para una protección adecuada de la información.

3) Introducir los elementos comunes que deben guiar la actuación de las administraciones públicas en materia de seguridad de las tecnologías de la información.

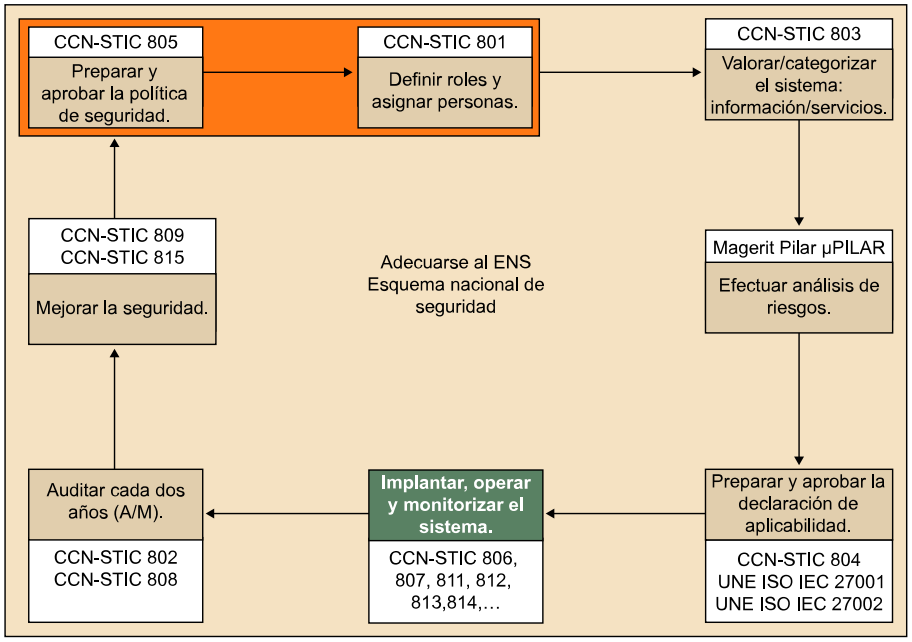
4) Aportar un lenguaje común para facilitar la interacción de las administraciones públicas, así como la comunicación de los requisitos de seguridad de la información en la industria.

5) Aportar un tratamiento homogéneo de la seguridad que facilite la cooperación en la prestación de servicios de Administración electrónica cuando participan varias entidades.

6) Facilitar un tratamiento continuado de la seguridad.

Para la consecución de estos objetivos, el ENS plantea un Plan de adecuación en la disposición transitoria del Real Decreto 3/2010, de 8 de enero. De acuerdo con lo que establecía esta disposición, los sistemas de las administraciones debían adecuarse al ENS en el plazo de 12 meses desde su entrada en vigor. No obstante, en el caso de que hubiera circunstancias que impidieran la plena aplicación, la Administración debía adoptar un Plan de adecuación que dispusiera los plazos de ejecución, que en ningún caso podría superar los 48 meses desde la entrada en vigor. La complejidad de la materia, así como la evolución constante y exponencial tanto de los sistemas de información como de las ciberamenazas, no han permitido a la mayoría de las administraciones públicas cumplir en plazo con el objetivo marcado por el legislador. Precisamente, la modificación del ENS introduce un nuevo plazo de 24 meses para adecuarse a las nuevas prescripciones establecidas, que se pueden conceptualizar en las siguientes[31]:

(31)Disposición transitoria única Real Decreto 951/2015.



Fuente: http://administracionelectronica.gob.es/pae_Home/pae_Estrategias/pae_Seguridad_Inicio/pae_Esquema_Nacional_de_Seguridad.html#.VsGVhvnhCWs.

Cabe destacar que en el camino al cumplimiento del ENS, habrá que llevar a cabo una serie de actuaciones, para lo cual es muy útil tomar como punto de partida la planificación que propone en su portal de Administración electrónica el Ministerio de Hacienda y Administraciones Públicas.

Para clarificar las previsiones del ENS, cada fase lleva aparejada una guía de implantación elaborada por el Centro Criptológico Nacional (CCN-STIC). Estas guías, editadas por el Centro Criptológico Nacional, y sin carácter imperativo respecto a su cumplimiento, difunden metodologías y recomendaciones para el adecuado seguimiento de lo dispuesto en el ENS, de acuerdo con lo previsto en el artículo 29 del Real Decreto 3/2010. En la actualidad, existen 49 guías a disposición de las administraciones públicas[32].

(32)Ver https://www.ccn-cert.cni.es/guias/indice-de-guias.html.

A grandes rasgos, las actuaciones se pueden concretar en las siguientes:

- Preparar y aprobar la política de seguridad, CCN-STIC 805 Política de seguridad de la información[33].

- Llevar a cabo un análisis de riesgos que incluya la valoración de las medidas de seguridad existentes.

- Preparar y aprobar la declaración de aplicabilidad de las medidas del anexo II ENS, CCN-STIC 804 Medidas e implantación del esquema nacional de seguridad[34].

- Implantar, operar y monitorizar las medidas de seguridad a través de la gestión continuada de la seguridad correspondiente.

- Auditar la seguridad CCN-STIC 802 Auditoría del Esquema Nacional de Seguridad[35] y CCN-STIC 808, verificación del cumplimiento de las medidas en el esquema nacional de seguridad[36].

- Informar sobre el estado de la seguridad CCN-STIC 815 métricas e indicadores en el esquema nacional de seguridad[37] y CCN-STIC 824, informe del Estado de seguridad[38].

(33)Véase https://goo.gl/IvmdW8.

(34)Véase https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/800-Esquema_Nacional_de_Seguridad/804-Medidas_de_implantacion_del_ENS/804_medidas_de_ implantacion_del_ens.pdf.

(35)Véase https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/800-Esquema_Nacional_de_Seguridad/802-Auditoria_ENS/802-Auditoria_ ENS-jun10.pdf.

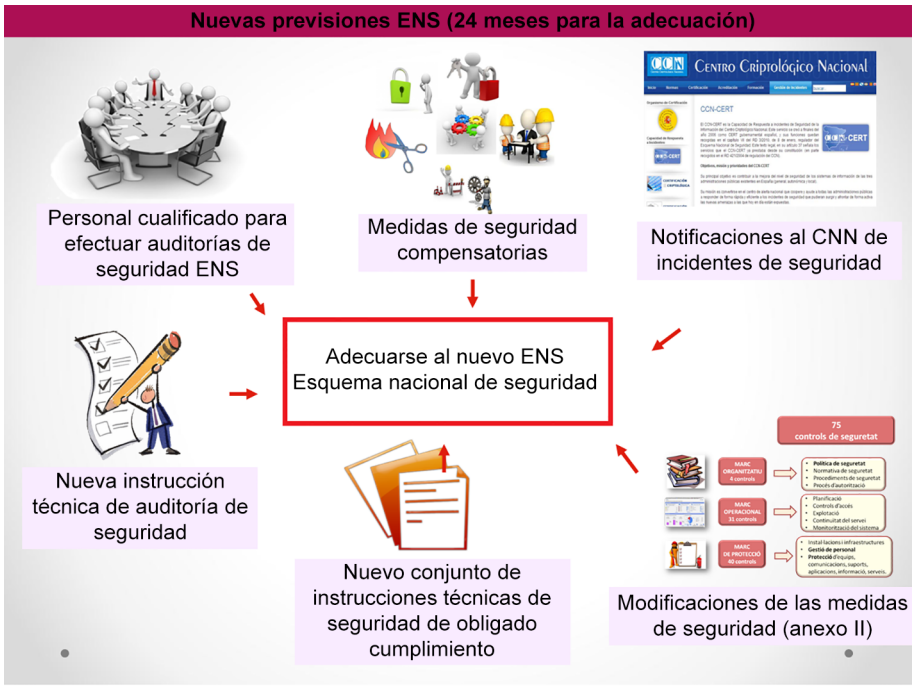
(36)Véase https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/800-Esquema_Nacional_de_Seguridad/808/808-Verificacion_del_cumplimiento_medidas_ ENS-sep11.pdf.

(37)Véase https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/800-Esquema_Nacional_de_Seguridad/815-Metricas_e_Indicadores_en_el_ENS/815_Metricas_e_indicadores_en_el_ENS-feb14.pdf.

(38)Véase http://administracionelectronica.gob.es/pae_Home/dms/pae_Home/documentos/Estrategias/pae_Seguridad_Inicio/824-Informe_del_estado_de_seguridad-sep12.pdf.

- Elaborar un Plan de adecuación para la mejora de la seguridad. CCN-STIC 806, Plan de adecuación del esquema nacional de seguridad[39].

(39)Véase https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/800-Esquema_Nacional_de_Seguridad/806-Plan_adecuacion_ENS/806_ENS-adecuacion_ene-11.pdf.



3. Recomendaciones y criterios para adecuar las organizaciones al ENS. El sistema de gestión de la seguridad de la información

A la hora de elaborar el Plan de adecuación al ENS por parte de las administraciones públicas, es importante identificar previamente el punto de partida de cada organización, y establecer una hoja de ruta específica integrando la seguridad como un proceso integral que afecta a todos y cada uno de los sistemas.

Uno de los organismos autonómicos que han publicado una guía con recomendaciones concretas para llevar a la práctica esta adecuación es el Centro de Seguridad de la Información de Cataluña (CESICAT), que destaca las siguientes:

1) Alinear la implantación de las medidas de seguridad previstas en la ENS con la estrategia de desarrollo de la Administración electrónica, en relación con los sistemas de información nuevos, que considere también los sistemas antiguos que se vean afectados por el proceso de modernización.

2) Alinear las medidas de protección previstas en la ENS con las medidas de seguridad previstas en el RD 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LO 15/1999, de 13 de diciembre, de protección de datos de carácter personal, ya que ciertamente una gran parte de los sistemas de información dentro del ámbito de aplicación de la ENS también gestionan datos de carácter personal. En este sentido, resulta muy recomendable crear una única estructura documental que demuestre el cumplimiento de los requisitos de seguridad y que trate de manera coherente e integrada ambas reglamentaciones.

3) Llevar a cabo un plan director de adecuación de los sistemas existentes, en especial los que ofrecen apoyo a las nuevas aplicaciones de Administración electrónica, pero que no se ven afectados por políticas de modernización, para cumplir con el principio de tratamiento integral de la seguridad.

4) Redactar la política de seguridad de la Administración y desplegarla mediante un cuerpo normativo bien documentado, alineado con las mejores prácticas identificadas en la normativa internacional, como por ejemplo la ISO 27000, y con una orientación a la futura certificación del proceso.

Es importante señalar que el proceso de adecuación al ENS tiene por finalidad el establecimiento de un sistema de gestión de la seguridad de la información (SGSI) tal y como se recoge en el anexo III, que exige la gestión continuada de la seguridad, en línea con los principios básicos relativos a «la seguridad como un proceso integral[40]», la «reevaluación periódica[41]», los requisitos mínimos

(40) Art. 5 RDENS.

(41) Art. 9 RDENS.

relativos a «organización e implantación del proceso de seguridad[42]», «mejora continua del proceso de seguridad[43]»; la «mejora continua del proceso de seguridad» y la «actualización permanente[44]».

(42)Art.12 RDENS.

(43)Art. 26 RDENS.

(44)Art. 42 RDENS.

Pese a que el plazo establecido en los esquemas ya ha sido superado con creces, lo cierto es que muchas administraciones públicas se encuentran en este momento en fases muy embrionarias de la implantación de un sistema de gestión de la seguridad de la información (SGSI).

Con anterioridad a la aprobación del ENS, las administraciones públicas podían utilizar como guía para la consecución del SGSI las recomendaciones y requisitos establecidos en la norma UNE ISO/IEC 27001:2007, cuyo anexo A enumera los controles que desarrolla la norma ISO 27002, que deben examinarse de manera complementaria.

La publicación del ENS supone que todas las administraciones públicas están obligadas a cumplir estrictamente con los requisitos mínimos y principios básicos en él incluidos, a diferencia de las normas ISO, que son de aplicación voluntaria. No obstante, las normas ISO prevén una visión integrada del sistema de gestión de la seguridad de la información que se concreta en la aplicación de un modelo de mejora continua de tipo PDCA (*plan*, *check*, *do*, *act*), que no aparece recogido en el ENS, y que puede resultar muy útil a las administraciones públicas para materializar su implantación.

Obviamente, a aquellas organizaciones que hayan iniciado el camino de la ISO 27001 o, incluso, se encuentren certificadas, les será más fácil poder alcanzar los objetivos del ENS, ya que las medidas de protección que se señalan en la norma internacional se recogen, en lo sustancial, en el Real Decreto.

Lo interesante para establecer una hoja de ruta realista de cara a implantar un SGSI es encajar las diferentes fases del ciclo PDCA con las fases establecidas para conseguir el cumplimiento integral del ENS. En este sentido (Aquilino, Renato y otros, 2013):

1) Fase *plan* (planificar): en esta fase, se establecen los objetivos y procesos necesarios para alcanzar el resultado esperado. Por tanto, se deberán establecer la política, los objetivos, procesos y procedimientos de los sistemas de gestión de la seguridad de la información, con la finalidad de obtener resultados alineados con las políticas y objetivos generales de la organización. Por tanto, esta fase *plan* se identifica con la elaboración del Plan de adecuación exigido en el ENS, y también con la determinación de la declaración de aplicabilidad.

2) Fase *do* (hacer): una vez elaborado y aprobado por el órgano competente el Plan de adecuación, junto con la declaración de aplicabilidad, se deberán implementar en esta fase la política, los controles, los procesos y procedimientos del sistema de gestión de seguridad. Por tanto, se deberán aplicar a todos los

sistemas de información de la organización que estén dentro del ámbito de aplicación del ENS, las medidas de seguridad necesarias en función de la categorización de estos sistemas y lo establecido en la declaración de aplicabilidad.

Como soporte en esta tarea de aplicación de las medidas de seguridad, se dispone de la guía CCN-STIC 804 de ayuda para la implantación de las medidas de seguridad exigidas por el ENS.

Finalmente, en esta fase se deberán implementar planes de formación y concienciación al personal de la organización.

3) Fase *check* (verificar): en esta fase hay que ejecutar procedimientos de supervisión y revisión del sistema de gestión. En otras palabras, se da cumplimiento aquí al principio de reevaluación periódica de la seguridad, comprobando que las medidas de seguridad sean las adecuadas y actualizándolas en caso necesario, para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección, llegando incluso a un replanteamiento de la seguridad, si fuera necesario.

Para este cometido, se dispone de la guía 815 de métricas e indicadores en las ENS. La tarea más determinante de esta fase es la realización de auditorías[45]. El ENS dispone la obligatoriedad de llevar a cabo auditorías ordinarias de los sistemas de información que se encuentran bajo su ámbito de aplicación para la verificación del cumplimiento de los requerimientos de seguridad recogidos en su articulado. Estas auditorías ordinarias se llevarán a cabo «al menos» cada dos años y será obligatoria para los sistemas y servicios cuya categoría sea de nivel medio o alto (en caso de nivel bajo, se precisa únicamente una autoevaluación).

(45)Art. 34 ENS.

Por otro lado, se harán auditorías con carácter extraordinario siempre que se produzcan modificaciones sustanciales en el sistema de información, que puedan repercutir en las medidas de seguridad requeridas.

La auditoría deberá ser llevada a cabo por personal cualificado e independiente del sistema o servicio que se está auditando.

Como medio de apoyo para hacer la auditoría, existe la guía CCN-STIC 802 de auditoría del esquema nacional de seguridad, que se completa con la guía CCN-STIC-808 de verificación del cumplimiento de las medidas del ENS.

De la misma manera, periódicamente se deberán revisar también las evaluaciones de riesgos y se tendrán que actualizar los planes de seguridad.

4) Fase *act* (actuar): en esta fase, se han de producir las tareas de mantenimiento y mejora del sistema de gestión, donde la función básica es aplicar en el sistema de gestión las medidas correctivas identificadas en el proceso de auditoría.

Llegados a esta última fase de *act*, y dado que se trata de ciclo de mejora continua, deberíamos volver a enlazar esta fase con la de *plan*, y así revisar de nuevo el sistema de manera que la seguridad esté evaluada periódicamente y de manera continua.

5) Declaración de conformidad al ENS. Una vez se ha implantado integralmente el ENS, habrá que publicar la declaración de conformidad[46]. Se trata de una declaración por escrito con la cual las administraciones públicas han de dar publicidad a la conformidad de sus sistemas a las disposiciones del ENS en sus sedes electrónicas, en un lugar de fácil acceso.

(46)Capítulo VIII del RDENS.

La guía CCN-STIC-809 concreta las pautas para la elaboración de una declaración de conformidad del ENS.

La declaración seguirá la siguiente estructura: la identificación del declarante, el contenido de la declaración y a partir de qué se declara la conformidad y con qué finalidad.

Actualmente, existen herramientas que permiten hacer un seguimiento de cada una de las fases indicadas y generar los informes y documentos requeridos por el ENS (declaración de aplicabilidad, declaración de conformidad, etc.). Son aplicaciones informáticas que, a diferencia de las herramientas ofrecidas por el Ministerio (PILAR o MAGERIT), que solo permiten hacer el análisis de riesgos, ofrecen una solución integral para la implantación de un SGSI.

Superadas las fases de implantación del ENS, lo que procede es dar publicidad, en las correspondientes sedes electrónicas, a la conformidad de los sistemas respecto al cumplimiento del ENS, tal y como se establece en anexo I del Real Decreto, que implica adoptar y manifestar que se han implementado las medidas de seguridad requeridas, atendiendo a la clasificación previa de los sistemas en categoría básica, media o alta, asegurando que tales medidas se mantienen a lo largo de todo el ciclo de vida del sistema.

Además será necesario someterse a las auditorías preceptivas que, de manera ordinaria, hay que llevar a cabo cada dos años para los sistemas de categoría media y alta (anexo I del ENS), y con carácter extraordinario, siempre que se produzcan modificaciones sustanciales en el sistema de información.

El anexo III del ENS precisa el alcance de la verificación estableciendo dos procedimientos que se resumen en el cuadro siguiente:

Procedimiento de verificación	Categoría de los sistemas afectados	Manifestación de conformidad	Resultado de la verificación	Análisis de la verificación
Autoevaluación: efectuada por el mismo personal que administra el sistema de información o aquel otro en quien hubiere delegado.	**Básica**	**Declaración de conformidad**	**Documento de autoevaluación**: indicando si cada medida de seguridad está implantada y sujeta a revisión regular y las evidencias que sustentan la valoración anterior.	Los documentos de autoevaluación serán analizados por el responsable de seguridad competente, que elevará las conclusiones al responsable del sistema para que adopte las medidas correctoras adecuadas.
Auditoría formal: con las garantías metodológicas y de independencia, profesionalidad y adecuación requeridas.	**Media / Alta**	**Certificación de conformidad**	**Informe de auditoría**: dictaminando sobre el grado de cumplimiento con el ENS, identificando sus deficiencias y sugiriendo, en su caso, posibles medidas correctoras o complementarias y las recomendaciones que se consideren oportunas. Deberá incluir o referenciar los criterios metodológicos de auditoría utilizados, el alcance y el objetivo de la auditoría y los datos, hechos y observaciones en los que se basen las conclusiones formuladas.	Los informes de auditoría serán analizados por el responsable de seguridad competente, que presentará sus conclusiones al responsable del sistema para que adopte las medidas correctoras adecuadas.

Fuente: *Guía de seguridad* (CCN-STIC-809).

4. Organización de la seguridad

De la lectura del ENS se desprende, claramente, que uno de los elementos estratégicos para conseguir implantar un sistema de gestión de la seguridad de la información es la necesidad de identificar a los responsables de velar por el cumplimiento de lo establecido en la política de seguridad aprobada por cada entidad, y que deberá ser conocida por todos los miembros de la organización.

En concreto, el artículo 10 del ENS resalta la función diferenciada de la seguridad que deberá recaer en el responsable de la información, el responsable del servicio y el responsable de la seguridad.

Aunque es responsabilidad de cada entidad establecer su propia organización de la seguridad, es importante tener en cuenta lo establecido en la Guía CCN-STIC 801 como marco de referencia en el que se recuerdan las responsabilidades generales en la gestión de la seguridad de los sistemas de información, proponiendo «figuras» o «roles» de seguridad que puedan asumir dichas responsabilidades. Sin embargo, esta división de responsabilidades enunciada en la guía es solo una recomendación, que cada organización debe encajar de la mejor manera posible en su estructura, siendo únicamente preceptivo lo que se encarga el propio ENS de recordar:

«La necesaria diferenciación entre la responsabilidad de la seguridad de los sistemas de información y la prestación de los servicios.»

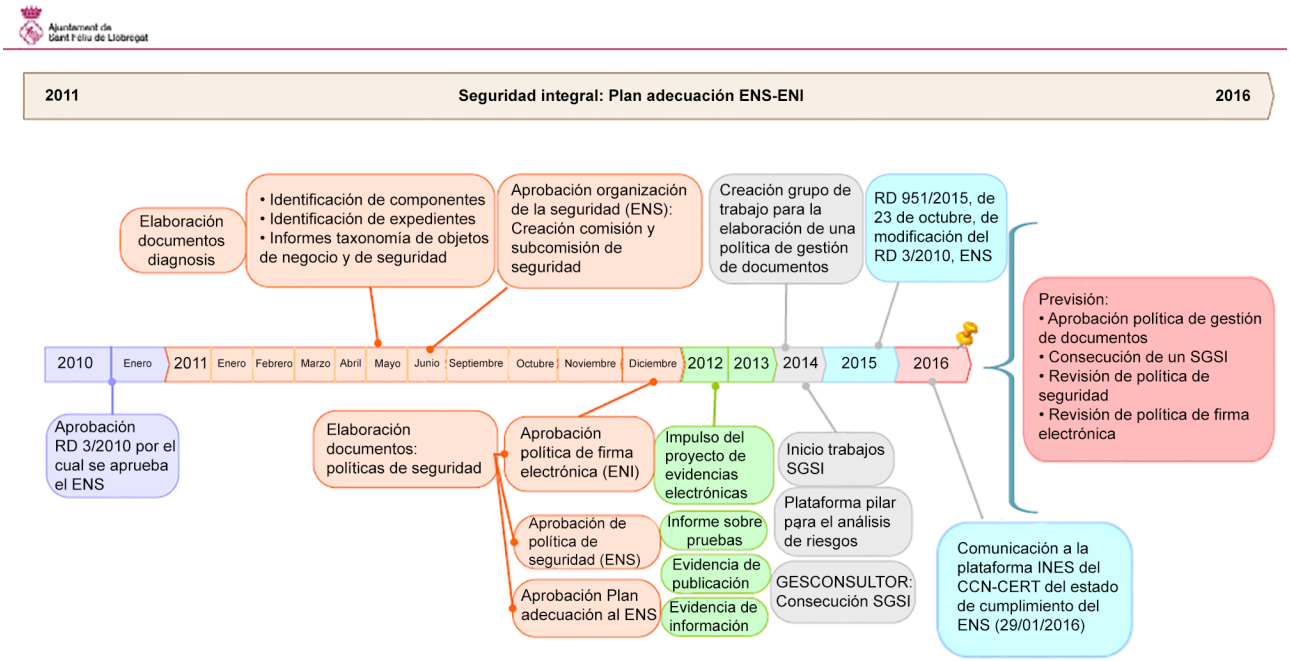
Será en la política de seguridad de cada organización donde deberán detallarse las atribuciones de cada responsable y cuáles son los mecanismos de coordinación y de resolución de conflictos.

Sin embargo, si el objetivo es tratar la seguridad como un proceso transversal e integral, parece razonable que la organización de la seguridad se plantee también desde una doble perspectiva: la seguridad de los sistemas de información y de los datos que se gestionan, es decir, las responsabilidades derivadas del cumplimiento del ENS y también las derivadas del cumplimiento de la normativa sobre protección de datos personales.

Existen distintas fórmulas de organización de la seguridad. Un buena práctica la podemos encontrar en el Ayuntamiento de Sant Feliu de Llobregat, donde se optó por una organización de la seguridad estructurada en dos órganos colegiados, la Comisión y la Subcomisión de Seguridad, que asumen los roles y las funciones de organización de la seguridad establecidos en el ENS, excepto el rol de administrador de seguridad del sistema, que recae en el responsable de la unidad de Informática.

La Comisión de Seguridad es un órgano de carácter más institucional, integrado por miembros del equipo de Gobierno y dirección, que además de ejercer las funciones exigidas por el ENS, asume también las funciones de responsable de fichero que se indican en el documento de seguridad en materia LOPD.

La adecuación a los esquemas del Ayuntamiento de Sant Feliu de Llobregat dibujada en el tiempo



5. La protección de los datos personales

Las administraciones públicas en el desarrollo de sus funciones recaban datos personales de la ciudadanía. En efecto, al solicitar una subvención o pagar impuestos a través de un formulario electrónico, más allá de poner en contacto a una persona con la Administración pública a través de medios electrónicos, se ponen en circulación datos personales como son el nombre y apellidos, la dirección, el número del documento de identidad o el de la cuenta corriente. Más allá de los problemas de seguridad que se puedan derivar de la circulación de estos datos, los medios electrónicos permiten acceder y agregar datos personales que, si bien en sí mismos pueden tener escaso valor, facilitan un perfil de la persona afectada que puede ser codiciado por otros sujetos. Además, todo esto puede suceder sin que la persona afectada tenga conocimiento y sin dejar ningún rastro que le permita controlar ni sus datos personales ni el uso que de ellos puedan hacer terceras personas.

De este modo, la Administración electrónica puede generar amenazas para la privacidad de las personas y poner en riesgo sus datos personales. Para hacer frente a las posibles amenazas y riesgos, se han adoptado diferentes normas y se han impulsado distintos mecanismos que persiguen regular el tratamiento de datos personales, garantizar su seguridad y asegurar su cumplimiento.

Como pone de manifiesto el documento elaborado por el grupo de trabajo sobre protección de datos del artículo 29, el éxito de algunos de los proyectos de Administración electrónica depende de complejas cuestiones relacionadas con la protección de datos a los que se debe prestar la atención adecuada[47].

(47)Ver http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2003/e-government_es.pdf (fecha de consulta: marzo del 2016).

5.1. El derecho a la protección de los datos personales. Evolución de los riesgos y evolución de la legislación

El derecho a la protección de los datos personales no tiene un reconocimiento explícito en la Constitución. Sin embargo, el Tribunal Constitucional ha afirmado que existe un derecho a la autodeterminación informativa o una libertad informática a partir de lo previsto en el art.18.4 CE, que establece que:

> «La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.»

Según el Tribunal Constitucional en su sentencia 253/1993, de 20 de julio:

> «En efecto, ha de tenerse presente, como ya se anticipaba en la decisión de este Tribunal que se acaba de mencionar, que el derecho fundamental al que estamos haciendo referencia garantiza a la persona un poder de control y disposición sobre sus datos personales. Pues confiere a su titular un haz de facultades que son elementos esenciales del derecho fundamental a la protección de los datos personales, integrado por los derechos que corresponden al afectado a consentir la recogida y el uso de sus datos personales y a conocer los mismos. Y para hacer efectivo ese contenido, el derecho a ser informado de quién posee sus datos personales y con qué finalidad, así como el derecho a oponerse a esta posesión y uso exigiendo a quien corresponda que ponga fin a la posesión y empleo de tales datos.»

La existencia del derecho a la protección de datos personales supone el reconocimiento de diferentes facultades como la de obtener el consentimiento informado para el tratamiento de los datos personales; el derecho a conocer la existencia de ficheros en los que se incluyen datos personales o los derechos de acceso, rectificación, cancelación y oposición.

Junto a este derecho, la Constitución reconoce, en su art. 18.1, el derecho a la intimidad que implica la existencia de un ámbito propio y reservado frente a la acción y el conocimiento de los otros, necesario para mantener una calidad mínima de la vida humana.

La jurisprudencia del Tribunal Constitucional ha ido delimitando el contenido de este derecho con respecto al previsto en el art.18.4 CE. Al respecto, es sumamente clara la sentencia 252/2000, de 30 de noviembre en la que se afirma que:

> «La función del derecho fundamental a la intimidad del art. 18.1 CE es la de proteger frente a cualquier invasión que pueda hacerse en aquel ámbito de la vida personal y familiar que la persona desea excluir del conocimiento ajeno y de las intromisiones de terceros en contra de su voluntad (por todas STC 144/1999, de 22 de julio, FJ 8). En cambio, el derecho fundamental a la protección de datos persigue garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado. En fin, el derecho a la intimidad permite excluir ciertos datos de una persona del conocimiento ajeno, por esta razón, y así lo ha dicho este Tribunal (SSTC 134/1999, de 15 de julio, FJ 5; 144/1999, FJ 8; 98/2000, de 10 de abril, FJ 5; 115/2000, de 10 de mayo, FJ 4), es decir, el poder de resguardar su vida privada de una publicidad no querida. El derecho a la protección de datos garantiza a los individuos un poder de disposición sobre esos datos.»

Así pues, tanto el objeto de los derechos como su contenido son distintos. En primer lugar, por lo que se refiere al objeto de ambos derechos, el derecho a la protección de los datos personales es más amplio que el derecho a la intimidad, puesto que no se limita a los datos íntimos de las personas sino que extiende la garantía a cualquier tipo de datos, sean íntimos o no, cuyo conocimiento por terceros pueda afectar a los derechos de la persona. En segundo lugar, por lo que respecta al contenido de los derechos, el derecho a la intimidad impone a las terceras personas el deber de abstenerse de toda intromisión en la esfera íntima de la persona y la prohibición de usar lo que haya sido conocido a través de esta intromisión. En cambio, el derecho a la protección de los datos personales atribuye a su titular un conjunto de facultades consistente en diferentes poderes jurídicos cuyo ejercicio impone a terceros deberes jurídicos, que sirven para garantizar a la persona un poder sobre sus datos personales.

La regulación de la protección de los datos personales tiene una relativamente corta aunque extensa historia. En primera instancia, cabe referirse al Convenio 108 del Consejo de Europa, de 28 de enero de 1981, de protección de las personas en relación con el tratamiento automatizado de los datos de carácter personal, cuyo objetivo era asegurar en el territorio de los estados firmantes que cada individuo, de manera independiente de su nacionalidad o residencia, viese respetado su derecho a la privacidad en el proceso automatizado de tratamiento de sus datos personales.

Para dar desarrollo a lo previsto en el art. 18.4 CE y en el marco del Convenio del Consejo de Europa, se adoptó la Ley orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal.

Posteriormente, la Directiva 95/46/CE, del Parlamento Europeo y del Consejo, de 24 de octubre, relativa a la protección de las personas físicas y la Directiva 2002/58/CE, del Parlamento Europeo y del Consejo, de 12 de julio, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas fijaron el marco común europeo en este ámbito.

Las normas europeas han sido incorporadas en nuestro ordenamiento jurídico a través de la Ley orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (LOPD), el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo y, en determinados aspectos, por la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información así como en otras normas en materia de telecomunicaciones. Asimismo, tres Comunidades Autónomas tienen en vigor normas con relación a la creación y gestión de los ficheros de datos personales por las administraciones públicas autonómicas o la creación de órganos autonómicos de garantía del derecho a la protección de datos (Andalucía, Cataluña y País Vasco).

Desde el punto de vista de la Administración electrónica, la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos reconoció el principio respecto al derecho a la protección de datos de carácter personal en el uso de los medios electrónicos y el derecho a la garantía de la seguridad y confidencialidad de los datos que figuren en ficheros. Asimismo, se previeron diferentes usos de los medios electrónicos con impacto en los datos personales como la transmisión de datos entre administraciones públicas, el intercambio electrónico de datos o el archivo de datos. En la actualidad, estos aspectos están regulados en la LPACAP y la LRJPS, como se expondrá en las próximas páginas.

Asimismo, debe tenerse en cuenta el Real Decreto 3/2010, de 8 de enero, por el que se aprueba el esquema nacional de seguridad.

Además de estas normas, hay que tener presente que algunas entidades públicas han adoptado códigos de conducta. La LOPD prevé la posibilidad de formular códigos tipos a los responsables de los ficheros, a través de acuerdos sectoriales, convenios administrativos o mediante decisiones de empresa, que establezcan las condiciones de organización, régimen de funcionamiento, procedimientos aplicables, normas de seguridad del entorno, programas o equipos, obligaciones de los implicados en el tratamiento y uso de la información personal. Estos códigos de conducta deben ser depositados e inscritos en el Registro General de Protección de Datos o en el registro autonómico correspondiente que dará traslado al registro para su inclusión en el registro gestionado por la AEPD.

Como ejemplo, se puede traer a colación el manual de buenas prácticas promovido por la Asociación de Municipios Vascos (EUDEL), que tiene por objeto regular el tratamiento de los datos de carácter personal que llevan a cabo las entidades locales, los organismos autónomos dependientes de ellas, así como de las sociedades dependientes o vinculadas a las mismas cuando su capital sea de mayoría pública y ejerzan potestades públicas, existentes en la Comunidad Autónoma del País Vasco.

Finamente, debe ponerse de relieve que en breve, el Reglamento europeo de protección de datos unificará y modernizará la regulación europea de la protección de datos y dará respuesta a los nuevos retos generados en los últimos años. El Reglamento europeo también apostará por la privacidad desde el diseño, las evaluaciones de impacto o la figura del *data protection officer* (DPO).

5.2. Los datos personales: concepto y derechos de las personas

Los datos personales son cualquier información concerniente a una persona física identificada o identificable, es decir, cuya identidad pueda determinarse, directamente o indirectamente, en particular, a través de un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social. Algunos datos personales son considerados sensibles y cuentan con una protección legal más elevada, tal y como se podrá observar a lo largo de las próximas páginas (por ejemplo, los datos relativos a la ideología, la afiliación sindical, la religión, el origen racial o étnico, la salud o la vida sexual).

De este modo, un dato personal no solo es una información numérica o alfanumérica sino que también tienen esta consideración las imágenes, la voz, las huellas digitales o los datos biométricos en la medida en se refieran a una persona física, siempre y cuando no se requieran plazos o actividades desproporcionadas. Asimismo, algunos datos estrechamente relacionados con la Administración electrónica, como la dirección del correo electrónico o la dirección IP, se deben considerar como datos personales siempre y cuando pueda haber una vinculación entre ellos y una persona concreta. En particular, en relación con la dirección IP, la Agencia Española de Protección de Datos[48] ha considerado que:

(48)Informe 327/03.

«Así pues, aunque no siempre sea posible para todos los agentes de Internet identificar a un usuario a partir de datos tratados en la Red, desde esta Agencia de Protección de Datos se parte de la idea de que la posibilidad de identificar a un usuario de Internet existe en muchos casos y, por lo tanto, las direcciones IP tanto fijas como dinámicas, con independencia del tipo de acceso, se consideran datos de carácter personal resultando de aplicación de la normativa sobre protección de datos.»

La LOPD no es aplicable a los datos referidos a personas jurídicas. Sin embargo, si los datos referidos a una persona jurídica pueden ser atribuibles a una persona física concreta, tienen la consideración de datos personales. Tampoco es de aplicación a las personas fallecidas.

En términos generales, cuando una Administración pública solicite datos a través de un formulario, solicitud, etc., se deberá informar al interesado de los siguientes extremos:

- Existencia de un fichero o tratamiento de datos de carácter personal.
- Finalidad del tratamiento de los datos.
- Destinatarios de la información.
- Datos que se solicitan y carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.
- Identidad y dirección del responsable del tratamiento de los datos.
- Consecuencias de la obtención de los datos o de la negativa de proporcionarlos.
- Posibilidad de ejercer los derechos de acceso, rectificación, cancelación y oposición.

Las administraciones públicas deben informar de manera claramente legible de los extremos anteriores en las páginas web, formularios o impresos que utilicen para la recogida de los datos personales.

Aviso legal

«El Ayuntamiento de Sant Feliu de Llobregat da estricto cumplimiento a la normativa vigente sobre protección de datos de carácter personal (LOPD) y la Ley de servicios de la sociedad de la información y correo electrónico (LSSICE). El usuario de la web da su consentimiento expreso e inequívoco y, por tanto, autoriza a incorporar los datos que facilita a los ficheros responsabilidad del Ayuntamiento de Sant Feliu de Llobregat y registrados en la Agencia Catalana de Protección de Datos. El uso de los datos personales tendrá carácter confidencial y se utilizarán únicamente para poder prestar los servicios del Ayuntamiento de Sant Feliu de Llobregat.

Usted podrá revocar el consentimiento otorgado en cualquier momento, así como ejercitar sus derechos de acceso, rectificación, cancelación y oposición, en los términos establecidos en la legislación vigente, dirigiendo un escrito al Ayuntamiento de Sant Feliu de Llobregat o enviando un correo electrónico a lopd@santfeliu.cat.»

https://www.santfeliu.cat/common/misc/widget_container.faces?xmid=11796 (fecha de consulta: marzo del 2016).

En el caso de que los datos no sean recabados del propio interesado, las administraciones públicas, como responsable del fichero, también deben informarle de forma expresa, precisa e inequívoca, dentro de los tres meses siguientes al momento del registro de los datos de la procedencia de los datos y de la existencia de un fichero, de la finalidad de la recogida de los datos, de los

destinatarios de la información, de la posibilidad de ejercitar los derechos y de la identidad y dirección del responsable del tratamiento; excepto que el tratamiento de los datos tenga finalidades históricas, estadísticas o científicas, sea imposible informar al interesado o exija esfuerzos desproporcionados.

Además de este derecho a ser informado sobre la recogida de datos, las personas tienen reconocidos por la LOPD otros derechos conocidos como derechos ARCO:

- **Derecho de acceso**. Todo interesado tiene derecho a solicitar y obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento, la finalidad del tratamiento que, en su caso, se esté efectuando, el origen y las comunicaciones llevadas a cabo o que se prevé hacer con ellos. Este derecho no debe confundirse con el derecho de acceso a la información pública, al que se hará referencia al hablar del Gobierno abierto.

- **Derecho de rectificación y cancelación**. Los interesados tienen derecho a que sus datos personales que sean inexactos o incompletos sean rectificados. Asimismo, tienen derecho a que los datos que resulten inadecuados o excesivos sean suprimidos.

- **Derecho de oposición**. Los interesados tienen derecho a que no se lleve a cabo el tratamiento de sus datos personales o que se cese en el que se esté haciendo en los supuestos previstos en la normativa. Por un lado, el interesado tiene derecho a oponerse al tratamiento de sus datos recabados sin su consentimiento cuando existan motivos fundados y legítimos relativos a una concreta situación personal en los supuestos en los que no sea necesario el consentimiento del afectado para el tratamiento de los datos de carácter personal, siempre que una ley no disponga lo contrario. Por otro lado, el interesado puede oponerse, previa petición y sin gastos, al tratamiento de los datos que le conciernan que formen parte de un listado elaborado con fines de publicidad y de prospección comercial obtenido de una fuente accesible al público. Finalmente, el interesado también tiene derecho a oponerse cuando el tratamiento tenga por finalidad la adopción de una decisión referida a él y basada únicamente en un tratamiento automatizado de sus datos.

En el caso de los datos incluidos en ficheros de titularidad pública, los derechos anteriores tienen algunas excepciones que en caso de ser aplicadas, deberá motivarse adecuadamente. Así, por ejemplo, la LOPD establece que los responsables de los ficheros pueden denegar el derecho de acceso, rectificación o cancelación en función de los peligros que se puedan derivar 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 llevando a cabo

o cuando su ejercicio obstaculice las actuaciones administrativas tendentes a asegurar el cumplimiento de las obligaciones tributarias y, en todo caso, cuando el afectado esté siendo objeto de actuaciones inspectoras.

Estos derechos son ejercitables dirigiendo una comunicación a la Administración pública responsable del fichero en la que se identifique al interesado, se recoja la petición en que se concreta la solicitud y se indique una dirección a efectos de notificación. El procedimiento para el ejercicio de los derechos debe ser sencillo, gratuito y ágil[49].

(49)1 mes en el caso del ejercicio del derecho de acceso y 10 días en el del ejercicio de los derechos de rectificación, cancelación y oposición.

Las agencias de protección de datos son competentes respecto a la tutela de los derechos anteriores y, en general, para resolver las reclamaciones que puedan interponer los interesados con relación a las actuaciones contrarias a lo dispuesto en la LOPD.

5.3. Los usos de datos personales por las administraciones públicas

El uso de datos personales por las administraciones públicas supone llevar a cabo un tratamiento, es decir, una operación o procedimiento técnico de carácter automatizado o no, que permite la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.

Lecturas recomendadas

M. Fernández (2003). *La protección de los datos personales en las administraciones públicas*. Madrid: Civitas-Agencia de Protección de Datos de la Comunidad de Madrid.

A. Troncoso (2008). «La administración electrónica y la protección de datos personales». *Revista Jurídica de Castilla y León*.

La LOPD establece una serie de principios que deben guiar cualquier tratamiento de datos personales:

- **Calidad de los datos**: los datos personales deben ser adecuados, pertinentes y no excesivos respecto a la finalidad para la que se obtienen y que sean exactos y actualizados.

- **Consentimiento**: el tratamiento de los datos personales requiere el consentimiento inequívoco del interesado. Existen datos como los relativos a la ideología, la afiliación sindical, la religión o las creencias que tienen una protección reforzada y requieren un consentimiento expreso y por escrito. Otros datos como los que se refieren al origen racial, la salud o la vida sexual únicamente pueden ser recogidos, tratados y cedidos cuando, por razones de interés general, así lo establezca una ley o el afectado lo consienta expresamente. Sin embargo, el principio del consentimiento tiene algunas excepciones. En particular, la LOPD prevé que no será preciso el

consentimiento cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las administraciones públicas en el ámbito de sus competencias atribuidas por una norma con rango de ley o de derecho comunitario o cuando se refieran a las partes de una relación administrativa.

- **Seguridad de los datos**: tal y como establece el art. 9 LOPD, «[e]l responsable del fichero, y, en su caso, el encargado del tratamiento deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural».

- **Secreto en el tratamiento de los datos**: el responsable del fichero y del tratamiento están obligados al secreto profesional.

- **Congruencia y racionalidad en su utilización**: según el art. 11 LOPD, «los datos de carácter personal objeto del tratamiento solo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado», excepto en los caso previstos en la ley.

5.4. La creación de ficheros de datos personales por las administraciones públicas

Los ficheros son cualquier conjunto de organizado de datos de carácter personal.

La creación de ficheros de datos por las administraciones públicas exige la adopción de una disposición general publicada en el *Boletín Oficial del Estado* o en el diario oficial correspondiente. Esta disposición debe indicar los siguientes elementos:

- 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 se puedan ejercer los derechos de acceso, rectificación, cancelación y oposición.

- Las medidas de seguridad con indicación del nivel básico, medio o alto exigible.

La concreción de la finalidad tiene una relevancia significativa para determinar si se ha llevado a cabo un uso ilegítimo de los datos personales o han cedido más allá de lo previsto en la LOPD.

Solo se pueden crear, modificar o suprimir a través de una disposición general publicada en el BOE o en el diario oficial correspondiente. Una vez creado el fichero, la Administración pública o el organismo responsable deberá comunicarlo a la Agencia Española de Protección de Datos o a la autoridad autonómica competente para su inscripción en el Registro General de Protección de Datos.

5.5. La obtención de datos por las administraciones públicas

Los datos personales se pueden obtener a través de diferentes fuentes.

En primer lugar, los datos personales se pueden obtener de la persona que los facilita directamente o manifiesta su consentimiento expreso para que sean recogidos con una finalidad concreta, no genérica. El suministro de datos puede ser voluntario o fruto de una obligación legal. El consentimiento se manifiesta respecto a un tratamiento que tiene una finalidad concreta. No es un consentimiento abstracto, sino para uno o varios tratamientos concretos. El consentimiento ha de ser inequívoco a través de una manifestación de voluntad, libre, inequívoca e informada, mediante la que el interesado consiente el tratamiento de los datos personales que le conciernen. El consentimiento es revocable cuando haya una causa justificada, aunque no tiene efectos retroactivos. En determinados casos, este consentimiento es reforzado para tratar determinados datos que tienen un carácter especialmente sensible.

La LOPD prevé diversas excepciones a la necesidad de consentimiento. En primer lugar, cuando los datos personales se recojan para el ejercicio de las funciones propias de las administraciones públicas en el ámbito de sus competencias. En segundo lugar, cuando se refieran a las partes de un contrato o precontrato de una relación de negocios, laboral o administrativa y sean necesarias para su mantenimiento o cumplimiento. En tercer lugar, cuando el tratamiento tenga por finalidad proteger un interés vital del interesado. En cuarto lugar, cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comunican los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado.

Precisamente, la obtención de datos de fuentes diferentes al interesado puede ser a través de las fuentes accesibles al público como los diarios y boletines oficiales, los censos promocionales, los repertorios telefónicos o los listados profesionales o como resultado de la cesión de datos de sujetos diferentes al in-

teresado. En general, las fuentes accesibles al público son ficheros que pueden ser consultados por cualquier persona sin que lo impida una norma limitativa o sin otra exigencia que, en su caso, el abono de una contraprestación. A pesar de que los datos se obtengan de una fuente accesible al público, no se pueden someter a cualquier tipo de tratamiento. Es necesario que el tratamiento se haga para la satisfacción de un interés legítimo del responsable del fichero o del tercero al que se comuniquen los datos y que se cumpla la condición de no vulnerar los derechos y libertades fundamentales del afectado.

Finamente, para la cesión de datos es necesario que estos sirvan para el cumplimiento de finalidades directamente relacionadas con las funciones legítimas del cedente y cesionario y el previo consentimiento del interesado. No obstante, están previstas diferentes excepciones a la regla del consentimiento previo.

5.6. La cesión de datos entre administraciones públicas

La interconexión de las bases de datos de las administraciones públicas puede representar una ventaja significativa para las personas en sus relaciones con las administraciones públicas. En efecto, es frecuente que las administraciones públicas, en el desarrollo de su actividad, precisen de datos personales que están en poder de otra Administración pública. Asimismo, no podemos desconocer el derecho de las personas a no aportar documentos que hayan sido elaborados por cualquier Administración. De hecho, como se ha visto en el módulo anterior, las administraciones públicas se deben relacionar entre sí y con sus órganos, organismos públicos o entidades vinculadas o dependientes a través de medios electrónicos que deberán garantizar la protección de los datos de carácter personal.

Lectura recomendada

Cerrillo, A. (2009). «La interoperabilidad y la protección de datos. La conexión de los registros de protección de datos». En: VV. AA. *La protección de datos en la administración electrónica*. Cizur Menor: Thomson-Reuters-Aranzadi-Agencia Española de Protección de Datos.

Para poder conocer estos datos es necesario que se lleve a cabo una cesión o comunicación de datos, es decir, que se revelen datos personales a una persona distinta del interesado.

La LOPD prevé un régimen específico para la cesión de datos entre administraciones públicas que contempla la posibilidad de que las administraciones públicas puedan cederse datos personales entre sí sin el consentimiento del interesado cuando se trate del ejercicio de las mismas competencias o de competencias diferentes que versen sobre la misma materia. Tampoco será necesario el consentimiento, entre otras situaciones, cuando la Administración obtenga o elabore los datos personales con destino a otra. Esta supone una ampliación al estricto régimen de la cesión de datos previsto que exige en términos generales el consentimiento del interesado, estar autorizada por una ley o encontrarse en alguno de los supuestos previstos en la propia ley.

En este punto, la dificultad surge al interpretar el alcance de la previsión legal a los efectos de determinar los tratamientos incluidos. Al respecto se ha pronunciado el Tribunal Supremo en su sentencia de 15 de abril del 2002, al reconocer que:

> «La cesión o comunicación de los datos entre administraciones públicas, mientras se lleve a cabo, precisa y únicamente, para alcanzar el fin o uno de los fines a los que obedece la creación misma del fichero y la propia recogida de aquellos, y no, por tanto, para el ejercicio de competencias diferentes o de competencias que versen sobre materias distintas, queda ya amparada por el consentimiento inicialmente prestado por el titular de los datos para su recogida y tratamiento. Es decir, en tal caso, huelga la necesidad de un nuevo consentimiento cuyo objeto específico sea aquella cesión o comunicación.»

El intercambio de datos se puede producir de diferentes maneras desde el punto de vista tecnológico, como facilitar la información bajo petición, permitir el acceso directo a las bases de datos o crear repertorios comunes de datos y documentos disponibles en entornos cerrados de comunicación. Cada una de estas posibilidades entraña riesgos de diferente intensidad a los que se debe dar la oportuna solución desde el punto de vista de la seguridad de los datos personales.

Cuando el intercambio de datos personales se produce en entornos cerrados de comunicación, la LRJSP prevé que los documentos electrónicos transmitidos serán considerados válidos a efectos de autenticación e identificación de los emisores y receptores si se cumplen las condiciones y garantías que se fijen y, en particular, se identifiquen los emisores y receptores autorizados y la naturaleza de los datos que hay que intercambiar. Estas condiciones deben ser fijadas bien por la Administración pública a la que pertenezcan los distintos participantes en la comunicación de datos, bien mediante convenio suscrito entre las distintas administraciones públicas participantes.

En relación con esta cuestión, resulta de interés traer a colación el catálogo de datos y documentos electrónicos en el que se incluye una relación actualizada de datos y documentos que están en poder de la Administración de la Generalitat de Cataluña y de otras administraciones e instituciones públicas y que se pueden obtener por medios electrónicos, al que se refiere el Decreto 56/2009, de 7 de abril, para el impulso y el desarrollo de los medios electrónicos en la Administración de la Generalitat de Cataluña.

Cuando el intercambio de datos se produce a través del acceso de una Administración pública a los datos relativos a los interesados que obren en poder de otras, se deberán especificar las condiciones, protocolos y criterios funcionales o técnicos necesarios para acceder a dichos datos con las máximas garantías de seguridad, integridad y disponibilidad. La LRJSP prevé que los datos disponibles serán estrictamente aquellos que sean requeridos por las administraciones públicas para la tramitación y resolución de los procedimientos y actuaciones de su competencia. Para ello, la Administración general del Estado, las administraciones autonómicas y las entidades locales crearán una red de comunicaciones que interconecte los sistemas de información de las administraciones

públicas y permita el intercambio de información y servicios entre las mismas. Esta red también debe facilitar la interconexión con las redes de las instituciones europeas y de los estados miembros.

Aunque no está previsto explícitamente, es conveniente facilitar al interesado información sobre las cesiones de datos entre administraciones públicas, especialmente cuando estas se lleven a cabo sin su consentimiento, tal y como propuso el grupo del artículo 29 en su informe sobre la Administración electrónica.

5.7. La seguridad de los datos personales

El uso de datos personales por las administraciones públicas exige la implantación de las medidas de seguridad previstas en la LOPD.

Las medidas de seguridad deben impulsarse por los responsables de los ficheros y los encargados de tratamiento. En efecto, los responsables de los ficheros tienen la obligación de garantizar la seguridad y guardar el secreto profesional de los datos a los que tienen acceso. Para ello tienen el deber, junto con los responsables de tratamiento, de adoptar las medidas de índole técnica y organizativa necesarias para garantizar la seguridad de los datos de carácter personal y evitar su alteración, pérdida, tratamiento o acceso no autorizado, según el estado de la tecnología, la naturaleza de los datos y los riesgos a los que estén expuestos. A su vez, pueden nombrar a un responsable de seguridad que será la persona o personas a las que el responsable del fichero haya asignado formalmente la función de coordinar y controlar las medidas de seguridad aplicables.

Para garantizar la seguridad, no se registrarán datos de carácter personal en ficheros que no reúnan las condiciones determinadas reglamentariamente.

Las medidas de seguridad persiguen garantizar la confidencialidad (permitir el conocimiento de los datos solo por los usuarios autorizados), integridad (impedir la alteración de la información) y disponibilidad de los datos (de manera que la información sea utilizada por los usuarios autorizados).

El responsable del fichero y todos aquellos que intervengan en cualquier fase del tratamiento de los datos personales están obligados al secreto profesional respecto de los datos. También tienen el deber de guardarlos incluso después de finalizar sus relaciones con el titular del fichero.

En función de los datos personales, las medidas de seguridad que se deberán adoptar serán diferentes. En efecto, el reglamento de desarrollo de la LOPD prevé que las medidas de seguridad exigibles a los ficheros y tratamientos se clasifican en tres niveles: básico, medio y alto.

- **Nivel básico**: todos aquellos datos personales que no estén incluidos en otros niveles de seguridad

- **Nivel medio**: ficheros o tratamientos de datos relativos a la comisión de infracciones administrativas; que sean responsables administraciones tributarias y se relacionen con el ejercicio de sus potestades tributarias; que sean responsables las entidades gestoras y servicios comunes de la Seguridad Social y se relacionen con el ejercicio de sus competencias; 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.

- **Nivel alto**: ficheros o tratamientos de datos de carácter personal que se refieran a datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual; que contengan o se refieran a datos recabados para fines policiales sin consentimiento de las personas afectadas; o que contengan datos derivados de actos de violencia de género.

En función del nivel, la normativa de desarrollo de la LOPD fija las medidas de seguridad que se deben adoptar en función del nivel de los ficheros o tratamientos de datos. Asimismo, es necesario tener en cuenta las medidas de seguridad que deban adoptar las administraciones públicas en aplicación de lo previsto en el Real Decreto 3/2010, de 8 de enero, por el que se aprueba el esquema nacional de seguridad.

Finalmente, es importante destacar que las administraciones públicas deben informar a los interesados de las medidas de seguridad adoptadas.

Aviso legal

La sede electrónica del Ayuntamiento de Vigo mantiene los niveles de protección de sus datos personales conforme a lo previsto en el Reglamento de desarrollo de la Ley orgánica 15/1999, y ha establecido todos los medios técnicos a su alcance para evitar la pérdida, mal uso, alteración, acceso no autorizado y robo de los datos que facilite a la sede electrónica del Ayuntamiento de Vigo.

https://sede.vigo.org/expedientes/sede_textos/texto.jsp?idt=sede_lopd&lang=cas (fecha de consulta: marzo del 2016).

5.8. El uso de *cookies* por las administraciones públicas

Las administraciones públicas generalmente usan en sus páginas web *cookies*, unos archivos que se depositan en el ordenador o dispositivo del usuario con el fin de conservar datos relativos a sus preferencias de navegación, recopilar información estadística o mejorar su experiencia de navegación. Con frecuencia, las *cookies* también se utilizan con fines publicitarios para mostrar al usuario publicidad basada en sus intereses o en sus hábitos de navegación.

El uso de *cookies* por las administraciones públicas puede tener un impacto en la privacidad de las personas. Por ello, desde diferentes instancias se ha llamado la atención sobre la necesidad de articular medidas con el fin de informar de manera clara y completa al usuario sobre la utilización de *cookies* y de recabar su consentimiento antes de instalarlas en su ordenador para asegurar que es consciente del uso de sus datos y las finalidades para las que son utilizados.

De este modo, cuando las administraciones públicas utilicen *cookies* deben:

- Informar al usuario sobre la utilización de *cookies* de manera clara y completa y sobre las finalidades del tratamiento de los datos que se recogen con las *cookies*. El usuario debe poder decidir si acepta o no el uso de estos archivos.

- Obtener el consentimiento del usuario para depositar las *cookies* y para leer las *cookies* depositadas. El consentimiento debe ser informado habiendo facilitado previamente al usuario toda la información sobre el uso de las *cookies*. El consentimiento se debe obtener antes de depositar o leer las *cookies*.

- Permitir al usuario revocar el consentimiento.

Lectura recomendada

Resulta de interés la consulta de la guía sobre el uso de las *cookies* impulsada por la Agencia Española de Protección de Datos. Accesible en: https://goo.gl/OJzAvA (fecha de consulta: marzo del 2016).

Las administraciones públicas deben informar de su política de *cookies*. Generalmente, las páginas web incluyen un enlace a un aviso legal específico en el que se informa sobre las *cookies* (funciones, tipos de *cookies* que utiliza la página web y su finalidad, propias o de terceros; técnicas de personalización, de análisis o de publicidad; forma de desactivar o eliminar las *cookies*, usuarios de las *cookies*; información obtenida a través de las *cookies*).

Política de *cookies*

El Ayuntamiento de Madrid informa acerca del uso de las *cookies* en su páginas web[50].

«Las *cookies* son archivos que se pueden descargar en su equipo a través de las páginas web. Son herramientas que tienen un papel esencial para la prestación de numerosos servicios de la sociedad de la información. Entre otros, permiten a una página web almacenar y recuperar información sobre los hábitos de navegación de un usuario o de su equipo y, dependiendo de la información obtenida, se pueden utilizar para reconocer al usuario y mejorar el servicio ofrecido.

Según cuál sea la entidad que gestione el dominio desde donde se envían las *cookies* y trate los datos que se obtengan, se pueden distinguir dos tipos: *cookies* propias y *cookies* de terceros.

Existe también una segunda clasificación según el plazo de tiempo que permanecen almacenadas en el navegador del cliente, pudiendo tratarse de *cookies* de sesión o *cookies* persistentes.

Por último, existe otra clasificación con cinco tipos de *cookies* según la finalidad para la que se traten los datos obtenidos: *cookies* técnicas, *cookies* de personalización, *cookies* de análisis, *cookies* publicitarias y *cookies* de publicidad comportamental.

Para más información a este respecto, podéis consultar la guía sobre el uso de las *cookies* de la Agencia Española de Protección de Datos.

(50)Véase http://www.madrid.es/portales/munimadrid/avisoLegal.html (fecha de consulta: marzo del 2016).

***Cookies* utilizadas en la Web del Ayuntamiento**

A continuación, se identifican las *cookies* que están siendo utilizadas en este portal y en la sede electrónica, así como su tipología y función.

La página web del Ayuntamiento de Madrid utiliza Google Analytics, un servicio de analítica web desarrollado por Google, que permite la medición y análisis de la navegación en las páginas web. En vuestro navegador, podréis observar varias *cookies* de este servicio que, según la tipología anterior, se trata de *cookies* propias, de sesión y de análisis. Podéis encontrar más información al respecto e inhabilitar el uso de estas *cookies* en esta página.

A través de la analítica web, se obtiene información relativa al número de usuarios que acceden a la web, el número de páginas vistas, la frecuencia y repetición de las visitas, su duración, el navegador utilizado, el operador que presta el servicio, el idioma, el terminal que utiliza o la ciudad a la que está asignada la dirección IP, información que posibilita un mejor y más apropiado servicio por parte de este portal web.

Otras *cookies* que se descargan son *cookies* de tipo técnico denominadas JSESSIONID y sdc.munimadrid.es y que permiten almacenar un identificador único por sesión a través del cual es posible vincular datos necesarios para posibilitar la navegación en curso y obtener estadísticas completamente anónimas de uso. Para usuarios registrados se utiliza, además, una *cookie* persistente miMadridLastVisited para almacenar las últimas páginas vistas y facilitar la personalización y navegación del usuario en el área personalizada de «Mi Madrid».

Por último, se descarga una *cookie* de tipo técnico denominada MadridCookiesPolicy, propia, de tipo técnico y con tiempo de expiración de un año. Esta *cookie* gestiona el consentimiento del usuario para el uso de las *cookies* en la página web, con el objeto de diferenciar los usuarios que las hayan aceptado, de modo no se les muestre información en la parte inferior de la página al respecto.

Aceptación de la política de *cookies*

El Ayuntamiento asume que aceptáis el uso de *cookies* al continuar navegando o cerrar expresamente el aviso de *cookies*. Esta información sobre la política de *cookies* está accesible tanto desde el aviso de la parte inferior que se muestra para usuarios que todavía no la han aceptado, como en la parte inferior del pie de cualquier página del portal en el enlace de aviso legal.

Ante esta información, es posible llevar a cabo las siguientes acciones:

- **Aceptar *cookies* o continuar navegando**. No se volverá a visualizar este aviso al acceder a cualquier página del portal durante la presente sesión y cualquier sesión con el mismo navegador efectuada durante un año.
- **Cerrar**. Se oculta el aviso de la página actual.
- **Más información**. Podréis obtener más información sobre qué son las *cookies*, conocer la política de *cookies* del Ayuntamiento y modificar la configuración del navegador.

Cómo modificar la configuración de las *cookies*

Podéis restringir, bloquear o borrar las *cookies* del Ayuntamiento o cualquier otra página web utilizando su navegador. En cada navegador la operativa es diferente. En los siguientes enlaces, podéis obtener instrucciones de cómo hacerlo.»

No todas las *cookies* exigen el cumplimiento de lo anterior. El grupo de trabajo del artículo 29 ha interpretado que no será necesario en relación con las *cookies* de entrada del usuario; de autenticación o identificación de usuario; de seguridad del usuario; de reproductor multimedia; de sesión para equilibrar la carga; de personalización de la interfaz de usuario y de complemento (*plug-in*) para intercambiar contenidos sociales[51].

(51)Véase http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp194_es.pdf (fecha de consulta: marzo del 2016).

5.9. La garantía de la protección del derecho a la protección de los datos personales

1) Las autoridades de protección de datos

La garantía de la protección del derecho a la protección de datos se instrumenta principalmente a través de la intervención de unas entidades de carácter independiente.

La Agencia Española de Protección de Datos es un ente de derecho público con personalidad jurídica propia y plena capacidad pública y privada, que actúa con independencia de las administraciones públicas en el ejercicio de sus funciones. Entre estas funciones, destacan:

- Velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación, especialmente en lo que respecta a los derechos de información, acceso, rectificación, oposición y cancelación de datos.

- Atender las peticiones y reclamaciones de los afectados.

- Emitir las autorizaciones que prevé la Ley, ordenar, en caso de ilegalidad, el cese en el tratamiento y la cancelación de los datos y ejercer la potestad sancionadora.

- Informar los proyectos de normas de desarrollo que incidan en materia de protección de datos.

Para desarrollar estas funciones, la ley atribuye a la Agencia diferentes potestades como la de resolución de las reclamaciones interpuestas por los interesados. Asimismo, tiene las potestades de investigación, inspección y sanción. Finalmente, también tiene atribuida potestad normativa para dictar las instrucciones necesarias para adecuar los tratamientos de datos a los principios de la LOPD.

Algunas comunidades autónomas han asumido la competencia para crear órganos de garantía de la protección de datos en el marco de lo que consideró la sentencia del Tribunal Constitucional 290/2000, de 30 de noviembre.

En Cataluña, en el 2003 se creó la Agencia Catalana de Protección de Datos para velar por el respeto de los derechos fundamentales y las libertades públicas en todo aquello relacionado con las operaciones efectuadas a través de procesos automatizados y manuales de datos personales. En Madrid también se creó la Agencia de Protección de Datos de la Comunidad de Madrid, que posteriormente fue suprimida en el 2012. En el País Vasco, existe la Agencia Vasca de Protección de Datos que actúa con independencia de las administraciones públicas y que vela por el cumplimiento de la legislación sobre protec-

ción de datos y controla su aplicación. Finalmente, en Andalucía se ha creado en el 2015 el Consejo de Transparencia y Protección de Datos de Andalucía que asumirá el ejercicio de las competencias en materia de protección de datos.

2) El régimen sancionador de las administraciones públicas

La protección de datos personales se lleva a cabo a través del establecimiento de un régimen sancionador que prevé la LOPD para aquellos casos en los que se infrinja el ordenamiento. Este régimen es diferente en función deque se trate de ficheros de titularidad privada o de titularidad pública. La potestad sancionadora corresponde a la Agencia Española de Protección de Datos y a las autoridades autonómicas de protección de datos en su ámbito de actuación.

Sin embargo, cabe advertir que en el caso de las administraciones públicas, las autoridades de control no pueden sancionarlas pecuniariamente si cometen una infracción prevista en la LOPD. En estos casos, el órgano sancionador dictará una resolución estableciendo las medidas que procede adoptar para que cesen o se corrijan los efectos de la infracción por parte de la Administración pública. Asimismo, en su caso, podrá proponer también la iniciación de actuaciones disciplinarias.

3) La responsabilidad patrimonial de las administraciones públicas por los daños ocasionados en materia de protección de datos

En el caso de que la utilización de los datos personales por las administraciones públicas cause un daño, se puede producir el surgimiento de responsabilidad patrimonial de las administraciones públicas. En este punto, debe estarse a lo previsto en la LRJPS.

Abreviaturas

AEPD. Agencia Española de Protección de Datos.

CE. Constitución Española.

ENS. Esquema nacional de seguridad.

LAECSP. Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos.

LOPD. Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

LPACAP. Ley 39/2015, de 1 de octubre, de procedimiento administrativo común de las administraciones públicas.

LRJPAC. Ley 30/1992, de 26 de noviembre, de régimen jurídico de las administraciones públicas y del procedimiento administrativo común.

LRJSP. Ley 40/2015, de 1 de octubre, de régimen jurídico del sector público.

SGSI. Sistema de gestión de la seguridad de la información.

Bibliografía

Cerrillo, A. (2009). «La interoperabilidad y la protección de datos. La conexión de los registros de protección de datos». En: VV. AA. *La protección de datos en la administración electónica*. Cizur Menor: Thomson-Reuters-Aranzadi-Agencia Española de Protección de Datos.

Fernández, M. (2003). *La protección de los datos personales en las administraciones públicas*. Madrid: Civitas-Agencia de Protección de Datos de la Comunidad de Madrid.

Troncoso, A. (2008). «La administración electrónica y la protección de datos personales». *Revista Jurídica de Castilla y León*.