LA ACTUACIÓN ADMINISTRATIVA AUTOMATIZADA EN EL ÁMBITO DE LAS ADMINISTRACIONES PÚBLICAS

Análisis jurídico y metodológico para la construcción y la explotación de trámites automáticos

---

Ignacio Alamillo Domingo

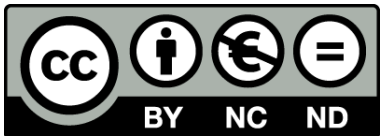
F. Xavier Urios Aparisi

Barcelona, 2011

Generalitat de Catalunya
Escola d'Administració Pública de Catalunya

Este estudio es fruto de una subvención de la Escuela de Administración Pública de Cataluña para el fomento de trabajos de investigación para la mejora de las administraciones públicas (Resolución GAP/2965/2008, de 17 de septiembre), y ha sido sometido a una avaluación externa que valida su contenido y recomienda su publicación.

Primera edición: mayo de 2011
ISBN: 978-84-694-3266-2
Dipòsit legal: B.21900-2011



Índice

1. Presentación

La regulación legal de las tecnologías de la información y las comunicaciones en el ámbito de las Administraciones Públicas no es, ni mucho menos, un fenómeno novedoso en España que, en su primera regulación con una vocación general y sistemática, encuentra su punto de partida en la ya lejana Ley 30/1992, de 26 de noviembre, del Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común y, en concreto, en su artículo 45, hoy en gran medida derogado. No obstante, es preciso reconocer que sólo ha sido en los últimos años cuando su uso ha experimentado un nivel considerable y, en consecuencia, se han evidenciado los inconvenientes y desajustes provocados por un marco normativo que, desde una visión prospectiva y por tanto ventajista, no se adecuaba ya a las necesidades de modernización tecnológica que planteaba la exigencia de una Administración Pública moderna y preparada para asumir a los desafíos de la sociedad de la información.

Hace poco más de tres años, la Ley 11/2007, de 22 de abril, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos (LAE) ha intentado ofrecer un marco normativo adecuado al referido contexto en el que, como su propia exposición de motivos afirma, "las Administraciones deben comprometerse con su época y ofrecer a sus ciudadanos las ventajas y posibilidades que la sociedad de la información tiene, asumiendo su responsabilidad de contribuir a hacer realidad la sociedad de la información". Sin embargo, como ya he mantenido en otro lugar,[1] aunque es preciso reconocer que se han producido avances significativos con la referida Ley, lo cierto es que se podía haber ido más allá, sobre todo teniendo en cuenta que se trataba de una oportunidad histórica para avanzar en la consolidación y el fortalecimiento de muchos de los principios del Estado democrático y haber conducido a un nuevo modelo de Administración Pública volcada efectivamente en resolver los problemas a la sociedad y a los ciudadanos, con su efectiva participación y su control, más allá de las limitaciones propias de los procesos electorales cada cuatro años. De ahí que

[1] «La nueva regulación legal del uso de las tecnologías de la información y las comunicaciones en el ámbito administrativo: ¿el viaje hacia un nuevo modelo de Administración, *electrónica*?». *Revista Catalana de Dret Públic*, núm. 35, pág. 242.

concluía con un deseo de que "la nueva regulación no se convierta en una excusa para un mero cambio de soporte que termine por justificar la versión actualizada de una indeseable *burocracia electrónica*".

La posterior consolidación en España de una corriente de opinión, no tanto doctrinal como sobre todo desde la valoración práctica, acerca de la necesidad de un nuevo modelo de Gobierno y Administración Pública basado en el uso de las tecnologías de la información y la comunicación —del que el denominado *Open Government* es uno de sus mejores exponentes—[2] parece abonar esta tesis, de manera que se reclama el aprovechamiento de las posibilidades que ofrece la tecnología para reformular tanto la actividad de las Administraciones Públicas como, desde una dimensión externa, las relaciones con los ciudadanos. En este sentido, la utilización de la tecnología en dicho ámbito se está empezando a concebir no ya como una simple oportunidad para la modernización de las estructuras y procedimientos sino, incluso y sobre todo, para la innovación, es decir, para alumbrar una nueva concepción de la Administración Pública que, a través de la tecnología, permita dar verdadera satisfacción a su razón de ser: el servicio a los intereses generales, esto es, a la sociedad y los ciudadanos, con eficacia y eficiencia, de manera que se erradique, de una vez por todas, la percepción tan frecuente en muchos ámbitos de que la Administración es un auténtico lastre social.

Precisamente, el reciente Plan de acción europeo sobre e-Government 2011-2015[3] establece entre sus ejes prioritarios el incremento de eficiencia y un efectiva atención a las prioridades de los usuarios, la mejora de los procesos organizativos y la reducción de las cargas administrativas así como, en última instancia, la necesidad de plantear los servicios electrónicos desde la perspectiva de la innovación. Se trata, en definitiva, de retos y desafíos a los que sólo puede aspirarse a partir de la actuación administrativa automatizada: resulta claramente ineficiente que, a pesar de los avances tecnológicos y sobre todo de las cuantiosas inversiones realizadas, las decisiones de las Administraciones Públicas sigan teniendo que estar basadas en la intervención directa de personas físicas cuando la misma no resulte necesaria u

[2] http://eadminblog.net/post/2007/05/27/administracion-abierta-open-government-un-modelo-a-partir-del-open-business

[3] http://ec.europa.eu/information_society/activities/egovernment/action_plan_2011_2015/index_en.htm

oportuna. Ahora bien, las enormes posibilidades que ofrece la tecnología a este respecto deben estar planteadas desde la necesaria primacía del Derecho y, en particular, de las normas jurídico-administrativas que aseguren que las decisiones administrativas son adoptadas con las máximas garantías.

Por ello, y por las razones que más adelante se enunciarán, el libro que el lector tiene en sus manos (o en su pantalla) era ciertamente necesario, ya que se trata de la primera monografía que aborda con carácter exclusivo esta trascendente problemática, de manera que se convierte en una referencia inexcusable a la hora de abordar cualquier iniciativa mínimamente ambiciosa de modernización administrativa. Más aún, la indiscutible cualificación de los autores constituye una garantía de que el tratamiento de los problemas que se abordan y las soluciones que se proponen no sólo se han planteado desde el conocimiento teórico sino, además y sobre todo, a la vista de su efectiva implicación en la realidad donde han de de aplicarse las medidas propuestas.

Todavía recuerdo cuando tuve la suerte de conocer a Ignacio Alamillo Domingo en Murcia allá por el año 2000, recién aprobado el Decreto-Ley 14/1999, con ocasión de la impartición de una conferencia sobre la firma electrónica en un momento en que dicha herramienta estaba teñida de unas connotaciones futuristas que prácticamente la situaban al margen de los círculos donde habitualmente nos movíamos los juristas: hoy día, sin lugar a dudas es uno de los máximos expertos europeos en relación con la gestión de las identidades electrónicas, en particular por lo que se refiere a su proyección en la prestación de servicios administrativos. Junto a él, Xavier Urios Aparisi aporta, desde su condición de jefe de la Asesoría Jurídica del Departamento de Gobernación y Relaciones Institucionales de la Generalitat de Catalunya, una sólida formación jurídico-administrativa que, más allá de la perspectiva teórica, se fundamenta en el conocimiento directo de los problemas que, en este proceso, ha de abordar el derecho dado que ha tenido que enfrentarse a ellos —y, sobre todo, solucionarlos, a veces de manera imaginativa— al prestar sus servicios en una organización que, sin duda, ha venido liderando la modernización tecnológica de la Administración Pública en España durante muchos años.

Así pues, desde la perspectiva que aporta el conocimiento efectivo de la materia, los autores han realizado una aportación de gran valía con esta obra ya que, en definitiva,

se han visto obligados a enfrentarse *cara a cara* con uno de los principales encorsetamientos de que adolecen las Administraciones Públicas españolas: la percepción del derecho y, en concreto, del derecho administrativo como un inconveniente para la modernización tecnológica de la Administración Pública que, como una de sus principales manifestaciones, determina la existencia de una cultura administrativa que, más allá de las estrictas exigencias del principio de legalidad propias de un Estado de derecho, reclama una regulación exhaustiva hasta el extremo; *reglamentista* en la más peyorativa acepción del término, en la que absolutamente todos los detalles deben estar regulados en la norma escrita, aun cuando esta solución dificulte e, incluso, impida cualquier intento de modernización en beneficio de una pretendida seguridad jurídica que, en definitiva, a medio plazo puede llegar a producir un efecto contrario al pretendido. Precisamente, este libro supone un avance decidido en esta ingente tarea, sobre todo teniendo en cuenta las deficiencias de la regulación que, en relación con la automatización de la actividad administrativa, contiene la LAE y que los autores lúcidamente abordan para ofrecer soluciones efectivas, ajustadas a las exigencias que plantea la realidad administrativa, tan necesitada de una auténtica renovación para hacer frente, a través de la tecnología, a algunos de los relevantes desafíos que la sociedad demanda con vehemencia a nuestras Administraciones Públicas.

En este sentido, desde una perspectiva tecnológica se enfrentan a conceptos nucleares del derecho administrativo como el principio de la competencia, el ejercicio de las potestades o, sobre todo, la teoría del órgano y, en concreto, la exigencia de que las decisiones administrativas sean adoptadas directamente por la persona física a la que corresponda su titularidad; entroncando de esta manera con el que, hasta ahora, había sido considerado el elemento subjetivo del acto administrativo. O, por lo que se refiere a la eventual invalidez de la actuación administrativa, la incidencia que pueda tener sobre la misma la deficiente programación de la aplicación informática utilizada es analizada con acierto por los autores a pesar de su dificultad, actualizando conceptos tradicionales de gran raigambre como la desviación de poder que, en este contexto, se proyectaría en la informática decisional aplicada a las Administraciones Públicas. Pero lejos de un ejercicio de erudición alejado de la realidad práctica a la que se refiere, el trabajo que ahora presento se centra en la realización de un análisis riguroso pero, al mismo tiempo, basado en el conocimiento directo de la materia y, por tanto, no debe sorprender que se planteen propuestas concretas en forma de

recomendaciones concretas y análisis de ejemplos concretos de actuaciones administrativas cuya automatización se propone en forma de tablas. Todo ello a partir de un análisis que tiene en cuenta tanto la perspectiva jurídica como la organizativa, la tecnológica e, incluso, la filosófica a través de la denominada *lógica deóntica*.

Ciertamente se podrían haber abordado otros problemas y aspectos aún latentes en relación con las actuaciones administrativas automatizadas o, incluso, haberlo hecho desde otras perspectivas, pero no es este prólogo el lugar más adecuado para entablar un debate doctrinal al respecto. Simplemente me gustaría explicitar la idea que he tratado de transmitir en los párrafos anteriores: mi recomendación de que lean con sumo interés este sugerente libro, ya que sin duda merece la pena.

Julián Valero Torrijos
Profesor titular de Derecho Administrativo
Universidad de Murcia

2. Introducción general

El objeto de este trabajo consiste en el análisis de la viabilidad jurídica y técnica de la automatización de los actos administrativos a partir de las reflexiones y los resultados principales de un trabajo de investigación patrocinado por la Escuela de Administración Pública de Cataluña realizado durante los años 2008 y 2009.

Durante esta investigación, se han tomado en consideración unos supuestos de actos administrativos que, en una primera aproximación, eran susceptibles de automatización. Una vez analizados, se han intentado extrapolar las condiciones jurídicas y técnicas que se tendrían que llevar a cabo con el fin de garantizar que la actuación administrativa automatizada se adecue al marco normativo de referencia y a las condiciones técnicas que hagan viable esta automatización.

En este sentido, durante la investigación se ha analizado cada uno de los elementos que tienen que ser considerados y en relación con los cuales el órgano responsable de la automatización ha de tomar decisiones concretas con el fin de garantizar que la automatización del acto administrativo no tan sólo se ajusta a la norma, sino también que no produce perjuicios o reducción de garantías en los administrados.

Se puede adelantar que el análisis se ha llevado a cabo desde la prudencia, puesto que la cautela es un principio o criterio básico a la hora de implementar la administración electrónica y, especialmente, más todavía cuando hablamos de la reducción de la capacidad de decisión de la voluntad humana, en la medida en que es la máquina la que toma decisiones. Sin embargo, el trabajo se ha conformado sobre la base de una programación previa que, lógicamente, parte de la factura humana, razón por la cual el análisis y las conclusiones se pueden considerar conservadoras.

2.1. Sobre la viabilidad de la automatización de procesos

No obstante, la primera conclusión a extraer es la viabilidad de la automatización de procesos, por las razones que posteriormente se presentarán y que se pueden concretar en una premisa: hay actuaciones administrativas que se pueden automatizar, e incluso razones de eficiencia recomiendan la automatización.

Las razones de esta conclusión son evidentes: se trata de situaciones en que el acto administrativo como expresión de una voluntad humana es reducido, porque este elemento volitivo se limita a menudo a la comprobación de unos elementos reglados, cosa que, en la práctica, se llega a convertir en un automatismo. En estos casos, no se aprecian problemas relevantes para la automatización. De todos modos, eso no significa una libertad absoluta para integrar una respuesta automática en determinadas actuaciones, sino que habrá que instrumentar un protocolo que asegure que la implementación del automatismo se lleva a cabo adecuadamente y, en la medida en que nos encontramos delante de actos administrativos, permitir el control de la legalidad de la actuación administrativa.

Esta adecuación, necesaria tanto en el ámbito normativo como en el ámbito técnico, es objeto de tratamiento en los capítulos 2 y 3 de este trabajo. En estos apartados se analizan los requerimientos jurídicos y técnicos que hay que tener en cuenta en la automatización y se intenta dar respuestas concretas a cada una de las cuestiones planteadas.

Finalmente, se ha generado una guía de recomendaciones que se presenta en este mismo capítulo. Esta guía intenta resumir las recomendaciones de carácter jurídico, de análisis y de diseño, como también sobre técnicas de sistema, de firma electrónica, de certificados de sello automático y de seguridad y auditoría, las cuales garantizarían, desde nuestro punto de vista, que la actuación administrativa automatizada se adecuara a la norma.

Hablamos necesariamente de adecuación a la norma, ya que es evidente que, en el ámbito del derecho administrativo, la sumisión a la norma es esencial, sin que otras fuentes del derecho como la costumbre resulten relevantes.

En este sentido, la investigación ha analizado, desde la teoría de las potestades administrativas, las actuaciones que las diferentes administraciones públicas tienen que llevar a cabo en el ámbito normativo a la hora de dar cobertura a esta automatización. Naturalmente, se ha partido de la base del marco jurídico vigente esencialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos y se ha hecho referencia sobre todo a la normativa catalana aprobada recientemente en el ámbito de la Administración de la Generalitat de Catalunya, en qué hay previsiones normativas específicas relativas a esta automatización.

Del análisis de esta normativa se han extraído conclusiones que, en principio, se pueden trasladar a otras administraciones públicas de carácter territorial las administraciones locales, con el límite evidente que supone el respeto al principio de autonomía local en este ámbito.

En la misma línea, en la medida en que las materias relativas a impulso, ordenación y desarrollo de los servicios electrónicos tienen un carácter organizativo, y que del artículo 103.1 y 2 de la Constitución deriva la indicación que las decisiones organizativas se tienen que adoptar de acuerdo con una ley, es esencial que los aspectos básicos de la automatización estén recogidos en una norma con rango de ley.

Esta habilitación se encuentra en el artículo 39 de la Ley 11/2007:

«En caso de actuación automatizada se debe establecer previamente el órgano u órganos competentes, según los casos, para la definición de las especificaciones, programación, mantenimiento, supervisión y control de calidad y, si ocurre, auditoría del sistema de información y de su código fuente. Asimismo, se tiene que indicar el órgano que tiene que ser considerado responsable a los efectos de impugnación.»

Este artículo tiene una naturaleza doble: se trata de un artículo principal, en la medida en que prevé los caracteres básicos de la automatización de una manera muy somera, pero, además, no tiene carácter básico, cosa que significa, que, en principio, otros titulares de la potestad legislativa podrían establecer requerimientos diferentes.

No obstante esta previsión, ya hemos avanzado que, difícilmente, la automatización de procesos no tendrá que respetar estos mínimos, dado que eliminarlos podría comportar una reducción de las garantías de la ciudadanía y de la transparencia de la actuación administrativa automatizada.

Esta habilitación legal de carácter estatal permite que las Comunidades Autónomas establezcan otros condicionantes de la actuación administrativa automatizada con normas con rango de ley, si bien en todo caso hará falta un despliegue reglamentario que complemente los criterios legales establecidos, que carecen de un nivel de concreción reservado al reglamento.

Además, existe igualmente la posibilidad que, al margen de la regulación legal de los aspectos básicos y el despliegue reglamentario correspondiente, se produzca una descarga de los aspectos más técnicos y cambiantes, que se pueden concretar con normas de rango inferior, en qué éstos se concreten y se sometan a un régimen de publicidad inferior (se trataría sobre todo de los aspectos más técnicos y de algunos organizativos).

En resumidas cuentas, al amparo de una previsión legal habilitante de carácter estatal y de una habilitación reglamentaria, se puede llevar a cabo la automatización de procesos en el marco legal establecido sin que sea necesario que todos los elementos técnicos se encuentren recogidos a las normas mencionadas anteriormente. No obstante, sí que hace falta que un instrumento normativo de nivel inferior recoja o regule estos aspectos técnicos o de detalle que, por su naturaleza, no es recomendable que se incluyan en una norma legal o reglamentaria, la cual, atendiendo a su naturaleza, es mucho más difícil de adaptar o de adecuar a las circunstancias técnicas que vayan variando.

En cualquier caso, el artículo 39 de la Ley 11/2007 enumera los elementos que han sido objeto de análisis: el órgano administrativo, la competencia, la definición de las especificaciones o los programas, la auditoría y el control de calidad, y la impugnación de la actuación administrativa automatizada.

2.2. Elementos a considerar a la hora de automatizar los actos administrativos

Los elementos siguientes han sido analizados a lo largo de la investigación. Todos ellos se presentan detalladamente al capítulo 2 de este trabajo.

2.2.1. El órgano administrativo

Aunque la automatización supone la desaparición de la voluntad humana *stricto sensu*, no plantea problemas por una razón doble: en primer lugar, por la habilitación legal existente para esta sustitución, y, en segundo lugar, por el hecho de que la desaparición de la voluntad humana es meramente aparente, ya que ésta se manifiesta mediante la programación que se debe confeccionar y aprobar con carácter previo a la automatización del acto de que se trate.

Esta programación parte de la realización de una metodología de análisis y diseño que parte del acto administrativo a automatizar – de su naturaleza y particularidades – y que se traslada a lo que tiene que ser una informatización correcta; es decir, conseguir que la respuesta de la máquina derive de una programación que responde a los criterios técnicos establecidos sobre la base de criterios jurídicos (la respuesta o la decisión de la máquina es, evidentemente y en última instancia, una actuación jurídica de la cual derivan efectos jurídicos).

En este sentido, las recomendaciones sobre análisis y diseño que se exponen en los capítulos 3 y 5 son enormemente relevantes, dado que la conexión o el entendimiento

entre el jurista y el técnico, siempre importante cuando hablamos de administración electrónica, es especialmente significativa en el ámbito de la automatización.

Por esta razón, la desaparición de la voluntad humana es meramente aparente, ya que la conjunción del análisis, evidentemente humano, de los aspectos jurídicos y técnicos por parte de personas habilitadas o capacitadas legalmente a este efecto – es decir, competentes – hacen que, en última instancia, la actuación administrativa automatizada se pueda considerar la exteriorización de una voluntad humana, de un órgano administrativo competente a estos efectos.

2.2.2. La competencia

La competencia del órgano parte de la base que, en el ámbito del derecho administrativo, la competencia es irrenunciable y la ejerce el órgano que la tiene atribuida legalmente.

En este caso, cuando hablamos de competencia, lo debemos hacer en un nivel doble: competencia para automatizar y competencia para determinar como automatizar.

2.2.2.1. Competencia para automatitzar

La competencia para automatizar supone una decisión discrecional del poder público, que decide que determinados actos administrativos son susceptibles de automatización. Tal como hemos indicado, esta decisión es claramente discrecional y previa a la automatización propiamente dicha, e incluso puede obedecer a criterios de valoración de riesgos a la hora de concretar los actos que se podrían automatizar.

Ya hemos advertido que, en principio, esta decisión se habría de tomar de acuerdo con criterios de prudencia, y que la automatización se tendría que trasladar inicialmente a las actuaciones que, por su naturaleza, tienen que plantear menos riesgos.

La investigación se ha centrado en diferentes supuestos, clasificados en tres grupos:

1) Los actos que se podrían llamar de *entrada*, en la medida en que tienen lugar en el momento inicial del procedimiento. Se trata de los recibos de registro electrónico, las comprobaciones automáticas de solicitudes y la digitalización automática de documentos.

2) Los actos *internos* del procedimiento, que se producen en el ámbito de la tramitación administrativa desde la vertiente interna. Son los actos de impulso automático del procedimiento, actos automáticos de constancia, las copias auténticas automáticas, la apertura y el cierre de libros, la foliación automática de documentos y las migraciones automáticas.

3) Los actos de *salida*, ya sean fruto de actos de comunicación con otras administraciones públicas o bien con la ciudadanía (las notificaciones propiamente dichas).

Del análisis de estos supuestos se han extraído las conclusiones de que la automatización no plantearía problemas desde la vertiente jurídica ni desde la vertiente técnica, sin perjuicio que se tienen que tomar decisiones concretas basadas en la plasmación documental del acto, el tipo de firma electrónica a utilizar y otros elementos que se tienen que singularizar en función de cada acto.

Al mismo tiempo, la decisión sobre la automatización tiene que implicar una mejora de la eficiencia administrativa, tanto desde la vertiente de funcionamiento como desde la vertiente económica. Desde la vertiente de funcionamiento, la automatización tiene que comportar una reducción de plazos, consecuencia ligada a la administración electrónica configurada globalmente pero que en la automatización de procesos tiene que ser todavía más evidente. Desde la vertiente económica, aunque es una obviedad, la automatización tiene que permitir liberar o destinar a otras actividades de interés general recursos humanos destinados tradicionalmente a trabajos que, aunque sea parcialmente, se pueden considerar mecánicos y que una máquina programada debidamente puede llevar a cabo.

En particular, hay que destacar que supuestos como la digitalización de documentos, los recibos de registro, la comunicación de datos entre administraciones públicas o las notificaciones administrativas son paradigmáticos en relación con las ventajas comentadas. No obstante, el resto de actuaciones no analizadas, aunque quizás son menos visibles, tampoco no dejan de tener relevancia en el funcionamiento ordinario de los órganos administrativos.

Las decisiones relacionadas con los actos administrativos susceptibles de ser automatizados se pueden tomar aisladamente, caso por caso, o bien en el marco de una política de planificación en que, aunque sea parcialmente, los criterios discrecionales se condicionan en el marco de planificación que haya sido determinado o aprobado.

En un segundo nivel, incluso se podría plantear la automatización de decisiones administrativas en que, aunque se basan aparentemente en el ejercicio de potestades discrecionales, hay elementos reglados que condicionan el contenido de la resolución a dictar. Éste sería el caso, por ejemplo, del otorgamiento de subvenciones – con la comprobación previa del cumplimiento de las condiciones objetivas de otorgamiento – o la denegación de subvenciones por falta de cumplimiento de los requisitos establecidos a la convocatoria – que se podría comprobar de manera automática mediante el control de la solicitud presentada, integrada si procede, a una notificación automática previa para enmendar la solicitud correspondiente.

De acuerdo con lo que hemos expuesto, las posibilidades de la automatización de la actuación administrativa son evidentes y claramente ventajosas para el funcionamiento de la Administración

2.2.2.2. Competencia para determinar como automatizar

Cuando el órgano administrativo competente haya determinado qué actos son susceptibles de automatización, hace falta instrumentalizar esta automatización. Se trata de una competencia de los órganos administrativos que tengan atribuidas estas

funciones de carácter técnico desde la doble vertiente, jurídicas y estrictamente técnicas, en relación con las actuaciones que se tienen que practicar.

En este segundo nivel, el margen de actuación es menos amplio, porque el marco normativo que hay que aplicar a la automatización considerada formalmente lo integra el conjunto de aspectos jurídicos y técnicos que tienen que ser evaluados y a los cuales se trata de dar respuesta mediante una programación adecuada.

En esta fase, habrá que concretar las condiciones jurídicas y técnicas de automatización con una programación lógica y de codificación que garantice que el acto administrativo emitido es correcto, completo, suficiente y no discriminatorio.

A la hora de determinar cómo se tiene que automatizar, hay que resolver igualmente aspectos concretos de la actuación administrativa en función del acto o el trámite de que se trate, como la firma electrónica a utilizar y los certificados de sello automático.

Como se ha indicado en el análisis, toda actuación administrativa automatizada es, en definitiva, una manifestación más de la manera de actuar de la Administración, en la medida en que implica, en última instancia, la emisión o la producción de actos administrativos. Este hecho lleva aparejada la identificación y la autenticación necesarias de quien produce el acto, la cual está ligada claramente a la competencia del órgano para llevar a cabo la actuación concreta.

Por esta razón, la utilización o la regulación del sello de órgano nos hará plantear la teoría general del acto administrativo y de la competencia del órgano administrativo, los supuestos en que esta figura se podría admitir, así como los límites a la informática decisional que se tendrán que establecer en la construcción y la aprobación de programas y aplicaciones.

2.2.2.3. Un tercer nivel de competencia

Al margen de los dos niveles de competencia expuestos, existiría un tercer nivel: el de la competencia que percibe directamente la ciudadanía, es decir, la actuación

administrativa concreta que deriva de la automatización del procedimiento y, en definitiva, de un hardware programado debidamente para producir actos con un contenido determinado en función de los presupuestos que concurran.

Este último concepto de competencia, desde la vertiente ciudadana, tiene que ser en principio irrelevante, ya que la actuación administrativa se tiene que configurar de manera indiferenciada tanto si se lleva a cabo presencialmente como si se hace por medios electrónicos y, en este último caso, incluso si es consecuencia de la automatización.

La capacidad de reaccionar que tiene el administrado o la administrada ante la actuación que la afecta será, sin embargo, una cuestión diferente. En este supuesto, de la misma manera que se puede instar la revisión del acto desde el punto de vista sustantivo – es decir, con respecto a su contenido material –, el acto también puede ser revisado desde la vertiente formal, configurada en torno a la regularidad formal de su producción (competencia del órgano, aptitud del titular, etc.).

2.2.2.4. La definición de las especificaciones y los programas

Ya hemos incidido anteriormente en el concepto de definición de las especificaciones y los programas, que gira en torno al cumplimiento de los requerimientos jurídicos y técnicos que son aplicables.

Además, hay que tener presente que, en el ámbito del derecho administrativo, un elemento esencial de la actuación administrativa es la motivación del acto, fundamental para controlar la regularidad. En el caso de la actuación administrativa automatizada, no hay una motivación aparente, puesto que las máquinas no pueden emitir declaraciones de voluntad propiamente dichas ni formular declaraciones de voluntad, de juicio, de conocimiento o de deseo, si recordamos la definición clásica de acto administrativo que hizo Zanobini.

Es por eso que la motivación del acto automatizado se relaciona de manera directa con la programación adecuada de la actuación, ya que en ésta se plasman los

criterios técnicos y jurídicos que, ante determinados supuestos, comportan determinadas consecuencias observadas en actos administrativos concretos.

Esta definición de las especificaciones y los programas nos ha llevado a evaluar si continúa siendo necesario aprobar los programas y las aplicaciones y difundir públicamente las características, como preveía el artículo 45.4 de la Ley 30/1992, de 26 de noviembre, de régimen jurídico de las administraciones públicas y del procedimiento administrativo común, teniendo presente que la Ley 11/2007 ha implicado justamente lo contrario: la desaparición de las obligaciones mencionadas (no regulando la cuestión y derogando el artículo 45.4).

Desde nuestro punto de vista, esta aprobación – ligada directamente a la doctrina de la vinculación positiva y las potestades administrativas – continúa resultando necesaria. Sin embargo, con respecto a la difusión pública, se pueden establecer sistemas de publicidad de las características de las aplicaciones que no impliquen necesariamente publicaciones en diarios oficiales, sino que se pueden sustituir por otros medios de difusión, como la incorporación de estas características en la sede electrónica corporativa.

Sea como sea, en el ámbito de la actuación administrativa automatizada se habla específicamente de la definición de las especificaciones y los programas, lo cual se tiene que entender equiparable a la aprobación.

Como regla general, esta aprobación se prevé ya en ámbitos como el derecho tributario, en el que la llevaría a cabo el órgano competente a efectos de impugnación. Eso garantizaría que el control del acto lo mantuviera quien, en última instancia, verificaría la regularidad de la actuación administrativa

2.2.2.5. La auditoria y el control de calidad

Otro elemento a evaluar en el ámbito de la actuación administrativa automatizada es el establecimiento de sistemas de auditoría y control de calidad.

Es evidente que la actuación administrativa automatizada se tiene que hacer de forma

segura. Se tiene que articular, por lo tanto, en torno a la seguridad de los sistemas y las aplicaciones utilizados, cosa que se puede acreditar mediante la auditoría de estos sistemas y de estas aplicaciones.

Este ámbito incluye dos fases claramente diferenciadas: el establecimiento y la implementación de sistemas de seguridad, por un lado, y la realización de auditorías que acrediten que la primera fase cumple los parámetros legales y técnicos exigibles, por el otro

En cuanto a la primera fase, y partiendo igualmente de los casos de uso de autenticación de los sujetos que intervienen en el procedimiento y de la documentación gestionada, se tienen que establecer normativas de seguridad, básicamente criptográfica, que garanticen la seguridad en las actuaciones administrativas mediante la definición de estándares, claves a utilizar, y de aplicación de las firmas electrónicas utilizadas.

Con respecto a la segunda fase, la auditoría de terceros de confianza, cualificados debidamente, es la que garantiza de forma más adecuada que la implementación de la automatización, desde la vertiente de la seguridad, resulta correcta.

2.2.2.6. Impugnación de l'actuación administrativa automatizada

La capacidad de reaccionar del administrado o la administrada ante los actos administrativos que lo afectan es un derecho básico que, en el ámbito de la actuación administrativa automatizada, se tiene que enfocar desde una perspectiva doble:

- el control del acto administrativo producido, y
- el control de la regularidad o la corrección de la programación realizada.

Esta capacidad de reaccionar nos ha conducido igualmente a evaluar las consecuencias de la falta de cumplimiento de los requerimientos que resulten aplicables a la automatización.

Aplicando la teoría general de la invalidez de los actos jurídicos, si la actuación administrativa automatizada no se encuentra amparada en una habilitación suficiente, la regularidad del mecanismo de producción de actos administrativos se rompe.

Este vicio entraría en la consideración de invalidez absoluta, que, trasladada al ámbito del derecho administrativo, determinaría un supuesto de nulidad absoluta, ya sea para considerar que se trata de un acto dictado por un órgano manifiestamente incompetente (letra b del artículo 62.1 de la Ley 30/1992), ya sea por un supuesto de prescindir totalmente del procedimiento (letra e del mismo artículo).

En este sentido, la regla general sería la nulidad de pleno derecho, vicio determinante de la actuación administrativa que, en el ámbito de la utilización de los medios electrónicos, es especialmente significativo vista la falta de confianza que la utilización de estos medios genera todavía actualmente en los administrados.

Eso nos tiene que llevar a ser prudentes a la hora de implementar la automatización de procesos. No podemos caer en una automatización irracional y arbitraria, sino que lo que es recomendable es automatizar los procesos que lo permiten claramente y, a la vista de los resultados alcanzados, plantear la automatización de procesos de decisión más complejos.

Por otra parte, sería igualmente posible que el vicio que se produjera no fuera la nulidad de pleno derecho, sino la anulabilidad de las actuaciones administrativas realizadas, la cual podría tener lugar en los supuestos de una programación inadecuada. Eso deriva del carácter restrictivo que se predica de la nulidad de pleno derecho, aplicable tan sólo a los supuestos establecidos taxativa y legalmente como aquéllos que llevan aparejada la nulidad de pleno derecho (que son los mencionados en el artículo 62.1 de la Ley 30/1992). En este sentido, en la medida en que una programación inadecuada no se metería en ninguno de los supuestos taxativos de nulidad lleno derecho, se tendría que considerar una causa de anulabilidad, recogida en el artículo 63 de la Ley 30/1992.

Por contra, una programación indebida o cualquier otro defecto de carácter parecido no se podría considerar una actuación administrativa irregular, ya que difícilmente se producen los supuestos previstos legalmente. En cualquier caso, habría que remitirse

a las circunstancias del caso concreto a los efectos de evaluar este punto (por ejemplo, una notificación más allá del plazo establecido legalmente por razón de la caída del servidor se podría considerar un acto de notificación irregular, siempre que no se hubiera producido el silencio administrativo positivo y que la notificación fuera de un acto de contenido negativo).

Finalmente, se podría producir una desviación informática de poder, cosa que implicaría trasladar al campo de la informática decisional la doctrina de la desviación de poder. En este sentido, la desviación de poder, configurada como a supuesto de anulabilidad, tendría lugar cuando la programación de los programas y las aplicaciones que tienen que llevar a cabo la actuación administrativa automatizada correspondiente, aunque aparentemente se adecua a la legalidad aplicable, se ha realizado para una finalidad o persigue una finalidad diferente de la que prevé el ordenamiento jurídico. En definitiva, ligaría con la idea de que la motivación del acto administrativo automatizado deriva de la programación practicada y aprobada debidamente.

2.3. Otras cuestiones objeto de análisis

La investigación ha incidido en otros aspectos de la actuación administrativa automatizada:

- Los derechos de los ciudadanos como límite de la automatización.
- Los límites de la actuación administrativa automatizada.

2.3.1. Los derechos de los ciudadanos como límite de la automatización

A la recomendación de prudencia a la hora de automatizar los actos administrativos, se debe añadir que, como consecuencia de la automatización, los derechos de los ciudadanos en sus relaciones con las administraciones públicas no se pueden reducir.

Estos derechos deben ser los que reconoce la normativa específica, particularmente la Ley 11/2007, pero también habrá que respetar todos los derechos que reconoce el ordenamiento jurídico con carácter general.

Tan sólo una norma con rango de ley podría alterar este régimen de derechos, como consecuencia del principio de legalidad y de la reserva de ley en la materia.

2.3.2. Los límites de la actuación administrativa automatizada

La automatización de procesos no se puede trasladar a cualquier actuación administrativa. En este sentido, la automatización es más viable en el ámbito de las potestades regladas que en el ámbito de las potestades discrecionales.

El sello de órgano también obliga a revisar el régimen de recursos administrativos y los medios de impugnación, porque el recurso de alzada o de reposición, admitidos tradicionalmente como medios de impugnación o recursos ordinarios en el ámbito del derecho administrativo, no pueden ser trasladados a la actuación administrativa automatizada sin ninguna matización. A título de ejemplo, en el caso del recurso de reposición, no nos encontraríamos con una reposición por parte del mismo "órgano" que decidió el acto impugnado; en el caso del recurso de alzada, si el órgano competente es el que ha acordado la automatización del acto y ha aprobado las condiciones de esta automatización, nos encontraríamos de facto con un recurso de reposición. Así, en la práctica, significaría trasladar al mismo órgano que ha tomado la decisión de automatizar una actuación administrativa determinada la resolución de los recursos que se puedan interponer.

Paralelamente, la automatización debe quedar excluida de todos aquellos supuestos en que haya un elemento subjetivo o una valoración en la actuación administrativa, así como una motivación más allá de aquélla que sea viable predeterminar mediante una programación concreta. De lo contrario, se estarían vulnerando los principios generales del procedimiento administrativo y, además, se produciría una rebaja de los derechos de los ciudadanos que no estaría amparada por la Ley 11/2007

En resumidas cuentas, corresponde a cada Administración determinar los supuestos y los trámites a los que se puede aplicar el sello de órgano, si bien esta determinación no se puede llevar a cabo indiscriminadamente, sino a partir de una valoración adecuada de los actos administrativos que se pueden hacer de forma automatizada, de acuerdo con el principio de proporcionalidad, y sin que se produzca una merma de garantías del administrado o la administrada.

Para acabar, también hay que tener presente el respeto a la normativa de protección de datos. La automatización no puede partir de la base del tratamiento indiscriminado de datos de carácter personal de que disponga la Administración para evaluar determinados aspectos, sino que se tendrá que hacer respetando plenamente la normativa mencionada.

Así se prevé en el artículo 13 de la Ley orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. En cualquier caso, esta previsión se tiene que interpretar en términos muy estrictos, sin hacer una interpretación restrictiva ni tampoco extensiva, ya que eso impide la toma de decisiones derivada de datos que posee la Administración, lo cual no es la finalidad de la Ley orgánica de protección de datos.

2.4. Recomendaciones para la automatización de la actuación administrativa

En resumidas cuentas, se puede concluir que la actuación administrativa automatizada es jurídicamente viable y que el marco jurídico actual habilita la implementación. No obstante, no hay bastante con una habilitación legal genérica, sino que hace falta un despliegue en un segundo nivel, al margen de determinados aspectos técnicos que pueden ser objeto de regulaciones de rango inferior.

Por otra parte, la automatización requiere una decisión previa del órgano competente que, en función de la naturaleza del acto, determine, por razones de interés general, la automatización. Esta circunstancia comportará el desarrollo de unas tareas

administrativas, jurídicas y técnicas para hacer efectiva la automatización en el marco jurídico y técnico aplicable. Asimismo, hará falta determinar las condiciones de programación que garanticen que el contenido del acto se adecua a la finalidad prevista y establecer, con una concreción lógica y técnica adecuada, las condiciones de producción del acto.

La aprobación más o menos formal de estos programas y especificaciones no excluye una supervisión de la actuación administrativa producida, tanto desde la vertiente interna como la que derive de la reacción del destinatario del acto, que, con carácter general, puede reaccionar ante una actuación administrativa que lo afecta. Concretamente, si se trata de un acto administrativo automatizado, podrá reaccionar tanto respecto al contenido como pasa en cualquier acto administrativo como con respecto a las condiciones de la automatización. Ya hemos avanzado que, según los casos, se podría llegar a declarar la nulidad de pleno derecho de la actuación producida.

2.4.1. Recomendaciones jurídicas

Recomendación 1.1.	La automatización de los procesos se debe adecuar al marco jurídico vigente, en particular, el artículo 39 de la Ley 11/2007 y la normativa dictada en despliegue de esta Ley.
Recomendación 1.2.	La automatización supone una decisión previa discrecional del órgano competente, que tiene que determinar los actos administrativos susceptibles de automatización y controlar la programación de las aplicaciones con el fin de garantizar que la emisión de los actos administrativos automatizados se adecua a las condiciones de aplicación
Recomendación 1.3.	Como regla general, son susceptibles de automatización los actos administrativos reglados. La automatización de la actuación administrativa en el ejercicio de potestades discrecionales es más complicada
Recomendación 1.4.	La automatización de procesos no tiene que significar una reducción de las garantías de los administrados, que han de tener la posibilidad de reaccionar ante la actuación administrativa automatizada para defender sus derechos y sus intereses legítimos
Recomendación 1.5.	La automatización requiere la aprobación de los programas y las aplicaciones por parte del órgano competente, que, además, tendría que difundir públicamente las características a efectos de garantizar el derecho de la ciudadanía y la transparencia en la actuación administrativa.
Recomendación 1.6.	La actuación administrativa automatizada se tiene que producir de acuerdo con una atribución expresa de competencias, que actuará igualmente como límite de su ejercicio.

Recomendación 1.7.	La identificación y la autenticación de la actuación administrativa automatizada se practicarán de acuerdo con los criterios o las políticas de firma electrónica aplicables, en función del acto, el trámite o el servicio de que se trate.
Recomendación 1.8.	La motivación del acto administrativo automatizado se integra por la adecuada programación. Por esta razón, sólo se podrá reaccionar ante el acto administrativo emitido mediante la revisión de esta programación (posibilidad de revisión o de reacción que se tiene que dar al administrado).
Recomendación 1.9.	La automatización de procesos al margen de la normativa habilitante configura un supuesto de nulidad de pleno derecho, mientras que una programación indebida se puede integrar en un supuesto de anulabilidad.

2.4.2. Recomendaciones sobre ciclo de vida del software

Recomendación 2.1.	Adoptar una metodología de gestión del ciclo de vida del software para reducir los riesgos de errores en la automatización. Resulta bastante evidente, según nuestra opinión, que no disponer de una metodología más o menos formalizada y madura para desarrollar el software que soporta la aplicación de actuación administrativa automatizada implica asumir una serie de riesgos, especialmente en relación con posibles errores de programación, que se pueden actualizar en forma de una programación inadecuada del sistema y, por lo tanto, en motivo de impugnación de la actuación por parte de las partes afectadas.
Recomendación 2.2.	Evaluar formalmente, en la fase de análisis de viabilidad del sistema, la posibilidad de automatizar actos administrativos de

voluntad en consideración a dos factores principales: la configuración del acto administrativo como potestad reglada o la predeterminación razonable de los casos en qué actúa la discrecionalidad administrativa, por una parte, y de la informatización correcta de la norma aplicada, especialmente en términos de la necesaria motivación-justificación de los actos automáticos, que a opinión nuestra se tendrá que incorporar al texto de la resolución de forma particularmente detallada, sobre todo en los actos de voluntad y en los actos de juicio.

Recomendación 2.3. Una vez decidida que hacer la actuación de forma automatizada es viable, hay que tratar específicamente el aspecto lógico y semántico en relación con los sistemas de actuación administrativa automatizada, teniendo en cuenta las necesidades de satisfacción y compleción en la interpretación de la norma o conjunto de normas a aplicar de manera automática, con el fin de cumplir el criterio de la programación adecuada.

Recomendación 2.4. Durante las fases de análisis y diseño, hay que involucrar intensamente personal experto en el ámbito legal con el fin de garantizar un análisis adecuado de los requisitos funcionales a partir de una interpretación jurídica apropiada de las normas en que se basarán los actos administrativos y, muy especialmente, los de naturaleza decisoria. Según nuestra opinión, el analista informático necesita apoyo específico para poder transformar la norma jurídica en un conjunto de reglas programables.

Recomendación 2.5. En la fase de diseño, antes de especificar los componentes, se tiene que llevar a cabo una verificación y una validación con la finalidad de analizar la consistencia entre los diferentes modelos y formalizar la aceptación del diseño de la arquitectura del sistema por parte de los usuarios de explotación y sistemas. A nuestro entender, es necesario involucrar en esta verificación

y en esta validación personal experto en cuestiones legales que pueda garantizar la consistencia entre el diseño y la interpretación legal fijada en las etapas anteriores, con el fin de evitar posibles errores.

Recomendación 2.6. En la fase de construcción del software, hay que utilizar metodologías de desarrollo seguro y técnicas de calidad, ya que la automatización de la actuación exige una diligencia particular en el proceso de producción de una decisión que ya no toma una persona, sino un sistema programado adecuadamente. Si la calidad y la seguridad del software son importantes en cualquier aplicación, en el software de actuación automática son absolutamente imprescindibles.

Recomendación 2.7. En la fase de explotación, y en relación con el mantenimiento del software, hay que implementar una función de vigilancia de las normas jurídicas que soportan actuaciones automáticas para detectar las derogaciones con tiempo suficiente para actualizar el sistema o, si ocurre, detenerlo y evitar decisiones automáticas basadas en normas derogadas.

2.4.3. Recomendaciones especiales sobre la viabilidad del sistema

Recomendación 3.1. Las herramientas lógicas jurídicas (deóntica, refutable y descriptiva) nos pueden ayudar a adquirir y formalizar los conocimientos jurídicos de la norma a automatizar, así como a establecer mecanismos de validación, con la finalidad de reducir los riesgos inherentes a la actuación administrativa automatizada.

En particular, el uso de una lógica modal híbrida, con elementos de lógica deóntica y refutable, muy especialmente en el

contexto de la lógica de la acción, constituye un elemento muy potente para obtener una interpretación objetiva y esmerada de los aspectos estructurales de la norma y de su comportamiento argumentador (lo cual permite una cierta previsibilidad de las posibles aplicaciones de la norma en caso de conflicto, sea judicial o administrativo, en términos de proceso).

Por otra parte, el uso de la lógica descriptiva y de las ontologías nos permite un formalismo de representación del conocimiento jurídico que actúa como base para el diseño de aplicaciones jurídicas adelantadas.

Recomendación 3.2.

La aplicación que permite la actuación administrativa automatizada es una aplicación de informática jurídica de decisión. Esta aplicación se tiene que basar intensamente en el análisis lógico de las proposiciones normativas, aunque cada Administración pública tendrá la potestad de decidir el lenguaje que se tiene que aplicar.

Mientras que en algunos casos se optará por una aproximación de sistema experto (basado en una representación plena del conocimiento del dominio jurídico involucrado) y el uso de lenguajes de programación lógica capaces de decidir en tiempo de ejecución, en la mayoría de casos existirá una primera fase de análisis y diseño de la aplicación que tendría que considerar las herramientas de formalización y de interpretación lógica indicadas a la recomendación anterior. Posteriormente se codificará un programa utilizando lenguajes y métodos de computación tradicionales, a menudo obedeciendo a criterios de eficiencia computacional y de coste.

Recomendación 3.3.

La interpretación lógica puede quedar formalizada en diversos momentos a lo largo del ciclo de vida del software que ofrece apoyo a la actuación administrativa automatizada:

- Una primera posibilidad es realizar y formalizar la interpretación lógica en la fase de análisis funcional y diseño del software. En este caso, la interpretación es un proceso llevado a cabo por un intérprete humano. El proceso generará un conjunto de casos que más tarde tienen que servir para codificar de forma informática el tratamiento de estos casos (la funcionalidad del programa que permite la actuación administrativa automatizada).

- Una segunda posibilidad, complementaria del anterior, consiste a realizar y formalizar la interpretación lógica en el momento de construir el software y, en concreto, en el proceso de codificación informática. Nuevamente la interpretación se un proceso llevado a cabo por un intérprete humano, pero en el mismo momento de producir el código del programa.

- Una tercera posibilidad es realizar y formalizar la interpretación lógica en forma de reglas a aplicar en el momento de ejecución del programa, sin que en el código del programa se encuentre ninguna lógica de funcionamiento de la aplicación. Constituye un ejemplo de esta tercera posibilidad la llamada programación lógica, basada en el uso de programas razonadores, como sucede en los llamados sistemas expertos y, más recientemente, en la Web semántica. Habrá que evaluar con mucho cuidado esta posibilidad, ya que estas técnicas presentan problemas de rendimiento.

- Una cuarta posibilidad es diseñar el sistema de manera tal que sea él mismo quien genere, a partir de la lectura y la comprensión de la norma jurídica, tanto la representación del conocimiento jurídico como las reglas de inferencia

lógica necesarias para aplicar las normas. Sólo en este caso podríamos considerar que existe una verdadera interpretación por parte de la máquina, que, a pesar del volumen de experiencias realizadas, especialmente en el dominio de la búsqueda de textos jurídicos, no consideramos practicable en la actualidad y por tanto, no recomendamos.

- Por otra parte, se tiene que considerar la utilidad de estas herramientas en los procesos de verificación del software producido. Efectivamente, una de las posibilidades más interesantes que ofrecen las herramientas lógicas que hemos presentado es, precisamente, la posibilidad de evaluar formalmente el programa que ofrece apoyo a la actuación administrativa automatizada, de forma integrada durante el proceso de construcción o como procedimiento de evaluación de la idoneidad del programa en momentos posteriores, durante el proceso natural de mantenimiento del programa, que en este caso ocurre particularmente relevando por el hecho que el sistema experimentará ordinariamente el impacto de los cambios normativos.

2.4.4. Recomendaciones sobre firma electrónica

Recomendación 4.1.	Analizar detalladamente los requisitos de firma de la aplicación en términos de autenticidad, integridad y confidencialidad. Por ejemplo, con la metodología PADS desarrollada por la Agencia Catalana de Certificación, una herramienta diseñada específicamente para analizar los requisitos en relación con los actos documentados que se producen dentro de los procesos y los procedimientos de la Administración y sus organismos y entidades, públicos o privados.

Recomendación 4.2.	Definir una normativa de firma electrónica que determine cómo se debe generar la firma de los actos automáticos, con qué certificados, qué controles se aplicarán para verificar los permisos y los privilegios, si la firma se sellará con la fecha y la hora, de qué manera se verificarán los certificados, qué algoritmos se podrán utilizar para firmar y, muy especialmente, qué quiere decir legalmente el acto de firmar y qué controles de software se aplicarán para garantizar la autenticidad de la voluntad del firmante.
Recomendación 4.3.	Desarrollar la normativa de firma electrónica en forma de estándares técnicos de niveles de firma (alto, medio y bajo), estándares de firma para los diferentes tipos de actas (resolver, expedir una copia, certificar, notificar, etc.), en guías de firma (PDF, ODF, Word, WS, S/MIME, etc.) y procedimientos de firma.

2.4.5. Recomendaciones sobre certificados de sello automático

Recomendación 5.1.	Analizar detalladamente los requisitos de certificación de la aplicación en términos de autenticidad, integridad y confidencialidad. Por ejemplo, con la metodología PADS desarrollada por la Agencia Catalana de Certificación, una herramienta diseñada específicamente para analizar los requisitos en relación con los actos documentados que se producen dentro de los procesos y los procedimientos de la Administración y sus organismos y entidades, públicos o privados.
Recomendación 5.2.	Utilizar certificados de sello de Administración pública, órgano o entidad público de elevada calidad y seguridad, preferiblemente

en hardware criptográfico con la seguridad certificada, de acuerdo con las normas ISO Common Criteria EAL4+ (con un perfil de protección adecuado, como CEN 14167) o FIPS 140-2 nivel 3.

Recomendación 5.3. Utilizar certificados de sello de Administración pública, órgano o entidad público sin datos personales del titular del órgano o cargo, ya que entonces sólo se podrán utilizar mientras esta persona mantenga la titularidad. La actuación administrativa automática permite que el funcionamiento del órgano, como unidad administrativa, se pueda mantener a pesar de la ausencia del titular, cosa que a opinión nuestra es una ventaja importante de esta figura legal.

Recomendación 5.4. Utilizar un sistema basado en doble certificado de sello, de manera que la posible pérdida de un certificado de sello no implique el paro de la operación del sistema de actuación administrativa automatizada.

Recomendación 5.5. Definir una normativa de certificación de clavo pública que recoja las recomendaciones anteriores y otras que la Administración pública considere necesarias con el fin de regular adecuadamente el ciclo de vida de los certificados de sello, ya que la posibilidad de llevar a cabo la actuación administrativa automatizada depende de la disponibilidad y la operatividad de los certificados.

Recomendación 5.6. Desplegar la normativa de certificación de clavo pública mediante estándares de certificación, tipo de certificados a adquirir o admitir, procedimientos de admisión de certificados, procedimientos de adquisición de certificados y de una base datos de certificados válidos.

2.4.6. Recomendaciones sobre seguridad y auditoria

Recomendación 6.1. Analizar detalladamente los casos de uso de seguridad del sistema, incluyendo al menos los siguientes:

- Casos de uso de autenticación de los actores y de la documentación gestionada por los sistemas.
- Casos de uso de firma electrónica de documentación por los actores.
- Casos de uso de firma electrónica de transporte seguro de mensajes entre actores y sistemas, como en el caso de la mensajería de servicios web entre sistemas remotos.
- Casos de uso de archivo de firma electrónica.
- Casos de uso asociados a las evidencias electrónicas, incluyendo los procedimientos judiciales y administrativos en papel.

Recomendación 6.2. Definir una normativa de seguridad criptográfica que especifique las normas de uso en relación con la criptografía, incluyendo estándares para implementarlos a la organización, ya que la actuación administrativa automatizada se basa en el uso de la criptografía y, por lo tanto, hay que regular el uso de manera apropiada con la legislación y las necesidades de la Administración pública o la entidad de derecho público.

Recomendación 6.3. Desplegar la normativa de seguridad criptográfica mediante estándares de implementación de infraestructura criptográfica, estándares y procedimientos en relación con los algoritmos seguros y guías de uso de la criptografía en las aplicaciones, con recomendaciones conformes a la legislación aplicable.

Recomendación 6.4. Definir una normativa de seguridad criptográfica que especifique las normas de uso en relación con la criptografía, incluyendo estándares para implementarlos a la organización,

ya que la actuación administrativa automatizada se basa en el uso de la criptografía y, por lo tanto, hay que regular el uso de manera apropiada con la legislación y las necesidades de la Administración pública o la entidad de derecho público.

Recomendación 6.5. Desplegar la normativa de gestión de claves mediante estándares de infraestructura técnica de gestión de claves, procedimientos previos a las operaciones de gestión de claves, procedimientos operativos de gestión de claves y procedimientos posteriores de gestión de claves.

Recomendación 6.6. Definir una normativa de desarrollo seguro aplicable a la aplicación de actuación administrativa automatizada y a la aplicación de firma electrónica que da soporte.

Recomendación 6.7. Implantar o ampliar la función de auditoría de calidad y de seguridad con el fin de velar por la aplicación de las normativas y el despliegue correspondiente. En particular, consideramos imprescindible auditar la aplicación del ciclo de vida del software (cuándo la aplicación sea de decisión), auditar el código y, en todo caso, auditar la aplicación de las medidas de seguridad y firma electrónica.

3. Análisis jurídico general de la automatización de los actos administrativos

Este capítulo trata de establecer los requisitos legales y de control técnico necesarios para hacer efectiva la automatización de los trámites en el marco del respeto a la legalidad vigente.

El objetivo de este análisis es ofrecer criterios y controles legales y tecnológicos iniciales en relación con la posibilidad de realizar trámites de manera automática y crear un marco de referencia que aporte la seguridad jurídica necesaria a esta nueva posibilidad legal.

Primero de todo hace falta, pues, diferenciar claramente los requisitos o requerimientos jurídicos y técnicos.

3.1. Los requisitos jurídicos de la actuación administrativa automatizada

Con respecto a los requerimientos jurídicos, hay que destacar la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos. De acuerdo con la disposición final primera, esta Ley atribuye carácter básico a una parte significativa de sus preceptos, al amparo del artículo 149.1.18.a de la Constitución, que atribuye al Estado la competencia sobre las bases del régimen jurídico de las administraciones públicas y sobre el procedimiento administrativo común.

Esta Ley ha representado un avance importante con respecto a la regulación de la administración electrónica en el Estado español. El rasgo principal es que reconoce el derecho de los ciudadanos a relacionarse con las administraciones públicas a través de medios electrónicos y, correlativamente, la obligación de las administraciones públicas de dotarse de medios y sistemas electrónicos a fin de que este derecho se

pueda ejercer. Tal como se reconoce en la exposición de motivos, «esta Ley pretende hacer el paso del podrán al deberán». Además, la Ley establece los principios que informan a la administración electrónica, regula los derechos de los ciudadanos, así como el uso de los medios electrónicos en relación con diferentes fases del procedimiento administrativo, y prevé los mecanismos de cooperación y colaboración interadministrativa para el impulso de la administración electrónica.

No obstante, a pesar del amplio contenido, la Ley no determina un modelo específico de administración electrónica, sino que configura o enumera los elementos básicos que informan el procedimiento administrativo y define los rasgos básicos de esta regulación desde la vertiente de garantías del ciudadano, de manera tal que concede a cada una de las administraciones públicas la libertad de escoger las opciones que considere más idóneas a la hora de configurar un procedimiento administrativo. Sea como sea, eso no podía ser de otra manera si se tiene en cuenta su carácter básico, que no puede agotar la capacidad normativa de la Comunidad Autónoma, sin perjuicio del hecho que, cuando hablamos del uso de los medios electrónicos, existe una importante vertiente autoorganizativa, concretada en las decisiones que adopta o puede adoptar cada Administración y que, en cualquier caso, tendrán que garantizar unos derechos básicos de los ciudadanos y un tratamiento administrativo común.

La disposición final 3a.3 de la Ley 11/2007 establece que, en el ámbito de las comunidades autónomas, los derechos de los ciudadanos recogidos en la misma Ley podrán ser ejercidos a partir del 31 de diciembre de 2009, siempre que la disponibilidad presupuestaria lo permita.

Tal como hemos indicado, una parte significativa de la Ley 11/2007 tiene carácter básico, aunque justamente la previsión del artículo 39 no la tiene, cosa que, en principio, permitiría que las comunidades autónomas, en desarrollo de políticas propias, incorporaran requerimientos diferentes de los establecidos legalmente a la Ley 11/2007. Sin embargo, podemos avanzar que difícilmente se podrá establecer un nivel de garantías inferiores a las que prevé aquel artículo, porque de lo contrario la seguridad jurídica podría salir maltrecha.

En este sentido, hay que recordar al tenor literal del artículo 39 de la Ley 11/2007: «En caso de actuación automatizada se tiene que establecer previamente el órgano u

órganos competentes, según los casos, para la definición de las especificaciones, programación, mantenimiento, supervisión y control de calidad y, si ocurre, auditoría del sistema de información y de su código fuente. Asimismo, se tiene que indicar el órgano que tiene que ser considerado responsable a los efectos de impugnación.»

A pesar de carecer de carácter básico, este artículo ya nos da los rasgos básicos que hay que considerar con respecto a la automatización de procesos, los cuales tendrán que ser tratados tanto desde la vertiente normativa como desde la vertiente técnica.

Desde la vertiente normativa, se tienen que analizar diferentes elementos enumerados en la norma no como mínimo normativo común desde el punto de vista básico, pero sí desde el punto de vista material o práctico: la competencia del órgano, que extenderá su actuación en relación con la definición de las especificaciones técnicas o los programas que tienen que dar respuesta a una actuación administrativa determinada.

Esta competencia que se configura desde el punto de vista inicial o primario también tendrá que verificar o asegurar el mantenimiento o la supervisión de estos programas y aplicaciones a efectos de asegurar la calidad o garantizar que no se pueda producir un mal funcionamiento. Hay que remarcar que, en definitiva, un mal funcionamiento derivaría en una actuación administrativa irregular susceptible de dar lugar a un supuesto de nulidad de pleno derecho o de anulabilidad (si bien también nos podríamos encontrar ante una mera irregularidad no invalidante, en función de los casos).

Finalmente, como garantía esencial del procedimiento administrativo común encontramos el derecho de revisión de los actos administrativos, regulado a los artículos 102 y siguientes de la Ley 30/1992, de 26 de noviembre, de régimen jurídico de las administraciones públicas y del procedimiento administrativo común.

Este derecho de revisión implica la capacidad que tiene el administrado o la administrada de reaccionar ante cualquier actuación administrativa que lo afecta con la finalidad de evitar situaciones de indefensión material que irían en contra de la tutela judicial efectiva garantizada por el artículo 24 de la Constitución española. Esta reacción se puede producir dentro del procedimiento administrativo mismo, mediante los recursos establecidos legalmente (sin perjuicio de la posibilidad de revisión de

oficio de los actos administrativos que puede llevar a cabo la Administración cuando se dan los supuestos establecidos legalmente), o ya en la vía judicial, mediante el control que llevan a cabo los tribunales de justicia de la legalidad de la actuación administrativa (tal como regula el artículo 106 de la Constitución).

Cuando nos encontramos ante la actuación administrativa automatizada, esta reacción del particular puede alcanzar dos vías de impugnación: por razones formales o por razones materiales o de fondo.

La diferenciación en cuanto a las vías de impugnación se produce también en el ámbito del procedimiento administrativo considerado tradicionalmente, aunque cuándo hablamos de actuación administrativa automatizada se ha de tener presente que, si bien los motivos de impugnación por razones materiales siempre serán los mismos –tanto si se trata de una actuación administrativa automatizada como si no –,[4] en el caso de la actuación administrativa automatizada la impugnación por razones formales es sustancialmente diferente. El motivo es que en la medida en que esta impugnación se centra en la adecuación al ordenamiento jurídico o la regularidad formal de la actuación administrativa, habrá que analizar justamente si la automatización de los procesos se ha llevado a cabo de manera correcta, cosa que supondrá evaluar, en primer lugar, la posibilidad de que esta automatización o eliminación de la voluntad humana sea factible, y, en segundo lugar, si las aplicaciones o los programas han sido configurados adecuadamente.

[4] Hay que tener presente que la actuación administrativa automatizada no produce sino un acto administrativo, configurado como declaración de voluntad, de conocimiento, de juicio o de deseo, que se encuentra sometido a unos requisitos de validez material y de eficacia que son los mismos tanto si nos encontramos ante actos administrativos de naturaleza presencial como realizados por medios electrónicos, y, por este motivo, su impugnación en este ámbito lo sería siempre por las mismas razones materiales o de fondo.

3.1.1. La actuación administrativa automatizada y la programación de esta actuación

Con respecto a la voluntad humana, o la declaración de voluntad, ya hemos comentado que, en el caso de la actuación administrativa automatizada, su formulación se traslada a la aplicación correspondiente. Sin embargo, eso no significa que aquélla desaparezca, porque la declaración de voluntad emanada existe igualmente, si bien se traslada a un momento temporal anterior, que es el de la programación de acuerdo con criterios que se podrían llamar de lógica jurídica. El anexo de la Ley 11/2007 lo reconoce de esta manera cuando define la aplicación como el «programa o conjunto de programas cuyo objeto es la resolución de un problema mediante el uso de informática».

Aunque se tiene que reconocer que la utilización del término problema no es muy acertada, describe claramente cuál es la finalidad de una aplicación: ofrecer una solución técnica a un planteamiento jurídico; es decir, establecer una programación determinada que garantice que la emisión de un acto administrativo concreto cumple los requerimientos materiales de contenido que el acto administrativo correspondiente tiene que garantizar.

En definitiva, se trata de trasladar al campo de la programación informática los elementos subjetivos, objetivos y formales que integran el acto administrativo correspondiente y garantizar que el acto administrativo responde a la misma finalidad que la que correspondería al mismo acto administrativo proveniente de una voluntad humana.

Siguiendo a GARCÍA DE ENTERRÍA, diferenciaremos cada uno de los elementos:

1) Elemento subjetivo. El acto administrativo debe proceder del titular apto del órgano competente de la Administración pública competente, por lo cual exige al mismo tiempo tres requisitos:

    a. Que proceda de una entidad de derecho público con capacidad y competencia para dictarlo.

b. Que proceda de un órgano competente objetiva, funcional y territorialmente para dictarlo. Así, el artículo 62.1 de la Ley 30/1992 dispone el siguiente: «Los actos de las administraciones públicas son nulos de pleno derecho en los casos siguientes: [...] Los que dicte un órgano manifiestamente incompetente en razón de la materia o del territorio.»
c. Aptitud del titular del órgano ante el órgano (cuando el titular ha sido adscrito) y ante las partes interesadas (siempre que no concurra ningún motivo de abstención del artículo 28.2 de la Ley 30/1992).

2) Elemento objetivo. El contenido del acto administrativo tiene que ser, como cualquier acto jurídico:

   a. Posible y lícito o ajustado al ordenamiento jurídico. Por eso, según el artículo 62, son nulos: «c) Los que tengan un contenido imposible. d) Los que sean constitutivos de infracción penal o se dicten como consecuencia de ésta.»
   b. Determinado o determinable.
   c. Adecuado a los fines que persigue y ajustado al ordenamiento jurídico.

3) Elemento causal. Lo integran dos elementos:

   a. La constatación del presupuesto de hecho que justifica que el acto se dicte.
   b. La causa en sentido estricto, que es la adecuación o la congruencia del acto con el fin que en él se persigue.

4) Elemento teleológico, de manera que si la Administración ejercita la potestad para un fin diferente del predeterminado por el derecho hablaremos de arbitrariedad o de desviación de poder.

Prácticamente todos estos elementos son trasladables a la automatización de procesos, si bien cada uno se tiene que diferenciar a la hora de tratar la automatización.

Con respecto a los elementos subjetivos, relacionados con el concepto de órgano administrativo, tenemos que enfocar la cuestión desde la vertiente del principio de

legalidad y la doctrina de las potestades administrativas, tal como trataremos de forma separada.

Contrariamente, los elementos objetivos son los que, en la medida en que se refieren al contenido del acto administrativo, tienen que derivar de lo que haya sido objeto de programación.

Ciertamente, la programación o la adecuación de un procedimiento administrativo determinado a la actuación automatizada tendrá que incluir tanto el elemento subjetivo como el elemento objetivo. A pesar de eso, mientras que el elemento subjetivo es una cuestión previa que está predeterminada y que se podría considerar que no varía, el elemento objetivo se producirá cada vez que se emita el acto administrativo, y su contenido no se puede encontrar predeterminado, sino que será consecuencia de los parámetros introducidos para su producción.

Por su parte, los elementos causal y teleológico concurren igualmente en cualquier acto administrativo. Su reflejo en la actuación administrativa automatizada se produce también en el ámbito de programación, en la medida en que ésta tiene que responder a una finalidad propia y específica del acto administrativo concreto. Además, el elemento teleológico se configura por el principio según el cual cualquier actuación administrativa tiene que responder a razones de interés general. Por lo tanto, cualquier vulneración informática de estos dos elementos podría suponer incurrir en una desviación de poder.

En este sentido, tan sólo una programación adecuada puede permitir que la producción del acto correspondiente respete las garantías formales y materiales necesarias y sea, consecuentemente, válido.

El artículo 44.2 de la Ley 26/2010, de 3 de agosto, de régimen jurídico y de procedimiento de las administraciones públicas de Cataluña, indica que "sólo son susceptibles de actuación administrativa automatizada los actos que se puedan adoptar con una programación basada en criterios y parámetros objetivos". Con esta previsión se pretende, por una parte, delimitar el ámbito de la automatización a estos supuestos en que se puedan predeterminar las condiciones de realización del acto de manera objetiva y, por otra parte, configura esta programación como el parámetro de

legalidad a controlar, lo que es relevante a la hora de valorar y, si ocurre, revisar la actuación administrativa realizada en base a esta programación.

3.1.2. El control de la actuacion administrativa automatizada

Es evidente que el principio de validez de los actos administrativos se puede trasladar a la actuación administrativa automatizada, y que el control de esta actuación administrativa pasará por el control de una programación adecuada. Se trata de discernir si la informática decisional que configura el acto administrativo produce un acto administrativo de manera apropiada.

Éste sería el control que se podría llamar *natural* del acto administrativo, si bien hay que añadir otro que se podría denominar *control previo* y que se relaciona con el principio de legalidad y la doctrina de las potestades administrativas.

3.1.3. La doctrina de las potestades administrativas

El concepto de *potestad* fue elaborado en contraste con el concepto de derecho subjetivo dentro de la categoría genérica de los poderes jurídicos o facultades de obrar atribuidos por el ordenamiento jurídico a los sujetos con respecto a intereses o bienes protegidos por este ordenamiento.

Así, a diferencia del derecho subjetivo, la potestad:

1) No deriva de una relación jurídica, sino directamente del ordenamiento jurídico.
2) No recae sobre ningún objeto determinado, sino que tiene un carácter genérico.
3) No se traduce en una pretensión concreta, sino en una posibilidad abstracta de producir efectos jurídicos.
4) Se corresponde con una situación de sumisión de otros sujetos a los eventuales efectos jurídicos derivados del ejercicio de la potestad.

5) No se atribuye en beneficio de su titular, sino de terceras personas, ya que la Administración tiene que ejercitar sus potestades para perseguir el interés público. Por este motivo, las potestades administrativas son potestades-función, lo cual excluye poderes absolutos.

Según GARRIDO FALLA, la potestad administrativa se puede definir como un poder de actuación genérico que, ejercido de acuerdo con las normas jurídicas, produce situaciones jurídicas en que quedarán obligados sujetos en que, con anterioridad, estaban simplemente en una situación abstracta de sumisión.

En cualquier caso, a fin de que la Administración pueda ejercitar cualquier potestad hace falta que previamente le haya sido atribuida por ley con carácter expreso y específico.

No obstante, la exigencia de carácter expreso se tiene que matizar con la doctrina de los poderes implícitos o inherentes del derecho anglosajón, de acuerdo con la cual aunque no se otorguen expresamente por la ley, se tienen que entender atribuidos aquellos poderes que sean implicación necesaria de los que se otorguen expresamente.

En cuanto al principio de legalidad como pilar fundamental del estado de derecho, hay que decir que no se caracteriza no tan sólo por el reconocimiento y la tutela de los derechos públicos subjetivos de los ciudadanos, sino también por la forma en que este objetivo se alcanza: mediante la sumisión de la Administración a la ley, que constituye el principio de legalidad y se formuló inicialmente concibiendo la ley como fuente y justificación de todas las actuaciones de los poderes ejecutivo y judicial.

La formulación inicial del principio de legalidad construida entorno a la exigencia de la ley previa partía de dos justificaciones bien claras:

1) En primer lugar, una general basada en la idea roussoniana de que la legitimidad del poder procede de la voluntad comunitaria cuya expresión típica es la ley.

2) En segundo lugar, el principio técnico de la división de poderes, por el cual el ejecutivo tiene como misión ejecutar la ley dictada por el legislativo.

Como indica MUÑOZ MACHADO[5], el legislador no es plenamente libre a la hora de decidir el grado de predeterminación con que tiene que utilizar las potestades administrativas por el hecho de que se requiere una densidad normativa mínima que, en determinadas materias, queda reservada a la ley. Eso se produce porque el legislador no puede dejar totalmente abiertas sus decisiones a fin de que la Administración las complete o las concrete, dado que eso significaría la ruptura de la reserva de ley, que exige que la ley regule con densidad suficiente las cuestiones principales que suscita la materia reservada.

Así pues, una regulación insuficiente rompería el principio de seguridad jurídica, la certeza de que tal principio impone a las normas, la previsibilidad de las consecuencias de la regulación, la igualdad de trato ante situaciones reiteradas que sean susceptibles de tratamiento igual, y la confianza legítima.

A la hora de analizar la doctrina de la potestad administrativa, en la fase 1 ya avanzamos que es esencial distinguir las potestades regladas de las potestades discrecionales.

3.1.4. Las potestades regladas y las potestades discrecionales

La ley puede determinar todas y cada una de las condiciones de ejercicio de la potestad o bien puede definir alguna de las condiciones de ejercicio de la potestad y dejar a la estimación subjetiva de la Administración el resto de condiciones (el cómo, el cuándo y el sentido).

Eso nos lleva a distinguir las potestades regladas de las discrecionales.

En relación con la discrecionalidad, se han formulado dos teorías:

---

[5] Muñoz Machado, S. Tratado de derecho administrativo y derecho público general I. Ed. Iustel, 2a edición, 2006, pág. 519.

1) Teoría de la vinculación negativa, según la cual se entiende permitido a la Administración aquello que la ley no le prohíbe. De esta manera, hay un "espacio libre de ley" en el cual la Administración opera discrecionalmente; por eso la actividad administrativa discrecional se desarrollaría siempre fuera de la ley y sería, por lo tanto, incontrolable por los tribunales.

2) Teoría de la vinculación positiva, de acuerdo con la cual se entiende prohibido a la Administración lo que no está permitido por la ley, de manera que toda la actividad administrativa tiene que estar cubierta por el derecho. Así, la actividad discrecional se desarrollará siempre dentro de la ley. No hay, pues, discrecionalidad al margen de la ley, sino sólo en virtud de ley y en la medida que la ley lo haya dispuesto.

Esta última es la teoría que ha sido reconocida mayoritariamente en el ámbito doctrinal y que se ampararía en el artículo 9 de la Constitución, que advierte que ésta garantiza el principio de legalidad y la interdicción de la arbitrariedad de los poderes públicos.

La exposición de motivos de la Ley de la jurisdicción contenciosa administrativa de 1956 consignaba el rasgo básico de la discrecionalidad: «la discrecionalidad surge cuando el ordenamiento jurídico atribuye a algún órgano la competencia para apreciar en un supuesto dado aquello que sea de interés general».

Por lo tanto, la discrecionalidad aparece por autorización legal. Por este motivo, en cualquier acto discrecional existen unos elementos reglados que actúan como límites, y que son los siguientes:

1) La existencia y la extensión de la potestad.
2) La competencia.
3) La forma.
4) El procedimiento.
5) La finalidad a perseguir en la actuación administrativa.
6) Los supuestos fácticos o de hecho.
7) Los principios generales del derecho.

3.1.5. La automatización de procesos

De acuerdo con lo que hemos expuesto, y trasladando estas reflexiones a la actuación administrativa automatizada, se puede hablar de discrecionalidad en un doble sentido: con carácter previo, y en relación con los actos administrativos discrecionales que puedan ser automatizados.

La discrecionalidad previa supone que, de la misma manera que la Administración puede determinar, en el marco de la ley, qué procedimientos se pueden tramitar electrónicamente e, incluso, al amparo de la previsión del artículo 27.6 de la Ley 11/2007, se puede imponer obligatoriamente la realización de estos procedimientos por medios electrónicos[6], la Administración correspondiente puede determinar discrecionalmente qué actos administrativos son susceptibles de automatización.

Si volvemos al anexo de la Ley 11/2007, observamos que define la actuación administrativa automatizada como aquella «actuación administrativa producida por un sistema de información adecuadamente programado sin necesidad de intervención de

[6] Cabe recordar que el apartado 4 del artículo 27 indica que "Reglamentariamente, las Administraciones Públicas podrán establecer la obligatoriedad de comunicarse con estas utilizando sólo medios electrónicos, cuando los interesados se correspondan con personas jurídicas o colectivos de personas físicas que con motivo de su capacidad económica o técnica, dedicación profesional u otros motivos acreditados tengan garantizado el acceso y la disponibilidad de los medios tecnológicos necesarios", previsión que, en el ámbito de la Administración de la Generalitat, ha concretado el artículo 13 del Decreto 56/2009, que, bajo la rúbrica "Obligatoriedad en el uso de los medios electrónicos", indica lo siguiente: "Mediante orden del consejero o consejera competente en la materia se puede imponer, por causas objetivas justificadas, a las personas jurídicas, públicas o privadas o colectivos de personas físicas, la obligación de utilizar sólo medios electrónicos para la comunicación con los entes previstos en la letra a) del artículo 2.1, siempre que por razón de la capacidad económica o técnica, dedicación profesional u otros motivos acreditados tengan garantizados el acceso y la disponibilidad de los medios electrónicos necesarios."

una persona física en cada caso singular. Incluye la producción de actos de trámite o resolutorios de procedimientos, así como de meros actos de comunicación».

De este concepto, podemos extraer dos conclusiones: en primer lugar, la supresión de la intervención de la persona física en la actuación administrativa materialmente considerada, y, en segundo lugar, el concepto omnicomprensivo que se contiene en la definición.

Eso significa que la Administración dispone de la potestad discrecional de automatizar los procesos en el marco de la normativa vigente.

3.1.6. El marco normativo en relación con la automatización de procesos

La normativa vigente contiene una norma habilitante genérica, configurada por el artículo 39 de la Ley 11/2007, que, con respecto a la Administración de la Generalitat, ha sido desplegada por el artículo 34 del Decreto 56/2009[7]. Es al amparo de esta habilitación legal que se puede proceder a la automatización de procesos.

Igualmente, el artículo 44.1 de la Ley 26/2010, de 3 de agosto, de régimen jurídico y procedimiento de las admnistraciones públicas de Cataluña indica que "Las administraciones públicas catalanas pueden hacer actuaciones automatizadas para

[7] Este artículo 34 indica: “El ejercicio de la competencia mediante la actuación administrativa automatizada.

1. Los entes previstos en la letra a) del artículo 2.1 deben impulsar la automatización de los procesos que por sus características y por razones de eficiencia lo justifiquen, sin que se produzca ninguna reducción de garantías del administrado o la administrada y, en su caso, determinando el órgano responsable a efectos de impugnación.

2. El departamento competente en materia de administración electrónica, con la colaboración del Centro de Telecomunicaciones y Tecnologías de la Información, establece los requerimientos técnicos y formales de los sistemas que automaticen la actuación administrativa. Asimismo, determina los criterios de programación, mantenimiento, supervisión y control de calidad de estos sistemas."

constatar la concurrencia de los requisitos que establece el ordenamiento jurídico, declarar las consecuencias previstas, adoptar las resoluciones y comunicar o certificar los datos, los actos, las resoluciones o los acuerdos que consten en sus sistemas de información, mediante la utilización del sistema de firma electrónica que determinen".

De conformidad con este marco normativo, estatal y autonómico, nos encontramos con un nivel de regulación doble: la normativa estatal, que se puede considerar meramente posibilitadora de esta automatización, y la normativa autonómica. Por esta razón es necesario un despliegue efectivo en que se concreten las condiciones de ejercicio, ya sea con normas de carácter reglamentario, ya sea con normas que, con rango de ley, desarrollen políticas propias.

Eso es lo que ha hecho la Administración de la Generalitat de Catalunya, con el artículo 44 de la Ley 26/2010, y la previsión reglamentaria mencionada antes, sin perjuicio del hecho de que, tal como se desprende del análisis del mismo Decreto, éste haya adoptado una fórmula que se puede considerar nueva a la hora de enfocar las soluciones técnicas, la cual pasa por la desreglamentación formal de los aspectos técnicos.

La regulación que se hace en el Decreto 56/2009 se apoya en una concepción innovadora en la medida en que se despliegan, con rango reglamentario, los aspectos básicos que hay que considerar a la hora de implementar o incorporar la tramitación electrónica al procedimiento administrativo.

No obstante, se produce una descarga de los aspectos más técnicos y cambiantes. Éstos se remiten a unos protocolos que, en cada uno de sus ámbitos, son aprobados por los titulares de los departamentos correspondientes y objeto de publicación en la sede corporativa[8].

La voluntad de la regulación es evitar una reglamentación excesiva sin que se produzcan problemas de seguridad jurídica. Este objetivo se quiere alcanzar no tan

[8] Se trata de los protocolos de trámites y servicios, el protocolo de interoperabilidad, el protocolo de firma y el protocolo de archivos.

sólo con la transparencia derivada de la publicidad en la sede corporativa de los protocolos correspondientes, sino también mediante un procedimiento de elaboración en que se garantiza la intervención de un órgano corporativo competente en materia de recursos comunes de los departamentos, la Comisión de Coordinación Corporativa, regulada por el Decreto 146/2007. La finalidad es que, en ámbitos como los que son objeto de regulación en el decreto objeto de informe, las soluciones adoptadas se puedan aplicar o trasladar al conjunto de los organismos de la Administración de la Generalitat.

Como hemos indicado, la aprobación de estos protocolos la lleva a cabo cada uno de los departamentos competentes por razón de la materia: atención ciudadana, administración electrónica, archivos. Con respecto a la actuación administrativa automatizada, se prevé igualmente que el Departamento competente en materia de administración electrónica establezca los requerimientos técnicos y formales de los sistemas que automaticen la actuación administrativa, así como los criterios de programación, mantenimiento, supervisión y control de calidad de los sistemas.

Con respecto a esta desreglamentación, la Comisión Jurídica Asesora, en el Dictamen 22/2009, emitido en relación al Proyecto de decreto, matizó estos protocolos indicando lo siguiente: «Aparece así un tercer nivel normativo que, vista la complejidad tecnológica de la materia, tendría que cumplir la función de establecer las normas y los procedimientos más técnicos que posibilitaran el uso de los medios electrónicos en el sector público. Sin embargo, no es éste el único cometido de los protocolos, o, al menos, no se deduce claramente de las diferentes remisiones del Proyecto; y en ocasiones estos protocolos parecen, más bien, estar llamados a regular incluso ámbitos reservados a la ley [...] en Consecuencia, esta Comisión tiene que concluir, formulando la observación con carácter esencial, que existe la necesidad de que, en el Proyecto, por una parte, se clarifique la naturaleza normativa de estos protocolos y se señale si son aprobados o no mediante un reglamento en los términos previstos en el artículo 40.1 de la Ley 13/2008, de 5 de noviembre, de la Presidencia de la Generalitat y del Gobierno. («Las disposiciones reglamentarias dictadas por el Gobierno o por el presidente o presidenta de la Generalitat adoptan forma de decreto. Las disposiciones reglamentarias dictadas por los consejeros adoptan forma de orden.») en este sentido, una esmerada definición clara y segura del concepto, naturaleza, procedimiento y alcance del protocolo como instrumento de intervención,

ya sea en el cuerpo del texto o en el glosario a que se alude al final del fundamento jurídico siguiente, puede contribuir a aclarar las dudas que la suya previsión suscita.

Por otra parte, y en la medida en que no existe una ley previa, hay que delimitar más esmeradamente el contenido de cada uno de estos protocolos a fin de que éste se ciña a regular los aspectos más técnicos del uso de los medios electrónicos en cada uno de los ámbitos sobre los cuales se proyectan, eso es, los criterios operativos de actuación (art. 6.3), y que se les imposibilite, con eso, a suplir funcionamiento y materialmente los ámbitos propios de la ley.»

Según eso, la Comisión Jurídica Asesora admite la viabilidad jurídica de los protocolos mencionados, si bien somete esta posibilidad a un condicionante doble:

- Por una parte, los protocolos se deben ceñir, en su contenido, a la regulación de aspectos técnicos y organizativos.
- Por otra parte, haría falta delimitar la naturaleza jurídica y admitir la consideración de estos protocolos como disposiciones de carácter general.

En este sentido, incorporando las previsiones de la Comisión Jurídica Asesora, se introdujeron unas modificaciones en el texto del Proyecto que delimitaban el concepto y el contenido de estos protocolos y determinaban la naturaleza jurídica.

Este marco se puede trasladar igualmente a la automatización de procesos en la medida que, al amparo de una previsión legal habilitante, de carácter estatal o autonómico, y una habilitación reglamentaria, se puede llevar a cabo la automatización de procesos en el marco legal establecido, sin que sea necesario que todos los elementos técnicos estén recogidos a las normas mencionadas anteriormente. Sin embargo, sí que hará falta que un instrumento normativo de nivel inferior recoja o regule estos aspectos técnicos o de detalle que, por su naturaleza, no es recomendable que se incluyan en una norma legal o reglamentaria la cual es mucho más difícil de adaptar o adecuar a las circunstancias técnicas que vayan variando.

Estas mismas reflexiones se podrían trasladar al ámbito local, en el que la potestad reglamentaria manifestada mediante la aprobación de las ordenanzas locales es expresión de la potestad normativa que caracteriza igualmente estos entes locales territoriales. De acuerdo con eso, serían las ordenanzas correspondientes los que podrían concretar, en un primer nivel, las condiciones en que la automatización de procesos sería viable desde el punto de vista jurídico, siempre al amparo de la previsión legal correspondiente, ya sea la del artículo 39 de la Ley 11/2007, ya sea la de la norma legal autonómica correspondiente. En un segundo nivel habría instrumentos normativos de rango inferior (cómo podría ser un decreto de alcaldía) que podrían contener los elementos técnicos y organizativos mutables.

Esta posibilidad de que sea una norma autonómica la que concrete con rango legal las condiciones de automatización deriva del carácter no básico del artículo 39 de la Ley 11/2007, sin perjuicio de la necesaria reserva de ley que existe en la materia, ya que, según los artículos 103.1 y 2 de la Constitución, las decisiones organizativas se tienen que adoptar de acuerdo con una ley. Por otra parte, como prevé el artículo 84 del Estatuto de autonomía de Cataluña, también las leyes son las que establecen las competencias propias de los entes locales.

En definitiva, la regulación del uso de medios electrónicos ante la Administración requiere una ley que establezca el primer marco normativo, el cual dota de estabilidad y de previsibilidad las normas inferiores que lo tienen que ejecutar, además de cumplir con las reservas funcionales y materiales exigidas. En efecto, ya se ha dicho que el ordenamiento jurídico exige, para una regulación completa y estable de esta materia, una ley previa, la cual es la llamada a perfilar las bases del modelo de administración electrónica a aplicar, a desarrollar el contenido y el ejercicio de los derechos de los ciudadanos en la relación con la Administración y a vincular, si fuera el caso, con obligaciones concretas, las administraciones locales en cuanto al uso de medios electrónicos en sus relaciones internas y las comunicaciones recíprocas con otras administraciones.

Esta función es la que desarrolla la Ley 11/2007, sin perjuicio que las comunidades autónomas, como es el caso de Cataluña, al amparo de la previsión del artículo 111

del Estatuto de Autonomía[9], pueda desarrollar políticas propias y, incluso, establecerlas como aplicables en relación con todas las administraciones públicas catalanas.

En cualquier caso, esta extensión de la norma no es ilimitada, sino que queda condicionada a una serie de límites, uno de los cuales es el de la autonomía local[10].

El principio constitucional de autonomía implica que los municipios y las provincias han de tener un mínimo de competencias que se puede considerar irreductibles en la medida en que, si bien se pueden reordenar, no pueden ser eliminadas completamente (STC 32/1981, FJ 3º). Además, «esa reordenación no puede afectar en el contenido competencial mínimo [...] garantizado como imperativo de la autonomía local» [STC 214/1989, FJ 4 t b)]. En este sentido, «el legislador puede disminuir o acrecentar laso competencias hoy existentes, pero no eliminarlas miedo entero, y, lo que se más, el debilitamiento de su contenido sólo puede hacerse cono razón suficiente y nunca en daño del inicio de autonomía» [STC 32/1981, FJ 3º; STC 214/1989, FJ 13 c)].

La STC 32/1981 ya estableció una doctrina que el Tribunal Constitucional ha recogido reiteradamente en pronunciamientos posteriores: «Como titulares de un derecho a la autonomía constitucionalmente garantizada, las comunidades locales no pueden ser dejadas en lo que toca a la definición de sus competencias y la configuración de sus

---

[9] "En las materias que el Estatuto atribuye a la Generalitat de forma compartida con el Estado, corresponden a la Generalidad la potestad legislativa, la potestad reglamentaria y la función ejecutiva, en el marco de las bases que fije el Estado como principios o mínimo común normativo en normas con rango de ley, excepto en los supuestos que se determinen de acuerdo con la Constitución y el presente Estatuto. En ejercicio de estas competencias, la Generalitat puede establecer políticas propias. El Parlamento debe desarrollar y concretar a través de una ley aquellas previsiones básicas."

[10] Cabe recordar que el artículo 159.2 del Estatuto de Autonomía de Cataluña atribuye a la Generalidad la competencia compartida en materia de régimen jurídico y procedimiento de las administraciones públicas catalanas y, de acuerdo con el apartado 6 del mismo artículo, las competencias de la Generalitat especificadas en los apartados 1, 3, 4 y 5 deben ejercerse respetando el principio de autonomía local.

órganos de gobierno a la interpretación que cada comunidad autónoma pueda hacer de ese derecho [...] La garantía constitucional es de carácter general y configuradora de un modelo de Estado, y ello conduce, como consecuencia obligada, a entender que corresponde al mismo la fijación de principios o criterios básicos en materia de organización y competencia de general aplicación en todo el Estado.»

Sin embargo, la normativa estatal básica, por aplicación del artículo 149.1.18 CE, se articula en relación con dos elementos fundamentales que integran esta garantía institucional, que son la estructura organizativa y el régimen de competencias. En definitiva, como señala reiteradamente el Tribunal Constitucional, lo que es materialmente básico son todas aquellas cuestiones relacionadas con la autonomía consagrada constitucionalmente, es decir, estructura orgánica y, especialmente, competencial de las entidades locales.

Asimismo, como aprecia la STC 27/1987, la autonomía local no impide establecer fórmulas de relación interadministrativa que comporten la coordinación de los entes locales en el ámbito autonómico que, sin menoscabar las competencias de las entidades locales, supongan un límite de éstas cuando se fijen medios o sistemas de relación que hagan posible la información recíproca, la homogeneidad técnica en determinados aspectos y la acción conjunta y, en definitiva, se eviten contradicciones y se reduzcan disfunciones. Por esta razón, la coordinación puede constituir igualmente un límite al pleno ejercicio de las competencias propias de las corporaciones locales.

Trasladando estos principios al ámbito de la administración electrónica y, en particular, a la actuación administrativa automatizada, tenemos que concluir que cada Administración pública estatal, autonómica o local ha de tener un margen de autonomía amplio a la hora de configurar los criterios de automatización y, con rango de ley, los únicos límites a establecer serían aquéllos que hagan posible la homogeneidad técnica en determinados aspectos y la interoperabilidad.

3.1.7. Los derechos de los ciudadanos como límite de la automatización

Naturalmente, hay otros límites que se tienen que respetar, como los derechos que reconoce el ordenamiento jurídico a los ciudadanos en sus relaciones con las administraciones públicas. Con respecto a estos derechos, la Ley 11/2007 recoge, en el artículo 4, dentro de los principios generales, el «principio de legalidad en cuanto al mantenimiento de la integridad de las garantías jurídicas de los ciudadanos ante las administraciones públicas establecidas a la Ley 30/1992, de régimen jurídico de las administraciones públicas y del procedimiento administrativo común, cosa que comporta una reserva de ley con respecto al mantenimiento de estas garantías de que tiene que disfrutar la ciudadanía».

Se tienen que añadir igualmente los principios que la Ley 29/2010, del 3 de agosto, del uso de los medios electrónicos en el sector público de Cataluña, en su artículo 4, reconoce y que informan la incorporación de los medios electrónicos en las actuaciones del sector público de Cataluña. Estos principios, aunque no son exclusivos de la automatización de los procesos, son aplicables a ésta, dado que la automatización es una manifestación más de la incorporación de los medios electrónicos a la actuación administrativa.

En resumidas cuentas, la automatización de procesos, como una manifestación más de la adaptación de los procedimientos presenciales a su tramitación electrónica, requiere una norma habilitante, con rango de ley, que así lo posibilite. Además, esta habilitación tiene que contener las especificaciones necesarias que establezcan las condiciones de ejercicio y que, simultáneamente, garanticen los derechos de los ciudadanos.

Estos derechos de los ciudadanos resultarían garantizados con la posibilidad de reaccionar contra el acto administrativo emitido, ya sea por razones de carácter sustantivo, relacionadas con el contenido intrínseco del acto producido, ya sea por razones de carácter formal, relativas al proceso de automatización mismo.

3.1.8. Control de la automatización

Ya hemos indicado que este proceso de automatización es una decisión discrecional y, como tal, susceptible de control de acuerdo con los parámetros que se detallan acto seguido.

1) La existencia y la extensión de la potestad.

No habría problemas jurídicos cuando existiera la norma habilitante. Actualmente se puede considerar que el artículo 39 de la Ley 11/2007 no es suficiente, puesto que requiere que se desarrolle o se concrete el contenido.

2) La competencia, la forma y el procedimiento.

Se trataría de elementos del acto administrativo que responderían a lo que tendría que ser una programación adecuada, con coherencia entre los aspectos técnicos y los jurídicos.

3) La finalidad a perseguir en la actuación administrativa.

Es evidente que la actuación administrativa tiene que responder a una persecución del interés general, sin perjuicio de las finalidades particulares o los bienes jurídicos que tiene que proteger la actuación administrativa concreta.

En principio, la actuación administrativa automatizada no plantearía ninguna diferencia con respecto a una actuación administrativa no automatizada, exceptuando el caso de que se aprovechara esta automatización para alterar las condiciones de ejercicio, en perjuicio del administrado o la administrada.

4) Los supuestos fácticos o de hecho.

En el caso de la actuación administrativa automatizada, responderían a un supuesto doble: en primer lugar, los supuestos fácticos o de hecho que justifican la actuación administrativa propiamente dicha, al margen de su forma de realización; en segundo lugar, desde un punto de vista más técnico, estaría la comprobación de las

condiciones de programación que han condicionado o predeterminado un resultado o una respuesta automática de la máquina.

5) Los principios generales del derecho.

Como criterio general, los principios generales del derecho administrativo son aplicables y, en caso de que nos ocupa, tendrían, en particular, su manifestación en el con respecto a todos y cada uno de los principios generales que la utilización de los medios electrónicos requiere con carácter específico[11], y, en general, el respeto a todos los derechos que, con carácter general, reconoce el ordenamiento jurídico a los administrados en sus relaciones con la Administración.

3.1.9. La planificación de la actuación administrativa

Otro elemento a considerar es la posibilidad de que la Administración planifique o programe la actuación administrativa. Esta potestad planificadora, esencialmente discrecional, significa el establecimiento de un programa o de una planificación que predeterminará el contenido de los actos administrativos emitidos por los órganos administrativos.

Eso supone la transformación de una potestad discrecional en reglada, que es justamente lo que se produce con la automatización de procesos, en qué potestades originariamente discrecionales pasan a ser regladas como consecuencia de una planificación determinada o, incluso, en sentido estricto, de una programación determinada.

Esta diferencia no es meramente aparente, ya que mientras que en las potestades discrecionales existen diferentes posibilidades, todas igual de válidas, en las potestades regladas hay una única posibilidad, porque la programación informática

[11] Se trataría, fundamentalmente, los principios generales enumerados en el artículo 4 de la Ley 11/2007.

realizada tendrá que responder de manera idéntica a todas las situaciones en que concurran los requisitos establecidos jurídicamente y técnicamente.

Eso nos llevaría, con una automatización de procesos llevada a cabo adecuadamente, a un cumplimiento mucho más estricto del principio de igualdad, que garantiza el trato igual a los iguales. No obstante, es evidente que el límite se encontrará en la base de la programación, dado que existe un núcleo duro de las decisiones administrativas que difícilmente se podrá automatizar.

En cualquier caso, tal como exponemos, las previsiones legales relativas a la automatización de los actos administrativos son genéricas, con respecto a la tipología de actas susceptibles de automatizar, lo que permite un margen amplio de discrecionalidad a la hora de tomar esta decisión, siempre con el necesario cumplimiento de todos los parámetros y condiciones previas que la justifiquen y con pleno con respecto a los principios y garantías a observar.

3.2. La programación de la actuación administrativa automatizada

Ya hemos comentado que los requerimientos jurídicos y los técnicos son esenciales a la hora de articular el procedimiento administrativo electrónico. Con respecto a la automatización, la programación trata de dar respuesta a dos planteamientos: el derivado de la tramitación electrónica propiamente dicha y el derivado de la automatización en la producción del acto administrativo estrictamente.

3.2.1. La aprobación de los programas y las aplicaciones

En los dos casos, se tiene que plantear si se requiere la aprobación y la publicación de los programas y las aplicaciones tal como se exigía antes de que entrara en vigor la Ley 11/2007 o si, contrariamente, la aprobación y la publicación ya no son necesarias.

Podemos avanzar que la aprobación de los programas y las aplicaciones es necesaria, porque, a pesar del silencio de la Ley 11/2007[12], la normativa puede exigir esta aprobación (cómo pasa en determinados ámbitos) e, independientemente de que esta previsión acabe siendo superada, siempre tendrá que existir un acto aprobatorio, más o menos formal, por parte del órgano administrativo competente, de estos programas y aplicaciones. Una cuestión diferente será la publicidad y la transparencia que se puedan exigir a estos actos aprobatorios.

Como planteamiento previo, la Ley 11/2007 ha derogado algunos preceptos de la Ley 30/1992. Entre éstos está el artículo 45.4, que decía el siguiente: «Los programas y las aplicaciones electrónicas, informáticas y telemáticas que tengan que ser utilizados por las administraciones públicas para el ejercicio de sus potestades tienen que ser previamente aprobados por el órgano competente, el cual tiene que difundir públicamente las características.»

No obstante, la Ley 11/2007 no indica si, a partir de esta derogación, se han hecho innecesarias la aprobación y la publicación de los programas. Tan sólo trata la cuestión en el artículo 39, relativo a la actuación administrativa automatizada de conformidad con el cual habrá un órgano regulador «[...] para la definición de las especificaciones, programación, mantenimiento, supervisión y control de calidad y, si ocurre, auditoría del sistema de información y de su código fuente. Asimismo, se tiene que indicar el órgano que tiene que ser considerado responsable a los efectos de impugnación».

Eso significaría que, al margen de lo que se pueda entender con carácter general en el ámbito de los procedimientos administrativos tramitados electrónicamente, en el ámbito de la actuación administrativa automatizada no se ha eliminado la obligación de aprobación, sin perjuicio que sean los órganos correspondientes los que regulen el

[12] El Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, no contiene ninguna previsión al respecto, aunque deroga el Real Decreto 263/1996, de 16 de febrero, que regulaba la utilización de técnicas electrónicas, informáticas y telemáticas por parte de la Administración General del Estado, que exigía a todos los efectos la aprobación y la publicación de los programas y las aplicaciones.

sistema de aprobación y difusión de los programas y las aplicaciones utilizados en cada caso. Sea como sea, se trataría de una cuestión ligada a la potestad autoorganizativa de cada una de las administraciones.

Evidentemente, esta aprobación tiene que disponer previamente de los informes técnicos pertinentes que aseguren la legalidad de la aplicación, la seguridad, la normalización de los medios de acceso y la conservación de los soportes utilizados.

Si analizamos otras normativas, comprobamos que, en el ámbito del Principado de Asturias, para adaptarse a la Ley 11/2007 se aprobó el Decreto 115/2008, de 20 de noviembre, de modificación del Decreto 111/2005, de 3 de noviembre, sobre registro telemático.

No obstante, la cuestión es tratada tan sólo tangencialmente:

«Los registros telemáticos recibirán las solicitudes, escritos y comunicaciones que le sean presentados siempre que se cumplan las siguientes condiciones:
a) Que las solicitudes, escritos y comunicaciones se soporten en los formularios electrónicos habilitados en el efecto para cada uno de los trámites, servicios o procedimientos.
b) Que se utilicen los sistemas de identificación electrónica y de firma electrónica admitidos en cada caso en la norma reguladora del registro.

Para cada servicio, procedimiento o trámite podrá admitirse más de un sistema de identificación electrónica y, en su caso, de firma electrónica.»

Más adelante se define el formulario electrónico como «un documento electrónico estructurado, con campos de información predefinidos, que sirve de soporte para la carga de las solicitudes, escritos y comunicaciones referidas en trámites o procedimientos administrativos susceptibles de recepción y remisión mediante registro telemático y que se encuentra disponible a tal efecto en el portal o la intranet corporativos de la Administración del Principado de Asturias».

Así pues, a pesar de la derogación expresa del artículo 45.4 de la Ley 30/1992 y el silencio de la Ley 11/2007, se indica que los trámites, los servicios o los

procedimientos se llevarán a cabo en los «formularios habilitados en el efecto» y disponibles en «el portal o la intranet corporativos de la Administración del Principado de Asturias».

Con respecto a Cataluña, el Decreto 56/2009 prevé la aprobación del procedimiento y, implícitamente, de los programas y las aplicaciones que dan apoyo. No obstante, se establece que sea el director o la directora de servicios de cada uno de los departamentos, u órganos equivalentes, quien determine o acredite el cumplimiento del protocolo correspondiente a la hora de autorizar la incorporación de un procedimiento o de un servicio determinado a la tramitación electrónica y su utilización por parte del ciudadano.

Juzgamos correcto este criterio de la necesaria aprobación de los programas y las aplicaciones: por una parte, en la medida que respeta la existencia necesaria de un acto administrativo aprobatorio, de acuerdo con la doctrina de las potestades administrativas y de la vinculación positiva; y, por otra parte, porque incluye la existencia necesaria de un informe técnico favorable del Centro de Telecomunicaciones y Tecnologías de la Información, hecho que garantiza igualmente el cumplimiento de las garantías técnicas[13].

---

[13] El artículo 10 del Decreto 56/2009 dispone: "1. La tramitación electrónica de cualquier servicio requiere la evaluación y aprobación del cumplimiento del protocolo de servicios y trámites electrónicos, en cuanto a los aspectos técnicos y de gestión de los programas y aplicaciones que lo ejecuten. Esta aprobación la hace el órgano competente, previo informe técnico favorable a que se refiere el apartado 3, así como el correspondiente informe organizativo.

2. Es competente para la aprobación de los programas y aplicaciones al director o directora de servicios de cada departamento u órgano equivalente. En el caso de los organismos autónomos, entidades de derecho público vinculadas o dependientes y otros entes incluidos en el ámbito de aplicación de este Decreto, se debe tener en cuenta lo dispuesto en sus normas reguladoras.

3. Los programas y aplicaciones que dan soporte a la tramitación electrónica requieren un informe técnico favorable del Centro de Telecomunicaciones y Tecnologías de la Información, mediante las áreas TIC de cada departamento, en relación con las especificaciones sobre la

Igualmente, en el campo de la contratación administrativa, el Decreto 96/2004, de 20 de enero, por el cual se regula la utilización de los medios electrónicos, informáticos y telemáticos en la contratación de la Administración de la Generalitat, prevé la aprobación de programas y aplicaciones, en el artículo 12.1[14].

Al margen de lo que establezcan o no establezcan con carácter general la Administración general del Estado y las comunidades autónomas, hay que mencionar, igual que en el caso de la contratación pública, ámbitos específicos de regulación en que la materia está regulada de manera que se podría calificar de completa.

Éste es el caso del ámbito tributario, en el cual la Ley 58/2003, general tributaria, de 17 de diciembre, indica, en el artículo 96 («utilización de tecnologías informáticas y

---

adecuación del programa o la aplicación a este Decreto y las disposiciones dictadas en su desarrollo, y en particular:

a) La seguridad de la aplicación: preservación de la disponibilidad, de la confidencialidad y de la integridad de los datos tratados por la aplicación.

b) La normalización de los sistemas de acceso: especificaciones técnicas sobre los medios, códigos y formatos de acceso.

c) La conservación de los formatos utilizados: proporción entre la durabilidad de los formatos y el tiempo en que los datos han de mantener incluidos.

d) La interoperabilidad y reutilización de la aplicación.

4. Una vez cumplidos los requisitos del apartado 1, el servicio se incorpora a la sede electrónica corporativa y está a disposición de los ciudadanos y ciudadanas."

[14] "Los programas y las aplicaciones informáticas para la gestión de la contratación de los departamentos, organismos autónomos y empresas públicas deben ser objeto de aprobación por Orden del / de la consejero / a de Economía y Finanzas, previos los informes técnicos de la Comisión de Coordinación Interdepartamental de Gestión y de Tecnologías de la Información y Comunicaciones y de la Agencia Catalana de Certificación y el informe de la Junta Consultiva de Contratación Administrativa. Estos programas y aplicaciones deben contener las políticas de seguridad y las especificaciones técnicas que aseguren la efectividad de los controles criptográficos de firma electrónica exigidos por el artículo 7 y los controles criptográficos de cifrado exigidos por el artículo 8 de este Decreto, así como los mecanismos de seguridad, algoritmos, longitudes de claves y procedimientos de auditoría del sistema que permitan certificar el secreto de las proposiciones hasta el momento en que proceda su apertura."

telemáticas»): «1. La Administración tributaria tiene que promover la utilización de las técnicas y los medios electrónicos, informáticos y telemáticos necesarios para el desarrollo de su actividad y el ejercicio de sus competencias, con las limitaciones que la Constitución y las leyes establezcan.»

El mismo precepto establece, a continuación, lo siguiente: «2. Cuando sea compatible con los medios técnicos de que disponga la Administración tributaria, los ciudadanos se pueden relacionar para ejercer sus derechos y cumplir sus obligaciones a través de técnicas y medios electrónicos, informáticos o telemáticos con las garantías y los requisitos previstos en cada procedimiento.

3. Los procedimientos y las actuaciones en que se utilicen técnicas y medios electrónicos, informáticos y telemáticos tienen que garantizar la identificación de la Administración tributaria actuante y el ejercicio de su competencia. Además, cuando la Administración tributaria actúe de forma automatizada se garantiza la identificación de los órganos competentes para la programación y supervisión del sistema de información y de los órganos competentes para resolver los recursos que se puedan interponer.

4. Los programas y las aplicaciones electrónicos, informáticos y telemáticos que tengan que ser utilizados por la Administración tributaria para el ejercicio de sus potestades tienen que ser aprobados previamente por ésta en la forma que se determine por reglamento.

5. Los documentos emitidos, sea cuál sea su soporte, por medios electrónicos, informáticos o telemáticos por la Administración tributaria, o los que ésta emita como copias de originales almacenados por estos mismos medios, así como las imágenes electrónicas de los documentos originales o sus copias, tienen la misma validez y eficacia que los documentos originales, siempre que quede garantizada la autenticidad, integridad y conservación y, si ocurre, la recepción por parte del interesado, así como el cumplimiento de las garantías y los requisitos exigidos por la normativa aplicable.»

El Real decreto 1065/2007, de 27 de julio, por el cual se aprueba el Reglamento general de las actuaciones y los procedimientos de gestión e inspección tributaria y de

despliegue de las normas comunes de los procedimientos de aplicación de los tributos, establece, en el artículo 85 («aprobación y difusión de aplicaciones»):

«1. En los supuestos de actuación automatizada a que se refiere el artículo anterior, las aplicaciones informáticas que efectúen tratamientos de información cuyo resultado sea utilizado por la Administración tributaria para el ejercicio de sus potestades y por las cuales se determine directamente el contenido de las actuaciones administrativas, tienen que ser previamente aprobadas mediante una resolución del órgano que tiene que ser considerado responsable a los efectos de la impugnación de los correspondientes actos administrativos. Cuando se trate de diferentes órganos de la Administración tributaria no relacionados jerárquicamente, la aprobación corresponde en el órgano superior jerárquico común de la Administración tributaria de que se trate, sin perjuicio de las facultades de delegación establecidas en el ordenamiento jurídico.

2. Los interesados pueden conocer la relación de las mencionadas aplicaciones mediante consulta en la página web de la Administración tributaria correspondiente, que tienen que incluir la posibilidad de una comunicación segura de conformidad con lo que prevé el artículo 83.3.»

En esta línea, la Resolución de 16 de abril de 2004, de la Dirección General de la Agencia Estatal de Administración Tributaria, regula la generación y el archivamiento de documentos electrónicos a partir de documentos en soporte papel, así como la emisión de copias en papel de estos documentos electrónicos, y aprueba los programas y las aplicaciones a utilizar, al amparo del Real decreto 263/1996, como indica su exposición de motivos. Habrá que ver en qué medida el Real decreto 1671/2009 afecta a esta normativa.

Existen otros ámbitos jurídicos en que también se regula la aprobación de aplicaciones, como el tráfico y la Seguridad Social.

En relación al tráfico, hay que hacer referenciaa la Resolución de 27 de marzo de 2006, de la Dirección General de Tráfico, por la cual se aprueban las aplicaciones de los registros en soporte informático de la Dirección General de Tráfico utilizados para el ejercicio de potestades administrativas y se regula la conservación permanente de

los datos de los registros de vehículos y de conductores e infractores con finalidades históricas, científicas y estadísticas[15].

En el ámbito de la Seguridad Social, la Resolución de 18 de septiembre de 2007, de la Tesorería General de la Seguridad Social, aprueba determinadas aplicaciones informáticas para la gestión de inscripción de empresas, de afiliación de trabajadores y de recaudación de recursos del sistema de la Seguridad Social. En esta misma línea se manifiesta la Resolución de 3 de agosto de 2006, del Instituto Nacional de la Seguridad Social, por la cual se aprueban determinadas aplicaciones informáticas para la gestión de las prestaciones del sistema de la Seguridad Social.

---

[15] El articulo 1 dispone: "La presente Resolución tiene por objeto la adecuación de las aplicaciones de los Registros en soporte informático de la Dirección General de Tráfico, utilizados para el ejercicio de potestades administrativas, a lo dispuesto en el artículo 9 del Real Decreto 263/1996, así como regular la conservación permanente de los datos que obran en los Registros de Vehículos y de Conductores e Infractores.

En consecuencia, se aprueban las siguientes aplicaciones utilizadas para el ejercicio de potestades administrativas:

- Registro de Vehículos.
- Registro Central de Infractores.
- Manipuladores de placas de matrícula.
- Centros autorizados de reciclado y descontaminación (CARD).
- Autorizaciones complementarias y especiales de circulación.
- Personas.
- Centros de Reconocimiento.
- Escuelas de Conductores.
- Expedientes de sanción.
- […]

Los órganos competentes para la resolución de los procedimientos adoptados mediante estas aplicaciones son las Jefaturas Provinciales y Locales de Tráfico o el órgano que se determine en su caso, en virtud de lo dispuesto en el Reglamento General de Conductores, el Reglamento General de Vehículos y el artículo 5.h del Texto Articulado de la Ley sobre Tráfico, Circulación de Vehículos a Motor y Seguridad Vial. Los usos y accesos de estas aplicaciones serán los previstos para cada fichero en la Orden INT/3764/2004, de 11 de noviembre."

Éste es el marco normativo vigente, en relación con el cual se podría plantear si la Ley 11/2007 ha modificado esta obligación de aprobación y difusión pública.

Hay que tener presente que autores como VALERO TORRIJOS hacen referencia a la defectuosa técnica legislativa utilizada por la Ley 11/2007 con respecto a la derogación de la aprobación de los programas y las aplicaciones[16]. Además, señalan que, al margen de la naturaleza jurídica de la aprobación de los programas y las aplicaciones, se trata de un requisito esencial para asegurar la sujeción plena a la ley y al derecho de las aplicaciones y los servicios de la administración electrónica desde una perspectiva material, de manera tal que exista un control efectivo sobre el funcionamiento de estas herramientas y se asegure plenamente que los órganos administrativos son los que actúan y controlan sus decisiones, sin que eso implique renunciar al uso de las nuevas tecnologías.

Sin embargo, la aprobación de los programas y las aplicaciones se puede analizar igualmente desde el punto de vista de la teoría general del acto administrativo y el ejercicio de potestades administrativas, basado en la doctrina de la vinculación positiva.

El artículo 56 de la Ley 30/1992 establece: «Los actos de las administraciones públicas sujetas al derecho administrativo son ejecutivos de acuerdo con lo que dispone esta Ley.» El artículo 57, por su parte, dice así: «1. Los actos de las administraciones públicas sujetas al derecho administrativo se presumen válidos y producen efectos desde la fecha en que se dictan, a menos que se disponga de lo contrario.»

A pesar del silencio de la Ley 11/2007, parece evidente que siempre tendrá que existir un acto administrativo en qué el funcionario o la funcionaria competente tome la decisión de poner en producción un programa o una aplicación determinados al efecto que lo puedan utilizar los administrados mediante el acceso al trámite o el servicio de que se trate en la sede electrónica correspondiente. Lógicamente, este personal tiene

---

[16] VALERO TORRIJOS, J. *El régimen jurídico de la e-Administración*. Granada: Ed. Comares, 2a edición, 2007, pág. 79.

que estar habilitado al efecto, es decir, facultado en razón de su competencia para llevar a cabo esta aprobación.

3.2.2. La difusión pública de la aprobación

En cualquier caso, aunque podemos entender que siempre será necesaria la aprobación de los programas o aplicaciones al margen del elemento o el criterio formal que se requiera para esta aprobación, lo que se ha comentado hasta ahora no resuelve la cuestión relativa a la difusión pública de las características de este software.

Con carácter general, el artículo 58.1 de la Ley 30/1992 indica que «se deben notificar a los interesados las resoluciones y los actos administrativos que afecten a sus derechos e intereses, en los términos que prevé el artículo siguiente.»

Por esta razón, si la Administración tiene que utilizar unos programas y unas aplicaciones determinados, tiene que haber un acto aprobatorio y, en la medida en que eso afecta a los administrados, se tendría que plantear si es necesaria una notificación y si, por el hecho de que se trata de un acto dirigido a una pluralidad indeterminada interesados, haría falta la publicación en el Boletín Oficial correspondiente o bien habría bastante con una difusión pública de sus características, tal como se prevé en el ámbito tributario.

En este sentido, existiría la posibilidad de que la aprobación no lleve aparejada la publicación subsiguiente. Además, incluso en la regulación hasta hace poco vigente, con referencia a los actos que no inciden de manera directa en la resolución, el artículo 5 del Real decreto 263/1996, ya no vigente, preveía un segundo supuesto ante la regla general de aprobación de programas. En aquel supuesto se señalaba que incluso no era necesaria la aprobación de los programas de carácter instrumental que efectuaran tratamientos de información auxiliares o preparatorios de decisiones administrativas sin determinar el contenido.

Independientemente de la falta de vigencia de este Real decreto y de la falta de

concreción de lo que se tenía que entender por aquellos actos administrativos internos, la realidad es que aquellos actos administrativos tenían un carácter residual y, con respecto a su ámbito de aplicación, tenían que ser objeto de una interpretación restrictiva, ya que difícilmente nos encontraremos con actos que, aunque sea indirectamente, determinen el contenido de la decisión administrativa.

Ya hemos manifestado que cuando el artículo 39 de la Ley 11/2007 habla de la actuación administrativa automatizada se limita a indicar que «se tiene que establecer previamente el órgano u órganos competentes, según los casos, para la definición de las especificaciones, programación, mantenimiento, supervisión y control de calidad y, si ocurre, auditoría del sistema de información y de su código fuente». Por lo tanto, no incluye ninguna referencia ni mención a una publicación posterior, lo cual podría conducir a pensar que ésta no es necesaria.

Además, es importante señalar que la Ley 11/2007 recoge igualmente el principio de neutralidad tecnológica. Eso hace conveniente la existencia de un órgano que, a la hora de aprobar los programas y las aplicaciones correspondientes, verifique, entre otros, el cumplimiento del principio mencionado.

Este principio aparece recogido en el artículo 4.i) de la Ley 11/2007, que establece lo siguiente: «Principio de neutralidad tecnológica y de adaptabilidad al progreso de las técnicas y sistemas de comunicaciones electrónicas garantizando la independencia en la elección de las alternativas tecnológicas por los ciudadanos y por las administraciones públicas, así como la libertad de desarrollar e implantar los avances tecnológicos en un ámbito de libre mercado. A estos efectos las administraciones públicas tienen que utilizar estándares abiertos así como, si procede y de forma complementaria, estándares que sean de uso generalizado por los ciudadanos.»

Así pues, en cumplimiento de este principio general, sería exigible que se cumpla la garantía de la independencia de la alternativa tecnológica escogida y que la discrecionalidad que pueda tener la Administración a la hora de determinar estas soluciones tecnológicas se encuentre limitada por la tendencia a utilizar estándares abiertos o, si procede, programas y aplicaciones en que la interoperabilidad esté garantizada.

Hay que tener presente que la interoperabilidad, el intercambio de datos y la colaboración son muy importantes: si no hay entendimiento entre las aplicaciones que utilicen las administraciones públicas, el desarrollo de los medios electrónicos se puede ver afectado. Además, la automatización de procesos puede partir muchas veces de la comunicación de datos entre administraciones públicas, en el marco del derecho reconocido en el artículo 6.2.b) de la Ley 11/2007, de no exigir datos y documentos que estén en poder de las Administraciones Públicas[17]. En estos casos, la interoperabilidad es esencial, y quedará garantizada diseñando los programas de la manera más estándar posible y con los requisitos de compatibilidad que posibiliten el cumplimiento de este principio.

Hay otros artículos de la Ley 11/2007 que regulan aspectos relacionados con la aprobación y la difusión pública. Es el caso de los esquemas nacionales de interoperabilidad y de seguridad, previstos en el artículo 42, los cuales tienen que establecer las reglas que tiene que respetar cualquier sistema puesto a disposición por cualquier Administración pública. En el mismo sentido, es importante la reutilización de sistemas que establece el artículo 45[18].

---

[17] Artículo 6.2.b): "Además, los ciudadanos, en relación con la utilización de los medios electrónicos en la actividad administrativa, y en los términos previstos en esta Ley, tendrán los siguientes derechos:

[...]

b) A no aportar los datos y documentos que obren en poder de las administraciones públicas, las cuales deben utilizar medios electrónicos para obtener dicha información siempre que, en el caso de datos de carácter personal, tengan el consentimiento de los interesados en los términos que establece la Ley Orgánica 15/1999, de Protección de Datos de carácter personal, o una norma con rango de Ley lo determine, salvo restricciones de acuerdo con la normativa aplicable a los datos y documentos recogidos. El consentimiento se puede emitir y aceptar por medios electrónicos."

[18] "1. Las administraciones titulares de los derechos de propiedad intelectual de aplicaciones, desarrolladas por sus servicios o el desarrollo de las que haya sido objeto de contratación, las pueden poner a disposición de cualquier Administración sin contraprestación y sin necesidad de convenio.

2. Las aplicaciones a que se refiere el apartado anterior podrán ser declaradas de fuentes abiertas, cuando de ello derive una mayor transparencia en el funcionamiento de la

En esta misma línea, la Ley 29/2010, de 3 de agosto, del uso de los medios electrónicos en el sector público de Cataluña, en su artículo 25, regula la reutilización de las aplicaciones y los servicios[19].

Hace falta tener presente, también en este sentido, el Real decreto 4/2010, de 8 de enero, por el cual se regula el Esquema Nacional de Interoperabilidad en el ámbito de la administración electrónica, y el Real decreto 3/2010, de 8 de enero, por el cual se regula el Esquema Nacional de Seguridad en el mismo ámbito. Los dos reales decretos son dictados con carácter básico, al amparo del artículo 149.1.18 de la Constitución.

Una vez aprobados, hará falta que cualquier aplicación los respete, circunstancia que habrá que comprobar a la hora de aprobar la aplicación correspondiente con el fin de garantizar que se cumplen los estándares que establecen estos esquemas.

Finalmente, hay que tener presente un precepto de la Ley 11/2007, el artículo 27.4, en sede de comunicaciones electrónicas: «Las administraciones tienen que publicar, en el correspondiente diario oficial y en la misma sede electrónica, los medios electrónicos que los ciudadanos pueden utilizar en cada caso en el ejercicio de su derecho a comunicarse.»

Administración pública o se fomente la incorporación de los ciudadanos a la sociedad de la información."

[19] "1. Las entidades que integran el sector público, para prestar sus servicios, deben potenciar el uso de las aplicaciones que han sido desarrolladas por otras entidades del sector público.

2. Las entidades que integran el sector público deben velar para que las aplicaciones que desarrollan se basen en criterios y estándares que faciliten la interoperabilidad y que puedan ser reutilizadas por otras entidades del sector público.

3. Las entidades del sector público deben impulsar la creación de bancos de recursos y aplicaciones de las administraciones públicas que puedan ser reutilizados para facilitar el aprovechamiento de las aplicaciones, así como su desarrollo colaborativo."

Realmente, este precepto distorsiona la cuestión, sobre todo si partimos del concepto omnicomprensivo de medio electrónico que utiliza la Ley 11/2007 en su anexo[20]. En cualquier caso, debemos interpretar este artículo de acuerdo con la ubicación donde se encuentra – comunicaciones electrónicas – y en el contexto del artículo – referente a los canales de comunicación que puede utilizar al ciudadano a la hora de relacionarse con la Administración pública cuando ésta ejerce potestades administrativas. No obstante, la misma Comisión Jurídica Asesora, en el Dictamen 22/2009, mencionado más arriba, ha interpretado esta previsión como la subsistencia de la obligación de publicar oficialmente los procedimientos y los servicios que se pueden tramitar de manera electrónica.

3.3. La automatización de procesos y el ejercicio de la competencia

La existencia de una pluralidad de entes en el seno de cada una de las administraciones públicas exige que se distribuya entre ellas la titularidad de las funciones públicas. Sin embargo, además, la existencia de diversos órganos dentro de un ente público obliga a distribuir igualmente entre ellos las funciones a realizar en relación con las particularidades atribuidas al ente sobre la base del principio de legalidad y potestad autoorganizativa.

3.3.1. La competencia administrativa

Podemos definir el concepto de competencia administrativa como lo hace GARCÍA DE ENTERRÍA: «la medida de la potestad que corresponde a cada órgano».

[20] "Medio electrónico: mecanismo, instalación, equipo o sistema que permite producir, almacenar o transmitir documentos, datos e informaciones; incluyendo cualesquiera redes de comunicación abiertas o restringidas como Internet, telefonía fija y móvil u otros."

En cuanto a la naturaleza del concepto, la competencia administrativa no obedece tan sólo a la necesidad de distribuir el trabajo, sino también a la voluntad de ser una garantía para los administrados. Tanto la Ley 30/1992, de 26 de noviembre, de régimen jurídico de las administraciones públicas y del procedimiento administrativo común, como la Ley 13/1989, de 14 de diciembre, de organización, funcionamiento y régimen jurídico de la Administración de la Generalitat, disponen, como regla general, que la competencia es irrenunciable y la tiene que ejercer el órgano que la tiene atribuida, salvo determinadas excepciones (como la avocación o la delegación).

Hay que tener presente que los conceptos de competencia y de potestad son usados habitualmente de manera indiferenciada. En este sentido, es paradigmático el artículo 2.4 de la Ley 6/1997, de organización y funcionamiento de la Administración general del Estado (LOFAGE), cuando indica que «las potestades y competencias administrativas que, en cada momento, tengan atribuidas la Administración General del Estado y sus Organismos Públicos por el ordenamiento jurídico, determinan la capacidad de obrar de una y de otros».

En cualquier caso, podemos entender por potestades un concepto más amplio, referido a poderes de actuación de carácter más genérico no identificados con la materia sobre la cual recaen o el sector en el cual operan. Por contra, la competencia es un concepto más concreto, referido a un sector o un ámbito de actuación específico.

En cuanto a las clases, se distinguen las siguientes:

1) Una competencia subjetiva, o conjunto de funciones cuya titularidad se atribuye a un ente con preferencia a los otros.

2) Una competencia orgánica, como aquella parte de las funciones de un ente cuyo ejercicio se atribuye a uno de los órganos del ente.

Finalmente, con respecto a los criterios de delimitación, se distingue:

- Competencia jerárquica.

- Competencia material.
- Competencia territorial.

El criterio jerárquico se refiere a la preferencia de un órgano concreto para ejercer la función en relación con los suyos superiores o inferiores. Los otros dos criterios atienden en el plano horizontal, eso es, entre órganos de un mismo nivel jerárquico, ya sea en relación con la materia o con el ámbito territorial de actuación.

La determinación competencial es una manifestación de la potestad autoorganizativa, que se entiende como el conjunto de facultades que tiene cada Administración por configurar su estructura (es decir, la posibilidad de autoorganizarse).

En cuanto a la titularidad, habrá que acudir a la normativa reguladora de cada Administración. En particular, en el ámbito de la Administración general del Estado se ha impuesto la reserva de ley para la regulación del Gobierno, del Consejo de Estado y de los organismos públicos. No obstante, por real decreto el presidente o la presidenta puede variar el número, la denominación y las competencias de los ministerios y las secretarías el Estado (artículos 61 y 8.3 de la LOFAGE).

Asimismo, el artículo 10 de la LOFAGE dispone que las subsecretarías, las secretarías generales, las secretarías generales técnicas, las direcciones generales, las subdirecciones generales y los órganos similares se crean, se modifican y se suprimen por real decreto del Consejo de Ministros. Por su parte, los órganos de nivel inferior a subdirección general se crean, se modifican y se suprimen por orden del ministro respectivo.

En el ámbito de la Administración de la Generalitat, tanto la Ley 13/1989 como la Ley 13/2008, de 5 de noviembre, de la presidencia de la Generalitat y del Gobierno, reconocen en el Gobierno responsabilidades organizativas amplias, como ahora crear comisiones dentro del mismo gobierno; crear, agrupar, modificar, dividir o suprimir los departamentos fijados por la ley, y realizar las modificaciones y las innovaciones organizativas en los diversos niveles. Paralelamente, atribuye a los consejeros potestad reglamentaria en materia de organización de sus departamentos.

En el ámbito local, los órganos políticos básicos de los municipios y las provincias están regulados en la Ley de bases de régimen local. Los órganos inferiores, de nivel administrativo, los regula cada corporación – que debe aprobar un reglamento orgánico – y las normas supletorias que dicten las Comunidades Autónomas.

En cuanto a los principios de la potestad organizativa, ésta se tiene que inspirar y tiene que respetar el artículo 103 de la Constitución, que establece: «La Administración pública sirve con objetividad los intereses generales y actúa de acuerdo con los principios de eficacia, jerarquía, descentralización, desconcentración y coordinación, con sometimiento pleno a la ley y al Derecho.» Estos principios han sido reiterados por el artículo 3 de la Ley 30/1992, el cual añade tres principios más:

1) La distinción entre gobiernos y administraciones.
2) El principio de cooperación.
3) El principio de personalidad jurídica única, de acuerdo con el cual el artículo 3.4 de la Ley 30/1992 establece el siguiente: «Cada una de las administraciones públicas actúa, para el cumplimiento de sus finalidades, con personalidad jurídica única.» (Asimismo lo recoge el artículo 2 de la Ley 13/1989.)

3.3.2. La competencia y la actuación administrativa automatizada

De acuerdo con lo que hemos expuesto, el concepto de *competencia* es esencial a la hora de tratar la actuación administrativa, y, en el caso de la actuación administrativa automatizada, tiene que haber igualmente una atribución expresa de competencias.

De la misma manera, ya hemos indicado que cada Administración pública disfruta de una autonomía muy grande a la hora de crear, modificar y extinguir sus órganos, cosa que se manifestará también en la actuación administrativa automatizada, en un nivel doble:

- El primer nivel (tratado previamente) sería la decisión discrecional de automatizar un procedimiento determinado, cosa que exigirá una actuación de

adecuación jurídica y técnica a los condicionantes que la actuación administrativa concreta requiere.

- El segundo nivel, relacionado directamente con el anterior, tiene que ver con la vertiente jurídica: consistiría en la adecuación de su estructura organizativa a la existencia de un órgano que, programado debidamente, produjera actos administrativos de manera automatizada.

En cualquier caso, como indica el artículo 44.3 de la Ley 26/2010, "la actuación administrativa automatizada no afecta a la titularidad de la competencia de los órganos administrativos ni las competencias atribuidas para resolver los recursos administrativos".

A título de ejemplo, la normativa tributaria prevé, por ejemplo, que la automatización deberá partir del órgano administrativo responsable a efectos de impugnación, que es lo que comprobaría, en última instancia, la regularidad de la actuación administrativa emitida

En cualquier caso, el concepto de competencia es básico a la hora de hablar de actuación administrativa por medios electrónicos. Hace falta recordar que esta figura está recogida en la normativa tributaria, en particular en los artículos 96.3 y 100.2 de la Ley 58/2003, de 17 de diciembre, general tributaria. Además, se ha previsto, con carácter general, la posible automatización de los procesos en los artículos mencionados.

El primero de estos artículos señala: «Los procedimientos y las actuaciones en que se utilicen técnicas y medios electrónicos, informáticos y telemáticos tienen que garantizar la identificación de la Administración tributaria actuante y el ejercicio de su competencia. *Además, cuando la Administración tributaria actúe de forma automatizada se garantiza la identificación de los órganos competentes para la programación y supervisión del sistema de información y de los órganos competentes para resolver los recursos que se puedan interponer*.»

El segundo de estos artículos extiende la posible utilización de la actuación administrativa automatizada a los actos resolutorios. En particular, establece: «Tiene

la consideración de resolución la respuesta efectuada de forma automatizada por la Administración tributaria en los procedimientos en que esté prevista ésta forma de finalización.»

Ciertamente, la figura ha sido usada en el ámbito tributario con cierta profusión, sin que el sello de órgano haya presentado problemas especiales en las relaciones juridicotributarias. Sin embargo, este hecho no nos puede llevar a entender que la experiencia se puede trasladar fácilmente a cualquier esfera de la actuación administrativa. Por una parte, que su uso no haya generado problemas también proviene del hecho de que incluso su utilización en la esfera tributaria es, hoy por hoy, reducida, por lo cual la casuística con respecto al número de problemas todavía no es relevante. Por otra parte, el concepto esencialmente de deber que caracteriza la obligación tributaria, la actuación en masa y reiterada en el tiempo, significan unos presupuestos de hecho que no se pueden trasladar al resto de las relaciones juridicoadministrativas, dado que los caracteres mencionados anteriormente presentan matices significativos en el procedimiento administrativo común.

Al margen de la normativa tributaria, nos tenemos que plantear la viabilidad de la figura en el seno del procedimiento administrativo, como también los problemas que puede generar.

Finalmente, hay que añadir que la misma Ley 11/2007 recoge la exigencia general del respeto a la competencia en el artículo 33.1[21].

[21] Artículo 33.1: “La gestión electrónica de la actividad administrativa debe respetar la titularidad y el ejercicio de la competencia por la administración pública, órgano o entidad que la tenga atribuida y el cumplimiento de los requisitos formales y materiales establecidos en las normas que regulen la correspondiente actividad. A estos efectos, y en todo caso bajo criterios de simplificación administrativa, se impulsará la aplicación de medios electrónicos a los procesos de trabajo y la gestión de los procedimientos y de la actuación administrativa."

3.3.3. La identificación y la autenticación en la actuación administrativa automatizada

Aparte de la competencia configurada de manera abstracta, hay que hablar también de la titularidad de ésta, que se manifiesta mediante el ejercicio de la competencia por parte de su titular, lo cual requiere igualmente su identificación y autenticación.

El capítulo II de la Ley 11/2007 (artículos 13 y siguientes) regula la identificación y la autenticación, tanto de los ciudadanos como de las administraciones públicas (secciones 2ª y 3ª), mientras que la sección 4ª se refiere a la interoperabilidad y a la acreditación y la representación de los ciudadanos.

Esta regulación parte del principio de libre prestación de servicios de certificación, que deriva de la Ley 59/2003, de 19 de diciembre, de firma electrónica, y de la Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la cual se establece un marco comunitario para la firma electrónica. Al mismo tiempo, la Ley 11/2007 apuesta claramente por el DNI electrónico, que se admite incluso como medio para acreditar el ejercicio de la competencia por parte del personal al servicio de las administraciones públicas.

Por otra parte, el sello de órgano se recoge en el artículo 18 de la Ley 11/2007, bajo la rúbrica «Sistemas de firma electrónica para la actuación administrativa automatizada». En estos casos, se sigue la regla general de exigir «la identificación y la autenticación del ejercicio de la competencia», exigible en toda actuación administrativa, con la condición que en la actuación automatizada se puede llevar a cabo mediante dos sistemas:

«a) Sello electrónico de una administración pública, órgano o entidad de derecho público, basado en certificado electrónico que reúna los requisitos exigidos por la legislación de firma electrónica.
b) Código seguro de verificación vinculado a la administración pública, órgano o entidad y, si se pega, a la persona firmante del documento; en todo caso se tiene que permitir la comprobación de la integridad del documento mediante el acceso a la sede electrónica correspondiente.»

De todo aquello expuesto con anterioridad deriva que, desde la vertiente técnica, hay que hacer una determinación doble: de un lado, la programación de los programas y las aplicaciones que lleven a cabo esta actuación administrativa automatizada, y, por otra parte, la existencia de rasgos básicos del procedimiento (como la delimitación de los medios de identificación) que se tendrán que concretar o definir en el marco de la ley reguladora.

Además, no se puede dejar de lado el cambio significativo que ha comportado la Ley 11/2007 en materia de identificación. A diferencia de la Ley 59/2003, de 19 de diciembre, de firma electrónica, en que se optaba claramente por la firma electrónica reconocida, la Ley 11/2007 cambia radicalmente esta concepción: otorga la posibilidad de escoger el tipo de firma a utilizar para cada procedimiento o trámite y admite criterios de riesgos a la hora de determinar qué firma se tendrá que utilizar.

En definitiva, la Ley 11/2007 consagra el criterio de determinación de medidas de seguridad para los procedimientos administrativos basado en el análisis de riesgos y en el uso de múltiples sistemas técnicos. Esta circunstancia implica, primero, una cierta continuación de los criterios contenidos a la Ley 30/1992, y, después, representa el final de la tendencia a la adopción de la firma electrónica reconocida como paradigma de la identificación y la autenticación.

Así, las leyes de firma establecen la validez legal de la firma electrónica, a la cual no se podrá negar efectos únicamente por el hecho de encontrarse en forma electrónica. Sin embargo, eso no quiere decir que se pueda utilizar cualquier firma, en cualquier entorno, sin apoyo jurídico adicional.

También hace falta tener presente que la normativa permite la construcción y la operación de sistemas cerrados de usuarios y aplicaciones basados en contratos de firma electrónica (firma electrónica convencional o contractual) o normativas específicas de firma electrónica (firma electrónica normativa), cosa que se puede trasladar a la actuación administrativa automatizada en función del procedimiento, el trámite o la actuación que sea objeto del proceso de automatización, los destinatarios del acto y la finalidad última de éste.

3.4. El órgano administrativo y la compentencia en relación a la automatización

Si hablamos de actuación administrativa automatizada, y en la medida en que el artículo 5 de la Ley 11/2007 nos remite al anexo para determinar el sentido de los términos utilizados, hay que decir que este anexo define la actuación administrativa automatizada como la «actuación administrativa producida por un sistema de información adecuadamente programado sin necesidad de intervención de una persona física en cada caso singular. Incluye la producción de actos de trámite o resolutorios de procedimientos, así como de meros actos de comunicación».

Ya hemos puesto de manifiesto el carácter omnicomprensivo de la definición. No obstante, esta definición tan amplia no se puede adoptar: habrá que delimitarla por la simple razón que existen determinados tipos de actos administrativos que tendrían que quedar excluidos de la actuación administrativa automatizada.

Prima facie, hablar de sello de órgano hace que nos planteamos dos conceptos: *competencia administrativa* y *órgano administrativo*.

3.4.1. La superación del concepto tradicional de órgano administrativo

Ya hemos indicado que la competencia es irrenunciable y la ejerce el órgano que la tiene atribuida legalmente (artículo 12 de la Ley 30/1992). Esta atribución legal nos conduce al concepto de *órgano administrativo*, concebido tradicionalmente como una pluralidad de puestos de trabajo que dependen de una misma dirección.

El concepto legal de *órgano administrativo* se ha equiparado tradicionalmente con el de *unidad administrativa*, igual que lo hace la misma Ley 30/1992 en diferentes artículos (artículos 11, 14.2, 16.1, 38, 70.1 y 110.1). El primero de estos preceptos, relativo a la creación de órganos administrativos, alude, en el apartado segundo, a los requisitos de creación de un órgano administrativo, entre los cuales está la forma de integración en la Administración pública de que se trate y su dependencia jerárquica.

La Ley 6/1997, de 14 de abril, de organización y funcionamiento de la Administración general del Estado (LOFAGE), en el artículo 5.2, habla de los órganos administrativos en los términos siguientes: «*Tendrán la consideración de órganos las unidades administrativas a las que se las atribuyan funciones que tengan efectos jurídicos frente a terceros*, o cuya actuación tenga carácter preceptivo.»

El artículo 7 precisa: «*Las unidades administrativas son los elementos organizativos básicos de las estructuras orgánicas. Las unidades comprenden puestos de trabajo o dotaciones de plantilla vinculados funcionalmente por razón de sus cometidos y orgánicamente por una jefatura común*. Pueden existir unidades administrativas complejas, que agrupan dos o más unidades menores.»

El órgano administrativo ha sido configurado tradicionalmente en torno a dos elementos: uno subjetivo (personas físicas integradas en el órgano) y otro objetivo (medios materiales de que dispone), necesarios para el cumplimiento de las atribuciones o competencias del órgano.

Eso nos lleva a evaluar si serían válidas las actuaciones administrativas sin este elemento personal, es decir, llevadas a cabo directamente por medios electrónicos o informáticos programados debidamente. En definitiva, se trata de discernir si la voluntad humana es esencial para la producción de actos administrativos o si, al contrario, podemos prescindir de ella.

La respuesta, obviamente, debe ser positiva: hay actos administrativos que, por su singularidad, son susceptibles de automatización, por razones de interés general, y eliminan la voluntad humana. En cualquier caso, ya hemos indicado que esta eliminación es relativa, porque ha sido manifestada previamente mediante la programación realizada.

No obstante, algunos autores rechazan la posibilidad de automatización porque consideran que los actos administrativos, en tanto que son declaraciones de voluntad, no pueden provenir de las máquinas[22].

Hoy día esta concepción se debe entender superada, ya que los avances tecnológicos hacen viable – e incluso recomendable desde el punto de vista de la eficiencia administrativa – que puedan ser automatizadas decisiones administrativas que, aunque implican una declaración de voluntad *ex novo*, se integran por la comprobación del cumplimiento de unos requisitos o condicionantes establecidos de manera clara y concreta.

Previamente hemos mencionado supuestos en que la automatización resultaría pacífica – es decir, no plantearía situaciones de inseguridad jurídica – y permitiría liberar numerosos recursos personales y materiales que se podrían dirigir al ejercicio o el cumplimiento de otras funciones administrativas (no hace falta sino pensar en la automatización de la notificación de los actos administrativos a partir de los datos existentes en el expediente administrativo y, evidentemente, con cumplimiento de todos los requisitos que la normativa exige para la notificación electrónica, o bien en los actos de certificación.)

El artículo 44.1 de la Ley 26/2010 enumera una serie de supuestos o actuaciones administrativas automatizables[23]. Si los analizamos, podemos ver que son supuestos ciertamente amplios que permiten trasladar la automatización a muchos ámbitos de la actuación administrativa.

Especialmente significativos serían la comunicación o certificación de datos, y la constatación de la concurrencia de requisitos, declarando las consecuencias que se derivan.

---

[22] PARADA, J.R. *Régimen jurídico de las administraciones públicas y del procedimiento administrativo común*. Madrid: Marcial Pons, 2a edición, 1999, pàg. 194.

[23] "... constatar la concurrencia de los requisitos establecidos en el ordenamiento jurídico, declarar las consecuencias previstas, adoptar las resoluciones y comunicar o certificar los datos, los actos, resoluciones o acuerdos que consten en sus sistemas de información ... "

Sobre esta base, existirían supuestos que serían susceptibles de automatización, como la denegación de subvenciones por falta de cumplimiento de los elementos reglados establecidos para el otorgamiento o bien la suspensión de actos administrativos de contenido económico en el ámbito tributario por la comprobación de la prestación de la garantía.

En estos casos, la inexistencia de la intervención humana no puede llevar a negar la posibilidad de automatización. Tenemos que reiterar que la intervención humana existe, en primer lugar, en la decisión de automatización; en segundo lugar, en el establecimiento de las condiciones informáticas de producción del acto, y, en tercer lugar, en la supervisión del cumplimiento o el funcionamiento adecuado de estas condiciones. Además, se pueden añadir sistemas de auditoría informática que garanticen el funcionamiento adecuado de las aplicaciones.

Por todo lo que hemos expuesto, cuando hablamos de sello de órgano estamos introduciendo un nuevo elemento en los conceptos mencionados más arriba, dado que aparentemente tenemos que prescindir del elemento personal.

3.4.2. El sello de órgano

El artículo 18.2 de la Ley 11/2007 establece que «los certificados electrónicos a que se hace referencia en el apartado 1.a) [sello de Administración pública, órgano o entidad de derecho público] tienen que incluir el número de identificación fiscal y la denominación correspondiente, y pueden contener la identidad de la persona titular en el caso de los sellos electrónicos de órganos administrativos»

Por una parte, vemos que al lado del sello de órgano se admite el sello de Administración pública y el de entidad de derecho público, como también que, en el caso del sello de órgano, aunque sea con carácter potestativo, se habla de la identidad de la persona titular, cosa que nos lleva a plantearnos si esta persona titular tendrá que existir necesariamente o no.

La Ley 11/2007 no resuelve esta cuestión de una manera directa, si bien parece admitir la posibilidad que el sello de órgano no esté ligado a un titular determinado a la vista de lo que dispone el artículo 39, de acuerdo con el cual «en caso de actuación automatizada se tiene que establecer previamente el órgano u órganos competentes, según los casos, para la definición de las especificaciones, programación, mantenimiento, supervisión y control de calidad y, si ocurre, auditoría del sistema de información y de su código fuente. *Asimismo, se debe indicar el órgano que tiene que ser considerado responsable a los efectos de impugnación*».

Se debe destacar que establece la indicación del órgano que tiene que ser considerado responsable a los efectos de impugnación. Eso supone el establecimiento de una ficción jurídica que permita el ejercicio del derecho de reacción contra un acto producido mediante una actuación administrativa automatizada, a través de la interposición del recurso correspondiente

3.4.3. El sello de órgano y el acto administrativo: principales problemas

El sello de órgano rompe la concepción tradicional del acto administrativo como declaración de voluntad, de juicio, de conocimiento o de deseo, llevado a cabo por un órgano, administrativo en el ejercicio de una potestad administrativa (ZANOBINI), ya que la declaración que deriva de un sello de órgano difícilmente puede recibir alguno de los calificativos mencionados anteriormente.

En una primera aproximación, las declaraciones de voluntad y de conocimiento pueden ser susceptibles de automatización. Por contra, las declaraciones de juicio o de deseo difícilmente se pueden predeterminar o programar y, consiguientemente, su automatización se podría considerar no viable.

En resumidas cuentas, el sello de órgano obliga a replantearse el concepto de acto administrativo y toda la cadena de producción de este tipo de actas. Hay que añadir a eso que la convivencia del sello de órgano con el sello de Administración pública y el sello de entidad de derecho público plantea problemas adicionales en cada uno de estos supuestos.

En relación con el sello de Administración pública, hay que tener presente la diferenciación entre actos políticos y administrativos – de especial trascendencia con respecto a su revisión[24] –, la competencia para ejecutar los actos exteriorizados de forma automática, el control de estos actos y las responsabilidades que se pudieran derivar.

En cualquier caso, por la naturaleza misma de los actos políticos, que son manifestación de una voluntad política, diferenciada de la voluntad administrativa, que liga con el funcionamiento ordinario de la Administración, los primeros difícilmente se podrían automatizar.

En definitiva, la automatización de procesos y decisiones administrativos ligaría más con el concepto de actividad administrativa estrictamente dicha, dejando de lado la actuación política.

Otro de los aspectos a considerar cuando nos encontramos con la actuación administrativa automatizada y el sello de órgano es de la motivación de los actos administrativos, ya que a nadie se le escapa que los supuestos tasados de motivación de los actos administrativos del artículo 54 de la Ley 30/1992 suponen, en la práctica, configurar la motivación como la regla general.

En el caso de la automatización administrativa, desaparece la motivación del acto configurada tradicionalmente, porque ésta pasa a integrarse en el mecanismo de producción de la actuación administrativa.

En este sentido, una programación concreta determina un resultado concreto, y es en función de esta programación que el acto administrativo se configura con un contenido determinado. En definitiva, la motivación tiene una finalidad muy concreta, que es conocer la razón de ser de la actuación administrativa, y posibilitar en segunda

---

[24] El control de los actos políticos lo es sólo en relación con la tutela de los derechos fundamentales y las libertades públicas y la existencia de elementos reglados (artículo 2 de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso Administrativa).

instancia que el administrado o la administrada reaccione ante esta actuación, en caso de que no se haya adecuado a las finalidades de interés general que las administraciones públicas tienen que atender.

Por este motivo, si la motivación del acto administrativo automatizada se integra por una programación adecuada, tan sólo mediante la revisión de esta programación se podrá reaccionar ante el acto administrativo emitido.

Esta posibilidad de reaccionar está condicionada por el hecho que la presunción de validez del acto administrativo, aplicable igualmente en el ámbito de la automatización, traslada la carga de reaccionar al administrado o la administrada. Así pues, tratándose de programas y aplicaciones, tendremos que atenernos a una prueba pericial técnica que acredite que la programación no ha sido efectuada debidamente, ya que si bien la Ley de enjuiciamiento civil admite cualquier medio de prueba que resulte útil y pertinente[25], será una prueba pericial informática la más idónea para acreditar una programación adecuada. Con respecto a aspectos concretos (como una firma electrónica concreta), también se podría utilizar una certificación de producto o servicio.

Hay que recordar que éste es el criterio que recoge, en materia de firma electrónica, el artículo 3.8 de la Ley 59/2003, en redacción que da la Ley 56/2007, de 28 de diciembre, de medidas de impulso de la sociedad de la información[26].

---

[25] Artículo 326.2 de la Ley de Enjuiciamiento Civil.

[26] Artículo 3.8: "El soporte en que se hallen los datos firmados electrónicamente será admisible como prueba documental en juicio. Si se impugnare la autenticidad de la firma electrónica reconocida con la que se hayan firmado los datos incorporados al documento electrónico se procederá a comprobar que se trata de una firma electrónica avanzada basada en un certificado reconocido, que cumple todos los requisitos y condiciones establecidos en esta Ley para este tipo de certificados, así como que la firma se ha generado mediante un dispositivo seguro de creación de firma electrónica.
La carga de realizar las citadas comprobaciones corresponderá a quien haya presentado el documento electrónico firmado con firma electrónica reconocida. Si dichas comprobaciones obtienen un resultado positivo, se presumirá la autenticidad de la firma electrónica reconocida con la que se haya firmado dicho documento electrónico siendo las costas, gastos y derechos

Todos estos elementos (tipología del acto, contenido del acto, plasmación documental), así como los sujetos que intervienen en su realización, son, entre otros, elementos que integran o configuran el acto y tienen que ser tomados en consideración a la hora de plantear la automatización.

Es cierto que existen supuestos en qué el sello de órgano puede ser de aplicación, sin presentar problemas en la práctica – como podría ser la foliación del expediente administrativo que se contiene en el artículo 32.2 de la Ley 11/2007 –, pero se debe utilizar de manera moderada y de acuerdo con el principio de proporcionalidad que establece el apartado g) del artículo 4 de la Ley 11/2007, que exige «las garantías y medidas de seguridad adecuadas a la naturaleza y circunstancias de los diferentes trámites y actuaciones».

En este mismo sentido, resulta notable que la única referencia expresa al uso del sello para un acto concreto que hace la Ley 11/2007 aluda a la posibilidad de automatizar el proceso de digitalización de documentos en soporte papel y a la obtención de las copias electrónicas correspondientes, que se contiene en el artículo 30.3 de la Ley, quizás con la intención de evitar la necesidad que un funcionario tenga que confrontar la copia con el original, otro uso que puede resultar pacífico.

No podemos desdeñar que, desde el punto de vista de la responsabilidad, podría tentar el hecho de dejar de lado la firma del funcionario competente a favor del sello de órgano o de Administración, pero su uso generalizado produciría inseguridad jurídica. Eso, por otra parte, nos obliga a plantearnos el tipo de firma electrónica a utilizar, que, como regla general, será la firma electrónica reconocida.

---

que origine la comprobación exclusivamente a cargo de quien hubiese formulado la impugnación. Si, a juicio del tribunal, la impugnación hubiese sido temeraria, podrá imponerle, además, una multa de 120 a 600 euros.
Si se impugna la autenticidad de la firma electrónica avanzada, con la que se hayan firmado los datos incorporados al documento electrónico, se estará a lo establecido en el apartado 2 del artículo 326 de la Ley de Enjuiciamiento Civil."

Igualmente, habrá que tener presente si la actuación administrativa se produce en entornos cerrados o si, contrariamente, produce una eficacia externa en relación con el ciudadano. En cada uno de estos casos se tendrá que actuar de manera diferenciada

Volviendo a la regulación legal, el artículo 38.2 de la Ley 11/2007 limita la adopción y la notificación de resoluciones de forma automatizada a los procedimientos en que así esté previsto, pero no se establece ninguno condicionante material a esta posibilidad, aunque podemos entender que, como regla general, la resolución automatizada de los procedimientos administrativos se tiene que justificar debidamente – razón por la cual tendrá carácter excepcional.

En cualquier caso, habrá que atenerse a la naturaleza de los actos y a su contenido, e incluso a la regulación legal de éstos.

A título de ejemplo, la suspensión de los actos administrativos a raíz de la interposición de un recurso se produce de manera automática si, transcurrido el plazo de treinta días desde la solicitud, ésta no ha sido resuelta. A partir de esta previsión legal, nada impide la configuración informática de la suspensión de un acto administrativo en el supuesto de que no se haya producido la resolución en el plazo mencionado.

Más todavía, en algunos ámbitos – como el tributario – la suspensión se entiende otorgada automáticamente por la simple prestación de la garantía correspondiente, sin necesidad de no justificar ninguna razón o motivo con el fin de suspender la ejecutividad de los actos administrativos.

De acuerdo con esta previsión, nada impediría articular un procedimiento automatizado en qué, una vez constatada la prestación de la garantía mencionada, la misma máquina, programada debidamente por la comprobación de la identidad entre la cuantía objeto de reclamación y la que es objeto de garantía (con una posible comprobación en línea), dictara una resolución que otorgara esta suspensión.

En esta línea, podemos hacer referencia a la Resolución de 12 de julio de 2010, del Instituto Social de la Marina y del Servicio Público de Empleo Estatal, por la que se

regula la tramitación electrónica automatizada de diversos procedimientos en materia de protección por desempleo del Régimen Especial de los Trabajadores del Mar (B.O.E. nº. 225, de 16 de septiembre de 2010), que prevé la automatización de determinados procesos administrativos no complejos[27].

Aparte de los actos resolutorios, los actos de trámite constituyen un ámbito de la actuación administrativa en que la automatización presenta múltiples posibilidades.

Así, existen los actos de trámite que, a pesar de su naturaleza, se dirigen de manera directa a la persona interesada (como el acto de incoación de un procedimiento sancionador, con la notificación correspondiente), los cuales, muchas veces, a pesar de no ser susceptibles de recurso, requieren una automatización compleja por el hecho de que se trata de decisiones de juicio de la Administración. Hay que diferenciar estos actos de trámite de los llamados de dirección e impulso, que se llevan a cabo a efectos de garantizar el desarrollo del procedimiento en todos sus trámites; a menudo estos actos no tienen una eficacia directa hacia los ciudadanos, sino que limitan sus efectos a lo que sería la esfera más interna.

Hay que tener presente que en muchos ámbitos de la actuación administrativa relacionada con el ejercicio de potestades ablatorias o sancionadoras, en qué el ejercicio de la actividad de policía está acondicionada al cumplimiento estricto de plazos para dictar y notificar el acto, y en qué el transcurso del tiempo determina muchas veces la caducidad del procedimiento y la consiguiente impunidad de la persona responsable, se articulan sistemas de control de la actividad con alarmas que pretenden asegurar que la persona responsable dicte la resolución correspondiente o ponga fin al procedimiento y practique la notificación correspondiente dentro del plazo establecido al efecto.

En resumidas cuentas, la automatización se podría trasladar a las actuaciones regladas, incluso en los supuestos de actos de carácter constitutivo. Sin embargo,

---

[27] "...a) Solicitudes de alta y reanudación de las prestaciones contributivas por desempleo y de los subsidios por desempleo (...) b) Solicitudes de prórrogas de los subsidios por desempleo (...) c) (...) suspensiones o extinciones del derecho".

esta automatización sólo sería viable cuando la decisión que hay que tomar se pudiera deducir de un proceso de tratamiento de datos programado debidamente y sometido a medidas de control y supervisión adecuados.

3.5. Límites de la actuación administrativa automatizada

No se puede dejar de lado que la actuación administrativa tiene que responder siempre a razones de interés general y que un límite de la actuación administrativa, sobre todo en relación con los actos discrecionales, se configura por la prohibición de la desviación de poder, que supone la prohibición del ejercicio de potestades administrativas para finalidades diferentes de las previstas al ordenamiento jurídico.

La existencia de desviación de poder y la falta de motivación son supuestos de anulabilidad de los actos administrativos dictados. Esta previsión es importante, ya que la Administración a veces aplica la actuación administrativa automatizada a determinados procesos y establece modelos de respuesta en que se prevén todas las posibilidades. Eso pasa, por ejemplo, en las resoluciones de los procedimientos sancionadores en materia de tráfico, en qué se alude al hecho de las alegaciones formuladas, si ocurre, y lo que denotan es que este modelo se puede trasladar al supuesto en que se hayan formulado alegaciones o no o, lo que es lo mismo, estableciendo una presunción del hecho que, en definitiva, la Administración no ha tenido en cuenta el contenido de las alegaciones – si han sido formuladas –, sino que practica un automatismo absoluto en la decisión del procedimiento.

Es evidente que la Administración pública debe buscar criterios de eficiencia, pero no a cualquier precio, y menos todavía cuando pueden resultar perjudicados derechos o garantías de los administrados en el procedimiento administrativo en que tienen la condición de personas interesadas.

Por otra parte, tal como hemos subrayado, la actuación administrativa automatizada se puede definir como la producida por un sistema de información programado adecuadamente sin necesidad de intervención de una persona física en cada caso singular.

Eso nos llevaría a excluir la actuación administrativa automatizada de todos aquellos supuestos en que hay discrecionalidad por parte de la Administración y a aplicarla

solos a supuestos claramente reglados. Sin embargo, no se puede ignorar que, hoy en día, los actos administrativos contienen diferentes elementos reglados y discrecionales que tienen que ser valorados conjuntamente, lo cual dificulta todavía más la predeterminación informática de la decisión administrativa

Hay que tener en cuenta que los actos administrativos se tienen que vincular a un responsable, que puede ser objeto, dado el caso, de tener que someterse a responsabilidades disciplinarias. El mismo concepto de funcionario que contiene el artículo 24 del Código Penal no concuerda con la admisión genérica del sello de órgano ni con las diferentes tipificaciones penales existentes.

El sello de órgano también obliga a revisar el régimen de recursos administrativos y los medios de impugnación, dado que el recurso de alzada o de reposición, admitidos como a mediados de impugnación, no pueden ser utilizados de manera automática y, en el caso del recurso de reposición, nunca sería una reposición por parte del mismo "órgano" que decidió el acto impugnado.

Además, ya hemos comentado que el criterio general para la automatización de procesos, en los supuestos en que está regulado actualmente, pasa por la decisión previa del órgano administrativo responsable a los efectos de recursos. Eso comporta, en la práctica, trasladar al mismo órgano que ha tomado la decisión de automatizar una actuación administrativa determinada la resolución de los recursos que se puedan interponer y, al mismo tiempo, dejar sin responder qué es el que pasaría en los casos de los actos susceptibles de recurso de alzada, en qué la automatización habría sido decidida por el órgano que conoce del recurso de alzada y, si se impugnara esta automatización, nos encontraríamos en la práctica ante un recurso que, siendo aparentemente de altura, es objeto de conocimiento por parte del mismo órgano, que, por el hecho de que acuerda la automatización y como responsable de la decisión, se podría considerar responsable del acto.

Asimismo, la admisión del sello de órgano es una manifestación de que la informática manda o puede mandar y de qué la persona física pierde o puede perder el control. Por esta razón, el régimen de recursos es – o debe ser – una garantía mínima a fin de que los derechos de los ciudadanos en sus actuaciones ante las administraciones públicas no queden perjudicados.

Igualmente, el sello de órgano debe quedar excluido de todos aquellos supuestos en que haya un elemento subjetivo, valoración o motivación en la actuación administrativa. De lo contrario, se estarían vulnerando los principios generales del procedimiento administrativo y, por otra parte, se produciría una rebaja de los derechos de los ciudadanos no amparada por la Ley 11/2007. Éste sería el caso de las declaraciones de juicio que hemos mencionado antes, como la emisión de un informe jurídico, que, obviamente, nunca podrá ser automatizada.

Aparte de estas previsiones relativas al contenido material o sustantivo del acto administrativo y la viabilidad de la automatización de éste, resulta necesario considerar los problemas de la aplicación de la legislación vigente en materia de firma electrónica al caso particular del sello de órgano. En efecto, aunque no se puede considerar que un sello de órgano sea una firma electrónica (ni avanzada ni reconocida, porque sencillamente es una institución nueva y completamente diferente de la firma), el artículo 18 de la Ley 11/2007 determina que el sello de órgano debe estar «basado en certificado electrónico que reúna los requisitos exigidos por la legislación de firma electrónica».

Esta manifestación genera algunos problemas de aplicación práctica, ya que la normativa de firma electrónica está orientada a la documentación electrónica de los actos jurídicos por personas físicas, por lo cual puede resultar complejo determinar la aplicación directa.

Como ejemplos particulares de problemas a resolver en esta aplicación de la Ley 59/2003 podemos citar los siguientes:

- La necesidad o no de utilizar un dispositivo seguro de creación de sello (por aplicación analógica de la necesidad de uso de dispositivo seguro de creación de firma electrónica, ex artículo 24 de la Ley 59/2003).

- El tratamiento de los límites de uso de los certificados de sello de órgano, posibilidad que nos parece, más que conveniente, absolutamente necesaria para evitar posibles abusos del sello, especialmente en caso de robo de éste.

- El tratamiento de la representación legal tienen determinados órgano, que, en el caso del sello, quizás se tendría que limitar de manera expresa.

En resumidas cuentas, corresponde a cada Administración determinar los supuestos y los trámites en que se puede aplicar el sello de órgano, si bien esta determinación no se puede llevar a cabo indiscriminadamente, sino a partir de una valoración adecuada de los actos administrativos que se pueden hacer de forma automatizada, de acuerdo con el principio de proporcionalidad, y sin que se produzca una merma de garantías del administrado o la administrada.

Una cuestión también que hay que considerar con respecto a la actuación administrativa automatizada es la que deriva del tratamiento de datos de carácter personal. Tal como señala VALERO TORRIJOS, en relación con los actos administrativos discrecionales la automatización ha de tener en cuenta el margen de decisión de que dispone el órgano administrativo para adoptar la decisión[28]. También se debe tener presente la previsión del artículo 13 de la Ley orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, conforme al cual se reconoce el derecho de los ciudadanos «a no estar sometidos a una decisión con efectos jurídicos, sobre ellos o que los afecte de manera significativa, que se base únicamente en un tratamiento de datos destinadas a evaluar determinados aspectos de su personalidad», legitimándolos para impugnar los actos administrativos que impliquen una valoración de su comportamiento, el fundamento único del cual sea un tratamiento de datos de carácter personal que ofrezca una definición de sus características o de su personalidad.

[28] VALERO TORRIJOS, J. *Op. cit*., pág. 75.

3.6. Nulidad o anulabilidad de la actuación administrativa automatizada

Hasta ahora hemos tratado los diferentes elementos o criterios jurídicos que se tienen que considerar a la hora de automatizar los procesos. La falta de cumplimiento de estos criterios significa un vicio o un defecto que, en función de los supuestos, puede afectar al acto emitido, lo cual nos lleva a analizar la invalidez de los actos jurídicos.

La teoría de la invalidez de los actos jurídicos es propia de la parte general del derecho civil y comuna para todas las ramas jurídicas. Así, el artículo 6.3 del Código Civil establece que «los actos contrarios a las normas imperativas y a las prohibitivas son nulos de pleno derecho, salvo que en ellas se establezca un efecto distinto para lo caso de contravención».

Esta disconformidad con respecto a la ley o esta invalidez puede provenir:

1) De la falta de algún elemento esencial para la formación del acto o el negocio jurídico (inexistencia).
2) De la celebración de un acto viciando, un mandato o una prohibición legal (nulidad de pleno derecho).
3) De la existencia de un vicio o un defecto del acto (nulidad relativa o anulabilidad).

Podemos trasladar esta distinción al ámbito administrativo, con algunos matices:

1) En primer lugar, en derecho administrativo la teoría de la invalidez se agota en el estudio de dos únicas categorías: nulidad absoluta y anulabilidad. Así, autores como GARRIDO FALLA señalan que el tratamiento jurídico de la inexistencia no se tiene que diferenciar del de la nulidad absoluta.

2) En segundo lugar, a diferencia de lo que pasa en el derecho común, en derecho administrativo la regla general está constituida, pues, por la

presunción de validez de todas las actuaciones administrativas, y por eso mismo el acto administrativo inválido está dominado por la regla básica de la anulabilidad, mientras que la nulidad de pleno derecho se reserva a los supuestos indicados taxativamente en el artículo 62 de la Ley 30/1992 o en una disposición de rango legal que la regule expresamente con este carácter.

3) En tercer lugar, existen vicios que ni siquiera dan lugar al vicio de la anulabilidad, como las irregularidades no invalidantes (artículo 63.2 de la Ley 30/1992).

4) Finalmente, el principio del *favor acti* no sólo limita la nulidad y crea las irregularidades no invalidantes, sino que facilita técnicas de garantía de conservación del acto.

En este sentido, ya hemos indicado que la regla general es la anulabilidad. La nulidad se aplica exclusivamente en los supuestos que fija taxativamente la ley, que son los enumerados en el artículo 62.1 de la Ley 30/1992[29].

[29] "Los actos de las Administraciones públicas son nulos de pleno derecho en los casos siguientes:

a) Los que lesionen los derechos y libertades susceptibles de amparo constitucional.
b) Los dictados por órgano manifiestamente incompetente por razón de la materia o del territorio.
c) Los que tengan un contenido imposible.
d) Los que sean constitutivos de infracción penal o se dicten como consecuencia de ésta.
e) Los dictados prescindiendo total y absolutamente del procedimiento legalmente establecido o de las normas que contienen las reglas esenciales para la formación de la voluntad de los órganos colegiados.
f) Los actos expresos o presuntos contrarios al ordenamiento jurídico por los que se adquieren facultades o derechos cuando se carezca de los requisitos esenciales para su adquisición.
g) Cualquier otro que se establezca expresamente en una disposición de rango legal."

Si trasladamos los conceptos de la invalidez de los actos administrativos a la actuación administrativa automatizada, tenemos que distinguir los supuestos que se pueden producir, ya que la consecuencia jurídica que deriva de cada uno también es diferente.

Ya hemos advertido que, de acuerdo con la doctrina de las potestades administrativas, cualquier actuación tiene que estar amparada en una norma habilitadora, la cual en un primer nivel se configura por una norma con rango de ley habilitadora y una norma de segundo nivel que concreta las condiciones de aplicación.

Este principio, aplicable con carácter general a la realización de actos administrativos por medios electrónicos, se puede trasladar igualmente a la actuación administrativa automatizada. Por eso hace falta que la actuación administrativa automatizada esté amparada en una habilitación suficiente: si ésta no se produce, se rompe la regularidad del mecanismo de producción de actos administrativos.

Este vicio entraría en la consideración de invalidez absoluta y, trasladada al ámbito del derecho administrativo, determinaría un supuesto de nulidad absoluta, ya sea para considerar que se trata de un acto dictado por un órgano manifiestamente incompetente (letra b del artículo 62.1), ya sea por un supuesto de prescindir totalmente del procedimiento (letra e del mismo artículo).

Esto significa que una automatización de procesos hecha al margen de los criterios establecidos por la normativa habilitadora o que no se adecuara a esta normativa sería incardinable en un supuesto de nulidad de pleno derecho.

Esta nulidad de pleno derecho supone:

1) La imposibilidad de convalidación, ya que ésta sólo es predicable de los actos anulables.

2) La suspensión automática de la ejecutividad del acto nulo de pleno derecho cuando es impugnado alegando esta nulidad (artículo 111 de la Ley 30/1992).

3) La posibilidad de que la Administración declare de oficio la nulidad, previo dictamen favorable del Consejo de Estado u órgano consultivo equivalente de la Comunidad Autónoma. En cambio, si se trata de actos anulables, la Administración los deberá declarar lesivos para el interés público y, posteriormente, impugnar ante el orden jurisdiccional contencioso administrativo.

4) Los efectos de la declaración son *ex tunc*, es decir, desde la fecha en que se dicta el acto. Por contra, la anulabilidad produce efectos *ex nunc*, es decir, desde la fecha en que se declara.

Así pues, la regla general sería la nulidad de pleno derecho, vicio determinante de la actuación administrativa que, en el ámbito de la utilización de los medios electrónicos, es especialmente significativo vista la falta de confianza que la utilización de estos medios todavía genera actualmente entre los administrados.

Por otra parte, nos podríamos plantear la posibilidad de anulabilidad de las actuaciones administrativas llevadas a cabo, la cual se podría producir en los supuestos de una programación inadecuada. Eso deriva del carácter restrictivo que se predica de la nulidad de pleno derecho, aplicable exclusivamente a los supuestos antes mencionados. Por contra, una programación inadecuada se consideraría o se podría considerar una causa de anulabilidad, recogida en el artículo 63 de la Ley 30/1992[30].

[30] "1. Son anulables los actos de la Administración que incurran en cualquier infracción del ordenamiento jurídico, incluso la desviación de poder.
2. No obstante, el defecto de forma sólo determinará la anulabilidad cuando el acto carezca de los requisitos formales indispensables para alcanzar su fin o dé lugar a la indefensión de los interesados."

En cambio, una programación indebida o cualquier otro defecto no se podría considerar actuación administrativa irregular, ya que difícilmente se producen los supuestos legalmente previstos a este efecto[31].

Finalmente, se podría producir una desviación informática de poder, cosa que implicaría trasladar al campo de la informática decisional la doctrina de la desviación de poder[32]. En este sentido, la desviación de poder, configurada como a supuesto de anulabilidad, tendría lugar cuando la programación de los programas y las aplicaciones que tienen que llevar a cabo la actuación administrativa automatizada correspondiente, aunque aparentemente se adecua a la legalidad aplicable, se ha realizado para una finalidad o persigue una finalidad diferente de la que prevé el ordenamiento jurídico.

Esta finalidad que se convertiría en desviación de poder puede ser privada, pero también pública: sería pública cuando la finalidad perseguida fuera diferente de la prevista y fijada por la norma que atribuye la potestad correspondiente. Sería el caso, por ejemplo, en que una automatización determinada no persiguiera una mejora en la prestación de los servicios hacia los ciudadanos, sino privarlos del ejercicio de derechos o de garantías que les reconoce el ordenamiento jurídico.

En estos casos, ya hemos indicado que la sanción sería la de la anulabilidad. No obstante, por el hecho de que se trata del elemento psicológico o volitivo que guía la

---

[31] Serían: 1) Actos carentes de los requisitos formales no indispensables para alcanzar su finalidad y que no originen indefensión. 2) Actuaciones administrativas realizadas fuera del tiempo establecido, que sólo implicarán la anulabilidad del acto cuando así lo imponga la naturaleza del término o plazo. 3) Actuación de autoridades y personal al servicio de las administraciones públicas cuando concurran motivos de abstención, que no implicará necesariamente la invalidez de los actos en que hayan intervenido (artículo 28.3 de Ley 30/92), sin perjuicio, cuando proceda, de la responsabilidad.

[32] Cabe recordar que la desviación de poder se define como el ejercicio de las potestades administrativas para fines distintos de los previstas en el ordenamiento jurídico. En definitiva, se trata de aquellos supuestos en que la Administración se separa de la persecución del interés general que debe guiar su actuación.

actuación administrativa, acreditar la existencia es ciertamente dificultoso, aunque no se exige jurisprudencialmente una prueba plena.

4. Técnicas de determinación de la viabilidad informática de la actuación administrativa a automatizar

La actividad de las administraciones públicas se tiene que desarrollar con un grado elevado de garantías para los ciudadanos, como contrapunto de los poderes exorbitantes de que disponen con el fin de poder cumplir con su función.

La actuación administrativa automatizada, como hemos analizado en el capítulo anterior, genera una serie de riesgos particulares que hay que dirigir suficientemente para evitar que esta nueva posibilidad se convierta en fuente de conflictos y problemas de ineficacia.

Hace falta recordar que el anexo de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, define la actuación administrativa automatizada como el «actuación administrativa producida por un sistema de información adecuadamente programado sin necesidad de intervención de una persona física en cada caso singular. Incluye la producción de actos de trámite o resolutorios de procedimientos, así como de meros actos de comunicación».

Cómo hemos visto, el requisito esencial para poder llevar a cabo una actuación administrativa automatizada es la programación adecuada del sistema de información, concepto jurídico indeterminado que hay que llenar de contenido, ya que una programación inadecuada puede implicar la anulación en el mejor de los casos de uno o de todos los actos singulares dictados de forma automatizada.

En este sentido, también resulta conveniente recordar que el *Gran Diccionario de la Lengua Catalana* define el término *adecuado, -ada* como «apropiado, proporcionado, completamente suficiente, en un objeto, a un fin, a un propósito». Así pues, resultará necesario, en principio, garantizar que la interpretación de la norma que se codifica de forma informática es lo bastante completa para no producir discriminación al ciudadano afectado por el acto singular, como veremos posteriormente.

Aunque la Ley 11/2007 no define legalmente el concepto de *sistema de información*, sí que aporta una definición de *aplicación*, en el sentido de «programa o conjunto de programas cuyo objeto es la resolución de un problema mediante el uso de informática» - en este caso, la necesidad de efectuar un acto administrativo singular, sea decisorio, de constancia, etc.

El primer paso para llegar a una programación adecuada de una aplicación es precisamente la interpretación "informática" de la norma reguladora de la actuación administrativa a automatizar, aspecto del cual nos ocupamos a continuación.

4.1. La interpretación de las normas jurídicas

El problema de la interpretación de las normas de derecho privado ha sido abordado con profundidad por CASTÁN[33], que, siguiendo a SAVIGNY, introduce las modalidades principales de la interpretación e identifica los elementos principales del proceso de interpretación:

- El elemento literal o filológico, que constituye el primer estadio del proceso interpretativo, porque, al expresar la ley con palabras[34], hay que obtener el significado verbal que resulte, de acuerdo con las reglas gramaticales.

  En caso de conflicto de posibles significaciones, habrá que escoger, en general, el significado que se repute más idóneo en razón de conexión con otros términos del precepto interpretado o de la materia de que se trate.

---

[33] CASTÁN TOBEÑAS, J. *Teoría de la aplicación e investigación del derecho. Metodología y técnica operatoria en derecho privado positivo*. Madrid: Instituto Editorial Reus, 1947.

[34] Y, en concreto, a menudo en lenguaje natural, poco definido y que presenta posibles ambigüedades, vaguedades y otros problemas en cuanto a una interpretación adecuada.

Asimismo, tradicionalmente se ha considerado que cuando un término tiene un significado común y otro técnico, en general hay que escoger el significado común, dado que la norma se dirige a una generalidad de personas. Este aspecto ha generado la aparición de definiciones «a los efectos de esta norma» de manera más o menos generalizada, sobre todo en los sectores del ordenamiento jurídico más tecnificados, como el derecho administrativo – por contraste con el derecho privado, por ejemplo –, el derecho tributario y la Seguridad Social.

- El elemento lógico, racional o teleológico, que completa y controla los resultados de la interpretación gramatical. La interpretación lógica se efectúa atendiendo a los elementos de la fórmula legislativa (lógica interna) y a los elementos que forman el presupuesto de la norma (lógica externa). Mientras que la lógica interna implica el conjunto de deducciones e inducciones que permite comprender la voluntad del legislador (*ratio legislatoris*), la lógica externa es un proceso más profundo orientado a comprender el fundamento y la finalidad esencial de la norma (*ratio legis*), así como la oportunidad de esta norma (*occasio legis*).

  Posteriormente abordaremos con más profundidad la interpretación lógica, por su íntima relación con la automatización de la aplicación de la norma.

- El elemento sistemático, que consiste en relacionar la norma que hay que interpretar con aquéllas otras que integran una institución jurídica, y cada institución con el resto, hasta llegar a los principios fundamentales del sistema jurídico.

- El elemento histórico, que permite mejorar la comprensión de la norma en consideración a los precedentes históricos, sean remotos o inmediatos, así como a los trabajos preparatorios de la ley (aunque casi toda la doctrina considera que éstos últimos tienen un valor muy relativo).

- El elemento comparativo, que consiste en analizar la norma de acuerdo con el derecho comparado siempre como medio subsidiario en la interpretación.

- El elemento sociológico, que permite considerar la norma a la luz de las exigencias de la vida real y de los intereses y las necesidades de la colectividad.

- El elemento práctico (técnico y económico), que consiste en analizar la norma de acuerdo con el elemento de hecho que la norma disciplina, y que trata de elementos de naturaleza técnica o del sustrato económico de las relaciones jurídicas. Se trata de un factor incluido en los elementos lógico y sociológico de la interpretación.

Con respecto a las reglas de interpretación, CASTÁN diferencia las reglas legales de las reglas doctrinales, aun advirtiendo de la necesidad de aplicar las reglas doctrinales y, en particular, los aforismos jurídicos con mucha cautela. Finalmente, CASTÁN identifica los cuatro tipos de interpretación que se detallan acto seguido, según la función que cumplen:

- Interpretación declarativa, que se dirige a explicar el texto de la ley, especialmente cuando presenta ambigüedades, oscuridad o vaguedades. Esta interpretación puede ser estricta o lata según se dé un sentido más limitado o más amplio a un término concreto, de acuerdo con el resto de términos de la norma a interpretar.

- Interpretación restrictiva, que ofrece como resultado restringir el significado de los términos legales cuando expresan más de lo que quiso al legislador. Sería procedente en casos como los siguientes: si el texto contradice otro texto de la ley, si la ley contiene una contradicción o si la norma, sin interpretación restrictiva, va más allá de la finalidad para la cual fue ordenada.

- Interpretación extensiva, que amplía el significado natural de los términos legales cuando expresan menos de lo que quiso al legislador. Ocurriría en casos como los siguientes: si la ley adopta una expresión concreta en lugar de una expresión abstracta más adecuada para la finalidad perseguida por la norma o si la ley pronuncia un concepto general que aplica por vía indicativa o

demostrativa a casos particulares (incluyendo los argumentos por identidad de razón y *a fortiori*).

- Interpretación modificativa, que opera cuando la expresión literal de la norma da a entender algo cualitativamente diferente de aquello querido por el legislador, y que fundamentaría casos de inaplicación legal o de desplazamiento de la aplicación de las normas en casos de conflicto. Vale decir que se trata de un tipo de interpretación que la doctrina considera aplicable, en general, a la mejora de una expresión normativa concreta, igual que sucede con las interpretaciones restrictiva y extensiva.

En palabras de CASTÁN, la interpretación no es una operación mecánica en que no existe un cierto margen de libertad y discrecionalidad, aunque en cualquier caso se trata de un acto de ciencia, y no político; una justa ponderación de los elementos gramaticales, logicosistemático, históricos y finalistas o teleológicos, que parece la forma más segura de llegar a una interpretación que posea un valor de verdad y rectitud (LEGAZ).

Paralelamente, CASTÁN advierte de los peligros asociados a una construcción puramente lógica de las normas jurídicas, la cual podría llegar a reducir la ciencia jurídica a una especie de matemática del derecho (HERNÁNDEZ-GIL), advertencia que compartimos plenamente y que la doctrina iusfilosófica más autorizada ha mostrado posteriormente.

4.2. La interpretación lógica de las normas

Vistas la importancia de la interpretación lógica y su íntima conexión con el lenguaje informatizado, a continuación exponemos algunas de las perspectivas que ha trabajado la doctrina científica más reciente.

La lógica es la ciencia que estudia sistemáticamente los enunciados válidos o formalmente verdaderos (entendiendo que un enunciado es formalmente verdadero si

son verdaderos todos los enunciados que tienen el mismo esquema lógico) o que trata de la relación de consecuencia entre enunciados. Además, sin embargo, de la lógica propiamente dicha, actualmente se incluyen dentro del título de lógica las investigaciones metalógicas, las cuales comprenden la teoría de la deducción o el estudio de las propiedades de los conjuntos de axiomas y la semántica formal.

En otras palabras, podemos decir que la lógica es el estudio de los razonamientos bien hechos. La lógica analiza la estructura de los razonamientos y señala las condiciones de su validez. Por lo tanto, es el procedimiento sistemático y fundado que nos permite diferenciar un razonamiento correcto, o válido, de otro de incorrecto, o inválido. Así pues, es también el estudio de la deducción lógica o de la inferencia lógica.

Se puede hablar del inicio de la lógica moderna a partir del álgebra de BOOLE, interpretable como lógica de clases y de enunciados. DE MORGAN y PEIRCE crearon la lógica de relaciones. FREGE introdujo los cuantificadores, dio la primera versión sistemática y enteramente formalizada del cálculo de predicados y emprendió la reducción de la aritmética a la lógica. RUSSELL y WHITEHEAD impusieron, en *Principia mathematica* (1910-1913), el simbolismo más simple de PEANO y evitaron la inconsistencia del sistema de FREGE con la teoría de los tipos.

En cuanto a las investigaciones metalógicas, es imposible exagerar la importancia del descubrimiento de GÖDEL sobre la compleción del cálculo de predicados de primer orden (1930) y la incompletitud de las lógicas de orden superior (1931). La respuesta a la cuestión sobre la decidibilidad de la lógica, descrita por HILBERT como la más importante, la dio CHURZ (1936) como negativa con respecto a la lógica de predicados de primer orden, pero se continúa investigando, con resultados positivos, la decidibilidad de clases de fórmulas.

Por *semántica* tenemos que entender la parte de la lógica que corresponde en el ámbito de lo que se denomina *metalógica* y que estudia los sistemas lógicos desde el punto de vista de sus posibles interpretaciones, principalmente la interpretación normal, o pensada al elaborar el sistema, si es que tal interpretación existe. Denominada también *teoría de los modelos*, la semántica de los lenguajes formales se debe distinguir de la *semántica lingüística* o *semántica de los lenguajes naturales*.

Aunque el estudio sistemático de la semántica lógica es posterior al estudio de los problemas sintácticos y es obra sobre todo de TARSKI y de CARNAP, algunas nociones semánticas son tan antiguas como la misma lógica y se pueden encontrar ya en ARISTÓTELES.

La semántica moderna tiene sus precedentes en BOLZANO y FREGE, y es con TARSKI que alcanza sus fundamentos, puesto que este autor se propone definir la noción de verdad sólo para los lenguajes formales de estructura totalmente explícita y, así, definir previamente la noción de *cumplimiento*, o *satisfacción*, para las fórmulas elementales, de dar después una definición recursiva de satisfacción para toda clase de fórmulas y de ofrecer finalmente la noción de *verdad* para oraciones o fórmulas sin variables libres. La obra de TARSKI permitió emprender con rigor el estudio del carácter de satisfacción y de compleción, como también de los modelos, de los sistemas axiomáticos, como veremos más adelante.

Concretando un poco más, GARCÍA GONZÁLEZ[35] indica que la lógica fue desarrollada en un intento de crear un lenguaje universal basado en principios matemáticos, de manera que se basa en principios formales que deberemos tener en cuenta a la hora de considerar si un lenguaje de representación del conocimiento (por ejemplo, de un conjunto de normas que ordenan una actuación que automatizamos) es una lógica:

- Vocabulario: colección de símbolos representados como caracteres, palabras, iconos o sonidos, símbolos que se dividen en cuatro grupos:
    - Símbolos lógicos, que son independientes del dominio de conocimiento, como pueden ser calificadores como "∀" o conectivas como "∧".
    - Constantes, que son independientes del dominio de conocimiento e identifican individuos, propiedades o relaciones en este dominio o universo de discurso, como por ejemplo "representante".

[35] GARCÍA GONZÁLEZ, R. *A Semantic Web Approach to Digital Rights Management*. Ph.Thesis. Barcelona: Universitat Pompeu Fabra, 2005.

  - Variables, que son símbolos ilimitados aplicados de acuerdo con los cuantificadores.
  - Símbolos de puntuación, que separan o agrupan otros símbolos, como las comas y los paréntesis.

- Sintaxis: una lógica debe tener reglas gramaticales que determinen como se combinan los símbolos para formar sentencias correctas.

- Semántica: es necesario realizar manifestaciones con significación, lo cual comprende una teoría de referencia que determine cómo se relacionan las constantes y las variables con los objetos en el universo de discurso. Además, incluye una teoría de la verdad que permite diferenciar manifestaciones verdaderas de manifestaciones falsas.

- Inferencia: se lleva a cabo mediante reglas que determinan cómo se generan unos patrones a partir de los otros, cosa que permite mecanismos de razonamiento y la generación de nuevo conocimiento, además de poder justificar cómo se ha llegado a una conclusión.

Un lenguaje formal o un cálculo lógico permite decidir:

1. Si un símbolo pertenece al lenguaje.
2. Si una fórmula determinada es una expresión bien formada del lenguaje.
3. Si una secuencia sintáctica de fórmulas constituye una demostración o una deducción. En todo caso, un cálculo o un procedimiento de deducción pone de manifiesto que todo razonamiento válido equivale a una expresión lógica que siempre es verdadera. Una expresión tal es una «verdad lógica» o una «verdad formal».

La lógica de enunciados o proposiciones y la lógica de predicados – conocida también por lógica de primer orden – son dos lenguajes lógicos formales. La distinción entre el uno y el otro se basa en la diferente capacidad expresiva del lenguaje. Los símbolos (alfabeto) del lenguaje de lógica proposicional se refieren, básicamente, a enunciados

y a conexiones entre enunciados, y dejan intacta su estructura interna, mientras que los símbolos (alfabeto) de la lógica de predicados penetran en el interior de los enunciados y hacen referencia a los términos de que se componen los enunciados.

4.3. Los lenguajes de la lógica

Hoy día, casi todos los lenguajes de la lógica se ordenan en torno a la lógica de primer orden y se pueden clasificar de acuerdo con seis parámetros (GARCÍA GONZÁLEZ):

- Sintaxis: la diferencia más obvia – pero menos importante – entre los diferentes lenguajes lógicos es la notación que utilizan, ya que, en términos de potencia expresiva, las diferencias sintácticas no son relevantes.

  La lógica de primer orden tipada es una extensión sintáctica de la lógica de primer orden, tiene idéntica semántica y existen sustituciones sintácticas directas para traducir entre ellas:

  $(\forall x{:}t)\ \varphi(x) \equiv (\forall x)\ (t(x) \rightarrow \varphi(x))$ y $(\exists x{:}t)\ \varphi(x) \equiv (\exists x)(t(x) \wedge \varphi(x))$.

- Operadores: cada lenguaje lógico define un conjunto de operadores permitidos o de combinaciones entre éstos.

  La lógica de primer orden dispone de los operadores comunes de Boole: conjunción ($\wedge$), disyunción ($\vee$), negación ($\neg$), implicación ($\rightarrow$) y equivalencia ($\equiv$), más los cuantificadores universal ($\forall$) y existencial ($\exists$). También se pueden introducir algunos cuantificadores extendidos:

  Exactamente un cuantificador: $\exists!$, $(\exists!x)\ \varphi(x) \equiv (\exists x)\ (\varphi(x) \wedge \neg(\exists y)\ (\varphi(y) \wedge y \neq x))$.

  Cuantificador existencial único: $\exists!!$, $(\forall x)\ (\exists!!y)\ \psi(x,y) \equiv (\forall x)\ (\exists!y)\ (\psi(x,y) \wedge \neg(\exists z)\ (\psi(z,y) \wedge z \neq x))$.

  La lógica de Horn es un subconjunto de la lógica de primer orden que no tiene disyunción ($\vee$) en las conclusiones de la implicación ($\rightarrow$).

La lógica de enunciados o proposicional también es un subconjunto de la lógica de primer orden, sin cuantificadores.

- Teoría demostrativa: diferentes lenguajes lógicos restringen o amplían las pruebas permitidas. La lógica lineal restringe la prueba y permite que cada proposición sólo se utilice una vez en una demostración; la lógica no monótona, en cambio, extiende los procedimientos de prueba introduciendo asunciones por defecto que resultan consistentes con lo que se conoce en cada momento, y que podrían ser refutadas. La lógica refutable (*defeasible logic*) es un buen ejemplo.

- Teoría del modelo: define de qué manera la lógica se relaciona con el mundo, por ejemplo mediante los valores de verdad de las manifestaciones lógicas. La lógica de primer orden opera con los valor verdad/falso, mientras que la lógica difusa es multievaluada y utiliza factores de certeza, desde 0.0, que es ciertamente verdad, hasta 1.0, que es ciertamente falso.

- Ontología: una lógica no interpretada no tiene predicados predefinidos para no representar a ningún sujeto, sino que sólo dispone de símbolos y cuantificadores, operadores de Boole y variables. En la práctica, para facilitar el uso, algunos lenguajes lógicos incluyen predicados y axiomas predefinidos en forma de ontologías nativas. La teoría de conjuntos se utiliza para ofrecer fundamentos matemáticos, mientras que la lógica temporal y la lógica dinámica ofrecen ontologías temporales.

- Metalenguaje: es un lenguaje sobre el lenguaje. Se puede utilizar para definir, modificar o extender cualquier otro lenguaje.

  La lógica de primer orden se puede utilizar como metalenguaje de cualquier otro lenguaje lógico, incluyendo la misma lógica de primer orden.

  La lógica modal es una extensión metalingüística de la lógica de primer orden. Introduce verbos auxiliares que, en lugar de describir el mundo tal como es, describen el mundo tal como tiene que ser o tendría que ser o bien como

puede ser o podría ser. Los operadores modales se interpretan como obligación (□) y permiso (◊).

La lógica modal básica asume dos modos:

p debe ser necesariamente cierto (ha de): $\Box p \equiv \neg \Diamond \neg p$.
p puede ser posiblemente cierto (puede): $\Diamond p \equiv \neg \Box \neg p$.

La lógica deóntica se encuadra dentro de la lógica modal y resulta, como veamos, particularmente apropiada para los entornos normativos, como el sistema legal. A causa del hecho de que las leyes pueden ser infringidas (aunque existan sanciones previstas), no se puede considerar que nada obligatoriamente verdad sea verdad, de forma que hay que asumir el modo siguiente:

Cualquier cosa obligatoriamente cierta es de forma permisiva cierta; es decir, cualquier cosa obligatoria está permitida: $\Box p \rightarrow \Diamond p$.

Con respecto a la lógica como método de interpretación objetivo de la norma jurídica, tenemos que presentar brevemente la temática de la inferencia lógica, que se puede llevar a cabo mediante deducciones, abducciones, inducciones y analogías, como exponemos a continuación:

- La deducción – denominada también inferencia lógica porque es un tipo de razonamiento que trata de capturar la lógica – tiene como principal característica que preserva la verdad tal como determina la semántica, de forma que, de premisas verdaderas, garantiza una conclusión también verdadera. Las lógicas que permiten este tipo de razonamiento se llaman lógicas consistentes.

  Los tests semánticos, establecidos por el operador de implicación lógica o consecuencia lógica $\models$, ofrecen criterios para evaluar las reglas de inferencia. La consecuencia lógica opera en el nivel notacional, mientras que la inferencia

opera en el nivel referencial. Las reglas de inferencia definen el operador de demostrabilidad ⊢, que indica que alguna cosa se puede probar.

La implicación lógica es más fundamental que la demostrabilidad, porque deriva la verdad de las fórmulas de los hechos sobre el mundo. La demostrabilidad depende de las reglas de inferencia de una versión particular de la lógica, y estas reglas tienen que ser justificadas en términos de implicación lógica. Así, las propiedades deseables de la inferencia son:

- La satisfacción, que significa que todo aquello demostrable es verdad. Las reglas de inferencia son consistentes si la demostrabilidad ⊢ preserva la verdad como determina la implicación lógica semántica ⊨.

  $(\forall s{:}\text{Situación})(\forall p,q{:}\text{Proposición})\ (s \models p \rightarrow (p \vdash q \rightarrow s \models q))$.

- La completitud, que es el reverso de la satisfacción, de manera que todo lo que es verdad se puede demostrar.

  $(\forall s{:}\text{Situación})(\forall p,q{:}\text{Proposición})\ ((s \models p \rightarrow s \models q) \rightarrow p \vdash q))$.

Las reglas de inferencia en lógica proposicional, sin cuantificadores, son las siguientes:

Modus ponens: de p y $p \rightarrow q$, deriva q.
Modus tollens: de $\neg q$ y $p \rightarrow q$, deriva $\neg p$.
Silogismo hipotético: de $p \rightarrow q$ y $q \rightarrow r$, deriva $p \rightarrow r$.
Silogismo disjuntivo: de $p \vee q$ y $\neg p$, deriva q.
Conjunción: de p y q, deriva $p \wedge q$.
Adición: de p, deriva $p \vee q$.
Sustracción: de $p \wedge q$, deriva p.

Las reglas de inferencia para la deducción con cuantificadores son las que

mostramos acto seguido. Junto con las anteriores, conforman las reglas deductivas de la lógica de primer orden:

> Instanciación universal: de (∀x) φ (x), deriva φ (c), donde c es cualquier constante.
>
> Instanciación existencial: de φ (c), deriva (∃x) φ (x).
>
> Retirada de cuantificadores: si x no esté libre en φ, entonces de (∃x) φ deriva φ, y de (∀x) φ deriva φ.
>
> Adición de cuantificadores: de φ deriva (∀x) φ o (∃x) φ, donde x es cualquier variable.
>
> Sustitución de iguales por iguales: de los términos s y t donde s = t, deriva φ (t) de φ (s).

- La abducción es un proceso de generación de explicaciones posibles, y no se puede considerar un método válido de inferencia porque permite conclusiones falsas. Se podría resumir con la fórmula siguiente: de b ∧ a → b entonces quizás a.

- La inducción es un proceso de inferencia involucrado en el aprendizaje que trata de anticipar como se comporte un sistema. De una serie de actos, produce una generalización. No se puede considerar tampoco un método válido de inferencia porque no garantiza la verdad, y requiere la retracción de proposiciones cuando se encuentran contradicciones. Se puede expresar con la fórmula siguiente: de P (a), P (b)… concluye (∀x) P (x).

- La analogía es una combinación de inducción de segundo orden con la deducción que no preserva la verdad ni la falsedad. Sin embargo, resulta muy útil para la la argumentación o el razonamiento basado en casos. Se puede expresar con la fórmula siguiente: de P(a) → P(b) ∧ R(a) → R(b) puede que Q(a) → Q(b).

Resulta evidente anticipar la importancia del aspecto lógico y semántico en relación con los sistemas de actuación administrativa automatizada, en consideración a las necesidades de satisfacción y compleción en la interpretación de la norma o conjunto de normas a aplicar de forma automática, con el fin de cumplir el criterio de programación adecuada.

En el ámbito informático en general y, por lo tanto, en lo que ahora nos interesa, el lenguaje lógico de base a utilizar es la lógica de predicados de primer orden, si bien veremos que se han definido también otros lenguajes lógicos de aplicación más específica a la comprensión de la norma (lógica deóntica) o del proceso de razonamiento jurídico argumentador no monótono (lógica refutable), que en general son representables mediante lógica de primer orden. Asimismo, en cuanto a la representación del conocimiento jurídico, la lógica descriptiva será un aspecto de relevancia notable, además de una herramienta muy eficiente para describir los elementos del problema jurídico que trata el sistema de actuación administrativa automática.

4.4. La lógica en la doctrina jurídica reciente

A pesar de que al final de la primera mitad del siglo XX la doctrina jurídica hablaba de manera general de una crisis importante del derecho y, como conexión con ésta, del descrédito de todas las formas de positivismo y, por lo tanto, de la lógica jurídica, algunos desarrollos de la teoría del derecho a partir de la Segunda Guerra Mundial han implicado un nuevo interés por los estudios de lógica jurídica, partiendo de la filosofía analítica y, en particular, de la problemática del análisis del lenguaje de la Escuela de Oxford, en el contexto más general del estudio de la lógica de la ciencia tratada en el Círculo de Viena fundado por MORITZ SCHLICK, como expone BEUCHOT[36].

[36] BEUCHOT, M. *Historia de la filosofía del lenguaje*. Méjico: Fondo de Cultura Económica, 2006.

FASSÒ[37] ha detallado el resurgimiento del interés por el análisis lógico del lenguaje, incluyendo el lenguaje jurídico. KELSEN – en su última etapa –, ROSS y HART son buenos ejemplos de la recepción parcial de la filosofía analítica, la cual se muestra en su preocupación por clarificar el funcionamiento de los instrumentos lingüísticos de la investigación y determinar el uso correcto de estos instrumentos. La filosofía analítica y del lenguaje ha tenido un impacto considerable en la metodología de la interpretación del derecho y de la misma teoría del derecho.

Después de su contacto con los neopositivistas de los Estados Unidos de América, Kelsen llegará a reconocer que entre el acto de voluntad – que es un hecho y, por tanto, un ser – y la validez de la forma – que es un deber ser – existe un nexo, y que la validez es el significado del acto de voluntad, cosa que implica que la norma es la forma lógica de un mandato.

Como indica PÉREZ LUÑO[38], KELSEN distingue la proposición normativa de la norma jurídica: mientras que ésta última supone una prescripción establecida por la autoridad jurídica, la proposición normativa es un juicio formulado por la doctrina en que se describe la norma. El "deber ser" que hay en los dos términos (proposición normativa y norma jurídica) es diferente: prescriptivo en la norma jurídica y simplemente descriptivo en la proposición normativa. Eso implica que una proposición normativa pueda ser considerada verdadera o falsa en función de la correspondencia de su contenido con la realidad normativa descrita, y que la norma jurídica sólo pueda ser válida o inválida, pero que no tenga sentido predicar de una norma el carácter de veracidad o falsedad, cosa que implicaría la imposibilidad de una lógica de las normas.

ROSS considera la normatividad del derecho una clase de lenguaje que constituye un fenómeno real: así, un sistema de normas es válido si es idóneo para funcionar como un esquema de interpretación del conjunto de acciones sociales correspondiente, de manera tal que sea posible comprender este conjunto de acciones como un todo coherente de significados y motivación, y que dentro de este conjunto sea posible, con

---

[37] FASSÒ, G. *Historia de la filosofía del derecho (3). Siglos XIX y XX*. Madrid: Pirámide, 1988.

[38] PÉREZ LUÑO, A.E. *Manual de informática y derecho*. Barcelona: Ariel, 1996.

ciertos límites, la previsión. Para ser válida, la aserción de la norma tiene que ser verificable empíricamente, con referencia a hechos sociales.

HART, representante de la jurisprudencia analítica de AUSTIN, tomará de KELSEN el concepto de norma como concepto central del derecho, y distinguirá normas primarias – que imponen obligaciones – de normas secundarias – de reconocimiento. Las normas secundarias proporcionan a los particulares y a los funcionarios públicos el medio para individualizar las normas obligatorias.

Partiendo también de la concepción neopositivista, BOBBIO plantea el problema de la cientificidad jurisprudencial entendiendo la jurisprudencia como análisis del lenguaje del legislador, que confiere a este lenguaje el carácter de discurso riguroso en relación con todo enunciado que sea coherente con el resto de enunciados del sistema. Eso circunscribe la teoría de BOBBIO a la teoría general del derecho normativista y formalista[39].

FROSINI[40] sostiene que, a pesar del resurgimiento del derecho natural después de la Segunda Guerra Mundial, se ha podido advertir un cambio en los intereses de la literatura jurídica con respecto a los aspectos semánticos, lógicos y tecnológicos del derecho. FROSINI denomina *derecho artificial* a esta orientación, una nueva perspectiva que se abre de la posibilidad de utilizar las invenciones electrónicas para solucionar problemas de orden jurídico.

Para FROSINI, el punto de mediación que ha permitido asociar la cibernética a la jurisprudencia ha sido la posibilidad de usar la lógica simbólica en el ámbito cultural de los estudios jurídicos, a los cuales ha llegado desde los estudios de filosofía matemática. El jurista tiene que efectuar una tarea de reducción del problema jurídico a su dimensión lógica con el fin de someter este problema a un proceso de transformación que se lleva a cabo de manera rigurosamente tecnológica; eso nos da

---

[39] Aunque sin rendirse al reduccionismo que implicaría limitarse al análisis formal de las normas, en perjuicio del valor del derecho, que corresponderá a la filosofía del derecho, o de su eficacia, que corresponderá a la sociología del derecho.

[40] FROSINI, V. *Cibernética, derecho y sociedad*. Madrid: Tecnos, 1982.

un producto de derecho artificial, producido por un razonamiento perfectamente objetivo o, mejor, totalmente tecnificado.

FASSÒ identifica la renovación del interés por los estudios de lógica jurídica precisamente como consecuencia de la misma actitud racionalista que informa el movimiento de la filosofía analítica, como evolución y concreción del uso general de la lógica jurídica que en general se ha podido encontrar en las teorías generales del derecho.

En este sentido, se puede observar un importante interés por los siguientes tipos de lógica y su aplicación al dominio legal:

- La lógica deóntica, como subespecie de lógica modal.
- La lógica refutable.
- La lógica descriptiva.

4.5. La lógica deóntica

La lógica del derecho ha sido considerada inicialmente lógica de las normas, o del lenguaje normativo[41], que se denomina lógica deóntica, y son exponentes destacados VON WRIGHT y KALINOWSKI, así como ALCHOURRÓN y BULYGIN[42].

Más allá de la pluralidad y la heterogeneidad de las acepciones de la lógica deóntica, PÉREZ LUÑO[43] señala que implica precisamente la posibilidad de no extender las inferencias lógicas no tan sólo a las descripciones, sino también a las prescripciones, cosa que permite la construcción de una lógica de las normas, una "lógica sin verdad"

---

[41] FASSÒ, G. *Historia de la filosofía del derecho…* , *op. cit*.

[42] ALCHOURRÓN, C.E. y BULYGIN, E. *Introducción a la metodología de las ciencias jurídicas y sociales*. Buenos Aires: Astrea, 1987.

[43] PÉREZ LUÑO, A.E. *Manual de informática…*, *op. cit.*

aplicable a las consecuencias y las relaciones lógicas de las normas en función de su uso sintáctico en un contexto de deducción.

Como expone ALARCÓN[44], la expresión *lógica deóntica* fue utilizada por primera vez en el sentido actual en 1951 por GEORG H. VON WRIGHT[45]. Junto con los conceptos modales aléticos (necesidad, posibilidad, contingencia), con los conceptos modales existenciales (universalidad, existencia, vacuidad) y con los conceptos modales epistémicos (aquello verificado, aquello indeterminado, aquello falsificado), introdujo los conceptos modales deónticos: aquello obligatorio, aquello permitido, aquello prohibido.

Los presupuestos de la lógica deóntica inicial de VON WRIGHT, de carácter monádico, son los siguientes: 1) las cosas que llamamos *obligatorias*, *permitidas* o *prohibidas* son actos entendidos no en sentido individual, sino como propiedad que los califica; 2) con respecto a quién realiza el acto (el agente), existe un valor de ejecución del acto y un valor de no ejecución del acto, análogos a los valores clásicos de la verdad y la falsedad.

En esta primera conceptualización de la lógica deóntica, que se denomina *sistema estándar de lógica deóntica*, las variables y las constantes son análogas a las utilizadas en la lógica de enunciados, con algunas particularidades: las variables incorporan las letras O (de manera que Op quiere decir que es obligatorio hacer p) y P (de manera que Pp quiere decir que está permitido o no está prohibido hacer p), y las constantes reciben el significado deóntico correspondiente:

> " - " se refiere a la negación deóntica, de manera que "-Op" quiere decir que no es obligatorio hacer p

---

[44] ALARCÓN, C. «Las lógicas deónticas de Georg H. Von Wright», Revista DOXA, núm. 26, 2003.

[45] Aunque existen antecedentes de sistemas deónticos desde la obra de ERNST MALLY de 1926 denominada *The Basic Laws of Ought: Elements of the Logic of Willing*, como reporta GERT-JAN LOKHORST, «Mally's Deontic Logic», *The Stanford Encyclopedia of Philosophy (Winter 2008 edition)*.

" ^ " se refiere a la conjunción deóntica, de manera que O (p ^ q)" quiere decir que es obligatorio hacer p y q, y Op ^ Oq quiere decir que es obligatorio hacer p y es obligatorio hacer q

" v " se refiere a la disyunción deóntica, de manera que O (p v q) quiere decir que es obligatorio hacer p o q, y Op v Oq quiere decir que es obligatorio hacer p y es obligatorio hacer q

" ↔ " Se refiere a la coimplicación o equivalencia deóntica, de manera que Op ↔ Oq quiere decir que si y sólo si es obligatorio hacer p entonces es obligatorio hacer q

" → " se refiere a la implicación deóntica, de manera que "O (p → q)" quiere decir que es obligatorio p si se da p.

Adicionalmente, VON WRIGHT añade reglas específicas de inferencia deóntica a las ya existentes en la lógica proposicional ordinaria. En primer lugar, añade dos reglas sobre la interdefinibilidad:

OA → PA indica que si es obligatorio hacer p, entonces está permitido hacer p

PA ↔ -O-A indica que si está permitido hacer p, entonces no es obligatorio no hacer p.

En segundo lugar, introduce reglas para la distribución de operadores semánticos. Y, en tercer lugar, introduce tres "leyes sobre el compromiso":

OA ^ O (A → B) → OB indica que si es obligatorio hacer p, y hacer p implica obligación de hacer q, entonces también es obligatorio hacer q (que se considera tautológico)

PA ^ O (A → B) → PB indica que si está permitido hacer p, y hacer p obliga a hacer q, entonces también está permitido hacer q

-PB ^ O (A → B) → -PA indica que si no está permitido hacer q, y hacer p obliga a hacer q, entonces p tampoco está permitido.

La lógica deóntica monádica también surgió a partir de los trabajos de KANGER i ANDERSON sobre la reducción de la lógica modal, con características parecidas al sistema deóntico estándar.

Posteriormente, a raíz de algunas paradojas detectadas en el sistema estándar, VON WRIGHT – y otros autores interesados en la lógica deóntica – introduce diversas ampliaciones añadiendo operadores diádicos, que permiten expresar, de manera implícita o explícita, relaciones entre dos argumentos que constituyen el antecedente y la consecuencia de la implicación deóntica.

Los sistemas diádicos disponen de tres estratos:

> La lógica proposicional clásica, basada en el estudio formal de las expresiones p, q...
> La lógica del cambio, basada en el estudio formal de las expresiones T, en la cual el evento descrito por pTq es una transformación de un estado inicial de cosas descritas por p hasta un estado final de cosas descrito por q.
> La lógica de la acción, basada en el estudio formal de las expresiones df, en la cual d (-pTp) indica que un agente, en una ocasión determinada, provoca el estado de cosas descrito por p, mientras que f (-pTp) indica que un agente, en una ocasión determinada, se abstiene de provocar el estado de cosas descrito por q.
> Por otra parte, con el símbolo " / " se introduce la posibilidad de describir mandatos, como en el caso de O (pTp) / qTpq).

Para PÉREZ LUÑO[46], la lógica deóntica – aunque esta conclusión se puede predicar, en términos generales, del resto de lógicas que presentamos – resulta muy relevante para la informatización del lenguaje jurídico, por un motivo doble: porque cuanta más estructuración lógica tenga el lenguaje jurídico, más fácil será su formalización informática, y porque la posibilidad de proyectar reglas lógicas sintácticas de las normas permite facilitar las operaciones del ordenador.

Actualmente la lógica deóntica es una de las ramas importantes de estudio de la interpretación de las normas, tanto legales como en otros sistemas normativos sociales, junto con otras modalidades de lógica modal, como la lógica temporal o la lógica condicional, y otros retos que ha presentado en cuanto a la posibilidad de

[46] PÉREZ LUÑO, A.E. *Manual de informática…*, *op. cit.*

razonar se pueden satisfacer mediante sistemas de razonamiento no monótono, como la lógica refutable.

Su aplicación práctica a los efectos de este trabajo es que permite evaluar el conjunto de normas en términos modales monótonos y ofrecer una primera interpretación de aquello que obliga una norma, de aquello que permite o que prohíbe, especialmente en términos de la relación entre las diferentes normas del sistema a automatizar.

Un ejemplo de aplicación jurídica basada en lógica deóntica lo constituye el sistema CLIME, según reportan BOER, HOESKTRA y WINKELS[47]. Se trata de un sistema de consejo legal basado en la web orientada a las normativas internacionales sobre clasificación de barcos, que realiza una gestión del conocimiento de las normativas y, en lo que ahora nos interesa, implementa un control de consistencia semiautomático relativo a las mismas normas. Esta experiencia muestra cómo se puede aplicar la lógica deóntica en torno a regulación típicamente administrativa.

Aunque no se puede sostener que la lógica deóntica sea absolutamente válida o útil para el razonamiento automatizado en razón de los retos que los sistemas deónticos todavía afrontan, sí que puede resultar útil para formalizar la interpretación puramente normativa de las normas a aplicar, cosa que permite ganar objetividad en el proceso interpretativo sin dejar de lado otros criterios lógicos de interpretación.

4.6. La lógica refutable

La denominada – con una cierta impropiedad – *lógica de argumentación* (denominada *nueva retórica* por FROSINI) ha aparecido con fuerza. Se preocupa por la lógica del procedimiento o del debate judicial (incluyendo el "procedimiento administrativo"), con una fuerte orientación a la lógica de aquello probable, a pesar de no ser absolutamente y científicamente "cierto".

---

[47] BOER, A; HOEKSTRA, R. i WINKELS, R.. «The CLIME Ontology», *Second International Workshop on Legal Ontologies*, 2001.

Esta concepción deriva de la constatación de la operativa de los casos particulares cuya prueba, como se muestra especialmente en el momento del proceso, se efectúa con argumentaciones de probabilidad y verosimilitud, y no con demostraciones de verdad. Esta corriente fue iniciada por PERELMAN, y son representantes de la misma TOULMIN y VIEHWEG (FASSÒ).

Entre nosotros, ATIENZA[48] ha indicado que el derecho es esencialmente una actividad de argumentación que tiene que ver con el lenguaje, con la lógica y con otras formas de argumentación poco tratadas en la cultura jurídica contemporánea, como la tópica, la retórica y la dialéctica.

La llamada *lógica de argumentación* ha sido particularmente desarrollada mediante los sistemas de razonamiento no monótono, y en especial por la lógica refutable (*defeasible logic*).

LUGER y STUBBLEFIELD[49] mantienen que la no monoticidad es un aspecto importante de la resolución de problemas y del razonamiento basado en sentido común que realizan las personas.

La lógica de predicados se basa en las asunciones de suficiencia en la descripción de predicados del dominio de la aplicación, de consistencia en la base de informaciones (ausencia de contradicciones entre las informaciones) y de incremento de la información (mediante las reglas de inferencia y, en concreto, de la deducción, que aumentan la información de forma monótona), condiciones que no se pueden considerar en muchos dominios, como en el caso jurídico.

Ante los sistemas monótonos, los sistemas no monótonos ofrecen mecanismos de razonar cuando no disponemos de bastante conocimiento sobre los predicados (por ejemplo, cuándo no se conoce la condición de verdad de un predicado, sobre la

---

[48] ATIENZA, M. *El derecho como argumentación*. Barcelona: Ariel Derecho, 2006.

[49] LUGER, G.F i STUBBLEFIELD, W.A. *Artificial Intelligence. Structures and strategies for complex problem solving*. Reading, Massachusetts: Addison-Wesley,1998.

inocencia de una persona) o considerando la información como una asunción vencible, es decir, que se puede modificar en consideración a información nueva.

Siguiendo a KOONS[50], podemos indicar que las aproximaciones lógicas al razonamiento vencible tratan esta materia como el estudio de las relaciones de consecuencia no monótona, en contraste con la monoticidad de la lógica clásica.

Una relación de consecuencia es una relación matemática que modela qué se sigue lógicamente a partir de qué. Estas relaciones se pueden definir de diversas formas: como relaciones de HILBERT, de TARSKI o de SCOTT. Así, una relación de consecuencia de HILBERT es una relación entre pares de fórmulas; una relación de TARSKI es una relación entre conjuntos de fórmulas (posiblemente infinitas) y fórmulas individuales, y una relación de SCOTT es una relación entre dos conjuntos de fórmulas.

En el caso de las relaciones de HILBERT y TARSKI, $A \models B$ o $\Gamma \models B$ significa que la fórmula B sigue de la fórmula A o del conjunto de fórmulas Γ. En el caso de las relaciones de SCOTT, $\Gamma \models \Delta$ significa que la verdad conjunta de todos los miembros de Γ implica (en algún sentido) la verdad de al menos un miembro de Δ. Hasta este momento, los estudios de lógica no monótona han definido relaciones de consecuencia lógica del estilo hilbertiano o tarskiano, más que en el sentido de SCOTT.

Una relación de consecuencia lógica de TARSKI es monótona sólo si satisface la condición siguiente, para todas las fórmulas p y todos los conjuntos Γ y Δ:

Si $\Gamma \models p$, entonces $\Gamma \cup \Delta \models p$.

Cualquier relación que no cumpla esta condición es no monótona. Una relación de consecuencia refutable – es decir, que se puede modificar en función de información nueva – debe ser necesariamente no monótona.

---

[50] KOONS, R. «Defeasible reasoning», *The Stanford Encyclopedia of Philosophy (Spring 2009 edition)*.

En la lógica no monótona de MCDERMOTT-DOYLE y en la lógica autoepistémica de MOORE, se introduce un operador modal M, que representa un tipo de posibilidad epistémica. Las reglas por defecto tienen la forma siguiente: ((p & Mq) → q); es decir, si p es verdad y q es "posible" (en el sentido relevante), entonces q también es verdad.

GOVERNATORI y ROTOLO[51] presentan el contenido de una teoría refutable como una estructura (F,R,$\succ$) donde F es un conjunto finito de hechos, R es un conjunto finito de reglas, y $\succ$ es una relación acíclica de superioridad sobre R. Los hechos se identifican con literales y son manifestaciones indiscutibles. Una regla expresa una relación entre un conjunto de premisas y una conclusión.

La lógica refutable permite establecer tres tipos de reglas sobre la fuerza de las relaciones:

- Reglas estrictas, con la forma $A_1, ..., A_n \rightarrow B$, que son los más fuertes, ya que cuando las premisas son indisputables siempre se da la conclusión.

- Reglas vencibles, con la forma $A_1, ..., A_n \Rightarrow B$, que describen los casos en que la conclusión se da cuando las premisas son tentativamente ciertas.

- Vencedores, con la forma $A_1, ..., A_n \sim> B$, que consideran las situaciones en que las premisas no garantizan las conclusiones, de manera que las premisas sólo impiden a otra norma soportar una postura contraria.

De forma parecida, una conclusión se puede etiquetar como definitiva o refutable, y podría ser retractable si aparecen nuevas premisas. La lógica refutable se basa en una teoría demostrativa constructiva para las conclusiones, de manera que podemos decir que existe una derivación para una conclusión y que no podemos dar una

[51] GOVERNATORI, G. y ROTOLO, A. «Changing legal systems: abrogation and annulement. Part I: Revision of defeasible theories», *Deontic logic in computer science*. Berlín: Springer, 2008.

derivación para una conclusión. Eso permite etiquetar las conclusiones de acuerdo con la notación siguiente:

> +ΔB, que quiere decir que disponemos de una demostración definitiva para B, para la cual sólo utilizamos hechos y reglas estrictas, como en el caso del razonamiento monótono propio de la lógica de predicados de primer orden.
>
> -ΔB, que quiere decir que no es posible construir una demostración definitiva para B.
>
> +δB, que quiere decir que disponemos de una demostración refutable para B.
>
> -δB, que quiere decir que no es posible dar una demostración refutable para B.

La lógica refutable es un formalismo escéptico, ya que, en caso de conflicto entre dos conclusiones sobre un mismo caso, las considera las dos poco probables – más que contradictorias entre ellas – mientras no se disponga de informaciones adicionales, un problema que se puede superar mediante el establecimiento de relaciones de superioridad entre las diferentes conclusiones.

De esta manera, la demostración refutable funciona al estilo argumentador: primero se trata de buscar un argumento a favor de la conclusión que se quiere probar; en segundo lugar, un argumento en contra de la conclusión que se trata de probar, y en tercer lugar, una refutación del argumento contrario, mostrando que éste no está fundamentado (por ejemplo, no se dan las premisas) o refutándolo (por ejemplo, porque es más débil lógicamente).

Cómo sucede con la lógica deóntica, a la cual ha ayudado a avanzar en algunos de los retos formales a que se enfrenta, la lógica refutable es objeto de un estudio reciente, teórico y práctico, muy amplio. Eso permite utilizarla como herramienta en el proceso interpretativo de la norma jurídica a automatizar, en este caso con una visión menos normativa del sistema, en beneficio de la dinámica del descubrimiento de la solución legal, más adecuada por vía de argumentación lógica, proposicional y modal

4.7. La lógica de descripción

Recientemente, en el dominio de la representación del conocimiento, y como evolución de diversos formalismos, encontramos la lógica de descripción, que permite representar el conocimiento de un dominio de aplicación (el "mundo") definiendo los conceptos relevantes del dominio (la terminología) y después utilizándolos para especificar propiedades de los objetos y de los individuos que ocurren en este dominio (la descripción del mundo).

Las lógicas de descripción han permitido avanzar mucho en la creación de sistemas de razonamiento aplicado a una amplia variedad de dominio, incluyendo el dominio legal, en conjunción con la construcción de ontologías. Por este motivo las presentamos sucintamente, y de esta manera cerramos la visión de conjunto de los formalismos para la interpretación lógica de las normas jurídicas.

Siguiendo a BAADER y NUTT[52], podemos exponer las características principales de la lógica de descripción. En primer lugar, a diferencia de otros formalismos de representación del conocimiento, las lógicas de descripción están equipadas – como su nombre indica – con una semántica formal basada en lógica. En segundo lugar, enfatizan el razonamiento como servicio principal ofrecido: el razonamiento permite inferir conocimiento representado implícitamente a partir del conocimiento explícito contenido en la base de conocimiento.

Las lógicas de descripción soportan la clasificación de conceptos y de individuos. La clasificación de conceptos determina relaciones de subconceptos y superconceptos entre los conceptos de una terminología concreta, también nombradas *relaciones de subsunción*, y de esta manera permite estructurar la terminología en forma de

[52] BAADER, F. i NUTT, W. «Basic description logics», *Description Logic Handbook*, editat per F. Baader, D. Calvanese, D.L. McGuinness, D. Nardi, P.F. Patel-Schneider. Cambridge University Press, 2002.

jerarquía de subsunción. Esta jerarquía ofrece información útil sobre la conexión entre diferentes conceptos, y se puede utilizar para acelerar otros sistemas de inferencia.

La clasificación de los individuos (o de los objetos) determina si un individuo concreto es siempre una instancia de un concepto determinado (por ejemplo, si esta relación de instancia viene dada por la descripción del individuo y la definición del concepto), y entonces ofrece información útil sobre las propiedades de un individuo.

Desde la perspectiva de la lógica, hay que decir que las lógicas de descripción son subconjuntos de la lógica de predicados de primer orden, como mantienen NARDI y BRACHMAN[53]. De hecho, el lenguaje de lógica de descripción ALC corresponde al fragmento de lógica de primer orden que se obtiene restringiendo la sintaxis a fórmulas que contengan dos variables. Asimismo, las lógicas de descripción están fuertemente relacionadas con las lógicas modales; específicamente, los conceptos ALC son directamente traducibles a fórmulas en lógica multimodal K.

Una aplicación de estos tipos de lógicas es la conceptualización del dominio legal, por ejemplo de las tipologías de representantes de las personas (representantes legales, representantes voluntarios) y de los roles definidos de forma normativa que los cumplen (de manera que el tutor es un representante legal de una persona incapaz, o el administrador único es el representante legal de una sociedad limitada), como en el caso del sistema PASSI desarrollado por la Agencia Catalana de Certificación[54].

A partir de esta conceptualización u ontología, se pueden implementar los mecanismos de razonamiento que permiten las lógicas de descripción, que son bastante eficientes a causa de un equilibrio entre expresividad y tratabilidad, y se puede dejar en otros mecanismos lógicos la resolución de otros problemas.

---

[53] NARDI, D. i BRACHMAN, R.J. «An introduction to description logics», *Description Logic Handbook*, editat per F. Baader, D. Calvanese, D.L. McGuinness, D. Nardi, P.F. Patel-Schneider. Cambridge University Press, 2002.

[54] ALAMILLO, I. y URIOS, X. «La gestión de identidades y capacidades por las Administraciones Públicas». TECNIMAP, 2006.

5. Análisis de casos relevantes de uso de automatización

En esta sección presentamos algunos casos relevantes de uso de automatización que, según nuestra opinión, resultan idóneos para aplicar esta nueva posibilidad reconocida legalmente:

- La expedición automática de recibo de registro electrónico.
- La comprobación automática de datos de solicitud.
- La digitalización automática de documentos.
- El impulso automático del procedimiento.
- El acto automático de constancia electrónica.
- La expedición automática de copia auténtica electrónica.
- La apertura y el cierre automático de libros electrónicos.
- La foliación automática de expedientes.
- La migración automática de documento electrónico.
- Los intercambios automáticos de datos entre administraciones públicas.
- La remisión automática de comunicación electrónica al ciudadano.

Con respecto a la posibilidad de automatizar actos administrativos de voluntad, ciertamente dependerá de dos factores principales: por un lado, la configuración del acto administrativo como potestad reglada o la predeterminación razonable de los casos en que actúa la discrecionalidad administrativa, y, por otra parte, la correcta informatización de la norma aplicada, en especial en términos de la necesaria motivación-justificación de los actos automáticos, que de acuerdo con nuestro criterio se tendrá que incorporar al texto de la resolución de forma particularmente detallada, sobre todo en los actos de voluntad y en los actos de juicio[55].

[55] En caso de que los consideremos de posible ejecución automática, ya que resulta más fácil, incluso intuitivamente, admitir que se puede programar una máquina para tomar decisiones,

GARCÍA DE ENTERRÍA y FERNÁNDEZ[56] sostienen que la motivación deb ser suficiente, debe dar razón plena del proceso lógico y jurídico que ha determinado la decisión. Este hecho conecta con la necesidad de codificar y poder reconstruir, para cada caso singular, las reglas lógicas – ya hemos visto que en una aproximación híbrida, con la aplicación de un método integrado por la lógica de predicados de primer orden, por las lógicas modales, deóntica y refutable aplicables, y por la lógica descriptiva en cuanto a la representación del dominio de conocimiento jurídico – que han sido aplicadas en el acto administrativo automático singular.

A continuación presentamos una serie de tablas analíticas que muestran la evaluación de los actos anteriores.

5.1. La expedición automàtica de recibo de registro electrónico

1. ¿Cuál es el contenido del acto?	- Descripción del acto. La emisión de recibo de registro electrónico consiste en la producción de un documento acreditativo de la presentación a un registro electrónico de una solicitud, escrito o comunicación. - Tipo de acto (del ciudadano/de la Administración, otros). Se trata de un acto administrativo, a solicitud del ciudadano, que puede disponer voluntariamente.

---

mientras que no parece posible que una máquina tenga juicio, aunque sea capaz de realizar inferencias lógicas, como hemos expuesto.

[56] GARCÍA DE ENTERRÍA, E. i FERNÁNDEZ, T.R. *Curso de derecho administrativo I*. Thomson-Civitas, 2008.

- Efectos que produce dentro del proceso (inicia, acaba, otros).

  Su efecto dentro del proceso administrativo es generar una prueba documental sobre el acto del ciudadano dirigido a la Administración.

2. ¿Cuál es la normativa aplicable al acto?

- Identificación de las normas aplicables.

  El artículo 35 de la Ley 30/1992, de 26 de noviembre, de régimen jurídico de las administraciones públicas y del procedimiento administrativo común, indica que, entre otros, los ciudadanos tienen derecho a obtener una copia sellada de los documentos que presenten, cuando lo aporten junto con los originales, así como a la devolución de los documentos originales, excepto cuándo estos originales tengan que constar en el procedimiento, derecho que se concreta en la correspondiente obligación de la Administración, prevista en el artículo 38.5 de la misma Ley 30/1992.

  El artículo 6.1 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, reconoce a los ciudadanos el derecho a relacionarse con las administraciones públicas utilizando medios electrónicos para el ejercicio de los derechos que prevé el artículo 35 de la Ley 30/1992, y concreta, en el artículo 24.1, la obligación de crear registros electrónicos para la recepción y la remisión de solicitudes, escritos y comunicaciones.

  El artículo 25.3 de la Ley 11/2007 establece que los registros electrónicos tienen que emitir automáticamente un recibo consistente en una copia autenticada del escrito, la solicitud o la

comunicación de que se trate, que tiene que incluir la fecha y la hora de presentación y el número de entrada de registro.

Asimismo, el artículo 25.4 de la Ley 11/2007 regula que se pueden aportar documentos que acompañen la correspondiente solicitud, escrito o comunicación, siempre que cumplan los estándares de formato y requisitos de seguridad que determinen los esquemas nacionales de interoperabilidad y de seguridad. Los registros electrónicos tienen que generar recibos acreditativos de la entrega de estos documentos que garanticen la integridad y el no rechazo de los documentos aportados.

- Significación jurídica del acto (acto reglado/discrecional y otras consideraciones).

  Se trata de un acto absolutamente reglado que la Administración tiene que llevar a cabo siempre que lo solicite el ciudadano, en el momento de presentar un escrito al registro, aunque el ciudadano puede disponer libremente.

- Condiciones jurídicas necesarias para que el acto se pueda realizar.

  Las condiciones jurídicas son las aplicables al acto de presentación de la solicitud, escrito o comunicación en el registro electrónico; es decir, las generales de capacidad y legitimación para actuar.

- Obligación legal o administrativa de documentar el acto.

  Como hemos indicado anteriormente, resulta exigible documentar el acto cuando lo solicita el ciudadano, aunque de la lectura del artículo 25.3 de la Ley 11/2007 se podría considerar que la

obligación existe siempre, incluso cuando el ciudadano no lo solicita. Esta lectura no modifica el hecho de que el recibo está disponible por parte del ciudadano, que puede decidir no conservarlo.

3. ¿Quién realiza el acto?

- Persona física (ciudadano).
  No aplicable.
- Trabajador de la Administración (si procede, funcionario).
  No aplicable.
- Órgano unipersonal de la Administración.
  La emisión del recibo de registro la lleva a cabo el registro, que tiene la consideración de órgano administrativo.

4. ¿En qué condición realiza el acto?

- En nombre propio y por cuenta propia.
  No aplicable.
- En calidad de órgano de una persona jurídica pública o privada (representación orgánica).
  En el caso de la emisión de recibo de presentación a un registro presencial, el funcionario de registro actúa en calidad de órgano de una persona jurídica pública o privada (representación orgánica).
  Podemos avanzar que esta actuación, en caso de ser realizada de forma automática, no exigirá lógicamente la determinación previa de la calidad en que no actúa ninguna persona.
- En calidad de representante legal de una persona física o jurídica, pública o privada.
  No aplicable.
- En calidad de representante voluntario de una persona física o jurídica, pública o privada.

No aplicable.

- En calidad de representante profesional de una persona física o jurídica (representación presunta).

  No aplicable.

5. ¿Existe posibilidad de sustitución personal?

   - Actos estrictamente personales.

     No aplicable.

   - Cualquier representante.

     No aplicable.

   - Cualquier persona física con una cualidad concreta (p. ej., cualquier trabajador público de un grupo).

     En el caso de la emisión de recibo de presentación a un registro presencial, cualquier funcionario de registro puede ejecutar el acto.

     Podemos avanzar que esta actuación, en caso de ser realizada de forma automática, no exigirá lógicamente la determinación previa de la posibilidad de sustitución personal.

6. ¿Genera un documento nuevo, se manifesta sobre un documento existente previamente o sobre un registro (de expediente o de libros)?

   - Genera un documento nuevo.

     En el caso del registro electrónico, el artículo 25.3 de la Ley 11/2007 exige la generación de un documento nuevo, consistente en la copia autenticada del escrito, la solicitud o la comunicación de que se trate, que tiene que incluir la fecha y la hora de presentación y el número de entrada de registro.

     Por su parte, el artículo 25.4 de la Ley 11/2007 obliga a la generación de recibos acreditativos de la entrega desde documentos complementarios aportados al procedimiento a que garanticen la integridad y el no rechazo de estos documentos.

- Se plasma en un documento existente.
  El recibo de registro, en el caso de la presentación presencial, se plasma en un documento ya existente, que precisamente es la copia de la solicitud, el escrito o la comunicación dirigida a la Administración, y que tiene que aportar al ciudadano.
- Se registra, sin generar manifestación documental.
  No aplicable.

7. ¿Requiere la comprobación previa de la identidad de quien realiza el acto?

- Sí/No.
  Sí, normalmente la aplicación de registro identifica al funcionario que actúa. También habrá que identificar el órgano de registro cuando actúe automáticamente.
  Determinación del método de identificación y autenticación de la persona que actúa.
  En principio, parece que se puede identificar la persona que opera el registro mediante cualquier sistema válido y, en concreto, resulta habitual hacerlo mediante nombre de usuario y palabra de paso, identificación que no trasciende a la gestión de la aplicación de registro, y que por lo tanto no es conocida por el ciudadano.
  Podemos avanzar que esta actuación, en caso de ser realizada de forma automática, tendrá que identificar el registro mediante el sello de órgano correspondiente, a nombre del mismo registro o de la Administración que es titular.
- Valoración del nivel de evidencia del método utilizado, de acuerdo con el esquema de CATCert.
  Como hemos indicado anteriormente, la

identificación de la persona que opera el registro es de nivel 1 o superior, mientras que la identificación del registro electrónico automatizado se tiene que hacer con nivel 3 o superior.

8. ¿Requiere la comprobación previa de la cualidad de quien realiza el acto?

- Sí/No.
  Sí, aunque esta comprobación se realiza de forma interna a la aplicación de registro y no es conocida por el ciudadano.
  En el caso de la actuación automatizada, se considera necesario comprobar la corrección del sello a utilizar, de manera que se utilice el sello adecuado para la producción de los sellos de registro.
- Comprobación de la facultad de actuación, orgánica o legal.
  Se comprueba la condición de persona habilitada para operar el registro, cuando ocurre.
- Comprobación de un apoderamiento o de una autorización, en representación voluntaria.
  No aplicable.
- Comprobación de la condición de profesional de colectivo autorizado.
  No aplicable.

9. ¿Requiere una comunicación confidencial previa o posterior?

- Sí/No.
  En general, no, pero depende del contenido de la copia sellada de registro, ya que si contiene datos personales de nivel alto (como una solicitud motivada por una discapacidad), entonces habrá que garantizar el secreto de la comunicación de retorno del recibo.
- Determinación del método de protección utilizado.

El método de protección a utilizar depende del mecanismo de comunicación utilizado. Por ejemplo, si la comunicación con el registro se produce a través de la sede electrónica, como resulta conveniente, entonces probablemente se utilizarán los mismos mecanismos de confidencialidad para proteger la entrega del recibo.

10. ¿Es de ejecución automàtica o mecànica total o parcialmente?

- Sí/No.
  El acto de emisión de recibo se puede llevar a cabo de manera manual o automática indistintamente.
- Determinación de los tratamientos automáticos o mecánicos.
  El automatismo posible consiste en la generación, el sellado y la entrega al ciudadano del recibo de registro.

5.2. La comprobación automática de datos de solicitud

1. ¿Cuál es el contenido del acto?

- Descripción del acto.
  La comprobación automática de datos de solicitud consiste en la verificación de estos datos, utilizando informaciones almacenadas en sistemas propios o pertenecientes a otras administraciones, con la posibilidad de llenar, totalmente o parcialmente, el formulario con la finalidad que el ciudadano verifique la información y, si ocurre, la modifique y la complete.

- Tipo de acto (del ciudadano/de la Administración, otros).

  Se trata de un acto administrativo, si procede a solicitud del ciudadano.
- Efectos que produce dentro del proceso (inicia, acaba, otros).

  El efecto de este acto en el proceso es detectar errores en los datos de la solicitud, por una parte, y facilitar al ciudadano la tarea de rellenar el formulario, por otra parte.

2. ¿Cuál es la normativa aplicable al acto?

- Identificación de las normas aplicables.

  El artículo 35.3 de la Ley 11/2007 dispone que los sistemas normalizados de solicitud pueden incluir comprobaciones automáticas de la información aportada con respecto a datos almacenados en sistemas propios o pertenecientes a otras administraciones y, incluso, pueden ofrecer el formulario rellenado, totalmente o parcialmente, con la finalidad que el ciudadano verifique la información y, si ocurre, la modifique y la complete.
- Significación jurídica del acto (acto reglado/discrecional y otras consideraciones).

  Se trata de un acto discrecional para la Administración que la ley autoriza con vistas a facilitar y promover el uso de los sistemas normalizados de solicitud.
- Condiciones jurídicas necesarias para que el acto se pueda realizar.

  Las condiciones jurídicas son las aplicables al acto de presentación de la solicitud, el escrito o la comunicación en el registro electrónico; es decir, las generales de capacidad y legitimación para

actuar.

- Obligación legal o administrativa de documentar el acto.

  Según nuestra opinión, hará falta documentar el resultado de la comprobación automática, y, en caso de detección de errores en la solicitud, comunicarlos en unidad de acto al ciudadano para que los corrija.

3. ¿Quién realiza el acto?

- Persona física (ciudadano).

  No aplicable.

- Trabajador de la Administración (si procede, funcionario).

  No aplicable.

- Órgano de la Administración.

  La comprobación se configura legalmente como un acto automático. Por lo tanto, lo tiene que llevar a cabo el órgano correspondiente, que hay que identificar con precisión, y que en general corresponde al órgano responsable del sistema normalizado de tramitación.

4. ¿En que condición realiza el acto?

- En nombre propio y por cuenta propia.

  No aplicable.

- En calidad de órgano de una persona jurídica pública o privada (representación orgánica).

  Aplicable, ya que los actos de comprobación se tienen que imputar en el órgano responsable del sistema normalizado de tramitación.

- En calidad de representante legal de una persona física o jurídica, pública o privada.

  No aplicable.

- En calidad de representante voluntario de una persona física o jurídica, pública o privada.

No aplicable.

- En calidad de representante profesional de una persona física o jurídica (representación presunta).

  No aplicable.

5. ¿Existe posibilidad de sustitución personal?

   - Actos estrictamente personales.

     No aplicable.
   - Cualquier representante.

     No aplicable.
   - Cualquier persona física con una calidad concreta (p. ej., cualquier trabajador público de un grupo).

     No aplicable.

6. ¿Genera un documento nuevo, se manifesta sobre un documento existente previamente o sobre un registro (de expediente o de libros)?

   - Genera un documento nuevo.

     El resultado positivo de las comprobaciones se puede plasmar en un documento específico.
   - Se plasma en un documento existente.

     El resultado positivo de las comprobaciones se puede plasmar en la misma solicitud.
   - Se registra, sin generar manifestación documental.

     El resultado de las comprobaciones se puede registrar en el sistema normalizado de solicitud.

7. ¿Requiere la comprobación previa de la identidad de quien realiza el acto?

   - Sí/No.

     Sí.
   - Determinación del método de identificación y autenticación de la persona que actúa.

     Sello de actuación administrativa automática o código seguro de verificación.
   - Valoración del nivel de evidencia del método utilizado, de acuerdo con el esquema de CATCert.

Nivel 3.

8. ¿Requiere la comprobación previa de la condición de quien realiza el acto?
   - Sí/No.
     No, ya que se utiliza un sello de actuación administrativa automática.
   - Comprobación de la facultad de actuación, orgánica o legal.
     No aplicable.
   - Comprobación de un apoderamiento o de una autorización, en representación voluntaria.
     No aplicable.
   - Comprobación de la condición de profesional de colectivo autorizado.
     No aplicable.

9. ¿Requiere una comunicación confidencial previa o posterior?
   - Sí/No.
     No.
   - Determinación del método de protección utilizado.
     No aplicable.

10. ¿Es de ejecución automática o mecánica, total o parcialmente?
    - Sí/No.
      Sí, tal como determina de manera expresa la ley.
    - Determinación de los tratamientos automáticos o mecánicos.
      El automatismo consiste en la comprobación de informaciones almacenadas en sistemas propios o pertenecientes a otras administraciones, cosa que implica los automatismos correspondientes a los intercambios de los datos correspondientes.

5.3. La digitalización automática de documentos

1. ¿Cuál és el contenido del acto?

- Descripción del acto.

  La digitalización automática consiste en el cambio de soporte de un documento, del soporte papel al soporte electrónico, mediante tecnología de captura y tratamiento posterior de la imagen.

- Tipo de acto (del ciudadano/de la Administración, otros).

  Se trata de un acto administrativo, si procede a solicitud del ciudadano.

- Efectos que produce dentro del proceso (inicia, acaba, otros).

  La digitalización automática no produce ningún efecto particular en un procedimiento, sino que permite disponer de un soporte de sustitución del papel (una copia auténtica del original, que lo puede sustituir).

2. ¿Cuál es la normativa aplicable al acto?

- Identificación de las normas aplicables.

  El artículo 30.2 de la Ley 11/2007 establece que las copias realizadas por las administraciones públicas, utilizando medios electrónicos, de documentos emitidos originalmente por las administraciones públicas en soporte papel tienen la consideración de copias auténticas siempre que se cumplan los requerimientos y las actuaciones que prevé el artículo 46 de la Ley 30/1992, de régimen jurídico de las administraciones públicas y del procedimiento administrativo común.

  Por su parte, el artículo 30.3 de la Ley 11/2007

determina que las administraciones públicas pueden obtener imágenes electrónicas de los documentos privados aportados por los ciudadanos, con su misma validez y eficacia, a través de procesos de digitalización que garanticen la autenticidad, la integridad y la conservación del documento imagen, del cual se tiene que dejar constancia. Esta obtención se puede hacer de manera automatizada, mediante el sello electrónico correspondiente.

En tercer lugar, el artículo 30.4 de la Ley 11/2007 establece que, en los casos de documentos emitidos originalmente en soporte papel de los cuales se hayan efectuado copias electrónicas de acuerdo con lo que dispone este artículo, se pueden destruir los originales en los términos y con las condiciones que establezca cada Administración pública.

Finalmente, el artículo 31.1 de la misma Ley 11/2007 indica que se pueden almacenar por medios electrónicos todos los documentos utilizados en las actuaciones administrativas, cosa que afianza la noción de la digitalización de documentos en expedientes administrativos.

- Significación jurídica del acto (acto reglado/discrecional y otras consideraciones).

  Se trata de un acto discrecional para la Administración.

- Condiciones jurídicas necesarias para que el acto se pueda realizar.

  Las condiciones incluyen el nombramiento del órgano competente y la determinación de los mecanismos que permiten acreditar la constancia de la integridad y de la autenticidad de la copia

producida a partir de la digitalización.

- Obligación legal o administrativa de documentar el acto.

  La digitalización produce una copia auténtica que documenta el acto.

3. ¿Quién realiza el acto?

- Persona física (ciudadano).

  No aplicable.

- Trabajador de la Administración (si procede, funcionario).

  No aplicable.

- Órgano de la Administración.

  La digitalización se configura como un acto automático. Por lo tanto, lo tiene que llevar a cabo el órgano correspondiente, que hay que identificar con precisión, y que en general corresponde al órgano responsable del sistema de digitalización o al titular de la documentación.

4. ¿En qué condición realiza el acto?

- En nombre propio y por cuenta propia.

  No aplicable.

- En calidad de órgano de una persona jurídica pública o privada (representación orgánica).

  Aplicable, ya que los actos de digitalización se deben imputar al órgano responsable que haya sido nombrado.

- En calidad de representante legal de una persona física o jurídica, pública o privada.

  No aplicable.

- En calidad de representante voluntario de una persona física o jurídica, pública o privada.

  No aplicable.

- En calidad de representante profesional de una persona física o jurídica (representación

presunta).
No aplicable.

5. ¿Existe posibilidad de sustitución personal?
   - Actos estrictamente personales.
     No aplicable.
   - Cualquier representante.
     No aplicable.
   - Cualquier persona física con una condición concreta (p. ej., cualquier trabajador público de un grupo).
     No aplicable.

6. ¿Genera un documento nuevo, se manifesta sobre un documento existente previamente o sobre un registro (de expediente o de libros)?
   - Genera un documento nuevo.
     La digitalización genera un documento nuevo, una copia auténtica.
   - Se plasma en un documento existente.
     No aplicable.
   - Se registra, sin generar manifestación documental.
     La digitalización puede implicar la extracción de datos del documento, que se registrarán en alguna aplicación, como la aplicación de registro (en el caso de digitalización de documentos de entrada) o de gestión documental o de archivo (en el caso de expedientes ya existentes).

7. ¿Requiere la comprobación previa de la identidad de quien realiza el acto?
   - Sí/No.
     Sí.
   - Determinación del método de identificación y autenticación de la persona que actúa.
     Sello de actuación administrativa automática o código seguro de verificación.
   - Valoración del nivel de evidencia del método utilizado, de acuerdo con el esquema de

	CATCert. Nivel 4, ya que la copia digitalizada puede sustituir el original en papel, que eventualmente será destruido por la Administración, de acuerdo con lo que determine la normativa reglamentaria aplicable.
8. ¿Requiere la comprobación previa de la condición de quien realiza el acto?	- Sí/No. No, ya que se utiliza un sello de actuación administrativa automática. - Comprobación de la facultad de actuación, orgánica o legal. No aplicable. - Comprobación de un apoderamiento o de una autorización, en representación voluntaria. No aplicable. - Comprobación de la condición de profesional de colectivo autorizado. No aplicable.
9. ¿Requiere una comunicación confidencial previa o posterior?	- Sí/No. No. - Determinación del método de protección utilizado. No aplicable.
10. ¿Es de ejecución automática o mecánica, total o parcialmente?	- Sí/No. Sí, tal como determina de forma expresa la ley, como a mínimo en el caso del artículo 30.3. - Determinación de los tratamientos automáticos o mecánicos. El automatismo consiste en la creación de un documento electrónico, con la consideración de copia, que representa de manera fidedigna la imagen del documento original en soporte papel.

5.4. El impulso automático del procedimento

1. ¿Cuál es el contenido del acto?

- Descripción del acto.

  El impulso automático del procedimiento consiste en el conjunto de actos de trámite que permiten que avance ordenadamente la instrucción del procedimiento.

- Tipo de acto (del ciudadano/de la Administración, otros).

  Se trata de un acto administrativo.

- Efectos que produce dentro del proceso (inicia, acaba, otros).

  El efecto de este acto en el proceso es hacer avanzar el procedimiento administrativo eliminando los obstáculos que impidan, dificulten o retrasen el ejercicio lleno de los derechos de los interesados o el respeto a sus intereses, disponiendo lo que resulte necesario para evitar y eliminar toda anormalidad en la tramitación del procedimiento, y garantizar su terminación dentro del plazo establecido legalmente.

2. ¿Cuál es la normativa aplicable al acto?

- Identificación de las normas aplicables.

  El artículo 41 de la Ley 30/1992, de 26 de noviembre, de régimen jurídico de las administraciones públicas y del procedimiento administrativo común, determina la responsabilidad de los titulares de las unidades administrativas y del personal al servicio de las administraciones públicas que tengan a cargo la resolución o el despacho de los asuntos.

Por su parte, el artículo 74.1 de la Ley 30/1992 determina que el procedimiento, que se somete al principio de celeridad, se tiene que impulsar de oficio en todo sus trámites.

En este sentido, el artículo 75.1 de la Ley 30/1992 dispone que hay que acordar en un solo acto todos los trámites que, por su naturaleza, admitan un impulso simultáneo y no sea obligatorio su cumplimiento sucesivo.

El artículo 78 de la Ley 30/1992 establece que los actos de instrucción necesarios para la determinación, el conocimiento y la comprobación de los datos en virtud de los cuales se tenga que pronunciar la resolución, los tiene que realizar de oficio el órgano que tramite el procedimiento, sin perjuicio del derecho de los interesados en proponer aquellas otras actuaciones que requieran su intervención o constituyan trámites establecidos legalmente o reglamentariamente.

Finalmente, el artículo 36 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, determina, en el apartado 1, que las aplicaciones y los sistemas de información utilizados para la instrucción por medios electrónicos de los procedimientos tienen que garantizar el control de los tiempos y los plazos, la identificación de los órganos responsables de los procedimientos y la tramitación ordenada de los expedientes, y facilitar la simplificación y la publicidad de los procedimientos, mientras que el apartado 2 indica que los sistemas de comunicación utilizados en la gestión electrónica de los procedimientos para las comunicaciones entre los órganos y las unidades

interventores a los efectos de emisión y recepción de informes u otras actuaciones tienen que cumplir los requisitos que establece la Ley 11/2007.

- Significación jurídica del acto (acto reglado/discrecional y otras consideraciones).

  No aplicable en general a la categoría de actos de impulso, ya que la significación jurídica será predicable de cada acto concreto.

- Condiciones jurídicas necesarias para que el acto se pueda realizar.

  Los actos de impulso requieren la existencia de un procedimiento formalmente abierto.

- Obligación legal o administrativa de documentar el acto.

  Según nuestra opinión, habrá que documentar de manera suficiente los actos de impulso, de acuerdo con la normativa aplicable a cada acto.

  Puede ser conveniente, en relación con la responsabilidad del órgano instructor, documentar la secuencia de actos de instrucción a efectos de controlar los plazos, típicamente mediante una herramienta de BPM (business process management, gestión de procesos de negocio).

3. ¿Quién realiza el acto?
   - Persona física (ciudadano).
     No aplicable.
   - Trabajador de la Administración (si procede, funcionario).
     Aplicable.
   - Órgano de la Administración.
     Aplicable.

4. ¿En qué condición realiza el acto?
   - En nombre propio y por cuenta propia.
     No aplicable.
   - En cualidad de órgano de una persona jurídica pública o privada (representación orgánica).
     Aplicable.
   - En cualidad de representante legal de una persona física o jurídica, pública o privada.
     No aplicable.
   - En cualidad de representante voluntario de una persona física o jurídica, pública o privada.
     No aplicable.
   - En cualidad de representante profesional de una persona física o jurídica (representación presunta).
     No aplicable.

5. ¿Existe posibilidad de sustitución personal?
   - Actos estrictamente personales.
     No aplicable.
   - Cualquier representante.
     No aplicable.
   - Cualquier persona física con una cualidad concreta (p. ej., cualquier trabajador público de un grupo).
     Aplicable.

6. ¿Genera un documento nuevo, se manifesta sobre un documento existente previamente o sobre un registro (de expediente o de libros)?
   - Genera un documento nuevo.
     El acto de impulso se puede plasmar en un documento específico.
   - Se plasma en un documento existente.
     No aplicable.
   - Se registra, sin generar manifestación documental.
     El acto de impulso se puede registrar en la aplicación de negocio que gestiona el procedimento.

7. ¿Requiere la comprobación previa de la identidad de quien realiza el acto?
   - Sí/No.
     Sí.
   - Determinación del método de identificación y autenticación de la persona que actua.
     Sello de actuación administrativa automática o código seguro de verificación.
   - Valoración del nivel de evidencia del método utilizado, de acuerdo con el esquema de CATCert.
     Nivel 3 o superior.

8. ¿Requiere la comprobación previa de la condición de quien realiza el acto?
   - Sí/No.
     No, ya que se utiliza un sello de actuación administrativa automática.
   - Comprobación de la facultad de actuación, orgánica o legal.
     No aplicable.
   - Comprobación de un apoderamiento o de una autorización, en representación voluntaria.
     No aplicable.
   - Comprobación de la condición de profesional de colectivo autorizado.
     No aplicable.

9. ¿Requiere una comunicación confidencial previa o posterior?
   - Sí/No.
     No.
   - Determinación del método de protección utilizado.
     No aplicable.

10. ¿Es de ejecución automática o mecánica, total o parcialmente?
    - Sí/No.
      Sí, siempre que el acto concreto de impulso lo permita
    - Determinación de los tratamientos automáticos o mecánicos.
      Depende del acto concreto de impulso del procedimento.

5.5. El acto automático de constancia electrónica

1. ¿Cuál es el contenido del acto?
   - Descripción del acto.
     El acto automático de constancia consiste en una declaración de conocimiento por parte de la Administración en relación con una información registrada en un documento, un expediente o un libro de la Administración.
   - Tipo de acto (del ciudadano/de la Administración, otros).
     Se trata de un acto administrativo, típicamente a solicitud del ciudadano o de una autoridad competente.
   - Efectos que produce dentro del proceso (inicia, acaba, otros).
     Su efecto dentro del proceso administrativo es generar una prueba documental sobre la

información manifestada.

2. ¿Cuál es la normativa aplicable al acto?

- Identificación de las normas aplicables.
  La Ley 30/1992, de 26 de noviembre, de régimen jurídico de las administraciones públicas y del procedimiento administrativo común, no establece un régimen concreto para los actos de constancia, que, por contra, se manifiestan en otros actos, como la expedición de certificaciones y notas simples informativas, las cuales normalmente se reglamentan por la normativa sectorial o específica que les resulta de aplicación.
- Significación jurídica del acto (acto reglado/discrecional y otras consideraciones).
  Se trata de un acto absolutamente reglado que la Administración tiene que llevar a cabo siempre que lo solicite el ciudadano o la autoridad competente.
- Condiciones jurídicas necesarias para que el acto se pueda realizar.
  Las condiciones jurídicas necesarias para la realización del acto las determina el tipo de acto de constancia.
  Resultan particularmente relevantes las normas sobre expedición de certificados, ya que normalmente se trata de una facultad reservada a un órgano concreto, en algunos casos con la garantía de fe pública.
- Obligación legal o administrativa de documentar el acto.
  El acto de constancia se produce habitualmente mediante la forma documental escrita, en algunos casos con rigurosas formalidades, como en el caso de los certificados emitidos por las

secretarías de las entidades locales.

3. ¿Quién realiza el acto?
   - Persona física (ciudadano).
     No aplicable.
   - Trabajador de la Administración (si procede, funcionario).
     No aplicable.
   - Órgano unipersonal de la Administración.
     El acto de constancia lo ha de realilzar el órgano administrativo competente

4. ¿En que condición realiza el acto?
   - En nombre propio y por cuenta propia.
     No aplicable.
   - En calidad de órgano de una persona jurídica pública o privada (representación orgánica).
     Aplicable.
   - En calidad de representante legal de una persona física o jurídica, pública o privada.
     No aplicable.
   - En calidad de representante voluntario de una persona física o jurídica, pública o privada.
     No aplicable.
   - En calidad de representante profesional de una persona física o jurídica (representación presunta).
     No aplicable.

5. ¿Existe posibilidad de sustitución personal?
   - Actos estrictamente personales.
     No aplicable.
   - Cualquier representante
     No aplicable.
   - Cualquier persona física con una condición concreta (p. ej., cualquier trabajador público de un grupo).

No aplicable.

6. ¿Genera un documento nuevo, se manifesta sobre un documento existente previamente o sobre un registro (de expediente o de libros)?
   - Genera un documento nuevo.
     Los actos de constancia se manifiestan en documentos específicos, como los certificados o las notas simples informativas. Asimismo, se pueden plasmar en copias auténticas de documentos al poder de la Administración.
   - Se plasma en un documento existente.
     No aplicable.
   - Se registra, sin generar manifestación documental.
     No aplicable.

7. ¿Requiere la comprobación previa de la identidad de quien realiza el acto?
   - Sí/No.
     Sí.
   - Determinación del método de identificación y autenticación de la persona que actúa.
     Sello de actuación administrativa automática o código seguro de verificación.
   - Valoración del nivel de evidencia del método utilizado, de acuerdo con el esquema de CATCert.
     Nivel 3 para las notas simples informativas y nivel 4 para las certificaciones.

8. ¿Requiere la comprobación previa de la condición de quien realiza el acto?
   - Sí/No.
     No, ya que se utiliza un sello de actuación administrativa automática.
   - Comprobación de la facultat de actuación, orgánica o legal.
     No aplicable.
   - Comprobación de un apoderamiento de una autorización, en representación voluntaria.

No aplicable.

- Comprobación de la condición de profesional de colectivo autorizado.

  No aplicable.

9. ¿Requiere una comunicación confidencial previa o posterior?
   - Sí/No.

     En general, no, pero depende del contenido del ato de constancia, ya que si contiene datos personales de nivel alto, entonces será necesario garantizar el secreto del acto de constancia.
   - Determinación del método de protección utilizado.

     El método de protección a utilizar depende del mecanismo de comunicación que se utilice para entregar el documento de constancia (nota simple o certificación).

10. ¿És de ejecución automática o mecánica, total o parcialmente?
    - Sí/No.

      Sí.
    - Determinación de los tratamientos automáticos o mecánicos.

      El automatismo posible consiste en la generación, el sellado y la entrega del documento con el acto de constancia.

5.6. La expedición automática de copia auténtica electrónica

1. ¿Cuál es el contenido del acto?
   - Descripción del acto.

     La expedición de una copia auténtica electrónica deriva de un acto de información o de acceso a información por parte de la Administración, en

relación con un documento, típicamente integrado en expediente de la Administración.

También se realizan copias automáticas auténticas para ingresar documentos administrativos o privados mediante su digitalización en papel, caso que no se trata en este documento, ya que se analiza en un caso de uso específico.

- Tipo de acto (del ciudadano/de la Administración, otros).

  Se trata de un acto administrativo, típicamente a solicitud del ciudadano o de una autoridad competente.

- Efectos que produce dentro del proceso (inicia, acaba, otros).

  Su efecto dentro del proceso administrativo es generar una prueba documental sobre la información manifestada.

2. ¿Cuál es la normativa aplicable al acto?

- Identificación de las normas aplicables.

  La Ley 30/1992, de 26 de noviembre, de régimen jurídico de las administraciones públicas y del procedimiento administrativo común, determina, en el artículo 35.a), que los ciudadanos tienen derecho a conocer en cualquier momento el estado de tramitación de los procedimientos en que tengan la consideración de interesados, y a obtener una copia de los documentos contenidos en estos procedimientos.

  Por su parte, el artículo 37.1 de la Ley 30/1992 determina que los ciudadanos tienen derecho a acceder en los registros y en los documentos que formen parte de un expediente y permanezcan en los archivos administrativos, independientemente

de su forma de expresión, gráfica, sonora o en imagen, o el tipo de soporte material en qué figuren, siempre que estos expedientes correspondan a procedimientos finalizados en la fecha de la solicitud. El apartado 8 del mismo artículo 37 indica que el derecho de acceso implicará el de obtener copias o certificaciones de los documentos cuyo examen sea autorizado por la Administración.

El artículo 45.5 de la Ley 30/1992 establece que los documentos emitidos, independientemente de su soporte, por medios electrónicos, informáticos y telemáticos por las administraciones públicas, o los que éstas emitan como a base de originales almacenados por estos mismos medios, tienen que disfrutar de la validez y la eficacia de documento original siempre que quede garantizada la autenticidad, la integridad y la conservación y, si ocurre, la recepción por parte de la persona interesada, así como el cumplimiento de las garantías y los requisitos exigidos por esta Ley o de otros.

El artículo 46 de la Ley 30/1992 dispone que cada Administración pública tiene que determinar reglamentariamente los órganos que tengan atribuidas las competencias de expedición de copias auténticas de documentos públicos y privados, y que las copias de cualesquiera documentos públicos tienen que disfrutar de la misma validez y eficacia que éstos, siempre que exista constancia de su autenticidad.

Por su parte, el artículo 30.2 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, indica que las

copias realizadas por las administraciones públicas, utilizando medios electrónicos, de documentos emitidos originalmente por las administraciones públicas en soporte papel tienen la consideración de copias auténticas siempre que se cumplan los requerimientos y las actuaciones que prevé el artículo 46 de la Ley 30/1992, de régimen jurídico de las administraciones públicas y del procedimiento administrativo común.

El artículo 30.4 de la Ley 11/2007 establece que las copias realizadas en soporte papel de documentos públicos administrativos emitidos por medios electrónicos y firmados electrónicamente tienen la consideración de copias auténticas siempre que incluyan la impresión de un código generado electrónicamente u otros sistemas de verificación que permitan contrastar la autenticidad mediante el acceso a los archivos electrónicos de la Administración pública, órgano o entidad emisora.

Finalmente, el artículo 32.3 de la Ley 11/2007 determina que el envío de expedientes se puede sustituir a todos los efectos legales por la puesta a disposición del expediente electrónico, y el interesado tiene derecho a obtener una copia.

- Significación jurídica del acto (acto reglado/discrecional y otras consideraciones).

  Se trata de un acto absolutamente reglado que la Administración tiene que realizar siempre que lo solicite el ciudadano o la autoridad competente.

- Condiciones jurídicas necesarias para que el acto se pueda realizar.

  Las condiciones jurídicas necesarias para la

realización del acto son la determinación previa del órgano competente y de los mecanismos de constancia de la autenticidad de la copia.

- Obligación legal o administrativa de documentar el acto.

  La copia auténtica se debe documentar, normalmente en forma de fotocopia compulsada, cosa que en caso de copia electrónica será una reproducción, con o sin cambio de formato, con la diligencia correspondiente de ser copia auténtica.

3. ¿Quien realiza el acto?

- Persona física (ciudadano).

  No aplicable.
- Trabajador de la Administración (si procede, funcionario).

  No aplicable.
- Órgano unipersonal de la Administración.

  La copia auténtica la ha de realizar el órgano administrativo competente.

4. ¿En que condición realiza el acto?

- En nombre propio y por cuenta propia.

  No aplicable.
- En calidad de órgano de una persona jurídica pública o privada (representación orgánica).

  Aplicable.
- En calidad de representante legal de una persona física o jurídica, pública o privada.

  No aplicable.
- En calidad de representante voluntario de una persona física o jurídica, pública o privada.

  No aplicable.
- En calidad de representante profesional de una persona física o jurídica (representación presunta).

No aplicable.

5. ¿Existe posibilidad de sustitución personal?
   - Actos estrictamente personales.
     No aplicable.
   - Cualquier representante.
     No aplicable.
   - Cualquier persona física con una condición concreta (p. ej., cualquier trabajador público de un grupo).
     No aplicable.

6. ¿Genera un documento nuevo, se manifesta sobre un documento existente previamente o sobre un registro (de expediente o de libros)?
   - Genera un documento nuevo.
     Aplicable.
   - Se plasma en un documento existente.
     No aplicable.
   - Se registra, sin generar manifestación documental.
     No aplicable.

7. ¿Requiere la comprobación previa de la identidad de quien realiza el acto?
   - Sí/No.
     Sí.
   - Determinación del método de identificación y autenticación de la persona que actua.
     Sello de actuación administrativa automática o codigo seguro de verificación.
   - Valoración del nivel de evidencia del método utilizado, de acuerdo con el esquema de CATCert.
     Nivel 4.

8. ¿Requiere la comprobación previa de la condición de quien realiza el acto?
   - Sí/No.
     No, ya que se utiliza un sello de actuación administrativa automática.
   - Comprobación de la facultad de actuación,

	orgánica o legal. No aplicable. - Comprobación de un apoderamiento o de una autorización, en representación voluntaria. No aplicable. - Comprobación de la condición de profesional de colectivo autorizado. No aplicable.
9. ¿Requiere una comunicación confidencial previa o posterior?	- Sí/No. En general, no, pero depende del contenido de la copia auténtica, ya que si contiene datos personales de nivel alto, entonces habrá que garantizar el secreto. - Determinación del método de protección utilizado. El método de protección a utilizar depende del mecanismo de comunicación que se utilice para entregar la copia auténtica.
10. ¿Es de ejecución automática o mecánica, total o parcialmente?	- Sí/No. Sí. - Determinación de los tratamientos automáticos o mecánicos. El automatismo posible consiste en la generación, el sellado y la entrega de la copia auténtica.

5.7. La apertura y el cierre automático de libros electrónicos

1. ¿Cuál es el contenido del acto?	- Descripción del acto. La apertura y el cierre de libros consiste en la

	secuenciación de los registros que forman parte de un libro electrónico mediante el encadenamiento criptográfico de los registros u otras técnicas similares. El acto de apertura implica la creación y la firma del primer registro, a partir del cual empieza la cadena de registros, mientras que el acto de cierre finaliza la cadena y protege toda la secuencia con un sello de fecha y hora final. Los actos de encadenamiento criptográfico de registros, que se realizan entre el segundo registro (encadenado con el primero) y el cierre (encadenado con el último registro), se llevan a cabo sin nueva identificación del órgano. - Tipo de acto (del ciudadano/de la Administración, otros). Se trata de un acto administrativo. - Efectos que produce dentro del proceso (inicia, acaba, otros). Su efecto dentro del proceso administrativo es formalizar y proteger las inserciones del libro electrónico, ya que no se podrán añadir ni retirar registros por el hecho de que están encadenados de forma criptográfica.
2. ¿Cuál es la normativa aplicable al acto?	- Identificación de las normas aplicables. La normativa sectorial a menudo identifica la necesidad de disponer de libros legalizados o tramitados. - Significación jurídica del acto (acto reglado/discrecional y otras consideraciones). Se trata de un acto absolutamente reglado que la Administración debe realizar siempre que lo determine la normativa aplicable.

	- Condiciones jurídicas necesarias para que el acto se pueda realizar. Las condiciones jurídicas necesarias para la realización del acto son la determinación previa del órgano competente y del supuesto legal de la obligación de legalizar o tramitar libros, que indica la normativa sectorial, como la normativa de régimen local. - Obligación legal o administrativa de documentar el acto. Sí, mediante el sistema de libro electrónico, con encadenamiento criptográfico de los registros.
3. ¿Quien realiza el acto?	- Persona física (ciudadano). No aplicable. - Trabajador de la Administración (si procede, funcionario). No aplicable. - Órgano unipersonal de la Administración. La apertura y el cierre los ha de llevar a cabo el órgano administrativo competente, responsable de la llevanza del libro.
4. ¿En qué condición realiza el acto?	- En nombre propio y por cuenta propia. No aplicable. - En calidad de órgano de una persona jurídica pública o privada (representación orgánica). Aplicable. - En calidad de representante legal de una persona física o jurídica, pública o privada. No aplicable. - En calidad de representante voluntario de una persona física o jurídica, pública o privada. No aplicable.

	- En calidad de representante profesional de una persona física o jurídica (representación presunta). No aplicable.
5. ¿Existe posibilidad de sustitución personal?	- Actos estrictamente personales. No aplicable. - Cualquier representante. No aplicable. - Cualquier persona física con una condición concreta (p. ej., cualquier trabajador público de un grupo). No aplicable.
6. ¿Genera un documento nuevo, se manifesta sobre un documento existente previamente o sobre un registro (de expediente o de libros)?	- Genera un documento nuevo. No aplicable. - Se plasma en un documento existente. No aplicable. - Se registra, sin generar manifestación documental. Aplicable, ya que se registra en el mismo sistema de libro electrónico.
7. ¿Requeiere a comprobación previa de la identidad de quien realiza el acto?	- Sí/No. Sí. Los actos concretos de encadenamiento criptográfico de un registro con el anterior, que sucede entre la apertura y el cierre, no requieren nueva identificación. - Determinación del método de identificación y autenticación de la persona que actúa. Sello de actuación administrativa automática. - Valoración del nivel de evidencia del método utilizado, de acuerdo con el esquema de CATCert.

Nivel 3 o superior.

8. ¿Requiere la comprobación previa de la condición de quien realiza el acto?
   - Sí/No.
     No, ya que se utiliza un sello de actuación administrativa automática.
   - Comprobación de la facultad de actuación, orgánica o legal.
     No aplicable.
   - Comprobación de un apoderamiento o de una autorización, en representación voluntaria.
     No aplicable.
   - Comprobación de la condición de profesional de colectivo autorizado.
     No aplicable.

9. ¿Requiere una comunicación confidencial previa o posterior?
   - Sí/No.
     No, ya que el índice no contiene datos personales.
   - Determinación del método de protección utilizado.
     No aplicable.

10. ¿Es de ejecución automática o mecánica, total o parcialmente?
    - Sí/No.
      Sí.
    - Determinación de los tratamientos automáticos o mecánicos.
      El automatismo posible consiste en la apertura y el cierre del libro, así como el encadenamiento o sucesión criptográfico de los registros.

5.8. La foliación automática de expedientes

1. ¿Cuál es el contenido del acto?

- Descripción del acto.

  La foliación automática o electrónica de expedientes consiste en la secuenciación de los documentos que forman parte del expediente mediante un índice firmado electrónicamente.

- Tipo de acto (del ciudadano/de la Administración, otros).

  Se trata de un acto administrativo.

- Efectos que produce dentro del proceso (inicia, acaba, otros).

  Su efecto dentro del proceso administrativo es formalizar y proteger el expediente.

2. ¿Cuál es la normativa aplicable al acto?

- Identificación de las normas aplicables.

  El artículo 32.2 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, indica que la foliación de los expedientes electrónicos se tiene que llevar a cabo mediante un índice electrónico firmado por la Administración, el órgano o la entidad actuante, según proceda. Este índice tiene que garantizar la integridad del expediente electrónico y permitir recuperarlo siempre que haga falta, y es admisible que un mismo documento forme parte de diferentes expedientes electrónicos.

- Significación jurídica del acto (acto reglado/discrecional y otras consideraciones).

  Se trata de un acto absolutamente reglado que la Administración debe realizar siempre que lo

	determine la normativa aplicable. - Condiciones jurídicas necesarias para que el acto se pueda realizar. Las condiciones jurídicas necesarias para la realización del acto son la determinación previa del órgano competente y del supuesto legal de la obligación de foliar, que indica la normativa sectorial, como la normativa de régimen local. - Obligación legal o administrativa de documentar el acto. La foliación obliga a generar el índice del expediente.
3. ¿Quién realiza el acto?	- Persona física (ciudadano). No aplicable. - Trabajador de la Administración (si procede, funcionario). No aplicable. - Órgano unipersonal de la Administración. La foliación la debe realizar el órgano administrativo competente, responsable del expediente.
4. ¿En qué condición realiza el acto?	- En nombre propio y por cuenta propia. No aplicable. - En calidad de órgano de una persona jurídica pública o privada (representación orgánica). Aplicable. - En calidad de representante legal de una persona física o jurídica, pública o privada. No aplicable. - En calidad de representante voluntario de una persona física o jurídica, pública o privada. No aplicable.

	- En calidad de representante profesional de una persona física o jurídica (representación presunta). No aplicable.
5. ¿Existe posibilidad de sustitución personal?	- Actos estrictamente personales. No aplicable. - Cualquier representante. No aplicable. - Cualquier persona física con una condición concreta (p. ej., cualquier trabajador público de un grupo). No aplicable.
6. ¿Genera un documento nuevo, se manifesta sobre un documento existente previamente o sobre un registro (de expediente o de libros)?	- Genera un documento nuevo. Aplicable. - Se plasma en un documento existente. No aplicable. - Se registra, sin generar manifestación documental. No aplicable.

7. ¿Requiere la comprobación previa de la identidad de quien realiza el acto?	- Sí/No. Sí. - Determinación del método de identificación y autenticación de la persona que actua. Sello de actuación administrativa automàtica o código seguro de verificación. - Valoración del nivel de evidencia del método utilizado, de acuerdo con el esquema de CATCert. Nivell 3 o superior.
8. ¿Requiere la comprobación previa de la condición de quien realiza el acto?	- Sí/No. No, ya que se utiliza un sello de actuación administrativa automática. - Comprobación de la facultat de actuación, orgánica o legal. No aplicable. - Comprobación de un apoderamiento o de una autorización, en representación voluntaria. No aplicable. - Comprobación de la condición de profesional de colectivo autorizado. No aplicable.
9. ¿Requiere una comunicación confidencial previa o posterior?	- Sí/No. No, ya que el índice no contiene datos personales - Determinación del método de protección utilizado. No aplicable.
10. ¿Es de ejecución automática o mecánica, total o parcialmente?	- Sí/No. Sí. - Determinación de los tratamientos automáticos o mecánicos.

El automatismo posible consiste en la generación y el sellado del índice.

5.9. La migración automática de documento electrónico

1. ¿Cuál es el contenido del acto?
   - Descripción del acto.
     La migración automática de un documento electrónico es un caso particular de la expedición automática de copia en que se produce un cambio del formato del documento, por ejemplo de formato ODF (ofimático) a formato PDF (presentación).
   - Tipo de acto (del ciudadano/de la Administración, otros).
     Se trata de un acto administrativo.
   - Efectos que produce dentro del proceso (inicia, acaba, otros).
     Su efecto dentro del proceso administrativo es generar una prueba documental sobre la información manifestada.

2. ¿Cuál es la normativa aplicable al acto?
   - Identificación de las normas aplicables.
     El artículo 45.5 de la Ley 30/1992 indica que los documentos emitidos, independientemente de su soporte, por medios electrónicos, informáticos y telemáticos por las administraciones públicas, o los que éstas emitan como a base de originales almacenados por estos mismos medios, tienen que disfrutar de la validez y la eficacia de documento original siempre que quede

garantizada la autenticidad, la integridad y la conservación y, si ocurre, la recepción por el interesado, así como el cumplimiento de las garantías y los requisitos exigidos por esta ley o de otros.

El artículo 46 de la Ley 30/1992 dispone que cada Administración pública tiene que determinar reglamentariamente los órganos que tengan atribuidas las competencias de expedición de copias auténticas de documentos públicos y privados, y que las copias de cualesquiera documentos públicos tienen que disfrutar de la misma validez y eficacia que éstos, siempre que exista constancia de su autenticidad.

Por su parte, el artículo 30.1 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, establece que las copias realizadas por medios electrónicos de documentos electrónicos emitidos por el mismo interesado o por las administraciones públicas, manteniendo o no el formato original, tienen inmediatamente la consideración de copias auténticas con la eficacia que prevé el artículo 46 de la Ley 30/1992, de régimen jurídico de las administraciones públicas y del procedimiento administrativo común, siempre que el documento electrónico original esté al poder de la Administración y que la información de firma electrónica y, si ocurre, de sellado de tiempo permitan comprobar la coincidencia con el documento mencionado.

Finalmente, el artículo 31.2 de la Ley 11/2007 determina que los documentos electrónicos que contengan actos administrativos que afecten

derechos o intereses de los particulares se tienen que conservar en soportes de esta naturaleza, ya sea en lo mismo formado a partir de lo cual se originó el documento o en otro asegure la identidad y la integridad de la información necesaria para reproducirlo. Se tiene que asegurar en todo caso la posibilidad de trasladar los datos a otros formatos y apoyos|soportes que garanticen el acceso desde diferentes aplicaciones.

- Significación jurídica del acto (acto reglado/discrecional y otras consideraciones).

  Se trata de un acto absolutamente reglado que la Administración tiene que realizar siempre que lo requiera la estrategia de preservación documental.

- Condiciones jurídicas necesarias para que el acto se pueda realizar.

  Las condiciones jurídicas necesarias para la realización del acto son la determinación previa del órgano competente y de los mecanismos de constancia de la autenticidad de la copia resultante de la migración.

- Obligación legal o administrativa de documentar el acto.

  La copia auténtica se tiene que documentar, normalmente en un documento con cambio de formato, con la diligencia correspondiente de ser una copia auténtica.

3. ¿Quién realiza el acto?

- Persona física (ciudadano).

No aplicable.

Trabajador de la Administración (si procede funcionario).

No aplicable.

- Órgano unipersonal de la Administración.
  La copia auténtica la ha de llevar a cabo el órgano administrativo competente.

4. ¿En qué condición realiza el acto?
   - En nombre propio y por cuenta propia.
     No aplicable.
   - En calidad de órgano de una persona jurídica pública o privada (representación orgánica).
     Aplicable.
   - En calidad de representante legal de una persona física o jurídica, pública o privada.
     No aplicable.
   - En calidad de representante voluntario de una persona física o jurídica, pública o privada.
     No aplicable.
   - En calidad de representante profesional de una persona física o jurídica (representación presunta).
     No aplicable.

5. ¿Existe posibilidad de sustitución personal?
   - Actos estrictamente personales.
     No aplicable.
   - Cualquier representante.
     No aplicable.
   - Cualquier persona física con una condición concreta (p. ej., cuaquier trabajador público de un grupo).
     No aplicable.

6. ¿Genera un documento nuevo, se manifesta sobre un documento existente previamente o sobre un registro (de expediente o de libros)?
   - Genera un documento nuevo.
     Aplicable.
   - Se plasma en un documento existente.
     No aplicable.
   - Se registra, sin generar manifestación documental.
     No aplicable.

7. ¿Requiere la comprobación previa de la identidad de quien realiza el acto?
   - Sí/No.
     Sí.
   - Determinación del método de identificación y autenticación de la persona que actua.
     Sello de actuación administrativa automática o código seguro de verificación .
   - Valoración del nivel de evidencia del método utilizado, de acuerdo con el esquema de CATCert.
     Nivell 4.

8. ¿Requiere la comprobación previa de la condición de quien realiza el acto?
   - Sí/No.
     No, ya que se utiliza un sello de actuación administrativa automática.
   - Comprobación de la facultad de actuación orgànica o legal.
     No aplicable.
   - Comprobación de un apoderamiento o de una autorización, en representación voluntaria.
     No aplicable.
   - Comprobación de la condición de profesional de colectivo autorizado.
     No aplicable.

9. ¿Requiere una comunicación confidencial previa o posterior?
   - Sí/No.
     En general, no, pero depende del contenido de la copia auténtica, ya que si contiene datos personales de nivel alto, entonces se habrá de garantizar el secreto
   - Determinación del método de protección utilizado.
     El método de protección a utilizar depende del mecanismo de comunicación que se utilice para entregar la copia auténtica.

10. ¿Es de ejecución automática o mecánica, total o parcialmente?
    - Sí/No.
      Sí.
    - Determinación de los tratamientos automáticos o mecánicos.
      El automatismo posible consiste em la generación, eñl sellado y la entrega de la copia auténtica.

5.10. Los intercambios automáticos de datos entre administraciones públicas

1. ¿Cuál es el contenido del acto?
   - Descripción del acto.
     El intercambio automático entre administraciones públicas consiste en el envío o la puesta a disposición de un documento por parte de una administración pública en otra. El acto de intercambio es muy parecido al acto de comunicación por el cual una administración solicita a otra unos datos concretos, que son devueltos por la Administración requerida,

típicamente en sustitución de certificados administrativos de datos.

- Tipo de acto (del ciudadano/de la Administración, otros).

  Se trata de un acto administrativo.

- Efectos que produce dentro del proceso (inicia, acaba, otros).

  Su efecto dentro del proceso administrativo es generar una prueba documental sobre el intercambio efectuado.

2. ¿Cuál es la normativa aplicable al acto?

- Identificación de las normas aplicables.

  El artículo 6.2.b) de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, consagra el derecho de los ciudadanos a no aportar los datos y los documentos que estén al poder de las administraciones públicas, las cuales tienen que utilizar medios electrónicos para obtener la información mencionada, siempre que, en el caso de datos de carácter personal, tengan el consentimiento de los interesados en los términos que establece la Ley orgánica 15/1999, de protección de datos de carácter personal, o una norma con rango de ley lo determine, a menos que haya restricciones de acuerdo con la normativa aplicable a los datos y los documentos recogidos. El consentimiento se puede emitir y aceptar por medios electrónicos.

  Por su parte, el artículo 9.1 de la Ley 11/2007 establece que, para un ejercicio eficaz del derecho reconocido en el apartado 6.2.b), cada Administración tiene que facilitar el acceso de las administraciones públicas restantes a los datos

relativos a los interesados que figuren en poder suyo y estén en soporte electrónico, especificando las condiciones, los protocolos y los criterios funcionales o técnicos necesarios para acceder a los datos mencionados con las máximas garantías de seguridad, integridad y disponibilidad, de conformidad con lo que dispone la Ley orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal y su normativa de despliegue. El apartado 2 del artículo 9 especifica que la disponibilidad de los datos está limitada estrictamente en las que las administraciones restantes requieren a los ciudadanos para la tramitación y la resolución de los procedimientos y las actuaciones de su competencia de acuerdo con su normativa reguladora, y que el acceso a los datos de carácter personal, además, está sometido al cumplimiento de las condiciones que establece el artículo 6.2.b) de la Ley 11/2007.

Finalmente, el artículo 13.3.d) de la Ley 11/2007 determina que las administraciones públicas pueden utilizar, para su identificación electrónica y para la autenticación de los documentos electrónicos que produzcan, sistemas de intercambio electrónico de datos en entornos cerrados de comunicación, de acuerdo con lo que se haya acordado específicamente entre las partes.

Esta previsión se despliega en el artículo 20 de la Ley 11/2007, que en el apartado 1 prevé que los documentos electrónicos transmitidos en entornos cerrados de comunicaciones establecidos entre administraciones públicas, órganos y entidades

de derecho público se consideran válidos en los efectos de autenticación e identificación de los emisores y los receptores en las condiciones que establece el presente artículo, mientras que el apartado 4 indica que en todo caso se tiene que garantizar la seguridad del entorno cerrado de comunicaciones y la protección de los datos que se transmitan.

- Significación jurídica del acto (acto reglado/discrecional y otras consideraciones).

  Se trata de un acto absolutamente reglado que la Administración tiene que realizar siempre que lo determine la normativa aplicable, para dar cumplimiento al derecho de los ciudadanos.
- Condiciones jurídicas necesarias para que el acto se pueda realizar.

  Las condiciones jurídicas necesarias para la realización del acto son la determinación previa del órgano competente y del supuesto legal de la obligación de efectuar el intercambio electrónico de datos.
- Obligación legal o administrativa de documentar el acto.

  El intercambio se debe producir, normalmente, en forma documentada, a efectos de incorporar la evidencia de los datos en el expediente.

3. ¿Quién realiza el acto?

- Persona física (ciudadano).

  No aplicable.
- Trabajador de la Administración (si procede funcionario).

  No aplicable.
- Órgano unipersonal de la Administración.

  El intercambio lo debe realizar el órgano

administrativo competente.

4. ¿En qué condición realiza el acto?
   - En nombre propio y por cuenta propia.
     No aplicable.
   - En calidad de órgano de una persona jurídica pública o privada (representación orgánica).
     Aplicable.
   - En calidad de representante legal de una persona física o jurídica, pública o privada.
     No aplicable.
   - En calidad de representante voluntario de una persona física o jurídica, pública o privada.
     No aplicable.
   - En calidad de representante profesional de una persona física o jurídica (representación presunta).
     No aplicable.

5. ¿Existe posibilidad de sustitución personal?
   - Actos estrictamente personales.
     No aplicable.
   - Cualquier representante.
     No aplicable.
   - Cualquier persona física con una condición concreta (p. ej., cualquier trabajador público de un grupo).
     No aplicable.

6. ¿Genera un documento nuevo, se manifesta sobre un documento existente previamente o sobre un registro (de expediente o de libros)?
   - Genera un documento nuevo.
     Aplicable.
   - Se plasma en un documento existente.
     No aplicable.
   - Se registra, sin generar manifestación documental.
     No aplicable.

7. ¿Requiere la comprobación previa de la identidad de quien realiza el acto?

- Sí/No.
  Sí.
- Determinación del método de identificación y autenticación de la persona que actúa.
  En principio, parece que debería ser el sello de actuación administrativa automática o código seguro de verificación, pero de acuerdo con el artículo 20 de la Ley 11/2007 se tienen que admitir, también, otros tipos de certificados de carácter más técnico que legal, como los a menudo denominados certificados de componente o de aplicación segura o de servidor seguro, aunque estas posibilidades tendrán que haber estado previstas expresamente por el convenio regulador del intercambio electrónico de datos.
- Valoración del nivel de evidencia del método utilizado, de acuerdo con el esquema de CATCert.
  Nivel 3 o superior, de acuerdo con lo que se determine en el convenio regulador del intercambio electrónico de datos.

8. ¿Requiere la comprobación previa de la condición de quien realiza el acto?

- Sí/No.
  No, ya que se utiliza un sello de actuación administrativa automática o un mecanismo alternativo de características similares.
- Comprobación de la facultad de actuación, orgánica o legal.
  No aplicable.
- Comprobación de un apoderamiento o de una autorización, en representación voluntaria.
  No aplicable.

- Comprobación de la condición de profesional de colectivo autorizado.
  No aplicable.

9. ¿Requiere una comunicación confidencial previa o posterior?
   - Sí/No.
     En general, no, pero depende del contenido del intercambio electrónico de datos, ya que si contiene datos personales de nivel alto, entonces habrá que garantizar el secreto.
   - Determinación del método de protección utilizado.
     El método de protección a utilizar depende del mecanismo de intercambio que se utilice.

10. ¿Es de ejecución automática o mecánica, total o parcialmente?
    - Sí/No.
      Sí.
    - Determinación de los tratamientos automáticos o mecánicos.
      El automatismo posible consiste en la generación, el sellado y la entrega del intercambio de datos.

5.11. La remisión automática de comunicación electrónica al ciudadano

1. ¿Cuál es el contenido del acto?
   - Descripción del acto.
     La remisión automática de comunicación electrónica al ciudadano consiste en el envío o la puesta a disposición del ciudadano de un documento que instrumenta una comunicación entre la Administración y el mismo ciudadano.
   - Tipo de acto (del ciudadano/de la Administración, otros).
     Se trata de un acto administrativo.

	- Efectos que produce dentro del proceso (inicia, acaba, otros). Su efecto dentro del proceso administrativo es generar una prueba documental sobre la comunicación efectuada.
2. ¿Cuál es la normativa aplicable al acto?	- Identificación de las normas aplicables. La Ley 30/1992, de 26 de noviembre, de régimen jurídico de las administraciones públicas y del procedimiento administrativo común, determina, en el artículo 34, que los órganos administrativos tienen que anotar en su registro la salida de los escritos y las comunicaciones oficiales dirigidas en otros órganos o particulares, previsión que encuentra su paralela en el artículo 24.1 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, que establece la necesidad de registrar la remisión de comunicaciones electrónicas. El artículo 58.1 de la Ley 30/1992 impone la obligación de notificar a los interesados las resoluciones y los actos administrativos que afecten sus derechos e intereses, de acuerdo con lo que determina el artículo 59. Por su parte, el artículo 27.2 de la Ley 11/2007 dispone que las administraciones públicas tienen que utilizar medios electrónicos en sus comunicaciones con los ciudadanos, siempre que así lo hayan solicitado o consentido expresamente. La solicitud y el consentimiento, en todo caso, se pueden emitir y pedir por|para medios electrónicos. El apartado 3 del artículo 27 de la Ley 11/2007 indica que las comunicaciones a través de medios

electrónicos son válidas siempre que haya constancia de la transmisión y la recepción, de las fechas y del contenido íntegro de las comunicaciones, y se identifiquen fidedignamente el remitente y el destinatario.

El apartado 5 del mismo artículo 27 determina que los requisitos de seguridad e integridad de las comunicaciones se tienen que establecer en cada caso de manera por la cual es apropiado al carácter de los datos que son objeto, de acuerdo con criterios de proporcionalidad, de conformidad con lo que dispone la legislación vigente en materia de protección de datos de carácter personal.

Como norma especial, el apartado 7 del artículo 27 establece que las administraciones públicas tienen que utilizar preferentemente medios electrónicos en sus comunicaciones con otras administraciones públicas. Las condiciones que rigen estas comunicaciones se tienen que determinar entre las administraciones públicas participantes.

Finalmente, el artículo 38 de la Ley 11/2007 establece minuciosamente los requisitos para la realización de notificaciones telemáticas.

- Significación jurídica del acto (acto reglado/discrecional y otras consideraciones).

  Se trata de un acto absolutamente reglado que la Administración tiene que realizar siempre que lo determine la normativa aplicable.

- Condiciones jurídicas necesarias para que el acto se pueda realizar.

  Las condiciones jurídicas necesarias para la realización del acto son la determinación previa

	del órgano competente y del supuesto legal de la obligación de efectuar la comunicación. - Obligación legal o administrativa de documentar el acto. La comunicación se debe producir, normalmente, en forma documentada, ya que el ciudadano lo debe poder conservar por sus propios medios.
3. ¿Quien realiza el acto?	- Persona física (ciudadano). No aplicable. - Trabajador de la Administración (si procede, funcionario). No aplicable. - Órgano unipersonal de la Administración. La comunicación la ha de llevar a cabo el órgano administrativo competente o el órgano inferior, y se ha de indicar la autoridad de la que proviene, de acuerdo con el artículo 55 de la Ley 30/1992.
4. ¿En qué condición realiza el acto?	- En nombre propio y por cuenta propia. No aplicable. - En calidad de órgano de una persona jurídica pública o privada (representación orgánica). Aplicable. - En calidad de representante legal de una persona física o jurídica, pública o privada. No aplicable. - En calidad de representante voluntario de una persona física o jurídica, pública o privada. No aplicable. - En calidad de representante profesional de una persona física o jurídica (representación presunta). No aplicable.

5. ¿Existe posibilidad de sustitución personal?
   - Actos estrictamente personales.
     No aplicable.
   - Cualquier representante.
     No aplicable.
   - Cualquier persona física con una condición concreta (p. ej., cualquier traajador público de un grupo.
     No aplicable.

6. ¿Genera un documento nuevo, se manifesta sobre un documento existente previamente o sobre un registro (de expediente o de libros)?
   - Genera un documento nuevo.
     Aplicable.
   - Se plasma en un documento existente.
     No aplicable.
   - Se registra, sin generar manifestación documental.
     No aplicable.

7. ¿Requiere la comprobación previa de la identidad de quien realiza el acto?
   - Sí/No.
     Sí.
   - Determinación del método de identificación y autenticación de la persona que actúa.
     Sello de actuación administrativa automática o código seguro de verificación.
   - Valoración del nivel de evidencia del método utilizado, de acuerdo con el esquema de CATCert.
     Nivel 3 o superior.

8. ¿Requiere la comprobación previa de la condición de quien realiza el acto?
   - Sí/No.
     No, ya que se utiliza un sello de actuación administrativa automática.
   - Comprobación de la facultad de actuación, orgánica o legal.

	No aplicable. - Comprobación de un apoderamiento o de una autorización, en representación voluntaria. No aplicable. - Comprobación de la condición de profesional de colectivo autorizado. No aplicable.
9. ¿Requiere una comunicación confidencial previa o posterior?	- Sí/No. En general, no, pero depende del contenido de la comunicación, ya que si contiene datos personales de nivel alto, entonces habrá que garantizar el secreto. - Determinación del método de protección utilizado. El método de protección a utilizar depende del mecanismo de comunicación que se utilice
10. ¿Es de ejecución automática o mecánica, total o parcialmente?	- Sí/No. Sí. - Determinación de los tratamientos automáticos o mecánicos. El automatismo posible consiste en la generación, el sellado y la entrega de la comunicación.

6. La actuación administrativa automatizada y el ciclo de vida del software

Una vez presentada nuestra visión sobre la interpretación "informática" de la norma a automatizar, en particular sobre la base de los diferentes lenguajes lógicos y su aplicación al dominio jurídico, así como algunos casos relevantes para la automatización, hay que entrar en la discusión sobre la naturaleza de la aplicación o el software que permite la actuación administrativa automatizada y sobre la idoneidad de las metodologías de ingeniería existentes actualmente para crear un producto con bastante calidad para "delegar" el ejercicio de la potestad administrativa, que es lo que en definitiva encontramos en el caso de la actuación administrativa sin intervención humana en cada caso singular.

6.1. La naturaleza del tipo de aplicación que ofrece soporte a la actuación administrativa automatizada

Una cuestión sin duda relevante en el contexto analizado es precisamente la determinación de la naturaleza correspondiente al tipo de aplicación que ofrece soporte a la actuación administrativa automatizada, es decir, cuál es la funcionalidad de la aplicación.

Ante la concepción clásica de la aplicación informática como auxiliar de la persona física que aplica el derecho, encontramos en estas aplicaciones una orientación completamente diferente, que se corresponde, más que con la informática documental o de oficina, con la que ha sido denominada *informática jurídica decisional*.

FROSINI recoge las primeras experiencias en materia de automatización de problemas jurídicos a partir de las propuestas de LOEVINGER, que había denominado *jurimetría* a esta posibilidad, y de HOFFMANN, que la denominó *lawtomation*, indicando uno de los

principios que posteriormente han sido recogidos por la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos.

En efecto, se indica que, para la difusión del uso de las calculadoras electrónicas y de los procedimientos cibernéticos en general – hay que recordar que el trabajo de FROSINI se remonta a los años sesenta – entre los juristas, se requiere, en general, incluso antes que una racionalización acabada en la producción jurídica, una simplificación de los conceptos, los métodos y las técnicas tradicionales. Asimismo, FROSINI recoge la crítica ya inicial que SPENGLER realizó a estos tipos de sistemas, indicando que una «justicia hecha a máquina» da lugar a un nuevo fetichismo, aumenta la rigidez conceptual de los juristas y favorece la pérdida del sentido de la responsabilidad personal, en especial a partir de una conceptualización puramente analítica que puede conducir a malentendidos radicales de normas, sentencias y documentos jurídicos.

A pesar de estas reservas iniciales, en el año 1963 KERIMOV[57] anunciaba una planificación interesante – y, en opinión nuestra, bastante actual – de los objetivos de investigación y aplicación de la automatización legal en la extinta Unión Soviética. En esta obra aparece recogido explícitamente el objetivo de analizar las instituciones de derecho público partiendo de la teoría de los juegos, con simulaciones electrónicas para encontrar los medios más eficaces y racionales para aplicarlas. Esta planificación se concretó parcialmente en experiencias de cálculo de la posibilidad de jubilación de trabajadores a petición propia.

Entre nosotros, PÉREZ LUÑO[58] mantiene que la informática jurídica tiene como objeto la aplicación de la tecnología de la información al derecho. Considera que se trata de una disciplina bifronte de metodología tecnológica y objeto jurídico, que precisamente condiciona la aplicación de este método.

---

[57] KERIMOV, D.A. «Future applicability of cybernetics to jurisprudence in the U.S.S.R», *Modern Uses of Logic in Law*, 1963, citado por FROSINI.

[58] PÉREZ LUÑO. A.E. *Manual de informática…*, *op. cit*.

PÉREZ LUÑO distingue tres grandes tipos de aplicaciones de informática jurídica:

- La informática jurídica documental, cuyo objeto es la automatización de los sistemas de información relativos a las fuentes del conocimiento jurídico: legislación, jurisprudencia y doctrina.

- La informática jurídica de gestión, que tiene como objeto la automatización de las tareas rutinarias que se desarrollan en cualquier oficina, incluyendo el despacho jurídico o administrativo.

- La informática jurídica de decisión, integrada por procedimientos dirigidos a la sustitución o la reproducción, total o parcial, de las actividades del jurista mediante la aplicación de la programación algebraica o lógica, en este caso, especialmente desde la rama de la informática identificada con la expresión general de inteligencia artificial, y, en particular, desde la disciplina de los sistemas expertos y de la ingeniería del conocimiento.

  En particular, el autor menciona la aparición de proyectos y prototipo de sistemas expertos jurídicos en liquidaciones tributarias, cálculo de indemnizaciones por accidentes laborales o de tráfico, predicción de las consecuencias jurídicas en casos de impacto medioambiental o condiciones de adquisición de la nacionalidad y derecho de familia.

En relación con la informática jurídica de decisión, que sería el tipo dentro del cual tenemos que inscribir las aplicaciones informáticas que ofrecen soporte a la actuación administrativa automática, PÉREZ LUÑO advierte, en la tradición general – a la cual nos adherimos – que se debe considerar insuficiente la inferencia lógica – más o menos representativa, como hemos visto anteriormente – ya que sustituye la interpretación del derecho por parte de las personas por el razonamiento subyacente.

En efecto, en la medida de que las máquinas pueden procesar informaciones y establecer inferencias lógicas, pero no pueden comprender la multiplicidad de circunstancias que concurren en las conductas humanas, no parece adecuada la suplantación plena del intérprete por el cálculo matemático del ordenador, sino que

sólo en aspectos de la experiencia rutinaria, estandarizados, formalizables y con variables predeterminadas cerradas es posible recurrir a sistemas completamente automáticos.

Sin embargo, la adopción de esta posición no implica que el alcance de la actuación administrativa automatizada tenga que ser reducido: los casos evaluados a lo largo de este trabajo de investigación presentados anteriormente son excelentes candidatos a la automatización.

Podemos indicar que la aplicación que permita la actuación administrativa automatizada será una aplicación de informática jurídica de decisión que se tiene que basar intensamente en el análisis lógico de las proposiciones normativas, aunque será potestad de cada Administración pública decidir el lenguaje a aplicar.

Mientras que en algunos casos se optará por una aproximación de sistema experto, basado en una representación plena del conocimiento del dominio jurídico involucrado y el uso de lenguajes de programación lógica capaces de decidir en tiempo de ejecución, en la mayoría de casos existirá una primera fase de análisis y diseño de la aplicación que tendría que considerar las herramientas de formalización y de interpretación lógica presentadas anteriormente. Posteriormente se codificará un programa utilizando lenguajes y métodos de computación tradicionales, a menudo obedeciendo a criterios de eficiencia computacional y coste[59].

Sea como sea, en opinión nuestra es absolutamente necesario gestionar adecuadamente el ciclo de vida del software o la aplicación que implementa la actuación administrativa automatizada mediante metodologías de calidad y seguridad, independientemente de la orientación escogida.

[59] En este sentido, LUGER, G.F. i STUBBLEFIELD, W.A. *Artificial Intelligence…*, *op. cit.*

6.2. La gestión del ciclo de vida del software

Hay que remarcar que la referencia al análisis y al diseño de la aplicación de actuación administrativa automatizada, así como el resto de aspectos identificados, de seguridad, de auditoría del código, etc., que derivan de la interpretación del artículo 39 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, se tienen que entender como procesos e interfaces del ciclo de vida del software, es decir, como fases de un proceso más amplio, que es el proceso de desarrollo de sistemas de información, el cual se tiene que definir y gestionar dentro de la Administración pública que implementa la actuación administrativa automatizada.

Aplicar una metodología – más o menos formalizada y madura – para el desarrollo del software que soporta la aplicación de actuación administrativa automatizada implica asumir una serie de riesgos, especialmente en relación con posibles errores de programación, que se pueden actualizar en forma de una programación inadecuada del sistema y, por lo tanto, convertirse en motivo de impugnación de la actuación por parte de los afectados.

Resulta, por lo tanto, necesario presentar de forma sucinta una metodología de ciclo de vida del software. En el Estado español, el Consejo Superior de Administración Electrónica del Ministerio de Administraciones Públicas ha desarrollado la metodología MÉTRICA, que se describe a continuación. Existen muchas otras metodologías de desarrollo, algunas bastante más actualizadas que MÉTRICA, de manera que la elección de MÉTRICA se lleva a cabo a efectos puramente didácticos y, sobre todo, por su utilización en el sector público estatal.

La metodología MÉTRICA versión 3 ofrece a las organizaciones un instrumento útil para la sistematización de las actividades que dan soporte al ciclo de vida del software dentro del marco que permite alcanzar los objetivos siguientes:

- Proporcionar o definir sistemas de información que ayuden a conseguir las finalidades de la organización mediante la definición de un marco estratégico para el desarrollo de estos sistemas.

- Dotar a la organización de productos de software que satisfagan las necesidades de los usuarios concediendo una mayor importancia al análisis de requisitos.

- Mejorar la productividad de los departamentos de sistemas y tecnologías de la información y las comunicaciones permitiendo una mayor capacidad de adaptación a los cambios y teniendo en cuenta la posible reutilización.

- Facilitar la comunicación y la comprensión entre los diferentes participantes en la producción de software durante el ciclo de vida del proyecto teniendo en cuenta su papel y su responsabilidad, así como las necesidades de todo el mundo.

- Facilitar la operación, el mantenimiento y el uso de los productos de software obtenidos.

Con respecto a estándares, se ha considerado referencia principal el modelo de ciclo de vida de desarrollo propuesto a la norma ISO 12207 Information Technology / Software Life Cycle Processes. Siguiendo este modelo, se ha elaborado la estructura de MÉTRICA versión 3, en la cual se distinguen procesos principales (planificación, desarrollo y mantenimiento) e interfases (gestión de proyectos, aseguramiento de la calidad, seguridad y gestión de proyectos) con el objetivo de ofrecer soporte al proyecto en los aspectos organizativos.

Además de la norma ISO 12207 – cuya primera publicación data de 1995 –, entre los estándares de referencia hay que destacar las normas ISO/IEC TR 15504/SPICE Software Process Improvement and Assurance Standards Capability Determination, UNE-EN-ISO 9001:2000 Sistemas de Gestión de la Calidad. Requisitos, UNE-EN-ISO 9000:2000 Sistemas de Gestión de la Calidad. Fundamentos y Vocabulario, y el estándar IEEE 610.12-1990 Standard Glossary of Software Engineering Terminology. Igualmente, se han considerado otras metodologías como SSADM, Merise, Information Engineering, MAGERIT. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información – promovida por el Consejo Superior de Informática (hoy Consejo Superior de Administración Electrónica) – y EUROMÉTODO.

Desde otra perspectiva, hay que indicar que MÉTRICA describe únicamente los procesos y las actividades del ciclo de vida del software, pero no tiene en consideración aspectos de mejora de capacidades ni de madurez relativos a este ciclo de vida.

Asimismo, hace falta tener en cuenta que desde la publicación de MÉTRICA versión 3 ha tenido lugar una importante evolución en los estándares internacionales de referencia, cosa que aconseja evaluar la conveniencia de utilizar MÉTRICA o, por contra, adherirse a las normas más recientes, entre las cuales podemos mencionar las siguientes:

- ISO/IEC 12207:2008, que actualiza la versión anterior de esta norma, así como las correcciones técnicas de los años 2002 y 2004.

- ISO/IEC 14764:2006, que amplía los detalles sobre el proceso de mantenimiento de software descrito a la ISO/IEC 12207 en relación con la planificación, la ejecución y el control, la revisión y la evaluación, y el cierre del proceso de mantenimiento.

- ISO/IEC 15288:2008, que establece un marco de trabajo común para describir el ciclo de vida de los sistemas creados por humanos, de manera armonizada con la norma ISO/IEC 12207 en el caso de los sistemas de información.

- ISO/IEC 15940:2006, que define los servicios de uno entorno a ingeniería de software que se pueden utilizar de manera genérica o para la producción automatizada de software.

- ISO/IEC 16085:2006, que define un proceso para la gestión del riesgo en el ciclo de vida de sistemas o del software, indistintamente.

En el mismo sentido, parece bastante necesario complementar la metodología MÉTRICA con un marco concreto que permita precisamente evaluar, de manera continuada o por etapas, la implementación de los procesos de desarrollo de software, como también otros procesos relacionados, para lo cual se podría utilizar, por ejemplo,

el modelo CMMI for Development (Integración de Modelos de Madurez de Capacidades para el Desarrollo), publicado por el Instituto de Ingeniería del Software de la Universidad Carnegie Mellon, de los Estados Unidos de América.

6.2.1. Los procesos de desarrollo de sistemas de información

MÉTRICA divide el proceso de desarrollo de sistemas de información en cinco procesos para facilitar la comprensión y atendiendo a su amplitud y complejidad:

- Estudio de viabilidad del sistema.
- Análisis del sistema de información.
- Diseño del sistema de información.
- Construcción del sistema de información.
- Implantación y aceptación del sistema.

La necesidad de reducir el ciclo de desarrollo de los sistemas de información ha orientado a muchas organizaciones hacia la elección de productos software del mercado cuya adaptación a sus requerimientos significaba un esfuerzo bastante inferior al de un desarrollo a medida, para no hablar de los costes de mantenimiento.

Esta decisión, estratégica en muchas ocasiones para una organización, se tiene que tomar con las precauciones necesarias, y es una realidad que está cambiando el escenario del desarrollo del software.

Otra consecuencia de este hecho es la práctica, cada vez más habitual en las organizaciones, de la contratación de servicios externos en relación con los sistemas y las tecnologías de la información y las comunicaciones. Eso conduce a la necesidad

de gestionar y controlar adecuadamente estos servicios externos y el riesgo implícito[60] a fin de que los resultados representen un beneficio para la organización.

6.2.1.1. El estudio de viabilidad del sistema

El objetivo de este proceso es analizar un conjunto concreto de necesidades con la idea de proponer una solución a corto plazo. Los criterios con que se hace esta propuesta no tienen que ser estratégicos, sino tácticos y relacionados con aspectos económicos, técnicos, legales y operativos. Ya en este momento se tiene que considerar la especial relevancia y los riesgos particulares que puede implicar la realización de actuaciones administrativas automatizadas, como desarrollemos detalladamente más adelante.

Los resultados del estudio de viabilidad del sistema tienen que constituir la base para tomar la decisión de continuar adelante o de abandonar. Si se decide continuar adelante, pueden surgir uno o diversos proyectos que afecten uno o diversos sistemas de información. Estos sistemas se tienen que desarrollar de acuerdo con el resultado obtenido en el estudio de viabilidad y teniendo en cuenta la cartera de proyectos para la estrategia de implantación del sistema global.

Se ha considerado que este proceso es obligatorio, aunque el nivel de profundidad con que se ejecute dependerá de cada caso. La conveniencia de hacer el estudio de la situación actual depende del valor añadido previsto para la especificación de requisitos y para el planteamiento de alternativas de solución. En las alternativas, se consideran típicamente soluciones "a medida", soluciones basadas en la adquisición de productos software del mercado o soluciones mixtas.

---

[60] En relación con la externalización, véase RAMIÓ, C., SALVADOR, M. i GARCIA, O., *Els determinants i la gestió de l'externalització a Catalunya. Món local i món autonòmic*. Barcelona: Escola d'Administració Pública de Catalunya, 2007.

6.2.1.2. El anàlisis del sistema de información

El propósito de este proceso es conseguir la especificación detallada del sistema de información a través de un catálogo de requisitos y una serie de modelos que cubran las necesidades de información de los usuarios para los cuales se tiene que desarrollar el sistema de información, y que tienen que ser la entrada al proceso de diseño del sistema de información.

En primer lugar, se debe describir el sistema de información a partir de los productos generados en el proceso de estudio de viabilidad del sistema. Se delimita el alcance, se genera un catálogo de requisitos generales y se describe el sistema mediante unos modelos iniciales de alto nivel.

Se recogen de manera detallada los requisitos funcionales que el sistema de información tiene que cubrir – aspecto que resulta especialmente sensible en el caso de la actuación administrativa automatizada, que tiene que interpretar de una manera particularmente completa y esmerada la norma jurídica a aplicar – y se catalogan, hecho que permite establecer la trazabilidad a lo largo de los procesos de desarrollo. Además, se identifican los requisitos no funcionales del sistema, es decir, las facilidades que tiene que proporcionar el sistema y las restricciones a que se encontrará sometido en cuanto a rendimiento, frecuencia de tratamiento, seguridad, etc.

Para facilitar el análisis del sistema, se deben identificar los subsistemas de análisis y se deben elaborar los modelos de casos de uso y de clases, en desarrollos orientados a objetos, y de datos y procesos, en desarrollos estructurados. Hay que desarrollar una actividad específica para la definición de interfaces de usuario a medida que se van depurando los requisitos y los modelos anteriores. Asimismo, hay que especificar todas las interfaces entre el sistema y el usuario, como formatos de pantallas, diálogos, formados de informes y formularios de entrada.

Una vez acabados los modelos, se debe llevar a cabo un análisis de consistencia mediante una verificación y una validación, cosa que puede forzar la modificación de algunos de los modelos obtenidos. Como también trataremos posteriormente, esta actividad adquiere una relevancia particular en el caso de la definición funcional de un

procedimiento administrativo que incorpore la actuación administrativa automatizada, ya que ofrece la oportunidad de detectar carencias y errores en la interpretación de la norma en que se basará la actuación administrativa automatizada mencionada.

Después de hacer este análisis de consistencia, se elabora la especificación de requisitos de software, que constituye un punto de referencia en el desarrollo del software y la línea base de referencia para las peticiones de cambio sobre los requisitos especificados inicialmente.

En este proceso se inicia también la especificación del plan de pruebas, que se tiene que completar en el proceso correspondiente al diseño del sistema de información.

En estas actividades es muy importante la participación de los usuarios a través de técnicas interactivas – como diseño de diálogos y prototipos –, las cuales permiten que los usuarios se familiaricen con el nuevo sistema y colaboren en la construcción y el perfeccionamiento de éste.

Tal como hemos avanzado, en el caso de la actuación administrativa automatizada hay que involucrar intensamente personal experto en el ámbito legal en estas actividades para garantizar un análisis adecuado de los requisitos funcionales, a partir de una interpretación jurídica apropiada de las normas en que se basarán los actos administrativos y, muy especialmente, los de naturaleza decisoria.

6.2.1.3. El diseño del sistema de información

El propósito del diseño del sistema de información es obtener la definición de la arquitectura del sistema y del entorno tecnológico que le tiene que ofrecer apoyo, junto con la especificación detallada de los componentes del sistema de información. A partir de esta información, se generan todas las especificaciones de construcción relativas al sistema, así como la especificación técnica del plan de pruebas, la definición de los requisitos de implantación y el diseño de los procedimientos de migración y carga inicial, cuando ocurra.

Este proceso consta de un primer bloque de actividades, que se desarrollan en paralelo, con el objetivo de obtener el diseño de detalle del sistema de información que comprende la partición física del sistema de información (independiente de un entorno tecnológico concreto), la organización en subsistemas de diseño, la especificación del entorno tecnológico sobre el cual se despliegan aquellos subsistemas, y la definición de los requisitos de operación, administración del sistema, seguridad y control de acceso.

Igual que en el proceso de análisis del sistema de información, antes de especificar los componentes se tiene que hacer una verificación y una validación con el fin de analizar la consistencia entre los diferentes modelos y formalizar la aceptación del diseño de la arquitectura del sistema por parte de los usuarios de explotación y sistemas.

Como también hemos indicado anteriormente, parecería necesario involucrar en esta verificación y en esta validación personal experto que pueda garantizar la consistencia entre el diseño y la interpretación legal que se fijó en las etapas anteriores, con la finalidad de evitar posibles errores.

Además, consideramos que resulta particularmente importante establecer controles técnicos que garanticen la seguridad de las operaciones, en el sentido que expondremos más adelante.

6.2.1.4. La construcción del sistema de información

La construcción del sistema de información tiene como objetivo final la construcción y la prueba de los diferentes componentes del sistema de información a partir del conjunto de especificaciones lógicas y físicas correspondientes, obtenido en el proceso de diseño del sistema de información. Se desarrollan los procedimientos de operación (no son necesarios en el caso de la actuación administrativa automatizada) y seguridad, y se elaboran los manuales de usuario final (tampoco resultan necesarios en el caso de la actuación administrativa automatizada) y de explotación, cuando proceda.

Para conseguir este objetivo, se debe recoger la información relativa al producto del diseño de especificaciones de construcción del sistema de información, preparar el entorno de construcción, generar el código de cada uno de los componentes del sistema de información y efectuar, a medida que se vaya finalizando la construcción, las pruebas unitarias de cada uno y las pruebas de integración entre subsistemas.

Si hubiera que llevar a cabo una migración de datos, sería en este proceso donde se ejecutaría la construcción de los componentes de migración y los procedimientos de migración y carga inicial de datos.

6.2.1.5. La implantación y la aceptación del sistema

Este proceso tiene como objetivo principal la entrega y la aceptación del sistema en su totalidad, que puede comprender diversos sistemas de información desarrollados de manera independiente, según se haya establecido en el proceso de estudio de viabilidad del sistema. El segundo objetivo es llevar a cabo las actividades oportunas para pasar a la producción del sistema.

Se establece el plan de implantación, una vez revisada la estrategia de implantación, y se detalla el equipo que lo ejecutará.

Para la iniciación de este proceso se toman como punto de partida los componentes del sistema probados de manera unitaria e integrados en el proceso construcción del sistema de información, así como la documentación asociada.

El sistema se tiene que someter a las pruebas de implantación con la participación del usuario de operación, que tiene la responsabilidad, entre otros aspectos, de comprobar el comportamiento del sistema en las condiciones más extremas. El sistema se tiene que someter igualmente a las pruebas de aceptación que tiene que ejecutar al usuario final.

También en este caso podemos llamar ya la atención sobre la necesidad de establecer controles propios en el caso de la aceptación del sistema de información que ofrece apoyo a la actuación administrativa automatizada.

En este proceso se elabora el plan de mantenimiento del sistema, de manera tal que el responsable del mantenimiento conozca el sistema antes de que pase a producción.

Finalmente, se establece el acuerdo de nivel de servicio requerido una vez se inicie la producción. Este acuerdo hace referencia a los servicios de gestión de operaciones, de soporte a usuarios, y al nivel de acuerdo con el cual se deben prestar estos servicios.

6.2.2. El proceso de mantenimiento de sistemas de información

El objetivo de este proceso es obtener una nueva versión de un sistema de información a partir de las peticiones de mantenimiento que hacen los usuarios con motivo de un problema detectado en el sistema o bien por la necesidad de mejorarlo.

Ante una petición de cambio de un sistema de información ya en producción, se efectúa un registro de las peticiones, se diagnostica el tipo de mantenimiento y se decide si se da respuesta o no – en función del plan de mantenimiento asociado al sistema afectado por la petición –, y se establece con qué prioridad.

La definición de la solución de la necesidad o el problema planteado por el usuario, que hace el responsable de mantenimiento, incluye un estudio de impacto, la valoración del esfuerzo y del coste, las actividades y las tareas del proceso de desarrollo a realizar y el plan de pruebas de regresión.

En este proceso también hay que indicar la necesidad de establecer controles específicos en el caso de la actuación administrativa automatizada, sobre todo derivados de la necesidad de detectar y tratar correctamente los cambios sobre el sistema de información motivados por una modificación (o derogación) de la norma

jurídica. En efecto, se podría dar la situación que, una vez derogada una norma, el sistema automatizado continuara tomando decisiones administrativas de acuerdo con la norma derogada, las cuales resultarían incorrectas, lógicamente.

Por lo tanto, hay que considerar con especial cuidado el procedimiento de mantenimiento del software, por ejemplo mediante un proceso de registro en una base de datos de las normas que han sido objeto de automatización. Una persona deberá hacer el seguimiento de la normativa, de manera que, una vez haya sido derogada una norma que dé cobertura a procedimientos automáticos, lo pueda detectar y evaluar el impacto, con el fin de detener eventualmente el sistema y abrir un procedimiento de mantenimiento.

Normalmente habrá bastante tiempo desde la publicación de la norma hasta la entrada en vigor de la norma sustitutiva. Eso permitirá hacer las modificaciones oportunas, siempre que se haya previsto este mantenimiento evolutivo.

El proceso de registro y seguimiento se podría automatizar en la medida que los editores de las fuentes escritas del derecho – en particular, los diarios oficiales – adopten estándares de publicación de normas en XML, como MetaLex[61], cosa que permitiría identificar las normas derogatorias sin intervención humana y generar la alerta pertinente.

6.3. Algunos requisitos específicos de la aplicación de actuación administrativa automatizada

En la fase de análisis, MÉTRICA recoge una serie de técnicas orientadas a construir al modelo de casos de uso y de clases, en desarrollos orientados a objetos, y de datos y procesos, en desarrollos estructurados. En este punto hay que garantizar que la

[61] CEN CWA 15710:2007. MetaLex (Open XML Interchange Format for Legal and Legislative Resources).

interpretación logicoinformática de la norma es completa y adecuada, es decir, que no quedan casos válidos no considerados, o que no se producen ambigüedades ni errores que impliquen discriminación para los ciudadanos derivada de una decisión inadecuada. Aquí tenemos que introducir la discusión sobre la interpretación lógica del derecho (aplicando lógica deóntica, por ejemplo).

Hay que remarcar la importancia del análisis de consistencia en la fase de análisis funcional y de diseño técnico (doble control), ya que representan puntos de control para detectar problemas en la interpretación en lógica informática de la norma jurídica aplicable. Podemos hacer una cierta crítica al modelo de roles participantes en la gestión del proyecto de desarrollo, dado que MÉTRICA no considera la participación de expertos legales en ninguna fase de la metodología.

Todas las lógicas jurídicas que hemos presentado (deóntica, refutable y descriptiva), aplicadas en forma de lógicas híbridas en un proceso reglado y controlado de interpretación normativa, nos pueden ayudar a adquirir y formalizar los conocimientos jurídicos de la norma a automatizar, así como a establecer mecanismos de validación; de rebote, eso reducirá los riesgos inherentes a la actuación administrativa automatizada

En particular, el uso de una lógica modal híbrida, con elementos de lógica deóntica y refutable, muy especialmente en el contexto de la lógica de la acción, constituye un elemento muy potente para obtener una interpretación objetiva y esmerada de los aspectos estructurales de la norma y de su comportamiento argumentador (lo cual permite una cierta previsibilidad de las posibles aplicaciones de la norma en caso de conflicto, sea judicial o administrativo, en términos de proceso).

Por otra parte, el uso de la lógica descriptiva y de las ontologías nos permite un formalismo de representación del conocimiento jurídico que actúa como base para el diseño de aplicaciones jurídicas adelantadas.

En este sentido, la interpretación lógica puede quedar formalizada en diversos momentos a lo largo del ciclo de vida del software que ofrece apoyo a la actuación administrativa automatizada:

- Una primera posibilidad es realizar y formalizar la interpretación lógica en la fase de análisis funcional y diseño del software. En este caso, la interpretación es un proceso llevado a cabo por un intérprete humano. El proceso generará un conjunto de casos que más tarde tienen que servir para codificar de forma informática el tratamiento de estos casos (la funcionalidad del programa que permite la actuación administrativa automatizada).

- Una segunda posibilidad, complementaria del anterior, consiste en realizar y formalizar la interpretación lógica en el momento de construir el software y, en concreto, en el proceso de codificación informática. Nuevamente la interpretación es un proceso llevado a cabo por un intérprete humano, pero en el mismo momento de producir el código del programa.

- Una tercera posibilidad es realizar y formalizar la interpretación lógica en forma de reglas a aplicar en el momento de ejecución del programa, sin que en el código del programa se encuentre ninguna lógica de funcionamiento de la aplicación. Constituye un ejemplo de esta tercera posibilidad la llamada *programación lógica*, basada en el uso de programas razonadores, como sucede en los llamados *sistemas expertos* y, más recientemente, en la Web semántica.

  En este caso, la interpretación es un proceso realizado sólo parcialmente por un intérprete humano, que colabora en el proceso de representación del conocimiento jurídico y codifica las reglas que después permitirán al programa, mediante operaciones lógicas, decidir los casos en los cuales resulta aplicable esta norma, en una especie de interpretación puramente logicista o mecánica.

- Una cuarta posibilidad es diseñar el sistema de manera tal que sea él mismo quien genere, a partir de la lectura y la comprensión de la norma jurídica, tanto la representación del conocimiento jurídico como las reglas de inferencia lógica necesarias para aplicar las normas. Sólo en este caso podríamos considerar que existe una verdadera interpretación por parte de la máquina, que, a pesar del volumen de experiencias realizadas, especialmente en el dominio de la búsqueda de textos jurídicos, no consideramos practicable en la actualidad.

- Por otra parte, se debe considerar la utilidad de estas herramientas en los procesos de verificación del software producido. Efectivamente, una de las posibilidades más interesantes que ofrecen las herramientas lógicas que hemos presentado es, precisamente, la posibilidad de evaluar formalmente el programa que ofrece apoyo a la actuación administrativa automatizada, de forma integrada durante el proceso de construcción o como procedimiento de evaluación de la idoneidad del programa en momentos posteriores, durante el proceso natural de mantenimiento del programa, que en este caso ocurre particularmente relevante por el hecho que el sistema experimentará ordinariamente el impacto de los cambios normativos.

Evidentemente, el hecho de no disponer – o de no hacer uso – de estas herramientas no quiere decir en ningún caso que el producto resultante – es decir, el programa o la aplicación que ofrece apoyo a la actuación administrativa automática – sea incorrecto o de baja o poca calidad, pero es cierto que con la actuación administrativa automatizada se produce una situación nueva: es el mismo programa el que decide sin la intervención de ninguna persona concreta. Así, se podría dar el caso de un órgano administrativo concreto (una dirección general, por ejemplo) que, teniendo vacante la plaza por cese del director o directora (motivado por un cambio electoral, ponemos por caso), continúa tomando decisiones administrativas que producen efectos internos y externos.

Se trata de un escenario muy diferente del actual, en qué el ordenador sencillamente asiste o prepara una decisión humana, y que obliga a alcanzar una comprensión muy esmerada de las normas a aplicar por vía de una interpretación que no puede quedar en manos de la figura del analista informático – ya lo podemos adelantar –, sino que requiere el concurso y la participación de los expertos en el dominio legal y de la conciencia de la persona titular del órgano impulsor de la automatización.

Esta necesidad – que, si es importante en general, nos parece extraordinariamente relevante en el caso de la actuación automatizada – exige revisar las metodologías del ciclo de vida del software y establecer requisitos y condiciones específicos, ya que la actuación administrativa automatizada es resultado de un producto de ingeniería y tiene que ser tratado como tal.

6.4. La determinación de los requisitos de formalización documental electrónica

A partir del análisis de la funcionalidad de la aplicación, hay que detallar los requisitos de seguridad de la aplicación en términos de autenticidad, integridad y confidencialidad del producto documental que la aplicación genera.

Para llevar a cabo esta tarea, disponemos de diferentes herramientas, entre las cuales podemos mencionar la metodología PADS desarrollada por la Agencia Catalana de Certificación[62].

El análisis PADS es una herramienta que se propone para analizar los requisitos en relación con los actos documentados que se producen dentro de los procesos y los procedimientos de la Administración y sus organismos y entidades, públicos o privados.

El objetivo de este análisis es obtener un catálogo de requisitos de los actos documentados del procedimiento que describa las necesidades en cuanto a los niveles funcionales de seguridad de servicio.

---

[62] ALAMILLO, I., MARTÍNEZ, D., SELTSIKAS, P. i PAPAS, N.. «Designing a Modelling Methodology for Legal Workflows», *Legal Knowledge and Information Systems - JURIX 2007: The Twentieth Annual Conference on Legal Knowledge and Information Systems, Leiden, The Netherlands, 12-15 December 2007*. Frontiers in Artificial Intelligence and Applications 165. IOS Press. Amsterdam. 2007.

El análisis de los procesos (P)

Los procesos son, en una visión muy simplificada, secuencias de acontecimientos que conducen a un resultado concreto. Estos acontecimientos pueden consistir en hechos o en acciones que desencadenan un paso adelante o hacia atrás dentro del proceso.

El procedimiento administrativo es un buen ejemplo de proceso regulado, totalmente o parcialmente, de acuerdo con la ley, que determina el flujo, el contenido y los efectos.

Junto con los procedimientos administrativos, podemos encontrar procesos correspondientes a la prestación de servicios públicos o, incluso, a la prestación de servicios privados por parte de las administraciones públicas y sus organismos.

La primera tarea a desarrollar en el análisis PADS es la definición del proceso en el cual se quiere incorporar la firma electrónica. Existen múltiples definiciones de procedimientos, desde los más informales en lenguaje natural hasta el uso de lenguajes formales de definición y de ejecución de procesos[63].

Esta guía no adopta ningún modelo formal para la definición de los procesos, ya que este análisis es instrumental con respecto a la determinación de los documentos generados en la ejecución de los procesos, y, en especial, de los requisitos de firma correspondientes. Sin embargo, se recomienda la adopción de un método formal, apropiado al tipo de aplicación y al entorno del negocio concreto.

Los aspectos a considerar son los siguientes:

1. ¿Cuál es el contenido del proceso?
   - Descripción del proceso.
   - Modalidad de gestión (servicio en gestión privada, gestión pública, procedimiento

[63] A este efecto, actualmente existen iniciativas que trabajan en la definición de estándares de ámbito internacional en relación con la notación de procesos de negocio (BPMN), lenguajes de definición de procesos de negocio (BPDL o XBPL) o ejecución de procesos de negocio (WS BPEL).

	administrativo). - Efectos que produce el proceso.
2. ¿Cuál es la normativa aplicable al proceso?	- Identificación de las normas aplicables. - Significación jurídica del proceso. - Condiciones jurídicas necesarias para que el proceso se pueda realizar.
3. ¿Cuál es el flujo de trabajo?	- Listado o gráfico de los eventos que lo conforman, incloyendo los actos y los hechos relevantes, así como las conexiones correspondientes.
4. ¿Cuáles son los procesos relacionados?	- Procesos anteriores. - Procesos coetáneos. - Procesos posteriores.

6.4.1. El análisis de los actos (A)

Una vez hemos identificado los procesos, procede analizar los actos evaluando cada acto por separado.

Los actos son, en definitiva, los verbos correspondientes a la acción (del ciudadano, de la Administración o de terceras personas o entidades) que inicia, impulsa o acaba el proceso. Se diferencian de los hechos o las omisiones en que habitualmente hay que documentarlos.

Algunos ejemplos habituales son:

- Solicitar, presentar (solicitudes, declaraciones, documentos complementarios, alegaciones, recursos). En este tipo de acto es frecuente introducir una parte importante de la relación telemática con las administraciones públicas, bien

directa con la persona interesada o con una tercera persona que presenta en nombre suyo.

- Registrar (de entrada, de salida, en un libro o registro administrativo).
- Informar, dar visto bueno y otros actos parecidos.
- Resolver.
- Notificar, comunicar y otros actos parecidos.

Captar la naturaleza exacta de cada acto resulta esencial para las futuras fases de análisis:

- Por ejemplo, no todos los actos se manifiestan en documentos independientes, sino que resulta frecuente encontrar diversos actos documentados en el mismo instrumento. Un caso paradigmático es un documento de autorización de pago, que incorpora actos de diferentes órganos cuya plasmación se recoge en el mismo documento. Por lo tanto, habrá que distinguir los actos de los documentos.

- En algunos actos, puede resultar indiferente quien es la persona física de que lo produce, tal como sucede en algunos actos preparatorios de una resolución administrativa, en qué cualquier trabajador público de un grupo concreto podría preparar el expediente por el hecho que el acto legalmente válido lo llevará a cabo un órgano administrativo unipersonal superior, por ejemplo. Otro caso parecido es el del simple impulso del procedimiento o los traslados de expedientes, que no tienen relevancia externa y que, por lo tanto, no tienen que revestir las formalidades de los actos administrativos.

- Por contra, en otros actos precisamente la persona que los realiza es absolutamente esencial, así como la calidad del proceso de actuación con medios electrónicos.

Los aspectos a considerar son los siguientes:

1. ¿Cuál es el contenido del acto?
   - Descripción del acto.
   - Tipo de acto (del ciudadano/de la

	Administración, otros). - Efectos que produce dentro del proceso (inicia, acaba, otros).
2. ¿Cuál es la normativa aplicable al acto?	- Identificación de las normas aplicables. - Significación jurídica del acto (acto reglado/discrecional y otras consideraciones). - Condiciones jurídicas necesarias para que el acto se pueda realizar. - Obligación legal o administrativa de documentar el acto.
3. ¿Quien realiza el acto?	- Persona física (ciudadano). - Trabajador de la Administración (si procede, funcionario). - Órgano unipersonal de la Administración.
4. ¿En qué condición realiza el acto?	- En nombre propio y por cuenta propia. - En calidad de órgano de una persona jurídica pública o privada (representación orgánica). - En calidad de representante legal de una persona física o jurídica, pública o privada. - En calidad de representante voluntario de una persona física o jurídica, pública o privada. - En calidad de representante profesional de una persona física o jurídica (representación presunta).
5. ¿Existe posibilidad de sustitución personal?	- Actos estrictamente personales. - Cualquier representante. - Cualquier persona física con una condición concreta (p. ej., cualquier traajador público de un grupo.

6. ¿Genera un documento nuevo, se manifesta sobre un documento existente previamente o sobre un registro (de expediente o de libros)?	- Genera un documento nuevo. - Se plasma en un documento existente. - Se registra, sin generar manifestación documental.
7. ¿Requiere la comprobación previa de la identidad de quien realiza el acto?	- Sí/No. - Determinación del método de identificación y autenticación de la persona que actúa. - Valoración del nivel de evidencia del método utilizado, de acuerdo con el esquema de CATCert.
8. ¿Requiere la comprobación previa de la condición de quien realiza el acto?	- Sí/No. - Comprobación de la facultad de actuación, orgánica o legal. - Comprobación de un apoderamiento o de una autorización, en representación voluntaria. - Comprobación de la condición de profesional de colectivo autorizado.
9. ¿Requiere una comunicación confidencial previa o posterior?	- Sí/No. - Determinación del método de protección utilizado.
10. ¿Es de ejecución automática o mecánica, total o parcialmente?	- Sí/No. - Determinación de los tratamientos automáticos o mecánicos.

6.4.2. El análisis de los documentos y los registros (D)

Con respecto a los actos a documentar, hay que identificar las salidas documentales que generan, así como los requisitos formales correspondientes, tanto en documentos independientes como en colecciones de documentos (libros electrónicos) o registros administrativos electrónicos.

Algunos ejemplos habituales son:

- Las solicitudes de servicios públicos o en relación con procedimientos administrativos.
- Las resoluciones administrativas y sus notificaciones.
- Los recursos de todo tipo.
- Los libros o los registros electrónicos administrativos.
- Las certificaciones y las copias.

Los aspectos a considerar son los siguientes:

1. ¿Cuál es el contenido del documento?	- Descripción del documento. - Tipo de documento (privado, administrativo, público).
2. ¿Cuál es la normativa aplicable al documento?	- Identificación de las normas aplicables.
3. ¿Qué requisitos formales son exigibles?	- Necesidad de ser original, copia simple o copia auténtica. - Necesidad de incorporar una firma. - Necesidad de incorporar una marca, un registro o un sello. - Necesidad de incorporar la fecha y/o la hora. - Necesidad de incorporar un rol, un cargo u otra condición subjetiva o personal.

4. ¿Qué requisitos de acreditación del contenido son exigibles?	- Necesidad de acreditar la personalidad jurídica. - Necesidad de acreditar la capacidad para actuar en nombre de tercero. - Necesidad de aportar acreditación objetiva del contenido.
5. ¿Quiénes son los destinatarios del documento?	- Personas o entidades destinatarias directas del documento. - Personas o entidades a las cuales puede llegar el documento, indirectamente (por ejemplo, mediante la entrega por parte del destinatario inicial).
6. ¿Cuál es el plazo de vida previsto del documento?	- Número de años que el documento permanece en circulación. - Número de años que el documento permanece archivado.

6.4.3. El análisis de las firmas o los sellos (S)

En el caso de los actos documentados, finalmente resulta necesario identificar los requisitos de autenticidad, de integridad y, habitualmente, de imputación de la calidad de autor u otras cualidades, hecho que nos conduce al análisis de los requisitos de firma.

En este punto, y de acuerdo con los requisitos del acto y del documento correspondiente, hay que determinar los aspectos concretos de la firma o el sellado automático:

1. ¿Cuál es el significado jurídico de la firma?	- Descripción del tipo de significado. - Indicación de si la firma es mancomunada, solidaria, siguiente dentro de una secuencia o de otro tipo.
2. ¿Qué condición personal acredita la firma?	- Autor u otra condición (en sustitución, por delegación o por otro mecanismo). - Actúa en nombre propio o en representación.
3. ¿Hay que acreditar la fecha de la firma independientemente de la fecha del documento?	- Sí/No.
4. ¿La firma se debe producir después de otra firma?	- Sí/No. - Orden de las firmas.

6.4.4. Utilizar certificados digitales para el servicio

Durante la ejecución del análisis PADS llevado a cabo anteriormente habremos encontrado necesidades relativas a la autenticación robusta de los actores o la necesidad de proteger información confidencial, y especialmente la necesidad de firmar documentos electrónicos, funcionalidades que se basan en certificados.

El objetivo de esta fase es identificar el catálogo de requisitos de certificación, que detalla los relativos a los certificados que hay que utilizar como soporte de las operaciones criptográficas de autenticación, de firma y de cifrado.

Los aspectos a considerar son los siguientes:

1. ¿Qué tipos de certificados se necesitan?
   - Persona física.
     - Individuales/ciudadano.
     - Profesionales.
     - Vinculación a entidad.
     - Representación.
   - Persona jurídica.
   - Entidad sin personalidad jurídica.
   - Dispositivo.
   - Servidor seguro.
   - Sede electrónica.
   - Sello electrónico.
   - Personal al servicio de la Administración.

2. ¿Qué usos hay que dar a los certificados?
   - Autenticación.
   - Firma digital.
   - Cifrado.

3. ¿Qué aplicaciones específicas han de soportar los certificados?
   - Firma de documentos.
   - Correo electrónico S/MIME.
   - Canal seguro SSL/TLS.
   - Seguridad de servicios web.
   - Firma de código.
   - Firma de aplicación.
   - TSA, OCSP, otros.

4. ¿Qué estrategias de certificación digital hay que establecer?
   - Emisión de certificados con entidad de certificación propia.
   - Emisión de certificados en colaboración con CATCert (adquisición de certificados).
     - Para uso propio.
     - Para dotar a terceras personas o entidades.

- Admisión de certificados de otras entidades de certificación.

6.4.5. Preparación de los casos de uso de seguridad de la aplicación

Los casos de uso del servicio son un conjunto de escenarios que describen las interacciones entre un usuario y un sistema de información a efectos de establecer los requisitos correspondientes. Los casos de uso tienen un ciclo de vida complejo y, de hecho, se transforman durante su evolución, desde la fase de descubrimiento, implementación y aceptación por parte de los usuarios. Así pues, hay diversas formas de representar los casos de uso en función del momento evolutivo del caso de uso durante las fases de análisis, desarrollo, implementación y prueba del software.

Es bastante habitual agruparlos en diagramas de casos de uso, que muestran las relaciones entre los actores – usuarios o sistemas – y los diferentes casos de uso, cosa que permite visualizar rápidamente la funcionalidad global del servicio. Otra representación utilizada habitualmente en relación con los casos de uso son los diagramas de secuencias de interacción y los diagramas de actividades, especificados de acuerdo con el lenguaje universal de modelización (UML, *universal modeling language*).

En esta fase inicial conviene preparar los casos de uso relativos a las funciones de seguridad criptográfica del servicio, entre los cuales habría que considerar los siguientes:

- Casos de uso de autenticación de los actores y de la documentación gestionada por los sistemas.
- Casos de uso de firma electrónica de documentación por los actores.
- Casos de uso de firma electrónica de transporte seguro de mensajes entre actores y sistemas, como en el caso de la mensajería de servicios web entre sistemas remotos.
- Casos de uso de archivo de firma electrónica.

- Casos de uso asociados a las evidencias electrónicas, incluyendo los procedimientos judiciales y administrativos en papel.

Por otra parte, no es extraño que la definición y la descripción de los casos de uso evolucionen a medida que se trabaja, de manera que podemos encontrar los estados siguientes:

- Casos de uso identificados recientemente, con poca descripción además del nombre del caso de uso.
- Casos de uso descritos sucintamente, en general de manera poco rigurosa.
- Descripción inicial de las secuencias de acciones que conforman el caso de uso.
- Identificación de la secuencia de acciones esenciales que conforman el caso de uso.
- Casos de uso descritos detalladamente, en forma narrativa o conversativa.
- Casos de uso descritos completamente, sin ambigüedades, que permiten la comprensión total, exacta y verificable del sistema.

Se recomienda redactar los casos de uso de seguridad de la manera más detallada posible o de manera que contengan, como mínimo, la identificación de la secuencia de las acciones que resultan esenciales en relación con el caso de uso, porque muchos incidentes de seguridad derivan de una definición incompleta del escenario.

Como resultado de este análisis, se tiene que obtener el catálogo de casos de uso de seguridad del servicio de acuerdo con las categorías siguientes:

- Diagrama de casos de uso.
- Diagrama de secuencias de interacción de los casos de uso.
- Diagrama de actividades relativas a los casos de uso.

6.5. Anàlisis de los requisitos de firma o sellado y certificación de los casos de uso de automatización

A continuación exponemos, como caso práctico, el análisis de los requisitos de firma o sellado y certificación de los casos de uso siguientes, presentados en el capítulo 4 anterior.

6.5.1. La expedición automàtica de recibo de registro electrónico

1. ¿Cuál es el significado jurídico de la firma?
   - Descripción del tipo de significado.
     La firma acredita la condición de órgano administrativo de registro y garantiza la validez del recibo acreditativo de la presentación.
   - Indicación de si la firma es mancomunada, solidaria, siguiente dentro de una secuencia o de otro tipo.
     No aplicable.

2. ¿Qué condición personal acredita la firma?
   - Autor u otra condición (en sustitución, por delegación o por otro mecanismo).
     La firma acredita la condición de autor del documento.
   - Actúa en nombre propio o en representación.
     El registro actúa en nombre propio, ejerciendo la competencia propia.

3. ¿Hay que acreditar la fecha de la firma independientemente de la fecha del documento?
   - Sí/No.
     Sí, debido a la relevancia y los efectos externos, especialmente en relación con los plazos administrativos, se considera necesario acreditar la fecha de la firma independientemente de la fecha del documento presentado.

4. ¿La firma se debe producir después de otra firma?
   - Sí/No.
     No aplicable.
   - Orden de las firmas.
     No aplicable.

5. ¿Qué tipos de certificados se necesitan?
   - Persona física.
     - Individuales/ciudadano.
       No aplicable.
     - Profesionales.
       No aplicable.
     - Vinculación a entidad.
       No aplicable.
     - Representación.
       No aplicable.
   - Persona jurídica.
     No aplicable.
   - Entidad sin personalidad jurídica.
     No aplicable.
   - Dispositivo.
     No aplicable.
   - Servidor seguro.
     No aplicable.
   - Sede electrónica.
     No aplicable.
   - Sello electrónico.
     Aplicable, en caso de emisión automática del recibo de registro.
   - Personal al servicio de la Administración.
     Aplicable, en caso de emisión manual del recibo de registro, cosa que ja se anticipa poco conveniente.

6. ¿Qué usos hay que dar a los certificados?	- Autenticación. No aplicable. - Firma digital. Aplicable. - Cifrado. No aplicable.
7. ¿Qué aplicaciones específicas han de soportar los certificados?	- Firma de documentos. Aplicable, ya que el recibo será, típicamente, un documento de presentación, como un PDF. - Correo electrónico S/MIME. No aplicable. - Canal seguro SSL/TLS. No aplicable. - Seguridad de servicios web. Aplicable a la entrega de recibos en comunicaciones interadministrativas. - Firma de código. No aplicable. - Firma de aplicación. No aplicable. - TSA, OCSP, otros. Aplicable, en la medida en que es necesario disponer de sello de fecha y hora, lo que puede implicar la instalación de una entidad de sellado de fecha y hora.
8. ¿Qué estrategias de certificación digital hay que establecer?	- Emisión de certificados con entidad de certificación propia. Aplicable. - Emisión de certificados en colaboración con CATCert (adquisición de certificados). o Para uso propio.

Aplicable.

- o Para dotar a terceras personas o entidades.

  No aplicable.

- Admisión de certificados de otras entidades de certificación.

  No aplicable, porque no hay recepción de recibos de otras administraciones, sino únicamente emisión de recibos propios.

6.5.2. La comprobación automática de datos de solicitud

1. ¿Cuál es el significado jurídico de la firma?
   - Descripción del tipo de significado.

     La firma acredita la condición de órgano administrativo que actúa y garantiza la validez del proceso de comprobación de la solicitud.
   - Indicación de si la firma es mancomunada, solidaria, siguiente dentro de una secuencia o de otro tipo.

     No aplicable.
2. ¿Qué condición personal acredita la firma?
   - Autor u otra condición (en sustitución, por delegación o por otro mecanismo).

     La firma acredita la condición de autor del documento.
   - Actúa en nombre propio o en representación.

     El órgano actúa en nombre propio, ejerciendo la competencia propia o por delegación.
3. ¿Hay que acreditar la fecha de la firma independientemente de la
   - Sí/No.

     No se considera necesario acreditar la fecha de la firma independientemente de la fecha del

	fecha del documento?	documento de comprobaciones.
4.	¿La firma se debe producir después de otra firma?	- Sí/No. No aplicable. - Orden de las firmas. No aplicable.
5.	¿Qué tipos de certificados se necesitan?	- Persona física. o Individuales/ciudadano. No aplicable. o Profesionales. No aplicable. o Vinculación a entidad. No aplicable. o Representación. No aplicable. - Persona jurídica. No aplicable. - Entidad sin personalidad jurídica. No aplicable. - Dispositivo. Aplicable. - Servidor seguro. No aplicable. - Sede electrónica. No aplicable. - Sello electrónico. Aplicable. - Personal al servicio de la Administración. No aplicable.
6.	¿Qué usos hay que dar a los certificados?	- Autenticación. No aplicable. - Firma digital.

Aplicable.

- Cifrado.

  No aplicable.

7. ¿Qué aplicaciones específicas han de soportar los certificados?

- Firma de documentos.

  Aplicable, ya que el documento específico será, típicamente, un documento estructurado.

- Correo electrónico S/MIME.

  No aplicable.

- Canal seguro SSL/TLS.

  No aplicable.

- Seguridad de servicios web.

  Aplicable para la realización de comunicaciones interadministrativas necesarias para obtener datos que permitan llevar a cabo las comprobaciones automáticas.

- Firma de código.

  No aplicable.

- Firma de aplicación.

  No aplicable.

- TSA, OCSP, otros.

  No aplicable.

8. ¿Qué estrategias de certificación digital hay que establecer?

- Emisión de certificados con entidad de certificación propia.

  Aplicable.

- Emisión de certificados en colaboración con CATCert (adquisición de certificados).
  - Para uso propio.

    Aplicable.
  - Para dotar a terceras personas o entidades.

    No aplicable.
- Admisión de certificados de otras entidades de

certificación.

Aplicable, para la verificación de las firmas de comunicaciones interadministrativas necesarias para obtener datos que permitan llevar a cabo las comprobaciones automáticas.

6.5.3. La digitalizació automática de documentos

1.	¿Cuál es el significado jurídico de la firma?	- Descripción del tipo de significado. La firma acredita la condición de órgano administrativo de registro y garantiza la validez del proceso de digitalización. - Indicación de si la firma es mancomunada, solidaria, siguiente dentro de una secuencia o de otro tipo. No aplicable.
2.	¿Qué condición personal acredita la firma?	- Autor u otra condición (en sustitución, por delegación o por otro mecanismo). La firma acredita la condición de autor del documento. - Actúa en nombre propio o en representación. El órgano actúa en nombre propio, ejerciendo la competencia propia.
3.	¿Hay que acreditar la fecha de la firma independientemente de la fecha del documento?	- Sí/No. Se considera necesario acreditar la fecha de la firma independientemente de la fecha del documento digitalizado, ya que hay que garantizar en qué momento se ha creado la copia digital.
4.	¿La firma se debe producir después de otra firma?	- Sí/No. No aplicable. - Orden de las firmas. No aplicable.
5.	¿Qué tipos de certificados se necesitan?	- Persona física. o Individuales/ciudadano. No aplicable.

  - o Profesionales.
    No aplicable.
  - o Vinculación a entidad.
    No aplicable.
  - o Representación.
    No aplicable.
- Persona jurídica.
  No aplicable.
- Entidad sin personalidad jurídica.
  No aplicable.
- Dispositivo.
  No aplicable.
- Servidor seguro.
  No aplicable.
- Seu electrònica.
  No aplicable.
- Sello electrónico.
  Aplicable.
- Personal al servicio de la Administración.
  No aplicable.

6. ¿Qué usos hay que dar a los certificados?
   - Autenticación.
     No aplicable.
   - Firma digital.
     Aplicable.
   - Cifrado.
     No aplicable.

7. ¿Qué aplicaciones específicas han de soportar los certificados?
   - Firma de documentos.
     Aplicable.
   - Correo electrónico S/MIME.
     No aplicable.
   - Canal seguro SSL/TLS.
     No aplicable.

	- Seguridad de servicios web. No aplicable. - Firma de código. No aplicable. - Firma de aplicación. No aplicable. - TSA, OCSP, otros. No aplicable.
8. ¿Qué estrategias de certificación digital hay que establecer?	- Emisión de certificados con entidad de certificación propia. Aplicable. - Emisión de certificados en colaboración con CATCert (adquisición de certificados). o Para uso propio. Aplicable. o Para dotar a terceras personas o entidades. Aplicable a la dotación de certificados propios a entidades contratadas para el proceso de digitalización. - Admisión de certificados de otras entidades de certificación. Aplicable a las copias digitalizadas por otras Administraciones Públicas.

6.5.4. El impulso automático del procedimiento

1. ¿Cuál es el significado jurídico de la firma?	- Descripción del tipo de significado. La firma acredita la condición de órgano administrativo que actúa y garantiza la validez del acto de impulso.

	- Indicación de si la firma es mancomunada, solidaria, siguiente dentro de una secuencia o de otro tipo. No aplicable.
2. ¿Qué condición personal acredita la firma?	- Autor u otra condición (en sustitución, por delegación o por otro mecanismo). La firma acredita la condición de autor del documento. - Actúa en nombre propio o en representación. El órgano actúa en nombre propio, ejerciendo la competencia propia o por delegación.
3. ¿Hay que acreditar la fecha de la firma independientemente de la fecha del documento?	- Sí/No. No se considera necesario acreditar la fecha de la firma independientemente de la fecha del documento correspondiente.
4. ¿La firma se debe producir después de otra firma?	- Sí/No. No aplicable. - Orden de las firmas. No aplicable.
5. ¿Qué tipos de certificados se necesitan?	- Persona física. o Individuales/ciudadano. No aplicable. o Profesionales. No aplicable. o Vinculación a entidad. No aplicable. o Representación. No aplicable. - Persona jurídica. No aplicable.

- Entidad sin personalidad jurídica.
  No aplicable.
- Dispositivo.
  No aplicable.
- Servidor seguro.
  No aplicable.
- Sede electrónica.
  No aplicable.
- Sello electrónico.
  Aplicable.
- Personal al servicio de la Administración.
  No aplicable.

6. ¿Qué usos hay que dar a los certificados?
   - Autenticación.
     No aplicable.
   - Firma digital.
     Aplicable.
   - Cifrado.
     No aplicable.

7. ¿Qué aplicaciones específicas han de soportar los certificados?
   - Firma de documentos.
     Aplicable, ya que el documento específico será, típicamente, un documento estructurado.
   - Correo electrónico S/MIME.
     Aplicable cuando el acto de impulso implica una comunicación por correo electrónico seguro.
   - Canal seguro SSL/TLS.
     No aplicable.
   - Seguridad de servicios web.
     Aplicable cuando el acto de impulso implica la realización de comunicaciones interadministrativas necesarias para obtener datos.
   - Firma de código.

No aplicable.

- Firma de aplicación.

  No aplicable.

- TSA, OCSP, otros.

  No aplicable.

8. ¿Qué estrategias de certificación digital hay que establecer?

- Emisión de certificados con entidad de certificación propia.

  Aplicable.

- Emisión de certificados en colaboración con CATCert (adquisición de certificados).
  - Para uso propio.

    Aplicable.
  - Para dotar a terceras personas o entidades.

    No aplicable.
- Admisión de certificados de otras entidades de certificación.

  Aplicable, para la verificación de las firmas de comunicaciones interadministrativas necesarias para obtener datos en algunos actos de impulso.

6.5.5. El acto automático de constancia electrónica

1. ¿Cuál es el significado jurídico de la firma?

- Descripción del tipo de significado.

  La firma acredita la condición de órgano administrativo que actúa y garantiza la validez del documento.

- Indicación de si la firma es mancomunada, solidaria, siguiente dentro de una secuencia o de otro tipo.

  No aplicable.

2. ¿Qué condición personal acredita la firma?
   - Autor u otra condición (en sustitución, por delegación o por otro mecanismo).
     La firma acredita la condición de autor del documento.
   - Actúa en nombre propio o en representación.
     El órgano actúa en nombre propio, ejerciendo la competencia propia.

3. ¿Hay que acreditar la fecha de la firma independientemente de la fecha del documento?
   - Sí/No.
     Sí, debido a la relevancia y los efectos externos del documento, especialmente en el caso de los certificados.

4. ¿La firma se debe producir después de otra firma?
   - Sí/No.
     Depende.
   - Orden de las firmas.
     La normativa sectorial determina, en algunos casos de expedición de certificados, la necesidad de que firmen varias personas (como en el caso de los certificados de los acuerdos de los órganos colegiados, en que firma el secretario del órgano con el visto bueno del presidente). Hay que considerar las implicaciones de este flujo de firma en caso de automatización del trámite, ya que en principio se utilizará el sello del órgano.

5. ¿Qué tipos de certificados se necesitan?
   - Persona física.
     - Individuales/ciudadano.
       No aplicable.
     - Profesionales.
       No aplicable.
     - Vinculación a entidad.

No aplicable.

- o Representación.

  No aplicable.

- Persona jurídica.

  No aplicable.

- Entidad sin personalidad jurídica.

  No aplicable.

- Dispositivo.

  No aplicable.

- Servidor seguro.

  No aplicable.

- Sede electrónica.

  No aplicable.

- Sello electrónico.

  Aplicable.

- Personal al servicio de la Administración.

  No aplicable.

6. ¿Qué usos hay que dar a los certificados?

- Autenticación.

  No aplicable.

- Firma digital.

  Aplicable.

- Cifrado.

  No aplicable.

7. ¿Qué aplicaciones específicas han de soportar los certificados?

- Firma de documentos.

  Aplicable, ya que el documento correspondiente al acto de constancia será, típicamente, un documento de presentación, como un PDF.

- Correo electrónico S/MIME.

  No aplicable.

- Canal seguro SSL/TLS.

  No aplicable.

- Seguridad de servicios web.

Podría ser aplicable a los actos automáticos de constancia integrados en comunicaciones interadministrativas.

- Firma de código.
  No aplicable.
- Firma de aplicación.
  No aplicable.
- TSA, OCSP, otros.
  Aplicable, en la medida en que es necesario disponer de sello de fecha y hora, lo que puede implicar la instalación de una entidad de sellado de fecha y hora.

8. ¿Qué estrategias de certificación digital hay que establecer?

- Emisión de certificados con entidad de certificación propia.
  Aplicable.
- Emisión de certificados en colaboración con CATCert (adquisición de certificados).
  - Para uso propio.
    Aplicable.
  - Para dotar a terceras personas o entidades.
    No aplicable.
- Admisión de certificados de otras entidades de certificación.
  Aplicable en caso de recepción de documentos de constancia emitidos por otras Administraciones.

6.5.6. La expedición automática de copia auténtica electrónica

1. ¿Cuál es el significado jurídico de la firma?	- Descripción del tipo de significado. La firma acredita la condición de órgano administrativo que actúa y garantiza la validez del documento. - Indicación de si la firma es mancomunada, solidaria, siguiente dentro de una secuencia o de otro tipo. No aplicable.
2. ¿Qué condición personal acredita la firma?	- Autor u otra condición (en sustitución, por delegación o por otro mecanismo). La firma acredita la condición de autor del documento. - Actúa en nombre propio o en representación. El órgano actúa en nombre propio, ejerciendo la competencia propia.
3. ¿Hay que acreditar la fecha de la firma independientemente de la fecha del documento?	- Sí/No. Sí, debido a la relevancia y los efectos externos del documento.
4. ¿La firma se debe producir después de otra firma?	- Sí/No. Depende. - Orden de las firmas. La normativa sectorial determina, en algunos casos de expedición de copia auténtica, la necesidad de que firmen varias personas, especialmente cuando la copia goza de fe pública. Hay que considerar las implicaciones de este flujo de firma en caso de automatización del

trámite, ya que en principio se utilizará el sello del órgano.

5. ¿Qué tipos de certificados se necesitan?
   - Persona física.
     - Individuales/ciudadano.
       No aplicable.
     - Profesionales.
       No aplicable.
     - Vinculación a entidad.
       No aplicable.
     - Representación.
       No aplicable.
   - Persona jurídica.
     No aplicable.
   - Entidad sin personalidad jurídica.
     No aplicable.
   - Dispositivo.
     No aplicable.
   - Servidor seguro.
     No aplicable.
   - Sede electrónica.
     No aplicable.
   - Sello electrónico.
     Aplicable.
   - Personal al servicio de la Administración.
     No aplicable.

6. ¿Qué usos hay que dar a los certificados?
   - Autenticación.
     No aplicable.
   - Firma digital.
     Aplicable.
   - Cifrado.
     No aplicable.

7. ¿Qué aplicaciones específicas han de soportar los certificados?

- Firma de documentos.
  Aplicable, ya que el documento correspondiente a la copia auténtica será, típicamente, un documento de presentación, como un PDF.
- Correo electrónico S/MIME.
  No aplicable.
- Canal segur SSL/TLS.
  No aplicable.
- Seguridad de servicios web.
  Podría ser aplicable a los actos automáticos de expedición de copia auténtica integrados en comunicaciones interadministrativas.
- Firma de código.
  No aplicable.
- Firma de aplicación.
  No aplicable.
- TSA, OCSP, otros.
  Aplicable, en la medida en que es necesario disponer de sello de fecha y hora, lo que puede implicar la instalación de una entidad de sellado de fecha y hora.

8. ¿Qué estrategias de certificación digital hay que establecer?

- Emisión de certificados con entidad de certificación propia.
  Aplicable.
- Emisión de certificados en colaboración con CATCert (adquisición de certificados).
  - Para uso propio.
    Aplicable.
  - Para dotar a terceras personas o entidades.
    No aplicable.
- Admisión de certificados de otras entidades de certificación.

Aplicable en caso de recepción de copias auténticas emitidas por otras Administraciones.

6.5.7. La apertura y el cierre automático de libros electrónicos

1. ¿Cuál es el significado jurídico de la firma?	- Descripción del tipo de significado. La firma acredita la condición de órgano administrativo que actúa y garantiza la validez del libro. - Indicación de si la firma es mancomunada, solidaria, siguiente dentro de una secuencia o de otro tipo. No aplicable.
2. ¿Qué condición personal acredita la firma?	- Autor u otra condición (en sustitución, por delegación o por otro mecanismo). La firma acredita la condición de autor del acto de apertura y cierre del libro. - Actúa en nombre propio o en representación. El órgano actúa en nombre propio, ejerciendo la competencia propia.
3. ¿Hay que acreditar la fecha de la firma independientemente de la fecha del documento?	- Sí/No. No.
4. ¿La firma se debe producir después de otra firma?	- Sí/No. No. - Orden de las firmas. No aplicable.

5. ¿Qué tipos de certificados se necesitan?
   - Persona física.
     - Individuales/ciudadano.
       No aplicable.
     - Profesionales.
       No aplicable.
     - Vinculación a entidad.
       No aplicable.
     - Representación.
       No aplicable.
   - Persona jurídica.
     No aplicable.
   - Entidad sin personalidad jurídica.
     No aplicable.
   - Dispositivo.
     No aplicable.
   - Servidor seguro.
     No aplicable.
   - Sede electrónica.
     No aplicable.
   - Sello electrónico.
     Aplicable.
   - Personal al servicio de la Administración.
     No aplicable.

6. ¿Qué usos hay que dar a los certificados?
   - Autenticación.
     No aplicable.
   - Firma digital.
     Aplicable.
   - Cifrado.
     No aplicable.

7. ¿Qué aplicaciones específicas han de soportar los certificados?
   - Firma de documentos.
     No aplicable.
   - Correo electrónico S/MIME.

No aplicable.

- Canal seguro SSL/TLS.
  No aplicable.
- Seguridad de servicios web.
  No aplicable.
- Firma de código.
  No aplicable.
- Firma de aplicación.
  No aplicable.
- TSA, OCSP, otros.
  No aplicable.

8. ¿Qué estrategias de certificación digital hay que establecer?

- Emisión de certificados con entidad de certificación propia.
  Aplicable.
- Emisión de certificados en colaboración con CATCert (adquisición de certificados).
  - Para uso propio.
    Aplicable.
  - Para dotar a terceras personas o entidades.
    No aplicable.
- Admisión de certificados de otras entidades de certificación.
  Aplicable en caso de recepción de libros diligenciados o legalizados por otras Administracions Públicas.

6.5.8. La foliación automática de expedientes

1. ¿Cuál es el significado jurídico de la firma?

- Descripción del tipo de significado.
  La firma acredita la condición de órgano

		administrativo que actúa y garantiza la validez del documento. - Indicación de si la firma es mancomunada, solidaria, siguiente dentro de una secuencia o de otro tipo. No aplicable.
2.	¿Qué condición personal acredita la firma?	- Autor u otra condición (en sustitución, por delegación o por otro mecanismo). La firma acredita la condición de autor del documento. - Actúa en nombre propio o en representación. El órgano actúa en nombre propio, ejerciendo la competencia propia.
3.	¿Hay que acreditar la fecha de la firma independientemente de la fecha del documento?	- Sí/No. No.
4.	¿La firma se debe producir después de otra firma?	- Sí/No. No. - Orden de las firmas. No aplicable.
5.	¿Qué tipos de certificados se necesitan?	- Persona física. o Individuales/ciudadano. No aplicable. o Profesionales. No aplicable. o Vinculación a entidad. No aplicable. o Representación. No aplicable.

	- Persona jurídica. No aplicable. - Entidad sin personalidad jurídica. No aplicable. - Dispositivo. No aplicable. - Servidor seguro. No aplicable. - Sede electrónica. No aplicable. - Sello electrónico. Aplicable. - Personal al servicio de la Administración. No aplicable.
6. ¿Qué usos hay que dar a los certificados?	- Autenticación. No aplicable. - Firma digital. Aplicable. - Cifrado. No aplicable.
7. ¿Qué aplicaciones específicas han de soportar los certificados?	- Firma de documentos. Aplicable, ya que el documento correspondiente al acto de constancia será, típicamente, un documento estructurado, com un XML. - Correo electrónico S/MIME. No aplicable. - Canal seguro SSL/TLS. No aplicable. - Seguridad de servicios web. No aplicable. - Firma de código. No aplicable.

- Firma de aplicación.
  No aplicable.
- TSA, OCSP, otros.
  No aplicable.

8. ¿Qué estrategias de certificación digital hay que establecer?
   - Emisión de certificados con entidad de certificación propia.
     Aplicable.
   - Emisión de certificados en colaboración con CATCert (adquisición de certificados).
     - Para uso propio.
       Aplicable.
     - Para dotar a terceras personas o entidades.
       No aplicable.
   - Admisión de certificados de otras entidades de certificación.
     Aplicable en caso de recepción de expedientes indizados por otras Administraciones Públicas.

6.5.9. La migración automática de documento electrónico

1. ¿Cuál es el significado jurídico de la firma?
   - Descripción del tipo de significado.
     La firma acredita la condición de órgano administrativo que actúa y garantiza la validez del documento.
   - Indicación de si la firma es mancomunada, solidaria, siguiente dentro de una secuencia o de otro tipo.
     No aplicable.

2. ¿Qué condición personal
   - Autor u otra condición (en sustitución, por

	acredita la firma?	delegación o por otro mecanismo). La firma acredita la condición de autor del documento. - Actúa en nombre propio o en representación. El órgano actúa en nombre propio, ejerciendo la competencia propia.
3.	¿Hay que acreditar la fecha de la firma independientemente de la fecha del documento?	- Sí/No. Sí, debido a la relevancia y los efectos externos del documento.
4.	¿La firma se debe producir después de otra firma?	- Sí/No. No. - Orden de las firmas. No aplicable.
5.	¿Qué tipos de certificados se necesitan?	- Persona física. o Individuales/ciudadano. No aplicable. o Profesionales. No aplicable. o Vinculación a entidad. No aplicable. o Representación. No aplicable. - Persona jurídica. No aplicable. - Entidad sin personalidad jurídica. No aplicable. - Dispositivo. No aplicable. - Servidor seguro. No aplicable.

	- Sede electrónica. No aplicable. - Sello electrónico. Aplicable. - Personal al servicio de la Administración. No aplicable.
6. ¿Qué usos hay que dar a los certificados?	- Autenticación. No aplicable. - Firma digital. Aplicable. - Cifrado. No aplicable.
7. ¿Qué aplicaciones específicas han de soportar los certificados?	- Firma de documentos. Aplicable, ya que el documento correspondiente a la copia auténtica será, típicamente, un documento ofimático o de presentación, com un PDF. - Correo electrónico S/MIME. No aplicable. - Canal seguro SSL/TLS. No aplicable. - Seguridad de servicios web. No aplicable. - Firma de código. No aplicable. - Firma de aplicación. No aplicable. - TSA, OCSP, otros. Aplicable, en la medida en que es necesario disponer de sello de fecha y hora, lo que puede implicar la instalación de una entidad de sellado de fecha y hora.

8. ¿Qué estrategias de certificación digital hay que establecer?
   - Emisión de certificados con entidad de certificación propia.
     Aplicable.
   - Emisión de certificados en colaboración con CATCert (adquisición de certificados).
     - Para uso propio.
       Aplicable.
     - Para dotar a terceras personas o entidades.
       No aplicable.
   - Admisión de certificados de otras entidades de certificación.
     Aplicable en caso de recepción de copias auténticas emitidas por otras Administraciones.

6.5.10. Los intercambios automáticos de datos entre administraciones públicas

1. ¿Cuál es el significado jurídico de la firma?
   - Descripción del tipo de significado.
     La firma acredita la condición de órgano administrativo que actúa y garantiza la validez del documento.
   - Indicación de si la firma es mancomunada, solidaria, siguiente dentro de una secuencia o de otro tipo.
     No aplicable.

2. ¿Qué condición personal acredita la firma?
   - Autor u otra condición (en sustitución, por delegación o por otro mecanismo).
     La firma acredita la condición de autor del documento.
   - Actúa en nombre propio o en representación.

El órgano actúa en nombre propio, ejerciendo la competencia propia.

3. ¿Hay que acreditar la fecha de la firma independientemente de la fecha del documento?
   - Sí/No.
     Sí, debido a la relevancia y los efectos externos del documento.

4. ¿La firma se debe producir después de otra firma?
   - Sí/No.
     No.
   - Orden de las firmas.
     No aplicable.

5. ¿Qué tipos de certificados se necesitan?
   - Persona física.
     - Individuales/ciudadano.
       No aplicable.
     - Profesionales.
       No aplicable.
     - Vinculación a entidad.
       No aplicable.
     - Representación.
       No aplicable.
   - Persona jurídica.
     No aplicable.
   - Entidad sin personalidad jurídica.
     No aplicable.
   - Dispositivo.
     Aplicable en sistemas cerrados de comunicación, si lo prevé así el convenio previsto en el artículo 20 de la Ley 11/2007.
   - Servidor seguro.
     Aplicable en sistemas cerrados de comunicación, si lo prevé así el convenio previsto en el artículo 20 de la Ley 11/2007.

	- Sede electrónica. No aplicable. - Sello electrónico. Aplicable. - Personal al servicio de la Administración. No aplicable.
6. ¿Qué usos hay que dar a los certificados?	- Autenticación. No aplicable. - Firma digital. Aplicable. - Cifrado. No aplicable.
7. ¿Qué aplicaciones específicas han de soportar los certificados?	- Firma de documentos. Aplicable, ya que el documento correspondiente a la transmisión de datos podrá ser un documento de presentación, como un PDF. - Correo electrónico S/MIME. No aplicable. - Canal seguro SSL/TLS. No aplicable. - Seguridad de servicios web. Aplicable, ya que la transmisión de datos se realizará típicamente mediante servicios web automáticos. - Firma de código. No aplicable. - Firma de aplicación. No aplicable. - TSA, OCSP, otros. Aplicable, en la medida en que es necesario disponer de sello de fecha y hora, lo que puede implicar la instalación de una entidad de sellado

de fecha y hora.

8. ¿Qué estrategias de certificación digital hay que establecer?
   - Emisión de certificados con entidad de certificación propia.
     Aplicable.
   - Emisión de certificados en colaboración con CATCert (adquisición de certificados).
     - Para uso propio.
       Aplicable.
     - Para dotar a terceras personas o entidades.
       No aplicable.
   - Admisión de certificados de otras entidades de certificación.
     Aplicable a la recepción de transmisiones de datos originadas por otras Administracions Públicas.

6.5.11. La remisión automática de comunicación electrónica al ciudadano

1. ¿Cuál es el significado jurídico de la firma?
   - Descripción del tipo de significado.
     La firma acredita la condición de órgano administrativo que actúa y garantiza la validez del documento.
   - Indicación de si la firma es mancomunada, solidaria, siguiente dentro de una secuencia o de otro tipo.
     No aplicable.

2. ¿Qué condición personal acredita la firma?
   - Autor u otra condición (en sustitución, por delegación o por otro mecanismo).
     La firma acredita la condición de autor del documento.

- Actúa en nombre propio o en representación.
  El órgano actúa en nombre propio, ejerciendo la competencia propia.

3. ¿Hay que acreditar la fecha de la firma independientemente de la fecha del documento?
   - Sí/No.
     Sí, debido a la relevancia y los efectos externos del documento.
4. ¿La firma se debe producir después de otra firma?
   - Sí/No.
     No.
   - Orden de las firmas.
     No aplicable.

5. ¿Qué tipos de certificados se necesitan?
   - Persona física.
     - Individuales/ciudadano.
       No aplicable.
     - Profesionales.
       No aplicable.
     - Vinculación a entidad.
       No aplicable.
     - Representación.
       No aplicable.
   - Persona jurídica.
     No aplicable.
   - Entidad sin personalidad jurídica.
     No aplicable.
   - Dispositivo.
     No aplicable.
   - Servidor seguro.
     No aplicable.
   - Sede electrónica.
     No aplicable.
   - Sello electrónico.
     Aplicable.

	- Personal al servicio de la Administración. No aplicable.
6. ¿Qué usos hay que dar a los certificados?	- Autenticación. No aplicable. - Firma digital. Aplicable. - Cifrado. No aplicable.
7. ¿Qué aplicaciones específicas han de soportar los certificados?	- Firma de documentos. Aplicable, ya que el documento correspondiente a la comunicación será, típicamente, un documento de presentación, como un PDF. - Correo electrónico S/MIME. Aplicable a comunicaciones sin valor legal realizadas por correo electrónico. - Canal seguro SSL/TLS. No aplicable. - Seguridad de servicios web. No aplicable. - Firma de código. No aplicable. - Firma de aplicación. No aplicable. - TSA, OCSP, otros. Aplicable, en la medida en que es necesario disponer de sello de fecha y hora, lo que puede implicar la instalación de una entidad de sellado de fecha y hora.
8. ¿Qué estrategias de certificación digital hay que establecer?	- Emisión de certificados con entidad de certificación propia. Aplicable.

- Emisión de certificados en colaboración con CATCert (adquisición de certificados).
    - Para uso propio.
      Aplicable.
    - Para dotar a terceras personas o entidades.
      No aplicable.
- Admisión de certificados de otras entidades de certificación.
  Aplicable en caso de recibir acuses de recibo producidos por los sistemas de entrega de comunicaciones electrónicas.

7. Los requisitos de seguridad de la aplicación de actuación administrativa automatizada

En esta sección se tratan los requisitos de seguridad de la aplicación de actuación administrativa automatizada, sobre todo teniendo en cuenta las necesidades de protección de una clave privada de sello de acto automatizado.

7.1. Las aplicaciones informáticas de firma electrónica y los activos a proteger

En este primer apartado presentamos los activos utilizados por las aplicaciones informáticas de firma electrónica. También tratamos la problemática de seguridad, que motiva la necesidad de utilizar dispositivos seguros de firma electrónica dentro del marco de la Directiva y la Ley de firma electrónica, y de acuerdo con los estándares técnicos internacionales.

Presentaremos, pues:

- Los dispositivos, en sentido amplio, de uso de la firma electrónica.
- Los algoritmos criptográficos relacionados con la firma electrónica.
- Los datos informáticos relacionados con la firma electrónica.

7.1.1. Los dispositivos para el uso de la firma electrónica

7.1.1.1. El dispositivo de creación de firma electrónica

Un dispositivo de creación de firma electrónica es un programa o un sistema informático (un producto) que sirve para aplicar los datos de creación de firma (de conformidad con el artículo 24.2 de la Ley 59/2003, de 19 de diciembre, de firma electrónica).

Esta definición conecta la creación de la firma electrónica con la aplicación (el uso) de los datos de creación de firma, de manera que el poseedor del dispositivo es la persona que puede crear la firma, sea o no el suscriptor del certificado.

Por este motivo, la firma será imputable al suscriptor en la medida en que una persona no autorizada no pueda aplicar los datos de creación de firma. Eso justifica la necesidad de disponer de los datos de activación de la firma electrónica para poder hacer esta imputación.

Por otra parte, no forma parte de este dispositivo la aplicación de creación de firma, que, de hecho, utiliza este dispositivo de creación en condiciones de seguridad. Así, esta aplicación puede ser independiente y única o bien un conjunto de aplicaciones, incluso distribuidas, las cuales, además, pueden utilizar protocolos e interfaces de programación de servicios de seguridad de terceros, siempre bajo su responsabilidad.

7.1.1.2. El dispositivo de verificación de firma

Un dispositivo de verificación de firma electrónica es, de acuerdo con el artículo 25.2 de la Ley 59/2003, un programa o un sistema informático que sirve para aplicar los datos de verificación de firma.

Según esta concepción, cualquier poseedor de la clave pública de una persona la puede "aplicar" para comprobar la validez de la firma electrónica. Por lo tanto, el legislador se olvida de otros elementos que tendrá que aplicar esta persona para poder completar el proceso de verificación, como la construcción de una ruta de certificación hasta una raíz fiable, para comprobar la validez del certificado que contiene la clave pública, o la verificación de todos los certificados de la ruta.

Los dispositivos de verificación de firma tienen que garantizar que el procedimiento de verificación cumple una serie de requisitos generales siempre que eso sea posible técnicamente, un concepto jurídico indeterminado que hay que resolver con las normas técnicas nacionales e internacionales aplicables, o, faltando éstas, con las especificaciones técnicas voluntarias, como CEN CWA 14171, sobre procedimientos de verificación de firma electrónica.

Desde la perspectiva de la comprobación de los requisitos expuestos anteriormente, los fabricantes o los importadores pueden utilizar el mecanismo de la certificación de productos de firma electrónica del artículo 27 de la Ley 59/2003.

7.1.2. Los algoritmos criptográficos

Los algoritmos que tienen como finalidad el tratamiento del secreto de la información se llaman criptográficos y son esenciales para la firma electrónica avanzada, dado que soportan el uso de cifras seguras para la producción y la comprobación de la firma electrónica.

Un algoritmo es una función matemática ejecutada por un producto informático, formado habitualmente por un hardware y un software.

En consecuencia, los algoritmos criptográficos residen en el corazón de la firma electrónica (avanzada y reconocida, pero no necesariamente en el caso de la firma ordinaria).

7.1.2.1. Los algoritmos de resumen

El algoritmo de resumen permite obtener una versión reducida de un documento que hay que firmar. Esta versión resumida se puede enviar junto con el documento con el fin de garantizar que el documento no ha sido manipulado (propiedad que se denomina *integridad documental electrónica*).

Este sistema se aplica, en relación con la firma electrónica avanzada, porque las operaciones ejecutadas con algoritmos de firma son muy lentas y, adicionalmente, incrementan de manera considerable el volumen del documento firmado. Para evitar estos inconvenientes, lo que realmente se firma es este resumen, y no el documento entero.

Hay también un gran número de aplicaciones que requieren la integridad documental, pero no la firma electrónica, y, por lo tanto, también utilizan estos algoritmos de resumen.

El algoritmo de resumen tiene que garantizar una serie de condiciones:

- Debe ser irreversible, es decir, no se tiene que poder obtener el documento original a partir del resumen.

- Debe ser único para cada documento e infalsificable, es decir, no tienen que existir dos o más resúmenes iguales para documentos diferentes ni dos resúmenes diferentes para el mismo documento.

Los dos algoritmos de resumen que se utilizan habitualmente son MD5 y SHA-1, aunque ya se han propuesto sustitutos como RIPEMD-160 y SHA-224. En concreto, MD5 ya ha sido declarado obsoleto para bastantes aplicaciones, incluyendo la generación de resúmenes para firmas electrónicas.

7.1.2.2. Los algoritmos de firma electrónica

El algoritmo de firma electrónica se basa en una cifra asimétrica – es decir, formada por una clave privada y una clave pública – que permite "firmar" documentos con la clave privada y verificar la firma con la clave pública.

Criptográficament, *firmar* es generar un dato matemático asociado al documento electrónico, de la misma manera que, en el mundo físico, *firmar* es producir un grafismo fijado al soporte material que contiene el documento.

Esta firma ofrece también la propiedad denominada *integridad documental electrónica*, que permite determinar que un documento no ha sido manipulado, así como la propiedad denominada autenticación, que permite comprobar qué entidad ha originado el documento.

La cifra utilizada por el algoritmo de firma se llama legalmente *dato de firma electrónica*. Concretamente, la clave privada de firma se llama *dato de creación de firma electrónica*, mientras que la clave pública de firma recibe el nombre de *dato de verificación de firma electrónica*.

El algoritmo de firma debe garantizar una serie de condiciones:

- Debe ser irreversible en un sentido doble: en primer lugar, no se tiene que poder obtener la clave privada a partir de la clave pública; en segundo lugar, no se tiene que poder obtener la clave privada a partir de la firma.

- Debe ser única para cada documento e infalsificable, es decir, no se tiene que poder obtener una firma idéntica a la del documento original a partir de una manipulación del documento original.

Los dos algoritmos de firma electrónica que se utilizan habitualmente son RSA y DSA.

Además, para obtener la clave pública hace falta que esta clave haya sido certificada por un prestador de servicios de certificación en quien se confíe.

Cuando el certificado ha sido emitido de acuerdo con los requisitos de la Ley 59/2003, de firma electrónica, y la firma ha sido producida utilizando un dispositivo seguro de creación de firma electrónica, entonces la firma permite hacer la imputación legal del documento electrónico al firmante identificado en el certificado. Esta propiedad se llama, con cierta incorrección, *no repudio de origen* o no *rechazo de origen*, términos que hay que sustituir por *irrefutabilidad de origen*.

La suma de todos estos factores se resume con el concepto de *autenticidad documental electrónica*, un elemento esencial de los servicios de evidencia electrónica.

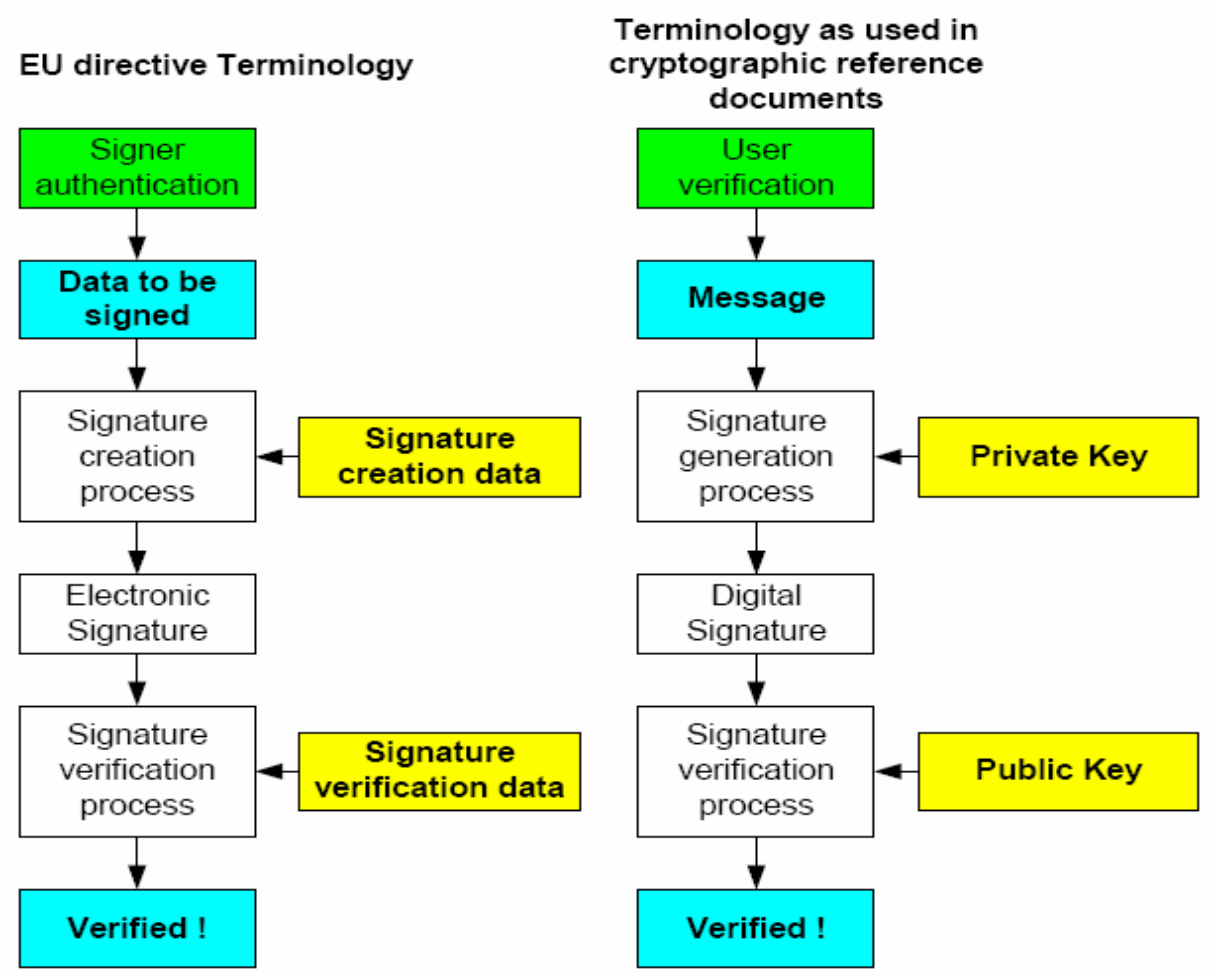
7.1.3. Los datos informáticos relacionados con la firma electrónica

En este apartado presentamos los conceptos legales relativos a los datos que hay que utilizar en los procesos de generación y verificación de firma.

Hay que advertir que una de las dificultades con que topamos a la hora de trabajar con los documentos legales es la terminología que utilizan, muy diferente de la de los documentos de cariz más técnico. Por ejemplo, mientras que legalmente se habla de la *autenticación del firmante*, desde una perspectiva más técnica se habla de la *verificación del usuario*. De manera parecida, mientras que legalmente se habla del documento o mensaje a firmar, técnicamente hay que hablar de datos a firmar, que es un conjunto de datos que incluye el documento, pero también otras informaciones necesarias para la firma electrónica.

Lo mismo sucede con el concepto legal de *firma electrónica avanzada (o reconocida)*, que se corresponde con el concepto técnico de *firma digital*, de manera tal que una firma digital es una firma electrónica avanzada, pero también hay firmas electrónicas que no son firmas digitales.

El esquema siguiente[64] muestra las diferencias terminológicas principales:



[64] CEN CWA 14890-1.

7.1.3.1. Los datos de creación y verificación de la firma electrónica

Los datos de creación de firma electrónica son, de acuerdo con el artículo 24.1 de la Ley 59/2003, de 19 de diciembre, de firma electrónica, los datos únicos, como códigos o claves criptográficas privadas, que el firmante utiliza para crear la firma electrónica.

Los datos de creación de firma se deben poder proteger contra la utilización indebida por parte de terceros, y a menudo se generan dentro de un dispositivo seguro de creación de firma del cual no se pueden extraer nunca. Tampoco pueden ser copiadas en ningún otro lugar.

Por su parte, los datos de verificación de firma electrónica son, de conformidad con el artículo 25.1, los datos – no se dice que deban ser únicos, pero debemos entender la norma en este sentido – como códigos o claves criptográficas públicas, que utilizan los terceros destinatarios de comunicaciones y documentos firmados para verificar la firma electrónica.

La referencia a códigos o claves criptográficas – privadas y públicas – se hace para preservar la supuesta neutralidad tecnológica de la ley, aunque podemos decir que, en este punto, la normativa prevé claramente el caso de las cifras criptográficas asimétricas y los algoritmos de firma correspondientes.

Estas claves criptográficas son los elementos numéricos que forman una cifra criptográfica. Funcionan conjuntamente con los algoritmos criptográficos para generar firmas electrónicas y formas de autenticación o bien para hacer confidencial un documento.

Por este motivo, las claves son los elementos más importantes y críticos de los sistemas de seguridad en general y de los sistemas de firma en particular: conocer la clave de una persona implica adquirir la capacidad de identificarse o firmar en nombre suyo, como también poder acceder a datos secretos.

Como hemos visto, las claves criptográficas tienen la consideración legal de datos de creación y de verificación de firma electrónica, de acuerdo con los artículos 24.1 y 25.1 de la Ley 59/2003, de 19 de diciembre, de firma electrónica.

Consiguientemente, el conjunto más importante de medidas de seguridad en materia de firma electrónica tiene que ver con la generación, la protección y la gestión correctas de las claves privadas, tanto cuando corresponden a cifras simétricas como cuando corresponden a cifras asimétricas.

De manera coherente con esta necesidad, la regulación más importante en materia de los dispositivos que se consideran seguros para producir firmas electrónicas gira en torno a la gestión de las claves de los usuarios.

Una clave criptográfica de usuario es un dato numérico que forma parte de una cifra y que tiene que ser absolutamente secreto, porque sirve para autenticarse, firmar o acceder a datos confidenciales.

En las cifras simétricas, como las que se utilizan para generar la firma electrónica ordinaria, sólo existe una clave, que conocen tanto el firmante como el tercero que recibe el documento firmado. En este caso, las dos partes tienen que proteger el secreto de la clave.

En las cifras asimétricas, como las que se utilizan para generar la firma electrónica adelantada o reconocida, existen dos claves, de las cuales una es privada y la otra pública. Las personas que firman lo hacen con la clave privada, mientras que los terceros que reciben documentos firmados los verifican con la clave pública, que no hace falta que sea secreta.

De hecho, la idea es que la clave sea el máximo de pública posible, motivo por el cual se certifica la clave, en asociación con su titular, que posee la clave privada, para que se pueda entregar esta clave pública certificada a través de la red Internet y que llegue a cualquier potencial destinatario de documentos firmados.

Naturalmente, estas claves están correlacionadas mediante un vínculo matemático que permite utilizar una clave para hacer una acción (firmar, por ejemplo) y la otra

clave para deshacerla (por lo tanto, verificando la firma). Como también es evidente, sin este vínculo, propio de las cifras asimétricas, el sistema no funcionaría.

El vínculo, sin embargo, tiene que permitir garantizar la seguridad del sistema, de manera que el conocimiento de la clave pública no represente una amenaza para la clave privada (propiedad a menudo denominada *irreversibilidad*).

Concretamente, el artículo 24.3 de la Ley 59/2003 determina que las claves criptográficas producidas o utilizadas por los dispositivos seguros de creación de firma electrónica tienen que garantizar, de forma razonablemente segura, que no se podrá obtener la clave privada a partir de la clave pública.

Asimismo, las claves criptográficas han de tener una cierta longitud a fin de que sean seguras. Esta longitud, que es una propiedad de la clave, consiste en el límite superior del espacio numérico de la cifra, y, por lo tanto, determina el número de combinaciones que tendría que probar un atacante que quisiera adivinar la clave privada.

La longitud de la clave criptográfica se expresa en bits. Actualmente se considera que una clave privada de firma electrónica de usuario de 1.024 bits ya es absolutamente segura, mientras que la clave privada de un prestador de servicios de certificación normalmente tiene una longitud de 2.048 bits.

Vista su importancia, el titular de la clave criptográfica privada debe proteger esta clave convenientemente mediante un producto de firma electrónica que se considere *seguro*.

La misma definición de la firma electrónica adelantada hace referencia a la protección de la clave cuando indica que ésta ha sido creada por medios que el firmante puede mantener bajo su control exclusivo (artículo 3.2 de la Ley 59/2003), uno de los aspectos más controvertidos y complejos del sistema de firma electrónica.

También se refiere explícitamente el artículo 24.3 de la misma Ley, que establece que el dispositivo seguro de creación de firma debe permitir al firmante proteger los datos

de creación de firma electrónica de una manera fiable para evitar que sean utilizados por terceros no autorizados debidamente.

7.1.3.2. Los datos de activación de la firma electrónica

Los datos de activación de la creación de la firma electrónica son los datos que se utilizan para iniciar un proceso de creación de firma electrónica.

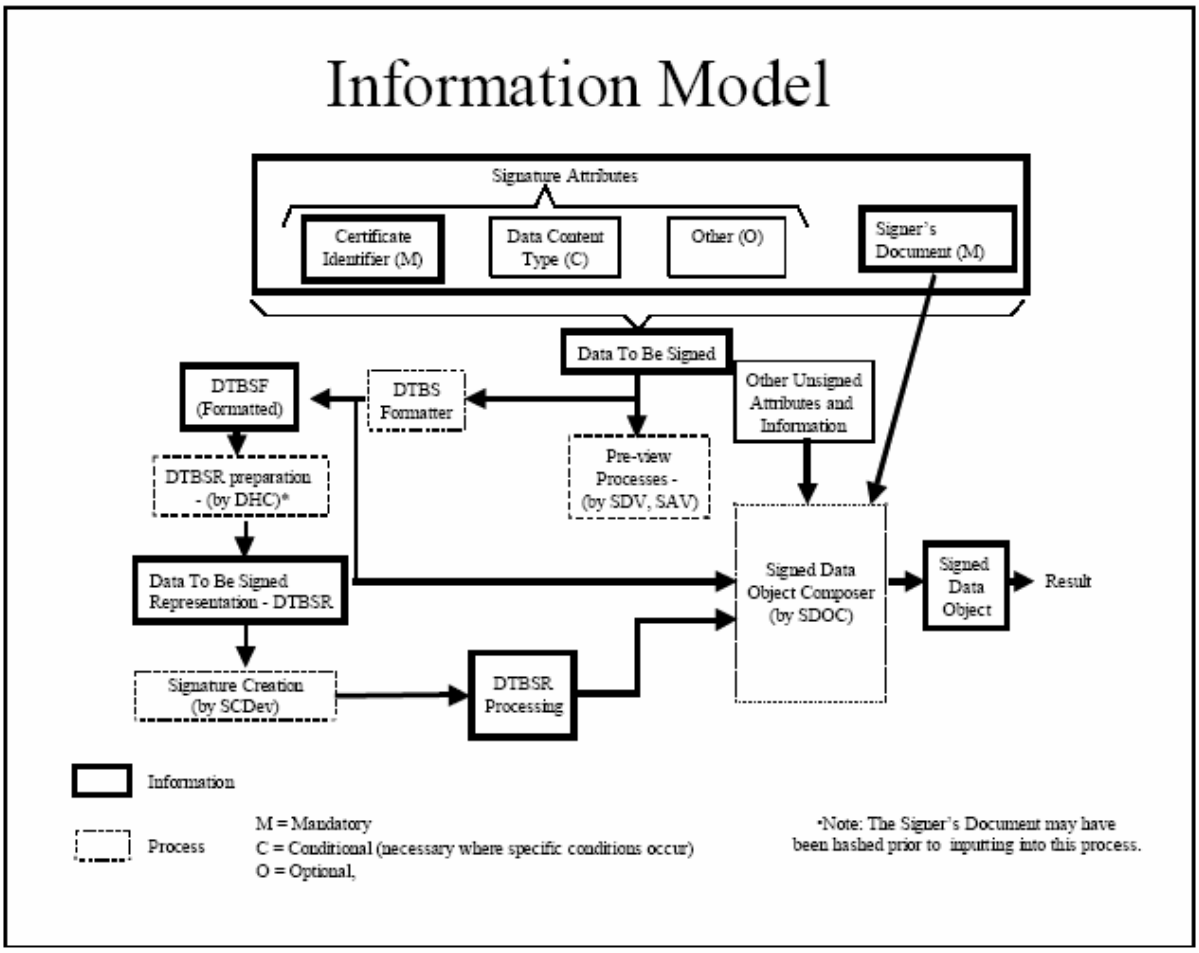
Aunque no aparecen definidos en la Ley 59/2003, su existencia y su necesidad conectan con la protección de los datos de creación de firma electrónica, ya que con los datos de activación – conocidos únicamente por el firmante o por las personas en quien éste "delegue" la creación de la firma – se puede acceder a los datos de creación de firma y "activar" el procedimiento de generación de la firma.

Precisamente este dato de activación de la creación de la firma electrónica es el mecanismo de protección más habitual de los datos de creación de firma electrónica que se menciona en el artículo 24.3.c) de la Ley 59/2003.

Los datos de activación son un dato alfabético y numérico que puede tener una longitud variable y que debería estar formada como mínimo por ocho caracteres, aunque muchas veces coincide con un número de identificación personal de cuatro dígitos.

7.1.4. El modelo de información de los productos de firma electrónica

El gráfico siguiente ilustra el modelo de información asociado a la creación de una firma electrónica:



En este gráfico, los acrónimos tienen los significados siguientes:

- DTBS (*Data To Be Signed*) significa los datos a firmar, que resultan de formar un conjunto con los elementos siguientes:

- El documento a firmar (*signer's document*), que es un dato que se debe hacer constar obligatoriamente[65].

  Se puede tratar de un documento en formato para revisión, como un documento de un procesador de textos, un mensaje de correo electrónico o un fichero, del cual se muestra una representación, particular, dependiendo de las capacidades del dispositivo que lo muestra, y, por lo tanto, puede ser diferente de la representación que verá el verificador de la firma.

  También se puede encontrar en formato no modificable, como en un fichero protegido (PDF, Postscript), y exponerse en un sistema con reglas que muestran igual el documento al firmante y al verificador.

  En algunos casos, el documento puede contener informaciones y datos que no resultan visibles al firmante, o incluso *código malicioso*, informaciones que pueden generar dudas sobre la firma electrónica y que, en consecuencia, se tratan como amenazas a la seguridad[66].

  También se puede encontrar en un formato que visualizan necesariamente de manera diferente el firmante y el verificador a pesar de representar la misma semántica, cómo pasa con los ficheros EDI, HTML, XML, SGML y otros.

  Finalmente, el documento puede contener otros objetos de firma electrónica creadas por otras personas.

---

[65] Lógicamente, si no tenemos un documento para firmar difícilmente podremos producir una firma útil, ya que firmaremos el resto de elementos que realmente son accesorios de la misma firma.

[66] Esto no quiere decir que no sea posible o legal firmar estos documentos, sino que habrá que probar que el firmante conoció efectivamente el contenido para que éste le vincule. Esta prueba forma parte de la pericial que se deberá practicar, hipotéticamente, sobre el software de creación de firma y, en especial, sobre su interfaz con el firmante.

- El tipo de contenido de datos a firmar (*data content type*), atributo que define el formato del documento a firmar, y, por derivación, las normas para visualizarlo al firmante y al verificador de la firma electrónica.

- La identificación del certificado de firma electrónica (*certificate identifier*) con que se podrá verificar esta firma, que también es un dato que se debe hacer constar de manera obligatoria[67].

  Con este dato se puede determinar exactamente el certificado que habrá que utilizar para verificar la firma electrónica, ya que un mismo firmante puede disponer de muchos certificados diferentes al mismo tiempo. También permite evitar los ataques de sustitución de certificados de firma electrónica por otros con semántica diferente[68].

- Otros datos, opcionalmente, como atribuciones del firmante, u otros documentos o informaciones.

  Uno de estos datos adicionales opcionales es el identificador de la política de firma electrónica (*signature policy identifier*), que indica el conjunto de normas de seguridad aplicable a la creación y la verificación de esta firma, así como de su significado jurídico, de manera independiente del contexto de la firma.

  Otro de estos datos es el identificador del tipo de compromiso de firma (*commitment type*), que indica, de forma expresa, el significado jurídico – o de otro tipo – de la firma electrónica. Cuando una política de firma electrónica contiene diversos tipos de compromisos, este dato posibilita conocer el tipo concreto de compromiso de acuerdo con el cual ha sido emitida esta firma.

---

[67] Véase ETSI TS 101733, sección 8.8.1.

[68] En este caso, se trata de la modificación de datos del certificado, respetando la clave pública.

Finalmente, los datos a firmar se pueden referir a roles, permisos, poderes, sellos de tiempo y otras informaciones.

- DTBSF (*Data To Be Signed Formatted*) significa los datos a firmar que ya han recibido el formato necesario previo a la generación del resumen criptográfico mediante el proceso de formato correspondiente.

  Este proceso resulta necesario para garantizar que los datos se encuentran en el orden correcto, de acuerdo con una estructura concreta de firma electrónica, como el formato SignedData definido por PKCS#7, CMS, XMLDSig o XAdES.

- DTBSR (*Data To Be Signed Representation*) significa la representación matemática de los datos a firmar formateadas, es decir, el resumen criptográfico de los datos a firmar que se utilizará para la creación de la firma electrónica.

- SDO (*Signed Data Object*) significa el objeto de datos firmados, que es el resultado, ya tratado, del proceso de firma.

  El objeto de datos firmados se encuentra en lo mismo formado que el DTBSF. Incorpora en su interior la firma digital producida a partir de la DTBSR, como también otros datos e informaciones que no han sido objeto de firma.

7.1.5. El dispositivo seguro de creación de firma electrónica

7.1.5.1. La definición del dispositivo seguro de creación de firma electrónica

Un dispositivo seguro de creación de firma electrónica es un dispositivo que, de acuerdo con el artículo 24.3 de la Ley 59/2003, cumple los requisitos siguientes:

- Los datos utilizados para la generación de la firma electrónica (es decir, la clave privada) se pueden producir sólo una vez. El dispositivo asegura razonablemente el secreto.

- Existe una seguridad razonable del hecho de que los datos utilizados para generar la firma electrónica no pueden derivar de los datos de verificación de firma (propiedad de irreversibles) o de la misma firma y del hecho que la firma está protegida contra la falsificación con la tecnología existente en cada momento (longitud de claves).

- Los datos de creación de la firma electrónica pueden ser protegidos de forma fiable por el firmante contra su utilización por terceros (datos de activación de la creación de firma).

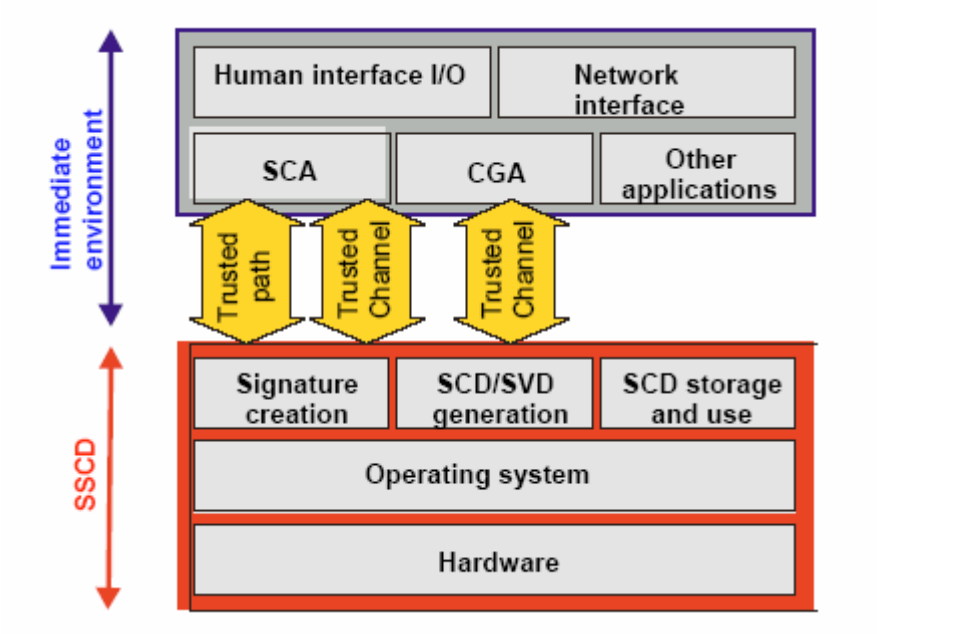
- El dispositivo no altera los datos o el documento que se debe firmar ni impide que éste se muestre al firmante antes del proceso de firma.

El dispositivo seguro es uno de los elementos requeridos para obtener una firma electrónica reconocida, directamente equivalente a la firma escrita, aunque las firmas electrónicas producidas con dispositivos que no disfrutan de esta consideración también pueden tener efectos, especialmente mediante un pacto entre las partes o una norma administrativa.

La mayor parte de las normas administrativas actuales hacen una interpretación muy flexible del concepto, de manera tal que el software de firma electrónica de uso amplio, como lo que incluyen los sistemas operativos más utilizados, se considera dispositivo seguro de creación de firma electrónica.

Ante esta postura, las normas europeas contienen una interpretación más estricta del concepto, que habitualmente conecta con el uso de un elemento físico o hardware – como una tarjeta criptográfica o un elemento similar – para poder considerar que el sistema de creación de firma electrónica es un dispositivo seguro.

Concretamente, CEN CWA 14169[69] ofrece un perfil de protección, escrito de acuerdo con la norma ISO 15408: Common Criteria, que determina criterios comunes para evaluar la seguridad de la información para dispositivos seguros de creación de firma electrónica (representados por el TOE, *target of evaluation*), con la estructura siguiente:



En este gráfico, hay que remarcar la diferencia entre el SSCD, que es el dispositivo seguro – y el objeto de las medidas de seguridad a implantar – y su entorno inmediato (*immediate environment*), que puede ser el ordenador personal del usuario, y con el cual es necesario que el dispositivo se relacione de manera fiable.

Así pues, podemos ver que entre el proceso de creación de firma y la aplicación de creación de firma (SCA, acrónimo de *signature creation application*) existe una ruta fiable (*trusted path*) para obtener los datos de autenticación del usuario y confirmar su voluntad[70], así como un canal fiable (*trusted channel*) para transmitir los datos para la

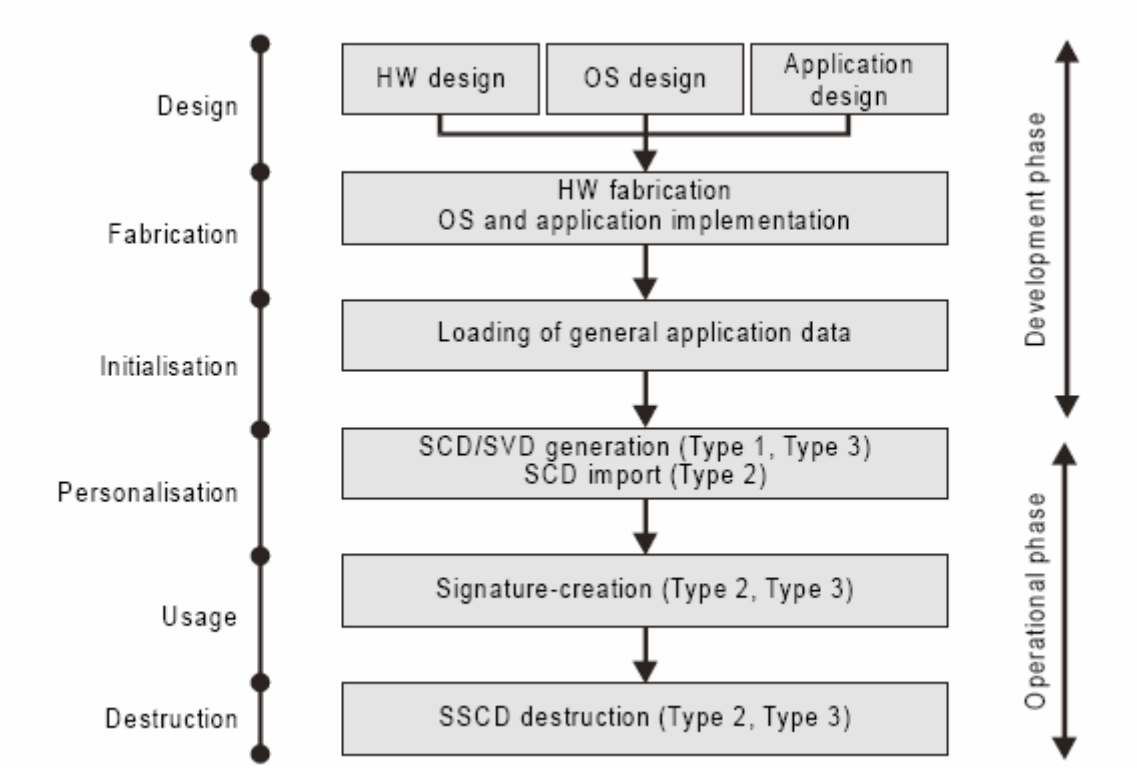
[69] Se trata de un perfil de protección muy adecuado para tarjetas, aunque, con algunas adaptaciones, también se puede utilizar para otros tipos de hardware.

[70] Excepto cuando el SSCD aporta él mismo la interfaz con el usuario; en este caso, ya se definen medidas de seguridad específicas para esta función dentro del TOE.

generación de la firma al SSCD, como ahora la representación de los datos a firmar (DTBSR, por ejemplo, el *hash* del documento).

Cuando el SSCD tiene la capacidad de generar claves de firma (con el proceso *SCD/SVD generation*), entonces también es necesario disponer de un canal fiable con la entidad de certificación (CGA, acrónimo de *certificate generation application*) para garantizar que los procesos para solicitar y obtener certificados son fiables.

A pesar de esta visión estructural del SSCD, hay que considerar las medidas de seguridad desde una perspectiva de ciclo de vida del dispositivo que debe prever los procesos siguientes:



Las amenazas contra el dispositivo identificadas por la especificación técnica CEN CWA 14169, para las cuales se determinan medidas de seguridad, son las siguientes:

- Ataques físicos al SSCD mediante sus interfaces.
- Divulgación de los datos de creación de firma mediante el almacenaje o la copia de estos datos fuera del dispositivo.

- Derivación de los datos de creación de firma a partir de datos públicos, como los datos de verificación de firma o firmas electrónicas generadas con estos datos de creación.
- Falsificación de la firma electrónica.
- Refutación de la firma electrónica.
- Falsificación de los datos de verificación de firma electrónica.
- Falsificación de la representación de los datos a firmar.
- Mal uso de la función de creación de firma con vistas a crear firmas sin el conocimiento del firmante.

Además, cómo veremos posteriormente, con respecto a las medidas de seguridad del entorno inmediato del SSCD, la especificación técnica CEN CWA 14170 ofrece un conjunto de medidas de seguridad funcional aplicable al software que funciona conjuntamente con dispositivos seguros de creación de firma electrónica (aplicaciones de firma electrónica) con el fin de garantizar un nivel apropiado de seguridad, en despliegue de la Directiva 99/93/CE.

La cuestión de la fiabilidad de la aplicación de firma electrónica es esencial, ya que el SSCD confía absolutamente en los datos que provienen de los canales de comunicación auténticos de la aplicación.

7.1.5.2. La acreditación de la cualidad de dispositivo seguro

Desde la perspectiva de la comprobación de los requisitos expuestos anteriormente, los fabricantes o los importadores pueden utilizar el mecanismo de la certificación de productos de firma electrónica del artículo 27 de la Ley 59/2003.

En relación con este mecanismo de certificación de los dispositivos seguros de creación de firma electrónica, hay que considerar las opciones siguientes:

- Cualquier producto de firma electrónica certificado en cualquier estado con un esquema nacional de evaluación y certificación de la seguridad de las

tecnologías de la información, siempre que el certificado de seguridad se haya hecho utilizando CC (*common criteria*) y un objetivo de seguridad que declare adherencia al perfil de protección CEN CWA 14169 (EAL4+) para dispositivos de creación de firma de tipo 3.

La lista de productos evaluados se puede consultar a la dirección web siguiente:
http://www.commoncriteriaportal.org/public/expert/index.php?menu=9

- Como segunda opción, se puede aceptar un producto certificado de acuerdo con CC (*common criteria*) con adherencia a otro perfil de protección, o sin adherencia a ningún perfil concreto, siempre que del análisis de su objetivo de seguridad se desprenda un nivel de seguridad equivalente.

- Como tercera opción, se puede aceptar un producto certificado con adherencia a un perfil de protección (o documento equivalente) de un esquema de evaluación y certificación de la seguridad de las tecnologías de la información diferente de CC (*common criteria*), siempre que del análisis correspondiente del perfil de protección o documento equivalente se desprenda un nivel de seguridad equivalente y que la metodología de evaluación ofrezca un nivel de rigor evaluador equivalente.

Muchos expertos consideran que solamente un software no puede ser de ninguna manera un dispositivo seguro de creación de firma electrónica, y, por lo tanto, que es imprescindible una tarjeta o equivalente para obtener la firma electrónica reconocida de acuerdo con la Ley 59/2003, de 19 de diciembre.

En este sentido, el uso de módulos criptográficos basados en software, aunque sean programados de forma bastante segura, tienen la problemática de tener que funcionar en sistemas que no resultan fiables en sí, como pasa con los sistemas operativos, de que funcionan en plataformas en las cuales acceden muchas personas, a menudo con capacidad de instalar muchas aplicaciones, de fuentes no controladas, y que pueden

recibir muchos ataques de seguridad, directamente o a través de las conexiones a Internet[71].

Eso implica la posibilidad que una aplicación fraudulenta pueda actuar incluso en contra del módulo criptográfico basado en software[72], o bien modificar o sustituir este módulo criptográfico[73].

Quizás es por este motivo que, hasta hoy, los únicos dispositivos seguros de creación de firma electrónica que han obtenido la certificación de seguridad a efectos de la Ley de firma electrónica se basan en hardware. En particular, los más utilizados son tarjetas (tradicionales o USB) con chip criptográfico, aunque ya se han empezado a evaluar otros productos de hardware, sobre todo hardware de firma centralizada.

Desde la perspectiva del programador de aplicaciones de creación de firma electrónica, esta problemática queda supuestamente resuelta por el dispositivo – y el software correspondiente – que suministra el fabricante o el importador o, cuando proceda, el prestador de servicios de certificación, como en el caso de CATCert cuando suministra la tarjeta, dado que con su garantía jurídica tiene suficiente para confiar.

Sin embargo, es importante entender la arquitectura de forma global, ya que quedará bajo la responsabilidad del programador de aplicaciones de creación de firma utilizar correctamente los mecanismos de comunicación segura entre el firmante y el dispositivo seguro, así como otros partos importantes del proceso de creación de firma.

De hecho, todo lo que no es el dispositivo seguro de creación de firma y su interfaz inmediata se considera *aplicación de creación de firma electrónica* y queda bajo la

---

[71] Por ejemplo, por virus o software espía (*spyware*).

[72] Mediante un *bypass*.

[73] Mediante una aplicación que imite el comportamiento del módulo criptográfico, por ejemplo, o un virus troyano que modifique el códido del módulo.

responsabilidad de su programador, en que tendrá que asegurar la aplicación mencionada ante potenciales ataques de terceros.

7.1.6. La arquitectura de programación de criptografia de los sistemas operativos

La complejidad de los sistemas criptográficos exige profundizar un poco en el modelo de implantación de la arquitectura de programación de criptografía a los sistemas operativos, en los que hay que distinguir los niveles o las capas siguientes:

- La capa de interfaz de servicios criptográficos con el dispositivo.
- La capa de interfaz de programación de servicios criptográficos.
- La capa de servicios criptográficos en entornos de ejecución virtual.
- La capa de interfaz de programación de servicios de seguridad.

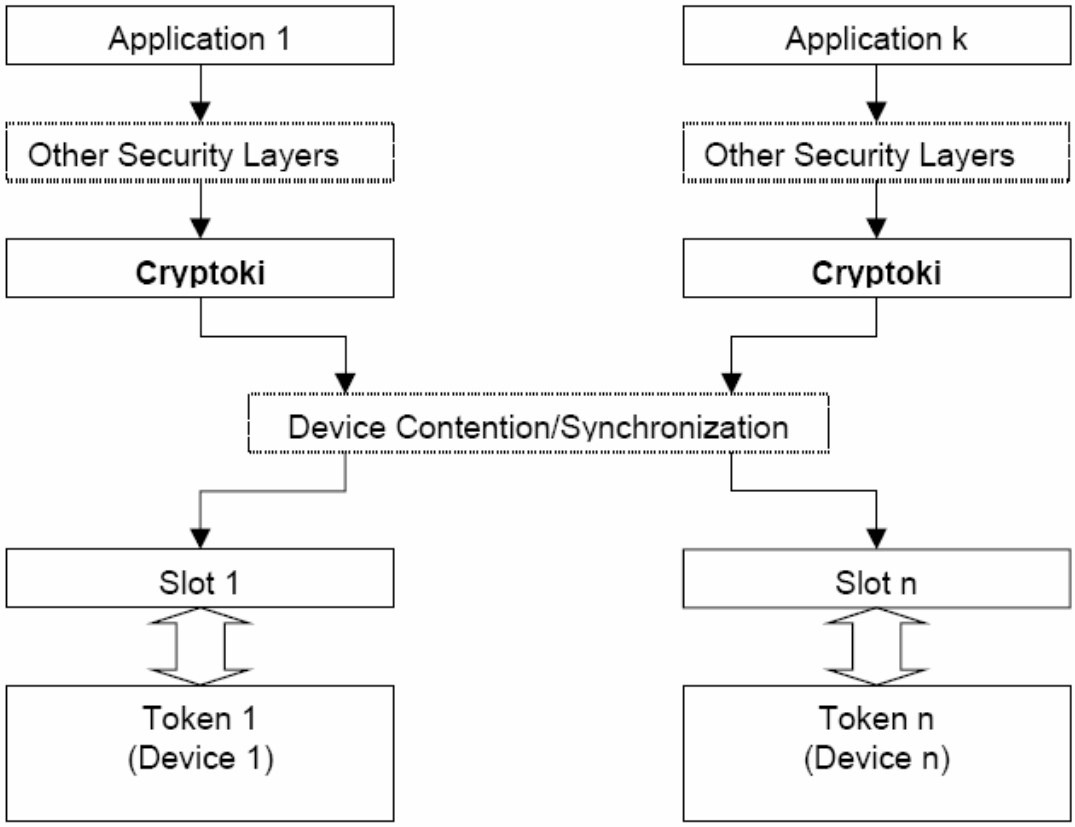
La capa de interfaz de servicios criptográficos con el dispositivo

A la complejidad de la separación entre el sistema del dispositivo – eventualmente seguro – de creación de firma y la aplicación, se añade el hecho que este dispositivo de creación de firma se relaciona con el sistema operativo sobre el cual trabajan las aplicaciones de firma electrónica mediante una o diversas interfaces de servicio, más o menos estándares, con la finalidad que el programador de la aplicación de creación de firma pueda interactuar con el dispositivo.

Muchas veces estas interfaces de servicio se llaman *módulos* o *proveedores de servicios criptográficos*. Las suministra el proveedor del dispositivo en circuito integrado y representan la capa inferior del sistema de programación de funciones criptográficas.

Estos módulos son los responsables iniciales de las operaciones criptográficas y de gestión de claves, y se utilizan mediante interfaces de programación de servicios criptográficos, que veremos acto seguido.

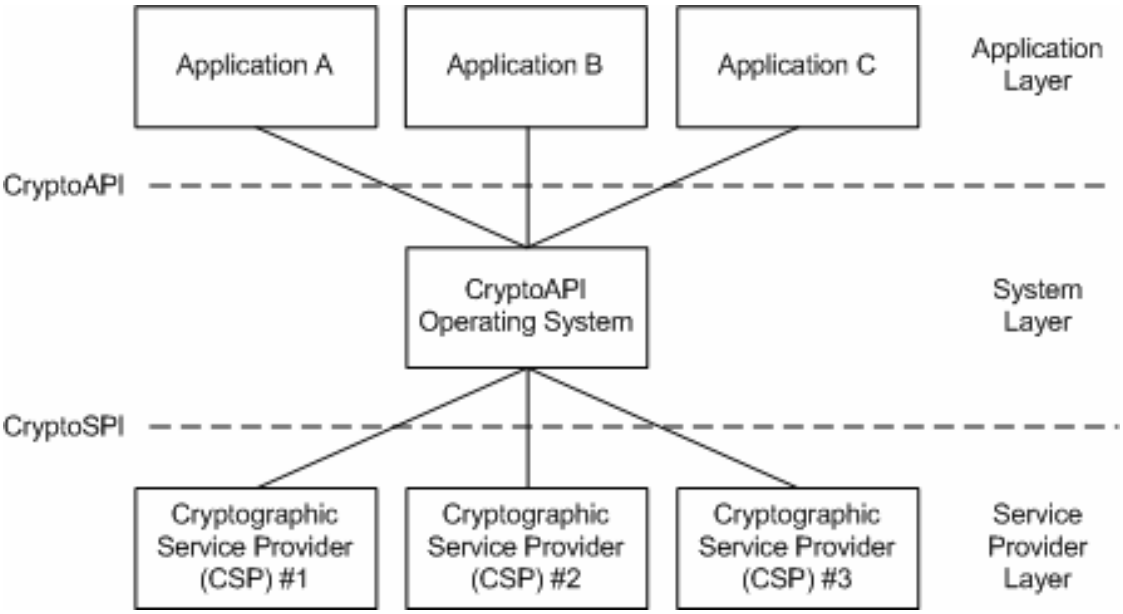
En general, para cualquier sistema operativo se puede utilizar Criptoki (PKCS#11) para definir una interfaz de servicios criptográficos abstracta, válida para cualquier tipo de elemento (denominado *token* en inglés) de seguridad, incluyendo tarjetas y otros dispositivos seguros de creación de firma. La ilustración siguiente muestra la arquitectura de Criptoki:



En el caso del sistema operativo Microsoft Windows, el proveedor de servicios criptográficos adopta obligatoriamente la forma de una biblioteca de enlaces dinámicos (DLL, *dynamic link library*) que implanta las funciones criptográficas de CryptoSPI, la interfaz de servicios criptográficos de la arquitectura de seguridad de Microsoft, a las cuales se accede con la interfaz de programación CryptoAPI.

Como medida de seguridad, cada CSP se tiene que firmar antes para poder ser utilizado con la versión de distribución del sistema operativo Windows.

La ilustración siguiente muestra la arquitectura de la familia de sistemas operativos Microsoft Windows:



Hay que decir que habitualmente todos los proveedores de dispositivos de firma electrónica (por ejemplo, tarjetas) suministran bibliotecas de enlaces dinámicos DLL para acceder con las dos interfaces de servicio, cosa que permite utilizar diferentes interfaces de programación criptográfica[74].

La capa de interfaz de programación de servicios criptográficos

[74] Aunque no es muy frecuente hacerlo, nada impide programar una aplicación con CryptoAPI que acceda a un módulo que exponga una interfaz PKCS#11 mediante una traducción (manual) de las funciones de programación de CryptoAPI a las funciones de servicio de criptografía de un módulo PKCS#11, trabajo que no será necesario realizar si el acceso al módulo se hace mediante el CSP correspondiente suministrado por el mismo fabricante del dispositivo.

Por encima de los módulos criptográficos, encontramos la interfaz de programación de servicios criptográficos. Tiene como objetivo facilitar la programación de las aplicaciones seguras de firma electrónica, envolviendo los llamamientos a las funciones de servicios criptográficos ofrecidas por los módulos criptográficos que hemos visto anteriormente.

Estas API permiten separar las aplicaciones (como el correo electrónico seguro, incluyendo los paquetes de seguridad y las interfaces de programación de servicios de seguridad que utilizan) de la criptografía. Las interfaces de programación de servicios criptográficos más utilizadas son las siguientes:

- API de acceso a proveedores de servicios o módulos criptográficos RSA Criptoki (PKCS#11, el estándar más independiente de sistemas operativos).

  Los proyectos basados en software libre Mozilla, cómo el cliente web Firefox o el cliente de correo electrónico Thunderbird, por ejemplo, han adoptado PKCS#11 como tecnología de seguridad criptográfica de base. Los usuarios pueden acceder en su tarjeta mediante el módulo criptográfico correspondiente. En caso de que no dispongan de tarjeta, pueden utilizar diferentes tokens basados en software, como el *softoken* suministrado con la licencia de Mozilla o como un objeto PSS de Safelayer con almacenaje en el ordenador personal o en otro dispositivo sólo de almacenaje, como una llave USB no criptográfica o un disco flexible[75], por ejemplo.

- API de acceso a proveedores de servicios o módulos criptográficos de Microsoft (CSP) mediante CryptoAPI, que es la interfaz de programación de

[75] Hay que advertir del riesgo de seguridad que supone la confusión entre los dispositivos (sean tarjetas tradicionales o en soporte USB) que sólo almacenan y los que realmente ejecutan las operaciones criptográficas en el dispositivo: mientras que en el primer caso las claves privadas salen del dispositivo cada vez que se deben utilizar – ya que las operaciones se realizan en la memoria del ordenador –, en el segundo caso las claves nunca abandonan el dispositivo, característica esencial para poder cualificar de seguro al dispositivo de creación de firma.

aplicaciones que se suministra[76] con el sistema operativo Microsoft Windows, y, en un nivel más bajo, mediante las funciones genéricas de CryptoSPI[77].

Microsoft ofrece también el componente cliente CAPICOM para facilitar el desarrollo rápido de aplicaciones de firma electrónica, escondiendo las complejidades de CryptoAPI en un objeto dinámico al cual hacer las llamadas de servicios pertinentes.

Como CryptoAPI sólo funciona en plataformas Windows, una aplicación que deba funcionar en diferentes plataformas (incluyendo Linux, por ejemplo) probablemente será programada utilizando Criptoki (PKCS#11), sin utilizar CryptoAPI, para aprovechar la máxima parte de código posible, con el correspondiente ahorro de coste y de tiempo. Otra opción consiste en utilizar una interfaz más abstracta que después pueda traducir los comandos de esta interfaz (firmar, cifrar...) a los correspondientes de PKCS#11 o CryptoAPI, como veremos a continuación.

La capa de servicios criptográficos en entornos de ejecución virtual

Los últimos años han empujado a la industria a la creación de entornos de ejecución virtual, como Java o. NET, para dar respuesta a una serie de necesidades cada vez más importantes. Entre estas necesidades podemos mencionar la portabilidad del código, la programación en múltiples entornos y plataformas y con múltiples lenguajes, la seguridad de la ejecución de código y la necesidad de operar en entornos web altamente distribuidos.

Un entorno de ejecución virtual es un sistema que controla la ejecución de código intermedio[78] que se evalúa y se ejecuta (cuándo ocurre, con compilación bajo

[76] Mediante las bibliotecas del sistema Advapi32.dll and Crypt32.dll.

[77] *Cryptographic service provider interface*.

[78] Un tipo de *bytecode*, como por ejemplo Microsoft Intermediate Language (MSIL).

demanda), con independencia de su lugar de "residencia", con políticas estrictas de contención y acceso a código y a datos.

En estos entornos el acceso directo al sistema está absolutamente restringido a los procesos ordinarios[79], por motivos inherentes a la definición arquitectónica de estos procesos, y resulta necesario disponer de clases, métodos e interfaces abstractas e independientes para acceder a las interfaces del sistema que hemos presentado anteriormente.

A menudo estas clases se llaman *código gestionado* por el entorno de ejecución virtual o, más explícitamente, por la máquina virtual.

Además, habitualmente estos entornos ofrecen propiedades de seguridad importantes, entre las cuales podemos mencionar una muy importante, como es la imposibilidad de acceder una aplicación en el espacio de memoria de otra aplicación de manera directa. Este hecho facilita la protección de las informaciones sensibles almacenadas en memoria, como una contraseña de usuario.

Algunas de estas clases, métodos e interfaces actúan como "envoltorios" de proveedores de servicios de criptografía (*wrappers*), aunque normalmente reciben también la denominación, más frecuente, de *proveedores criptográficos*, que no debemos confundir con los mencionados anteriormente, que realmente lo son en sentido estricto.

La diferencia entre ambos radica en el hecho de que la existencia de una clase Java o. NET que envuelve las funciones de un proveedor criptográfico no garantiza que realmente exista, en la plataforma en que finalmente se ejecuta el código, el CSP o módulo PKCS#11 necesario: se trata de una representación más bien abstracta de esta posibilidad para poder tener acceso desde la máquina virtual.

---

[79] A pesar de ello, explícitamente se puede ejecutar código “inseguro”, que accede al sistema, como por ejemplo con JNI en Java o con *unsafe* o *P/Invoque* en .NET; entonces es responsabilidad del programador asegurarse de aplicar controles muy estrictos al resultado de estas llamadas “inseguras”.

Los entornos basados en máquina virtual que podemos comentar son dos:

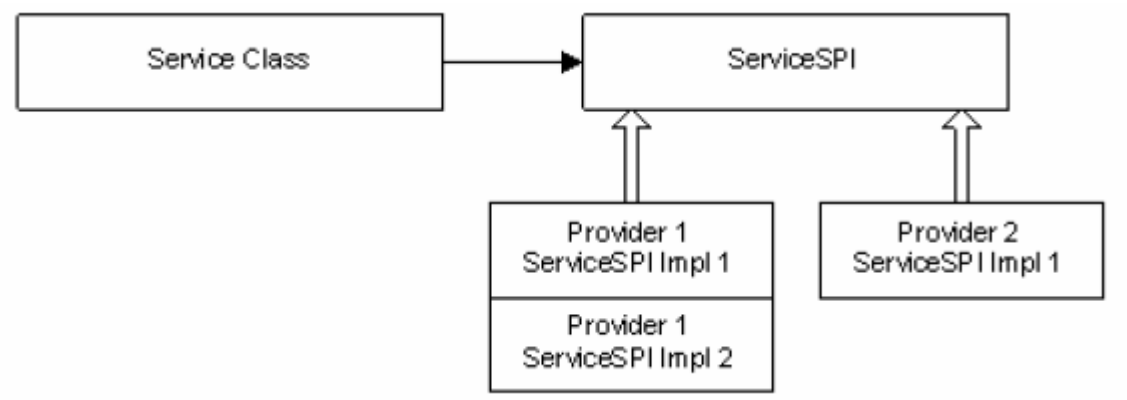
- Java Cryptography Architecture (JCA) / Java Cryptography Extension (JCE). Inicialmente estaban separados a causa de restricciones legales de exportación, pero a partir de la versión 1.4 de la Java Development Kit se han convertido en un único sistema, ya que JCE ha estado integrado como componente interno de la plataforma Java, en lugar de mantenerse como paquete opcional.

  JCA y JCE disponen de una arquitectura basada en proveedores, muy utilizada en las soluciones basadas en la plataforma Java. Estos paquetes consisten en los llamados *marcos de trabajo* (*frameworks*), que implantan la infraestructura requerida, y un número de proveedores adicionales, que suministran los algoritmos criptográficos. Normalmente estos proveedores son envoltorios criptográficos (*wrappers*) de objetos PKCS#11, lo cual permite la comunicación con las capas inferiores del sistema hasta llegar, cuando ocurra, en el dispositivo de firma electrónica.

  Los marcos de trabajo JCA y JCE son paquetes internos de Java y, por lo tanto, no se pueden reemplazar ni esquivar. Como ejemplo, el marco de trabajo JCE autentica a los proveedores JCE mediante su firma[80] por una entidad de certificación fiable (SUN o IBM).

[80] Una posibilidad para los vendedores independientes de interfaces criptográficas es no utilizar el marco de trabajo JCE e instalar uno propio.

La figura siguiente ilustra, de forma simple, el modelo de clases del marco de trabajo del proveedor JCA:



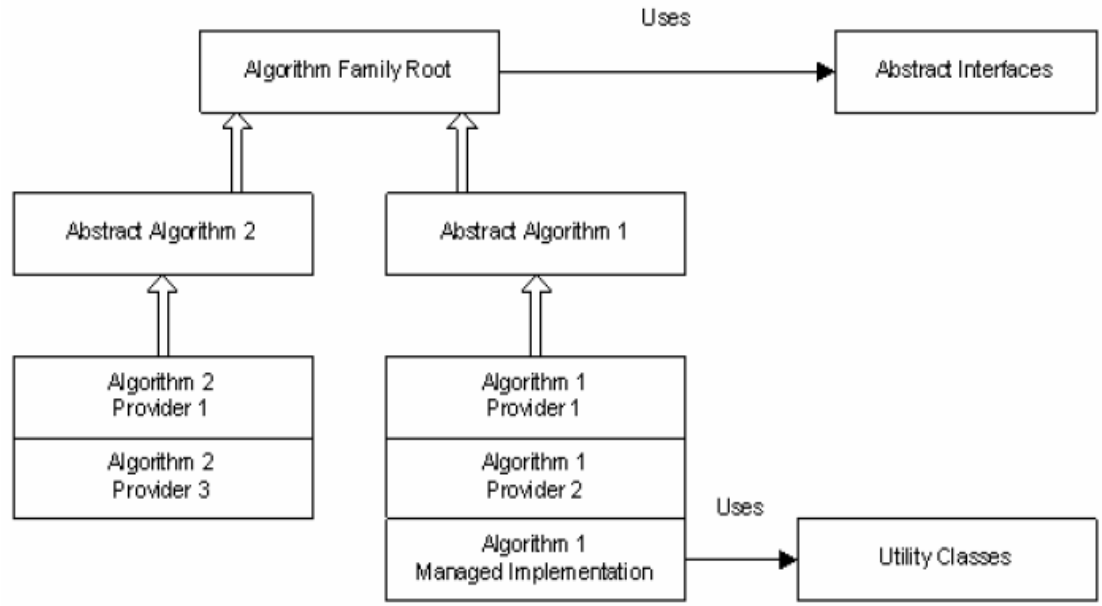
- Microsoft .NET, que se basa, sobre todo, en Microsoft CryptoAPI, el cual ya hemos comentado anteriormente. Muchos algoritmos criptográficos se implantan en forma de envoltorios gestionados por encima de CryptoAPI, y el sistema de gestión de claves se basa también en los contenedores de claves de los CSP.

  El modelo criptográfico de .NET, que se contiene en el espacio de nombre System.Security.Cryptography, se organiza horizontalmente en forma de capas, y verticalmente en forma de agrupaciones de tipo. Cada familia de algoritmos (simétricos, asimétricos...) integra a una agrupación vertical, jerárquica, que deriva de una clase única raíz de la familia, con dos capas por debajo de: una representación abstracta del algoritmo y su implantación concreta.

  Una característica importante de las clases raíz es que están protegidas, de manera que las aplicaciones no pueden producir extensiones. Eso quiere decir que la clase raíz de la familia de algoritmos asimétricos no permite hacer extensiones más allá de las abstracciones de RSA y DSA que suministra el sistema.

  Por convención de .NET, la clase de implantación se llama *proveedora* (*provider*) cuando es un envoltorio de un objeto CryptoAPI, y *gestionada* (*managed*) cuando es una implantación totalmente nueva.

La figura siguiente ilustra, de forma simple, la jerarquía de clases criptográficas de .NET:



La capa de interfaz de programación de servicios de seguridad

Por encima de las interfaces de programación de servicios criptográficos todavía podemos encontrar, opcionalmente, una capa adicional formada por las categorías de elementos siguientes:

- Paquetes de seguridad que implantan protocolos orientados a aplicaciones, los cuales hacen más simple la programación criptográfica para aquellas aplicaciones. Algunos ejemplos de los numerosos paquetes de seguridad que hay son:

    - o S/MIME y PGP/MIME, orientado al correo electrónico seguro y a la firma de ficheros.

- Netscape SSL – y sus evoluciones TLS y WTLS – orientado a los intercambios seguros, íntegros y confidenciales, de informaciones por Internet mediante HTTP.

- Interfaces de programación de servicios de seguridad, que envuelven y hacen uso de funcionalidades de criptografía de forma estándar y abstracta. Podemos citar, entre otros, los siguientes:

  - IETF GSS-API es una interfaz genérica de alto nivel de servicios de seguridad promovida desde el grupo Common Authentication Technology (CAT) del IETF, el organismo que impulsa los estándares de Internet. Dispone de un conjunto de extensiones para la protección de unidades de datos independientes (IDUP-GSS-API).

    GSS-API se diseñó para proteger comunicaciones con control de sesión, como File Transfer Protocol (FTP) entre entidades. IDUP-GSS-API, por su parte, no asume comunicaciones en tiempo real entre el emisor y el receptor de la comunicación, sino que protege cada unidad de datos, sea un fichero o un mensaje, de manera independiente del resto. Por lo tanto, resulta adecuado para proteger datos en aplicaciones de mensajería y es capaz de gestionar objetos de firma electrónica con valor evidencial.

  - Microsoft SSPI es una interfaz genérica de servicios de seguridad promovida por Microsoft, de forma paralela a GSS-API, que ofrece autenticación mutua entre entidades, así como autenticación y confidencialidad de mensajes. Vista su orientación a conexiones, es la base de los protocolos de "canal seguro" de Microsoft.

  - Open Group CSSM-API es una interfaz de gestión de servicios de seguridad que forma parte de la iniciativa de arquitectura común de seguridad de datos (CDSA).

CSSM-API ofrece un conjunto bastante importante de servicios de seguridad, como criptografía, gestión de certificados, políticas de confianza, almacenaje de datos o recuperación de claves.

7.2. La seguridad en la aplicación de creación de la firma electrónica

En el apartado anterior hemos visto que es responsabilidad del programador de aplicaciones la problemática de la seguridad en el proceso de creación de firma externo en el dispositivo seguro (que tiene no poca complejidad), y, en especial, la delicada situación de relacionarse con el firmante de una manera fiable y hacer de intermediario entre este firmante y su dispositivo de firma.

Los principales retos de seguridad que tienen que resolver las aplicaciones de firma electrónica son los siguientes[81]:

- Comunicación segura entre la aplicación de creación de firma electrónica y el dispositivo seguro correspondiente, incluyendo:

  - Identificación de la aplicación de creación de firma y dispositivo – seguro – de creación de firma, necesaria para el establecimiento del canal fiable[82].

  - Creación y mantenimiento de una ruta fiable que permita a la aplicación mostrar los datos a firmar y obtener el consentimiento del usuario cuando esta funcionalidad no la ofrezca directamente la interfaz del dispositivo seguro de creación de firma[83].

[81] CEN CWA 14355.

[82] Así como para evitar que falsas aplicaciones puedan conseguir firmas mediente usos fraudulentos.

[83] Por ejemplo, mediante la funcionalidad *card holder verification* (CHV).

  - Creación y mantenimiento de un canal fiable para comunicar los mandos en el dispositivo, como también la representación de los datos a firmar entre la aplicación de creación de firma y el dispositivo – seguro – de creación de firma, incluyendo la selección de los datos de creación de firma y la comunicación del consentimiento en el dispositivo[84].

- Gestión de la seguridad de los datos relativas a la firma, especialmente en relación con la ratificación del consentimiento del firmante por el dispositivo mediante un proceso de aceptación de la acción de firmar que garantice que la persona ha entendido las consecuencias del acto de firma, que resulta coherente con la política de seguridad del dispositivo.

- Tratamiento seguro del proceso de usuario previo y posterior a la creación de la firma electrónica, así como de la interfaz con el firmante.

El acuerdo del grupo de trabajo de firma electrónica del Comité Europeo de Normalización (CEN CWA 14170) ofrece un conjunto de medidas de seguridad funcional aplicable al software que funciona conjuntamente con dispositivos seguros de creación de firma electrónica (aplicaciones de firma electrónica) para garantizar un nivel apropiado de seguridad, en desarrollo de la Directiva 99/93/CE.

A pesar de no disfrutar de la consideración legal de norma técnica, CEN CWA 14170 es, hoy por hoy, el único documento aplicable en el Estado español, ya que no existe despliegue reglamentario de la Ley 59/2003, de 19 de diciembre, de firma electrónica, para interpretar los requisitos del artículo 24 de la Ley mencionada, en relación con las aplicaciones de creación de firma electrónica, de una manera objetiva, transparente y no discriminatoria.

---

[84] Funcionalidad que deberá aportar la biblioteca de programación de servicios criptográficos (PKCS#11, CSP u otra diferente), pero que hay que emplear correctamente, excepto cuando el sistema cree y utilice el canal fiable de manera transparente para el usuario.

7.2.1. El modelo funcional de creación de la firma electrónica

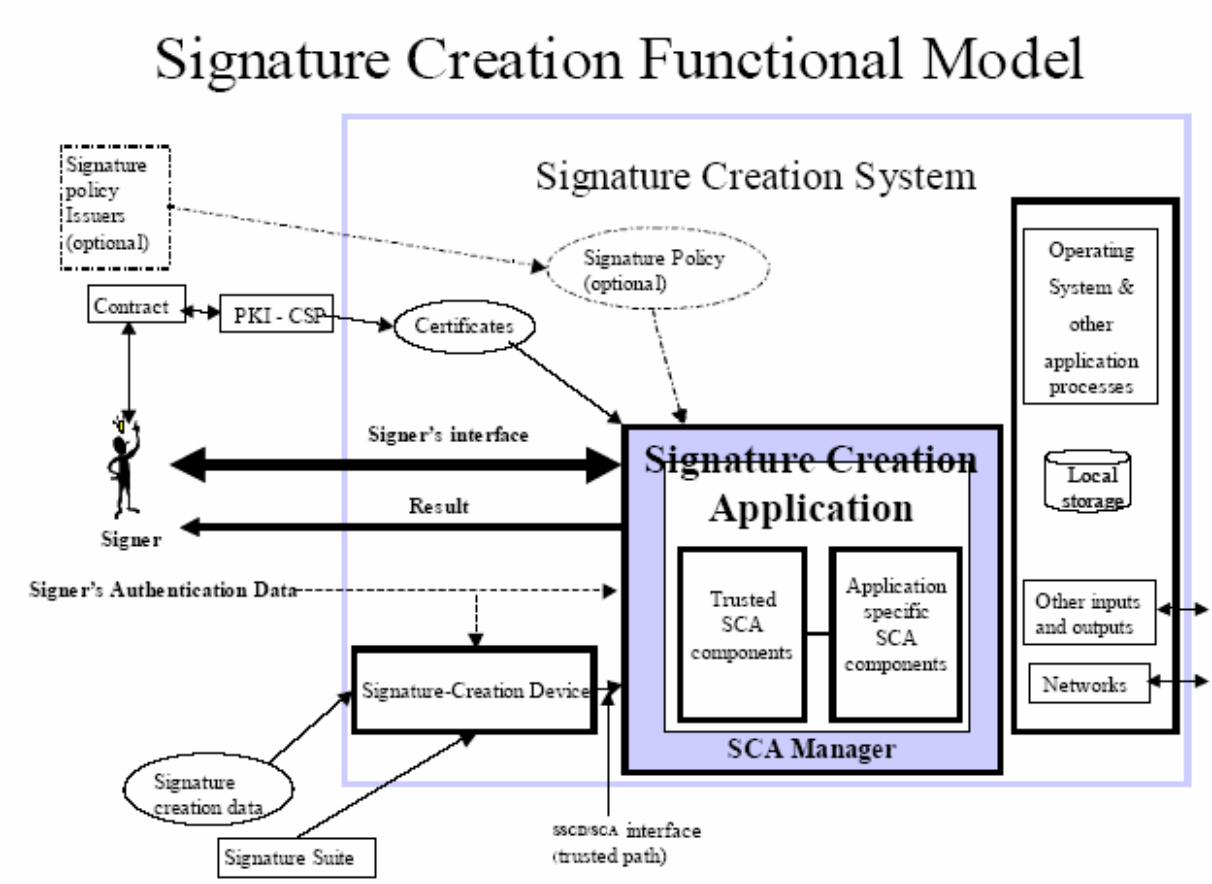
El objetivo de este modelo es explicar cuáles son los participantes principales en un sistema de creación de firma electrónica, de acuerdo con los diferentes entornos o escenarios en que trabajan, y las funciones que ejecutan, con un grado elevado de detalle, para llegar a entender sus necesidades de seguridad.

El entorno de creación de firma es el elemento más genérico del modelo, e incluye a un firmante que interactúa con un sistema de creación de firma.

El sistema de creación de firma contiene fundamentalmente los elementos siguientes:

- Una aplicación de creación de firma.
- Un dispositivo – seguro – de creación de firma.
- Un certificado electrónico reconocido de firma asociado al dispositivo de creación de firma.
- Opcionalmente, una política de firma electrónica, que indica los requisitos de seguridad técnica para la creación de la firma que tendrán que cumplir la aplicación de firma electrónica y el dispositivo.

El gráfico siguiente[85] ilustra el modelo funcional de creación de la firma electrónica:



El propósito de la aplicación de firma electrónica y del dispositivo de creación de firma es generar, a partir de un documento del firmante y de los atributos asociados a la firma – como la fecha y la hora de la firma o el rol de acuerdo con el cual el firmante crea la firma (cargo de la Administración pública, apoderado, delegado, etc.) –, el conjunto de los datos a firmar.

Posteriormente, se genera una firma electrónica avanzada – o reconocida, cuando el dispositivo es seguro y el certificado es reconocido – sobre los datos a firmar y, finalmente, un documento en soporte informático denominado *datos firmados*.

[85] CEN CWA 14170.

Lógicamente, es muy importante que las funciones de la aplicación de creación de firma electrónica y las comunicaciones entre la aplicación de creación de firma electrónica y el dispositivo – seguro – de creación de firma sean realmente fiables, porque de lo contrario esta aplicación podría engañar al usuario y obtener una firma electrónica para un documento diferente, por ejemplo, de lo que se muestra en la pantalla del ordenador.

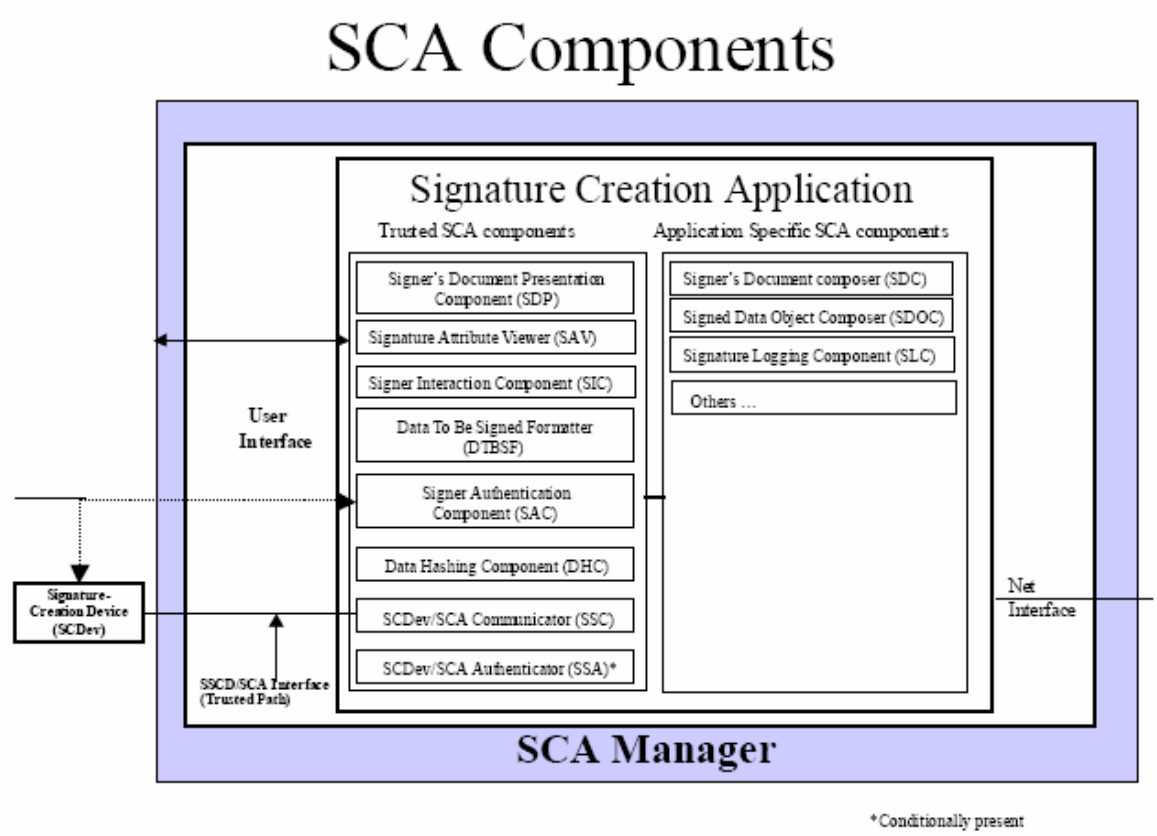
7.2.2. Los componentes fiables de la aplicación de firma electrónica

Para garantizar la fiabilidad de las funciones y las comunicaciones de la aplicación de firma electrónica, CEN CWA 14170 establece requisitos de seguridad en diferentes componentes que forman parte de la aplicación y distingue los componentes fiables de los componentes específicos de la aplicación.

Evidentemente, estos componentes no imponen ninguna restricción de arquitectura a los proveedores de aplicaciones de creación de firma, sino que suponen agrupaciones de funcionalidades útiles para determinar los requisitos de seguridad correspondientes.

Mientras que los componentes fiables son, en general, obligatorios, los componentes específicos de aplicación son opcionales y dependen de cada proveedor de aplicaciones de creación de firma.

La figura siguiente muestra los componentes de una aplicación de creación de firma:



Los componentes fiables de la aplicación de creación de firma son los siguientes:

- Componente de presentación del documento del firmante, que se utiliza para presentar el documento que el firmante escoge para firmar, mediante el componente de interacción con el firmante.

- Componente visor de atributos de firma, que se utiliza para visualizar los atributos de la firma que el firmante escoge para incorporar en la firma, mediante el componente de interacción con el firmante. Debe incluir la posibilidad de visualizar los contenidos principales del certificado – reconocido – del firmante.

- Componente de interacción con el firmante, que el firmante utiliza para interactuar con la aplicación de firma electrónica y controlar el proceso de creación de firma, así como para notificar informaciones de estado y de

errores de la aplicación. Este componente incluye todas las interacciones con el firmante excepto la autenticación.

- Componente de formateo de datos a firmar, que se utiliza para dar formato previo a un documento o a un resumen criptográfico de un documento, junto con los atributos de la firma, para pasarlo al componente de creación de resúmenes criptográficos.

- Componente de autenticación de firmante, que se utiliza para obtener credenciales conocidas por el firmante, o alguna muestra biométrica de éste, y preparar estos datos de autenticación para compararlas con los datos de autenticación del firmante almacenados en el dispositivo – seguro – de creación de firma electrónica.

- Componente de creación de resúmenes criptográficos, que se utiliza para producir la representación de los datos a firmar a partir de los datos a firmar formateados (que pueden estar resumidos totalmente o parcialmente de forma criptográfica o en texto en claro). Sólo se utiliza en caso de que el dispositivo – seguro – de creación de firma no genere sus propios resúmenes criptográficos.

- Componente de comunicación entre la aplicación de creación de firma electrónica y el dispositivo – seguro – de creación de firma, que se utiliza para gestionar la interacción entre los dos.

- Componente de autenticación entre la aplicación de creación de firma electrónica y el dispositivo – seguro – de creación de firma, que se utiliza para establecer una ruta fiable entre los dos cuando ésta no se puede establecer por mecanismos organizativos.

Asimismo, los componentes específicos de la aplicación de creación de firma pueden ser, entre otros, los siguientes:

- Componente de composición de documentos, que se utiliza para crear y editar documentos, mediante el componente de interacción con el firmante. Este componente no se utiliza en el caso de la actuación administrativa automatizada.

- Componente de composición de objetos de datos firmados, que se utiliza para dar formado al resultado del proceso de creación de firma, por ejemplo asociando la firma y los datos firmados, en un formato preferido por la aplicación – como el definido por ETSI TS 101733 o TS 101903.

- Componente de registro de firmas, que registra detalles importantes sobre las firmas producidas.

- Componente de indicación del poseedor del dispositivo – seguro – de creación de firma electrónica.

- Otros, de acuerdo con las necesidades de cada aplicación concreta.

7.3. La seguridad de las comunicaciones de la aplicación

En este apartado presentamos los requisitos de seguridad de las comunicaciones entre los diferentes componentes del sistema de firma, como entre la aplicación y el dispositivo de creación de firma electrónica, así como entre los diferentes componentes de la aplicación distribuida de firma electrónica, y el uso de las interfaces externas a la aplicación.

Podemos agrupar los requisitos en dos categorías:

- Requisitos de comunicación fiable entre componentes del sistema.
- Requisitos de las interfaces externas a la aplicación.

7.3.1. Los requisitos de comunicación fiable entre componentes del sistema

En primer lugar, se debe establecer una comunicación fiable entre los dos elementos del sistema de firma con la finalidad de proteger los datos relativos a la firma (datos de autenticación, datos a firmar, datos a firmar formateados y representación de los datos a firmar). Esta comunicación fiable será más exigente cuando la aplicación de firma se encuentre en un entorno público.

Como hemos visto, esta comunicación da cumplimiento al requisito de ruta fiable (*trusted path*) con el SSCD en relación con los datos de autenticación del firmante, y con el requisito de canal fiable (*trusted channel*) con el SSCD en relación con el resto de datos de la firma electrónica.

En segundo lugar, cuando la aplicación de creación de firma funcione de forma distribuida, con componentes en diferentes plataformas, es necesario proteger las comunicaciones entre estos componentes, ya que es posible que la información relativa a la firma circule por enlaces de comunicaciones potencialmente no fiables o por interfaces de aplicaciones internas también potencialmente no fiables, como también por módulos de software y hardware que podrían someter los datos relativos a la firma a vulnerabilidad en cuanto a integridad, autenticidad y confidencialidad.

Un caso de aplicación distribuida es el uso de servidores centrales de aplicación de firma electrónica (a veces denominiados *servidores de firmas*) conectados a sistemas de gestión documental o de gestión de expedientes, delante de los cuales el usuario solicita la firma, por ejemplo utilizando el estándar DSS[86].

En este caso, el usuario normalmente no posee físicamente el documento. Todas las operaciones se llevan a cabo de manera remota, entre dos sistemas que residen en

[86] DSS es un estándar producio por OASIS que permite la solicitud remota de generación y de verificación de firmas mediante servicios web.

plataformas diferentes, hecho que implica tener que establecer requisitos adicionales de seguridad para garantizar la fiabilidad global del sistema.

En tercer lugar, habitualmente el sistema en que reside la aplicación de firma electrónica ejecuta otros procesos informáticos y, además, dispone de periféricos y puertos de comunicaciones con otros sistemas. Todos estos elementos se deben considerar potencialmente no fiables.

Las amenazas identificadas son las siguientes:

- En relación con la comunicación fiable entre la aplicación y el dispositivo:

    - Alteración accidental o maliciosa de los componente de los datos a firmar. Consiste en el hecho de que los procesos de la infraestructura utilizada por la aplicación de firma electrónica alteran, por accidente o malintencionadamente, los datos a firmar, antes o después de recibir formado, o la representación resumida de forma criptográfica de estos datos seleccionados por el firmante, o cualquier otro dato de los protocolos de comunicación entre la aplicación y el dispositivo.

    - Ruptura accidental o maliciosa de la confidencialidad de los datos de autenticación del firmante, de los componentes de los datos a firmar o de los datos a firmar formateadas. Consiste en el hecho que la infraestructura de la aplicación de firma revela o copia a personas no autorizadas los datos de autenticación del firmante (por ejemplo, su contraseña), los componentes de los datos a firmar o los datos a firmar formateados.

    - Divulgación o uso erróneo de los datos de autenticación del firmante, de los componentes de los datos a firmar o de los datos a firmar formateadas por un sistema público de creación de firma operado por un proveedor de servicio. Consiste en el hecho que el sistema público de firma infringe la confidencialidad de los datos de autenticación del firmante, de los componentes de los datos a firmar o de los datos a firmar formateados.

- Sustitución de uno o diversos componentes de los datos a firmar o de los datos a firmar formateados. Consiste en el hecho de que la infraestructura de la aplicación de firma sustituye componentes de los datos a firmar, antes o después de recibir formado, de manera accidental o malintencionada, antes de que se complete el proceso de generación de firma.

- En relación con las aplicaciones distribuidas de creación de firma:

  - Ruptura de la integridad o la confidencialidad de los datos de autenticación del firmante en tráfico entre componentes de la aplicación distribuida de firma electrónica. Consiste en el hecho de que los datos de autenticación del firmante (por ejemplo, su contraseña) se corrompen, se alteran o se divulgan, accidentalmente o maliciosamente, mientras son transferidas entre los componentes de la aplicación distribuida de firma electrónica.

  - Ruptura de la integridad o la confidencialidad de los datos a firmar, antes o después del formateo, en tráfico entre componentes de la aplicación distribuida de firma electrónica. Consiste en el hecho que los datos a firmar o los datos a firmar formateadas se corrompen, se alteran o se divulgan, accidentalmente o maliciosamente, mientras son transferidos entre los componentes de la aplicación distribuida de firma electrónica.

- En relación con los procesos y los puertos de comunicaciones no fiables:

  - Interferencia producida por procesos y puertos de comunicaciones no fiables. Consiste en el hecho que los procesos y los puertos de entrada y salida del sistema de la aplicación de creación de firma electrónica que no están bajo el control de la aplicación pueden corromper o romper la confidencialidad de los datos de autenticación del firmante, de los datos a firmar con formato o sin o corromper los procesos de la misma aplicación de creación de firma electrónica.

Los requisitos de seguridad correspondientes son los siguientes:

- La aplicación debe mantener la integridad de:

    - Los datos a firmar, los datos a firmar formateadas, la representación de los datos a firmar y el resto de informaciones suministradas por el firmante.

    - Los intercambios de datos durante el flujo del protocolo de comunicación entre la aplicación y el dispositivo, mediante el uso de un canal seguro.

- La aplicación debe mantener la confidencialidad de los componentes de los datos a firmar, de los datos a firmar formateados y de los datos de autenticación del firmante.

- La aplicación que opere en un entorno público borrará de forma segura todos los datos relativos a una firma después de haber completado el proceso correspondiente.

- Cuando se utilice un sistema público de creación de firma, éste no deberá retener los datos de autenticación del firmante, de los componentes de los datos a firmar y de los datos a firmar formateados. Tampoco deberá copiar los datos mencionados a ninguna persona no autorizada por el firmante.

- La aplicación debe garantizar que los datos a firmar presentados al firmante son las mismos que los que éste seleccionó.

- La aplicación debe garantizar que los componentes de los datos a firmar utilizadas para crear los datos a firmar formateadas y la representación de los datos a firmar son los mismos que se presentaron al firmante, como también que los datos son idénticos a las que éste seleccionó.

- Cualquier dato de autenticación del firmante que sea transferido entre diferentes componentes distribuidos de la aplicación de creación de firma electrónica se tiene que transferir utilizando una ruta fiable que ofrezca integridad y confidencialidad.

- Los datos a firmar con formato o sin que sean transferidos entre diferentes componentes distribuidos de la aplicación de creación de firma electrónica se tienen que transferir utilizando un canal fiable que ofrezca integridad y confidencialidad.

- Todos los procesos y los puertos de entrada y salida del sistema de la aplicación de creación de firma electrónica que no estén bajo el control de la aplicación se cerrarán o se monitorizarán para evitar interferencias.

7.3.2. Los requisitos de las interfaces externas a la aplicación[87]

Las interfaces externas a la aplicación de firma electrónica implican diversos riesgos para la aplicación. Podemos mencionar, entre otros, la posibilidad de ataque de sustitución o de modificación de la aplicación de firma electrónica o de sus componentes, así como vulnerabilidad debida a virus y otras formas de software malicioso.

Las amenazas identificadas son las siguientes:

- Compromiso de componentes de la aplicación por software malicioso. Consiste en el hecho de que el software malicioso importado corrompe componentes de la aplicación de firma electrónica.

[87] CEN CWA 14170, sección 18.

- Compromiso de componentes de la aplicación por intrusos. Consiste en el hecho de que el intruso corrompe componentes de la aplicación de firma electrónica.

- Compromiso de componentes de la aplicación por software falso instalado. Consiste en el hecho de que el software falso instalado genera firmas electrónicas inválidas.

Los requisitos de seguridad correspondientes son los siguientes:

- La aplicación de firma electrónica debe evitar ser corrompida por código malicioso y, en caso de que eso pase, tiene que existir un proceso para sanear los componentes corruptos.

- La aplicación de firma electrónica ha de mantener la integridad de sus componentes funcionales y evitar la posibilidad de que les corrompan intrusos.

- En relación con los componentes de la aplicación que se pueden descargar de la red, la descarga se tiene que hacer desde una fuente fiable, circunstancia que se indicará en la documentación del producto.

7.4. La seguridad de los datos de firma gestionados por la aplicación

En este apartado presentamos los requisitos de seguridad de los documentos, los datos y otras informaciones relativos en la firma electrónica que quedan dentro del ámbito de responsabilidad de la aplicación de firma electrónica.

Los ataques contra estos datos son especialmente importantes, ya que la manipulación, la corrupción o la sustitución del documento o de los datos a firmar, en cualquier momento del proceso, conducen a la generación de firmas falsas.

A pesar de los objetivos de seguridad que expondremos a continuación, conviene remarcar que es importante verificar el objeto firmado al finalizar el proceso, hecho que nos permitirá detectar y corregir posibles errores.

Podemos agrupar los requisitos en las categorías siguientes:

- Requisitos generales de seguridad de los datos a firmar.
- Requisitos de seguridad propios del documento a firmar.

- Requisitos de seguridad de los atributos de firma electrónica.
- Requisitos de seguridad del proceso de resumen y formateo de los datos a firmar.

7.4.1. Los requisitos generales de seguridad de los datos a firmar[88]

Existen situaciones que afectan a la seguridad global del sistema, resultantes de la manipulación de los datos a firmar por parte de la aplicación de firma electrónica, así como la producción de la estructura de datos que contiene el objeto firmado.

Por este motivo, hay que garantizar que los datos a firmar tienen una seguridad mínima, antes de continuar el proceso, y verificar la firma producida antes de entregarla a terceras personas.

Las amenazas identificadas son las siguientes:

- Generación de una firma inapropiada. Consiste en el hecho de que se genera una firma para un documento nulo, sin ningún contenido, de manera tal que la firma se genera sólo sobre los atributos de firma del documento.

- Ambigüedad del certificado del firmante que consta en la firma electrónica. Consiste en el hecho de que se puede asociar la firma a un certificado del firmante, con una semántica diferente de la prevista por el firmante.

- Generación de una firma incorrecta. Consiste en el hecho que se produce una firma incorrecta matemáticamente a causa de la corrupción de alguno de los datos a firmar o, especialmente, de la representación resumida de estos datos, por error de la aplicación o del dispositivo de creación de firma.

[88] CEN CWA 14170, secciones 7.5 y 7.6.

Los requisitos de seguridad correspondientes son los siguientes:

- Los datos a firmar deben incluir necesariamente un documento del firmante.

- La firma debe contener necesariamente el certificado del firmante seleccionado, cuando proceda, relativo a los datos de creación de firma utilizados para producir la firma electrónica, de acuerdo con la intención del firmante.

- Los datos a firmar deben contener el tipo de contenido de datos del documento del firmante siempre que esta información no conste en el mismo fichero.

- Hay que verificar la firma electrónica producida, aunque esta verificación no sea completa[89].

7.4.2. Los requisitos de seguridad propios del documento a firmar[90]

La aplicación de creación de firma electrónica tiene que garantizar que el documento que ve[91] al firmante en su pantalla es lo mismo que firmará. Este documento no ha sido ni será manipulado, corrupto ni sustituido desde el momento que al firmante lo habrá seleccionado y hasta la producción de la firma.

Para ofrecer estas garantías, hay que implantar las funciones de un componente de presentación del documento al firmante. Este componente tiene que conocer los tipos

---

[89] La verificación se puede referir a la corrección criptográfica de la firma digital, por ejemplo, antes de incrustarla en la estructura de datos del objeto firmado. Si ja hemos verificado el certificado anteriormente o si tenemos garantía de su vigencia, no es necesario volverlo a verificar.

[90] CEN CWA 14170, sección 8.

[91] El documento a mostrar tiene un tipo de contenido de datos concreto, que es el que se utiliza para llamar al módulo que interpreta y visualiza el documento. Así, por ejemplo, para el tipo de contenido PDF, llamamos al visor de Adobe Acrobat.

de contenido de datos asociados a los documentos que se pueden firmar, ya que entonces se pueden señalizar las situaciones propias de cada formato[92].

En el caso de la actuación administrativa automatizada, no se da la circunstancia que el documento sea presentado al firmante. Así pues, no será necesario implementar medidas de seguridad específicas, pero sí, en todo caso, que habrá que controlar cuál es el formato documental sobre el cual se tiene que generar la firma electrónica, sobre todo si se trata de una firma electrónica envuelta dentro del documento.

7.4.3. Los requisitos de seguridad de los atributos de firma electrónica[93]

La aplicación de firma electrónica debe garantizar la seguridad de los atributos de la firma electrónica mediante la funcionalidad de un componente de visualización de los atributos de firma electrónica que permita presentarles al firmante, con la finalidad que éste les pueda inspeccionar de manera fiable.

El firmante debería poder acceder a todos los atributos de la firma, pero especialmente a los siguientes:

- El certificado del firmante.
- El tipo de contenido de datos correspondiendo al documento del firmante, cuando se encuentra presente.
- La política de firma electrónica, cuando se encuentra presente.
- El tipo de compromiso de la firma electrónica, cuando se encuentra presente.

Se considera que el uso de un certificado que haya sido revocado o haya expirado constituye una amenaza de seguridad porque puede conducir a la producción de

---

[92] Por ejemplo, que el tipo de contenido tiene información invisible para el firmante, de lo cual deriva que no quedará vinculado por esta información, sino únicamente por la información que pudo ver cuando firmaba.

[93] CEN CWA 14170, sección 9.

firmas inválidas. La aplicación de firma electrónica debería comprobar la validez y el estado de revocación antes de finalizar el proceso general de firma electrónica[94].

Por otra parte, es imprescindible que el firmante pueda conocer el contenido del certificado de firma y escoja expresamente el certificado con que quiere firmar – cuando dispone de más de uno – para evitar errores que indudablemente afectarán a la validez de la firma electrónica correspondiente.

Las amenazas identificadas son las siguientes:

- Firma de un atributo incorrecto. Consiste en el hecho que la firma se aplica sobre atributos que no son apropiados para la firma que se desea generar.

- Alteración accidental o maliciosa de los atributos por parte de la aplicación. Consiste en el hecho de que la firma cambia de significado e intención a causa de la modificación, accidental o maliciosa, de los atributos por parte de la aplicación de firma electrónica.

- Referencia a un certificado de firma inválido. Consiste en el hecho de que el certificado de firma ha expirado o ha sido revocado y, por lo tanto, la firma ha sido producida inválidamente.

- Referencia a un certificado de firma incorrecto. Consiste en el hecho que la firma se asocia a un certificado diferente de lo que pretendía al usuario, cosa que puede implicar un cambio en el significado de la firma y producir errores de verificación

[94] Por ejemplo, mediante la consulta a la lista de revocación de certificados (CRL) o al servidor OCSP (protocolo en línea de estado de certificados).

Los requisitos de seguridad correspondientes son los siguientes:

- La aplicación de firma electrónica debe controlar los atributos a firmar.

- La aplicación de firma electrónica debe garantizar la integridad y la autenticidad de los atributos de la firma.

- La aplicación de firma electrónica debe informar al firmante de la presencia de texto oculto, macros o código activo en los atributos[95], siempre que no se trate de un comportamiento programado previamente, cosa que implica parar el proceso automatizado y permitir la inspección de estos atributos mediante un visor de los atributos firmados, con la capacidad de detectar las modificaciones de la presentación de los atributos firmados.

- La aplicación de firma electrónica debe comprobar el periodo de validez del certificado y su estado de revocación antes de finalizar el proceso de firma, y también impedir el uso en caso de invalidez.

- La aplicación de firma electrónica debe permitir al firmante la inspección de los principales elementos del certificado de firma con que firmará[96] en el momento de configurar el acto administrativo automatizado.

[95] Normalmente los atributos no contienen este tipo de datos, pero, si lo hacen, entonces hay que hacer consciente de ello al firmante.

[96] Esta obligación no implica que el firmante siempre deba escoger su certificado para firmar, ya que, si sólo tiene uno, es evidente que no se puede equivocar a la hora de escogerlo para la firma.

7.4.4. Los requisitos de seguridad del proceso de resumen[97] y formateado[98] de los datos a firmar

La aplicación de firma electrónica tiene que garantizar la seguridad del proceso de formateo de los datos a firmar, que se produce a partir del documento de firmante y de los atributos de firma.

En caso que los datos a firmar tengan que incluir el resumen criptográfico de los datos, entonces antes de finalizar el proceso de formateo se produce este resumen en las condiciones de seguridad necesarias[99]. Este resumen criptográfico también se llama, como hemos visto, *representación de los datos a firmar*.

En cuanto al proceso de resumen criptográfico, hay tres posibilidades:

- Producirlo íntegramente en la aplicación de firma electrónica.
- Producirlo parcialmente en la aplicación de firma electrónica y acabarlo en el dispositivo – seguro – de creación de firma electrónica.
- Producirlo íntegramente en el dispositivo – seguro – de creación de firma electrónica[100].

Las amenazas identificadas son las siguientes:

- En relación con el formateado de la firma:

    - Producción de datos a firmar incorrectos o incompletos. Consiste en el hecho de que, como resultado de un ataque, la aplicación no aplica

---

[97] CEN CWA 14170, sección 13.

[98] CEN CWA 14170, sección 12.

[99] Incluyendo, en función del algoritmo empleado, el *padding* del resumen.

[100] Esto requiere disponer de un canal de comunicación con el dispositivo de un ancho de banda considerable, como sucede con los dispositivos de hardware conectados físicamente al servidor de firma, mediante el bus de comunicaciones físicas (PCI, por ejemplo) o por red, cuando se quiere hacer sobre documentos de gran longitud.

todos los datos necesarios para la firma electrónica de acuerdo con un formato concreto (como el formato de firma de larga duración), o bien en el hecho de que la aplicación de firma recibe componentes de la firma que han sido falsificados.

- Algoritmo débil de resumen. Consiste en el hecho de que se pueden producir colisiones, es decir, que dos documentos diferentes pueden dar lugar al mismo resumen.

- Formato de entrada débil de firma electrónica. Consiste en el hecho de que se pueden producir problemas para computar la firma electrónica.

- Producción de la representación de los datos a firmar incorrecta o incompleta. Consiste en el hecho que la representación de los datos a firmar no contiene los componentes requeridos por la política de seguridad y por el firmante, lo cual puede producir un documento firmado incompleto y ambiguo.

Los requisitos de seguridad correspondientes son los siguientes:

- La aplicación de firma electrónica impondrá controles para verificar la validez, la autenticidad y la totalidad de los los componentes obtenidos para producir el formato correcto de firma escogido por el firmante.

- La aplicación de firma electrónica utilizará los algoritmos de resumen adecuados para la producción de la representación de los datos a firmar.

- La aplicación de firma electrónica utilizará los formatos de entrada de firma electrónica adecuados para la producción de la firma de los datos a firmar.

- La aplicación de firma electrónica tiene que garantizar la producción correcta de la representación de los datos a firmar.

7.5. La seguridad de los procesos con el firmante

En este apartado presentamos la seguridad de los procesos con el firmante – concretamente, de la interfaz entre el usuario y la aplicación – y la autenticación del usuario por parte de la aplicación.

La sección no incluye ningún aspecto relativo a la interacción segura entre la aplicación y el dispositivo (autenticación entre los dos elementos y comunicación segura posterior), cuestiones que ya se han explicado anteriormente.

Podemos agrupar los requisitos en las categorías siguientes:

- Requisitos de interacción segura entre el firmante y la aplicación.
- Requisitos de identificación y autenticación del firmante.

7.5.1. Los requisitos de interacción segura entre el firmante y la aplicación[101]

La interacción que se establece entre la aplicación de firma electrónica y el firmante es de vital importancia, puesto que el componente de interacción con el firmante se responsabiliza de captar la voluntad del firmante y traducirla correctamente a los procesos de creación de firma que se imputarán a la persona.

Evidentemente, esta problemática sólo existe cuando el dispositivo seguro de creación de firma electrónica delega a la aplicación la autenticación del firmante, porque, en caso contrario, sencillamente se aplica la política de seguridad del dispositivo que es lo que pasa en el caso de la actuación administrativa automática.

[101] CEN CWA 14170, sección 10.

7.5.2. Los requisitos de identificación y autenticación del firmante[102]

La aplicación de firma electrónica puede gestionar los mecanismos de identificación y autenticación del firmante en colaboración con el dispositivo – seguro – de creación de firma electrónica.

Esta posibilidad depende, en realidad, del proveedor del dispositivo seguro, ya que si su política es autenticar directamente, mediante su propia interfaz de usuario, como hemos visto, entonces la aplicación no se tendrá que interponer en aquella interacción directa.

Sin embargo, si el dispositivo de creación de firma no dispone de interfaz con el firmante, o cuando esta opción se pueda configurar a voluntad del firmante (mediante la correspondiente interfaz de gestión administrativa del dispositivo), la aplicación de firma electrónica se podrá hacer cargo de los aspectos de autenticación del firmante, siempre implantando una serie de medidas de seguridad.

En el caso de la actuación administrativa automatizada, los requisitos de identificación y de autenticación resultan aplicables en el momento de puesta en marcha de la aplicación, ya que ésta tiene que tener acceso a la clave privada del sello de órgano, administración pública o entidad de derecho público.

Las amenazas identificadas son las siguientes:

- Uso no autorizado del dispositivo – seguro – de firma electrónica. Consiste en el hecho de que una persona no autorizada obtiene acceso al dispositivo de creación de firma y, en consecuencia, puede falsificar firmas.

- Divulgación, por la aplicación de firma, de los datos de autenticación del firmante. Consiste en el hecho que los datos de autenticación del firmante, que la aplicación de firma conoce, son divulgados a terceras personas.

[102] CEN CWA 14170, sección 11.

- Introducción accidental de datos incorrectos de autenticación del firmante.

- Adivinamiento de los datos de autenticación del firmante. Consiste en el hecho de que un atacante adivina los datos de autenticación del firmante, por suerte o por un ataque de fuerza bruta.

- Intercepción y mal uso posterior de los datos de autenticación del firmante. Consiste en el hecho de que una tercera persona intercepta los datos de autenticación del firmante introducidos mediante el teclado del ordenador personal, o el teclado del dispositivo, y las utiliza posteriormente para suplantar la identidad del firmante.

- Compromiso del secreto de los datos de autenticación del firmante. Consiste en el hecho que una tercera persona obtiene los datos de autenticación del firmante sin romper la seguridad de la aplicación de firma electrónica, o del dispositivo seguro de firma electrónica, y los utiliza posteriormente para suplantar la identidad del firmante.

- Visualización, por la aplicación de firma, de los datos de autenticación del firmante. Consiste en el hecho de que la aplicación muestra los datos de autenticación del firmante que éste introduce, cosa que hace que puedan ser observados y conocidos por terceras personas.

- Error de tecleo de unos nuevos datos de autenticación del firmante durante el proceso de cambio de estos datos. Consiste en el hecho de que el firmante no podrá cambiar sus datos de autenticación, de manera que tendrá que conservar unos datos de autenticación que, con el tiempo, perderán fuerza.

Los requisitos de seguridad correspondientes son los siguientes:

- La aplicación de firma electrónica, cuando sea responsable de la autenticación del firmante, deberá proveer una función para llevar a cabo este proceso de manera segura.

- Cuando los datos de autenticación del firmante estén almacenados en la aplicación de firma electrónica, se deberán preservar de manera confidencial y se tendrán que borrar cuando ya no sean necesarios.

- La aplicación de firma electrónica, de manera coordinada con el dispositivo seguro de firma electrónica, deberá permitir diversos intentos de autenticación mediante un contador y una función de bloqueo, en caso de superación de los intentos permitidos. La aplicación no deberá dar información sobre el tipo de error cometido por la persona que se autentica.

- La aplicación de firma electrónica debe funcionar de manera coordinada con el dispositivo de firma electrónica en todo aquello referido a la política de seguridad de los datos de autenticación (especialmente longitudes de claves y semántica de la contraseña), y no debe impedir aplicar la política de cambio de contraseña del dispositivo de firma electrónica.

- La aplicación de firma que gestione la autenticación del firmante debe implantar una ruta fiable desde el teclado del ordenador, o desde el lector de tarjeta, hasta el dispositivo de firma electrónica.

- La aplicación de firma debe implantar una función de cambio de los datos de autenticación de firma, excepto cuando su política de seguridad lo prohíba y esta prohibición no suponga una interferencia con la política de cambio de contraseña del dispositivo de firma electrónica.

- La aplicación de firma electrónica no mostrará los datos de autenticación de firma, sino uno o más símbolos para indicar el tecleo de los datos. Estos símbolos no revelarán los datos de autenticación ni permitirán adivinarlos.

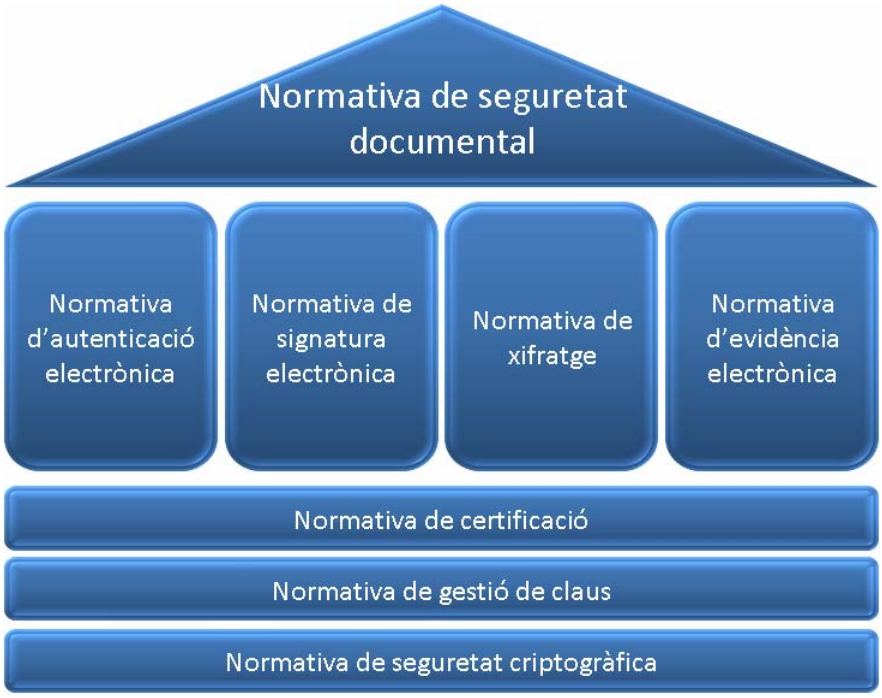
- La aplicación de firma electrónica requerirá la introducción dos veces de unos nuevos datos de autenticación y comprobará que los dos son idénticos antes de entregarlos al dispositivo de firma para el cambio.

8. Las normativas de seguridad criptogràfica de la aplicación de actuación administrativa automatizada

En este apartado se tratan las normativas de seguridad criptográfica de la aplicación de actuación administrativa automatizada. Analizamos el cuerpo normativo que se requiere para el aseguramiento de la seguridad de la aplicación, y, en especial, las normativas de firma electrónica, que desarrollamos de una manera particularmente intensa por su relevancia en términos de validez formal de los actos automáticos.

Las normativas de seguridad se estructuran en forma de documentos específicos de seguridad que hay que insertar dentro de la estructura documental del proceso general de seguridad de la organización. Cada documento de normativa implementa controles definidos por la norma ISO/IEC 27002:2005 y por otras normas relevantes.

A continuación se presenta de forma esquemática el conjunto de normas de seguridad criptográfica:



8.1. La normativa de seguridad documental

La normativa de seguridad documental se aplica a los diferentes tipos de documentos a formalizar y concreta de manera detallada la aplicación de las normativas y los estándares de autenticación, firma electrónica, cifrado y evidencia electrónica, cuando proceda.

Esta normativa se alinea con los requisitos de seguridad de gestión documental, de acuerdo con las normas ISO 15489 y MoReq 2, y se despliega en forma de estándares técnicos obligatorios para documentos tipo y expedientes concretos en guías o recomendaciones y en procedimientos operativos.

Asimismo, es necesario concretar un catálogo de formatos documentales electrónicos a utilizar (PDF, ODF, Word, WS, S/MIME ...) a efectos de establecer las normas de seguridad oportunas para cada formato.

Los contenidos principales son los siguientes:

- Establecimiento de principios generales de seguridad documental de acuerdo con la legislación (p. ej., Ley 11/2007).
    - Protección de datos personales.
    - Seguridad mínima.
    - Proporcionalidad.
    - Accesibilidad a la información y multicanalidad.
- Requisitos legales de seguridad documental.
    - Entradas de documentos.
    - Producción de documentos y copias.
    - Salida de documentos.
    - Formación de expedientes, conservación y archivo.

- Requisitos de gestión documental segura.

    - Producción de documentos originales electrónicos.

        - Originales internos (resolución).
        - Originales dirigidos a los ciudadanos (notificación).
        - Originales para publicar (edicto).

    - Producción de copias electrónicas.

        - Copia auténtica de documento original interno, para entregar al
        - ciudadano, si procede con cambio de formato (copia auténtica de una resolución).
        - Copia auténtica de documento externo, con cambio de soporte (digitalización) o de formato (de un formato ofimático a un formato de preservación).

Algunas aplicaciones de la norma son las siguientes:

- Estándar técnico de seguridad documental de resolución administrativa.
- Estándar técnico de seguridad documental de publicación.
- Estándar técnico de seguridad documental de factura electrónica.
- Estándar técnico de seguridad documental de expediente indizado.
- Estándar técnico de gestión de objetos de firma electrónica.

8.2. La normativa de autenticación

La normativa de autenticación concreta el conjunto de normas para la autenticación de una persona por medios electrónicos utilizando certificados de clave pública y otros mecanismos criptográficos y no criptográficos.

Esta normativa permite el cumplimiento de las secciones 9.1.2, 10.6.2, 10.8.2, 10.9.1, 11.2.3, 11.3.3, 11.4.2, 11.4.3, 11.5.2, 11.5.4, 11.5.6, 11.7.1 y 12.3.1 de la norma

ISO/IEC 27002:2005. Se despliega en forma de estándares obligatorios referidos a niveles de autenticación (alto, medio, bajo) y estándares de mecanismos de autenticación, en guías para la aplicación de mecanismos de autenticación y en procedimientos operativos.

Los actos electrónicos, así como los accesos a sistemas de información, se tienen que llevar a cabo dentro de un marco de trabajo que imponga la autenticación de los usuarios.

Tienen que existir una o diversas normativas de autenticación por escrito (o en soporte informático), firmadas debidamente (cuándo ocurra, electrónicamente), que determinen las condiciones de seguridad que hay que aplicar a los procedimientos de autenticación

En algunos casos, el mecanismo de autenticación puede hacer uso de mecanismos criptográficos basados en certificados digitales X.509v3.

Los contenidos principales son los siguientes:

- Información general.
    - Identificación de la normativa, consistente en identificación numérica y título textual correspondiente a la normativa.
    - Fecha de emisión.
    - Identificación del emisor de la normativa.
    - Periodo de validez de la normativa, con indicación de la entrada en vigor y la duración (si procede, indefinida).
    - Ámbito de aplicación de la normativa, con indicación del objetivo (a qué se aplica la normativa) y el subjetivo (a quien se aplica la normativa).

- Identificación.

    - Qué datos del certificado serán utilizados para la identificación de la persona o la entidad que se autentica.

    - Por ejemplo, se podría indicar que la identificación se hará mediante el dato NIF contenida al SubjectName del certificado. También se podrían establecer normas relativas a la identificación practicada por el prestador que emitió el certificado.

- Autenticación.

    - Normas relativas a protocolos y algoritmos. Por ejemplo, se podría indicar que la autenticación se realizará utilizando TLS 1.0, con determinados algoritmos de intercambio de claves y de cifrado.

    - Normas relativas al uso de prestadores de servicios de certificación, en el que se indiquen los certificados admitidos que se consideran válidos para esta acción de autenticación, así como los prestadores autorizados correspondientes.

    - Cuando proceda, hay que indicar el nivel de clasificación de CATCert sobre los certificados admitidos.

    - Normas sobre los puntos fiables para la construcción de rutas de certificados válidos, como las identificaciones de las entidades de certificación a raíz de los prestadores admitidos, como también normas sobre la gestión de estos certificados.

    - Normas sobre las rutas de certificación, con la indicación de si se podrán establecer otros modelos de confianza diferentes del jerárquico.

    - Normas relativas al uso de la información de estado de los certificados, indicando la obligatoriedad de verificar la firma electrónica y la forma de hacerlo entre las opciones siguientes:

- Uso de la entidad de validación de CATCert (administraciones públicas catalanas) u otros (sector privado).

- Uso de listas de revocación de certificados emitidas por el prestador de servicios de certificación.

- Uso del servicio de consulta en línea de certificados (OCSP) del prestador de servicios de certificación, cuando esté disponible.

- Uso de otros mecanismos de consulta de estado de certificados, cuando éstos estén disponibles (consulta web en el Registro de certificados).

Algunas aplicaciones de la norma son las siguientes:

- Estándar técnico de autenticación web (SSL/TLS).
- Estándar técnico de autenticación de servicios web (WSS).

8.3. La normativa de firma electrónica

La normativa de firma electrónica define cómo se tiene que generar la firma, con qué certificados, qué controles se aplicarán para verificar los permisos y los privilegios, si la firma se sellará con la fecha y la hora, de qué manera se verificarán los certificados, qué algoritmos se podrán utilizar para firmar y, muy especialmente, qué quiere decir legalmente el acto de firmar y qué controles de software se aplicarán para garantizar la autenticidad de la voluntad del firmante.

La normativa se despliega en forma de estándares técnicos de niveles de firma (alto, medio, bajo) y estándares de firma para los diferentes tipos de actos, en guías de firma (PDF, ODF, Word, WS, S/MIME ...) y procedimientos de firma.

Los actos y las manifestaciones de voluntad efectuados con medios electrónicos, cuando generan documentos con relevancia para el procedimiento administrativo, se tienen que firmar electrónicamente.

Debe existir una o diversas normativas de firma electrónica por escrito (o en soporte informático), firmadas debidamente (cuándo ocurra, electrónicamente), que determinen las condiciones de seguridad que hay que aplicar a los procedimientos de firma electrónica.

La normativa de firma electrónica debe hacer uso de mecanismos criptográficos basados en certificados digitales X.509v3 (normativa de firma electrónica adelantada) y, cuando ocurra, utilizar dispositivos seguros de creación de firma electrónica (normativa de firma electrónica reconocida).

Los contenidos principales son los siguientes:

- Información general.
    - Identificación de la normativa, consistente en identificación numérica y título textual correspondiente a la normativa.
    - Fecha de emisión.
    - Identificación del emisor de la normativa.
    - Periodo de validez de la normativa, con indicación de la entrada en vigor y la duración (si procede, indefinida).
    - Ámbito de aplicación de la normativa, con indicación del objetivo (a qué se aplica la normativa) y el subjetivo (a quien se aplica la normativa).
- Significado y manifestaciones vinculantes.
    - Describe qué quiere decir, fácticamente y legalmente, el hecho de producir una firma electrónica, así como otras manifestaciones

colaterales, en especial referidas al apoyo normativo a la firma electrónica o al acto y al reconocimiento correspondiente.

- Es la manifestación semántica explícita del acto y el compromiso (resolver favorablemente), y permite identificar de manera automática los documentos en consideración a los tipos de acto (muy importante a efectos del mantenimiento de la validez de la firma).

- Normas sobre aportación de datos de verificación de firma, por el firmante o, cuando proceda, por terceras personas, incluyendo:

  - El documento o el registro de transacción a firmar.

  - La identificación del firmante, en forma de certificado digital.

  - La fecha y la hora del acto.

  - La identificación de la política de firma electrónica aplicable.

  - La verificación de la firma, en forma documentada.

  - Las evidencias que sustentan la verificación practicada (como listas de revocación de certificados, consultas OCSP o informes de la entidad de validación de CATCert).

  - La fecha y la hora de la verificación de la firma.

- Validación de firma.

  - Normas relativas a protocolos y algoritmos. Es muy importante alinearlas con las recomendaciones del CNI-CCN-CERT en materia de firma electrónica (Guía CCN-STIC-405).

  - Normas relativas al uso de prestadores de servicios de certificación, en el que se indiquen los certificados admitidos que se consideran válidos

para esta acción de autenticación, así como los prestadores autorizados correspondientes.

- Cuando proceda hay que indicar el nivel de clasificación de CATCert sobre los certificados admitidos.

- Normas sobre los puntos fiables para la construcción de rutas de certificados válidos, como las identificaciones de las entidades de certificación a raíz de los prestadores admitidos, como también normas sobre la gestión de estos certificados.

- Normas sobre las rutas de certificación, con la indicación de si se podrán establecer otros modelos de confianza diferentes del jerárquico.

- Normas relativas al uso de la información de estado de los certificados, indicando la obligatoriedad de verificar la firma electrónica y la forma de hacerlo entre las opciones siguientes:

  - Uso de la entidad de validación de CATCert (administraciones públicas catalanas) u otros (sector privado).

  - Uso de listas de revocación de certificados emitidas por el prestador de servicios de certificación.

  - Uso del servicio de consulta en línea de certificados (OCSP) del prestador de servicios de certificación, cuando esté disponible.

  - Uso de otros mecanismos de consulta de estado de certificados, cuando éstos estén disponibles (consulta web en el Registro de certificados).

- Normas sobre el uso de roles, indicando si se utilizan y se indican dentro de la firma electrónica y, en caso afirmativo, si son roles alegados que habrá que comprobar o si son roles certificados:

- En este segundo caso, habrá que implantar una entidad de certificación de atributos que emita los certificados correspondientes.

- Normalmente esta posibilidad no se utiliza, aunque complementa el uso de certificados generalistas.

o Uso del sellado de fecha y hora, y de otras informaciones relativas al tiempo:

- La necesidad o no de utilizar sellos de fecha y hora criptográficos, y, en caso afirmativo, el formato y la normativa técnica y jurídica aplicables al sello de fecha y hora.

- La necesidad de que la manifestación de la fecha y la hora referida anteriormente se incorpore como un atributo en la firma electrónica, y si este atributo se firmará o no.

- La necesidad de que otras acciones sobre una firma como la verificación de ésta incorporen sellos de fecha y hora u otras manifestaciones sobre la fecha y la hora de la acción correspondiente.

- La precisión y la calidad de la manifestación de la fecha y de la hora, como también la sincronización de las fuentes de tiempo fiables con la hora UTC.

- Otras normas.

o Normas sobre formatos de firma electrónica (PKCS#7/CMS o XMLDSig/XAdES).

o Impresión del documento firmado electrónicamente (código de verificación electrónica).

- Visualización gráfica de la firma electrónica antes y después de la verificación.

Algunas aplicaciones de la norma son las siguientes:

- Estándar técnico de firma electrónica de actos de voluntad (definitivos/trámite).
- Estándar técnico de firma electrónica de actos de juicio.
- Estándar técnico de firma electrónica de actos de conocimiento.
- Estándar técnico de firma electrónica de actos de deseo.
- Estándar técnico de firma electrónica de formato documental PDF.

8.4. La normativa de cifrado

La normativa de cifrado concreta el conjunto de normas para el cifrado de comunicaciones y documentos por medios electrónicos utilizando certificados de clave pública y otros mecanismos criptográficos, de conformidad con la sección 12.3.1 de la norma ISO/IEC 27002:2005.

La normativa se despliega en forma de estándares de nivel de confidencialidad (alto, medio, bajo), estándares de mecanismos de cifrado o guías de cifrado (recomendaciones en relación con el cifrado).

Las informaciones sensibles, así como las que contengan datos personales de nivel alto, se tienen que cifrar con el fin de proteger la confidencialidad.

Debe existir una o diversas normativas de cifrado por escrito (o en soporte informático), firmadas debidamente (cuándo ocurra, electrónicamente), que determinen las condiciones de seguridad que hay que aplicar en los mecanismos de cifrado.

En algunos casos, el mecanismo de cifrado puede hacer uso de mecanismos criptográficos basados en certificados digitales X.509v3.

Los contenidos principales son los siguientes:

- Información general.
    - o Identificación de la normativa, consistente en identificación numérica y título textual correspondiente a la normativa.
    - o Fecha de emisión.
    - o Identificación del emisor de la normativa.
    - o Periodo de validez de la normativa, con indicación de la entrada en vigor y la duración (si ocurre, indefinida).
    - o Ámbito de aplicación de la normativa, con indicación del objetivo (a qué se aplica la normativa) y el subjetivo (a quien se aplica la normativa).
- Cifrado.
    - o Normas relativas a protocolos y algoritmos. Por ejemplo, se podría indicar que el mecanismo a utilizar es XML Encryption, con determinados algoritmos de cifrado.
    - o Normas relativas al uso de prestadores de servicios de certificación, en el que se indiquen los certificados admitidos que se consideran válidos para esta acción de autenticación, así como los prestadores| autorizados correspondientes
    - o Cuando proceda, hay que indicar el nivel de clasificación de CATCert sobre los certificados admitidos.
    - o Normas sobre los puntos fiables para la construcción de rutas de certificados válidos, como las identificaciones de las entidades de certificación a raíz de los prestadores admitidos, como también normas sobre la gestión de estos certificados.

- Normas sobre las rutas de certificación, con la indicación de sí se podrán establecer otros modelos de confianza diferentes del jerárquico.

- Normas relativas al uso de la información de estado de los certificados, indicando la obligatoriedad de verificar la firma electrónica y la forma de hacerlo entre las opciones siguientes:

  - Uso de la entidad de validación de CATCert (administraciones públicas catalanas) u otros (sector privado).

  - Uso de listas de revocación de certificados emitidas por el prestador de servicios de certificación.

  - Uso del servicio de consulta en línea de certificados (OCSP) del prestador de servicios de certificación, cuando esté disponible.

  - Uso de otros mecanismos de consulta de estado de certificados, cuando éstos estén disponibles (consulta web en el Registro de certificados).

Algunas aplicaciones de la norma son las siguientes:

- Estándar técnico de cifrado SSL/TLS/WTLS.
- Estándar técnico de cifrado de servicios web (WSS).
- Estándar técnico de cifrado CMS.
- Estándar técnico de cifrado XML.

8.5. La normativa de evidencia electrónica

La normativa de evidencia electrónica concreta el conjunto de normas para la producción y la gestión de todo el ciclo de vida de los registros de actividad a efectos

de disponer de registros con valor probatorio suficiente (BS 10008:2008), sobre todo en el caso de las actuaciones no formalizadas documentalmente (NIST SP 800-92).

La normativa se despliega en forma de estándares de gestión de registros de actividad (*logs*) para la publicación de informaciones o los registros internos, en procedimientos de evidencia electrónica y en guías de aplicación de la normativa de evidencia electrónica, con recomendaciones.

Los contenidos principales son los siguientes:

- Generación y captura de evidencias.
    - Interpretación y extracción de datos.
    - Filtraje de acontecimientos.
    - Agregación de eventos.
- Almacenaje de evidencias.
    - Rotación de registros.
    - Archivo, incluyendo la retención y la preservación.
    - Compresión de registros.
    - Reducción de registros.
    - Conversión de registros.
    - Normalización de registros.
    - Comprobación de integridad de registros.
- Análisis de evidencias.
    - Correlación de eventos.
    - Revisión de registros de seguridad.
    - Informes sobre registros de seguridad.
    - Informes de evidencia.
- Disposición (eliminación) de los registros de seguridad.

8.6. La normativa de certificación

La normativa de certificación define como es debido prestar el servicio de certificación. Deben disponer de ella los prestadores de servicios de certificación para sus propios servicios, o los usuarios, para definir los requisitos y las condiciones que exigirán a los prestadores que les suministren certificados (adquisición o admisión de certificados).

La normativa se desarrolla en forma de estándares de certificación, tipo de certificados a adquirir o admitir – incluyendo certificados de persona física, certificados de persona jurídica, certificados de entidad sin personalidad, certificados de sello de órgano... –, de procedimiento de admisión de certificados, procedimientos de adquisición de certificados, y en una base datos de certificados admitidos.

Los contenidos principales son los siguientes:

- Información general.
    - Presentación.
        - Tipo y clases de certificados.
        - Relación entre la normativa de certificación y otros documentos.
    - Nombre del documento e identificación.
    - Comunidad de usuarios de certificados, de acuerdo con la ley aplicable (p. ej., Ley 11/2007).
        - Prestadores de servicios de certificación.
        - Entidades de registro.
        - Suscriptores y entidad usuaria de los certificados.

- Uso de los certificados.

  - Tal vez el aspecto más importante es definir adecuadamente para qué finalidad tiene que servir se admite el uso de cada tipo de certificado descrito anteriormente.

  - Por ejemplo, uso general en el procedimiento administrativo, uso tributario o autorizaciones de uso específicas para certificados de entidad sin personalidad jurídica.

- Administración de la normativa.

  - Organización que administra la especificación.
  - Datos de contacto de la organización.
  - Procedimiento de aprobación.

- Requisitos de operación del ciclo de vida de los certificados.

  - Solicitud de emisión de certificado.

    - Legitimación para solicitar la emisión.
    - Procedimiento de alta; responsabilidades.

  - Aceptación del certificado.
  - Uso del par de claves y del certificado.
  - Renovación de certificados sin renovación de claves.
  - Renovación de certificados con renovación de claves.
  - Modificación de certificados.
  - Revocación y suspensión de certificados.

    - Causas de revocación de certificados.Legitimación para solicitar la revocación.
    - Obligación de consulta de información de revocación de certificados.
    - Causas de suspensión de certificados.

- Quién puede solicitar la suspensión.

- Servicios de comprobación de estado de certificados.

  - Características de los servicios.
  - Disponibilidad de los servicios.

- Finalización de la suscripción.

- Perfiles de certificados y listas de revocación de certificados.

  - Perfiles de certificados admitidos.

    - Formatos de nombres.
    - Restricciones de nombres.

  - Perfil de la lista de revocación de certificados.

- Requisitos legales.

  - Obligaciones y responsabilidad civil.

    - Suscriptores de los certificados.
    - Entidad usuaria de los certificados, en su actuación como tercero.

  - Protección de datos personales.
  - Conformidad con la ley aplicable.

8.7. La normativa de gestión de claves

La normativa de gestión de claves detalla las normas de uso en relación con las claves criptográficas, de acuerdo con la normativa de seguridad criptográfica, para

cumplir los controles que prevé la norma ISO/IEC 27002:2006, secciones 12.3.1 y 15.1.6, y sobre la base de las recomendaciones de mejores prácticas contenidas en la publicación especial 800-57, partes 1 y 2, del NIST (EE.UU.).

La normativa se despliega en forma de estándares de infraestructura técnica de gestión de claves, procedimientos previos a las operaciones de gestión de claves, procedimientos operativos de gestión de claves y procedimientos posteriores de gestión de claves.

Todas las claves criptográficas se tienen que proteger de la modificación, la pérdida o la destrucción. Las claves criptográficas privadas y las claves secretas se tienen que proteger contra la divulgación no autorizada.

El hardware utilizado para generar, almacenar y archivar las claves criptográficas se tendría que proteger físicamente.

Los contenidos principales son los siguientes:

- Estándares, procedimientos y métodos seguros en relación con estos aspectos:

    - Generación de claves por diferentes sistemas criptográficos y aplicaciones.
    - Generación y obtención de certificados de clavo pública.
    - Distribución de claves a los usuarios, incluyendo la activación una vez hayan sido recibidas.
    - Almacenamiento de claves, incluyendo la manera cómo obtienen acceso a las claves los usuarios autorizados.
    - Cambio o actualización de claves, incluyendo normas sobre el momento en que hace falta cambiar o actualizar las claves y el procedimiento aplicable.
    - Gestión de claves comprometidas.
    - Revocación de claves, incluyendo la retirada o la desactivación.
    - Archivo de claves, especialmente en caso de información cifrada que haya sido archivada.

  - Destrucción de claves.
  - Registro y auditoría de operaciones relativas a gestión de claves.

- Periodos de activación y desactivación de claves, para reducir el riesgo de compromiso, de manera que las claves se puedan utilizar sólo durante un plazo concreto, de acuerdo con las circunstancias y el análisis de riesgo.

- Procedimientos para garantizar la autenticidad de las claves públicas mediante entidades de certificación.

- En caso de que haya terceros prestadores de servicios relacionados con la criptografía, hay que establecer acuerdos de nivel de servicio que traten específicamente cuestiones de responsabilidad, fiabilidad de los servicios y tiempos de respuesta garantizados.

8.8. La normativa de seguridad criptográfica

La normativa de seguridad criptográfica especifica normas de uso en relación con la criptografía, incluyendo estándares para su implementación a la organización, con el objetivo de cumplir los controles que prevé la norma ISO/IEC 27002:2006, secciones 12.3.1 y 15.1.6, y sobre la base de las recomendaciones de mejores prácticas contenidas en la publicación especial 800-57, partes 1 y 2, del NIST (EE.UU.), como también de las guías STIC del CNI.

La normativa se despliega en forma de estándares de implementación de infraestructura criptográfica, estándares y procedimientos en relación con los algoritmos seguros, estándar de código seguro de verificación y guías de uso de la criptografía en las aplicaciones, con recomendaciones conformes a la legislación aplicable.

Los contenidos principales son los siguientes:

- La aproximación de la dirección con respecto al uso de controles criptográficos dentro de la organización, incluyendo los principios generales de protección de la información.

- El nivel requerido de protección, de acuerdo con el análisis de riesgo correspondiente, teniendo en cuenta el tipo, la fortaleza y la calidad de los algoritmos criptográficos correspondientes.

- Uso del cifrado para la protección de informaciones sensibles transportadas mediante dispositivos móviles, con medios o dispositivos removibles o a través de líneas de comunicación.

- Aproximación a la gestión de claves, incluyendo los métodos para tratar la protección de las claves criptográficas y la recuperación de información cifrada en caso de pérdida, compromiso o daño de las claves.

- Determinación de los roles y las responsabilidades relacionados con los aspectos siguientes:

    - Implementación de la normativa.
    - Gestión de claves, incluyendo la generación de claves.

- Los estándares para conseguir la implementación efectiva de la normativa en toda la organización, mediante controles técnicos y de procedimiento.

- La valoración de impacto del uso de información cifrada sobre controles basados en inspección de contenidos, como antivirus.

- Aspectos legales:

    - Restricciones sobre la importación y/o la exportación de hardware y software que ejecutan operaciones criptográficas.
    - Restricciones sobre la importación y/o la exportación de hardware y software diseñados para que se incorporen funciones criptográficas.
    - Restricciones sobre el uso del cifrado.

- Métodos obligatorios o voluntarios que permiten a las autoridades públicas el acceso a informaciones cifradas utilizando hardware o software para garantizar la confidencialidad.