Vol. XXII | Enero 2020 | **#64**

Revista Española de Control Externo

Índice

Presentación

PASCUAL SALA SÁNCHEZ
Director

Entre los objetivos fundamentales que se ha propuesto desde su origen la *Revista Española de Control Externo* está el de situarse en la vanguardia doctrinal respecto a los cambios que se van produciendo tanto en la actividad económico-financiera del Sector Público como en su control. La conveniencia de elaborar un ejemplar monográfico sobre modernización tecnológica del sector público y de las instituciones encargadas de fiscalizar y enjuiciar su gestión, resulta sobradamente justificada. Este n.º 64 recoge artículos de expertos nacionales e internacionales del mayor prestigio y, en consecuencia, puede resultar muy útil a quienes estudian o practican la vertiente tecnológica de la administración y control de las finanzas públicas.

El primer artículo se titula: *Transformación digital y control externo en Alemania: retos y oportunidades*. Un interesante trabajo aportado por Kay Scheller, Presidente del Tribunal de Cuentas de la República Federal de Alemania, en el que nos describe cómo está abordando dicha Institución la transformación digital de sus procedimientos fiscalizadores mediante una estrategia orientada a salvaguardar y optimizar, sistemática y gradualmente, la eficacia del control externo en un sector público tecnológicamente avanzado.

Siguiendo en el ámbito internacional, aparece a continuación el artículo de Janar Holm, Presidente del Tribunal de Cuentas de Estonia, bajo el título: *Transformación digital en el sector público de Estonia. Beneficios y desafíos para la Oficina Nacional de Auditoría*. Se trata de una aportación doctrinal con reflexiones muy útiles sobre las ventajas y peligros de la administración electrónica, así como respecto a los cambios organizativos y funcionales que la generalización del entorno digital está obligando a afrontar al Supremo Órgano Fiscalizador Estonio.

Seguidamente encontramos el artículo: *La transformación digital en el Tribunal de Cuentas: aprovechando las nuevas tecnologías para contribuir a la mejora en la gobernanza pública,* de María Dolores Genaro Moya, Consejera del Tribunal de Cuentas Español, a quien hay que agradecer el papel especialmente relevante que ha desarrollado para impulsar este ejemplar monográfico, así como su participación en el mismo a través del trabajo antes citado, en el que nos expone de manera ordenada el proceso de transformación digital del Sector Público en España, la respuesta a este desafío que se ha ido dando desde el Tribunal de Cuentas y el enfoque que será necesario aplicar en el futuro para que, tanto la gestión como el control, no vayan por detrás de la modernización tecnológica sino liderándola.

El Área de Normativa y Servicios de Ciberseguridad del Centro Criptológico Nacional participa en este ejemplar de la Revista con el trabajo: *La ciberseguridad y su relevancia en el Sector Público. El papel del Centro Criptológico Nacional*. El texto se basa en la idea, lógica y coherente, de que garantizar la ciberseguridad en el ciberespacio, al tiempo que se respeta la privacidad y la libertad de los ciudadanos, se ha convertido en una de las prioridades estratégicas de los países más desarrollados, debido a su impacto directo en la seguridad nacional, en la competitividad de las empresas y en la prosperidad de la Sociedad en su conjunto. Partiendo de esta concepción inicial, el artículo desarrolla con exhaustividad el papel que desempeña el Centro Criptológico Nacional para garantizar la seguridad en el uso de las tecnologías de la información y las comunicaciones.

La evolución histórica de la protección de datos hasta su situación actual, es el estimulante tema que desarrolla María Jesús Casado Robledo, Responsable de Seguridad de la Información de la Intervención General de la Administración del Estado, en su trabajo: *Proteger la información ha sido una constante a lo largo de la Historia*. La autora incide, muy especialmente, en la importancia de distinguir las áreas de competencia de los conceptos Seguridad de la información, Ciberseguridad y Seguridad informática, pues es necesario entender que la Seguridad de la Información tiene un alcance más amplio que el tecnológico.

La Letrada del Tribunal de Cuentas Miriam Cernuda Salama, aporta a este número de la Revista un artículo titulado: *Informatización del Tribunal de Cuentas; especial referencia a la implantación de las nuevas tecnologías aplicadas al ejercicio de la función jurisdiccional de enjuiciamiento contable*. Se trata de un documento doctrinal que resulta muy necesario para que quede completo este ejemplar monográfico de la Revista, ya que desarrolla concienzudamente el impacto de la modernización tecnológica sobre la función jurisdiccional del Tribunal de Cuentas y lo hace, acertadamente, partiendo de la evolución y situación de las tecnologías de información y comunicaciones en los ámbitos administrativo y judicial del Estado.

El foro académico, en su vertiente investigadora, está representado por el artículo: *Blockchain: instrumento de transparencia y control del sector público,* de los profesores de la Universidad de Valencia José Luis Wanden-Berghe Lozano y Eliseo Fernández Daza. Tras definir el blockchain como una tecnología de bases de datos distribuidas, dónde la información se mantiene inmutable, verificable, consensuada y sin requerir de la existencia de un ente centralizador que intermedie para dar confianza, los autores identifican con claridad las razones por las que este instrumento puede beneficiar a la contabilidad y a la auditoría.

El apartado de artículos de este ejemplar n.º 64 incluye el trabajo: *La tecnología blockchain y su pretendida aplicación a la contratación pública como mecanismo para lograr mayor integridad,* de José Luis Quintana Cortés, socio del despacho jurídico Rodríguez Castaño Abogados. El texto aporta a este número monográfico de la Revista una visión del blockchain desde la perspectiva jurídica y un estudio original y laborioso de la aplicabilidad de este recurso tecnológico a la contratación pública.

La sección de artículos se cierra con el presentado por Antonio Minguillón Roy, Carlos García Burgos y Jorge Soler Iranzo, auditores de la Sindicatura de Cuentas de la Generalitat Valenciana, en el que bajo el título *Auditoría de la ciberseguridad de los principales ayuntamientos*

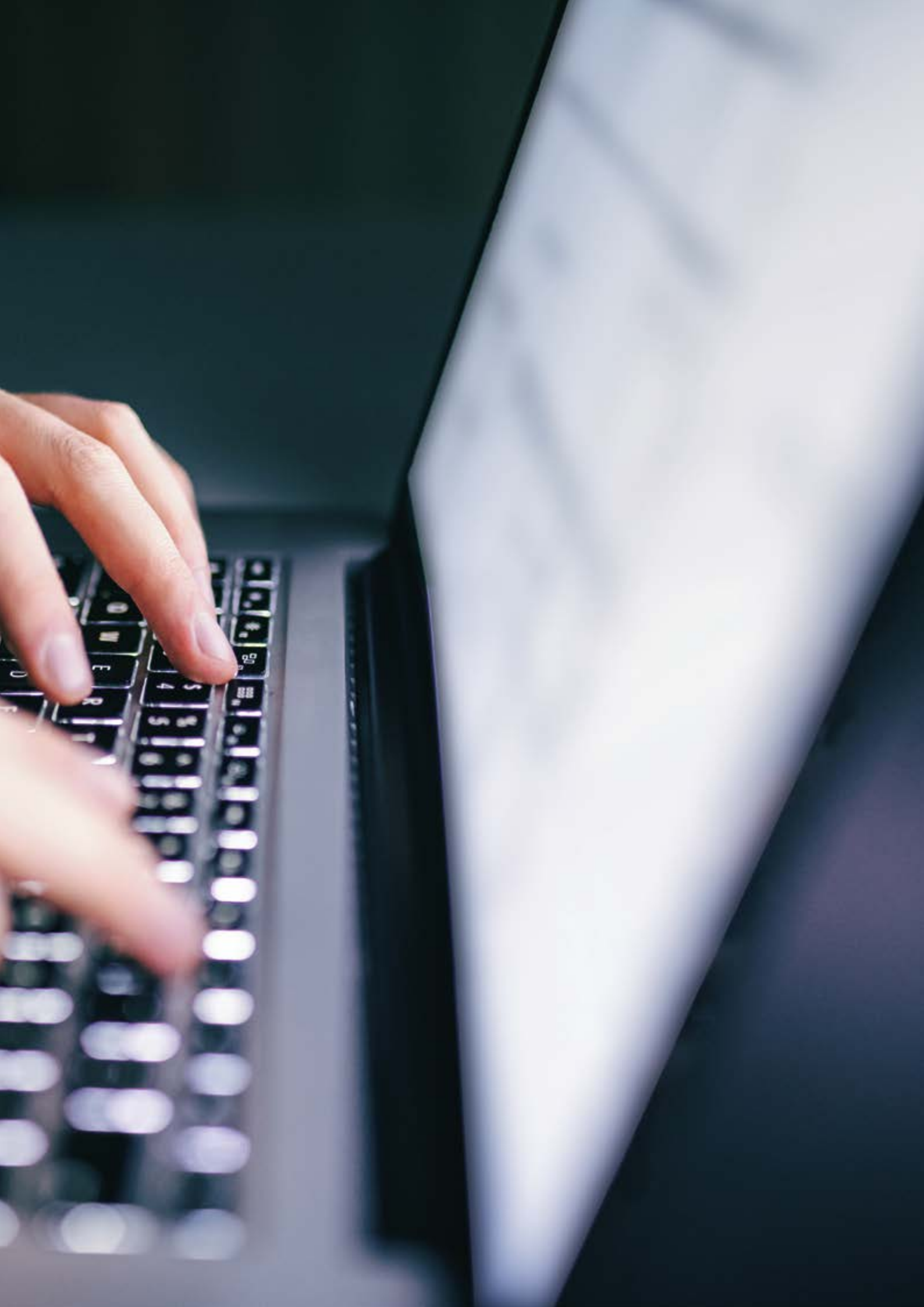
de la Comunidad Valenciana, se aporta un estudio práctico que no solo permite hacer un diagnóstico preciso de la situación en las corporaciones locales examinadas, sino también extraer conclusiones extrapolables a todo el Sector Público Local.

Finalmente, como en todos los ejemplares anteriores, aparece en el apartado *Legislación y Jurisprudencia* una recopilación exhaustiva y sistematizada de las principales normas de derecho positivo y criterios jurisprudenciales que han visto la luz en el tercer cuatrimestre del año 2019, y que aportan a la Revista Javier Medina Guijarro, Consejero del Tribunal de Cuentas, y José Antonio Pajares Giménez, Letrado de dicha Institución y miembro del Consejo Editorial de nuestra publicación.

Estoy convencido de que este monográfico sobre transformación digital va a resultar de extraordinario interés para estudiosos y profesionales de la modernización tecnológica del Sector Público y de su control, pues su contenido abarca trabajos procedentes de los ámbitos internacional y nacional, de las áreas de gestión y de las de control fiscalizador y jurisdiccional, así como, del mundo académico y del profesional, pero siempre con un denominador común, todos los artículos han sido elaborados por especialistas de acreditado prestigio.

ARTÍCULOS

Transformación digital



Transformación digital y control externo en Alemania: retos y oportunidades

KAY SCHELLER
Presidente del Tribunal Federal de Cuentas de Alemania

RESUMEN

La digitalización conlleva para el control externo no sólo numerosos retos, sino también oportunidades. Se trata de mucho más que convertir informaciones análogas en un formato digital. Por este motivo, el Tribunal Federal de Cuentas aspira a la transformación digital del propio procedimiento fiscalizador. Dicha transformación puede conducir a una nueva metodología fiscalizadora, nuevas conclusiones y nuevos productos de auditoría. No obstante, el proceso está sujeto a los límites establecidos por nuestro mandato constitucional y al marco legal vigente. En un mundo digitalizado, nuestra misión seguirá siendo la misma: desempeñar de la mejor manera nuestras funciones fundamentales, es decir, fiscalizar, asesorar e informar.

Para estructurar la transformación digital de nuestra actividad fiscalizadora, hemos elaborado un esquema de digitalización que indica tres campos de actuación con los siguientes títulos: ¿Qué auditamos? ¿Cómo auditamos? y ¿Qué instrumentos utilizamos para auditar?

Para lograr la transformación digital de la actividad fiscalizadora, hemos optado por un enfoque ágil que se apoya en la idea común de establecer un marco general que puede ser adaptado por las cincuenta divisiones de auditoría individuales del Tribunal Federal de Cuentas en función de sus necesidades que están inscritas en el esquema de digitalización mencionado. Gracias a este enfoque somos capaces de salvaguardar y optimizar sistemática y gradualmente nuestra capacidad fiscalizadora en un mundo digitalizado.

PALABRAS CLAVE

esquema de digitalización
transformación digital | enfoque ágil
Tribunal Federal de Cuentas de Alemania
retos

ABSTRACT

Digitization brings not only numerous challenges, but also opportunities for external control. It is about much more than converting analog information into a digital format. For this reason, the Federal Court of Audit aims at the digital transformation of the audit procedure itself. Such a transformation can lead to a new audit methodology, new conclusions and new audit products. However, the process is subject to the limits established by our constitutional mandate and the legal framework in force. In a digitized world, our mission will remain the same: to best perform our core functions, i.e., to audit, advise and report.

To structure the digital transformation of our auditing activity, we have developed a digitization scheme that indicates three fields of action under the following headings: What do we audit? How do we audit? and What instruments do we use to audit?

To achieve the digital transformation of the auditing activity, we have opted for an agile approach based on the common idea of establishing a general framework that can be adapted by the fifty individual auditing divisions of the Federal Court of Audit according to their needs, which are included in the aforementioned digitization scheme. Thanks to this approach we are able to systematically and gradually safeguard and optimize our auditing capacity in a digitized world. However, there is still a long way to go before we will be able to implement some of these ideas.

KEYWORDS

digitization scheme
digital transformation | *agile approach*
Federal Court of Audit of Germany
challenges

1. El concepto de la digitalización

La digitalización significa progreso, bienestar y cambio. Es una evolución que concierne a todos los ámbitos de la vida y del trabajo en cuanto al gobierno, la administración pública, la economía y al sector privado. Se trata de un fenómeno global que se caracteriza por un desarrollo particularmente dinámico y que frecuentemente es presentado como objetivo político.[1] Aunque se plantea la cuestión de si es imperativo digitalizar todos los ámbitos de la administración pública, la digitalización ya ha empezado de facto a transformar sustancialmente la integridad del entorno en el que el control externo desarrolla sus actividades.

Lo primero que se suele asociar a la digitalización de la actividad fiscalizadora son las nuevas posibilidades de analizar los datos. Sin embargo, es importante entender el alcance del impacto producido por la digitalización en la labor cotidiana de las Entidades Fiscalizadoras Superiores (EFS). La digitalización no sólo significa una simple adaptación de los métodos e instrumentos de análisis.[2] Se trata más bien de un proceso que afecta a todos los niveles estatales (Estado federal, Estados federados y entes municipales) y que supone una transformación de los métodos de trabajo, de los productos administrativos, del paisaje informático, de los requisitos de calificación para el personal nuevo y antiguo, de los procesos administrativos y de la cultura organizativa así como, y bastante frecuentemente a través de modificaciones legislativas, una adaptación de la cartera de actividades de las instituciones públicas.[3] Cada vez más, la digitalización está conduciendo a la interconexión de tareas administrativas a través de interfaces digitales con procesos administrativos de otras autoridades públicas en un contexto nacional e internacional, como por ejemplo cuando se trata de tramitar las solicitudes de asilo. Corresponderá a las EFS auditar estos importantes desarrollos sociales por el solo hecho de que las inversiones necesarias suponen una carga considerable para los presupuestos públicos.

La transformación digital del entorno interno y externo de la actividad fiscalizadora conducirá a nuevas conclusiones fiscalizadoras. Como la información a fiscalizar está frecuentemente disponible en forma digital, para auditar necesitamos introducir nuevos tipos de pruebas y establecer interfaces de comunicación con las entidades fiscalizadas. Debido al cambio impulsado por las tecnologías de información es también necesario desarrollar y cumplir normas adicionales que sirvan, por ejemplo, para mantener la calidad del procedimiento fiscalizador, que garanticen la protección de los datos e impidan su posible uso indebido.

A las EFS que asumen estos retos se les abren nuevas oportunidades, como por ejemplo, aplicar nuevas y eficientes herramientas fiscalizadoras, mejorar la corroboración de las pruebas fiscalizadoras y transmitir los resultados a través de nuevos formatos de comunicación. Así pues, la transformación digital representa no sólo un reto, sino también puede y debe facilitar el desempeño de las funciones fiscalizadoras definidas en la constitución.

1. Véase Hans Peter Bull, Digitalisierung als Politikziel -Teil I, publicado en: Report und Technik – Aufsätze, CR 7/2019.
2. Aroldo Cedraz de Oliveira, Control of Public Administration in the Digital Age, 2017, Presentation Chapter, página 30.
3. Un decreto del Gobierno Federal adoptado el 17 de diciembre de 2013 confirió al Ministerio Federal de Transportes e Infraestructura Digital la competencia para establecer una cobertura generalizada de la red de banda ancha que garantice el acceso de alta velocidad a internet en Alemania.

2. El contexto de la digitalización en Alemania

Por su estructura federal, Alemania se caracteriza por el alto grado de descentralización administrativa. Aparte del nivel federal, existen 16 Estados federados que poseen facultades autónomas que conciernen, entre otros, al ámbito de las finanzas y de la contabilidad pública. Por lo tanto, tenemos una estructura compleja desde el punto de vista de la legislación, la gobernanza, la jurisdicción, los presupuestos, la gestión de finanzas públicas y, por consiguiente, del control financiero externo. Por este motivo, en Alemania, la administración pública en general (incluido el Gobierno Federal), y las estrategias de transformación digital adoptadas por el sector público en concreto, forman parte de un escenario informático complejo y variado.

En la «Estrategia de implementación del Gobierno Federal: ¿Cómo configurar la digitalización?», publicada el 15 de noviembre de 2018 y modificada en septiembre de 2019, se identifican cinco campos que rigen la actuación gubernamental en todas las cuestiones relacionadas con la transformación digital.

CUADRO 1.
ESTRATEGIA DE DIGITALIZACIÓN DEL GOBIERNO FEDERAL

LOS CINCO CAMPOS DE ACTUACIÓN DE LA ESTRATEGIA DIGITAL

COMPETENCIA DIGITAL	INFRAESTRUCTURA Y EQUIPAMIENTO	INNOVACIÓN Y TRANSFORMACIÓN DIGITAL	SOCIEDAD Y TRANSICIÓN DIGITAL	MODERNIZACIÓN DEL ESTADO
invertir para aumentar los conocimientos de la ciudadanía, desde la infancia hasta la tercera edad	establecer, hasta finales de 2025, redes que permitan la transmisión de gigabits en zonas urbanas y rurales	promoción amplia e interprofesional de la industria 4.0	aumentar la calidad de vida, garantizando la seguridad	digitalizar todos los servicios públicos

Fuente: *Gobierno Federal.*

La decisión de implementar la estrategia digital fue precedida por una enmienda constitucional por la que se otorgó al Gobierno Federal el poder legislativo exclusivo para las cuestiones relativas a la digitalización de la administración pública.[4] Dicha reforma constitucional fue concebida para regular el acceso general y uniforme del Estado federal y de los Estados federados a sus servicios administrativos respectivos. En este contexto fue promulgada la Ley sobre la Mejora del Acceso en Línea a los Servicios Públicos,[5] cuyo objetivo es

4. Ley de Enmienda de la Constitución promulgada el 13 de julio de 2017, Boletín oficial del Estado federal I, página 2374.
5. Ley sobre la Mejora del Acceso en Línea a los Servicios Públicos, 14 de agosto 2017 (Boletín Oficial del Estado federal I, páginas 3122, 3138).

posibilitar la comunicación de la administración pública, la ciudadanía y las empresas a través de internet, independientemente de la hora y del lugar. También es preciso tener en cuenta las disposiciones del Reglamento General de Protección de Datos (RGPD) de la UE que han aumentado las exigencias en materia de recogida y procesamiento de datos.

Apoyándonos en lo anteriormente expuesto podemos extraer la siguiente pregunta clave: En lo que se refiere a los campos estratégicos de actuación de la administración federal, ¿quién determinará los pasos a seguir y el grado de la digitalización?: ¿se trata de las empresas que persiguen sus intereses económicos vinculados con la digitalización; de los gobiernos que fomentan los medios digitales intentando satisfacer las necesidades económicas o persiguiendo objetivos populares; de la ciudadanía que desea acceder, de forma sencilla y rápida, con su móvil, a unos servicios públicos digitalizados; o del personal de las administraciones públicas, y así también del personal de la EFS, que desea desarrollar de forma dinámica su ámbito de competencia?

Lo cierto es que la digitalización refuerza la interconexión del sector público y facilita la emisión de nuevos productos administrativos que pueden ser de utilidad para los responsables políticos, la ciudadanía y las empresas del sector privado. Por consiguiente, la respuesta a la pregunta de quién es el impulsor de innovación es la siguiente: Todos los actores tendrían que definir conjuntamente los siguientes pasos a tomar. Por ello, resulta crucial para las EFS a la hora de definir su estrategia de digitalización, comprender los procesos de transformación de las entidades fiscalizadas y alinear en consecuencia el grado de digitalización de sus propios procedimientos fiscalizadores.

Para garantizar que, en un mundo administrativo digitalizado, el Tribunal Federal de Cuentas pueda seguir ejerciendo de la mejor forma posible su mandato constitucional (controlar, asesorar, informar), hemos decidido adaptar nuestras capacidades, estructuras y procesos a las nuevas circunstancias, teniendo siempre en cuenta las exigencias relevantes en el ámbito de auditoría concreto.

3. La estrategia del Tribunal Federal de Cuentas

3.1. Mandato constitucional

Para comprender la estrategia de digitalización del Tribunal Federal de Cuentas es importante conocer las funciones legislativas y la estructura.

Nuestro mandato constitucional consiste en controlar la racionalidad económica y la regularidad de la gestión económico-financiera del Estado federal, así como de informar sobre los resultados de auditoría. Ello significa que sometemos a nuestra actividad fiscalizadora toda la gama de actividades del sector público federal, analizando si las operaciones de la administración federal cumplen con las disposiciones legales y si las autoridades han actuado conforme a los principios de eficiencia y eficacia. El Tribunal Federal de Cuentas examina los ingresos y los gastos anuales del Estado federal que ascienden a un importe superior a los 700 mil millones de euros. También son objetos de su control los patrimonios federales especiales, las entidades gestoras de la seguridad social y la actuación de los representantes federales en las empresas de derecho privado en las que el Estado federal tenga una participación.

El Tribunal Federal de Cuentas no está autorizado para dar instrucciones ni para imponer sanciones. Por ello, la implantación exitosa de sus recomendaciones fiscalizadoras depende exclusivamente de la contundencia de los argumentos que presente.

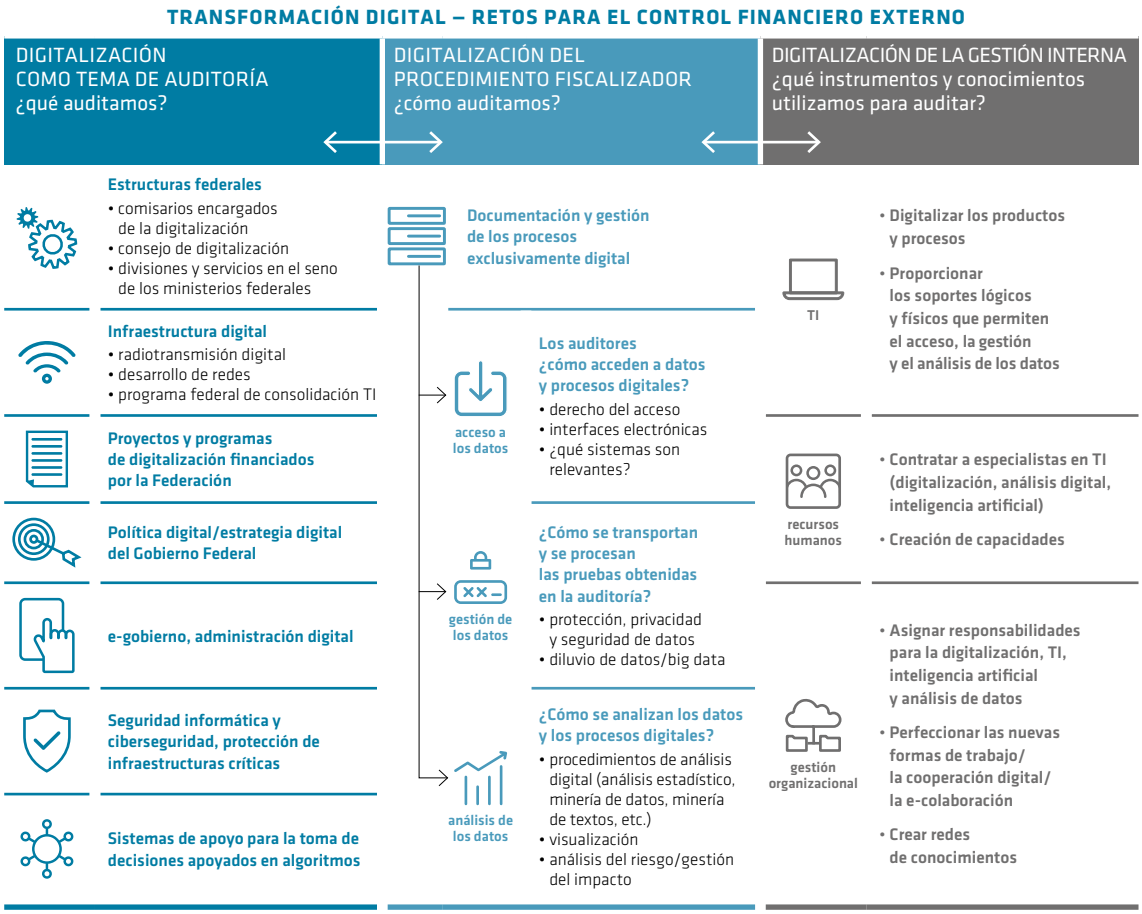
En este contexto, conviene también subrayar que el Tribunal Federal de Cuentas se caracteriza por una estructura colegial. Eso significa que la responsabilidad para el desempeño de sus funciones fiscalizadoras pertenece a los directores de los departamentos fiscalizadores y a los jefes de las divisiones de auditoría. Ellos integran los órganos colegiados bipersonales y deciden conjuntamente, y cuando proceda, junto al Presidente o Vicepresidente, sobre la programación y las misiones de auditoría, así como sobre los resultados fiscalizadores.

3.2. Esquema de digitalización y campos de actuación

Con el fin de crear unas bases sólidas para la digitalización de los procedimientos fiscalizadores, el Tribunal Federal de Cuentas ha elaborado un esquema en el que preguntas posibles son asignadas a tres diferentes campos de actuación interconectados entre sí:

- ¿Qué auditamos? (la digitalización como tema de auditoría)
- ¿Cómo auditamos? (la digitalización del procedimiento fiscalizador)
- ¿Qué instrumentos utilizamos para auditar? (la digitalización de la gestión interna)

CUADRO 2
ESQUEMA DE DIGITALIZACIÓN DEL TRIBUNAL FEDERAL DE CUENTAS



a) Campo de actuación 1: ¿Qué auditamos?

Debido al sistema federal de Alemania, compuesta por el Estado federal, los Estados federados y los entes municipales, los diferentes temas relacionados con la estrategia estatal de digitalización destacan por su complejidad. La estrategia requiere, además de un intercambio estrecho de los actores, considerables esfuerzos organizativos, humanos y financieros. Hasta el año 2025 están previstos, sólo por la consolidación de las infraestructuras informáticas federales, unos gastos que ascienden a varios mil millones de euros. A ello cabe añadir los gastos por la digitalización de los servicios administrativos federales.

CUADRO 3
CAMPO DE ACTUACIÓN 1

LA DIGITALIZACIÓN COMO TEMA DE AUDITORÍA	
Estructuras federales • comisarios para la digitalización • consejo de digitalización • divisiones y servicios en los ministerios federales	**Política digital/estrategia digital del Gobierno Federal**
Infraestructura digital • radiotransmisión digital • desarrollo de redes • programa federal de consolidación de TI	**e-gobierno, administración digital**
Proyectos y programas de digitalización financiados por la Federación	**Seguridad TI y ciberseguridad, protección de infraestructuras**
Sistemas de apoyo basados en algoritmos para la toma de decisiones	

Dada la importancia de estos proyectos de digitalización para el futuro, existe una fuerte necesidad de someterlos a la actividad fiscalizadora. Las preguntas de auditoría que solemos aclarar en este ámbito no difieren de aquellas que planteamos a la hora de llevar a cabo la actividad de auditoría clásica:

- ¿En qué consiste la estrategia del sector público?
- ¿Qué estructuras ha establecido el sector público?
- ¿Cómo se han transformado los procesos?

Los objetos sujetos al control son, por ejemplo, proyectos, estructuras, adquisiciones públicas y procesos digitales destinados a la gestión interna en el seno de la administración federal. Algunos de estos asuntos atañen a todas las entidades fiscalizadas (por ejemplo, el expediente electrónico, la factura electrónica, la legislación electrónica), otros son técnicos y se refieren a un ámbito especializado (por ejemplo, la introducción de la tarjeta sanitaria electrónica, la aplicación de inteligencia artificial en los servicios públicos de

empleo y en las autoridades de la administración financiera). Por lo tanto, cada una de las divisiones de auditoría del Tribunal Federal de Cuentas se enfrenta potencialmente a un objeto de control más o menos digitalizado.

Llegados a este punto surge la pregunta sobre si y de qué modo las divisiones de auditoría son capaces de enfrentar, mediante los recursos metodológicos, humanos y materiales que les han sido asignados, los asuntos arriba mencionados o si existe la necesidad de dotarlas con más recursos. Esta cuestión nos lleva a los dos campos de actuación consecutivos.

b) Campo de actuación 2: ¿Cómo auditamos?

El enfoque clásico de la auditoría, que consiste en estudiar los expedientes, realizar entrevistas y examinar los registros, ya no es suficiente para analizar los procesos administrativos digitalizados y los macrodatos. Sólo será posible auditar los objetos (parcial o totalmente) digitalizados si disponemos de una metodología apropiada y adaptada al mundo digitalizado.

CUADRO 4
CAMPO DE ACTUACIÓN 2

En primer lugar, el Tribunal Federal de Cuentas necesita, para desempeñar sus funciones fiscalizadoras, unos accesos estandarizados a las informaciones administrativas digitales. A tal fin, es esencial que las entidades proporcionen los datos solicitados a su debido tiempo, en la calidad requerida, en formato digital y que los datos estén adecuadamente protegidos.

Concretamente, el Tribunal Federal de Cuentas tendrá que modificar sus normas de auditoría para adaptarlas a los asuntos digitales actuales, como la inteligencia artificial y la gestión de datos. Asimismo, para fines fiscalizadores, también debe aplicar procedimientos y herramientas de análisis informático (como por ejemplo: análisis de datos, minería de textos y procesos,

visualización etc.). Los resultados obtenidos mediante este análisis tienen que ser fiables, lo que significa que los procesos deben ser reproducibles, además de que los resultados, métodos y procedimientos sean comprobables por terceras personas (por ejemplo, los tribunales).[6]

c) Campo de actuación 3: ¿Qué instrumentos utilizamos para auditar?

Para cumplir con los requisitos indicados en el esquema de digitalización, el Tribunal Federal de Cuentas tiene que emplear y reorganizar sus recursos adaptándolos a las necesidades y a las circunstancias. Esto vale también para el hardware y el software. Aparte de la construcción de la infraestructura de TI, tenemos que desarrollar los conocimientos necesarios de los auditores para capacitarlos a aplicar de forma fiable los nuevos instrumentos y métodos con la finalidad de obtener unos resultados de auditoría sólidos. También es imprescindible establecer una estructura que nos permita el intercambio, la interconectividad y la cooperación en el mundo digitalizado.

CUADRO 5
CAMPO DE ACTUACIÓN 3

LA DIGITALIZACIÓN DE LOS SERVICIOS ADMINISTRATIVOS INTERNOS	
TI	• Digitalizar los productos y procesos • Proporcionar el hardware y el software que permiten el acceso, la gestión y el análisis de los datos
recursos humanos	• Contratar a especialistas en TI (digitalización, análisis digital, inteligencia artificial) • Creación de capacidades
gestión organizacional	• Asignar responsabilidades para la digitalización, TI, inteligencia artificial y análisis de datos • Perfeccionar las nuevas formas de trabajo • Crear redes de conocimientos

4. Encuesta interna sobre la digitalización

Sin perjuicio del hecho de que la dinámica de la digitalización adquiere diferentes formas en los campos individuales de nuestra actividad fiscalizadora, la relevancia que reviste este proceso en el conjunto de los objetos a fiscalizar significa necesariamente la generación de un impacto también omnipresente en el seno nuestra Institución. Esto supone que se trata de un impacto que concierne a cada una de las divisiones de auditoría, independientemente de sus competencias concretas, puesto que la digitalización ha cambiado y seguirá cambiando

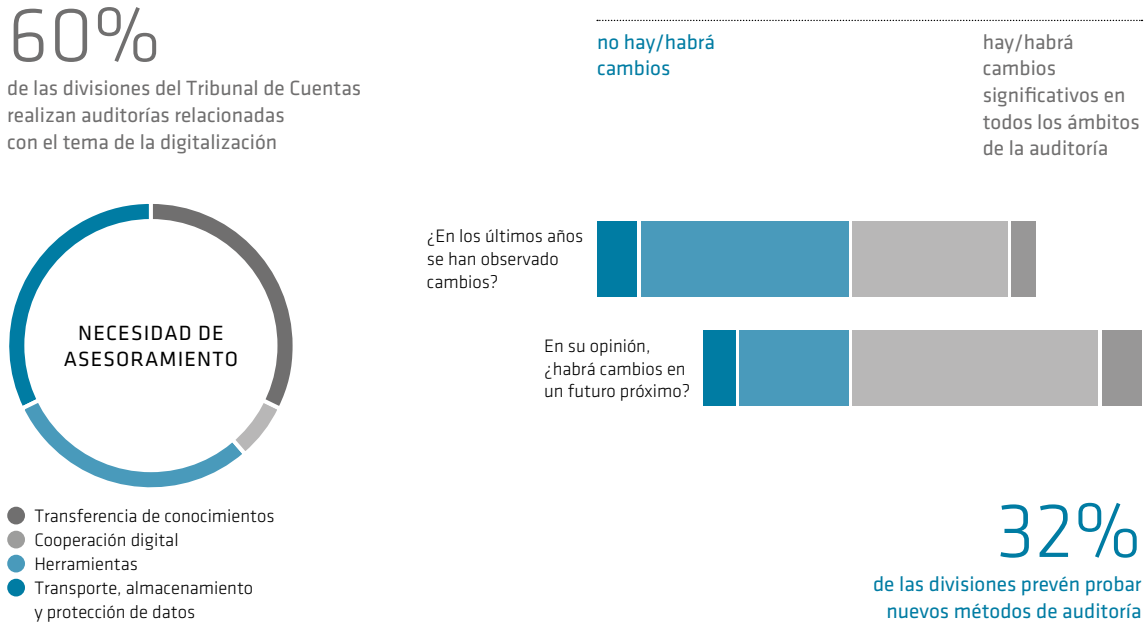
6. Jan Fasswald y Frank Scherwa, Digitalisierung der Verwaltung – Auswirkungen auf die Prüfung, publicado en «Neue Wege in der Finanzkontrolle», Schriftenreihe der Deutschen Universität für Verwaltungswissenschaften Speyer, Band 237, Hermann Hill / Holger Mühlenkamp (Hrsg.), 2019.

cada vez más no sólo el objeto de control en la fase planificadora y en la realización de la labor, sino también el interés suscitado a la hora de rendir los informes. Por ello, incumbe a cada órgano colegiado determinar la necesidad de acción para poder hacer frente a las nuevas circunstancias en su ámbito de competencia fiscalizadora.

Para determinar las necesidades, hemos realizado una encuesta en línea a todas las divisiones de auditoría. Cada división ha evaluado su situación actual en su ámbito de competencia y su progreso en los tres campos de actuación indicados en el esquema de digitalización.

Los resultados de la encuesta fueron analizados y comunicados internamente. Según ellos, en los tres campos de actuación no existen los mismos desafíos en el seno de nuestra Institución. A pesar de que la digitalización concierne a todas las divisiones, la dinámica de esta evolución no es siempre la misma. Así, por ejemplo, aplicar métodos de auditoría digitalizados resultará idóneo sobre todo si el objeto de control está formado por macrodatos. También difieren, en función de la división de auditoría, las necesidades de asesoramiento en TI.

CUADRO 6
RESULTADOS SELECCIONADOS DE LA ENCUESTA INTERNA

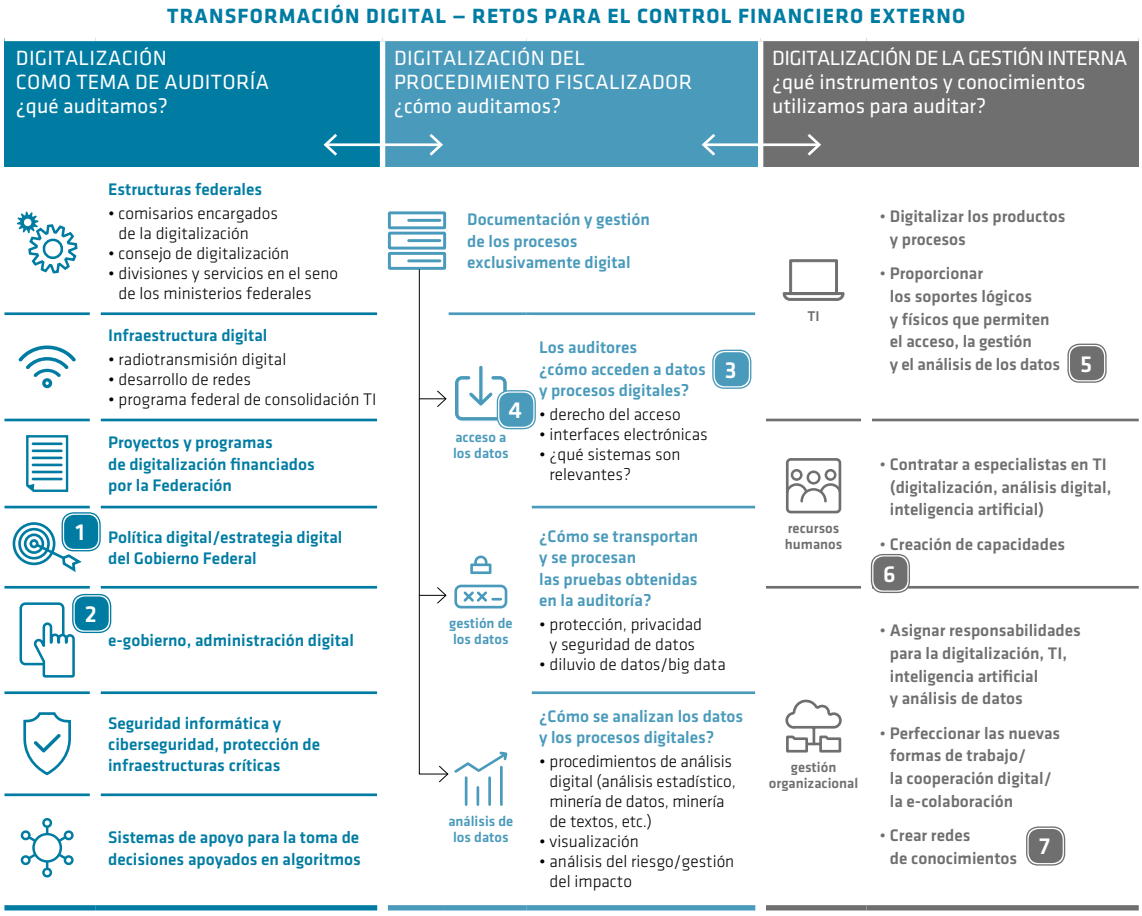


Visto lo anteriormente expuesto se puede deducir que hemos reconocido la digitalización como tema de auditoría. Para el futuro, las divisiones de auditoría prevén, en su respectivo ámbito de competencia, unos cambios aún más significativos. No obstante, cuando procedemos a obtener las pruebas fiscalizadoras en un entorno digitalizado, ya empiezan a surgir desafíos prácticos, por ejemplo, debido a los requisitos de seguridad informática y de protección de datos, unos requisitos que cada vez serán más exigentes.

5. Ejemplos prácticos

Para cada uno de los campos indicados en el esquema de digitalización hemos desarrollado posibles soluciones que nos ayudarán a responder a las necesidades de la digitalización.

CUADRO 7
EJEMPLOS DE POSIBLES SOLUCIONES



Caso 1: Cartera de auditorías de la inteligencia artificial

AI Made in Germany es el título de la estrategia federal de inteligencia artificial aprobada por el Gobierno Federal que aspira a ser un líder en IA y contribuir así a mejorar la eficiencia, calidad y seguridad de los servicios administrativos. Hasta el año 2025 incluido, el Estado federal prevé asignar aproximadamente 3 mil millones de euros a la implementación de dicha estrategia. Los recursos financieros serán repartidos entre once ministerios federales. Por este motivo, la auditoría de los recursos asignados será competencia de diferentes divisiones de auditoría del Tribunal Federal de Cuentas. Los asuntos a auditar no se distinguirán de aquellas planteadas en las auditorías *clásicas* de los proyectos y programas federales.

Caso 2: Inventario de fuentes de datos digitales para fines fiscalizadores

Una sinopsis que comprenda todos los datos de los registros y sistemas electrónicos de las entidades auditadas permitirá a cada una de las divisiones de auditoría extraer la información relevante sobre su respectivo ámbito de actividad fiscalizadora. A este efecto, se establecerá un inventario interno global con toda la metainformación sobre las fuentes de datos digitales al que tendrán acceso las divisiones de auditoría.

Caso 3: Clarificación jurídica

En los últimos años ocurrió repetidamente que las entidades fiscalizadas denegaban al Tribunal Federal de Cuentas acceder a los datos digitales. Si bien, en estos casos, conseguimos llegar a un mutuo acuerdo y una solución satisfactoria para ambas partes, solicitamos al legislador presupuestario una clarificación jurídica. El Parlamento aceptó nuestra propuesta y modificó el Código Financiero Federal. Ahora, según la nueva normativa, la obligación de las entidades fiscalizadas de conceder el acceso y de rendirnos la información incluye también «los datos almacenados informáticamente y su consulta automatizada».

Caso 4: Interfaces electrónicas

Para poder acceder a los datos necesarios, el Tribunal Federal de Cuentas suele recurrir a interfaces electrónicas que permiten, por ejemplo, consultar los datos de la Agencia Federal del Empleo. Gracias a estas interfaces, los auditores tienen, desde su oficina, el mismo acceso a los datos como en las auditorías llevadas a cabo in situ. No sólo pueden consultar los archivos, sino también transmitirlos a los sistemas del Tribunal a través de una conexión segura para someterlos, a continuación, a un análisis ulterior. Las ventajas son evidentes: de un lado, menos trabajo y menos gastos a la hora de obtener las pruebas, y de otro, procesos simplificados para las entidades fiscalizadas.

Caso 5: Gestores de la demanda de TI

Los departamentos de auditoría del Tribunal Federal de Cuentas han nombrado a gestores de la demanda de TI para que ejerzan la función de personas de contacto para las necesidades informáticas departamentales. A estos gestores les corresponde agrupar las necesidades de TI identificadas y actuar de enlace con nuestro servicio central de informática. Su tarea también consiste en informar internamente sobre las novedades del departamento, como por ejemplo sobre nuevas conclusiones fiscalizadoras en el ámbito digital o sobre las experiencias que se han ido adquiriendo en el empleo de los nuevos métodos de trabajo. De esta forma aseguramos que se mantengan informados todos los departamentos.

Caso 6: Fortalecer la creación de capacidades

Los auditores tienen la posibilidad de asistir a cursos de capacitación sobre métodos de auditoría digitales. Para 2020, hemos también organizado una capacitación dirigida al personal directivo sobre los métodos e instrumentos digitales de auditoría.

Caso 7: Comunidad de conocimientos sobre la digitalización

Para explotar el caudal de conocimientos internos, por ejemplo, en el campo del análisis de datos y en el empleo de herramientas digitales, estableceremos una plataforma digital de comunicación con la finalidad de facilitar el intercambio transversal y técnico en el seno de nuestra Institución. La plataforma servirá como herramienta que permita al personal intercambiar opiniones e ideas de forma espontánea, pragmática y más allá de los mecanismos de coordinación formales.

6. El enfoque ágil

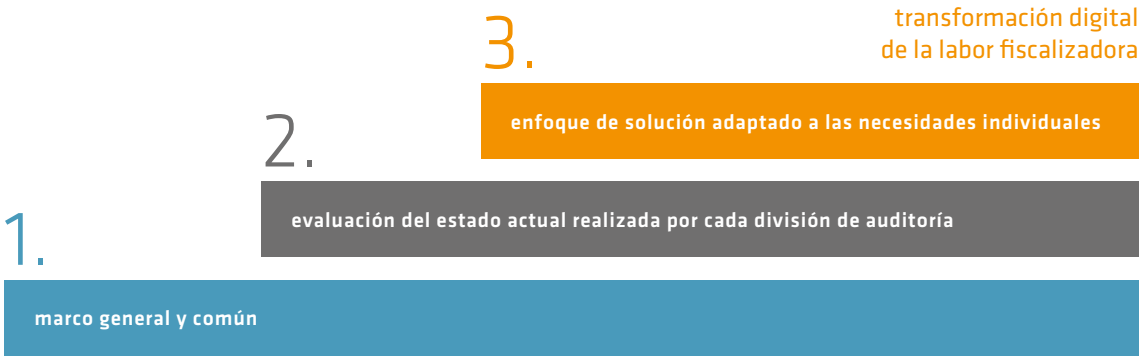
En el seno del Tribunal Federal de Cuentas existe la idea básica y común de que la digitalización tiene el potencial de abarcar a todos los ámbitos de la actividad fiscalizadora. Apoyándonos en esta idea básica, hemos adoptado un enfoque estructurado y ágil que:

- se basa en un análisis profundo de la situación actual,
- respeta la estructura colegiada y las competencias de nuestros Miembros,
- abarca los campos de actuación e identifica las necesidades,
- sitúa las necesidades en el esquema de digitalización y
- contribuye, por etapas, a la mejora de las capacidades fiscalizadoras en el mundo digitalizado.

El enfoque ágil permite desarrollar y ensayar métodos de trabajo y comunicación adecuados para un entorno digitalizado con el fin de identificar lo imprescindible para poder llevar a cabo una labor fiscalizadora efectiva. El concepto de la agilidad consiste en desarrollar, por etapas formales, soluciones coordinadas. Lo anteriormente dicho es especialmente importante para evitar que se abra una brecha digital en el seno de nuestra Institución, pero también entre el Tribunal Federal de Cuentas y el *cliente* (es decir, el gobierno, la comisión de presupuestos, la prensa y la ciudadanía). Es preciso mantener informadas a todas las unidades organizativas y aprovechar las buenas prácticas de eficacia probada. Sólo si se consigue este objetivo, la transformación digital aportará un valor añadido para todas las partes interesadas en el proceso.

CUADRO 8
ESTRATEGIA DE DIGITALIZACIÓN DEL TRIBUNAL FEDERAL DE CUENTAS

ETAPAS HACIA LA TRANSFORMACIÓN DIGITAL DE LA LABOR FISCALIZADORA



7. Conclusión

Para el Tribunal Federal de Cuentas, la digitalización significa más que convertir informaciones análogas en un formato digital. Teniendo en cuenta la digitalización del entorno interno y externo, tenemos que comprobar la idoneidad de todos los procesos, técnicas y productos de auditoría, planteándonos la pregunta de qué, cómo y con qué instrumentos

auditamos. En el marco de la estructura colegiada y de las competencias en los diferentes campos de actuación, el objetivo consiste en asegurar y, cuando sea posible, optimizar la capacidad fiscalizadora en un mundo digitalizado.

Aunque la digitalización es un fenómeno global que viene frecuentemente presentado como objetivo político no debe ser un fin en sí mismo, y siempre hay que mantener una perspectiva crítica. Esto vale especialmente para el Tribunal Federal de Cuentas que, a la hora de cumplir su misión constitucional, tiene que salvaguardar los fundamentos democráticos y constitucionales, evitando que la digitalización los socave. Asimismo, es nuestro deber salvaguardar la capacidad de acción autónoma del Estado para proteger a la ciudadanía, siempre moviéndonos en los límites establecidos por la Constitución de la República Federal de Alemania.

Como motor de la innovación, es preciso que la digitalización aporte siempre un valor añadido para el desempeño de las funciones constitucionales, asegurando una buena relación coste-beneficio y el cumplimiento de las reglas y normas vigentes.

La transformación digital de la labor fiscalizadora no será llevada a cabo en un corto plazo. Se parece más a un maratón que a una carrera de cien metros. Los factores clave para su éxito son:

- una idea básica y común sobre los campos de actuación digital,
- un enfoque estructurado y al mismo tiempo ágil,
- soluciones a medida e individuales, y
- la transformación digital en etapas de la labor fiscalizadora.

8. Referencias bibliográficas

BULL, Hans Peter, Digitalisierung als Politikziel -Teil I, *Report und Technik – Aufsätze, CR 7/2019.*

CEDRAZ DE OLIVEIRA, Aroldo, *Control of Public Administration in the Digital Age, 2017, Presentation Chapter, Page 30.*

FASSWALD, Jan y SCHERWA, Frank, Digitalisierung der Verwaltung – Auswirkungen auf die Prüfung, *Neue Wege in der Finanzkontrolle, Schriftenreihe der Deutschen Universität für Verwaltungswissenschaften Speyer, Band 237, Hermann HILL / Holger MÜHLENKAMP (Hrsg.), 2019.*

Transformación digital en el sector público de Estonia. Beneficios y desafíos para la Oficina Nacional de Auditoría

JANAR HOLM
Auditor General. Oficina Nacional de Auditoría de Estonia

RESUMEN

La digitalización ha abierto horizontes completamente nuevos para el sector público. Una transformación digital Inteligente y bien dirigida puede conducir a una evolución del estado a situaciones de mayor eficacia y transparencia. El protagonismo cada vez mayor de las tecnologías, si no se administrara de manera adecuada, podría afectar negativamente a las relaciones interinstitucionales agravando los problemas existentes en lugar de disiparlos. Los riesgos que derivan de dichos problemas necesitan una gestión correcta.

Hace unos 25 años, el sector público de Estonia se fijó como objetivo el desarrollo de la administración electrónica y el gobierno comenzó a desarrollar bases de datos, a potenciar un entorno seguro para el intercambio de información y para la certificación digital, así como a promover la creación de servicios de carácter electrónico. Para la Oficina Nacional de Auditoría de Estonia (a partir de ahora, NAOE) ha sido un desafío tener que abordar las innovaciones tecnológicas desde dos perspectivas simultáneamente: como observadora independiente, por un lado, y como entidad sujeta a dichas innovaciones, por otro.

Desde el punto de vista de su actividad externa, la NAOE debe garantizar que todos los sistemas de administración electrónica funcionen y que la aportación de datos, por quienes estén obligados a suministrarlos, se produce correctamente y sin retrasos. Por lo que respecta a su organización y actuaciones internas, la NAOE debe incorporar nuevas habilidades, herramientas, productos y comunicación, así como, posiblemente, un nuevo enfoque de las auditorías que debe realizar.

La transformación digital se ha convertido en una cuestión horizontal para la NAOE. De hecho, hay una serie de auditorías realizadas por la misma que se ocupan de la digitalización y de las nuevas cuestiones tecnológicas.

El caso de la NAOE resulta ilustrativo para mostrar que todas las Entidades Fiscalizadoras Superiores tienen que adaptarse a las novedades de este mundo cambiante y diagnosticar sus problemas, plantear soluciones y apoyar la buena gestión del sector público.

PALABRAS CLAVE

digitalización | administración electrónica | Estonia | datos | auditoría

ABSTRACT

Digitalization has opened up completely new horizons for the public sector. Smart and systematically driven digital transformation can lead to a more effective, more efficient and more open state. Without proper governance, the increasing role of technology could change relations in a way that reinforces existing problems rather than dissipating them. The risks associated with these problems need to be managed.

Around 25 years ago, the development of e-governance was set as the goal of the Estonian public sector and the government started to systematically build up databases, create a safe environment for data exchange and digital authentication and promote the creation of eservices. It has been a challenge for the National Audit Office of Estonia (NAOE) to cope with this new situation in its dual role as an independent observer of these events but at the same time being subject to the same changes.

Externally, the NAOE has to ensure that all e-governance systems are functioning as planned and delivering the data they are supposed to be delivering, and that their development is not lagging. Internally, the creation of new skills, tools, products, communication and possibly even a new approach to auditing is needed.

Digital transformation has become a horizontal topic for the NAOE. There are a number of audits conducted by the NAOE which deal with digitalization and new technology issues.

The case of the NAOE illustrates that supreme audit institutions also have a number of roles and functions in this changing world, whether that be highlighting problems, providing solutions or supporting good governance, but also certainly in changing themselves.

KEYWORDS

digitalization | *e-governance* | *Estonia* | *data* | *auditing*

1. Las Entidades Fiscalizadoras Superiores ante la administración digital

Las nuevas tecnologías e innovaciones digitales han penetrado en nuestras tareas cotidianas e interacciones y han remodelado nuestra sociedad, economía, cultura y estilo de vida. Estos cambios han afectado, en gran medida, a la forma en que vivimos, aprendemos, trabajamos y nos relacionamos socialmente.

En los últimos 25-30 años, la mayoría de los países han incorporado agendas digitales en sus políticas públicas. En la última década, la palabra «digital» ha comenzado a parpadear regularmente en el radar de políticos y responsables de la toma de decisiones en todo el mundo. Cada país y cada sociedad pueden convertirse en una comunidad digital, es decir, en una organización en la que la creación, distribución, uso e integración de la información digital resulten actividades económica, política y culturalmente relevantes. Muchos gobiernos están priorizando este proceso de modernización, dentro de sus agendas políticas.

La digitalización promete enormes beneficios pero también plantea desafíos complejos: nuevas tensiones respecto al acceso a los datos y a su control, la manipulación de la información, las amenazas cibernéticas, la desigualdad causada por la «brecha digital», etc. Por ejemplo, en la actualidad, más de la mitad de las personas utilizan internet de forma habitual pero la antes aludida «brecha digital» subsiste entre quienes hacen uso de la Red como medio para conseguir un crecimiento inclusivo y sostenible para la sociedad y aquellos que se han quedado atrás tecnológicamente hablando[1]. La situación en Europa también es insatisfactoria: ciento sesenta y nueve millones de europeos de entre 16 y 74 años de edad, que representan un 44% de la población europea total, no tienen habilidades digitales básicas.[2] Esto significa que una gran proporción de la población no puede beneficiarse plenamente de las ventajas de la sociedad digital. Esto, a su vez, conduce a una menor competitividad en el mercado laboral. Cada fenómeno puede tener efectos positivos y negativos, y la digitalización no es una excepción. George Westerman, científico investigador de la Iniciativa Sloan del MIT sobre la Economía Digital, ha dicho: «Cuando la transformación digital se hace bien, es como una oruga que se convierte en una mariposa, pero cuando se hace mal, todo lo que produce es una oruga muy rápida»[3].

La digitalización ha abierto horizontes completamente nuevos para la gestión del sector público y ha hecho posible la aparición de nuevas oportunidades, pero también nos amenaza con nuevos riesgos. Una transformación digital inteligente y sistemática del sector público puede impulsar un funcionamiento más eficaz y eficiente del mismo, así como potenciar una participación ciudadana más activa, una formulación de mejores políticas públicas, una gestión administrativa más transparente, una mejor creación de capacidad administrativa, unos servicios públicos de mayor calidad, así como un uso reflexivo de los fondos públicos.

1. ROOSNA, Sandra; RIKKE Raul (eds), 2019, p. 8.
2. Comisión Europea; Mercado único digital. Factsheet, 2017. https://ec.europa.eu/digital-singlemarket/en/news/digital-skills-gap-europe
3. Blog de Educación Ejecutiva del MIT Sloan. El imperativo de transformación del negocio digital. https://executive.mit.edu/blog/the-digital-business-transformation-imperative#.XbrlqEl7kcQ

Todos estos mecanismos de desarrollo son importantes, tanto a nivel estratégico como a nivel práctico, para las Entidades Fiscalizadoras Superiores (a partir de ahora, EFS). Se ha dicho que el desarrollo tecnológico es más rápido que nunca, pero resulta más preciso decir que el desarrollo tecnológico nunca será tan lento como ahora. El tren ya se está moviendo rápido y ganando, cada vez, más velocidad. Las EFS deben estar subidas en ese tren.

Ciberseguridad, brecha digital, aplicaciones digitales, big data, blockchain, interconexiones, servicios electrónicos, red de banda ancha, habilidades digitales eran términos que, hace diez años o incluso menos, no se hallaban entre los más importantes en el ámbito de las EFS.

Desde entonces, las EFS se han ido dando cuenta de la importancia de la modernización tecnológica. La Oficina Nacional de Auditoría de Finlandia, con la asistencia del Tribunal de Cuentas de Turquía, organizó un interesante Taller de Temas Emergentes de EUROSAI en noviembre de 2018 en Estambul[4]. Para preparar dicho Encuentro, la Oficina Nacional de Auditoría de Finlandia organizó un coloquio, a través de la Web, en el que planteaba las preguntas siguientes: ¿Cómo ve usted el futuro?, ¿cuáles son los problemas emergentes más importantes para las EFS?

Una de las principales conclusiones fue que los avances tecnológicos —Inteligencia Artificial, análisis avanzados de datos, automatización y robotización— constituían cuestiones de primer orden en el panorama de las cuestiones emergentes para las EFS. Hoy podemos decir que el futuro ya ha llegado: la digitalización y las nuevas tecnologías ya no son «problemas emergentes», sino cuestiones tan cotidianas para las Entidades Fiscalizadoras Superiores como la prevención y lucha contra el fraude o la ineficiencia en la gestión de los fondos públicos.

Hace unos 25 años, Estonia se fijó como objetivo conseguir el desarrollo de la administración electrónica, incorporando a la gestión llevada a cabo por el sector público las nuevas tecnologías, lo que ha cambiado la forma de enfocar y realizar las auditorías por la NAOE.

En los epígrafes siguientes voy a dar una breve descripción, desde el punto de vista de la auditoría, de los aspectos clave del desarrollo de la administración digital en Estonia y de cuáles han sido los desafíos que ha tenido que afrontar la NAOE y las soluciones que les ha dado.

2. Cambios en el entorno de auditoría: una visión general de la evolución de la política de administración electrónica en Estonia

La competencia de Estonia en el uso de las tecnologías digitales en beneficio de las personas ha evolucionado en paralelo con el rápido desarrollo de las tecnologías de la información y la comunicación. El gobierno decidió, con carácter general, que las políticas se adaptaran al desarrollo en lugar de someter el desarrollo a las políticas. Este fue el enfoque principal en

4. Véase también: http://www.eurosaiop.org/docs/upload/documents/Conlusions-from-the-EUROSAI-EmergingIssuesWorkshop-18122018_1549272383.pdf y https://www.eurosai.org/en/calendar-and-news/calendar/EUROSAIEmerging-Issues-Workshop-00001/

la primera década de planificación e implantación de la administración electrónica. Muchos aspectos de la política y de la estrategia de administración electrónica sólo se describieron después de que el gobierno los hubiera implantado tecnológicamente[5].

El método principal seguido se centró en aumentar el acceso de los ciudadanos a Internet y en mejorar la alfabetización digital, estimulando al mismo tiempo el desarrollo de nuevos servicios digitales. En 1996 se puso en marcha el Programa Tiger Leap. Este programa se basaba en tres pilares: ordenadores e Internet, formación básica de los profesores y cursos electrónicos en lengua nativa para instituciones de educación general. La Fundación Tiger Leap se constituyó en 1997 para conseguir estos objetivos. El primer paso consistió en proporcionar a todas las escuelas ordenadores y acceso a Internet, lo que se logró en 2001. También se organizaron cursos de TIC para profesores: miles de ellos participaron en uno de capacitación básica, de cuarenta horas, en 1997 y esta experiencia se fue repitiendo en los siguientes años[6].

El gobierno tomó la iniciativa en la gestión de la transformación digital partiendo de la idea de que no sólo era un usuario de tecnología para hacer más transparente y eficiente su gestión, sino que además le correspondía supervisar el impacto social de las nuevas tecnologías, por lo que necesitaba programar y liderar una hoja de ruta digital para Estonia. Las soluciones digitales afectan a todos los aspectos de la vida, por lo que deben encauzarse a través de procesos integradores y coordinados[7].

La política inicial sobre administración electrónica del país realmente se puso en marcha en 1998, cuando el Riigikogu (Parlamento Estonio) formuló sus principios esenciales.

La estrategia actual para el e-Estonia (la Agenda Digital 2020), fue aprobada por el gobierno en 2013 y revisada en 2018. Sus cuatro objetivos eran:

a. Una infraestructura TIC que apoyara el crecimiento económico, el desarrollo del Estado y el bienestar de la población;
b. La creación de un número creciente de puestos de trabajo con mayor valor añadido, la mejora de la competitividad internacional y una mayor calidad de vida.
c. Una gestión más inteligente y unos servicios proactivos.
d. La promoción de las exportaciones y la sensibilización respecto a la administración electrónica en Estonia[8].

Tres elementos (acuerdos organizativos, liderazgo y formulación de políticas) fueron los componentes clave para habilitar y apoyar el proceso de transformación digital. En un debate más largo no hay que olvidar que se necesitan cambios en el marco jurídico y recursos para desencadenar esos cambios. Conocer el punto de partida de la transformación digital resulta importante para que los auditores entiendan en qué contexto se mueven cuando diseñan sus auditorías e interpretan los datos que encuentran a través de ellas.

5. ROOSNA, Sandra; RIKKE Raul (eds), 2019, p. 40.

6. La Fundación de Tecnología de la Información para la Educación. Resumen histórico 1997-2017. https://www.hitsa.ee/about-us/historical-overview/1997-2000

7. ROOSNA, Sandra; RIKKE Raul (eds), 2019, pp. 8-9.

8. Ministerio de Asuntos Económicos y Comunicaciones. Agenda digital 2020 para Estonia, 2018. https://www.mkm.ee/sites/default/files/digital_agenda_2020_web_eng_04.06.19.pdf

2.1. Principios de la administración electrónica en Estonia

Por la misma razón, es decir, para entender correctamente su entorno profesional, el auditor debe conocer los objetivos y principios de la gestión pública que va a fiscalizar. Esto le ayudará a elegir mejor los criterios adecuados.

Según la definición de Naciones Unidas, la gestión electrónica o administración electrónica consiste en el uso de las TIC para prestar servicios públicos más eficientes a las empresas y ciudadanos, esto es, en conseguir un mejor cumplimiento de objetivos públicos a través del uso de medios digitales.

La finalidad que subyace en la administración electrónica, respaldada por un marco institucional eficaz de gobierno, es mejorar el funcionamiento interno del sector público mediante la reducción de los costes financieros y de los tiempos de tramitación, con el fin de integrar mejor los flujos de trabajo y los procesos, así como de permitir la utilización de recursos efectiva en todas las agencias del sector público con el objetivo de aplicar soluciones sostenibles[9]. La definición dada por el Diccionario de inglés de Cambridge añade expresamente una referencia a que la mejora de la calidad de los servicios públicos incrementa la participación ciudadana[10]. La administración electrónica ha sido una elección estratégica para Estonia, cuya política en la materia busca integrar los aspectos de la definición a la que se acaba de aludir e, incluso, llegar más lejos. Los objetivos del gobierno son el uso transparente y eficiente de las TIC en la administración estatal (Administración electrónica), la participación activa de los ciudadanos en los procesos de toma de decisiones (Participación electrónica) y la prestación de servicios públicos fáciles de usar en línea (Servicios electrónicos). También está entre esos objetivos el de mejorar la competitividad del país y, en general, el bienestar de su gente. El gobierno ha estado tratando de elevar el nivel de confianza de los ciudadanos hacia las organizaciones públicas y el gobierno, y también respecto a las innovaciones técnicas en el sector público. El Poder Ejecutivo espera satisfacer las expectativas de los ciudadanos facilitando una buena interacción entre ellos y las autoridades, en orden a mejorar el acceso a los servicios públicos y motivar a la sociedad a participar en la toma de decisiones.

Con la finalidad de alcanzar estos objetivos, el gobierno ha establecido siete principios para el desarrollo de su modelo de administración electrónica.

1. Integridad: los intercambios de datos, las comunicaciones telemáticas, las bases de datos y el registro de archivos son, gracias a la tecnología blockchain, independientes y fiables.
2. Transparencia: los ciudadanos tienen derecho a ver su información personal y a comprobar cómo está siendo utilizada por el gobierno.
3. Plataforma abierta: cualquier institución puede utilizar la infraestructura existente, que funciona como un recurso tecnológico abierto.
4. Evolución permanente, tanto del marco jurídico como de las tecnologías aplicadas.
5. Descentralización: no existe una base de datos única sino que todas las partes interesadas, ya sea un departamento gubernamental, ministerio o negocio, elige su propio sistema.

9. Naciones Unidas. Departamento de Asuntos Económicos y Sociales. Base de conocimiento de la administración electrónica de las Naciones Unidas. https://publicadministration.un.org/egovkb/en-us/About/UNeGovDD-Framework#whatis

10. Diccionario de Cambridge. https://dictionary.cambridge.org/dictionary/english/e-governance

6. Interconexión: todos los elementos del sistema están diseñados para que se puedan intercambiar datos de forma segura, así como para que sea posible trabajar en común armónicamente.
7. Cada institución recopila los datos una sola vez, lo que hace posible eliminar las duplicidades y el exceso de burocracia.

(Ver Principios de desarrollo y gestión del sistema de administración electrónica de Estonia[11]).

A continuación se exponen ejemplos representativos de la actuación que el gobierno ha realizado para lograr sus objetivos en materia de administración electrónica y para aplicar los principios fundamentales que la presiden[12]:

a. e-Cabinet (ejemplo de administración electrónica): la información necesaria para la toma de decisiones del Gobierno de la República (Gabinete) puede ser consultada directamente desde el sistema de información del e-Cabinet las 24 horas del día, evitando así la burocracia de tener que preparar documentaciones voluminosas. El e-Cabinet es una fuente de información y herramienta planificadora multiusuario que mantiene la información relevante organizada y actualizada en tiempo real, ofreciendo a los ministros una visión general de cada punto que se esté debatiendo.
b. Portal de actividad legislativa (ejemplo de administración electrónica): este sistema de información permite una preparación transparente y sin papeles de documentos de contenido político, proyectos de ley y reglamentos. Los ciudadanos también pueden ver qué documentos están abiertos a la consulta pública y solicitar actualizaciones sobre los temas que les interesen.
c. i-Votación (ejemplo de participación electrónica): es un método de votación complementario que facilita la accesibilidad a las elecciones. No debe confundirse con otros sistemas electrónicos de votación en los que sólo se utilizan los medios tecnológicos para votar y para que se registre el voto en un determinado colegio electoral. Desde 2005, la i-Votación ha permitido a los ciudadanos votar a su conveniencia, sin importar lo lejos que estuvieran de un colegio electoral. A mediados de 2019, la votación por Internet ya se utilizó sin importantes problemas de seguridad en 11 ocasiones, y más del 40% de los votantes prefieren este método[13].
d. Portal estatal eesti.ee (ejemplo de servicios electrónicos): se estableció como puerta de entrada a las agencias gubernamentales y a cientos de servicios públicos. Una vez se inicia la sesión en dicho portal con una identificación electrónica segura y de confianza para el gobierno, el usuario no tiene que repetir el proceso de inicio de sesión para acceder a cualquiera de los otros servicios que están disponibles.

Para cada auditor, estas iniciativas gubernamentales representan una intrigante lista de temas profesionales. Basándose en los objetivos y principios, el auditor tiene una identificación casi perfecta de los criterios aplicables a la auditoría de desempeño pero, por supuesto, en la práctica, como se verá posteriormente, no resulta tan sencillo.

11. El Centro de Información e-Estonia, guía e-Estonia, 2019, p. 10. https://investinestonia.com/wpcontent/uploads/eestonia-guide-veeb.pdf

12. Ejemplos de: La Academia de Gobierno Electrónico. Gobierno Electrónico. Factsheet, 2019. https://e-estonia.com/wpcontent/uploads/2019sept-facts-a4-v03-e-governance.pdf

13. El Centro de Información e-Estonia; i-Votación. Factsheet, 2019. https://e-estonia.com/wpcontent/uploads/2019sept-facts-a4-v02-i-voting.pdf

2.2. Habilitación de las piedras angulares de la administración electrónica de Estonia

Además de los objetivos y principios políticos, también hay otros componentes fundamentales que apoyan los procesos de prestación de servicios electrónicos gubernamentales, el intercambio de información y la facilitación de la gestión de datos digitales. Estas piedras angulares son el e-ID (identificación digital segura) y el X-Road (mecanismo seguro de intercambio de datos para los sistemas de información)[14]. La existencia de estas piedras angulares ha cambiado la forma en que la NAOE aborda las auditorías e interactúa con el ecosistema de administración electrónica existente.

2.2.1. Identidad digital segura

Hoy en día, cada estonio tiene una identidad digital emitida por el gobierno. Gracias al sistema de identidad electrónica (e-ID), el país ha logrado resolver uno de los principales problemas de su transformación digital: cómo identificar a las personas sin contacto físico presencial[15].

El e-ID permite la identificación digital de los usuarios a través de los sistemas de información y les facilita la posibilidad de firmar de forma segura todo tipo de documentos. En Estonia, desde el año 2000, una firma digital tiene el mismo valor legal que una firma caligráfica. En dicho país se producen anualmente casi 50 millones de firmas digitales, que es más que en toda la Unión Europea. La tarjeta de identificación y sus facultades pueden utilizarse tanto por los ciudadanos de Estonia como por los residentes electrónicos[16]. El e-ID ha sido la primera piedra angular de e-Estonia y permite a los ciudadanos beneficiarse de servicios electrónicos seguros, útiles, rápidos y sin problemas.

La identificación digital segura también permite a los auditores confiar en la autenticidad de los documentos, datos y otras pruebas digitales, lo que ahorra mucho tiempo durante las auditorías. Pero eso no quita para que quepa plantearse una pregunta: ¿Es el sistema e-ID en su conjunto completamente fiable? En relación con esta cuestión cabe destacar que la NAOE hace un seguimiento permanente del sistema, incluyendo la fiscalización del mismo en su Programa Anual de Auditorías.

2.2.2. X-Road: intercambio seguro de datos

Todas las organizaciones públicas tienden a elaborar sus propios sistemas de información, creando bases de datos relevantes para el Estado y proporcionando servicios públicos a sus ciudadanos. Se ponen en marcha a través de diferentes sistemas diseñados para adaptarse mejor a la función de la organización a la que se incorporan. Estas bases de datos son como islas, no están interconectadas con otras. Para hacer frente a este problema se estableció la plataforma X-Road. Esta plataforma se utilizó inicialmente sólo para realizar consultas en bases de datos nacionales, pero ahora también se usa como plataforma para modificar de manera segura los datos de varias bases de datos, para la transmisión de grandes conjuntos de datos y para realizar búsquedas en bases de datos.

14. ROOSNA, Sandra; RIKKE Raul (eds), 2019, p. 9.

15. ROOSNA, Sandra; RIKKE Raul (eds), 2019, p. 8.

16. El Centro de Información e-Estonia. E-Estonia. Factsheet, 2019. https://invest.gg.go.kr/wpcontent/uploads/sites/29/2019/01/1.e-estonia.pdf

El sistema X-Road funciona como una carretera segura de código abierto para el tráfico de datos. Enlaza bases de datos públicas y privadas, proporcionando acceso las 24 horas del día, 7 días a la semana. La falta de una base de datos principal centralizada es la única deficiencia que se aprecia en la administración electrónica de Estonia. Cada institución administra sus propios procesos y las instituciones gubernamentales pueden decidir independientemente qué plataformas y tecnologías enlazarán con el X-Road. El intercambio de datos entre organizaciones y sistemas de información está interconectado; en otras palabras, se trabaja de manera coordinada para que se solicite información al ciudadano «una sola vez»[17].

La columna vertebral de código abierto de e-Estonia, la X-Road, es un entorno invisible y crucial que, en opinión del gobierno, supone un ahorro anual de más de 1400 años de tiempo de trabajo para el sector público y para el privado[18].

¿Cómo funciona el X-Road invisible? Por ejemplo, al utilizar eI e-ID e iniciar sesión en el Portal de la Junta de Impuestos y Aduanas (TCB), el sistema puede extraer datos automáticamente del Registro de Población y crear una conexión con un banco para pagar los impuestos necesarios en los importes requeridos. De esta manera, el pago de un impuesto cuya liquidación ya esté preparada se puede abonar con un solo click. Esta operación puede efectuarse en apenas tres minutos y con la seguridad de que los datos privados, como por ejemplo los saldos de las cuentas corrientes, no pueden ser invadidos por personas o entidades públicas no autorizadas.

Las funcionalidades prácticas del X-Road se plasman en múltiples ejemplos.[19]

La NAOE también puede utilizar el sistema X-Road para intercambiar documentos. Las opciones del mismo permiten a los auditores trabajar sin tener que elaborar previamente una macrobase de datos, y se espera que en algún momento tengamos acceso en tiempo real a todos los datos que necesitamos del sistema de información de nuestra oficina.

2.2.3. Servicios electrónicos

Estas piedras angulares, junto con la gestión de datos, establecieron las condiciones para el desarrollo de los servicios electrónicos. En la actualidad, casi todos los servicios públicos digitales están disponibles, en Estonia, 24 horas al día, 7 días a la semana. La gente confía en las soluciones digitales, lo que provoca su uso generalizado.

A pesar de que el 99% de los servicios públicos que implican intercambio de información digital están disponibles electrónicamente, el gobierno se está esforzando en dar el siguiente paso: promover los servicios proactivos, también llamados servicios invisibles, para facilitar la mejor gestión posible de los datos que el Estado ya tiene. La prestación proactiva de servicios implica que el gobierno comienza a realizarlos sin una previa solicitud por los ciudadanos.[20]

17. ROOSNA, Sandra; RIKKE Raul (eds), 2019, p. 8.

18. El Centro de Información e-Estonia. E- Estonia. E-Governance, 2019. https://e-estonia.com/solutions/egovernance/

19. El Centro de Información e-Estonia. E-Estonia. Bloques de construcción de e-Estonia, 2019. https://eestonia.com/solutions/

20. El Centro de Información e-Estonia. E- Estonia. E-Governance, 2019. https://e-estonia.com/solutions/egovernance/

El gobierno ha delimitado 15 servicios personales y empresariales para comenzar: así, por ejemplo, el nacimiento de un hijo, la jubilación y las prestaciones sociales. Esto significa que los servicios públicos relativos a la vida personal o mercantil se activan con un máximo de una interacción o, idealmente, de forma automática en base a los eventos que tienen lugar en la vida de una persona.

En octubre de 2019, la Junta de Seguro Social de Estonia lanzó su primer servicio proactivo, en el que los padres podían acceder al servicio de beneficios familiares sin tener que recurrir al procedimiento tradicional. Dicha Junta se ha fijado el objetivo de desarrollar todos sus servicios sobre la base de no tener que pedir a los ciudadanos información que ya tenga el Estado, lo que significa actuar proactivamente y en la práctica, por ejemplo, que la inscripción de un recién nacido en el Registro Civil active todos los servicios públicos posteriores sin que los padres tengan que solicitarlo, lo que además de contribuir al bienestar de la ciudadanía supone un importante ahorro para el erario público.

Este nivel de servicios electrónicos significa que para la NAOE no hay ningún campo de operaciones gubernamentales en el que los aspectos tecnológicos sean irrelevantes. Hasta la fecha hemos centrado nuestra atención en servicios críticos como e-health (ver más abajo para más detalles), donde analizamos cómo se proporciona un servicio en particular, el sanitario. En las auditorías, los profesionales deben plantearse hasta qué punto la administración ha sacado el mayor partido posible a las tecnologías, así como los sistemas de TI existentes a la hora de prestar los servicios a la sociedad.

2.3. Gestión de datos y bases de datos

Otro avance que una buena administración electrónica permite es la consecución de una eficiente y segura gestión de datos. El gobierno y los municipios manejan una gran cantidad de datos digitales a través de archivos de servicios públicos y sistemas de información. La digitalización en el sector público, mediante el uso inteligente de la información, abre nuevos horizontes para la formulación de políticas eficaces y para la realización de auditorías modernas y automatizadas que ayuden a los gestores a mejorar la calidad de los servicios que se prestan a la ciudadanía.

2.3.1. Datos para una mejor gestión

Nadie puede poner en duda que el poder contar con datos fiables, actualizados y accesibles resulta fundamental para una mejor administración de los asuntos públicos. Basarse en la información es crucial para la aplicación de políticas, para la toma de decisiones, para el seguimiento de los progresos en el logro de metas estratégicas, para diseñar y poner en marcha nuevos servicios públicos y, especialmente, para garantizar una buena gestión contable y la participación ciudadana.

La digitalización del sector público y de los servicios públicos ha proporcionado datos que nos permiten supervisar y auditar eficazmente el progreso de las políticas nacionales. Además, también está creando oportunidades únicas de integración más allá del nivel nacional, como por ejemplo supervisar la aplicación de los objetivos de desarrollo sostenible diseñando, si fuera necesario, indicadores nuevos y más relevantes.

La digitalización ha proporcionado una nueva y poderosa herramienta para una gestión y planificación más eficaces. La digitalización del intercambio de información en el sector

público, los sistemas de información interconectada y los servicios electrónicos digitalizados han creado un entorno de formulación de políticas que permite adoptar decisiones gubernamentales con más rapidez y basadas en una mejor información. Los responsables de la toma de decisiones pueden analizar un flujo continuo y masivo de datos en diferentes formatos, conocido como Big Data.

Otro aspecto importante es que, en principio, el gobierno puede obtener información sobre casi cualquier ámbito político en tiempo real. Los datos actualizados y de fácil acceso proporcionan una oportunidad para una gestión estratégica nacional dinámica y para la aplicación de políticas. La digitalización permite comenzar a medir el progreso, en muchos casos en tiempo real, y aplicar indicadores de datos intensivos.

Desafortunadamente, nuestras auditorías y análisis indican que el sector público en Estonia no aprovecha todas las ventajas que le ofrecen los datos digitales. Esto se debe a lagunas en la capacidad de actuación, a restricciones en el uso de datos (especialmente en el caso de los datos personales) y, a menudo, también a la aparición de dilemas complejos. Por ejemplo, la NAOE se enfrenta ahora a dilemas éticos concretos en relación con el uso de Big Data y la elaboración de perfiles en auditorías en las que planeamos experimentar con análisis de datos avanzados. Pero a pesar de los desafíos y problemas, la digitalización ha aumentado la eficiencia del sector público de Estonia, reduciendo considerablemente el tiempo necesario para obtener y procesar diferentes tipos de información, y la NAOE no puede quedarse atrás.

En los últimos años, la NAOE ha auditado las bases de datos y el uso de datos por parte de las instituciones públicas. Cabe destacar dos ejemplos:

a. Uso de los datos de bienestar recopilados por las autoridades locales (diciembre de 2019): La NAOE auditó la recopilación, gestión y uso de la información requerida para la organización de servicios sociales y prestaciones por parte de los gobiernos locales. El enfoque se centró en la información recopilada respecto a las personas y en la carga burocrática que esto supuso para las autoridades locales. La auditoría también analizó cómo se utilizaba por el Estado la información recopilada por los municipios y la carga colateral de trabajo para los mismos.
   Esta cuestión es importante porque se recoge mucha información sobre el bienestar social, lo que resulta comprensible ya que las situaciones son a menudo complejas, y las soluciones mejores para elevar la calidad de vida de cada persona no resultan fácilmente identificables y aplicables. Al mismo tiempo, la recopilación de los datos de las personas implica un importante volumen de trabajo, por lo que se debe tener cuidado para no malgastar energías en la búsqueda de información irrelevante o que ya está recogida en otras bases de datos. Una gestión organizada de la información ayuda a reducir la burocracia, a mejorar la calidad y rentabilidad de los servicios y a desarrollar otros nuevos.
   Nos estamos encontrando que, en el ámbito del trabajo social local, ni la recopilación de la información ni la gestión y uso de la misma están bien organizadas actualmente. Existen descoordinaciones, así como soluciones incorrectamente adoptadas, a nivel local y estatal, lo que resulta problemático. Las consecuencias de estas disfunciones son la elevación excesiva de la carga de trabajo y el desaprovechamiento de la información. Se recopila mucha información innecesaria y ello supone una vulneración del principio de «una sola vez» (que pretende evitar que el funcionario trabaje inútilmente y que se perturbe al ciudadano para buscar unos datos que ya se tienen). La situación actual es también un buen ejemplo

de cómo los problemas no resueltos en el diseño, funcionamiento y desarrollo del sistema de información están empezando a afectar negativamente al desarrollo de la administración electrónica.

b. Resumen de las bases de datos conservadas en pueblos, ciudades y municipios (2017)[21]:
La NAOE ha investigado qué bases de datos tienen las entidades locales, cómo funcionan y si están sujetas a supervisión por el Estado.
Es importante para los contribuyentes tener un conocimiento general de los datos que se recogen sobre ellos, para así poder saber por qué se ha obtenido esa información y si se hace un uso prudente y discreto de ella. Una buena organización digital permite al ciudadano, además, acceder con facilidad a los servicios públicos sin tener que enredarse en complicaciones técnicas (como tener que reiterar con frecuencia el suministro o petición de unos mismos datos).
Como resultado de la auditoría, encontramos que los gobiernos locales tienen cientos de bases de datos, pero que no están aprovechando la posibilidad técnica de intercambiarlos de forma segura a través del X-Road. Por otra parte mucha información sigue archivada en soporte papel, lo que dificulta y retrasa su posible transmisión. Ninguna autoridad de supervisión ha incluido a los gobiernos municipales en su plan de trabajo. La competencia para ejercer esa supervisión se ha ido transfiriendo de una agencia a otra sin que se haya evaluado si este cambio frecuente de sedes de la citada competencia supervisora ha mejorado la calidad de la misma. El informe de auditoría también señaló que los registros nacionales se habían estructurado de acuerdo con las necesidades del Estado y que los requerimientos de información solicitados por los municipios no se habían atendido todavía.

Para apoyar la mejora de la gestión de la información y del uso del análisis de datos avanzados en el sector público, la NAOE presentará un informe de auditoría sobre la disponibilidad y el uso de datos para la gestión inteligente del Estado. Con la ayuda de esta auditoría esperamos encontrar respuestas a las preguntas: ¿Cuál es la situación en la realización de análisis de datos avanzados por parte del sector público?, ¿Cuáles son los principales obstáculos o barreras para realizar análisis de datos avanzados a mayor escala?

2.3.2. Aplicación de la administración electrónica para supervisar las acciones del gobierno

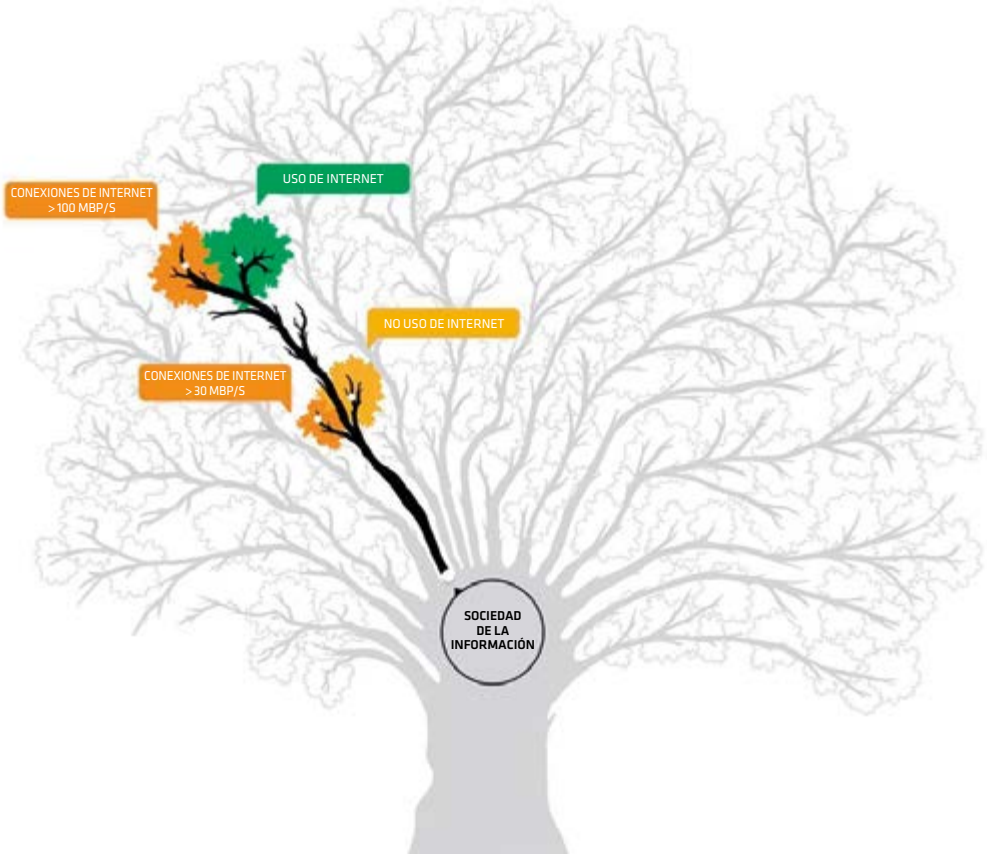
La digitalización y el fácil acceso a los datos también permiten crear sistemas de control más eficaz. En la comunidad de INTOSAI se entiende comúnmente que las EFS desarrollan un papel importante cuando informan sobre los progresos realizados en la consecución de los ODS. Aunque no es una iniciativa de la NAOE, permítanme dar un ejemplo práctico de cómo la digitalización, la administración digital y la gestión de datos pueden proporcionar una forma eficaz de realizar un seguimiento del progreso hacia los ODS.

Estadísticas Estonia es responsable de proporcionar datos nacionales comparables internacionalmente sobre el avance hacia objetivos estratégicos nacionales e internacionales. Con ese fin, ha desarrollado una plataforma de datos nacional que sirve como depósito central

21. La Oficina Nacional de Auditoría de Estonia. Resumen de bases de datos conservadas en municipios, pueblos y ciudades, 2017.
https://www.riigikontroll.ee/tabid/206/Audit/2420/language/en-US/Default.aspx

para toda la información nacional y utiliza datos en tiempo real, procedentes de bases de datos nacionales, a través de la plataforma de intercambio de información X-Road. Basándose en este depósito central, Estadísticas Estonia lanzó en octubre de 2019 una nueva aplicación web llamada el árbol de la verdad[22], un indicador de indicadores nacionales importantes, dando una imagen sencilla, honesta y objetiva de cómo funciona el país. El árbol de la verdad compara resultados utilizando los 135 indicadores medibles incluidos en el plan de acción del gobierno 2019-2023 (objetivos a corto plazo), en el programa de reforma Estonia 2020 (objetivos a medio plazo) y en la Estrategia Nacional de Estonia sobre Desarrollo: «Estonia Sostenible 21» (objetivos a largo plazo). El árbol muestra datos de 15 áreas de actividad y los resultados son visibles como hojas de color verde (objetivo alcanzado), amarillo (algunos progresos conseguidos) o rojo (se necesita una mejora significativa).

Las comparaciones que se reflejan en el árbol de la verdad son una buena base, tanto ahora como en el futuro, para planificar actividades estratégicas y analizar resultados[23]. La aplicación también facilita el trabajo de la NAOE indicando problemas y pidiendo explicaciones sobre por qué los indicadores muestran esos resultados concretos. Aquí es donde una auditoría puede y debe arrojar luz.



22. Véase también: https://tamm.stat.ee/

23. Estadísticas Estonia. El árbol de la verdad muestra cómo le va a Estonia, 2019. https://www.stat.ee/news-release-2019-123

3. Oficina Nacional de Auditoría de Estonia y transformación digital

Como ya se ha dicho, el entorno de auditoría ha cambiado para nosotros en las últimas décadas. Esto ha planteado el desafío, a la NAOE, de tener que hacer frente a la nueva situación desde una doble perspectiva: como observador independiente de los acontecimientos y como sujeto afectado por los mismos.

La visión de la NAOE ha sido que nuestra institución debe estar a la vanguardia del cambio y beneficiarse del mismo. Todo lo que sucede en el sector público debe estar, y así ha sido, en el horizonte de la NAOE. En apartados anteriores señalé algunos de los impactos que tiene la digitalización sobre nuestras actividades de auditoría y sobre el futuro de las mismas. Los cambios en curso relacionados con la digitalización y el desarrollo de nuevas tecnologías traen consigo cada vez más desafíos y nuevos riesgos, pero también nos permiten hacer el trabajo de nuestra Institución más eficiente y eficaz. La NAOE necesita subirse a la «ola».

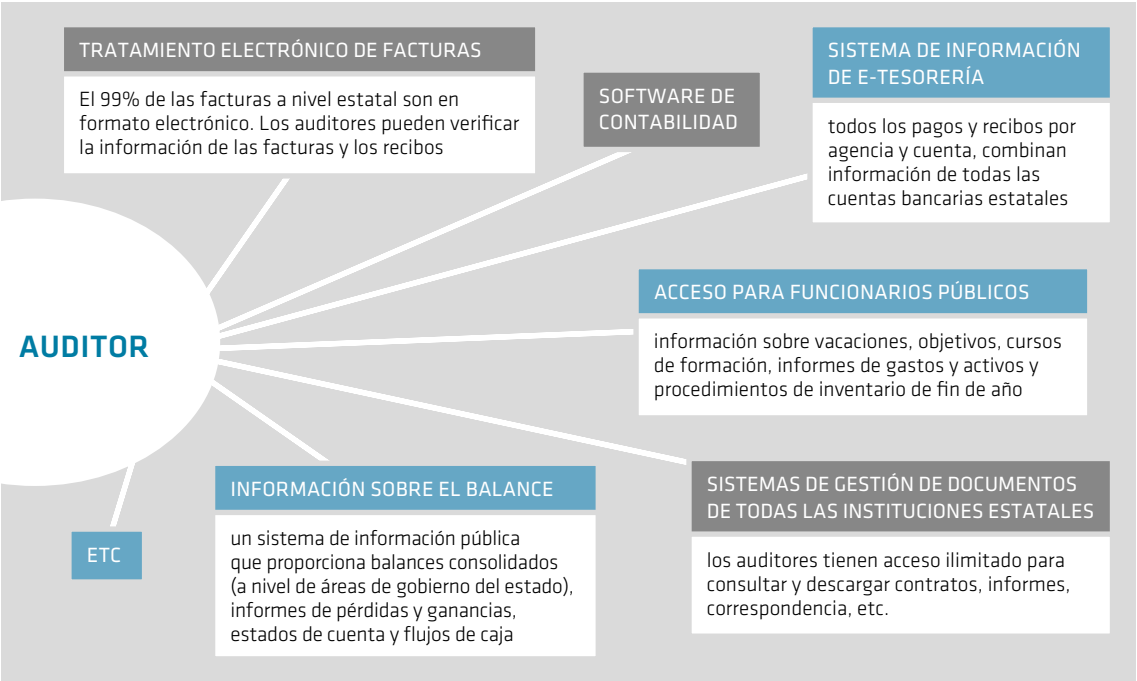
3.1. Transformación digital: beneficios para la NAOE

La digitalización del intercambio de información en el sector público, los sistemas de información interconectados y los servicios electrónicos digitalizados han creado un entorno que, si se aprovecha adecuadamente, permitirá a la NAOE obtener información sobre casi todas las áreas políticas en tiempo real. Por dar, simplemente, algún ejemplo, diremos que la digitalización permite una supervisión efectiva y multidisciplinar de diversas áreas y datos relativos al uso del dinero en diferentes sectores, a los usuarios de servicios públicos, a los costes de los servicios, a los procedimientos de ingresos y gastos, etc. Esta transformación tecnológica facilita también, sin tener que salir del edificio de la NAOE, la comprobación de contratos y facturas así como de la ejecución de los presupuestos de las entidades públicas y de otros documentos. La ley ha proporcionado a los auditores un fácil acceso a una abundante información. La NAOE no tiene que descargar datos en su servidor ni crear sistemas de información paralelos. En la mayoría de los casos tenemos acceso a esa información en tiempo real, lo que nos permite estar tan informados como los ministerios y otras autoridades públicas.

El acceso fácil y rápido a los datos contribuye a la mejora de la eficiencia en la planificación y realización de las auditorías. Se necesita menos tiempo y menos auditores y eso hace posible que se puedan realizar más fiscalizaciones. La adopción de nuevas tecnologías tiene la capacidad de reducir notablemente la cantidad de operaciones manuales realizadas por los auditores, ahorrando así tiempo.

La transformación digital ha cambiado significativamente la forma de organizar las auditorías, tanto en lo relativo a la evaluación anual del informe financiero consolidado del Estado, como en lo que se refiere a otras auditorías. Cualquier información necesaria para los auditores está disponible en las bases de datos a través de Internet o de redes propias (figura 1). El acceso a la información es sencillo y esta puede ser debidamente procesada porque todas las entidades gubernamentales han trasladado su contabilidad a un sistema

FIGURA 1
LOS AUDITORES TIENEN ACCESO REMOTO A TODAS LAS BASES DE DATOS NECESARIAS PARA LLEVAR A CABO LA AUDITORÍA FINANCIERA



y casi todas las facturas a nivel gubernamental son electrónicas[24]. La necesidad de desarrollar trabajo de campo resulta excepcional.

Al contrario que en la era previa a la transformación digital, ahora ya no es necesario contar con un gran número de auditores y ello ha supuesto una gradual reducción de la plantilla de la NAOE durante los últimos veinte años. El nuevo reto es diseñar e implantar controles más automatizados así como promover el análisis de datos en los procedimientos de auditoría.

Las nuevas tecnologías también ofrecen la oportunidad de aumentar el impacto de las auditorías. La presentación visual y las nuevas herramientas tecnológicas permiten elaborar informes más comprensibles. Mostrar la información en forma visual hace que sea más fácil explicar un problema. La digitalización y las nuevas aplicaciones creativas permiten elaborar relatos visuales en estos informes. Además, las auditorías pueden ser causa de la creación de nuevas herramientas digitales para los auditados.

Por ejemplo, en 2016 la NAOE llevó a cabo una auditoría sobre el estado de los registros inmobiliarios de los gobiernos locales así como sobre las decisiones municipales relativas a inversiones inmobiliarias[25]. Utilizamos y combinamos datos procedentes de varias bases

24. Factura electrónica significa una factura en formato electrónico estandarizado, no solo escaneada como un archivo PDF.

25. La Oficina Nacional de Auditoría de Estonia. Visión general de los bienes inmuebles de los gobiernos locales y su gestión, 2016. https://www.riigikontroll.ee/tabid/206/Audit/2413/OtherArea/1/language/et-EE/Default.aspx

digitales y obtuvimos una muy buena visión general del estado de los edificios e instalaciones en toda Estonia. Nuestros auditores llegaron a la conclusión de que no era suficiente presentar los resultados de la auditoría únicamente como una historia descriptiva o en formato PDF, por lo que crearon, en cooperación con Estadísticas Estonia, una aplicación[26] en la que cada gobierno local o sus habitantes podrían comprobar la situación de los inmuebles del gobierno local y cómo ésta afecta a la calidad de los servicios. Esta iniciativa, además de ser una herramienta tecnológica de trabajo, permite una percepción más eficaz de los resultados de la auditoría.

La digitalización y el fácil acceso a los datos aumentan, a través de un uso inteligente de la información, las oportunidades para hacer más sofisticados los análisis. Ya en 2012, la NAOE realizó una auditoría bajo el título: «Prevención de la corrupción en las transacciones del sector público local»[27]. En dicha fiscalización se revisaron transacciones de los gobiernos locales con un alto riesgo de corrupción. Auditamos operaciones realizadas por las autoridades municipales, con la finalidad de determinar si las mismas se habían abstenido de participar en actuaciones que les estuvieran vedadas por la normativa anticorrupción. Esta auditoría se practicó mediante el análisis de datos combinados procedentes del Registro Electrónico de Población y del Registro Electrónico Mercantil.

Pero la facilidad de acceso a la información no sólo implica oportunidades para la NAOE, sino también obligaciones. Recopilar información y verificar su exactitud ya no exige tanto tiempo como hace una década. La NAOE puede utilizar grandes cantidades de datos, analizarlos, recoger datos nuevos, examinarlos y así una y otra vez. Por lo tanto, el trabajo y los resultados de la NAOE no pueden ser los mismos que años atrás: la rápida disponibilidad de información significa que también necesitamos aumentar el ritmo de nuestros procesos de trabajo. Al mismo tiempo, la NAOE necesita utilizar su capacidad para generar más valor añadido utilizando nuevas técnicas. Los desarrollos de la administración electrónica en nuestro entorno de auditoría también nos obligan a repensar nuestro trabajo y a ofrecer una capacidad de respuesta adecuada a la nueva situación. Para ello se necesitan dos cosas: una externa y otra interna. Desde el punto de vista externo, la NAOE tiene que garantizar que todos los sistemas de administración electrónica funcionen según lo previsto, que los datos se están entregando y que el desarrollo de los sistemas no va retrasado. Desde el punto de vista interno, queda obligada a desarrollar nuevas habilidades, nuevos instrumentos de trabajo, mejores productos, canales de comunicación más fluidos y, posiblemente, un nuevo enfoque para las auditorías.

3.2. Transformación digital – necesidad de nuevas habilidades

Los nuevos desafíos exigen nuevas habilidades. El desarrollo tecnológico ha cambiado y sigue cambiando el trabajo de los auditores. Los métodos de auditoría «tradicionales» pueden resultar inadecuados si las entidades auditadas han adoptado nuevas soluciones tecnológicas. Un gran número de procedimientos en el sector público son completamente

26. Véase también: https://estat.stat.ee/StatistikaKaart/VKR

27. La Oficina Nacional de Auditoría de Estonia. Prevención de la corrupción en la organización del trabajo de municipios rurales y ciudades, 2012. https://www.riigikontroll.ee/tabid/206/Audit/2269/OtherArea/1/language/enU

digitales, por lo que es inevitable que las auditorías se lleven a cabo en el entorno digital, a través de los sistemas de información cuando sea posible y utilizando CAAT avanzados (Tecnología de Auditoría Asistida por ordenador), de manera que pueda hacerse una variedad de controles, extractos (digitales), análisis de registros, búsqueda de patrones, etc.

La adopción de nuevas tecnologías puede reducir notablemente la cantidad de operaciones manuales que corresponden a los auditores y, así, ahorrarles tiempo. Pero ello exige a estos profesionales nueva formación y capacidad para modificar sus métodos de trabajo. Por ejemplo, un auditor debe aumentar significativamente su conocimiento de las TIC para manejarse de manera fluida en las comprobaciones contables que se le asignen. La NAOE proporciona esta capacitación a nuestros auditores y considera que la misma es, actualmente, la adecuada para el desempeño de sus cometidos.

Si las entidades fiscalizadas han adoptado nuevas soluciones tecnológicas, los auditores deben ser capaces de afrontarlas. Algunas de esas modificaciones tecnológicas (como blockchain) son de naturaleza compleja, lo que significa que la auditoría de la aplicación y el uso de estas tecnologías requiere la participación de expertos (en este caso, expertos en criptografía), por ello es importante que los auditores estén capacitados para identificar las situaciones en las que les resulte necesario el apoyo de un especialista en modernización tecnológica.

La transformación digital en el sector público ha dado lugar a una situación en la que cada auditor también necesita ser algo así como un auditor de las TIC. Por ejemplo, cuando los auditores de la NAOE evalúan el informe financiero anual consolidado del Estado, también deben evaluar la fiabilidad de los sistemas contables y otros sistemas de información. Esto significa requisitos y competencias completamente nuevas para los auditores.

A pesar de estos desafíos y problemas, la digitalización ha aumentado la eficiencia del sector público y ha hecho posible que la NAOE haga su trabajo de manera más eficaz y eficiente. Como ya he dicho, el acceso en tiempo real a los datos constituye una oportunidad de primer orden para que la NAOE pueda compartir conocimientos y experiencias en los procesos de toma de decisiones derivados de nuestra función. Por último, pero no menos importante, hay que indicar que la habilidad del auditor tradicional de «hacer las preguntas correctas» y «elegir los temas correctos» todavía están muy vivos y son aún más relevantes cuanto más aumenta el ritmo del procedimiento de auditoría.

4. Transformación digital: nuevos retos y nuevos riesgos para la auditoría

Como se muestra en líneas anteriores, el alcance de la transformación digital es abrumador. Las nuevas tecnologías han llegado a todos los ámbitos de la administración pública y apenas hay algún campo de la auditoría que no tenga relación, al menos potencialmente, con la digitalización o el análisis de datos avanzado. Hay un número de auditorías realizadas por la NAOE que se ocupan directa o indirectamente de la digitalización y de los nuevos problemas tecnológicos. La transformación digital y la introducción de las nuevas tecnologías se han convertido en temas horizontales, y la NAOE lo ha reconocido examinando los aspectos TIC en casi todas las auditorías que llevamos a cabo.

En nuestras fiscalizaciones, comprobamos si existen riesgos significativos relacionados con la tecnología de la información que, de materializarse, tendrían un impacto negativo en la prestación de servicios públicos, en la gestión o en la contabilidad.

Si la auditoría de los aspectos informáticos se planifica sistemáticamente desde el principio en los planes de auditoría, facilita una buena oportunidad para realizar un meta - análisis sobre la acción de gobierno en la implantación digital (por ejemplo, una revisión panorámica de un concreto tipo de producto), así como para descubrir problemas sistémicos y hacer recomendaciones de alto impacto a la administración.

La NAOE presenta un informe anual al Riigikogu sobre los aspectos nacionales más importantes seleccionados por nuestra Institución. El informe de 2019 se centró en cuestiones macro, relacionadas con el desarrollo y la sostenibilidad del ecosistema de administración electrónica de Estonia y buscó dar respuestas a preguntas relativas al estado en que se encontraba la tecnologización en el sector público estonio[28].

En los párrafos siguientes voy a dar ejemplos de tres temas de auditoría muy importantes: seguridad, Inversiones en TIC y servicios electrónicos, los cuales llevan varios años siendo auditados por la NAOE.

4.1. Auditoría de la ciberseguridad

La ciberseguridad[29] es uno de los temas de administración electrónica más importantes para cada país. La alta dependencia de la infraestructura de las TIC y de los servicios electrónicos indujo al gobierno estonio a asegurarse de que las soluciones tecnológicas no serían un talón de Aquiles para la sociedad, sino una base segura para el desarrollo moderno. En este contexto, la seguridad cibernética no se considera un freno que restrinja la digitalización, sino una ayuda que hace posible una rápida innovación digital[30].

La mencionada red de interoperabilidad X-Road podría considerarse «territorio» oficial de Estonia en el ciberespacio y el esquema nacional de identidad electrónica (el e-ID) como el «pasaporte» para este territorio virtual. Ambos deben ser protegidos contra posibles amenazas. Para los servicios electrónicos, el e-ID y la X-Road son fundamentales para garantizar el más alto nivel posible de seguridad cibernética nacional. En 2007, el concepto de ciberseguridad aceptado en Estonia y las tecnologías a las que ya había dado lugar tuvieron que enfrentarse a la amenaza real que supuso una sucesión a gran escala de ataques cibernéticos contra su estructura TIC. Los proveedores de servicios de Internet fueron atacados, así como sitios web y sistemas de correo electrónico del gobierno, banca online y otros servicios electrónicos. Esta experiencia demostró que el ciberespacio de

28. Riigikontroll. Ilevaade riigi vara kasutamisest ja s-ilimisest 2018.–2019. aastal, 2019. https://www.riigikontroll.ee/Riigikontrollipublikatsioonid/Riigikontrolliaastaaruanneparlamendile/tabid/110/language/et-EE/Default.aspx.
La traducción al inglés se publicará a principios de 2020.

29. El término «seguridad cibernética» se utiliza como término general para aludir a la protección de datos digitales/información, protección de datos en formato electrónico, seguridad informática, seguridad de la red, seguridad de los servicios electrónicos, seguridad de las TIC, etc.

30. ROOSNA, Sandra; RIKKE Raul (eds), 2019, p. 42.

Estonia está suficientemente protegido, que es digno de confianza y que fue capaz de reponerse del daño sufrido[31]. Pero esto no puede hacernos bajar la guardia.

Dado que la información sobre casi todo se gestiona digitalmente, la seguridad cibernética es la cuestión clave. Una parte del desafío es la protección de los datos contra la divulgación involuntaria o el tratamiento no autorizado de los mismos. Pero aún más importante es la integridad de los datos: la confianza en que los sistemas de información están protegidos contra la modificación y la destrucción. Podemos imaginar la confusión que se produciría si alguien fuera capaz de modificar sin autorización los datos del catastro o del registro de la propiedad cambiando, por ejemplo, el nombre del titular de un inmueble o la extensión del mismo. También podemos concebir los efectos nefastos que derivarían de eventuales alteraciones sin autorización de datos digitales obrantes en el sistema de información de los servicios sanitarios, como por ejemplo el grupo sanguíneo de una persona.

Debe prestarse especial atención a la protección de la información porque los datos electrónicos tienden a considerarse menos seguros. Incluso si tal percepción no es necesariamente cierta, desde luego afecta a políticos sin formación y a ciudadanos que desconfían de las transacciones electrónicas porque temen que pueda haber lagunas en la seguridad de los datos y, por tanto, un margen para su manipulación. El Derecho y la tecnología deben trabajar juntos, aportando soluciones técnicas de obligado cumplimiento para proteger la información.

La ciberseguridad es la piedra angular de la creación de confianza en el contexto de la administración electrónica y las EFS tienen adjudicado un papel claro consistente en la realización de auditorías en áreas críticas, para así garantizar que la información integrada en las bases de datos públicas se guarde en condiciones de seguridad y que los sistemas de información se mantengan.

A lo largo de los años, la NAOE ha llevado a cabo varias auditorías centradas en la ciberseguridad y también ha realizado fiscalizaciones horizontales sobre cuestiones relacionadas con la seguridad cibernética. Destacan en este sentido dos ejemplos:

a. Trabajos para garantizar la seguridad y conservación de las bases de datos estatales cruciales de Estonia (2018)[32]: La NAOE auditó cómo el gobierno había seleccionado los datos y bases de datos que eran fundamentales para garantizar la sostenibilidad nacional. También comprobamos si la seguridad de la información estaba garantizada y con qué herramientas se contaba para mantenerla a corto y a largo plazo.
   La importancia de esta cuestión es obvia ya que existen escenarios de riesgo y un creciente número de incidentes de seguridad de la información, como ciberataques y fugas de datos, que pueden poner en peligro la información y bases de datos de mayor importancia para el Estado. Si los datos de importancia prioritaria para las administraciones públicas se modifican sin autorización, o si se filtran o destruyen, el Estado ya no será capaz de realizar las funciones que le corresponden.

31. ROOSNA, Sandra; RIKKE Raul (eds), 2019, p. 43.

32. La Oficina Nacional de Auditoría de Estonia. Garantizar la seguridad y conservación de las bases de datos nacionales estonias de importancia crítica, 2018.
https://www.riigikontroll.ee/tabid/206/Audit/2462/language/en-US/Default.aspx

La auditoría reveló que, a pesar de la puesta en funcionamiento del sistema de seguridad ISKE, había deficiencias significativas en la seguridad de la información contenida en varias bases de datos importantes, como las incorporadas a los dispositivos móviles. El gobierno ha tomado las medidas necesarias para la protección de datos críticos, pero el éxito de las mismas exige que vayan acompañadas de normas jurídicas imperativas.

b. Trabajos para la implantación de un sistema de medidas de seguridad TIC en los gobiernos locales (2018)[33]: La NAOE auditó si los datos confiados a los gobiernos municipales se gestionaban de forma segura.
El motivo de esta actuación fue que los datos personales no solo se encuentran en las agencias estatales sino también en las entidades locales. La prestación de unos mejores servicios públicos requiere y, a la vez, genera un elevado volumen de información y eso implica el riesgo de que los datos terminen en las manos equivocadas, sean destruidos, dañados, etc. Las bases de datos de los gobiernos estatal y locales intercambian información a través de X-Road, lo que significa que las debilidades a las que no se presta atención en los gobiernos locales se transmiten y pueden causar daños a una escala mucho mayor.
Descubrimos que la seguridad de los datos confiados a los gobiernos municipales no estaba adecuadamente garantizada. Los riesgos que amenazan la seguridad de las TIC todavía no se reconocen por muchas administraciones municipales, por lo que los requisitos establecidos por el Estado no se están cumpliendo pese a llevar en vigor casi diez años. La supervisión estatal es inadecuada y no obliga a los gobiernos locales a actuar. Tampoco las campañas de sensibilización ni el apoyo financiero del Estado han tenido el éxito que se esperaba.

4.2. Auditoría de las inversiones TIC

Desde el punto de vista de la auditoría clásica, también resulta absolutamente necesario abordar cuestiones de eficiencia en el ámbito de la administración electrónica. Esto es así porque el nivel de riesgos que acecha a las inversiones TIC suele ser mayor que el que amenaza a otras áreas del gasto público. A menudo, el coste de las TIC rebasa los límites del presupuesto, el plazo se excede significativamente, y los proyectos tecnológicos se interrumpen o no se alcanza en ellos la calidad pretendida. Las inversiones en software y en infraestructura TIC son más complejas que las realizadas en infraestructuras tradicionales.

Las EFS también deben tener en cuenta los riesgos asociados a las inversiones TIC. Esto significa, de nuevo, un desafío para los auditores. Además de preguntarse: «¿Permanecen los proyectos dentro de los límites presupuestarios?» o «¿se terminan los proyectos a tiempo?», los auditores tienen que responder a preguntas más específicas: «¿Se ha logrado el objetivo que se pretendía?, «¿son las soluciones implantadas fáciles de usar?» o «¿constituyen el método adecuado para alcanzar los objetivos?».

33. La Oficina Nacional de Auditoría de Estonia. Implementación del sistema de medidas de seguridad TIC en los gobiernos locales, 2018.
https://www.riigikontroll.ee/tabid/206/Audit/2466/language/en-US/Default.aspx.

La evaluación tanto de las inversiones TIC como de los sistemas de tecnología de la información de los auditados forma parte del programa de trabajo de la NAOE. Dos ejemplos:

a. Eficacia del desarrollo de una red de banda ancha en Internet de alta velocidad (2015)[34]:
   La NAOE auditó si el Estado había hecho todo lo posible para garantizar que todos los ciudadanos pudieran tener acceso ilimitado a Internet de alta velocidad para 2020. También analizamos si la red de cables de fibra óptica o la red básica de banda ancha que deberían garantizar una conexión a Internet de alta velocidad habían ayudado a la consecución de este objetivo.
   Encontramos que las posibilidades de los ciudadanos e instituciones estonios de utilizar Internet de alta velocidad a través de una red fija no habían mejorado significativamente (en 2015). Los proveedores de dispositivos móviles con Internet se habían beneficiado hasta ahora de la creación de la banda ancha básica. Conseguir que Internet de alta velocidad fuera accesible para todas las personas en Estonia en 2020 resultaba difícil por la falta de un plan de acción claro. El gobierno no ha logrado llegar a un acuerdo con los gestores de Internet sobre las normas de establecimiento y manejo de la red básica de banda ancha.

b. Gestión de los riesgos de desarrollo de software en el sector público (2019)[35]:
   La NAOE ha analizado por qué fallan a veces los proyectos de desarrollo de software del Estado.
   Se ha constatado que se gastan cantidades significativas de dinero en desarrollos de software y que tales desarrollos y los sistemas de información resultantes de los mismos tienen una importante función dentro de la gestión del sector público así como de la prestación de servicios.
   Como resultado de la auditoría y sobre la base de la evaluación de los proyectos, la NAOE describió los 13 riesgos más comunes y los principales factores de éxito apreciados en la gestión del desarrollo de software.

4.3. Auditoría de los servicios electrónicos

En una situación en la que casi todos los servicios públicos de Estonia están disponibles digitalmente y se utilizan con frecuencia, el funcionamiento del Estado depende de que estén operativos para el intercambio de información entre gobierno y ciudadano, gobierno y empresas, así como gobierno central y administraciones locales. Sería inaceptable que los servicios electrónicos no estuvieran disponibles o resultaran poco fiables o difíciles de manejar.

La evaluación de los servicios electrónicos de los sistemas de tecnología de la información de una entidad fiscalizada forma parte del programa de trabajo de la NAOE. Dos ejemplos:

a. Uso de los servicios electrónicos públicos (2016)[36]:
   La NAOE estudió cuatro sistemas de información para determinar si los ocho servicios electrónicos que proporcionan son de alta calidad y crean valor añadido, es decir, si

34. La Oficina Nacional de Auditoría de Estonia. Eficacia del desarrollo de una red de banda ancha o de Internet de alta velocidad, 2015.
https://www.riigikontroll.ee/tabid/206/Audit/2346/Area/4/language/en-US/Default.aspx

35. La Oficina Nacional de Auditoría de Estonia. Gestión de riesgos de desarrollo de software en el sector público, 2019.
https://www.riigikontroll.ee/tabid/206/Audit/2488/language/en-US/Default.aspx

36. La Oficina Nacional de Auditoría de Estonia. Utilidad de los servicios electrónicos públicos, 2016.
https://www.riigikontroll.ee/tabid/206/Audit/2411/language/en-US/Default.aspx

ahorran tiempo y dinero a los organismos que los proporcionan y a las personas que los utilizan. También analizó si los organismos medían la utilidad de los servicios y la mejoraban valiéndose de la información obtenida.

Es importante para los usuarios de servicios electrónicos que la calidad de los servicios públicos proporcionados por el Estado sea buena y les permita una relación fluida, rápida y barata con los organismos estatales, así como hacer uso de los servicios y beneficios proporcionados.

La NAOE sostiene que el Estado debe prestar más atención a la armonización de los requisitos que deben cumplir los servicios electrónicos para ser útiles, porque las diferentes agencias estatales entienden de manera distinta la facilidad de uso, la calidad y la modernidad de estos servicios. Aunque el Ministerio de Asuntos Económicos y Comunicaciones ha planteado numerosas recomendaciones para armonizar la calidad de los servicios electrónicos, las agencias no las han seguido suficientemente. El desarrollo de los servicios electrónicos públicos está fragmentado y necesita una orientación centralizada más fuerte.

b. Actividades del Estado en la implementación del sistema de e-salud (2014)[37]:

La NAOE evaluó si los objetivos fijados para la e-salud (la mayor calidad y eficiencia de la organización y prestación de los servicios sanitarios) se habían conseguido. Los cuatro principales proyectos de e-salud fueron revisados en la auditoría: Registros Electrónicos Sanitarios, Recetas Digitales, Registro Digital e Imágenes Digitales. También se analizaron los problemas encontrados en el desarrollo de la e-salud y los motivos que los provocaban.

La importancia de este tema no sólo reside en que permite una evaluación sectorial del funcionamiento de la administración electrónica sino en que se ve afectado por los cambios demográficos que se están produciendo en Estonia, donde la proporción de personas mayores está creciendo, los nacimientos por el contrario descendiendo y la esperanza de vida aumentando. Esto genera una creciente necesidad de atención sanitaria y servicios sociales, dándose además la circunstancia de que los pacientes son cada vez más exigentes respecto a la cantidad y calidad de los servicios que se les prestan. Una mayor implantación de las soluciones que permite e-salud ayuda a que el sistema sanitario sea más eficaz para preservar la salud de las personas a través de una mejor prevención y también contribuye a un uso más razonable de los recursos sanitarios. Las soluciones que ofrece la e-salud ahorran, además, tiempo a los pacientes.

La auditoría concluyó que los objetivos de e-salud no se habían alcanzado ya que, a pesar de los planes iniciales, los datos del sistema sanitario aún no podían utilizarse para el tratamiento de las enfermedades ni para la elaboración de las estadísticas nacionales ni para mantener registros o facilitar comprobaciones. Las recetas digitales representan la única solución electrónica creada por el Estado que se utilizaba en la práctica. El uso de grabaciones e imágenes digitales ha sido modesto y el Registro Digital no ha acabado de funcionar pese a los cinco años transcurridos desde su finalización. La razón que subyace al débil lanzamiento de e-salud es la falta de programación

37. La Oficina Nacional de Auditoría de Estonia. Actividades del Estado en la implantación del sistema de e-salud, 2014. https://www.riigikontroll.ee/tabid/206/Audit/2311/Area/21/language/en-US/Default.aspx

y de criterio sistemático de la actividad desarrollada desde el Ministerio de Asuntos Sociales en el desempeño de su función como gestor estratégico para la implantación y desarrollo de e-salud.

4.4. Establecimiento de criterios de auditoría: la Carta del Estado Electrónico

La NAOE también ha tomado la iniciativa en la definición de los derechos de los ciudadanos en e-Estonia. En 2007 auditamos la calidad de los servicios públicos en la sociedad de la información y observamos que, si bien la legislación prohibía el exceso de trabajo de las personas y permitía la administración electrónica, los organismos administrativos tendían a seguir prestando los servicios públicos de una manera más ventajosa para los funcionarios que para los ciudadanos. La principal conclusión de la auditoría fue que se mandaba a las personas de un sitio a otro con una frecuencia impropia de una administración electrónica. Con el fin de mejorar la situación, la NAOE decidió establecer principios de prestación de servicios públicos en un entorno digital y al mismo tiempo establecer criterios de auditoría para nosotros mismos.

El documento recibió el nombre de Carta del Estado Electrónico (2008) y fue diseñado para que fuera utilizado como estándar nacional para los servicios electrónicos[38]. La Carta enumera los derechos que tienen las personas cuando se comunican con agencias públicas a través de la administración electrónica. Permite a dichas agencias revisar sus operaciones con facilidad y establecer objetivos claros y sencillos de medir para, así, conseguir el establecimiento de procedimientos más centrados en los ciudadanos. La Carta también cubría la necesidad de adoptar criterios de auditoría y buenas directrices para el sector público. La NAOE y el Canciller de Justicia actualizaron la carta en 2018. En la situación actual, en la que la mayoría de los estonios se comunican a través de las TIC y la información a menudo se presenta, almacena y reenvía electrónicamente, es particularmente importante no agobiar innecesariamente a las personas y promover medios sencillos de comunicación electrónica[39].

5. Perspectiva de futuro: descubrir un paisaje desconocido

Las nuevas tecnologías y la digitalización han hecho que los datos sean accesibles y la gestión más transparente. Los medios de comunicación y los ciudadanos tienen acceso a información que antes solo podían conocer los gobiernos o las EFS.

La transformación digital es el resultado de la evolución natural, que nos ha llevado a una nueva situación, a un escenario desconocido. Estos cambios están modificando el funcionamiento de la sociedad y del sector público. Algunos de ellos son visibles y positivos, otros

38. La Carta del Estado Electrónico actualizada puede leerse en: https://www.riigikontroll.ee/Riigikontrollipublikatsioonid/Muudpublikatsioonid/Eharta/tabid/305/language/enUS/Default.aspx

39. La Oficina Nacional de Auditoría de Estonia. Carta del Estado Electrónico o de Derechos de todos en el Estado Electrónico, 2018. https://www.riigikontroll.ee/Riigikontrollipublikatsioonid/Muudpublikatsioonid/Eharta/tabid/305/language/enUS/Default.aspx

son problemáticos y traen consigo riesgos que deben ser abordados y que a veces resultaban invisibles pero que ahora están emergiendo en el proceso de desarrollo de las nuevas tecnologías. El Premio Nobel y ex economista jefe del Banco Mundial, Joseph Stiglitz, dijo una vez: «Tenemos que entender mejor estas nuevas tecnologías para poder conocer con mayor claridad hacia dónde nos dirigimos»[40].

La digitalización puede parecer un camino unidireccional hacia un futuro mejor, pero inevitablemente surgirán obstáculos inesperados. La dependencia de la tecnología y de los sistemas de información puede influir significativamente en los procesos de formulación de políticas. En el caso de Estonia, ha habido algunos supuestos en los que no se han adoptado o se han pospuesto decisiones políticas porque se ha visto que su ejecución habría supuesto la previa necesidad de cambios lentos y costosos en los sistemas de información. Por tanto, además de los problemas de manipulación de las redes sociales, la tecnología de la información puede convertirse, en la práctica, en otro problema (ocasionado por la administración) para la toma de decisiones políticas y para el funcionamiento de la Democracia. Tales problemas se pueden prevenir o, al menos, gestionar, pero eso no afecta al hecho de que hubieran sido impredecibles al comienzo del viaje. Este concepto de aceptar lo desconocido a veces puede ser incompatible con el enfoque del auditor clásico, en el que se espera certidumbre.

El Primer Ministro de la India, Narendra Mody, destacó el impacto positivo de la administración electrónica a través de la siguiente frase: «La administración electrónica puede traer un gobierno mínimo y una gestión máxima. Es fácil, eficaz y económica. Aporta empoderamiento, equidad y eficiencia a la economía. Es un instrumento muy útil para solucionar los problemas de la gente»[41]. Estoy de acuerdo con este punto de vista, pero el impacto del desarrollo digital no es en sí mismo positivo. Joseph Stiglitz subraya con razón que la digitalización tiene el potencial de aumentar la productividad de la economía, lo que podría mejorar la calidad de vida de todos, pero sólo si se gestiona correctamente.[42]

Sin una administración adecuada, el creciente papel de la tecnología en nuestras vidas podría cambiar las relaciones entre las personas (y entre estas y las instituciones) de manera que en lugar de resolver problemas existentes, los reforzase. Como se ha visto en el caso de la NAOE, las EFS tienen que asumir nuevas funciones en este mundo cambiante para poder así ayudar a identificar los problemas, a resolverlos y a potenciar la calidad de la gestión pública, lo que supone que las propias Instituciones Nacionales de Control tienen que cambiar y adaptarse a esa nueva realidad.

40. BBVA; «Premio Nobel Stiglitz explora los desafíos sociales que plantea la revolución digital», 2018. https://www.bbva.com/en/nobel-laureate-stiglitz-explores-the-social-challenges-posed-by-the-digitalrevolution/

41. MODI, Narendra; «India debe convertirse en una India digital, que es una sociedad basada en el conocimiento», 2014. https://www.narendramodi.in/india-should-become-a-digital-india-which-is-a-knowledge-based-societyand-economy-5977.

42. SAMPLE, Ian; «Joseph Stiglitz sobre inteligencia artificial: «Vamos hacia una sociedad más dividida», The Guardian, 2018. https://www.theguardian.com/technology/2018/sep/08/joseph-stiglitz-on-artificialintelligence-were-going-towards-a-more-divided-society

6. Bibliografía

BBVA; «El Premio Nobel Stiglitz explora los desafíos sociales que plantea la revolución», 2018. https://www.bbva.com/en/nobel-laureate-stiglitz-explores-the-socialchallenges-posed-by-the-digital-revolution/

Diccionario de Cambridge. https://dictionary.cambridge.org/dictionary/english/e-governance

El Centro de Información e-Estonia; E-Estonia. Bloques de construcción de e-Estonia, 2019. https://e-estonia.com/solutions/

El Centro de Información e-Estonia; E- Estonia. E-Governance, 2019. https://eestonia.com/solutions/e-governance/

El Centro de Información e-Estonia; Guía E-Estonia. https://investinestonia.com/wpcontent/uploads/eestonia-guide-veeb.pdf

El Centro de Información e-Estonia; E-Estonia. Factsheet, 2019. https://invest.gg.go.kr/wpcontent/uploads/sites/29/2019/01/1.e-estonia.pdf

El Centro de Información e-Estonia; i-Votación. Factsheet, 2019. https://e-estonia.com/wpcontent/uploads/2019sept-facts-a4-v02-i-voting.pdf

Comisión Europea; Mercado único digital. Factsheet, 2017. https://ec.europa.eu/digitalsingle-market/en/news/digital-skills-gap-europe

La Academia de Gobierno Electrónico; Gobierno Electrónico. Factsheet, 2019. https://e-estonia.com/wpcontent/uploads/2019sept-facts-a4-v03-e-governance.pdf

La Fundación de Tecnología de la Información para la Educación; Resumen histórico 1997-2017. https://www.hitsa.ee/about-us/historical-overview/1997-2000

Ministerio de Asuntos Económicos y Comunicaciones; Agenda digital 2020 para Estonia, 2018. https://www.mkm.ee/sites/default/files/digital_agenda_2020_web_eng_04.06.19.pdf

Blog de Educación Ejecutiva del MIT Sloan; El imperativo de transformación del negocio digital. https://executive.mit.edu/blog/the-digital-business-transformation-imperative#.XbrlqEl7kcQ

MODI, Narendra; «La India debe convertirse en una India digital, que es una sociedad y economía basadas en el conocimiento», 2014. https://www.narendramodi.in/india-should-become-a-digital-indiawhich-is-a-knowledge-based-society-and-economy-5977

La Oficina Nacional de Auditoría de Estonia; Actividades del Estado en la implementación de la e-salud, 2014. https://www.riigikontroll.ee/tabid/206/Audit/2311/Area/21/language/enUS/Default.aspx

La Oficina Nacional de Auditoría de Estonia; Eficacia del desarrollo de una banda ancha de Internet de alta velocidad, 2015. https://www.riigikontroll.ee/tabid/206/Audit/2346/Area/4/language/en-US/Default.aspx

La Oficina Nacional de Auditoría de Estonia. Garantizar la seguridad y conservación de las bases de datos nacionales estonias de importancia crítica, 2018. https://www.riigikontroll.ee/tabid/206/Audit/2462/language/en-US/Default.aspx

La Oficina Nacional de Auditoría de Estonia; Carta del Estado Electrónico o Derechos de todos en el Estado Electrónico, 2018. https://www.riigikontroll.ee/Riigikontrollipublikatsioonid/Muudpublikatsioonid/Eharta/tabid/305/language/en-US/Default.aspx

La Oficina Nacional de Auditoría de Estonia; Implementación del sistema de medidas de seguridad TIC en gobiernos locales, 2018. https://www.riigikontroll.ee/tabid/206/Audit/2466/language/enUS/Default.aspx

La Oficina Nacional de Auditoría de Estonia; Gestión de riesgos de desarrollo de software en el sector público, 2019. https://www.riigikontroll.ee/tabid/206/Audit/2488/language/enUS/Default.aspx

La Oficina Nacional de Auditoría de Estonia. Prevención de la corrupción en la organización del trabajo de municipios rurales y ciudades, 2012. https://www.riigikontroll.ee/tabid/206/Audit/2269/OtherArea/1/language/enUS/Default.aspx

La Oficina Nacional de Auditoría de Estonia. Resumen de bases de datos guardadas en municipios, pueblos y ciudades, 2017. https://www.riigikontroll.ee/tabid/206/Audit/2420/language/enUS/Default.aspx

La Oficina Nacional de Auditoría de Estonia. Visión general de los bienes raíces de los gobiernos locales y su gestión, 2016. https://www.riigikontroll.ee/tabid/206/Audit/2413/OtherArea/1/language/etEE/Default.aspx

La Oficina Nacional de Auditoría de Estonia. Utilidad de los servicios electrónicos públicos, 2016. https://www.riigikontroll.ee/tabid/206/Audit/2411/language/en-US/Default.aspx

ROOSNA, Sandra; RIKKE Raul (eds); e-Estonia: e-Governance in Practice, e-Governance, Academia, Tallin, 2019.

Riigikontroll. Ilevaade riigi vara kasutamisest ja s-ilimisest 2018.–2019. aastal, 2019. https://www.riigikontroll.ee/Riigikontrollipublikatsioonid/Riigikontrolliaastaaruanneparlamendile/tabid/110/language/et-EE/Default.aspx

SAMPLE, Ian; «Joseph Stiglitz sobre inteligencia artificial: «Vamos hacia una sociedad más dividida», The Guardian, 2018. https://www.theguardian.com/technology/2018/sep/08/joseph-stiglitz-on-artificialintelligence-were-going-towards-a-more-divided-society

Estadísticas Estonia. El árbol de la verdad muestra cómo le va a Estonia, 2019. https://www.stat.ee/news-release-2019-123

Naciones Unidas. Departamento de Asuntos Económicos y Sociales. Base de conocimientos de NU sobre gobierno electrónico. https://publicadministration.un.org/egovkb/en-us/About/UNeGovDD-Framework#whatis

La transformación digital en el Tribunal de Cuentas: aprovechando las nuevas tecnologías para contribuir a la mejora en la gobernanza pública

MARÍA DOLORES GENARO MOYA
Consejera del Tribunal de Cuentas[1]. Profesora Titular de la Universidad de Granada

RESUMEN

Las Tecnologías de la Información y la Comunicación han influido de forma muy significativa en numerosos aspectos de nuestra sociedad a lo largo de las últimas décadas. El Sector Público no ha sido ajeno a estas transformaciones y, consecuentemente, ha cambiado la forma de prestar los servicios, la forma de relacionarse con los ciudadanos, la forma de trabajar de los empleados públicos y ha mejorado la eficiencia y la calidad de los procedimientos de toma de decisiones. En este contexto, las Instituciones de Control Externo no pueden permanecer ajenas a la transformación digital que está teniendo lugar en las entidades públicas que fiscaliza y deben, por una parte, adoptar nuevos enfoques en las fiscalizaciones y, por otra, emplear nuevas herramientas para realizar sus funciones. El Tribunal de Cuentas ya comenzó a transitar este largo camino hacia la transformación digital hace unos años y cuenta con una estrategia a medio plazo para avanzar, teniendo en cuenta los retos que se presentan ante un escenario que evoluciona muy rápidamente y que implicará incrementar los recursos financieros y humanos dedicados a esta transformación. En este escenario, el diseño y ejecución de una estrategia a medio plazo que implique la creación de capacidades en la institución, que comprometa la inversión requerida en herramientas y proyectos y que cuente con el compromiso de los máximos órganos directivos es un pilar esencial para lograr superar los retos y enfrentarse a las amenazas que conlleva el propio proceso de transformación digital.

PALABRAS CLAVE

transformación digital
tecnologías de la información y la comunicación
rendición telemática
estrategia TIC

ABSTRACT

Information and Communication Technologies have had a significant influence on multiple aspects of our society over the past decades. The Public Sector has not been immune to the transformations that have taken place and, therefore, it has changed the way public services are provided, the way Public Administration interacts with citizens, the way civil servants carry out their daily work, and it has improved the efficiency and the quality of decision-making procedures. In this scenario, External Audit Institutions cannot ignore the digital transformation that has taken place in the public bodies that they will eventually audit, and therefore they must adopt new audit approaches and use new technological tools to perform their duties. A few years ago, the Spanish Court of Audit took the first steps along this path to digital transformation which mean that today it has a medium-term strategy so as to progress taking into account the challenges that lie ahead in a rapidly changing environment. This strategy and the profound transformation that it will eventually bring means increasing financial and human resources devoted to different areas affected by the transformation. In this context, to design and execute a medium term strategy, that commits to the required investment and that could have the commitment of both the Board and the President of the institution, is a key element in order to overcome future challenges and to face the threats posed by the digital transformation process.

KEYWORDS

digital transformation
e-information and communication technologies
online accountability
ICT strategy

1. Miembro de la Comisión de Estrategia TIC y Presidenta de la Comisión de Coordinación Tribunal de Cuentas-OCEX para el impulso de la administración electrónica.

«**Members of the International Organization of Supreme Audit Institutions (INTOSAI)**, (...) proclaimed that the future directions for public auditing depend on the SAIs' and INTOSAI's strong commitment to: (...) II. Responding effectively to opportunities brought by technological advancement, (...) - SAIs could promote the principle of availability and openness of data, source code and algorithms. - SAIs could aim to make better use of data analytics in audits, including adaptation strategies, such as planning for such audits, developing experienced teams for data analytics, and introducing new techniques into the practice of public audit[2].»

Declaración de Moscú
XXIII INCOSAI, Moscú, Septiembre, 2019

1. Introducción

Las Tecnologías de la Información y la Comunicación (TIC) llegaron para quedarse en numerosos ámbitos de nuestras sociedades y en nuestra vida cotidiana. Seguramente no todos percibimos los cambios que las TIC han introducido en nuestras vidas como necesariamente positivos, sin embargo, nos guste o no, son inevitables y debemos adaptarnos a ellos tanto en el ámbito personal como en el profesional. En este escenario, la Administración Pública y las instituciones que velamos por su buen funcionamiento, debemos adaptarnos y sacar el máximo partido a estas transformaciones incrementando la eficacia y eficiencia del trabajo diario y de los servicios públicos.

Tomando este punto de partida, el presente artículo aborda muy brevemente en el siguiente apartado la transformación digital que se ha producido en la administración pública española en las últimas décadas, como punto de partida para tratar de determinar de qué forma pueden utilizar las Instituciones de Control Externo (ICEX) las TIC aprovechando al máximo las ventajas que proporcionan para el ejercicio de sus funciones. A continuación, se describe el proceso de transformación digital que se viene produciendo en el Tribunal de Cuentas y cómo han sido superados los retos que han surgido en dicho proceso. Finalmente, se abordan las perspectivas futuras de una trasformación que no estará exenta de retos, dificultades y amenazas, y para la que se deberán identificar las prioridades, entre las que sin duda se encuentra la inversión en nuevos proyectos y herramientas y el desarrollo de capacidades a través de la formación del personal de la institución.

2. La transformación digital de la Administración Pública Española

Los relevantes cambios que la utilización de las TIC ha introducido en nuestras vidas afectan, con mayor o menor intensidad, a todos los ámbitos de las mismas, desde cómo nos relacionamos con los demás o en qué ocupamos nuestro tiempo de ocio hasta cómo diseñamos nuestros hogares para ahorrar energía y/o tiempo o, simplemente, hacerlos más cómodos. Lógicamente, de la misma forma, nuestro ámbito profesional y laboral se ha visto claramente afectado por la introducción, más o menos progresiva, de las TIC. Pocas profesiones —o quizás ninguna— han permanecido inmunes a dichos cambios durante las últimas

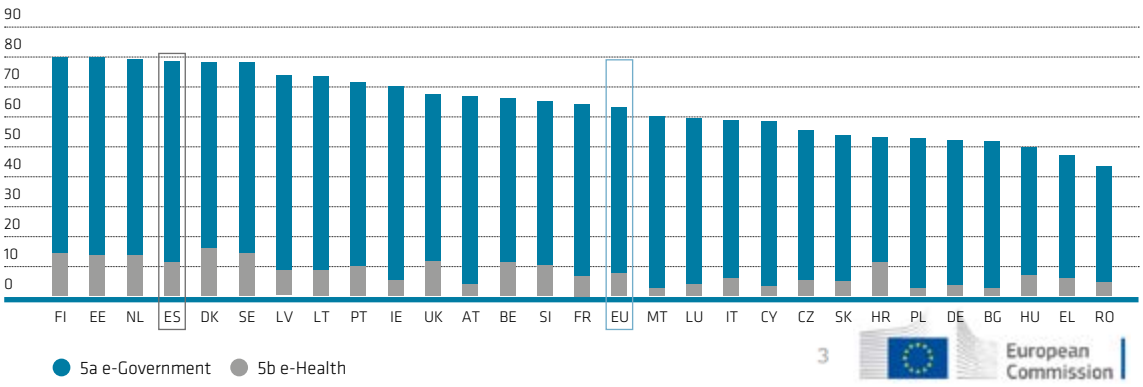
2. INTOSAI (2019a).

décadas, lo que ha conducido, en muchos casos, a un importante incremento de la productividad, a la reducción de empleo en ciertas actividades y a la creación de puestos de trabajo en aquellas vinculadas con el desarrollo de las TIC y su aplicación[3].

El sector público no ha sido una excepción a estos cambios y la introducción de las TIC no solamente ha afectado a la prestación de los servicios desde las instituciones públicas, sino que el entorno de trabajo del empleado público se ha modificado generando transformaciones relevantes en la forma de trabajar, en las herramientas empleadas a diario y en sus procedimientos, con el fin de adaptarse a este importante cambio de escenario. Expresiones como Esquema Nacional de Interoperabilidad (ENI), Esquema Nacional de Seguridad (ENS), Ciberseguridad, Administración Digital, Registro Electrónico, Gobierno Abierto, IA (Inteligencia Artificial) o Blockchain, entre muchos otros, son términos que con mayor o menor frecuencia utilizamos o escuchamos en nuestro trabajo diario los empleados públicos.

Este trascendental cambio en los servicios públicos se está produciendo con distinta intensidad y/o dificultad y con diferente grado de rapidez dependiendo fundamentalmente de las circunstancias de los países y de sus administraciones, así como de la voluntad y del nivel de preparación y formación de los trabajadores públicos implicados. Existen ejemplos de países en los que la administración pública es fundamentalmente digital, como es el caso de Finlandia o Estonia, que ocupan en 2019 los dos primeros puestos en el indicador de servicios públicos digitales del Índice de la Economía y la Sociedad Digitales (DESI) elaborado por la Unión Europea. Estonia es un claro ejemplo de un país que ha llegado a ser, en muy pocos años, una clara referencia al contar con un sector público altamente digitalizado. Por el contrario, encontramos países en los que este cambio se está produciendo a un ritmo más lento y se sitúan en las últimas posiciones en el ranking de digitalización, con un indicador de servicios públicos digitales del Índice DESI inferior a la media europea, como es el caso de Hungría, Grecia o Rumanía.

GRÁFICO 1.
ÍNDICE DE LA ECONOMÍA Y LA SOCIEDAD DIGITALES (DESI). SERVICIOS PÚBLICOS DIGITALES (2019)



Source: DESI 2019, European Commission
DESI Report 2019 - Digital Public Services

3. L. Gortazar (2018) realiza una interesante revisión de investigaciones recientes acerca del impacto de la digitalización en el empleo. En M.L. Rodríguez (2018) se analiza el avance de la digitalización en España, su impacto sobre las instituciones del Derecho del Trabajo y sugiere algunas medidas a adoptar en el proceso de transición hacia una economía digital, especialmente para evitar la bipolaridad que podría producirse en el mercado de trabajo a consecuencia de la digitalización.

En España, las TIC hacen posible, sin lugar a dudas, la prestación de los servicios públicos de una forma más eficiente, más productiva y con mayor inmediatez. Desde los trámites más sencillos —pedir una cita médica o realizar una matrícula universitaria— hasta los más complejos —presentar ofertas a un proceso de contratación pública, elaborar y remitir una factura electrónica, contar con teleasistencia domiciliaria o emplear aplicaciones móviles sanitarias[4]—, ya pueden ser realizados desde casa o desde la oficina sin desplazarse, a través de internet. Según el Informe DESI 2019, *«en el ámbito de los servicios públicos digitales, España ocupa el cuarto puesto entre los países de la UE, muy por encima de la media… El país obtiene un buen rendimiento en el indicador de datos abiertos, en el que se sitúa en segundo lugar. Existe un elevado nivel de interacción en línea entre las autoridades públicas y los ciudadanos. El 76% de los usuarios de internet españoles participa activamente en los servicios de administración electrónica.»* Como factores impulsores de estos cambios, se encuentran, lógicamente, los cambios tecnológicos y la demanda creciente de mejora de los servicios públicos por parte de los ciudadanos, pero también los cambios normativos introducidos, así como el carácter prioritario del desarrollo de la administración electrónica otorgado por parte del gobierno central, autonómico o local.

Un ejemplo reciente[5] de normas relevantes, lo constituyen las leyes 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas[6] junto con la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público[7], que contemplan la tramitación electrónica como la actuación habitual de las Administraciones Públicas. Con esta normativa, se pretende mejorar el cumplimiento de los principios de eficacia, eficiencia y de ahorro de costes, de las obligaciones de transparencia y de las garantías de los ciudadanos. Con anterioridad a estas ya habían entrado en vigor el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad (ENS) en el ámbito de la Administración Electrónica, así como el Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica, que recoge aspectos fundamentales en el funcionamiento y las relaciones entre las Administraciones Públicas. Dado el elevado y disperso

4. Los sistemas de salud andaluz y catalán, por ejemplo, han creado aplicaciones denominadas «App Salud Responde» y «AppSalut», respectivamente.

5. Con anterioridad, la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, ya consagraba el derecho de los ciudadanos a acceder electrónicamente a los servicios públicos e impulsó la implementación de las TIC en la Administración.

6. La Ley 39/2015 se refiere, entre otras cuestiones a los derechos de las personas en sus relaciones con las AAPP; a la asistencia en el uso de medios electrónicos; a los registros electrónicos; a los sistemas de identificación de los interesados en el procedimiento; a las notificaciones a través de medios electrónicos; a la emisión de documentos y a la validez y eficacia de las copias realizados por las Administraciones Públicas; a los documentos aportados por los interesados; y al archivo de documentos.

7. La Ley 40/2015 se refiere, entre otras cuestiones, a los sistemas de identificación electrónica y de firma electrónica del personal al servicio de las Administraciones Públicas; a la sede electrónica; al archivo electrónico de documentos; al intercambio de datos en entornos cerrados de comunicación; a la actuación administrativa automatizada; a la obligación de que las Administraciones se relacionen entre sí por medios electrónicos; al funcionamiento electrónico de los órganos colegiados; a los sistemas electrónicos de información mutua; a la gestión compartida de los servicios comunes que incluye los sistemas de información y comunicaciones; a la aplicación del ENI y del ENS; a la reutilización de sistemas y aplicaciones de propiedad de la Administración y a la transferencia de tecnología entre Administraciones.

número de normas que, de una u otra forma, regulan aspectos relacionados con la administración electrónica o digital, así como la importancia que el conocimiento de la regulación en la materia tiene para funcionarios, ciudadanos y empresas, la Secretaría General de Administración Digital ha venido promoviendo la elaboración de un Código de Administración Electrónica actualizado, que comprende *«la legislación relativa a la administración electrónica, para ofrecer una herramienta de interés y utilidad para los profesionales, gestores y estudiosos de la materia*[8]*»*.

Considerando el escenario descrito, resulta obvio afirmar que la utilización de las TIC está impulsando en el sector público una transformación que afecta necesariamente a las ICEX, en el ejercicio de su función, tanto en lo que respecta al ámbito objetivo del control —con una Administración Pública más *«digitalizada»* el análisis de los estados financieros de las entidades públicas va inevitablemente perdiendo peso en favor de la fiscalización de los procedimientos de gestión, de los sistemas de control interno, de las herramientas tecnológicas empleadas o de la calidad de los datos utilizados en la adopción de decisiones de gestión—, como al enfoque y a la metodología empleada en las fiscalizaciones. En relación con estos últimos aspectos, el control externo debería centrarse en determinar la eficacia y eficiencia de los servicios públicos, en evaluar el impacto y la eficacia de las políticas públicas o en analizar el funcionamiento, las incidencias y el buen uso de los sistemas de información en los que descansan cada vez más aspectos fundamentales de cualquier entidad pública. Otros aspectos relevantes son la seguridad de la información, de la protección de los datos de carácter personal o la coherencia y la corrección de las bases de datos que se emplean en la toma de decisiones de los gestores públicos.

Todos estos cambios se están produciendo a nivel mundial y vienen generando una creciente preocupación en el seno de las ICEX y de las organizaciones regionales, nacionales e internacionales que las agrupan, de forma que, desde hace algunos años, se vienen celebrando foros de debate en los que se aborda la digitalización desde diversos puntos de vista. De hecho, en el XXIII INCOSAI celebrado en Moscú el pasado mes de septiembre, uno de los dos temas centrales del encuentro fue *«Utilizando las TIC para desarrollar la Administración Pública»* y se adoptó la decisión de crear, en el seno de la INTOSAI[9], un Grupo de Trabajo sobre el Impacto de la Ciencia y la Tecnología en la Auditoría[10], que se centrará en los principales avances en áreas tales como inteligencia artificial, tecnología *blockchain*, ciberseguridad, análisis de datos o red de telefonía móvil 5G, entre otras.

Por otra parte, en marzo de 2019, se celebró en Jerusalén la III Conferencia Conjunta EUROSAI-ASOSAI *«Cuestiones Emergentes y Situaciones de Emergencia»,* en la que se dedicó un taller a abordar el tema *«Aprovechando al máximo las Tecnologías de la Información: Retos y oportunidades»*. Para su desarrollo, desde el Tribunal de Cuentas de España

8. Código de Administración Electrónica (2019).

9. INTOSAI: International Organization of Supreme Audit Institutions.

10. INTOSAI Working Group On Impact Of Science & Tech On Auditing: https://www.intosai.org/what-we-do/knowledge-sharing/working-groups

(que presentó y dirigió el taller) se lanzó una breve encuesta relacionada con este tema a las 50 Entidades Fiscalizadoras Superiores (EFS) miembros de EUROSAI[11] y a las 47 EFS miembros de ASOSAI[12], obteniéndose 34 y 12 respuestas, respectivamente, a cuyos resultados haremos referencia a lo largo del presente artículo, ya que contribuyen a trazar un diagnóstico del grado de utilización de las TIC en el trabajo diario de las EFS de países de nuestro entorno.

3. La utilización de las tecnologías de la información y la comunicación en una Institución de Control Externo

Como ya se ha mencionado, la introducción de las TIC en las Administraciones Públicas y en las Instituciones de Control, ha modificado diversos aspectos en el ejercicio del Control Externo, de forma tal que la implementación de las TIC en una ICEX puede extenderse, fundamentalmente, a tres ámbitos diferenciados:

a. La interacción con terceras partes: El proceso de intercambio de información.
b. Las herramientas para llevar a cabo el procedimiento fiscalizador.
c. La digitalización de los procedimientos internos.

3.a. La interacción con terceras partes: El proceso de intercambio de información

No cabe duda de que el núcleo de la actividad desarrollada por una ICEX se fundamenta en el intercambio de la información que ésta mantiene a lo largo del año con otras instituciones públicas y privadas, así como con personas físicas que se dirigen a la misma por distintos motivos. De esta forma, en ciertos meses del año se reciben las cuentas anuales que rinden las entidades públicas obligadas a ello y que constituyen uno de los puntos de partida de la actividad fiscalizadora. Pero además de las cuentas, a lo largo del procedimiento fiscalizador resulta imprescindible recibir numerosa y, en ocasiones, voluminosa documentación y/o bases de datos empleadas en las verificaciones. Además, una vez finalizada la fiscalización, la ICEX ha de remitir a las entidades fiscalizadas los resultados provisionales de los trabajos realizados o cualquier otra información de interés que surja a lo largo del procedimiento.

Pero también resulta muy relevante el intercambio de información que tiene lugar entre la institución y las personas físicas o jurídicas que se relacionan con ella por diferentes motivos: a lo largo de un procedimiento de contratación pública; durante los procesos de selección de personal, ya sea mediante procedimientos de concurso o de oposición; a través de la interposición de una denuncia ante la fiscalía o la sección de enjuiciamiento por un mal uso de los fondos públicos (en caso de contar con la competencia jurisdiccional, como es el

11. EUROSAI: European Organisation of Supreme Audit Institutions.

12. ASOSAI: Asian Organization of Supreme Audit Institutions.

caso del Tribunal de Cuentas de España); las peticiones que se reciben a través del portal de transparencia o las comunicaciones remitidas en un canal de denuncias, entre otros ejemplos posibles.

Lógicamente, en un entorno como el que hemos descrito en el apartado anterior, en el que tanto la Administración Pública como las empresas y los ciudadanos hacen uso de las TIC para relacionarse entre sí, resulta obvio que los mecanismos que establezca una ICEX para interactuar con terceros —ya sean estos públicos o privados— deben contar con un fuerte componente tecnológico que permita, como mínimo, que dicha interacción se produzca vía telemática. La forma más básica y obvia es la utilización del correo electrónico, pero se trataría de llegar a contar con una vía de intercambio de información que reúna ciertos requisitos de seguridad y veracidad, entre otros, que permita el tratamiento automatizado de la información recibida, especialmente cuando se reciben datos estructurados que pueden ser introducidos automáticamente en las herramientas que permitan su análisis y tratamiento para obtener unos resultados útiles para la fiscalización.

En la encuesta mencionada anteriormente se preguntó a las EFS miembros de EUROSAI si empleaban fundamentalmente medios telemáticos para establecer esta comunicación bidireccional con los organismos públicos que fiscalizan y algo más del 70 por 100 de las 34 EFS de EUROSAI que respondieron, confirmaron que sí los emplean, siendo este porcentaje muy similar —67 por 100— en el caso de las 12 respuestas recibidas de ASOSAI.

3.b. Las herramientas para llevar a cabo el procedimiento fiscalizador

Otro aspecto importante lo constituye la utilización de las TIC por parte de las entidades públicas que conforman el ámbito subjetivo de la actividad fiscalizadora de una ICEX, ya que ha constituido un revulsivo esencial como impulsor de importantes cambios en la metodología y en las herramientas que se han venido empleando a lo largo de las diferentes fases del procedimiento fiscalizador y, especialmente, en la realización de los trabajos de campo y en la elaboración de los informes. Así, el hecho de que la entidad pública fiscalizada cuente con un elevado grado de digitalización de sus procedimientos internos (contables, de gestión...) obligará inevitablemente al órgano de control a enfocar y desarrollar la fiscalización con una perspectiva diferente y, de forma obligada, a emplear las TIC más intensamente. Por ejemplo, seguramente deberán utilizar herramientas que permitan el análisis de datos, el procesamiento electrónico de información o el análisis de los sistemas informáticos de la entidad.

Por ejemplo, resultará esencial contar con una herramienta que permita la gestión electrónica de una fiscalización, incorporando procedimientos automatizados, gestión documental, intercambio de información entre los miembros del equipo o haga posible la supervisión de todo el proceso.

La necesidad para una ICEX de analizar grandes volúmenes de datos o *«big data»* a lo largo de una fiscalización ha crecido exponencialmente en pocos años, en la medida en que los gobiernos emplean y gestionan cada vez más esos datos para la toma de decisiones. La auditoría de *«big data»* implica mucho más que recopilar y analizar gran cantidad de información, por el contrario, supone realizar los trabajos de auditoría de una forma diferentes.

Por ejemplo, en lugar de auditar muestras, se puede auditar el conjunto de la población; se puede auditar todo un procedimiento o un programa y además, puede proporcionar nuevos métodos para mejorar la calidad de la auditoría a través de[13]:

- La eliminación de la limitación impuesta por los recursos humanos disponibles, la mejora de la eficiencia de la auditoría y la ampliación del alcance de la misma.
- La mejora de la capacidad de las EFS de proporcionar con antelación alertas sobre riesgos económicos y sociales a través de la realización de predicciones.
- La ampliación de los horizontes de las EFS para promover el desarrollo sostenible.

Ante este escenario, resulta evidente la necesidad de contar con potentes herramientas y personal capacitado para manejarlas y poder realizar el análisis de datos, aprovechando al máximo el potencial que nos brinda.

También resultaría muy útil, si bien aún constituye un reto, emplear aplicaciones de procesamiento de lenguaje natural para la explotación de grandes volúmenes de información no estructurada, como puede ser la información incluida en los pliegos de los contratos públicos o en las ofertas presentadas en las licitaciones de contratación.

En la encuesta mencionada anteriormente, se preguntó a las EFS si empleaban algún tipo de herramienta electrónica para llevar a cabo y para documentar las fiscalizaciones (TeamMate o similar), obteniéndose una respuesta afirmativa en el 76 por 100 de los casos en EUROSAI, entre los que en torno al 42 por 100 empleaban una herramienta hecha a medida. Este porcentaje descendía al 50 por 100 en ASOSAI, si bien estos contaban mayoritariamente con una herramienta a medida.

Por otra parte, se preguntó por el uso de técnicas y/o herramientas de análisis de datos (como IDEA o ACL) o de algún software estadístico (SPSS, R, Stata, entre otras) durante las fiscalizaciones, a lo que algo más del 80 por 100 de las respuestas en EUROSAI fueron afirmativas y apuntaban a un uso generalizado de IDEA, SPSS y STATA y algunas otras con menor frecuencia. En el caso de ASOSAI, este porcentaje se eleva hasta el 83 por 100, siendo las herramientas de utilización más frecuente las apuntadas anteriormente.

3.c. La digitalización de los procedimientos internos

Por otra parte, las Instituciones de Control deben dar ejemplo como instituciones modernas, altamente digitalizadas, en las que predomine la automatización y la simplificación de sus procedimientos internos, de forma que la utilización de tecnología la lleve a ser **más eficiente y** eficaz en el desempeño de sus funciones.

De esta forma, los trámites que se realizan diariamente, como la remisión de documentación y, en general, la tramitación de procedimientos internos, la gestión de las reuniones de los órganos colegiados de gobierno o la gestión del personal, pueden realizarse, sin duda, de forma más eficiente con la introducción de las TIC, de procedimientos automatizados y más inmediatos que redunden en la mejora del desempeño global de la institución de control.

13. INTOSAI (2019b).

En la encuesta a la que nos venimos refiriendo, se preguntó a las EFS si calificaban su institución como esencialmente *«electrónica o sin papeles»*, obteniéndose una respuesta afirmativa en el 47 por 100 de los casos en EUROSAI, descendiendo este porcentaje al 16 por 100 entre las respuestas procedentes de ASOSAI.

Finalmente, no debemos olvidar la relevancia de la seguridad de la información en una ICEX, que obliga a contar con potentes herramientas que eviten la filtración o el acceso no autorizado a datos personales o a información sensible, los ciberataques, o cualquier otro tipo de amenaza que pueda llegar a través de las herramientas tecnológicas. Este también debería ser un aspecto objeto de la máxima atención por la alta dirección de las instituciones, de forma que se identifiquen los riesgos y vulnerabilidades, protegiendo a la institución frente a ataques externos que pudieran ocasionar desde la obtención de información sensible hasta, incluso, la paralización de su actividad durante unos días.

4. La experiencia del Tribunal de Cuentas en la implementación de la tecnología en su ámbito de actuación

Desde hace más de una década el Tribunal de Cuentas de España viene realizando un enorme esfuerzo en la introducción de las TIC en todos sus ámbitos de actuación con el objetivo de llegar a ser una institución más eficiente, moderna, abierta y transparente, y para reducir progresivamente el uso del papel en sus comunicaciones tanto internas como externas.

Siguiendo el esquema empleado en el epígrafe anterior podemos enumerar algunas de las principales herramientas tecnológicas utilizadas en el seno del Tribunal de Cuentas:

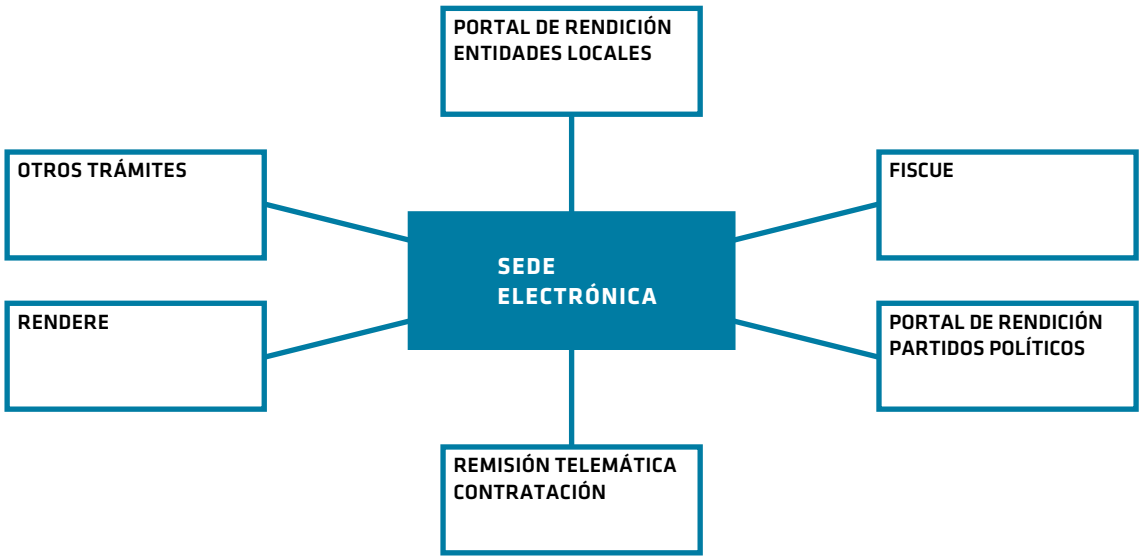
4.a. La interacción con terceras partes: El proceso de intercambio de información

El intercambio de información con las entidades auditadas constituye, sin lugar a duda, un pilar fundamental del procedimiento fiscalizador. Este intercambio comprende tanto la rendición de los estados contables regulada en la normativa correspondiente, como la remisión de documentación en relación con los procedimientos de gestión y de control interno, de bases de datos que permitan realizar análisis y cruces para detectar incidencias e, incluso, fraude o mala gestión, hasta el envío del anteproyecto de informe y la recepción de las correspondientes alegaciones remitidas por los auditados.

Asimismo, se han producido avances relevantes en la Sección de Enjuiciamiento, de forma que, con la creación del Tramitador Procesal, las labores que implican la tramitación de los procedimientos de exigencia de responsabilidad contable pueden llevarse a cabo de forma electrónica. El Tramitador se ha concebido como un entorno en el que se puede hacer el seguimiento, control y validación de las actuaciones a llevar a cabo en todas las unidades de la Sección de Enjuiciamiento, con la finalidad última de la creación del expediente digital. Esta plataforma está relacionada con otras aplicaciones que la complementan, como la aplicación de Registro o el Portafirmas Electrónico y un hito importante en el desarrollo final de esta herramienta será su conexión con el sistema de remisión telemática de los escritos, documentos y notificaciones que se originen en el procedimiento.

Teniendo en cuenta la trascendencia y la intensidad de la interacción del Tribunal de Cuentas con las entidades públicas auditadas, no resulta extraño, por tanto, que éste haya sido el ámbito en el que más se ha avanzado en el seno de la institución en términos de diseño e implementación de herramientas tecnológicas que faciliten y hagan más eficiente el proceso de remisión y de recepción de información tanto para el Tribunal como para los gestores públicos (**Figura 1**).

FIGURA 1.
ALGUNAS HERRAMIENTAS PARA LA RENDICIÓN TELEMÁTICA DE LOS ESTADOS CONTABLES, CONTRATOS PÚBLICOS Y OTRA INFORMACIÓN, IMPRESCINDIBLES PARA LA FISCALIZACIÓN



Fuente: Elaboración propia.

En este sentido, la sede electrónica del Tribunal de Cuentas (**Figura 2**) constituye el eje fundamental a través del cual se canaliza todo el intercambio telemático de información con terceras partes, sean estas entidades públicas, otros órganos de control interno y/o externo o personas físicas y jurídicas.

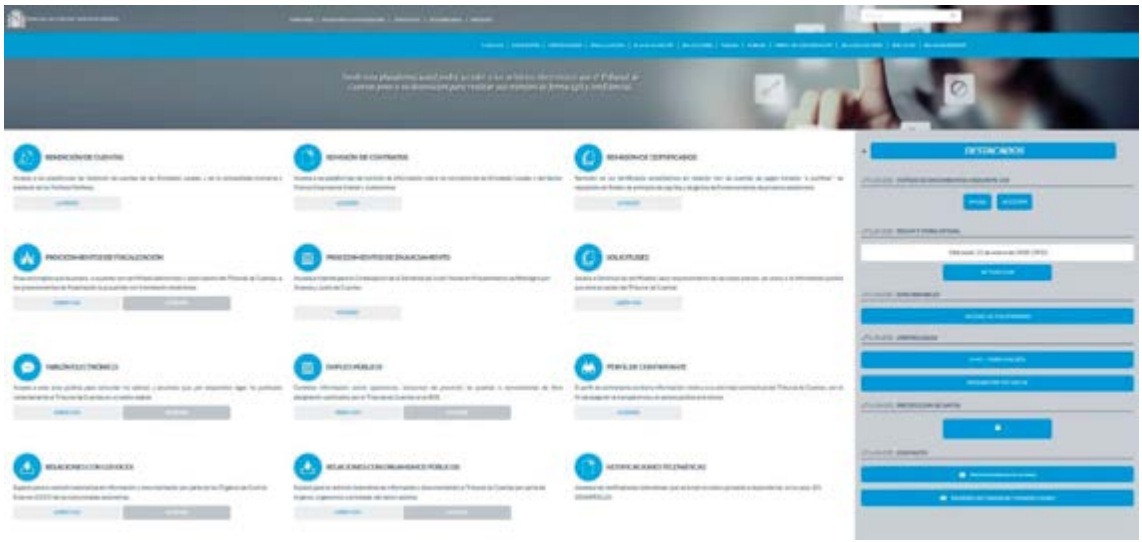
La primera experiencia relevante que se puso en marcha fue el Portal Rendición de Cuentas[14], en 2007, que permite el envío de las cuentas generales de las entidades locales, de las relaciones de contratos y de los expedientes de contratación, así como de los acuerdos contrarios a reparos formulados por el órgano de intervención local, anomalías en la gestión de ingresos y acuerdos con omisión de fiscalización previa[15]. Aunque esta iniciativa está

14. https://www.rendiciondecuentas.es/es/index.html

15. Este Portal comenzó siendo una Plataforma para la rendición de las cuentas de las entidades locales bajo la competencia fiscalizadora del Tribunal de Cuentas, sin embargo, se ha ido extendiendo progresivamente a otras materias relevantes como la información de los contratos públicos y convenios formalizados por las entidades locales y los acuerdos adoptados por dichas entidades contrarios a reparos formulados por el órgano de intervención. Para más información puede consultarse S. Alcázar y R. Pou (2018).

liderada por el Tribunal de Cuentas, en la actualidad cuenta con la participación de la Sindicatura de Comptes de la Generalitat Valenciana, la Audiencia de Cuentas de Canarias, la Cámara de Cuentas de Madrid, la Sindicatura de Comptes de les Illes Balears, el Consejo de Cuentas de Castilla y León, la Sindicatura de Cuentas del Principado de Asturias, la Cámara de Cuentas de Aragón, el Consello de Contas de Galicia y la Cámara de Cuentas de Andalucía. El Portal resulta actualmente una herramienta imprescindible que hace más eficaz y eficiente la fiscalización de las más de 8.000 entidades locales que se encuentran incorporadas y, por otra parte, permite conocer las cuentas de cualquier entidad local, ofreciendo acceso a la información económico-financiera de las mismas, contribuyendo así a una mayor transparencia de la Administración Local.

FIGURA 2.
SEDE ELECTRÓNICA DEL TRIBUNAL DE CUENTAS



Fuente: www.Tribunal de Cuentas.es

Con posterioridad al Portal, se han desarrollado también otras herramientas que hacen posible la rendición telemática de los estados contables de las entidades públicas de ámbito estatal, como es el caso de FISCUE (para la rendición de las cuentas anuales de las entidades del sector público estatal); RENDERE[16], herramienta diseñada para la remisión de los certificados acreditativos en relación con las cuentas de pagos librados «a justificar» y de reposición de fondos de anticipos de caja fija; y el Portal de Rendición de Partidos Políticos diseñado para el envío al Tribunal de Cuentas de las contabilidades ordinarias y electorales y toda la documentación adicional obligatoria por parte de las formaciones políticas[17] y otros obligados a ello.

16. https://sede.Tribunal de Cuentas.es/tribunal-de-cuentas/es/sede-electronica/GRCertificados/

17. https://sede.Tribunal de Cuentas.es/tribunal-de-cuentas/es/sede-electronica/GRCuentas/PartidosPoliticos/index.html

Por otra parte, para la rendición de contratos —relaciones anuales, expedientes e incidencias— por las entidades del Sector Público Estatal y Autonómico obligadas a ello, existe una Plataforma de Rendición Telemática de Contratos (RETECON[18]) que, a través de un portal web, permite la introducción de los datos y de los documentos relativos a los contratos formalizados por las entidades públicas estatales y autonómicas sometidas al control externo del Tribunal de Cuentas.

Finalmente, en relación con las comunicaciones con personas físicas o jurídicas resulta obligada la mención al Portal de Transparencia del Tribunal de Cuentas[19]; el canal para solicitar certificados para el reconocimiento de servicios previos prestados en cualquier Organismo Público o para la concesión de pensiones[20], así como las secciones de la sede electrónica dedicados a las ofertas de empleo público de la institución, al perfil del contratante o a la comunicación con los Órganos de Control Externo autonómicos, entre otros.

4.b. Las herramientas para llevar a cabo el procedimiento fiscalizador

Además de hacer posible la rendición telemática, las TIC ofrecen múltiples posibilidades para hacer más eficiente y eficaz el proceso de gestión y desarrollo de una fiscalización. Así, por ejemplo, en el Tribunal de Cuentas la herramienta empleada para la gestión de los papeles de trabajo ha sido hasta el momento *TeamMate*, aunque su uso ha sido muy desigual entre los diferentes equipos debido a distintas circunstancias. Adicionalmente, se han desarrollado las siguientes aplicaciones a medida para facilitar y agilizar diferentes fases de la fiscalización, contribuyendo al mismo tiempo a disminuir los errores y riesgos de auditoría:

- Análisis y fiscalización de la contratación (FISCON), es una aplicación flexible, integrada con la Plataforma de Rendición Telemática de Contratos, que permite obtener listados y estadísticas sobre la contratación rendida, seleccionar las muestras de los contratos a fiscalizar mediante la inclusión de distintos criterios en función de los objetivos de la fiscalización y extraer de forma automática una síntesis del resultado global obtenido del análisis de los contratos clasificando las deficiencias por tipos y fases de la contratación. Además, resulta de la máxima utilidad para realizar la planificación y supervisión continua de los trabajos durante la fiscalización.
- Base de datos de operaciones de la Administración General del Estado (OPERA), que permite la consulta, visualización y comprobación de las operaciones del presupuesto de gastos, de ingresos y las operaciones no presupuestarias de un determinado ejercicio. Cada una de las operaciones de gastos se enlaza directamente con su documento contable y su documentación soporte digitalizada.
- Aplicación para el examen y comprobación de la Cuenta General de la Seguridad Social (PROFISS), que posibilita analizar y comprobar tanto las cuentas individuales de las entidades que integran el Sistema de Seguridad Social, como la Cuenta General de la Seguridad Social.

18. https://contratacionestatalyautonomica.tcu.es

19. https://www.Tribunal de Cuentas.es/tribunal-de-cuentas/es/transparencia/index.html

20. https://sede.Tribunal de Cuentas.es/tribunal-de-cuentas/es/sede-electronica/GRSolicitudes/Certificados Archivo/Solicitudes.html

- Aplicación para la Fiscalización de la Contabilidad Electoral (FISCELECT), que se emplea en la realización de las diferentes comprobaciones comprendidas en las fiscalizaciones de las contabilidades electorales rendidas telemáticamente.

Junto a estas aplicaciones se utilizan, cada vez con mayor frecuencia, herramientas que permiten el tratamiento y análisis masivo de datos para detectar distintos tipos de deficiencias en áreas en las que la disponibilidad de datos fiables, consistentes, completos, exactos y pertinentes lo permite. IDEA, es el software de análisis de datos empleado con mayor frecuencia, si bien progresivamente el desarrollo de capacidades en el manejo de técnicas de análisis masivo de datos permitirá la utilización de herramientas alternativas disponibles en el mercado. Sin embargo, este quizás sea uno de los ámbitos menos explorados en el Tribunal en el desarrollo de las fiscalizaciones y, por tanto, el potencial de aprovechamiento en el futuro es muy elevado.

4.c. La digitalización de los procedimientos internos

En un entorno de trabajo como el que se ha descrito en los párrafos anteriores, resulta evidente la necesidad de contar con herramientas que permitan el uso de las tecnologías y el abandono progresivo del papel en los procedimientos internos del Tribunal de Cuentas. Para ello, se ha venido desarrollando la Plataforma de Gestión Electrónica (**Figura 3**), que cuenta con diferentes módulos que permiten progresivamente realizar la gestión de todos los procedimientos internos: Reuniones de órganos colegiados; tramitación de expedientes de fiscalización, de enjuiciamiento y de gestión diaria del Tribunal; registro; archivo; portafirmas electrónico y la herramienta de visualización de las comunicaciones recibidas a través de la sede electrónica de la institución.

FIGURA 3.
PLATAFORMA DE GESTIÓN ELECTRÓNICA DEL TRIBUNAL DE CUENTAS

Fuente: Elaboración propia.

Por otra parte, en lo que respecta a la seguridad de la información, el Tribunal de Cuentas aprobó en el año 2016 la creación de una Oficina de Seguridad de la Información que, dependiendo directamente de la Presidencia del Tribunal, vela por todo aquello relacionado con la política de seguridad de la información en la institución, especificando necesidades o requisitos y supervisando el cumplimiento de la legislación y de los controles implantados. Se adoptó así un modelo en el que el responsable de la seguridad de la información no forma parte del servicio TIC del Tribunal, de tal manera que *«La seguridad como función diferenciada»* constituye el pilar fundamental de la política de seguridad de la institución.

Naturalmente, el camino transitado hasta aquí no ha estado exento de dificultades, como resulta fácil imaginar teniendo en cuenta tanto el punto de partida, como la necesaria colaboración de los auditados en el proceso de transformación (Administraciones Públicas, fundamentalmente pero no exclusivamente), la aconsejable y fructífera colaboración con los OCEX autonómicos y, sobre todo, el elevado ritmo al que avanzan las TIC, lo cual dificulta la ingente tarea de *«estar al día»* en todo lo que ello implica para las labores fiscalizadora y de enjuiciamiento. A estas dificultades se han unido otras vinculadas a la disponibilidad de recursos, puesto que todos estos proyectos han demandado elevadas inversiones en desarrollos a medida o en adquisición de licencias de determinado *software,* junto con la movilización o la contratación de los recursos humanos especializados para concebir, diseñar, programar, supervisar y poner en marcha los proyectos. Junto a esto, la formación del personal para adquirir la capacitación en el uso de las nuevas herramientas ha representado uno de los retos a los que se ha enfrentado la institución en estos últimos años y lo seguirá haciendo en el futuro próximo.

Precisamente, una de las conclusiones a las que se llegó durante el taller desarrollado en Jerusalén en relación con las *lecciones aprendidas* por las EFS a lo largo de la implantación de las TIC, fue la necesidad de contar con una buena planificación del proceso de implantación, así como la importancia de invertir pensando en la evolución futura y la rapidez de los cambios en el área tecnológica.

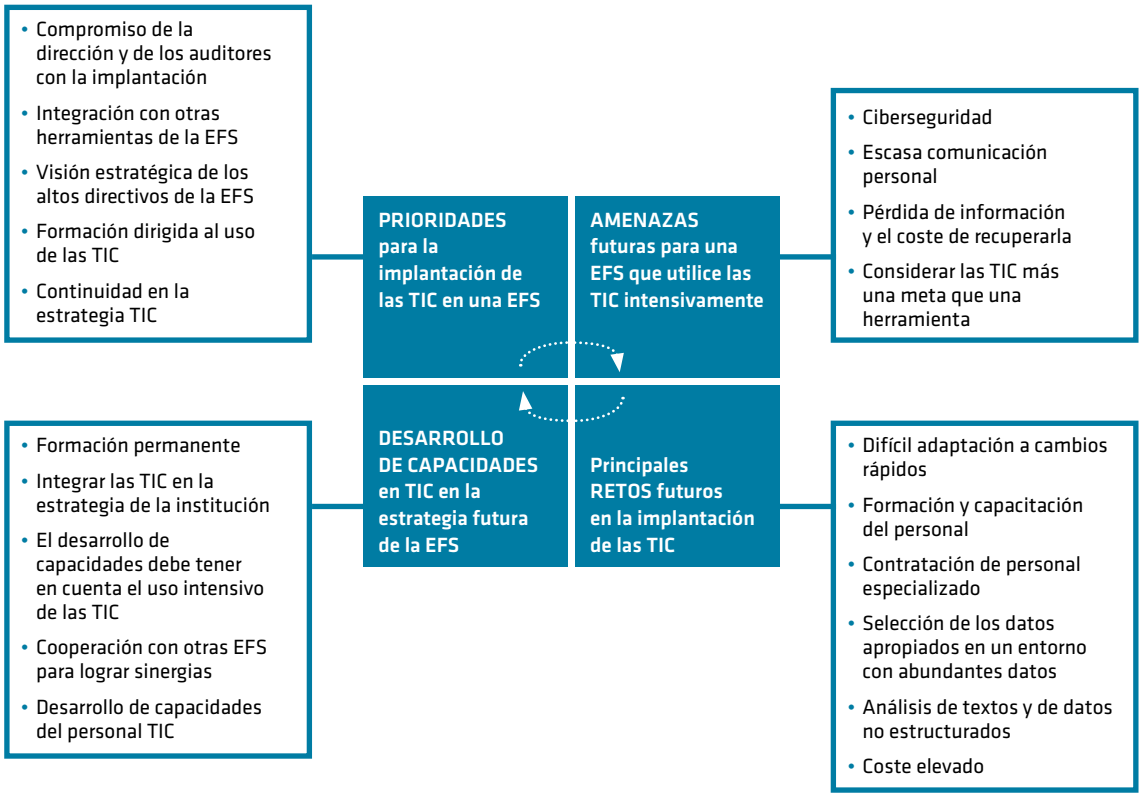
En este sentido, el Tribunal de Cuentas, tal y como se pone de manifiesto en el siguiente apartado de este artículo, en los últimos años ha venido adoptando las medidas oportunas para contar con la planificación adecuada y la inversión necesaria para afrontar este gran reto presente y futuro.

5. Conclusiones: mirando hacia el futuro

Durante el taller celebrado en la Conferencia Conjunta EUROSAI-ASOSAI mencionada anteriormente, tuvo lugar un debate alrededor de una serie de cuestiones ligadas a la evolución futura de las TIC y al proceso de digitalización de una EFS. Las principales conclusiones se recogen en la Figura 4 y se refieren tanto a los retos y prioridades que pueden surgir en la implantación de las TIC en las instituciones como las amenazas que se identifican y el enfoque de desarrollo de capacidades para afrontarla.

Algunas de las cuestiones que se reflejan en la Figura 4, vienen siendo abordadas por el Tribunal de Cuentas desde hace algunos años: formación dirigida a la utilización de nuevas herramientas, dedicación de recursos humanos y financieros a la implementación de las TIC en la institución, contratación de personal especializado en TIC y adaptación a cambios rápidos inducidos por la tecnología y la digitalización.

FIGURA 4.
LA IMPLANTACIÓN DE LAS TIC EN UNA INSTITUCIÓN DE CONTROL EXTERNO: PRIORIDADES, AMENAZAS, RETOS Y DESARROLLO DE CAPACIDADES



Obviamente, la formación y el desarrollo de capacidades del personal de la institución, especialmente de los auditores, se presenta como uno de los principales retos futuros a los que se debería dedicar especial atención y que implicarán el compromiso de la dirección de la institución en la dotación de los recursos financieros y humanos necesarios. El compromiso de los órganos directivos de la institución es, lógicamente, un pilar fundamental, puesto que deben impulsar, planificar y comprometer los recursos para que la implementación de las TIC y su utilización intensiva en los procedimientos de fiscalización (y de enjuiciamiento en el caso del Tribunal de Cuentas) se realice de manera efectiva.

También son relevantes, la continuidad en el proceso de implantación de las TIC; la contratación de personal TIC especializado y su formación continua; la elección de las

herramientas adecuadas para la realización de la fiscalización (i.e. análisis de datos no estructurados); la seguridad de la información que se maneja en el seno de la institución y la necesaria cooperación con otras instituciones para lograr sinergias.

En los últimos años se ha dado un paso muy relevante, al considerarse prioritario poner el acento en un pilar fundamental para impulsar y mantener vivo el proceso de digitalización de la institución: la gobernanza y la cooperación con otros organismos.

En lo que se refiere a la gobernanza del proceso de transformación digital en el Tribunal de Cuentas, el compromiso del Pleno de la institución se reflejó en la aprobación, a principios del año 2015, de la constitución de la Comisión de Estrategia TIC (CETIC) del Tribunal, con el objetivo de orientar y planificar los grandes cambios que se estaban produciendo en la institución en términos de digitalización y afrontar los retos a los que se habrá de enfrentar en el futuro a medida que la implantación de las TIC continúe avanzando. La Comisión está conformada actualmente por la presidenta del Tribunal y dos Consejeras (una en representación de la Sección de Fiscalización y otra de la Sección de Enjuiciamiento) y, entre otras funciones, se encarga de fijar las líneas estratégicas en materia TIC, estableciendo los proyectos de interés prioritario; y de proponer el programa de formación en materia TIC.

Junto con esta planificación y seguimiento ejercidos de forma continuada por la Comisión de Estrategia TIC, en 2018 se aprobó el Plan Estratégico de la institución para el periodo 2018-2021, en el que se incluyó un *Objetivo Específico 4.4: Modernizar los procedimientos internos e impulsar los proyectos de administración electrónica y la utilización de las TIC para reforzar la eficacia y eficiencia en el Tribunal de Cuentas* incardinado en el **Objetivo Estratégico 4: reforzar la gestión de los recursos humanos y materiales del Tribunal de Cuentas bajo los principios de eficiencia, economía, igualdad y transparencia**. Este objetivo específico recoge determinadas medidas que trazan a grandes rasgos las que serán las prioridades del Tribunal de Cuentas en lo que se refiere al proceso de digitalización y utilización de las TIC. Pero, además, podemos encontrar otras medidas a lo largo del Plan Estratégico 2018-2021 estrechamente vinculadas con dicho proceso, como pueden ser impulsar la realización de auditorías de sistemas informáticos o implantar un sistema electrónico de seguimiento de las recomendaciones incluidas en los informes de fiscalización.

De hecho, la realización de auditorías de sistemas de información representa todo un reto para el Tribunal, precisamente por las mismas razones ya apuntadas por A. Minguillón (2016), derivadas de la propia experiencia en este ámbito de la Sindicatura de Cuentas de la Comunidad Valenciana:

- La falta de conocimientos y formación del personal en una materia relativamente novedosa que requiere una cierta especialización.
- La falta de experiencia en el control interno público.
- La existencia de elementos de trabajo «no visibles» para el auditor.
- La dificultad para definir los objetivos de auditoría y la necesaria comunicación interna en los equipos conformados por auditores con diferentes perfiles.
- El imprescindible compromiso de la dirección de la ICEX.

Precisamente en relación con este tipo de auditoría, la INTOSAI, además de contar con un grupo de trabajo[21] desde el año 1989, en su momento elaboró la ISSAI 5300, que ha venido siendo la norma de referencia para la realización de estas auditorías. En la actualidad, tras el cambio hacia el Marco de Pronunciamientos Profesionales de INTOSAI, ha sido publicada en junio de 2019 la *«GUID INTOSAI 5100 Guidance on Audit of Information Systems»* que proporciona un marco para llevar a cabo este tipo de auditorías y constituye la base para el desarrollo de las futuras GUIDs 5100 a 5109 que versarán sobre este tema.

En lo que se refiere a la coordinación, la colaboración y cooperación del Tribunal de Cuentas con los OCEX autonómicos y con otras entidades públicas resulta un pilar fundamental para avanzar unívocamente en el proceso de digitalización de las instituciones.

En este sentido, en septiembre de 2018 se constituyó la Comisión de Coordinación Tribunal de Cuentas-OCEX para el impulso de la administración electrónica, bajo la presidencia de una Consejera del Tribunal de Cuentas, con el objetivo de fomentar la cooperación y colaboración entre las instituciones que la conforman en la implantación de las TIC, diseñando para ello estrategias conjuntas, impulsando la utilización de herramientas electrónicas en sus procedimientos y colaborando en actuaciones de formación, de asistencia técnica y de transferencia de conocimientos.

Además, en lo que respecta a la coordinación y colaboración con otras Administraciones Públicas, uno de los proyectos que tendrán mayor transcendencia y repercusión en la mejora de la gestión será la futura interconexión de la Plataforma de Contratación del Sector Público con las plataformas de rendición de la contratación, lo cual permitirá importar de forma automática la información alojada en la primera plataforma, evitando la doble rendición de la información contractual por parte de los gestores, junto con la posibilidad de realizar cruces automáticos de información durante las fiscalizaciones.

En el ámbito de la función del enjuiciamiento de la responsabilidad contable, se ha avanzado mediante la realización de convenios de colaboración con diversas instituciones como el Colegio de Notarios o el de Registradores de la Propiedad, así como con el Catastro, lo que ha introducido mayor facilidad y agilidad en los procedimientos en fase de ejecución de sentencias.

Pese a que podríamos mencionar algunos ejemplos adicionales de colaboración, en este sentido se debería seguir avanzando hacia una mayor interconexión e integración con las herramientas electrónicas de la administración, ya que este es un ámbito en el que pueden lograrse grandes progresos en el futuro.

A pesar de los avances logrados, el entorno progresa muy rápidamente, de forma que lejos de caer en la autocomplacencia, resulta más que nunca obligado, dedicar importantes esfuerzos a mantener el proceso de digitalización progresando a buen ritmo. En la era del Big Data, la inteligencia artificial y el Blockchain, tanto el Tribunal de Cuentas como los OCEX no deben quedar al margen de los grandes cambios que tendrán lugar en el mundo que nos rodea, muy al contrario, deberían dar ejemplo avanzando en paralelo al proceso de digitalización del sector público que auditan.

21. El INTOSAI WGITA se constituyó con el objetivo de apoyar a las EFS que forman parte del mismo, en el proceso de desarrollo de conocimientos y capacidades en relación con la auditoría de sistemas de información.

6. Referencias bibliográficas

ALCÁZAR, S. y POU, R. (2018): «La Plataforma de Rendición de Cuentas de las Entidades Locales: mucho más que un instrumento para la rendición de las cuentas del sector público local», *Revista Española de Control Externo*, Vol. XX, N.º 59, pp. 109-134.

Comisión Europea (2019): *«Digital Economy and Society Index Report 2019. Digital Public Services»*, Bruselas.

GORTAZAR, L. (2018): *«Transformación digital y consecuencias para el empleo en España. Una revisión de la investigación reciente»*, Documento de Trabajo - 2018/04, FEDEA. Madrid.

INTOSAI (2019a): *«Declaración de Moscú»*, XXIII INCOSAI, Moscú, Septiembre, 2019.

INTOSAI (2019b): «Using Information Technology to develop Public Administration», *International Journal of Government Auditing-Special INCOSAI XXIII Edition*, pgs.7-9. https://www.intosai.org/fileadmin/downloads/news_centre/events/congress/accords_declarations/EN_23_Moscow_Decl_300919.pdf

INTOSAI (2019c): *«GUID 5100.Guidance on Audit of Information Systems»*, www.issai.org

Ministerio de Política Territorial y Función Pública (2019): *«Código de Administración Electrónica»*, Edición actualizada a 16 de diciembre de 2019. BOE. https://www.boe.es/legislacion/codigos/codigo.php?id=029_Codigo_de_Administracion_Electronica

MINGUILLÓN, A. (2016): «El control externo y la auditoría de sistemas de información», *Revista Española de Control Externo*, Vol. XVIII, N.º 53, pp. 107-134.

RODRÍGUEZ, M. L. (2017): *«Plataformas, microworkers y otros retos del trabajo en la era digital»*, contribución a la Conferencia Nacional OIT «El futuro del trabajo que queremos», Madrid, 28 de marzo de 2017

Tribunal de Cuentas (2018): *«Plan Estratégico 2018-2021»*, https://www.tcu.es/tribunal-de-cuentas/export/sites/default/.content/pdf/PLAN_ESTRATEGICO_2018-2021.pdf

La ciberseguridad y su relevancia en el Sector Público. El papel del Centro Criptológico Nacional

ÁREA DE NORMATIVA Y SERVICIOS DE CIBERSEGURIDAD
DEL CENTRO CRIPTOLÓGICO NACIONAL

RESUMEN

Las posibilidades de comunicación y progreso que brindan las Tecnologías de la Información y la Comunicación (TIC) son innegables, al igual que la dependencia que la Sociedad tiene de ellas y los peligros y las amenazas que conllevan. Por ello, garantizar la ciberseguridad en el ciberespacio, al tiempo que se respeta la privacidad y la libertad de los ciudadanos, se ha convertido en una de las prioridades estratégicas de los países más desarrollados, debido a su impacto directo en la seguridad nacional, en la competitividad de las empresas y en la prosperidad de la Sociedad en su conjunto. Y precisamente, para proteger el ciberespacio español y coordinar la acción de los diferentes organismos de la Administración Pública en esta materia, surgió y se ha ido desarrollando el Centro Criptológico Nacional (CCN). Un Organismo, adscrito al Centro Nacional de Inteligencia (CNI), cuya principal responsabilidad es garantizar la seguridad de las TIC en las diferentes entidades del Sector Público, así como la seguridad de los sistemas que procesan, almacenan o transmiten información clasificada. Así, el CCN trabaja para mantener la infraestructura y los sistemas de información de todas las administraciones públicas con unos niveles óptimos de seguridad, proteger la información y el patrimonio tecnológico español, formar al capital humano y desarrollar las estrategias y marcos legales que permitan a España beneficiarse de todas las bondades de la tecnología, de forma segura.

PALABRAS CLAVE

ciberseguridad | ciberespacio | Capacidad de Respuesta a Incidentes (CCN-CERT) | certificación | Administración Pública

ABSTRACT

The possibilities of communication and progress offered by Information and Communication Technologies (ICT) are undeniable, as well as the dependence Society has on them and the dangers and threats they entail. Therefore, ensuring cybersecurity in cyberspace, while respecting the privacy and freedom of citizens, has become one of the strategic priorities of the most developed countries, due to its direct impact on national security, business competitiveness and the prosperity of the Society as a whole. And precisely in order to protect Spanish cyberspace and coordinate the actions of the different bodies of the Public Administration in this matter, the National Cryptologic Centre (CCN) was created and has been evolving ever since. A Body, attached to the National Intelligence Centre (CNI), which main responsibility is to guarantee the security of ICTs in the different Public Sector entities, as well as the security of the systems that process, store or transmit classified information. Thus, the CCN works to maintain the infrastructure and information systems with optimum levels of security, protect the country's information and technological heritage, train human capital and develop the enabling strategies and legal frameworks which allow Spain to make the most of all the benefits of technology, but in a safe manner.

KEYWORDS

cybersecurity | *cyberspace* | *CCN Computer Emergency Response Team* | *CERT* | *certification*

1. Panorama de la ciberseguridad

El avance de las Tecnologías de la Información y la Comunicación (TIC) presenta un nuevo paradigma. La expansión de Internet, con más de 4.000 millones de usuarios en todo el mundo, ha impulsado una profunda transformación de las estructuras mundiales. Los servicios públicos y su Administración, la educación, el ocio, el transporte, la cultura o las relaciones personales han experimentado un proceso de cambio absoluto, debido a la influencia que la tecnología ejerce sobre la sociedad. Tanto es así que en los últimos años se ha ido conformando una nueva realidad: el ciberespacio.

Este entorno global plantea un escenario de oportunidades económicas y sociales de gran alcance. Sin embargo, también conlleva una serie de riesgos, que se incrementan día a día. Las amenazas del ciberespacio, favorecidas por la rentabilidad económica o política, el bajo coste de las herramientas empleadas y la posibilidad de actuar desde cualquier lugar del mundo de manera anónima, se dirigen y afectan transversalmente a los sectores público y privado, así como a los ciudadanos.

En este contexto, los ciberdelincuentes, los hacktivistas o los propios Estados, son capaces de explotar las vulnerabilidades tecnológicas con el objetivo de recabar información, sustraer activos de gran valor y amenazar los servicios básicos para el normal funcionamiento de un país. Asimismo, la utilización de las técnicas de aprendizaje automático *(machine learning)* o el uso de modelos de Inteligencia Artificial (IA) son cada vez más frecuentes y sofisticados, evidenciando un creciente potencial para amplificar los riesgos existentes o crear nuevos riesgos; especialmente cuando el Internet de las Cosas (IoT) es capaz de conectar cientos de millones de dispositivos.

Así pues, garantizar e implementar seguridad en el ciberespacio, al tiempo que se respeta la privacidad y la libertad, se ha convertido en una de las prioridades estratégicas de los países más desarrollados, debido a su impacto directo en la seguridad nacional, en la competitividad de las empresas y en la prosperidad de la sociedad en su conjunto. El mundo ciber exige un compromiso constante ante la evolución tecnológica y la creciente sofisticación de los ataques.

2. Amenazas y desafíos del ciberespacio

El principal reto al que tiene que enfrentarse cualquier organización, ya sea pública o privada, es la protección de sus activos, siendo la información uno de los más destacados. Y para ello requiere de un entorno seguro y fiable que debe partir del conocimiento y la comprensión de los desafíos y las amenazas existentes, incluyendo las nuevas y emergentes que afectan al ciberespacio y perpetradas a través de muy diversas técnicas:

- **APT (Amenazas Persistentes Avanzadas).** Ataques selectivos de ciberespionaje o ciberssabotaje, contra un objetivo concreto, bien de la Administración, la industria o un sistema en particular, llevados a cabo bajo el auspicio de un país, por razones que van más allá de las meramente financieras/delictivas o de protesta política. Este ataque emplea diversas técnicas para proceder al robo de información sensible, tratando de permanecer oculto el mayor tiempo posible.

- **Ataques DDoS** (Denegación de Servicios Distribuido). Son aquellos provocados por un grupo de personas o bots que atacan a un sistema a la vez. Este flujo masivo de datos ocasiona que los recursos del servidor sean insuficientes, lo que provoca que colapse y deje de funcionar. Si se trata de un equipo que mantienen un sitio web o cualquier servicio online, este cae junto al servidor. Los ataques DDoS son una herramienta muy utilizada tanto con fines propagandísticos, como siendo parte de una de las fases de otros ataques más sofisticados y cuyo objetivo es la exfiltración de información.

- **Ransomware**. Se trata de código dañino desarrollado para secuestrar un dispositivo, una forma de explotación en la cual el atacante cifra los datos de la víctima y exige un pago por la clave de descifrado. Ha sido uno de los tipos de malware (programa dañino) que más ha aumentado en los últimos tiempos, junto con la minería oculta de criptomonedas.

- **Internet de las Cosas (IoT – *Internet of Things*)**. Redes de objetos físicos —artefactos, vehículos, edificios, electrodomésticos, vestimenta, implantes, software, etc.—; que disponen de conectividad en red lo que les permite recolectar información de todo tipo. Sus múltiples vulnerabilidades permiten que los dispositivos IoT se hayan utilizado como herramientas para llevar a cabo ciberataques (IoT en botnets), además de para espiar a sus usuarios o para manipular su entorno.

- **Tecnología Blockchain**[1]. El atractivo anonimato que permiten las transacciones de monedas virtuales al estar apoyadas en la red descentralizada Blockchain, así como la dificultad cada vez mayor de infección de ransomware, han propiciado que los cibercriminales se decanten cada vez más por una estrategia de ganar dinero de manera fraudulenta conocida como «cryptojacking».

- **Ataques a la cadena de suministro**. En las propias infraestructuras de descarga de servicios, en teoría de confianza, se ocultan distintas variedades de malware que logran infectar la aplicación antes de su instalación. El caso de CCleaner (software de limpieza) es uno de los ejemplos de este tipo de ataques. Los servidores de la empresa fueron comprometidos y la versión original del software fue cambiada por otra que contenía el malware, afectando a todos los usuarios que procedían a su descarga.

- **Cibercrimen como servicio (CaaS).** La industria de los ataques digitales constituye un potente modelo de negocio. La mayoría de sus servicios se ofrecen a través de lo que se conoce como la *deep web*[2] como si de una prestación legal se tratara: fraude online, malware, ataques de DDoS, ransomware, credenciales, etc. A veces, incluso, se ofrece soporte técnico las 24 horas y existen estrategias de marketing y plataformas de compraventa donde los cibercriminales pueden comprar más de 70.000 servidores comprometidos.

1. Blockchain o cadena de bloques: es una inmensa base de datos en donde los registros (los bloques) están enlazados y cifrados para proteger la seguridad y privacidad de sus transacciones. Está distribuida entre varios participantes (nodos) que se conectan en una red descentralizada, sin un ordenador principal. Son redes llamadas P2P que hablan entre sí usando el mismo lenguaje (protocolo). Se puede aplicar a todo tipo de transacciones (no tienen por qué ser necesariamente económicas).
2. Internet profunda, internet invisible o internet oculta es el contenido de la Red que no está indexado por los motores de búsqueda convencionales (bing, google, yahoo, etc.).

- **Hacktivismo.** Utilización de herramientas digitales ilegales o legalmente ambiguas, persiguiendo fines sociopolíticos. Es el traslado al mundo digital de los tradicionales grupos activistas. El tipo de acciones que realizan se basan principalmente en desfiguraciones de sitios webs, redirecciones, ataques de denegación de servicio, robo de información o sabotajes virtuales.
- **Ciberyihadismo.** Los grupos yihadistas y terroristas constituyen una amenaza, aunque todavía no se ha constatado que sean capaces de desarrollar ciberataques sofisticados. Sin embargo, no es menos cierto que parecen estar decididos a desarrollar esta vía de agresión, aun cuando hasta el momento los resultados más evidentes han sido las desfiguraciones y los ataques DDoS, todos ellos de naturaleza propagandística.
- **Desinformación.** Ciberamenaza en la que el arma viene dada por las tecnologías de comunicación digitales y la munición está constituida por información manipulada, sesgada o directamente falsa, que es difundida a la opinión pública por agentes no correctamente identificados, con técnicas automatizadas y con intenciones dañinas para un Estado o institución.
- **Guerra híbrida.** Las guerras de opinión pública se han convertido en una estrategia generalizada y recurrente a nivel global. Durante los últimos años se ha podido constatar y demostrar el interés que determinados Estados tienen por influir en el debate público de países extranjeros. Influenciar, alterar, incluso manipular la opinión pública de una nación considerada adversaria se está convirtiendo en una nueva arma de guerra que destaca por su eficacia, su relativo bajo coste y, sobre todo, por su compleja trazabilidad.

3. La ciberseguridad en la Administración española

La Administración Pública española no es ajena a este escenario. Los distintos legisladores han ido adecuando la necesidad de desarrollar la Sociedad de la Información y la administración electrónica (con todas las ventajas que ello reporta), con su protección y defensa. Siendo conscientes de que, por un lado, la Administración tiene que acompañar y promover en beneficio de los ciudadanos el uso de las comunicaciones y transformarse en una administración electrónica regida por el principio de eficacia que proclama el artículo 103 de nuestra Constitución. De otro, generar confianza y seguridad en el uso de estas tecnologías, protegiendo la **confidencialidad** de los datos; garantizando su **autenticidad** (el emisor es quien dice ser), su **integridad** (el mensaje que recibe el receptor no ha sido modificado), su **disponibilidad** (acceso a la información por personas autorizadas en el momento que así lo requieran) y sus necesidades de **trazabilidad** (registros de actividad asociados). Todo ello, combinado con la defensa de los derechos de los ciudadanos, algunos de los cuales son considerados por la Constitución como derechos fundamentales (caso del derecho a la intimidad y al secreto de las comunicaciones).

Por otra parte, la Administración necesita, a su vez, que la elaboración, conservación y utilización de determinada información se realice de forma segura para garantizar su funcionamiento eficaz al servicio del ciudadano y de los intereses nacionales (baste pensar,

por ejemplo, en la especial sensibilidad de la información contenida en los procedimientos judiciales electrónicos, o en los historiales médicos de los pacientes). Debe, por tanto, garantizar la protección de la información pública, sus sistemas y servicios, así como las redes que lo soportan. En consecuencia, debe dotarse de los medios adecuados para la protección y control del acceso a dicha información, y ha de regular unos procedimientos eficaces para su almacenamiento, procesamiento y transmisión seguros por medio de sistemas propios.

Estamos pues ante un escenario complejo, en el que se combinan, de un lado el hecho de que la transformación digital hace de las TIC el fundamento de los servicios prestados por las administraciones públicas, y, por otro lado, los crecientes los riesgos y ciberamenazas.

4. Marco jurídico de la ciberseguridad

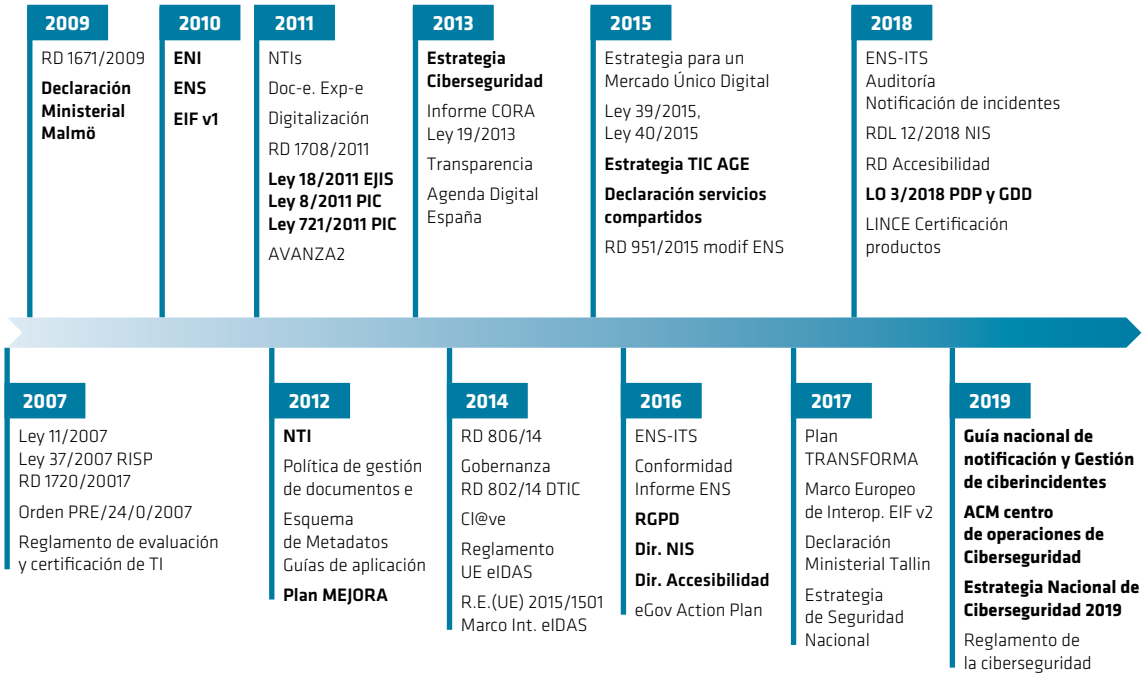
En toda actividad en la que desarrollan interacciones, se requiere de normas que regulen el comportamiento de los sujetos que en ella intervienen. Unas normas que no solo regulen los derechos y deberes, sino que además actúen como catalizadoras del sector y favorezcan la creación, el crecimiento y el fortalecimiento de la actividad.

En el sector de las TIC y su seguridad, ha sido necesario que las diferentes leyes existentes se adapten para regular y proteger a los ciudadanos y a las empresas de los atacantes cibernéticos, estableciendo también nuevas normas y protocolos que regulen las nuevas situaciones.

Un hito importante en el desarrollo de las TIC en nuestro país fue la **Ley 11/2007,** de 22 de junio, de **acceso electrónico de los ciudadanos a los Servicios Públicos**. En el preámbulo de dicha Ley se asegura que *«la Administración queda obligada a transformarse en una administración electrónica regida por el principio de eficacia que proclama el artículo 103 de nuestra Constitución»*. Una Administración moderna que *«haga del principio de eficacia y eficiencia su eje vertebrador siempre con la mira puesta en los ciudadanos»* y bajo el principio de seguridad en la implantación y utilización de los medios electrónicos, exigiendo al menos el mismo nivel de garantías y seguridad que se requiere para la utilización de medios no electrónicos. Todo ello, con la finalidad de crear las condiciones de confianza en el uso de los medios electrónicos, estableciendo las medidas necesarias para la preservación de la integridad de los derechos fundamentales y, en especial los relacionados con la intimidad y la protección de datos de carácter personal, por medio de la garantía de la seguridad de los sistemas, los datos, las comunicaciones, y los servicios electrónicos.

Pero la Ley, además, establece el **Esquema Nacional de Seguridad (ENS)** que, aprobado mediante **Real Decreto 3/2010, de 8 de enero** (actualizado en 2015) tiene por objeto determinar la política de seguridad en la utilización de medios electrónicos en su ámbito de aplicación y está constituido por los principios básicos y requisitos mínimos que permitan una protección adecuada de la información.

FIGURA 1
CRONOLOGÍA DE LEGISLACIÓN Y NORMATIVA EN MATERIA DE CIBERSEGURIDAD



La finalidad del ENS es «la creación de las condiciones necesarias de confianza en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones y los servicios electrónicos, que permita a los ciudadanos y a las Administraciones públicas, el ejercicio de derechos y el cumplimiento de deberes a través de estos medios».

Cinco años después, en 2015, se publicó su modificación a través del RD 951/2015, de 3 de octubre, en respuesta a la evolución del entorno regulatorio de las tecnologías de la información y de la experiencia de la implantación del propio Esquema. Se completó con la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas y la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público. Ambas vienen a configurar un escenario en el que la tramitación electrónica debe constituir la actuación habitual de las Administraciones en sus bmúltiples vertientes de gestión interna, de relación con los ciudadanos y de relación de aquellas entre sí.

En todo este proceso, el CCN en colaboración con el Ministerio de Política Territorial y Función Pública (anteriormente de Hacienda y Administraciones Públicas) ha participado activamente en su desarrollo e implementación. De hecho, buena parte de los instrumentos para la Adecuación al ENS han sido promovidos por el Centro Criptológico Nacional:

- Guías CCN-STIC (véase apartado correspondiente)
- Instrucciones técnicas
- Auditorías de Servicios web
- Análisis de riesgos, a través de la herramienta PILAR

- Cumplimiento del ENS, gracias a la solución CLARA, desarrollada por el CCN para analizar las características de seguridad técnicas definidas en el RD.
- Productos cualificados: desarrollo del Catálogo de Productos STIS (CPSTIC) que recoge las garantías de seguridad contrastadas para organismos del sector público o entidades privadas que den servicios a estos y que se encuentren afectadas por el ENS.

Del mismo modo, el CCN fijó en 2015 los criterios para alcanzar el cumplimiento con el ENS y su correspondiente Declaración y Certificación de Conformidad. Asimismo, desarrolló la solución INES (Informe Nacional del Estado de Seguridad) buscando cumplir con la obligación, por parte de las Administraciones Públicas, de evaluar regularmente el estado de la seguridad de los sistemas.

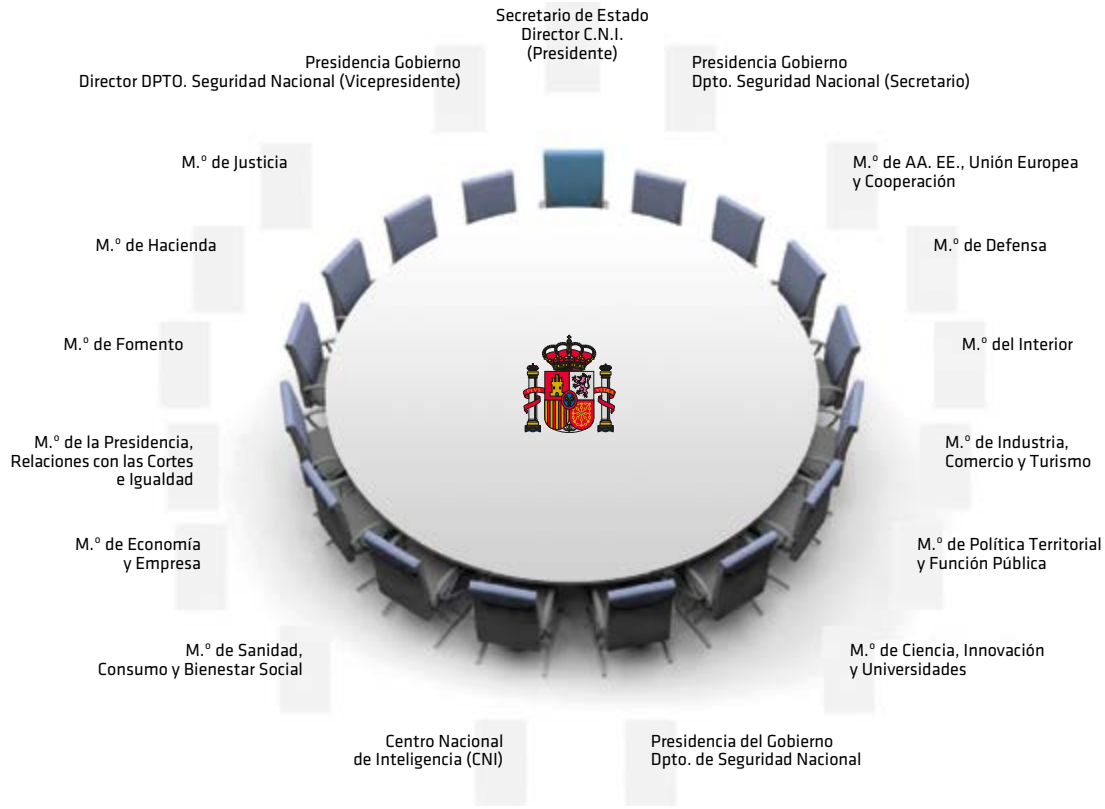
4.1. Estrategia Nacional de Ciberseguridad

Al ENS se han sumado otras iniciativas que, como la Estrategia Nacional de Ciberseguridad, vienen a marcar los pasos de nuestro país en el ámbito de la ciberseguridad. La primera de ellas se aprobó en 2013 y, la segunda, en 2019. Esta última desarrolla las previsiones de la Estrategia de Seguridad Nacional de 2017 en el ámbito de la ciberseguridad y garantizar el uso seguro y fiable del ciberespacio, protegiendo los derechos y las libertades de los ciudadanos y promoviendo el progreso económico. En ella se fijan cinco objetivos específicos para orientar la acción del Estado (véase figura 2).

FIGURA 2
OBJETIVOS DE LA ESTRATEGIA NACIONAL DE CIBERSEGURIDAD 2019

El Centro Nacional de Inteligencia ha participado activamente en la elaboración de esta Estrategia. No en vano, ha presidido el Consejo Nacional de Ciberseguridad desde su creación en 2014 como órgano de apoyo al Consejo de Seguridad Nacional, coordinador de los organismos con competencia en la materia a nivel nacional.

FIGURA 3
GOBERNANZA DE LA CIBERSEGURIDAD EN ESPAÑA.
REPRESENTANTES EN EL CONSEJO NACIONAL DE CIBERSEGURIDAD



4.2. Real Decreto-Ley en materia de administración electrónica, contratación de las administraciones públicas y telecomunicaciones

El 31 de octubre de este mismo año, el Consejo de Ministros aprobó el Real Decreto-ley por el que se adoptaban medidas urgentes por razones de seguridad en materia de administración electrónica, contratación de las administraciones públicas y telecomunicaciones. El texto, que entró en vigor el 5 de noviembre de 2019, una vez publicado en el BOE, incluye iniciativas sobre la documentación nacional de identidad, la identificación electrónica ante las administraciones, los datos que obran en poder de las mismas, la contratación pública y el sector de las telecomunicaciones.

Dentro de las medidas para reforzar la coordinación en materia de seguridad de las redes y sistemas de información, el RDL señala, en su artículo 11 que *«el Centro Criptológico Nacional (CCN) ejercerá la coordinación nacional de la respuesta técnica de los equipos*

de respuesta a incidentes de seguridad informática (CSIRT) en materia de seguridad de las redes y sistemas de información del sector público comprendido en la Ley 39/2015, de 1 de octubre, de Procedimiento Administrativo Común de las Administraciones Públicas, y en la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público».

El texto prosigue: *«Los CSIRT de las administraciones públicas consultarán, cuando proceda, con los órganos con competencias en materia de seguridad nacional, seguridad pública, seguridad ciudadana y protección de datos de carácter personal y colaborarán con ellos en el ejercicio de sus respectivas funciones..... El CCN ejercerá la función de enlace para garantizar la cooperación transfronteriza de los CSIRT de las administraciones públicas con los CSIRT internacionales, en la respuesta a los incidentes y gestión de riesgos de seguridad que les correspondan».*

4.3. Directiva NIS

El 6 de julio de 2016 la Unión Europea publicó en su Boletín Oficial la **Directiva (UE) 2016/1148** relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión (más conocida como Directiva NIS). Sin embargo, la trasposición al ordenamiento jurídico español se realizó dos años después; en concreto en el **Real Decreto-ley 12/2018, de 7 de septiembre**, de seguridad de las redes y sistemas de información.

La Directiva NIS busca mejorar la fragmentación existente en los Estados y homogeneizar los distintos planteamientos, estableciendo requisitos mínimos comunes en materia de desarrollo de capacidades y planificación, intercambio de información, cooperación y requisitos comunes de seguridad para los operadores de servicios esenciales y los proveedores de servicios digitales. A todos ellos les insta a adoptar las medidas oportunas para gestionar los riesgos en seguridad y notificar los incidentes que tendrían un efecto perturbador significativo a las Autoridades Nacionales Competentes, proponiendo la creación de una red de cooperación entre los diferentes Estados miembros.

4.4. Reglamento General de Protección de Datos

También en el año 2016, la UE aprobó el Reglamento General de Protección de Datos (RGPD) que, si bien entró en vigor en mayo de ese año, fue de aplicación a partir del 25 de mayo de 2018. Al tratarse de un Reglamento no necesita transposición al ordenamiento jurídico español, por lo que su contenido es directamente aplicable. Esta norma europea, desplazó a la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y su Reglamento de Desarrollo, e introdujo una serie de cambios en los tratamientos de datos personales que realicen los responsables, así como las notificaciones de brechas de seguridad que puedan afectar a estos y las evaluaciones de impacto en la protección de datos.

Con el fin de adaptar este marco normativo, en 2018, se aprobó el **Real Decreto-ley 5/2018, de 27 de julio**, de medidas urgentes para la adaptación del Derecho español a la normativa de la UE en materia de protección de datos. Posteriormente, se publicó la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales en donde se indicaba que el Esquema Nacional de Seguridad incluirá las medidas que deban implantarse en caso de tratamiento de datos personales para evitar

su pérdida, alteración o acceso no autorizado, adaptando los criterios de determinación del riesgo en el tratamiento de los datos a lo establecido en el artículo 32 del Reglamento (UE) 2016/679.

Ante la nueva situación, el CCN, junto a la Agencia Española de Protección de Datos (AEPD), estableció un mecanismo de colaboración, con el objetivo de ofrecer al sector público una referencia de cumplimiento normativo en materia de protección de datos y seguridad ante la entrada en vigor del RGPD.

Fruto de esta colaboración, el CCN-CERT y la AEPD trabajaron de forma conjunta para ofrecer una solución que facilitase esta labor. Así la herramienta PILAR incluye un módulo de cumplimiento que permite a las AAPP verificar los requisitos establecidos en el RGPD.

5. El papel del Centro Criptológico Nacional

A principios de los **años 80**, en el seno del **CESID**[3], se formó un departamento con un amplio conocimiento en materia de amenazas, vulnerabilidades y riesgos de los sistemas de información y comunicaciones. Su misión principal entonces era el desarrollo de material de cifra y algoritmos para la protección de la información clasificada, el desarrollo de requisitos de seguridad para estos sistemas y la acreditación de los mismos. Todo ello, siguiendo la línea trazada en materia de seguridad de las TIC por los países avanzados y por las organizaciones internacionales en las que nos integramos en aquellos años: OTAN y Unión Europea.

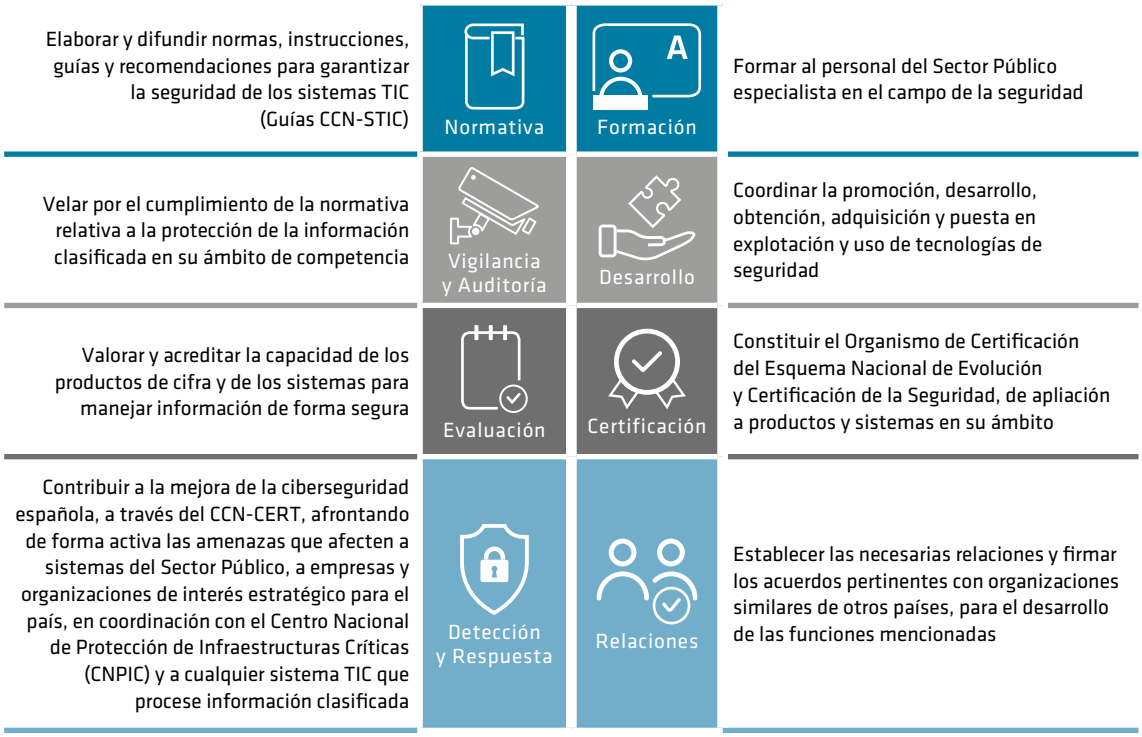
Este departamento fue el germen de lo que, en el **año 2002**, al crearse el **Centro Nacional de Inteligencia** (regulada por la **Ley 11/2002, de 6 de mayo**), recogía una de sus funciones principales (artículo 4): *Coordinar la acción de los diferentes organismos de la Administración que utilicen medios o procedimientos de cifra, garantizar la seguridad de las tecnologías de la información en ese ámbito, informar sobre la adquisición coordinada de material criptológico y formar al personal, propio o de otros servicios de la Administración, especialista en este campo para asegurar el adecuado cumplimiento de las misiones del Centro. Además, se añadía, la obligación de velar por el cumplimiento de la normativa relativa a la protección de la informa ción clasificada*. Esta misma Ley otorgaba al secretario de Estado Director del Centro Nacional de Inteligencia el desempeño de *«las funciones de Autoridad Nacional de Inteligencia y Contrainteligencia y la dirección del Centro Criptológico Nacional»*.

Previamente, en 1999, se promulgaron el **Real Decreto Ley 14/1999, de 17 de septiembre, sobre firma electrónica** (con el fin de fomentar la rápida incorporación de las nuevas tecnologías de seguridad de las comunicaciones electrónicas en la actividad de las empresas, los ciudadanos y las Administraciones pública), la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y, en 2002, la Ley 34/2002 de Servicios de la Sociedad de la Información y Comercio Electrónico.

3. Centro Superior de Información de la Defensa, creado por el Real Decreto 1558/77, como el primer Servicio de Inteligencia de carácter Nacional (https://www.cni.es/es/queescni/historia/elcesid/).

Esta normativa dirigida al desarrollo de la Sociedad de la Información, tenía que acompasarse con la participación de un organismo que, partiendo de un conocimiento de las tecnologías de la información y de las amenazas y vulnerabilidades, garantizara la seguridad de las TIC en las administraciones públicas, proporcionara una garantía razonable sobre la seguridad de productos y sistemas utilizados y velara por la información clasificada, para evitar el acceso a esta de individuos, grupos y Estados no autorizados. De ahí, el desarrollo del **Centro Criptológico Nacional**, regulado por el **Real Decreto 421/2004**.

FIGURA 4
FUNCIONES DEL CENTRO CRIPTOLÓGICO NACIONAL, SEGÚN RD 421/2004



6. Funciones y servicios del CCN

En su apuesta por colaborar con el Sector Público en la mejora de su seguridad, el Centro Criptológico Nacional ofrece una amplia variedad de servicios, ampliados gradualmente, que, en numerosas ocasiones son refrendados por Convenios de Colaboración. Dichos convenios son suscritos entre el Centro Nacional de Inteligencia y otros Organismos públicos, tales como el Consejo General del Poder Judicial (firmado en octubre de 2017), el Mando Conjunto de Ciberdefensa o las diferentes Comunidades Autónomas.

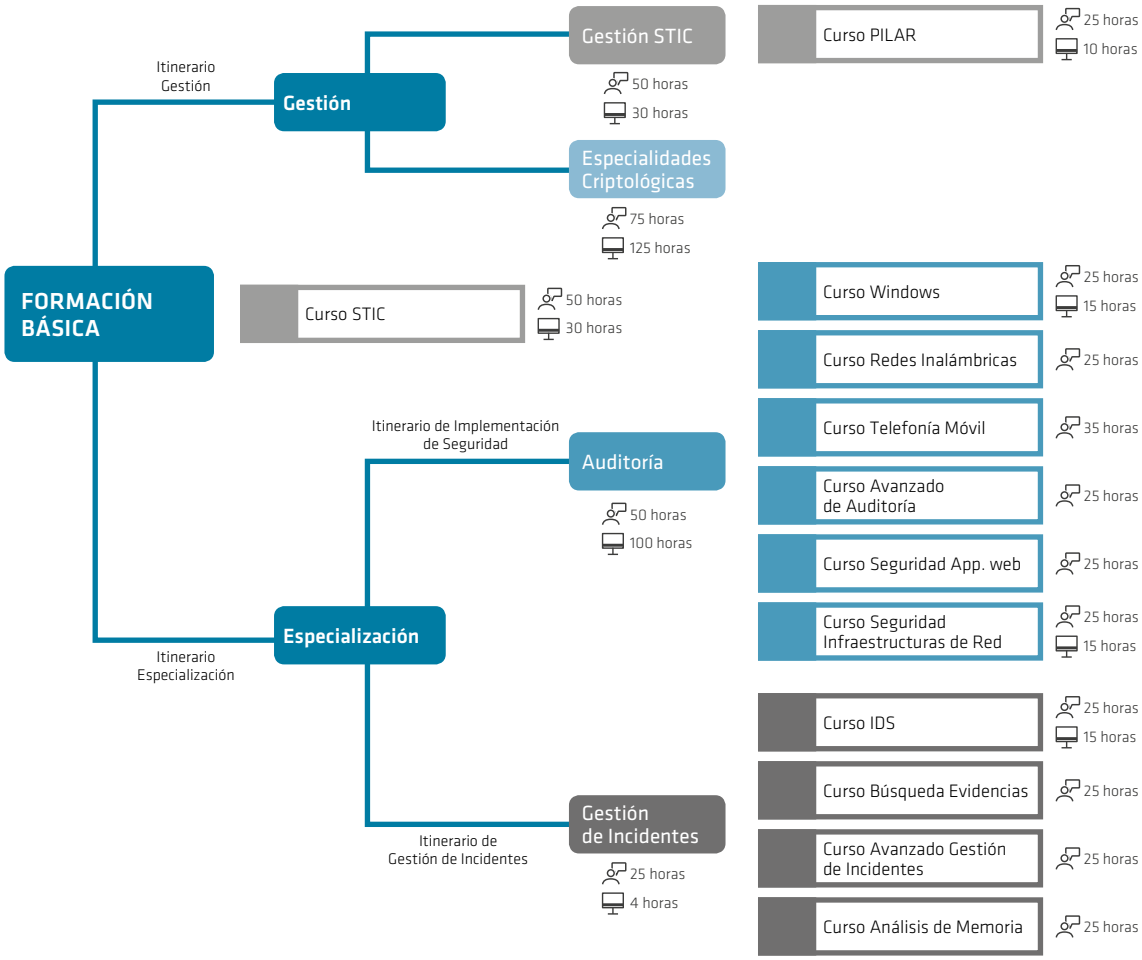
6.1. Formación y concienciación

Ante la necesidad de fomentar y desarrollar perfiles profesionales cualificados para el sector público, el CCN ofrece un amplio programa de cursos formativos, adaptado a las necesidades planteadas por su comunidad de referencia (aunque también están dirigidos al

sector privado e, incluso, a otros Estados). Este **Plan de Formación**, con un diseño curricular y flexible, se ha ido transformando a medida que lo han hecho las tecnologías, adaptándose así al nuevo escenario que presenta el ciberespacio. Se ha diseñado, además, atendiendo a la necesidad de capacitar, tanto presencialmente como a distancia, a profesionales cualificados, que disponen de distinto perfil y nivel de formación. Por este motivo, se ha establecido una formación BÁSICA que, a través del Curso STIC, introduce al alumno en el ámbito de la Seguridad de las Tecnologías de la Información y la Comunicación.

Completada la formación básica, el profesional que desee perfeccionar sus conocimientos podrá elegir entre dos (2) itinerarios diseñados para lograr tal fin, el itinerario de gestión y el de especialización (dirigido a personal con un perfil más técnico).

FIGURA 5
ITINERARIOS DE FORMACIÓN DEL CENTRO CRIPTOLÓGICO NACIONAL



Asimismo, además de VANESA (plataforma de retransmisión de sesiones formativas en directo), el Centro Criptológico Nacional permite a través de su página web la realización de distintos cursos en los que se emplea una metodología docente online, tanto en los contenidos como en los exámenes que se realizan una vez finalizados los cursos.

a) **Atenea**

La plataforma **Atenea** tiene por objeto que cualquier persona con inquietudes en el campo de la ciberseguridad pueda poner a prueba su conocimiento. Esta plataforma de desafíos se puso en marcha en diciembre de 2017 y, mediante una serie de retos de distinta dificultad y muy diversas temáticas (criptografía y esteganografía, exploiting, forense, análisis de tráfico, reversing, etc.), permite al usuario demostrar sus conocimientos y destrezas.

b) **Concienciación y sensibilización**

Desde sus orígenes, el CCN ha tenido entre sus principales objetivos fomentar el conocimiento y el uso seguro de las TIC. En esta apuesta por la cultura de la ciberseguridad entre todos los usuarios desarrolla y colabora en todo tipo de acciones de sensibilización, formación y divulgación de información y buenas prácticas de seguridad.

Con este objetivo, recopila algunos de los principales consejos que pueden darse a la hora de concienciar y facilitar el uso seguro de las Tecnologías de la Información y la Comunicación[4].

6.2. Normativa

Las Series CCN-STIC[5] son normas, instrucciones y recomendaciones desarrolladas por el CCN, de muy diversa temática, con el fin de mejorar el grado de ciberseguridad de las organizaciones. Periódicamente son actualizadas y completadas con otras nuevas, en función de las amenazas y vulnerabilidades detectadas (hoy en día, existen más de 350 Guías CCN-STIC). Todas ellas están disponibles para el personal de las AAPP.

6.3. Informes, avisos y vulnerabilidades

Asimismo, la Capacidad de Respuesta a Incidentes del CCN, CCN-CERT[6], ofrece información sobre el estado de la ciberseguridad con el fin de reducir tanto las vulnerabilidades técnicas (hardware y software) como humanas y de organización.

Su principal destinatario son los usuarios registrados de su portal o los organismos e instituciones adscritas a alguno de sus servicios, a los que notifica periódicamente diferentes avisos, alertas, vulnerabilidades e informes de diferentes materias.

6.4. Implementación de seguridad

Dada la importancia que tiene la información que manejan los sistemas de las TIC, es primordial que la Administración se asegure de que está protegida. De ahí, la necesidad de estar al día respecto a las amenazas y vulnerabilidades relacionadas con los sistemas y la implantación de un conjunto de medidas, tanto procedimentales como técnicas y organizativas, que permitan un entorno seguro.

En este sentido, en 2018, el CCN promovió la implementación en el Sector Público de un procedimiento de mejora continua de los niveles de seguridad en base a la adopción de compromisos a corto, medio y largo plazo por parte del propietario del Sistema. Todo ello,

4. Los ciberconsejos se encuentran disponibles en la web: https://www.ccn.cni.es/index.php/es/menu- formacion-es/ciberconsejos
5. https://www.ccn.cni.es/index.php/es/menu-guias-ccn-stic-es
6. CERT: Computer Emergency Response Team, siglas en inglés que vienen a definir a un Equipo de Respuesta a Incidentes que da servicio a una Comunidad, en este caso al Sector Público Español y a las empresas de interés estratégico para el país.

junto con una evaluación constante basada en la determinación de vulnerabilidades y deficiencias de configuración de los sistemas, sobre todo en aquellos que, por su origen y naturaleza, tienen grandes dificultades para cumplir con los requisitos de seguridad exigidos.

6.5. Detección y respuesta

Es misión del Centro Criptológico Nacional y de su Capacidad de Respuesta a Incidentes (CCN-CERT) contribuir a la mejora de la ciberseguridad española, siendo el centro de alerta y respuesta nacional que coopere y ayude a responder de forma rápida y eficiente a los ciberataques y a afrontar de forma activa las ciberamenazas, incluyendo la coordinación a nivel público estatal de las distintas Capacidades de Respuesta a Incidentes (CERT-CSIRT) o Centros de Operaciones de Ciberseguridad (SOC) existentes.

Es competencia del CCN-CERT la gestión de ciberincidentes que afecten a sistemas clasificados, del Sector Público y de empresas y organizaciones de interés estratégico (aquellas esenciales para la seguridad nacional y para el conjunto de la economía española). En este último caso, la gestión de ciberincidentes se realizará en coordinación con el Centro Nacional de Protección de Infraestructuras y Ciberseguridad (CNPIC), dependiente de la Secretaria de Estado de Seguridad del Ministerio del Interior.

6.6. Gestión y respuesta a ciberincidentes

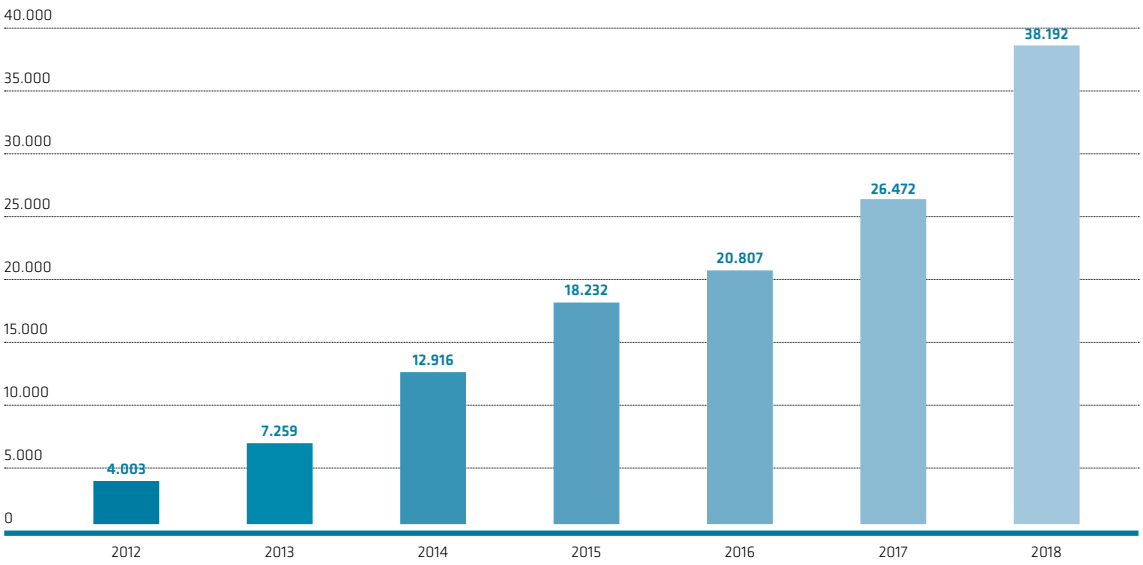
El CCN-CERT, como CERT Gubernamental Nacional, colabora con todos los organismos públicos y empresas de interés estratégico para el país en la detección, notificación, evaluación, respuesta, tratamiento, y aprendizaje de incidentes de seguridad de información o ciberincidentes que puedan sufrir sus sistemas.

En este proceso, realizado siempre en la más absoluta confidencialidad entre ambas partes, el CCN-CERT brinda apoyo técnico y operativo, tanto en las etapas de detección, como reacción, contención y eliminación. A ello se une una política preventiva, en la que trabaja un equipo de expertos destinados a investigar sobre técnicas empleadas, tendencias, soluciones y procedimientos más adecuados para hacerles frente, incluyendo metodologías para recopilar y analizar datos y eventos, procedimientos de tipificación de su peligrosidad y priorización de los mismos.

Actúa, además, como Nodo de Intercambio de Información de Ciberincidentes en los Sistemas de Información de las Administraciones Públicas y como principal coordinador con los distintos organismos.

Prueba de todo ello es el número de incidentes gestionados por el CCN-CERT durante los dos (2) últimos años que sumaron un total de 64.664; es decir casi 89 incidentes diarios durante el período de 2017 y 2018.

FIGURA 6
EVOLUCIÓN DE LOS INCIDENTES GESTIONADOS POR EL CCN-CERT

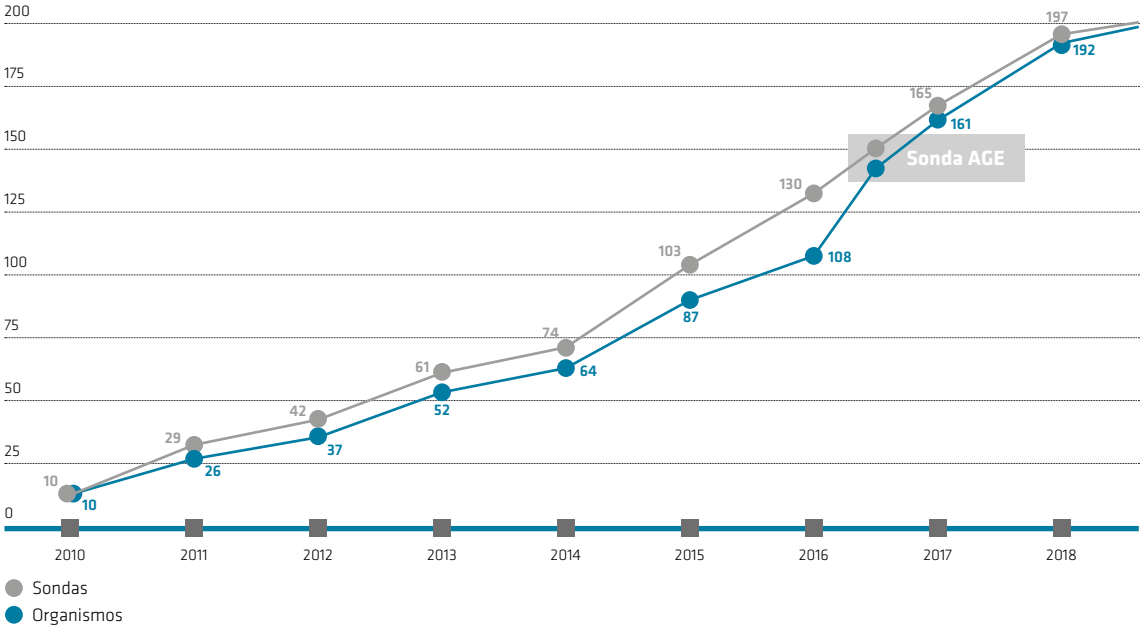


a) Sistema de Alerta Temprana (SAT)

El Sistema de Alerta Temprana (SAT) ha sido desarrollado por el CCN-CERT desde el año 2008. Su objetivo es prevenir antes de que se produzca un incidente o, por lo menos, detectarlo en un primer momento para reducir su impacto y alcance. Cuenta con tres (3) vertientes: **SAT- SARA**, para la monitorización de la Intranet de la Administración; **SAT-INET**, para las salidas de Internet de los organismos adscritos al servicio y **SAT-ICS**, para los Sistemas de Control Industrial.

A finales de 2018, 192 organizaciones se habían adherido al SAT-INET, lo que representaba un total de **197 sondas desplegadas** en organismos de la Administración General del Estado, Comunidades Autónomas, diputaciones provinciales, mancomunidades, ayuntamientos, confederaciones hidrográficas, puertos, universidades y empresas de interés estratégico.

FIGURA 7
EVOLUCIÓN DE LAS SONDAS DESPLEGADAS POR EL CCN-CERT



Por su parte, las **áreas de conexión de la red SARA han llegado a cincuenta (50)** (ministerios y organismos AGE, órganos constitucionales, organismos independientes y comunidades autónomas), mientras que el número de entidades con **SAT-ICS son ocho (8)** entre confederaciones hidrográficas, puertos, servicios sanitarios y nuclear.

6.7. Vigilancia y auditoría

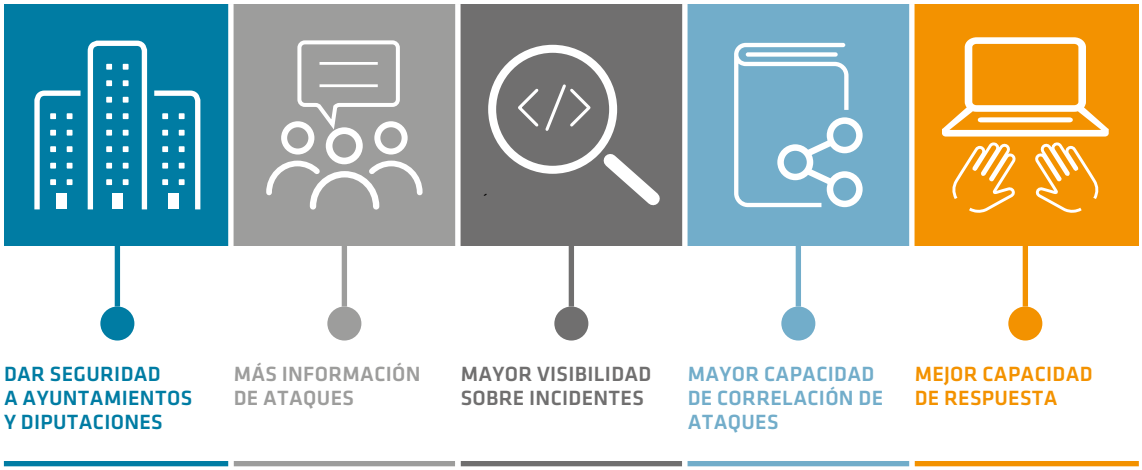
a) Centros de Operaciones de Ciberseguridad (SOC)

Otro paso dado para reforzar la capacidad de prevención, monitorización, vigilancia y respuesta a incidentes se ha dado a través de distintos **Centros de Operaciones de Ciberseguridad (SOC)**. A través de un **SOC** se supervisa a las personas, los procesos y la tecnología que intervienen en todos los aspectos operativos de la ciberseguridad.

El CCN-CERT ofrece servicios de vigilancia a diversos organismos de la Administración Pública, promocionando la creación de este tipo de Centros con el fin de optimizar los recursos que son críticos. Los primeros en desarrollarse fueron, en 2018, el **SOC-Justicia** y el **SOC de la Administración General del Estado (AGE)** y sus organismos públicos.

A ellos le seguirán, los centros destinados a las entidades locales. A través del **vSOC**, ayuntamientos y diputaciones tendrán más visibilidad e información sobre vulnerabilidades, fallos de configuración e incidentes, mayor capacidad de despliegue, protección y actuación, al disponer de una gestión centralizada que permitirá aumentar el número de entidades adscritas a cada vSOC.

FIGURA 8
OBJETIVOS DE LOS VSOC



b) Auditoría

En el ámbito de la vigilancia y la auditoría, el CCN evalúa el estado de la seguridad de los sistemas TIC. Del mismo modo, realiza inspecciones de seguridad que permiten verificar la seguridad implementada en un sistema y que los servicios y recursos utilizados cumplen con los mínimos especificados y requeridos en la política de la seguridad.

6.8. Promoción y desarrollo de productos de cifra y seguridad TIC

Dentro del marco de desarrollo de productos de seguridad y de cifra, el CCN se encarga, a partir de fondos I+D asignados, de cubrir las necesidades operativas de la Administración General del Estado para el desarrollo de Productos TIC que incluyan cifra y que permitan las comunicaciones seguras de información clasificada.

De este modo, coordina la promoción, desarrollo, obtención, adquisición, puesta en explotación y utilización de las tecnologías de seguridad de los sistemas TIC que incluyan cifra para procesar, almacenar o transmitir información de forma segura. Garantiza así que los productos utilizados por la Administración cumplen con los niveles de seguridad exigidos.

6.9. Certificación. Organismo de Certificación (OC)

La adquisición de un producto de seguridad TIC que va a manejar información nacional clasificada o información sensible debe estar precedida de un proceso de comprobación de que los mecanismos de seguridad implementados en el producto son adecuados para proteger dicha información.

La evaluación y certificación de un producto de seguridad TIC es el único medio objetivo que permite valorar y acreditar la capacidad de un producto para manejar información de forma segura.

En España, esta responsabilidad está asignada al CCN a través del RD 421/2004 de 12 de marzo. Concretamente, el Organismo de Certificación (OC) realiza **tres tipos de certificaciones** en función de los aspectos de seguridad que se evalúen, pero siempre referidos a productos y sistemas y servicios de seguridad TIC:

- **Certificación funcional:** El OC otorga certificaciones funcionales a aquellos productos que han superado las evaluaciones bajo las metodologías Common Criteria, ITSEC, ISO 19790 o LINCE. Que un producto disponga de una certificación funcional significa que ha superado con éxito un proceso de evaluación en un laboratorio independiente acreditado, a partir del cual se puede afirmar que su Declaración de Seguridad es cierta con un determinado nivel de confianza (EAL, en sus siglas en inglés).
- **Certificación criptológica:** este Organismo es también responsable de la evaluación, certificación y aprobación de los productos que protegen información nacional clasificada. Tiene la consideración de equipo de cifra con certificación criptológica, aquel equipo de cifra que ha sido evaluado y ha obtenido dicha certificación del CCN.
- **Certificación TEMPEST:** Todo dispositivo electrónico, y entre ellos los sistemas de las TIC, generan un campo electromagnético más o menos intenso que puede contener o estar relacionado con la información procesada en ese momento. Estas emanaciones pueden comprometer la seguridad ya que afectan directamente a la confidencialidad de la información. Esta vulnerabilidad, asociada a la posibilidad de detectar la radiación y reconstruir la información original, es conocida como TEMPEST.

6.10. Seguridad de productos TIC

Con el objetivo de facilitar la adquisición de productos y servicios de seguridad TIC a organismos del Sector Público o entidades privadas que den servicio a estos y que se encuentren afectados por el Esquema Nacional de Seguridad o manejen información clasificada, con unas garantías de seguridad contrastadas, el CCN publica y actualiza el Catálogo de Productos de Seguridad de las Tecnologías de la Información y la Comunicación (CPSTIC)[7].

7. Disponible en formato web (https://oc.ccn.cni.es) o en la Guía CCN-STIC (CCN-STIC 105).

Este Catálogo consta de dos partes: **Productos Aprobados** y **Productos Cualificados.** En el primero, se recogen aquellos productos que se consideran adecuados para el manejo de información clasificada, mientras que en el apartado de **Productos Cualificados** se incluyen aquellos que cumplen los requisitos de seguridad exigidos para el manejo de información sensible en el ENS, en cualquiera de sus categorías (Alta, Media y Básica).

FIGURA 9
TIPOS DE CERTIFICACIONES A LOS PRODUCTOS DE SEGURIDAD TIC REALIZADAS POR CCN-PYTEC

Para la inclusión de un producto en el catálogo, el CCN tendrá en cuenta una serie de criterios como la clasificación de la información que puede manejar (DIFUSIÓN LIMITADA, CONFIDENCIAL, RESERVADO, SECRETO), las características de seguridad del producto, la categoría del sistema de información en el que puede emplearse según lo definido en el ENS (ALTA, MEDIA, BÁSICA), las certificaciones aportadas, el grado de cumplimiento con los requisitos fundamentales de seguridad, y el entorno donde se vaya a emplear, etc. En función de esta información, se determinarán las pruebas o evaluaciones que deberá superar el producto de seguridad TIC correspondiente.

FIGURA 10
TIPOS DE PRODUCTOS INCLUIDOS EN EL CPSTIC

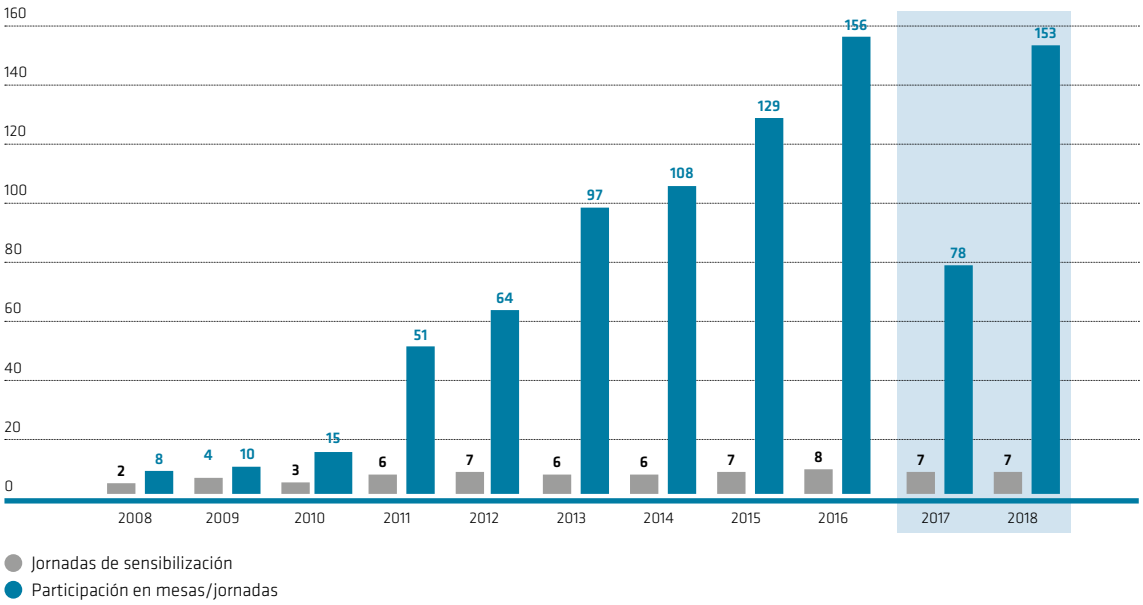
7. Soluciones de ciberseguridad

En su deseo de adaptarse a las exigencias cambiantes en materia de ciberseguridad, el CCN desarrolla distintas herramientas para los organismos a los que da servicio, con las que pretende mejorar la gestión de la ciberseguridad en cualquier organización. Así promueve y brinda a la Administración pública soluciones de Auditoría, detección, análisis, vigilancia e intercambio de información y formación del personal.

8. Relaciones y cultura de ciberseguridad

El CCN ha de velar también por la promoción en España de la cultura de la ciberseguridad, a través de iniciativas de intercambio de conocimientos entre todos los actores implicados. Para ello, acomete un gran número de acciones de información y sensibilización, al tiempo que promueve y participa en diferentes jornadas, congresos y cursos en materia de ciberseguridad.

FIGURA 11
JORNADAS DE SENSIBILIZACIÓN Y PARTICIPACIÓN EN MESAS REDONDAS DEL CCN



También, organiza, desde el año 2007, las Jornadas STIC CCN-CERT, evento que se ha convertido en el principal encuentro de expertos en ciberseguridad del país y donde se dan cita los principales responsables de seguridad de las Administraciones Públicas y de empresas de interés estratégico. Con un total de doce ediciones hasta la fecha, la última celebrada en 2019 fue inaugurada por Su Majestad el Rey Felipe VI.

9. Referencias

VEGA, GUILLERMO. «Cadena de bloques Guía básica para entender de una vez qué es eso del 'blockchain». *El País-Retina*: https://retina.elpais.com/retina/2017/07/13/tendencias/1499945987_724507. html

Real Decreto-ley por el que se adoptan medidas urgentes por razones de seguridad, de 31 de octubre.

Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.

Real Decreto-ley 5/2018, de 27 de julio, de medidas urgentes para la adaptación del Derecho español a la normativa de la Unión Europea en materia de protección de datos.

Resolución de 26 de julio de 2018, de la Subsecretaría, por la que se publica el Convenio en materia de ciberseguridad entre el Ministerio de Justicia y el Centro Nacional de Inteligencia.

Código de Derecho de la Ciberseguridad.

Instrucción Técnica de Seguridad (ITS) de Notificación de Incidentes de Seguridad.

Instrucción Técnica de Seguridad (ITS) de Auditoría de la Seguridad de los Sistemas de Información.

Instrucción Técnica de Seguridad (ITS) de conformidad con el Esquema Nacional de Seguridad.

Instrucción Técnica de Seguridad (ITS) de Informe del Estado de la Seguridad.

Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo de 6 de julio de 2016 (Directiva NIS).

Fe de erratas ENS.

R.D. 951/2015, de 23 de octubre, de modificación del R.D. 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

R.D. 806/2014, de 19 de septiembre. Organización e instrumentos operativos de las TIC en la AGE y sus Organismos Públicos.

R.D. 802/2014, de 19 de septiembre. Modificación funciones y estructuras de varios Ministerios.

Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.

Estrategia de Ciberseguridad Nacional 2013.

R.D. 13/2012, de 30 de marzo, por el que se transponen directivas en materia de comunicaciones electrónicas.

Real Decreto 704/2011 por el que se aprueba el Reglamento de protección de las infraestructuras críticas.

Ley 8/2011 por la que se establecen medidas para la protección de las infraestructuras críticas.

Ley Orgánica 5/2010 de Reforma del Código Penal.

R.D. 4/2010 Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.

R.D. 3/2010 Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

R.D. 1720/2007 Reglamento que desarrolla la Ley de protección de datos.

Orden PRE/2740/2007 del Reglamento de Evaluación y Certificación de las Tecnologías de la Información.

Ley 11/2007 de Acceso Electrónico de los Ciudadanos a los Servicios Públicos.

O.M. 76/2006 Política de Seguridad de la Información del Ministerio de Defensa.

R.D. 421/2004 Centro Criptológico Nacional.

Ley 59/2003 de Firma Electrónica.

R.D. 281/2003 Reglamento Registro General de la Propiedad Intelectual.

Ley 34/2002 Servicios de la Sociedad de la Información y Comercio Electrónico.

Ley 11/2002 reguladora del Centro Nacional de Inteligencia.

Ley Orgánica 2/2002 reguladora del control judicial previo al Centro Nacional de Inteligencia Directiva (UE) 2016/1148 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistema.

Real Decreto-ley 12/2018, de 7 de septiembre.

Proteger la información ha sido una constante a lo largo de la Historia

MARÍA JESÚS CASADO ROBLEDO
Responsable de Seguridad de la Información
Intervención General de la Administración del Estado

RESUMEN

Este artículo recoge algunas formas de proteger la información, mencionando el primer método documentado utilizado en Mesopotamia, pasando por el utilizado por Felipe II hasta el gran salto cualitativo que se dio en Alemania con las máquinas Enigma y Loren. La primera vez que se utilizó Enigma fue durante la Guerra Civil Española.

Distinguir las áreas de competencia de los conceptos Seguridad de la información, Ciberseguridad y Seguridad informática, es el núcleo de este artículo, pues es necesario entender que la Seguridad de la Información tiene un alcance más amplio que el tecnológico.

La Seguridad de la información requiere de una estructura organizativa en la que se reflejen sus tres áreas de responsabilidad: la especificación de las necesidades o requisitos, la operación de los sistemas y la supervisión.

Por último, la dificultad para establecer posibles equivalencias entre el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica y el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y la libre circulación de los datos.

PALABRAS CLAVE

información | informática | ciberseguridad | clave | responsabilidad

ABSTRACT

This article brings together some methods of protecting the information, mentioning the first documented method used in Mesopotamia, going through the one used by Felipe II to the quantum qualitative leap that took place in Germany with the Enigma and Loren machines. The first time Enigma was used was during the Spanish Civil War.

Distinguishing the areas of competence of the concepts of Information Security, Cybersecurity and Computer Security, is the core of this article, as it is necessary to understand that Information Security has a broader scope than merely the technological one.

Information Security requires an organizational structure that reflects its three areas of responsibility: the specification of needs or requirements, the operation of systems and the supervision.

Finally, the difficulty in establishing possible equivalences between el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica y el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y la libre circulación de los datos.

KEYWORDS

information | *computing* | *cybersecurity* | *key* | *responsibility*

1. Breve viaje por la historia

Desde que se tienen referencias escritas sobre la necesidad de evitar que la información llegue a manos de personas que puedan hacer un uso inadecuado ha sido y sigue siendo fundamental.

Para ello se utilizan técnicas que facilitan que la información no pueda llegar a manos equivocadas y se pueda realizar un uso inapropiado y pudiera alterarse.

Los vestigios[1] más antiguos se atribuyen a la civilización mesopotámica y datan del año 1.500 antes de Cristo (aC). El soporte que utilizaban eran tablillas de madera con unas dimensiones de 2 x 3 pulgadas. En este caso trataban de evitar que se conociese cómo fabricaban la cerámica, información muy valorada por aquel entonces.

Los métodos utilizados fueron principalmente dos: estenógrafos (ocultación de la información haciéndola imperceptible) o cifradores (alteración de la información para hacerla incomprensible).

Se encuentran ejemplos del uso de métodos estenógrafos en la obra magna «Los nueve libros de la Historia» escrita por Heródoto[2] (aproximadamente 484-425 aC) considerado el padre de la Historia. En concreto en el libro VII de dicha obra hace referencia al origen de la II Guerra Médica mediante el ataque de Jerjes rey de Persia a los griegos.

«En Susa (Persia) vivía Demarato, un espartano qué enterado de las intenciones de Jerjes, resolvió avisar a sus compatriotas. La cuestión era cómo enviar un mensajero que recorriese el Asia Menor y cruzase el estrecho de los Dardanerlos sin ser descubierto por los guardias persas. Para[3], resolverlo, tomó un cuadernillo de dos tablillas; rayó bien la cera que las cubría, y en la madera grabó con letras la resolución del rey. Hecho esto, volvió a cubrir con cera las letras grabadas, para que el portador del cuadernillo no fuera molestado por los guardias».

Dando un gran salto en la Historia y situándonos en el Imperio español en el que nunca se ponía el sol, regido por Felipe II (el Rey prudente), encontramos el uso de un método de cifrado basado en dos claves (general y particular).

«La clave general la compartía con los Secretarios de Estado y de la Guerra, los Virreyes, Gobernadores generales y Embajadores. La clave particular era distinta para cada uno de los anteriores dignatarios y sólo conocida por el interesado y Felipe II.

En palabras de Felipe II recogidas en su misiva del 19 de junio de 1581 al Duque de Medina Sidonia: Algunas veces ofrécense negocios tan graves e importantes y de tanto secreto que no será bueno escribirlos en cifra general, se os envía para este caso una particular en la cual no podéis escribir a los demás ministros, si no sólo a mí».

La clave general se cambiaba tras un tiempo prudencial, o bien cuando había indicios de que pudiera haber caído en manos enemigas. Se cambió, al menos, en los años 1556, 1562, 1564 y 1567.

1. Profesor Arturo Ribagorda.
2. Historiador griego.
3. Heródoto.

En siglos posteriores siguieron produciéndose avances en materia criptográfica. Se tiene que llegar a la 2.ª Guerra Mundial en la que se generalizo el uso de las máquinas de cifra. La más destacada fue Enigma aunque también jugó un papel importante Lorenz utilizada entre Hitler y su Estado Mayor.

«La primera vez que se utilizó Enigma fue en la Guerra Civil Española. La utilizaron los nacionales para las comunicaciones entre el Cuartel General de Salamanca, las diferentes unidades militares y dos representantes en el exterior, Roma y Berlín. El objetivo era evitar que los republicanos descifraran los mensajes telegráficos emitidos en el marco del avance hacia Madrid.

En diciembre de 1938, llegó a Sevilla, asignada al Ejército del Sur. En julio de 1939 pasó al Estado Mayor de la Segunda Región Militar en Sevilla»[4]*. Este ejemplar es parte de la colección estable del Museo Histórico Militar hispalense (Sevilla).*

Hedy Lamarr, ingeniera y actriz. En la cúspide de su carrera como actriz se la conocía como «la mujer más bella del cine». Ahora bien, se conoce muy poco, sobre su trabajo como ingeniera.

A partir de 1937 compaginó su carrera artística con sus trabajos de ingeniería con un colaborador, el compositor George Antheil. Ambos crearon su sistema de comunicación secreta. Invención que fue patentada y que ofrecieron al Gobierno de los EE.UU.

Este sistema empezó a utilizarse años más tarde cuando la empresa norteamericana Sylvania Electronics completó su desarrollo, reconociendo la patente de Lamarr y Antheil.

En el ámbito militar se utilizó en 1962 en la crisis de los misiles soviéticos en Cuba.

Cuando la tecnología digital se universalizó «el sistema de comunicación secreta» basado en la conmutación de frecuencias o salto de frecuencias, comenzó a utilizarse en las radiocomunicaciones seguras, la base para los sistemas Wifi, Bluetooth, GPS, teléfono móvil etc...

2. Definiciones

Uno de los objetivos de este artículo es exponer la diferencia entre Seguridad de la información, Seguridad informática y Ciberseguridad. Para ello, se utilizan términos específicos cuyo significado figura a continuación.

2.1. Seguridad

Concepto asociado a la certeza, falta de riesgo o contingencia. Podemos entender como seguridad un estado de cualquier sistema o tipo de información que nos indica que ese sistema (informático o no) e información están libres de peligro, daño o riesgo.

2.2. Sistema informático

Conjunto de datos, documentación, procedimientos y tratamientos informáticos en los que se apoyan, así como, bases de datos, redes de comunicaciones, sistemas de interconexión, sistemas de control de accesos de personas y equipos, etc...

4. Europa press /Andalucía /Sevilla. 14/02/2017, «Expuesta en Sevilla una máquina "Enigma" que Hitler regaló a Franco para encriptar mensajes».

2.3. Seguridad informática

Disciplina que utiliza métodos, procesos, técnicas que se encargan de proteger la información cuando se encuentra en un medio informático, así como, de la protección de la infraestructura tecnológica.

2.4. Sistema de información

Conjunto de aplicaciones, servicios o activos de tecnologías de la información u otros componentes que permiten el manejo de la información.

2.5. Seguridad de la información

Función de negocio que tiene la misión de establecer la política de seguridad y los elementos de control físicos, lógicos y legales de la información con el fin de garantizar la disponibilidad, autenticidad, integridad, confidencialidad y auditabilidad de la información que gestiona una organización en su conjunto.

Materia que tiene como fin la protección de la información y de los sistemas de la información del acceso, uso o divulgación no autorizada.

2.6. Ciberespacio

«El ciberespacio es un nuevo dominio para la acción humana. A diferencia de los otros dominios[5]*, que existen naturalmente, es una creación artificial como resultado de una ruptura tecnología que fue facilitada por importantes avances técnicos en el campo de los equipos electrónicos. Sin embargo, lo que propició definitivamente fue la estrecha unión de las telecomunicaciones con el tratamiento automático de los datos; todo ello en gran volumen, a gran velocidad y a escala global»*[6].

2.7. Ciberseguridad

«La ciberseguridad es la práctica de defender las computadoras y los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos. También se conoce como seguridad tecnología de la información o seguridad de la información electrónica»[7].

3. Seguridad informática, ciberseguridad y seguridad de la información ¿son denominaciones distintas para un mismo fin?[8]

Son conceptos relacionados, pero en ningún caso sinónimos. Esta confusión se ha mantenido hasta la actualidad debido a que las medidas de protección relativas a Seguridad informática y Ciberseguridad que se mencionarán a continuación son tecnológicas y, por tanto, se implementan en los Departamentos de tecnologías. En las Administraciones Públicas e incluso en una gran parte del Sector Privado siguen considerando que debe seguir así.

5. Tierra, mar y aire.
6. General de Brigada José Manuel Roldán Tudela.
7. Kaspersky labs.
8. Curso «Dirección y Gestión de la Seguridad a empleados de las Administraciones Públicas», Instituto Nacional de Administraciones Públicas (INAP), 2005.

No obstante, y teniendo en cuenta los requerimientos de las normativas, tanto europeas como españolas, en materia de protección de la información, contenga o no datos personales, distingue entre quien debe tomar las decisiones sobre el nivel de protección adecuado (Unidades de gestión, Responsables de la información) y quién debe garantizarlo mediante la implantación de medidas de seguridad tecnológicas (Departamentos de tecnologías). Lo expuesto no supone que los primeros deleguen la responsabilidad en los segundos.

Llegados a este punto considero apropiado hacer referencia a una frase resultado de una conversación que mantuvo Carlos Solís Salazar[9] con un colega profesor de Universidad. El profesor le dijo *«el problema*[10] *está en que los técnicos os habéis apropiado de la Seguridad de la información»*.

3.1. Seguridad informática

En los años 90 del siglo pasado coincidiendo con la aparición de los primeros virus informáticos y la universalización del uso de Internet, las decisiones sobre Seguridad se basaron principalmente en la tecnología y las adoptaron personas con una gran experiencia tecnológica.

A comienzos de la década (aparición de los primeros virus informáticos) se generalizó la instalación de antivirus en los ordenadores personales.

A finales de la década (universalización del uso de Internet) las medidas de protección estuvieron orientadas a salvaguardar las redes de comunicación y consistían en la instalación de un sencillo firewall (cortafuegos) que frenaba intentos de conexión no autorizados y ataques de denegación de servicio, poco complejos. Pronto esta protección quedó obsoleta dando paso a diseños más robustos, con zonas desmilitarizadas, detectores de intrusión, señuelos (honey pots), etc..., al poco tiempo dejó de ser suficiente.

Complementando a los primeros antivirus y firewalls, se incorporaron servicios adicionales como, entre otros, «alerta temprana», antivirus más sofisticados y controles de acceso a Internet. También en esta época empezó a hablarse del análisis y correlación de eventos, así como la recopilación y conservación de información útil para la investigación forense, que permitieran obtener evidencias, con posible validez legal.

Sin embargo, la implantación de herramientas de este tipo ha sido y es complicada debido a que requieren de, al menos, dos personas dedicadas, como mínimo, seis meses a jornada completa para que analicen los resultados que proporcionan y definir reglas eficientes que las doten de inteligencia.

Debido a la sofisticación de los métodos de ataque y del código malicioso, la estrategia de Seguridad, no sólo de la información, se ha enfocado más hacia la prevención que a la cura, es más proactiva que reactiva.

3.2. Origen y evolución de la Ciberseguridad

El Concepto de Ciberseguridad tuvo su origen en el ámbito militar en el año 2005 y se utilizó junto con el de Ciberdefensa hasta el año 2015. Ambas tenían por objeto hacer frente a las amenazas derivadas del Ciberespionaje y Ciberterrorismo. Este periodo coincidió con los siguientes cambios tecnológicos: telefonía móvil, redes sociales y servicios en cloud (en la nube).

9. Intervención online «Lo que considero que es Seguridad de la información».

10. (de que se utilicen como sinónimos estos conceptos).

Desde el año 2010 hasta 2019 los conceptos utilizados para hacer referencia a la Seguridad, siempre en su vertiente tecnológica, son los que se relacionan a continuación: Ciberresiliencia, Seguridad transparente, Defensa activa, Ciberinteligencia, Gobierno digital. En este periodo las amenazas detectadas empezaron a ser más complejas: APT[11], Hacktivismo, Ciberguerra, Conflicto híbrido y Desinformación.

Tanto la Seguridad informática como la Ciberseguridad se centran en la protección de la información cuando se encuentra en un medio informático, por tanto, salvaguardan la información digital.

Aun así, la Ciberseguridad va más allá, la mejor forma de ilustrar esta afirmación es recoger la definición de ISACA[12] *«la Ciberseguridad tiene como fin la protección de activos de información a través del tratamiento de amenazas que ponen en riesgo la información procesada, almacenada, transportada por los sistemas de información que se encuentran interconectados»*. En el caso de la Seguridad informática los sistemas pueden estar interconectados o no.

Hasta aquí sólo se ha hecho referencia a un medio: tecnológico y a un formato: digital.

3.3. Seguridad de la información

Sin embargo, la información puede mostrarse en **distintos formatos y estados.**

Formatos

1. Digital (medios electrónicos).
2. Físico (papel).
3. Inmaterial (conocimiento de las personas).

Estados:

1. Almacenada (armarios, cajones, soportes electrónicos, discos duros, servidores, usb, nube, etc...)
2. Procesada
3. En tránsito (redes de telecomunicación, moto o coche, etc...)
4. Verbal (conversación)
5. Impresa (documento digita o informe en papel)

«La Seguridad de la información abarca todas las áreas de nuestra organización y nuestra sociedad, independiente del medio en que se encuentre la información, en un medio físico, electrónico e incluso manejada por las personas»

Las personas somos uno de los vectores de ataque que afectan a la Seguridad. Se debe a que partimos del principio de confianza, lo que genera fallas de seguridad. Esta situación requiere concienciar a las personas teniendo en cuenta su perfil. De nada sirve que a nivel organizativo se adopten medidas de seguridad si a título particular, no actuamos con prudencia, aplicando el sentido común.

En resumen, la Seguridad protege la información, en cualquier formato, estado, medio en el que se encuentre y de quien la maneja.

11. Acrónimo anglosajón de Advance Persistent Threat.

12. ISACA (Information Systems Audit and Control Association).

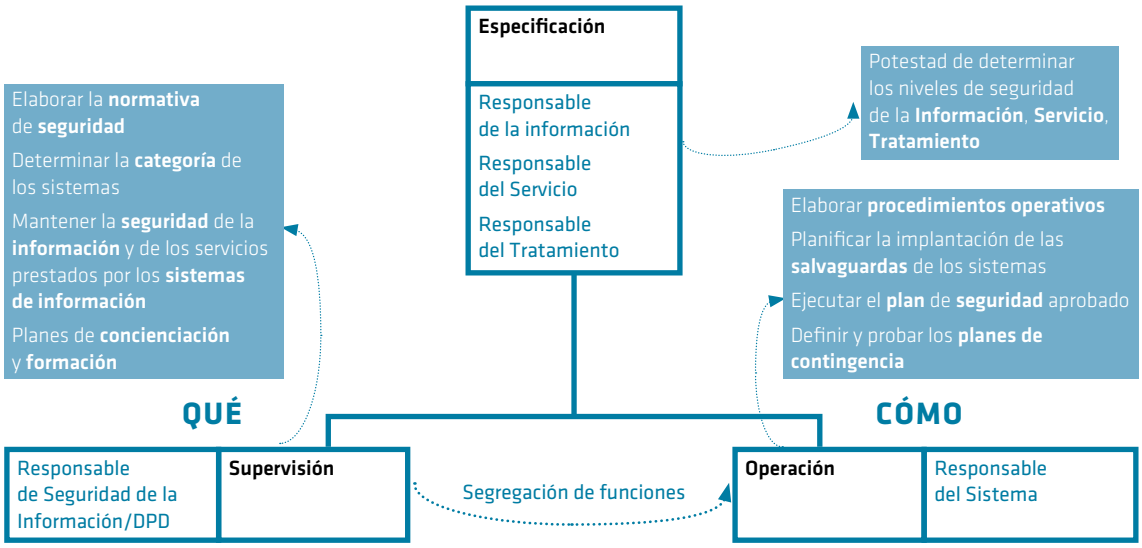
Las medidas de protección que se han de aplicar a la información deben ser proporcionales a su importancia y criticidad. Quienes conocen estos datos son los responsables de la información.

Este rol y su función en materia de Seguridad de la información se trata en el siguiente apartado.

4. Estructura organizativa. Comité de Seguridad de la Información. Responsable de Seguridad de la Información

La Seguridad ha de formar parte de la gobernanza al tratarse de una función transversal, por ello, es imprescindible que exista una estructura organizativa como la que se explica a continuación.

FIGURA 1.
ESTRUCTURA ORGANIZATIVA 1



En la organización de la Seguridad se distinguen tres bloques de responsabilidades:

1. La especificación de las necesidades o requisitos que le corresponde a los responsables de la información y de los servicios. Es posible que coincidan en el mismo órgano las responsabilidades de la Información y del servicio (es lo que se conoce como responsabilidades unificadas).

   Diferenciarlas tiene sentido cuando:
   1.1. El servicio maneja información de diferentes procedencias.
   1.2. La prestación del servicio no depende de la unidad que es responsable de la información.

2. La operación de los sistemas le corresponde al responsable del sistema.

3. La supervisión es competencia del Responsable de Seguridad de la Información.

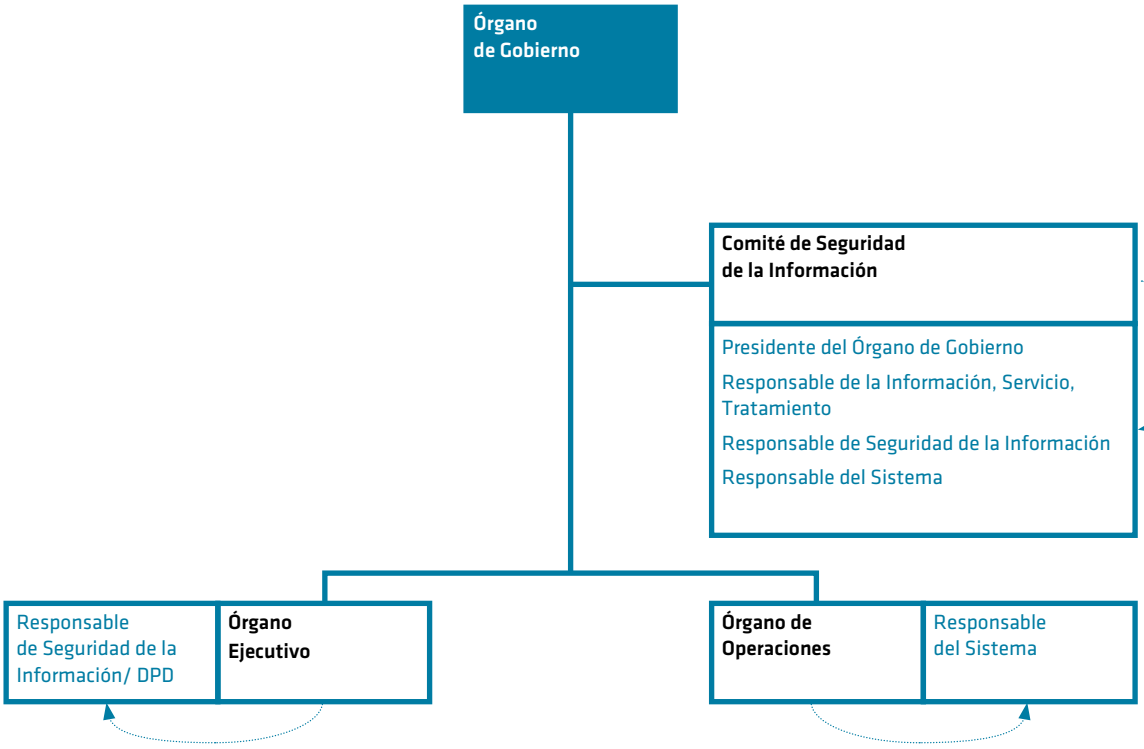
De acuerdo con el principio básico recogido en el artículo 10 del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica[13]: *«la seguridad como función diferenciada»:* la operación y la supervisión deben estar separadas.

La estructura organizativa expuesta debe estar imbricada en la estructura orgánica de la Organización incluyendo un órgano colegiado denominado CSI[14] en el que estén representadas todas las unidades de gestión y tecnológicas para que las decisiones que se adopten sean realistas y aplicables, teniendo en cuenta el principio de proporcionalidad entre funcionalidad y seguridad.

4.1. Comité de Seguridad de la Información

«La coordinación de la seguridad de las entidades del Sector Público es especialmente importante por exigencia de racionalización del gasto y para evitar disfunciones que propicien la aparición de brechas de seguridad provocadas por puntos débiles en los sistemas de información que posibiliten incidentes accidentales o, incluso, ciberataques»[15].

FIGURA 2.
COMPOSICIÓN DEL COMITÉ DE SEGURIDAD DE LA INFORMACIÓN (CSI)



13. Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
14. Comité de Seguridad de la Información.
15. Guía CCN-STIC 801 Responsabilidades y Funciones.

El CSI estará formado por el RSI[16] y por los representantes de otras unidades de la organización afectadas.

«El CSI no es un comité técnico, por ello, deberá recabar del personal técnico, propio o externo, la información pertinente para la toma de decisiones y asesoramiento».

El CSI desempeña un papel importante pues:

1. **Alinear las estrategias** con objeto de asegurar que los responsables de todos los departamentos de gestión y propietarios de la información apoyan la integración con las medidas y procesos de la seguridad.
2. **Aportar valor** mediante el asesoramiento y revisión de las iniciativas en seguridad con objeto de determinar que son adecuadas a las necesidades de cada uno de los centros a los que representan y aportan valor en términos de disponibilidad de los servicios.
3. **Integrar**, es decir, identifica los procesos críticos y establece prioridades para que se les proporcione el nivel adecuado de seguridad. Dirigen sus esfuerzos para conseguir incorporar la seguridad en todos los procesos.

4.2. Responsable Seguridad de la Información

Entre otras, podrá realizar las siguientes funciones:

1. Preparar los temas a tratar en las reuniones del CSI, aportando información puntual para la toma de decisiones.
2. Elaborar el acta de las reuniones.
3. Realizar directamente o mediante las personas en las que se delegue, las decisiones del CSI.
4. Analizar y proponer salvaguardas que prevengan incidentes similares a los que se hayan materializado.
5. Elaborar la declaración de aplicabilidad.
6. Elaborar los planes de concienciación y formación.
7. Validar los planes de continuidad.
8. Reportar al CSI del:
   a. Resumen consolidado de actuaciones en materia de seguridad.
   b. Resumen consolidado de incidentes relativos a la seguridad de la información.
   c. Estado de la seguridad del sistema, en particular del riesgo residual al que el sistema está expuesto.

16. Responsable de Seguridad de la Información.

5. Relación entre el Esquema Nacional de Seguridad y el Reglamento General de Protección de Datos[17] en el ámbito de las Administraciones Públicas

La redacción de este apartado está particularizada para las AA.PP[18].

5.1. Objetivos del RD 3/2010 y del RGPD o Reglamento[19]

Cuando se redactó el RD 3/2010 para la calificación de la información y categorización de los sistemas que la soportan se tuvo en cuenta la LOPD[20] y el RD 1720/2007[21]. En concreto, se tuvieron en cuenta los niveles de seguridad (BÁSICO, MEDIO y ALTO) que se les podían asignar a los datos personales en función de los tipos identificados por el RD 1720/2007.

Fue muy útil para la adaptación de las AA.PP. al ENS[22], facilitó el establecimiento de equivalencias entre los controles exigidos por ambas normativas.

De esta forma se consiguió más eficiencia, así como, el aprovechamiento de las sinergias derivadas del cumplimiento de la LOPD y del RD 1720/2007. En la tabla que figura a continuación se muestran algunas de las equivalencias detectadas.

TABLA 1.
CONTROLES

DOMINIOS	OBJETIVOS DE CONTROL	ENS	RD 1720/2007
Marco organizativo	Cuerpo normativo Auditorías de cumplimiento	• Política de seguridad • Normativa de seguridad • Proceso de autorización • Auditorías de seguridad – Cumplimiento legal – Cumplimiento técnico	• El documento de seguridad (88) • Funciones y obligaciones del personal (89.1) • Responsable de seguridad (95,109) • Registro de incidencias (100.2) • Auditoría (96.1,.2,.3 y 110)
Marco operacional	Control de acceso	• Identificación • Requisitos de acceso • Segregación de tareas • G. derechos acceso • Autenticación	• Identificación y autenticación (93.1,.2,.3,.4,98) • Control de accesos (91.1,.3,.5)
Medidas de protección	Gestión del personal	• Caracterización del puesto de trabajo • Deberes y obligaciones • Concienciación • Formación • Personal alternativo	• Funciones y obligaciones del personal (89.2)

17. Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y la libre circulación de estos datos.
18. Administraciones Públicas.
19. Reglamento General de Protección de Datos.
20. Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
21. Real Decreto, 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.
22. Esquema Nacional de Seguridad.

Desde que entró en vigor el RGPD la identificación de equivalencias con el ENS es más complicada, debido a que el Reglamento no contempla los niveles (BÁSICO, MEDIO y ALTO) para identificar el grado de protección a aplicar a los datos.

El RGPD fue de aplicación directa en España desde el mismo día que entró en vigor, es decir, no requería de un desarrollo normativo en nuestro País. En todo caso, sí que era necesario regular aspectos particulares que afectan a sectores o colectivos concretos.

Para reflejar estas singularidades se redactó la LOPDyGDD[23]. En su disposición adicional primera menciona explícitamente que se aplicarán las medidas de seguridad exigidas por el RD 3/2010 en su Anexo II.

A su vez, en el documento «El impacto del Reglamento General de Protección de Datos sobre la actividad de las Administraciones Públicas» elaborado por la AEPD[24], también se hace mención expresa al ENS: *«En el caso de las AAPP, la aplicación de las medidas de seguridad estará marcada por los criterios establecidos en el Esquema Nacional de Seguridad. No obstante, la aplicación de esas medidas no puede derivarse automáticamente de que se traten unos datos u otros*[25]*, sino que ha de ser la consecuencia de un análisis de riesgos específico para cada tratamiento»*.

El RD 3/2010 persigue la creación de las condiciones necesarias de confianza en el uso de los medios electrónicos, a través de la implantación de medidas para garantizar la seguridad de los sistemas, los datos (sean o no personales), las comunicaciones y los servicios electrónicos (tratamientos), que permita a los ciudadanos (interesados) y a las entidades de su ámbito de aplicación del ejercicio de derechos (sean o no los reconocidos por el Reglamento) y el cumplimiento de deberes a través de estos medios.

En el párrafo anterior se han mencionado datos, tratamientos, interesados, derechos, ellos términos utilizados en el RGPD y la LOPDyGDD, así como, equivalencias con los conceptos empleados por el ENS.

En relación con los datos en el documento elaborado por la AEPD «Lista orientativa de tipos de tratamiento que no requieren una evaluación de impacto relativa a la protección de datos según el artículo 35.5 RGPD», afirma que *«como medida de precaución se ha de considerar el dato personal de una forma extensiva, es decir, se ha de considerar que se tratan datos personales por defecto y, no asumir a priori, que no se pueda asignar dicha categoría a los datos tratados»*.

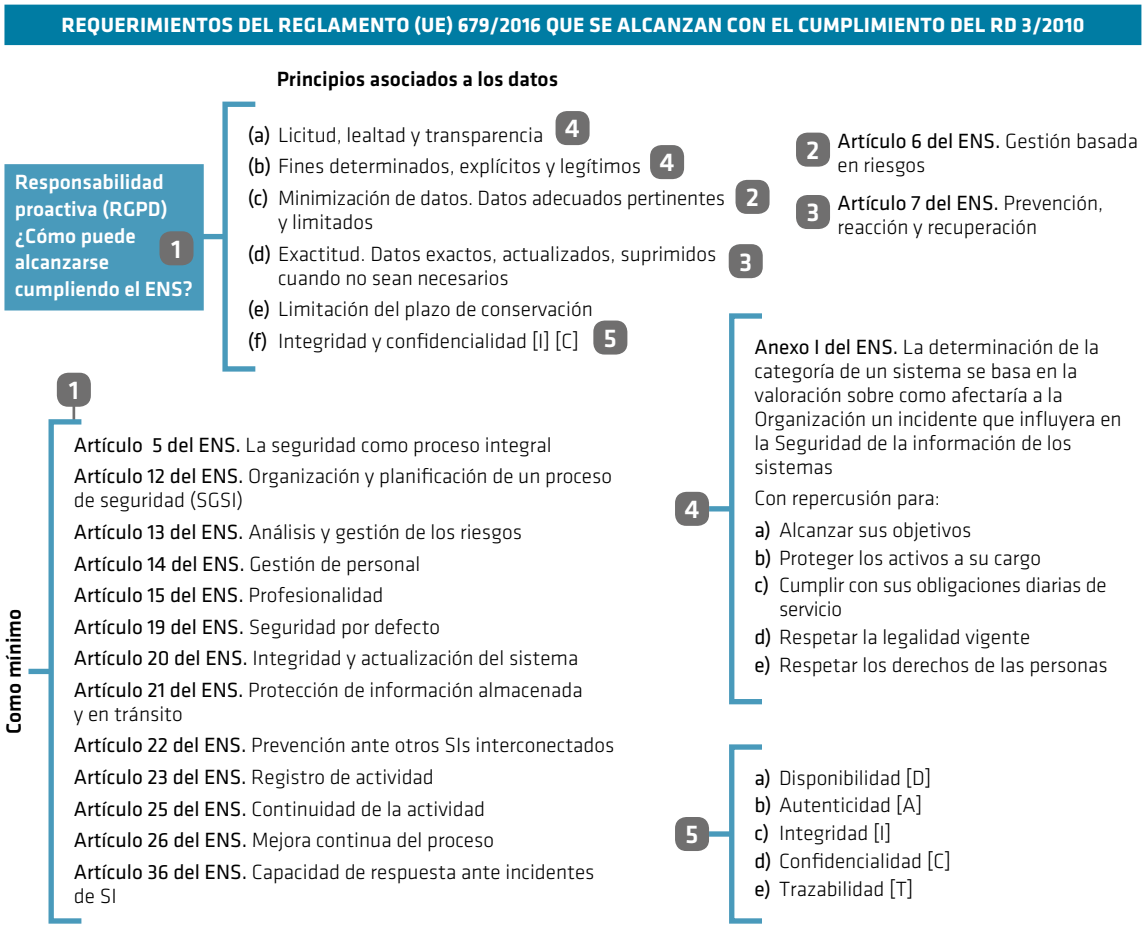
Teniendo en cuenta los requerimientos del RGPD y del ENS algunas de las equivalencias detectadas son las siguientes:

23. Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales.

24. Agencia Española de Protección de Datos.

25. Debido a que ya no se establecen niveles en los que encuadrar los tipos de datos personales tratados.

FIGURA 3
EQUIVALENCIAS ENTRE RGPD-ENS



Para ello he partido del principio «responsabilidad proactiva» regulado en el Reglamento ya que es el requerimiento principal exigido al responsable del tratamiento.

El precitado principio exige el cumplimiento de otros fundamentos asociados a los datos. En la figura 3 los fundamentos están representados en el bloque «Principios asociados a los datos».

El siguiente paso ha sido buscar las posibles equivalencias entre los principios y requisitos regulados en el articulado del RD 3/2010 y las medidas, técnicas y organizativas, del Anexo II del ENS.

«La protección de datos desde el diseño y por defecto»[26] es otro de los principios básicos regulados en el RGPD y tiene su equivalente en el requisito mínimo «Seguridad por defecto»[27].

26. Artículo 25 del RGPD.

27. Artículo 19 del ENS.

5.2. Responsable de Seguridad de la Información[28] y Delegado de Protección de Datos[29]

Desde que se aprobó el Reglamento surgieron dudas sobre si los roles RSI y DPD podían recaer sobre la misma persona. Surgieron dos tesis, la primera propugnaba la existencia de incompatibilidad y la segunda defendía todo lo contrario.

La controversia tuvo su origen en que en la primera tesis se considera que Seguridad informática es lo mismo que Seguridad de la información, mientras que en la segunda no.

En el apartado 3 del presente artículo «Seguridad informática, ciberseguridad y seguridad de la información ¿son denominaciones distintas para un mismo fin?» he clarificado las diferencias entre ambas materias. Una forma muy sencilla de entender esta diferencia es con un ejemplo un dato singular, en sí mismo no facilita un uso indebido del mismo.

María Jesús, es un dato personal ¿haciendo un uso inadecuado del mismo se pueden violentar los derechos de una persona?, entiendo que no. Ahora bien, si en un formulario se introduce María Jesús Casado Robledo, es difícil, aunque no imposible, que haya más personas con el mismo nombre y apellidos. Por consiguiente, con esos datos y todos los que se pueden asociar y si utilizamos los buscadores de Internet, es más fácil.

Si en el formulario se introducen más datos: domicilio, edad, con o sin hijos, estudios, puesto de trabajo, sueldo, cuenta corriente, etc... y después de la recogida (tratamiento) de esos datos a través del formulario, se almacenan (tratamiento) y posteriormente se decide hacer una transferencia bancaria (tratamiento) y alguien se hace con esos datos ya tratados, es decir, convertidos en información, sí que se puede hacer un mal uso de esa información. Por ejemplo, cambiar la cuenta corriente a la que hacer la transferencia.

Teniendo en cuenta el ejemplo anterior ¿qué parte de la información ha de gestionar el DPD y cuál el RSI?

Algunas de las cuestiones que realmente influyen en la posible incompatibilidad es que las personas que ejerzan esos roles:

- Estén capacitadas y formadas en las materias previstas en el RGPD.
- Tengan independencia en la toma de decisiones.
- Ausencia de conflicto de intereses.

Las dos tesis pueden ser válidas. Que se opte por una u otra será el resultado de evaluar las particularidades de cada organización y se adopten las medidas necesarias para garantizar la independencia del DPD[30].

28. RSI.

29. DPD.

30. AEPD: Informe 2018-0170: Incompatibilidad entre DPD y Responsable de Seguridad.

6. Conclusiones

La Seguridad de la información tiene por objeto proteger la información de los riesgos que puedan afectarla en sus diferentes formas o estados y por tanto engloba la seguridad informática y la ciberseguridad.

La Seguridad de la Información es una función transversal que ha de formar parte de la gobernanza de las organizaciones.

La Seguridad de la Información no es sólo un producto tecnológico (antivirus, proxy, detector de intrusión, etc...) que se compra, sino un proceso que se gestiona.

7. Bibliografía

ARTURO RIBAGORDA GARNACHO (2011): *«La escritura secreta. Una historia de 4.000 años». Solemne acto de apertura del curso académico 2011-2012 de la Universidad Carlos III de Madrid. Lección inaugural.*

CARLOS J. CARNICER GARCÍA y JAVIER MARCOS RIVAS (1998). *«Sebastián de Arbizu, espía de Felipe II».*

CENTRO CRIPTOLÓGICO NACIONAL (2019): *Guía de Seguridad de las TIC, CCN-STIC 801 Responsabilidades y Funciones* (marzo 2019).

— (2016) CCN-STIC *830 Ámbito de aplicación del Esquema Nacional de Seguridad* (septiembre 2016).

EL PAÍS, 10 de noviembre de 2015. «Hedy Lamarr, la actriz que inventó el Wifi».

HAIG ANDONIÁN ADLIAN (2012) «Ciclo de conferencias». Histarmar.

JAVIER AREITO BERTOLÍN (2008): *«Seguridad de la información. Redes, informática y sistemas de información»,* Universidad de Deusto, Paraninfo CENGAGE Learning.

JAVIER CANDAU ROMERO (2019): «Presentación Ciberseguridad en Sector Público», Centro Criptológico Nacional.

LUTXANA (2019): «El pensamiento creativo» (www.lutsana.es).

JOSÉ MANUEL ROLDÁN TUDELA (2013): *«Conciencia ciudadana de ciberseguridad, Monografía 137, necesidad de una conciencia nacional de ciberseguridad. La ciberdefensa: un reto prioritario»,* Escuela de Altos Estudios de la Defensa.

MARÍA JESÚS CASADO ROBLEDO (2005): «Dirección y Gestión de la Seguridad de la Información». Curso impartido en el INAP, 2005.

VARIOS AUTORES (2018): *«El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos»*. Adaptado al Proyecto de Ley Orgánica de Protección de Datos de 10 de noviembre de 2017, Wolters Kluwer.

Informatización del Tribunal de Cuentas; especial referencia a la implantación de las nuevas tecnologías aplicadas al ejercicio de la función jurisdiccional de enjuiciamiento contable

MIRIAM CERNUDA SALAMA
Letrada del Tribunal de Cuentas

RESUMEN

El Tribunal de Cuentas no puede permanecer ajeno al proceso de digitalización de la Administración Pública y los órganos del Estado. En el contexto de la sociedad de la información o era digital, la modernización de los servicios públicos exige la incorporación de las nuevas tecnologías aplicadas al funcionamiento de los entes administrativos con el fin de mejorar la prestación conferida al ciudadano. El Tribunal de Cuentas, atendiendo a una firme voluntad de modernización en el ejercicio de las funciones que le son constitucionalmente reconocidas, ha procedido a la incorporación progresiva de las mencionadas tecnologías mediante la implantación de complejos sistemas y desarrollos informáticos que permiten la realización más eficiente de su actuación. Analizaremos, en el presente trabajo, el proceso de digitalización del órgano, con especial referencia a los medios técnicos incorporados para el ejercicio de la función jurisdiccional de enjuiciamiento contable, no pudiendo entenderse, todo ello, sin abordar previamente el proceso de digitalización de la Administración Pública y de la Administración de Justicia.

PALABRAS CLAVE

servicio web | módulo Brahma | AL - SIGM | gestor procesal | Thot portafirmas electrónico

ABSTRACT

The Court of Audit cannot remain oblivious to the digitalization of Public Administration and Constitutional bodies. In the context of Information Society or digital era, the modernization of public services requires the incorporation of new technologies applied to the operation of administrative entities in order to improve the provision conferred on citizens. The Court of Audit, following a firm will to modernize the exercise of the functions that are constitutionally recognized, has proceeded to the progressive incorporation of the mentioned technologies through the implementation of complex computer systems and developments that allow the most efficient performance of their actions. We will analyze, in the present work, the process of digitizacion of the public body with special reference to the technical means incorporated for exercising the jurisdictional function of accounting prosecution, not being able to understand all this without previously addressing the process of digitalization of the Public Administration and the Administration of Justice.

KEYWORDS

web service | *Brahma module* | *AL - SIGM* | *procedural manager* | *Thot electronic signing sistem*

Breve aproximación a la administración electrónica: concepto, principales disposiciones normativas y aplicaciones prácticas

1. Administración electrónica: resultado de la adaptación al entorno de la Administración Pública

Hace ya más de una década el Estado español emprendió el proceso de informatización de la Administración Pública. En el contexto de la sociedad de la información o era digital, en que el uso de las tecnologías de la información y la comunicación (TIC) se encuentra generalizado, la modernización de los servicios públicos exigía la incorporación de los medios tecnológicos existentes aplicados a su funcionamiento[1]. La implantación de medios técnicos, electrónicos, informáticos y telemáticos en las administraciones públicas respondía así, a la voluntad de dotar de una mayor celeridad, eficiencia y seguridad al sistema, mejorando en definitiva, la prestación del servicio al ciudadano[2].

Actualmente, sin embargo, la incorporación de las nuevas tecnologías a la administración no se concibe ya como una mera tecnificación de su actividad, habiendo dejado de ser únicamente una herramienta puesta a su servicio para la consecución de los objetivos que le son propios, para convertirse en un elemento integrante del propio concepto de administración, constituyendo lo que denominamos administración electrónica o e-administración[3].

Al servicio pues, del ciudadano, la Administración queda obligada a transformarse en una administración electrónica regida por el principio de eficacia que proclama el artículo 103 de nuestra Constitución.[4, 5]

La Comisión Europea definió la administración electrónica o «e-government» como *«la utilización de las tecnologías de la información y la comunicación en las Administraciones*

1. En términos de la Exposición de Motivos de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, «las Administraciones deben comprometerse con su época y ofrecer a sus ciudadanos las ventajas y posibilidades de la sociedad de la información».
2. La Exposición de Motivos de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos afirma que «El mejor servicio al ciudadano constituye la razón de las reformas que tras la aprobación de la Constitución se han ido realizando en España para configurar una Administración moderna».
3. Araguàs Galcerà, Irene. *La Administración electrónica en España: de la «administración en papel» a la «e-administración»*. Revista chilena de derecho y ciencia política, agosto-diciembre 2012 págs. 109-139.
4. Así lo indica la Exposición de Motivos de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.
5. Artículo 103.1 de la Constitución Española: «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.»

Públicas, asociada a cambios en la organización y nuevas aptitudes del personal con el objetivo de mejorar los servicios públicos, reforzar los procesos democráticos y apoyar a las políticas públicas».[6]

2. Evolución normativa

La incorporación de la tecnología a la estructura y funcionamiento administrativos, es el resultado de un largo y dificultoso proceso de transformación normativa y de correlativa dotación a los entes públicos de los medios técnicos materiales necesarios al efecto.

2.1. Un primer reconocimiento: la RJPAc

La Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común («LRJPAC»), en su primera versión, contempló ya en su artículo 45, relativo a la «Incorporación de medios técnicos», la posibilidad de que los ciudadanos se relacionaran electrónicamente con las Administraciones Públicas cuando ello fuera compatible con los medios de que estas dispusieran. Se reconoció, asimismo, la necesidad de que estas impulsaran el empleo y aplicación de las técnicas y medios electrónicos, informáticos y telemáticos, para el desarrollo de su actividad y el ejercicio de sus competencias. Suponía, esta previsión, un primer y tímido avance.

Esa disposición, junto con la de la informatización de registros y archivos prevista en el artículo 38, en la redacción que le dio la Ley 24/2001, de 27 de diciembre, por la que se permitía la implantación de registros telemáticos para la recepción o salida de solicitudes, escritos y comunicaciones por medios informáticos, supuso un verdadero punto de partida en la utilización de los medios tecnológicos para relacionarse con las Administraciones Publicas.

La misma Ley 24/2001 modificó, asimismo, el artículo 59, permitiendo la notificación por medios telemáticos en los supuestos en los que el interesado hubiera señalado dicho medio como preferente o lo hubiera consentido expresamente.

2.2. El impulso determinante de la Ley 11/2007

La Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, supuso el impulso definitivo para la conformación de una administración digital. Reconoció el derecho, no ya la mera posibilidad, de los ciudadanos a relacionarse electrónicamente con las Administraciones Públicas, así como la obligación de éstas de dotarse de los medios y sistemas necesarios para que ese derecho pudiera ejercerse. Impuso, asimismo, a las Administraciones Públicas, la obligación de relacionarse electrónicamente entre ellas.

La Ley 11/2007, prevé la incorporación de los medios tecnológicos a la administración desde una doble perspectiva, interna y externa. En su vertiente interna, la informatización de su estructura interior permite maximizar la eficiencia de su funcionamiento, indicando el artículo 3.5 relativo a las «Finalidades de la Ley», que son fines de ésta: «Contribuir a la mejora del funcionamiento interno de las Administraciones Públicas, incrementando

6. Comunicación de la Comisión Europea, de 26 septiembre 2003, al Consejo, al Parlamento Europeo, al Comité Económico y Social Europeo y al Comité de las Regiones la Administración.

la eficacia y la eficiencia de las mismas mediante el uso de las tecnologías de la información, con las debidas garantías legales en la realización de sus funciones». A estos efectos, la propia exposición de motivos de la mencionada disposición ya señalaba que, «en cuanto al funcionamiento interno de la Administración, las nuevas tecnologías permiten oportunidades de mejora (eficiencia y reducción de costes) que hacen ineludible la consideración de las formas de tramitación electrónica, tanto para la tramitación electrónica de expedientes, como para cualquier otra actuación interna de la Administración». Pero también desde una perspectiva exterior, en cuanto a la comunicación o relación del ciudadano con los entes públicos, a cuyo efecto el artículo 3, en sus apartados primero y segundo, incluye entre las mencionadas finalidades de la Ley, las de «facilitar el ejercicio de derechos y el cumplimiento de deberes por medios electrónicos» y «facilitar el acceso por medios electrónicos de los ciudadanos a la información y al procedimiento administrativo, con especial atención a la eliminación de las barreras que limiten dicho acceso».

Para hacer efectivo el mencionado derecho a relacionarse electrónicamente con los entes públicos, la Ley 11/2007 incorpora por primera vez el concepto de sede electrónica, como dirección electrónica cuya gestión y administración corresponde a una Administración Pública, para la comunicación telemática con la administración.[7]

Se regulan, asimismo, las formas de identificación y autenticación, tanto de los ciudadanos como de los órganos administrativos en el ejercicio de sus competencias, habilitándose distintos instrumentos de acreditación, promoviéndose el uso general de la firma electrónica y determinando la obligación, para cualquier Administración, de admitir los certificados electrónicos reconocidos en el ámbito de la Ley de Firma Electrónica.

Se prevé la constitución de registros, comunicaciones y notificaciones electrónicas para la consecución digital de trámites administrativos. Se regula, asimismo, la creación de documentos y archivos electrónicos, las condiciones para reconocer la validez de los mismos y de las copias electrónicas, tanto las realizadas a partir de documentos emitidos originariamente en papel, como las copias de documentos que ya estuvieran en soporte electrónico y las condiciones para realizar en soporte papel, copia de originales emitidos por medios electrónicos, o viceversa.

Se regulan, por último, las condiciones en que se ha de hacer posible la gestión electrónica de los procedimientos, guardando un cierto paralelismo con la regulación de la Ley 30/1992, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, en cuanto a la iniciación, instrucción y terminación de aquellos por medios electrónicos.

2.2.1. Interoperabilidad y seguridad

El reconocimiento de aquellos derechos y obligaciones, trajo consigo importantes consecuencias prácticas derivadas, por un lado, de la necesidad de adaptación de la maquinaria administrativa a la actualidad tecnológica que permitiera el intercambio de datos que exige la actuación de los poderes públicos, y por otro, de la necesidad de salvaguardar

7. Artículo 10: «La sede electrónica es aquella dirección electrónica disponible para los ciudadanos a través de redes de telecomunicaciones cuya titularidad, gestión y administración corresponde a una Administración Pública, órgano o entidad administrativa en el ejercicio de sus competencias».

las garantías constitucionales y legales a los derechos de los ciudadanos que se relacionan con la Administración Pública, en los términos que determina el artículo 18.4 de la Constitución Española[8], constituyendo la protección de los derechos constitucionales el limite más estricto al uso de las tecnologías de la información. Estas necesidades determinaron la exigencia de garantizar la interoperabilidad —o capacidad de los sistemas de información y de los procedimientos a los que éstos dan soporte, de compartir datos y posibilitar el intercambio de información y conocimiento entre ellos—[9] y la seguridad en la utilización de medios electrónicos que permita la adecuada protección de la información. La propia ley se refiere, así, a la necesidad de creación de un esquema nacional de interoperabilidad y de un esquema nacional de seguridad[10], que dieron lugar al Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica y al Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.

2.3. CORA: una perspectiva global

Unos años más tarde, la Comisión para la Reforma de las Administraciones Públicas (CORA) propuso el objetivo de convertir las Administraciones Públicas en un factor de competitividad de la economía española, con medidas de racionalización de estructuras, procedimientos y recursos, plasmadas en su informe final presentado al Gobierno de España en junio de 2013, siendo más de la mitad de las medidas, directa o indirectamente, actuaciones relativas a tecnologías de la información y las comunicaciones (TIC)[11].

2.4. Leyes 39 y 40/2015

Las leyes 39/2015 y 40/2015 de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas y de Régimen Jurídico del Sector Público suponen un avance aún mayor.

Se refieren, respectivamente, a las relaciones de la administración con carácter ad extra —de las administraciones con los administrados— y ad intra —del funcionamiento interno de la administración y de las relaciones entre ellas—, abordando desde esta misma perspectiva el impulso de la digitalización.

Tal y como indica la Exposición de Motivos de la primera, «en el entorno actual, la tramitación electrónica no puede ser todavía una forma especial de gestión de los procedimientos

8. Artículo 18.4: «La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos».

9. Definición procedente del Glosario de términos del Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.

10. Artículo 42: Esquema Nacional de Interoperabilidad y Esquema Nacional de Seguridad. 1. El Esquema Nacional de Interoperabilidad comprenderá el conjunto de criterios y recomendaciones en materia de seguridad, conservación y normalización de la información, de los formatos y de las aplicaciones que deberán ser tenidos en cuenta por las Administraciones Públicas para la toma de decisiones tecnológicas que garanticen la interoperabilidad. 2. El Esquema Nacional de Seguridad tiene por objeto establecer la política de seguridad en la utilización de medios electrónicos en el ámbito de la presente Ley, y está constituido por los principios básicos y requisitos mínimos que permitan una protección adecuada de la información.

11. Acuerdo del Consejo de Ministros del 26 de octubre de 2012 para mejorar la eficiencia y eficacia de la actividad pública.

sino que debe constituir la actuación habitual de las Administraciones. Porque una Administración sin papel basada en un funcionamiento íntegramente electrónico no sólo sirve mejor a los principios de eficacia y eficiencia, al ahorrar costes a ciudadanos y empresas, sino que también refuerza las garantías de los interesados»[12].

La ley 39/2015, sistematiza y clarifica el régimen jurídico existente, integrando el contenido de las disposiciones 30/92 y 11/07 (derogando ambas) y dando un paso más, pues si bien reconoce el derecho de las personas físicas a relacionarse electrónicamente con la administración, lo impone como obligación a ciertos sujetos como a las personas jurídicas o las entidades sin personalidad jurídica[13].

Incluye otras importantes novedades en materia de administración electrónica como la regulación diferenciada de la identificación y firma electrónica, de modo que, con carácter general, sólo será necesaria la primera, y se exigirá la segunda cuando deba acreditarse la voluntad y consentimiento del interesado.

Impone, asimismo, la obligación a todas las administraciones de contar con un registro electrónico, o bien adherirse al de la Administración General del Estado, y de un archivo electrónico para los procedimientos finalizados.

Regula también, de forma novedosa, las notificaciones electrónicas, que habrán de ser preferentes, estableciéndose nuevas medidas que garanticen el conocimiento de la puesta a disposición de las notificaciones como: el envío de avisos de notificación, siempre que sea posible, a los dispositivos electrónicos y/o a la dirección de correo electrónico que el interesado haya comunicado, así como el acceso a sus notificaciones a través del Punto de Acceso General Electrónico de la Administración, que funcionará como un portal de entrada.

Por su parte, la Ley 40/2015, reitera la obligación de las administraciones de relacionarse electrónicamente entre ellas y contiene una nueva regulación de la sede electrónica, la firma y la actuación administrativa automatizada. Se prevé, asimismo, la generalización del uso de medios electrónicos por órganos colegiados, en cuanto a su constitución, celebración de sesiones, adopción de acuerdos y elaboración y remisión de las actas de sus reuniones.

12. Punto III de la Exposición de Motivos de la Ley 39/2015.

13. Artículo 14.2 2 de la Ley 39/2015: «En todo caso, estarán obligados a relacionarse a través de medios electrónicos con las Administraciones Públicas para la realización de cualquier trámite de un procedimiento administrativo, al menos, los siguientes sujetos:

a) Las personas jurídicas.

b) Las entidades sin personalidad jurídica.

c) Quienes ejerzan una actividad profesional para la que se requiera colegiación obligatoria, para los trámites y actuaciones que realicen con las Administraciones Públicas en ejercicio de dicha actividad profesional. En todo caso, dentro de este colectivo se entenderán incluidos los notarios y registradores de la propiedad y mercantiles.

d) Quienes representen a un interesado que esté obligado a relacionarse electrónicamente con la Administración.

e) Los empleados de las Administraciones Públicas para los trámites y actuaciones que realicen con ellas por razón de su condición de empleado público, en la forma en que se determine reglamentariamente por cada Administración».

2.5. Marco europeo

El desarrollo normativo nacional se enmarca en el contexto de exigencias y evolución normativa europea, cuyo punto de partida se sitúa en el Consejo Europeo de Lisboa y Santa María da Feira, celebrado en marzo del año 2000, del que surge la Estrategia Lisboa 2000. Se perfila como una estrategia global de política económica y social sobre la base del impulso de la Sociedad de la Información en la UE. Se concluye que las Tecnologías de la Información debían contribuir, de manera determinante, a la creación de una Europa competitiva. Le sucede la Estrategia Europa 2020, adoptada en el Consejo Europeo de 17 de junio de 2010, que fija la denominada Agenda Digital para Europa.

La Directiva 2006/123/CE, de 12 de diciembre de 2006, relativa a los servicios en el mercado interior, se aprobó con objeto de avanzar en la consecución del objetivo fijado por el Consejo Europeo de Lisboa. Establece, entre otras obligaciones para los Estados miembros, la de facilitar, por medios electrónicos, acceso a los trámites relacionados con las actividades de prestación de servicios. Fue transpuesta a nuestro ordenamiento por la Ley 17/2009, de 23 de noviembre, sobre el libre acceso a las actividades de servicios y su ejercicio.

En el marco de las mencionadas estrategias, se aprueban, por la Comisión, sucesivos planes para el impulso de la administración electrónica —*«Plan de acción sobre administración electrónica i2010: acelerar la administración electrónica en Europa en beneficio de todos»*, de 25 de abril de 2006, el *«Plan de Acción Europeo sobre Administración Electrónica 2011-2015 Aprovechamiento de las TIC para promover una administración pública inteligente, sostenible e innovadora»* y el *«Plan de acción de administración electrónica 2016-2020: se acelera la transformación digital de la administración»*—, que terminan de perfilar un plan de acción europeo para optimizar el funcionamiento de los poderes públicos por medio de la tecnología digital.

3. La administración electrónica en la práctica

La administración electrónica constituye hoy en día una realidad: más de 24 millones de españoles disponen ya de DNI electrónico, una de cada dos declaraciones del impuesto sobre la renta se hace vía telemática y el 90 % de los trámites con la Administración General del Estado pueden realizarse ya por medios electrónicos[14].

Un extensísimo conjunto de sistemas, aplicaciones y programas informáticos puestos a disposición de los operadores administrativos y del ciudadano, hacen posible el funcionamiento telemático de la administración en los términos referidos. Todos ellos constan en el Catálogo de Servicios de Administración Digital, elaborado por la Secretaría General de Administración Digital.

Algunos de estos sistemas son: en materia de identidad digital y firma electrónica, las plataformas cl@ve, cl@ve firma, @firma Port@firmas, o Auténtica. En materia de registros y representación del ciudadano ante las administraciones públicas: SIR, sistema de

14. Datos obtenidos de la sección de nuevas tecnologías de la página web del poder judicial www.poderjudicial.es.

interconexión de Registros, Registro Electrónico Común, Apodera (registro electrónico de apoderamiento de la administración General del Estado) o Habilita (registro de funcionarios habilitados). En materia de atención al ciudadano y a la empresa: PAG (Punto de Acceso General), 060 (Punto de acceso telefónico de las administraciones públicas) o la Carpeta ciudadana. En materia de sistemas de información transversales SIA (sistema de información administración) o DIR3 (Directorio Común de Unidades). En materia de comunicaciones y notificaciones al ciudadano: Dirección Electrónica Habilitada única o Punto único de notificaciones para todas las Administraciones Públicas o Notifica (Gestión de notificaciones). En materia de expediente documento y archivo electrónico: InSIDE (Infraestructura y Sistemas de Documentación Electrónica o Archive (Archivo definitivo de expedientes y documentos). En materia de comunicación y difusión: PAe (Portal de Administración Electrónica). En materia de gestión interna: FUNCIONA (Portal del Empleado Público) o ALMACÉN (para el envío y recepción de ficheros de gran tamaño). O en materia de infraestructuras de comunicación: Sara (Sistema de Aplicaciones y Redes para las Administraciones)[15].

Administración Electrónica de Justicia

1. La situación particular de la Administración de Justicia

Al igual que sucede en el ámbito genérico de la administración, *los avances en el uso de las nuevas tecnologías de comunicación constituyen un valioso instrumento para el desarrollo de las actuaciones de la Administración de Justicia, así como en su relación con los profesionales y los ciudadanos*.[16]

La Administración de Justicia, sin embargo, adscrita a un poder distinto e independiente al del resto de administraciones, el poder judicial, presenta características peculiares derivadas del ejercicio de la función que incumbe a los órganos jurisdiccionales que la integran, de juzgar y hacer ejecutar lo juzgado, que exige una particular adaptación del proceso de digitalización de su aparato, la cual se encuentra condicionada a la estricta observancia de la normativa procesal, en aras a garantizar el derecho constitucional a la tutela judicial efectiva[17].

15. Información obtenida del Catálogo de Servicios de Administración Digital, en el PAe, Portal de Administración Electrónica.

16. Exposición de Motivos de la Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia.

17. Tal y como indica la Exposición de motivos de la Ley 18/2011, «La Administración de Justicia presenta características que la diferencian de las restantes Administraciones públicas. En primer lugar, por la propia naturaleza de la función que la Administración judicial tiene atribuida, ya que se trata de un poder del Estado distinto del poder ejecutivo, en el que que se encuadran las Administraciones públicas que, además, debe satisfacer un derecho fundamental que a su vez vez es clave para sostener el Estado de Derecho».

La salvaguarda de este derecho —el de la obtención de tutela por jueces y tribunales—, determina que el proceso de digitalización sea especialmente sensible y deba acometerse con especial cuidado.

Efectivamente, la informatización de la Administración de Justicia o implantación de lo que se conoce como e-justicia, se ha emprendido de manera separada a la informatización del resto de las administraciones, regulándose en disposiciones normativas distintas que prevén instrumentos y sistemas diferentes con que adaptar la exigencia de modernización a sus peculiares necesidades.

Tal y como afirma la Exposición de Motivos de la Ley 18/2011, en atención a las peculiares características de la Administración de Justicia, «se ha considerado que la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, no es plenamente aplicable a la Administración de Justicia y es necesaria una regulación específica. Ello no quiere decir, no obstante, que no se hayan adoptado idénticos principios y valores en muchos aspectos».

2. Marco normativo

La actual Administración Judicial electrónica es fruto de una larga evolución normativa. Si bien la Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia, constituye el primer gran impulso, existen algunos precedentes.

2.1. Antecedentes a la Ley 18/2011

Ley Orgánica 16/1994, de 8 de noviembre, por la que se reformó la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, introdujo, por vez primera en nuestro ordenamiento jurídico, la posibilidad de utilización por los juzgados y tribunales, de medios técnicos, electrónicos e informáticos en el ejercicio de sus funciones jurisdiccionales.

El Pleno del Congreso de los Diputados aprobó el día 16 de abril de 2002 una proposición no de ley sobre la Carta de Derechos de los Ciudadanos ante la Justicia. Esta demandaba en su preámbulo una Justicia más abierta y capaz de dar respuesta a los ciudadanos de forma más ágil y eficaz. Su apartado 21, ahondando en la necesidad de que la justicia sea tecnológicamente avanzada, reconoce el derecho «a comunicarse con la Administración de Justicia a través del correo electrónico, videoconferencia y otros medios telemáticos con arreglo a lo dispuesto en las leyes procesales».

Posteriormente, la Ley 15/2003, de 26 de mayo, reguladora del régimen retributivo de las carreras judicial y fiscal, se refirió específicamente al objetivo general de transparencia proclamado en la Carta de Derechos de los Ciudadanos ante la Justicia, con la creación de un instrumento denominado Plan de Transparencia Judicial, aprobado por el Consejo de Ministros el 21 de octubre de 2005. Aquel identificaba como instrumento imprescindible para lograr el objetivo de transparencia, la plena utilización de las tecnologías de la información y la comunicación en la Administración de Justicia. Para ello se refería a la necesidad de hacer compatibles las distintas aplicaciones informáticas que se utilizan en

las oficinas judiciales, así como crear páginas de información en las Administraciones con competencias en materia de justicia. También se declara la necesidad de establecer sistemas adecuados de interconexión y sistemas de intercambio seguro de documentos en los procesos judiciales, así como garantizar la disponibilidad de los sistemas de comunicaciones entre las distintas sedes judiciales electrónicas.

Además, el Real Decreto 84/2007, de 26 de enero (actualmente derogado por el Real Decreto 1065/2015)[18] regula por primera vez, la implantación, en la Administración de Justicia, del sistema informático de telecomunicaciones *LexNet,* para la presentación de escritos y documentos, el traslado de copias y la realización de actos de comunicación procesal por medios telemáticos.

2.2. La Ley 18/2011

La Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y comunicación en la Administración de Justicia, supuso el impulso definitivo en la digitalización de la justicia. Surge en el contexto del «Plan Estratégico de Modernización del Sistema de Justicia 2009-2012».

Tal y como determina su Exposición Motivos , nace con el propósito de garantizar el derecho a obtener la tutela efectiva de los derechos de los ciudadanos ante los tribunales que reconoce el artículo 24.1 de la Constitución Española y en el artículo 14.1 del Pacto Internacional de Derechos Civiles y Políticos, mediante la modernización de la Administración de Justicia, como requisito esencial para consolidar el Estado de Derecho y mejorar la calidad de nuestra democracia.

En ella, por primera vez, se reconoce el derecho de los ciudadanos a relacionarse electrónicamente con la Administración de Justicia. Se reconoce, asimismo, el deber de utilización de los medios electrónicos por parte de los profesionales de la justicia y oficinas judiciales, así como la obligación de las Administraciones competentes de dotar a aquellos de los medios necesarios al efecto.

Todo ello llevó aparejado la necesidad de creación de un sistema que garantizara la interoperabilidad y seguridad, lo cual se concretó en la creación de un Esquema Judicial de interoperabilidad y seguridad[19].

Destaca, asimismo, la previsión de un Comité técnico estatal de la Administración judicial electrónica (creado por medio del Real Decreto 396/2013, de 7 de junio, por el que se regula el Comité técnico estatal de la Administración judicial electrónica) con importantes competencias en orden a favorecer la compatibilidad y a asegurar la interoperabilidad de los

18. Real Decreto 1065/2015, de 27 de noviembre, sobre comunicaciones electrónicas en la Administración de Justicia en el ámbito territorial del Ministerio de Justicia y por el que se regula el sistema *LexNET*.

19. A él se refiere la Ley en su artículo 45, por el que establece que «el Comité técnico estatal de la Administración judicial electrónica fijará las bases para el desarrollo del Esquema judicial de interoperabilidad y seguridad de modo que permita, a través de las plataformas tecnológicas necesarias, la interoperabilidad total de todas las aplicaciones informáticas al servicio de la Administración de Justicia.» El documento sobre Bases fue aprobado por pleno del CTEAJE con fecha 1 de junio de 2015, procediendo a su publicación el 6 de julio de 2015.

sistemas y aplicaciones empleados en la Administración de Justicia, así como para asegurar la cooperación entre las distintas Administraciones[20].

Como principales incorporaciones por las que se perfila el sistema de Administración judicial electrónica, la Ley prevé la creación de sedes judiciales electrónicas de los distintos órganos jurisdiccionales, equivalentes a direcciones electrónicas, a través de las cuales realizar cualesquiera actos procesales, así como acceder al contenido de los expedientes en los que se intervenga o se actúe como parte interesada. El artículo 10.1 afirma que «Se realizarán a través de sedes judiciales electrónicas todas las actuaciones, procedimientos y servicios que requieran la autenticación de la Administración de Justicia o de los ciudadanos y profesionales por medios electrónicos.» La norma regula concretamente la creación de dichas sedes, de las que podrán derivar otras subsedes con funciones más específicas, y qué contenidos mínimos deben ofrecer.

Por otro lado, se dispone la creación de un punto de Acceso General de la Administración de Justicia, a través del cual se podrá acceder a todas las sedes y subsedes del territorio nacional. El Punto de Acceso General será creado y gestionado por el Ministerio de Justicia conforme a los acuerdos que se adopten en el Comité técnico estatal de la Administración de Justicia electrónica.

La Ley prevé, asimismo, mecanismos de identificación y autenticación electrónica, tanto de los ciudadanos y profesionales como de la propia Administración de Justicia, para la realización de los trámites procesales por vía telemática que sustituyan la identificación presencial y la firma manuscrita. Los medios autorizados deberán resultar adecuados para garantizar la identidad de los firmantes y, en su caso, la autenticidad e integridad de los documentos electrónicos firmados[21].

La Ley prevé también, las condiciones para hacer posible la íntegra tramitación electrónica de los procedimientos judiciales. Se define y regula el expediente judicial electrónico, EJE, en términos de la Exposición de Motivos de la ley, el *«heredero digital de los "autos"»,* para propiciar la desaparición del soporte papel en la tramitación de los expedientes judiciales.

Así, el artículo 25, relativo a los «Criterios para la gestión electrónica» indica que *«la gestión electrónica de la actividad judicial respetará el cumplimiento de los requisitos formales y materiales establecidos en las normas procesales.»* Mientras que el Artículo 26 relativo al «Expediente judicial electrónico» lo define como *«el conjunto de documentos electrónicos correspondientes a un procedimiento judicial, cualquiera que sea el tipo de información que contenga».*

Se prevé que el foliado de los expedientes judiciales electrónicos se llevará a cabo mediante un índice electrónico, firmado por la oficina judicial actuante y que la remisión de expedientes se sustituirá a todos los efectos legales por la puesta a disposición del expediente judicial electrónico, teniendo derecho a obtener copia electrónica del mismo todos aquellos que lo tengan conforme a lo dispuesto en las normas procesales.

20. Previsto en los artículos 44 y 45 de la Ley 18/2011.

21. Artículo 14 de la Ley.

2.3. Otras disposiciones

Otras normas han contribuido a la configuración de una Administración de Justicia electrónica, como la Ley 42/2015, de 5 de octubre, de reforma de la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil, en que se incorporan al ámbito de la jurisdicción civil las disposiciones relativas a la utilización de los medios tecnológicos previstas en la Ley 18/2011, cuya Exposición de Motivos afirma *«que constituye una necesidad imperiosa acometer una reforma en profundidad de las diferentes actuaciones procesales para generalizar y dar mayor relevancia al uso de los medios telemáticos o electrónicos, otorgando carácter subsidiario al soporte papel.»* Destaca, asimismo, la Ley 19/2015, de 13 de julio, de medidas de reforma administrativa en el ámbito de la Administración de Justicia y del Registro Civil, en que se regulan las condiciones de celebración de la subasta notarial y judicial electrónica.

2.4. Marco europeo

En el entorno de la Unión Europea, la comunicación de la Comisión al Consejo, Parlamento y Comité Económico y Social Europeo de 30 de mayo de 2008 determinó la creación del Plan de Acción E-Justicia. Éste, creado con cargo a los programas financieros Justicia Civil y Justicia Penal, tiene como objetivo mejorar la eficacia de los sistemas judiciales europeos mediante la aplicación de las tecnologías de la información y comunicación en la gestión administrativa de los procesos judiciales. A tal fin, propuso la adopción de medidas coordinadas a nivel nacional y europeo, así como el uso de herramientas homogéneas de interconexión e intercambio de información.

3. Principales medios técnicos

En la práctica, diversas plataformas y aplicaciones informáticas implementan las previsiones normativas mencionadas, si bien la asunción de competencias, en materia de justicia, por parte de la mayoría de las Comunidades Autónomas, supone un obstáculo a la plena integración del sistema.

Tanto es así que, actualmente, conviven en la Administración de Justicia nueve sistemas distintos de gestión procesal electrónica, en particular *Adriano,* para la Comunidad Autónoma de Andalucía, *Atlante,* en Canarias, *Cicerone* en la Comunidad Valenciana, *Justizia.eus* en País Vasco, *Libra* en Madrid, *ThemisIIe.justicia.cat* en Cataluña, *Avantius* en Navarra, *Vereda* en Cantabria, *Fortuny* en el Ministerio Fiscal y *Minerva* en el Ministerio de Justicia, en Galicia y en las Comunidades Autónomas que no tienen asumidas competencias en la materia, es decir, Extremadura, Castilla-La Mancha, Castilla y León, Islas Baleares, Región de Murcia, Ceuta y Melilla[22].

Por medio de la Orden JUS/1126/2015, de 10 de junio, se crea la Sede Judicial Electrónica del Ministerio de Justicia que abarca el ámbito de sus competencias en materia de Administración de Justicia, es decir, Tribunal Supremo, Audiencia Nacional y las Comunidades Autónomas que no tienen asumidas competencias en materia de justicia antes mencionadas[23].

22. Datos obtenidos de la página web del Poder Judicial, www.poderjudicial.es

23. Cada Comunidad Autónoma ha regulado, asimismo, su propia sede electrónica y subsedes para realización digital de los trámites procesales en el ámbito de su respectiva jurisdicción.

En el ámbito de la Sede Judicial Electrónica del Ministerio de Justicia, se admitirán como medios de autenticación e identificación los certificados electrónicos de clave pública, no revocados, soportados por @firma (Plataforma de validación y firma electrónica del Ministerio de Hacienda y Administraciones Públicas), DNI electrónico, los sistemas cl@ve pin, cl@ve permanente y cl@ve[24].

Para la realización de comunicaciones y notificaciones electrónicas, el Real Decreto 1065/2015, de 27 de noviembre, sobre comunicaciones electrónicas en la Administración de Justicia en el ámbito territorial del Ministerio de Justicia y por el que se regula el sistema *LexNET,* deroga el Real Decreto 84/2007, de 26 de enero.

El sistema *LexNET* es un medio transmisión seguro de información que, mediante el uso de técnicas criptográficas, garantiza la presentación de escritos y documentos y la recepción de actos de comunicación, sus fechas de emisión, puesta a disposición y recepción o acceso al contenido de los mismos.

El sistema garantiza el contenido íntegro de las comunicaciones y la identificación del remitente y destinatario de las mismas mediante técnicas de autenticación adecuadas, de conformidad con lo dispuesto en la Ley 59/2003, de 19 de diciembre, de firma electrónica, y en el Reglamento UE Nº 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior.

Digitalización del Tribunal de Cuentas

1. La necesidad de informatización del Tribunal de Cuentas en el contexto generalizado de informatización de la Administración Pública

En el contexto de digitalización de la Administración Pública y de la Administración de Justicia, el Tribunal de Cuentas no podía permanecer inmóvil. «La evolución de la gestión en papel a la gestión electrónica de los procedimientos en las Administraciones Públicas, impulsada por la Ley 11/2007 de Acceso Electrónico de los Ciudadanos a los Servicios Públicos, es un impulso al que no puede permanecer ajeno el Tribunal de Cuentas».[25]

El Tribunal de Cuentas debía atender a las orientaciones estratégicas, nacionales y europeas y apostar de forma decidida por dirigir y reforzar aquellas acciones que vinieran a simplificar y modernizar su actividad.

24. Datos obtenidos en la página web de la Sede judicial Electrónica del Ministerio de Justicia, sede.mjusticia.gob.es

25. Tal y como dispuso el Informe de la Subdirección TIC, de 27 de mayo de 2015.

En atención a esta necesidad se creó, mediante Acuerdo del Pleno de 29 de octubre de 2012, la Unidad de Modernización Administrativa e Impulso de la Administración Electrónica, UMAIAE, con objeto de emprender la modernización de la institución mediante la implantación de las nuevas tecnologías. Ya en mayo de 2013, la Unidad elabora un Plan Director que tiene como objetivo el diseño de las líneas principales de evolución institucional que permitan alinear las nuevas tecnologías de la información y la comunicación a las estrategias de cambio proyectadas, afectando tanto a las estructuras como a las personas, buscando la mejora de procesos y la eficacia y eficiencia de los mismos.[26] Se pretendía dar un diagnóstico de las necesidades institucionales, organizativas, procedimentales y de sistemas con objeto de determinar los ejes básicos sobre los cuales vertebrar la modernización administrativa del Tribunal y el impulso en la digitalización de la institución.

El 29 de mayo 2014, el Pleno del Tribunal acordó la necesidad de establecer una estrategia común para los servicios informáticos, basados hasta entonces en pequeñas unidades TIC departamentales, por lo que el 24 octubre de 2014, se constituyó un Grupo de Trabajo de Informática integrado por el el Presidente del Tribunal, dos Consejeras y la Secretaria General, para la elaboración de una estrategia TIC. El 18 de noviembre 2014, el Grupo de Trabajo presentó una propuesta de unificación de los servicios mediante la creación de una Unidad TIC constituida por el personal informático del Tribunal. El 26 febrero 2015, el Pleno del Tribunal aprueba la propuesta y acuerda la creación de la Comisión de Estrategia TIC del Tribunal y de la Subdirección TIC (STIC).

La Comisión de Estrategia TIC (CETIC) es el Órgano Superior de Gobernanza TIC en el Tribunal de Cuentas. Está constituido por el Presidente del Tribunal, la Secretaria General, una Consejera de la Sección de Fiscalización y otra de la Sección de Enjuiciamiento en representación de los correspondientes Departamentos. Elabora, coordina y dirige la estrategia TIC del Tribunal, estableciendo directrices concretas de actuación que garanticen el alineamiento de los proyectos con los objetivos y prioridades del Tribunal. La Subdirección TIC (STIC) es la unidad encargada de poner en práctica la estrategia TIC conforme a las directrices que emanan de la Comisión de Estrategia. Está constituida por técnicos informáticos y depende orgánicamente de Secretaría General. Implementa, mantiene y administra la prestación de todos los servicios TIC del Tribunal conforme a acuerdos de nivel de servicio (ANS) comunes para todos los Departamentos.

El Plan Estratégico del Tribunal de Cuentas 2018-2021, aprobado por el Pleno el 25 de abril de 2018, incluye entre sus objetivos específicos:

- Modernizar los procedimientos internos e impulsar los proyectos de administración electrónica y la utilización de las TIC para reforzar la eficacia y eficiencia en el Tribunal de Cuentas.
- Elaborar un plan plurianual en el que se determinen las prioridades en el ámbito de las TIC y que comprenda una metodología de selección de proyectos a desarrollar y los procedimientos de gestión de los mismos.

26. En los términos indicados en el propio «Plan Director de Modernización del Tribunal de Cuentas».

- Potenciar el uso de herramientas tecnológicas y de procedimientos telemáticos en todos los ámbitos de actuación del Tribunal de Cuentas.
- Impulsar el desarrollo de una única aplicación informática en el Tribunal de Cuentas que permita un examen más dinámico, homogéneo y efectivo de la Cuenta General del Estado.
- Elaborar un programa de cumplimiento del Esquema Nacional de Seguridad y de la Ley Orgánica de Protección de Datos, en el que se definan las medidas a adoptar, los hitos y el calendario de su implantación.

2. Circunstancias concretas del Tribunal de Cuentas

En atención a las funciones constitucionalmente reconocidas —artículo 136 de la Constitución Española—[27], y a las disposiciones que conforman su régimen jurídico —Ley Orgánica 2/1982, de 12 de mayo, del Tribunal de Cuentas (LOTCU) y Ley 7/1988, de 5 de abril, de Funcionamiento del Tribunal de Cuentas (LFTCU)—, la digitalización del órgano debía suponer la implantación de mecanismos informáticos que permitieran la tramitación digital tanto de procedimientos fiscalizadores, para el control externo de la gestión económico financiera del Estado y del sector público; jurisdiccionales, para el enjuiciamiento de la responsabilidad contable en que incurran aquellos que tengan a su cargo el manejo de caudales o efectos públicos; y administrativos generales del órgano, en cuanto a los procesos de contratación o personal, entre otros.

Para ello, debía atenderse a los concretos trámites en que se materializa el ejercicio de la función fiscalizadora, en cuanto al examen y la comprobación de las cuentas del Estado y del sector público (y, actualmente, también de la contabilidad de los partidos políticos), el análisis de la actividad contractual y la elaboración de informes en que se plasmen los resultados obtenidos[28], así como los trámites en que se materializa el ejercicio de la función jurisdiccional en el enjuiciamiento de las responsabilidades contables[29], a través de los procedimientos de reintegro por alcance, juicio de cuentas y cancelación de fianzas.

27. Constitución Española, artículo 136:

1. El Tribunal de Cuentas es el supremo órgano fiscalizador de las cuentas y de la gestión económica de Estado, así como del sector público.
   Dependerá directamente de las Cortes Generales y ejercerá sus funciones por delegación de ellas en el examen y comprobación de la Cuenta General del Estado.
2. Las cuentas del Estado y del sector público estatal se rendirán al Tribunal de Cuentas y serán censuradas por éste.
   El Tribunal de Cuentas, sin perjuicio de su propia jurisdicción, remitirá a las Cortes Generales un informe anual en el que, cuando proceda, comunicará las infracciones o responsabilidades en que, a su juicio, se hubiere incurrido.
3. Los miembros del Tribunal de Cuentas gozarán de la misma independencia e inamovilidad y estarán sometidos a las mismas incompatibilidades que los Jueces.
4. Una ley orgánica regulará la composición, organización y funciones del Tribunal de Cuentas.

28. Conforme al artículo 2.a de la LOTCU «Son funciones propias del Tribunal de Cuentas: a) La fiscalización externa, permanente y consuntiva de la actividad económico-financiera del sector público».

29. Conforme al artículo 2.b de la LOTCU «Son funciones propias del Tribunal de Cuentas: b) El enjuiciamiento de la responsabilidad contable en que incurran quienes tengan a su cargo el manejo de caudales o efectos públicos.»

La digitalización debía realizarse también, atendiendo a las particularidades organizativas del órgano. Conforme al artículo 19 de la Ley Orgánica son órganos del Tribunal de Cuentas: a) El Presidente, b) El Pleno, c) La Comisión de Gobierno, d) La Sección de Fiscalización, e) La Sección de Enjuiciamiento, f) Los Consejeros de Cuentas, g) La Fiscalía y h) La Secretaría General del Tribunal de Cuentas. La Sección de Fiscalización, a su vez, se estructura en siete Departamentos de Fiscalización junto con una Unidad de Partidos Políticos y la Sección de Enjuiciamiento en tres Departamentos de Enjuiciamiento. La informatización debía atender a la compleja trama de relaciones entre ellos, con el consiguiente reto de interoperabilidad entre sistemas y programas.

Debía concebirse la informatización desde una perspectiva interna y externa. Efectivamente, la informatización debía atender a la creación de mecanismos de gestión electrónica que dinamizaran el funcionamiento del órgano desde su perspectiva exterior e interior.

En la perspectiva exterior, la incorporación de medios telemáticos debía responder a la necesidad de facilitar las distintas formas de comunicación con la gran variedad de agentes externos que se relacionan con el órgano en el ejercicio de las funciones que le competen, como entidades públicas de la más diversa naturaleza, OCEXs[30], gestores de fondos públicos, etc. y atender a la circunstancia de que, en el devenir de su funcionamiento, en el Tribunal se produce la recepción de un enorme volumen de documentación, tanto destinada a la Sección de Fiscalización, en el caso de la rendición de cuentas y contratos de las entidades públicas, como a la de Enjuiciamiento, en relación a lo que constituyen los «autos» de los expedientes de responsabilidad contable. Sin ignorar que la carga administrativa que supone a estas entidades tanto la rendición de cuentas, como la remisión de cuanta documentación les sea solicitada en el ejercicio de las funciones fiscalizadora y jurisdiccional, supone en sí mismo un coste que repercute negativamente en la calidad de los servicios prestados a la ciudadanía.

Desde la perspectiva interior, se debía atender al aspecto interno de la tramitación de los procedimientos en que se concreta la ejecución de las funciones del órgano, tanto fiscalizadora como jurisdiccional, así como en lo relativo a los procedimientos administrativos generales (de contratación, personal, etc.) para dinamizar el proceder de la institución, simplificando la actuación en que se concreta la gestión.

3. Proyecto de digitalización: perspectiva global y análisis de desarrollos informáticos concretos

Hasta la fecha, diversos desarrollos informáticos satisfacen las necesidades de digitalización del organismo.

La digitalización del Tribunal de Cuentas se ha llevado a cabo de manera progresiva, mediante la implantación de diversos desarrollos tecnológicos que habilitan la informatización de los diferentes aspectos de las actuaciones del órgano, tanto en lo concerniente al ejercicio de la función fiscalizadora como de la jurisdiccional o de enjuiciamiento. La interconexión de

30. Órganos de Control Externo.

todos los programas, sistemas y plataformas informáticas permitirá, una vez que se encuentren plenamente operativas, la realización digitalizada integral de las actuaciones en que se concreta la función del Tribunal de Cuentas.

3.1. Perspectiva global

Desde los comienzos, el proyecto de digitalización del Tribunal fue concebido como una solución integral que debía abarcar, en su conjunto, los distintos escenarios en que se concretaba la actuación de la Institución.

Por ello, las distintas plataformas, programas y sistemas informáticos desarrollados debían estar interconectados, integrándose en un todo para lograr una gestión electrónica completa de las actuaciones del Tribunal desde su comienzo hasta el final. Se trataba de crear una verdadera administración electrónica del órgano.

De una manera simplificada y con carácter genérico, el iter en que se concreta la actuación del Tribunal para el ejercicio de su función, comienza con la recepción de documentación (de la más diversa naturaleza y procedencia), continúa con la realización de los trámites en que se concreta la gestión interna de las actuaciones del órgano y finaliza con en el envío de la documentación, una vez gestionada, al archivo.

Efectivamente, las actuaciones del Tribunal comienzan con la solicitud de remisión o remisión de documentación al Tribunal, ya sean cuentas de los entes públicos o de los partidos políticos, documentación procedente de la actividad contractual de aquellos, documentación relativa a los procedimientos jurisdiccionales o relativos a personal, contratación del tribunal, relaciones internacionales, etcétera. Era por ello, imperativa la creación de una sede electrónica del Tribunal de Cuentas, o dirección web, a imagen y semejanza de las sedes electrónicas de la inmensa mayoría de los organismos públicos, que posibilitara la realización de los tramites con el órgano de manera telemática. La sede electrónica debía habilitar, asimismo, diversos canales a través de los cuales pudiera producirse la entrada digital, en el Tribunal, de la mencionada documentación. Se procedió, en atención a estas necesidades a la contratación externa para la creación de la Sede Electrónica del Tribunal de Cuentas. Conforme a las necesidades específicas de los distintos Departamentos, se fueron habilitando, asimismo, de forma progresiva, los canales mencionados[31]. Actualmente estos son:

- La *Plataforma de Rendición de Cuentas de las Entidades Locales,* a través de El Portal Rendición de Cuentas (iniciativa liderada por el Tribunal de Cuentas, con la participación de algunos OCEXs,) para el examen y comprobación de las cuentas de provincias, municipios, ayuntamientos y demás entidades locales, en cumplimiento de lo dispuesto en los artículos 212 y 223 del Real Decreto Legislativo 2/2004, de 5 de marzo, por el que se aprueba el texto refundido de la Ley Reguladora de las Haciendas Locales. Permite, también, la remisión de contratos de las mencionadas entidades.
- La *Plataforma de Remisión de Contratos,* que permite a las entidades del Sector Público Estatal y Autonómico remitir una relación de los contratos formalizados por ellas y sus

31. La entrada también podrá producirse en soporte papel a través del registro presencial, en que se procederá a su digitalización.

entidades dependientes, para cumplir con las exigencias previstas en los artículos 39 y 40 de la LFTCU y lo dispuesto en el Real Decreto Legislativo 3/2011, de 14 de noviembre, por el que se aprueba el texto refundido de la Ley de Contratos del Sector Público.

- La *Plataforma de Rendición de Cuentas de Partidos Políticos,* a través de la cual se remite la contabilidad anual de aquellos en atención al mandato contenido en la Ley Orgánica 8/2007, de 4 de julio, de financiación de partidos políticos, por el cual corresponde en exclusiva al Tribunal de Cuentas el control externo de la actividad económico-financiera de aquellos (la contabilidad procedente de procesos electorales se rendirá a través de la plataforma Hermes).
- La plataforma *Hermes, Comunicaciones y Notificaciones,* como vehículo electrónico concebido, entre otras utilidades, para la recepción segura de documentación de diversa naturaleza.
- El *Servicio Web,* como canal especialmente habilitado para la recepción de la documentación procedente de la IGAE, en la remisión de todas las cuentas procedentes de la Administración General del Estado (Cuenta General del Estado, Cuenta de la Administración General del Estado y de los sectores públicos fundacional y empresarial estatal) y de la IGSS, en cuanto a la remisión de la Cuenta General de la Seguridad Social, las cuentas de las entidades gestoras, de los servicios comunes y de las mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social.

La documentación en formato electrónico recibida a través de los canales mencionados, debía acceder al Tribunal a través de un registro electrónico que le diera entrada oficial en el órgano. Se creó, para satisfacer esta necesidad, el Registro Electrónico del Tribunal de Cuentas, objeto de reciente actualización mediante la implantación de una nueva aplicación de registro (*«Módulo de Registro»* integrado en la *Plataforma de Gestión Electrónica del Tribunal de Cuentas*). El Registro General asigna, así, a la documentación, un numero de entrada y la pone a disposición de las distintos Registros Internos a la que vaya dirigida a través de la función «Comunicaciones internas» de la aplicación.

Así, por medio de comunicación del Registro General con los Registros Internos, la documentación recibida se dirige a los distintos Departamentos o Unidades del Tribunal para la realización de los trámites que correspondan. Con carácter genérico, en el caso de cuentas, a los Departamentos de Fiscalización, en el caso de documentación de personal, a la Subdirección de Recursos Humanos para la realización de los trámites oportunos, o, en el caso de documentación relativa a procedimientos jurisdiccionales, a los Departamentos de Enjuiciamiento. Para la realización de los mencionados tramites de manera digital, era necesaria la implantación de un sistema de gestión electrónica interna del órgano. Se desarrolló para ello el módulo *«Brahma - Tramitación de Expedientes»* de la *Plataforma de Gestión Electrónica del Tribunal de Cuentas,* que comprende la posibilidad de tramitación electrónica de una gran variedad de procedimientos de entre la totalidad de los que se sustancian en el Tribunal (tramitación de Informes de Fiscalización, de contratos, el *«Gestor Procesal»* para los procedimientos jurisdiccionales, de personal, etc.)

El módulo *«Brahma - Tramitación de Expedientes»* de la Plataforma está, a su vez, conectado a diversos módulos, como *«Thot - Portafirmas Electrónico»,* para la firma digital de do-

cumentos, el módulo *«Ágora - Órganos Colegiados»,* para acceder a la documentación de las sesiones de aquellos y a la plataforma *Hermes, Comunicaciones y Notificaciones,* para la realización de comunicaciones y notificaciones electrónicas si ello fuere necesario.

Por último, una vez finalizada la tramitación, la documentación ya gestionada habría de enviarse al *Archivo Electrónico.*

Hasta aquí, un análisis global de lo que idealmente ha de constituir la gestión electrónica del Tribunal, sin perjuicio de que en la práctica, a día de hoy, aun se producen algunas disfuncionalidades derivadas de factores diversos, entre los que se encuentran la fase de implantación de algunas de las aplicaciones, que no se hayan plenamente operativas todavía (como en el caso del servicio de notificaciones de la plataforma *Hermes* o el *«Gestor Procesal»*), o la falta de interconexión entre sí de algunas de ellas (como en el caso de los módulos de *Archivo* y *Registro*).[32]

3.2. Desarrollos informáticos concretos

Realizaremos, a continuación, un examen detenido de algunas de las plataformas, programas y módulos implantados.[33]

— Registro Electrónico

Actualmente en el Tribunal de Cuentas se encuentran definidas tres oficinas de Registro General: una principal y dos auxiliares. Estas son, la Oficina Principal de Registro Presencial de la sede de la calle Fuencarral, la Oficina Auxiliar de Registro Presencial de la sede de la calle Padre Damián y la Oficina Auxiliar de Registro Electrónico. Las tres conforman el denominado Libro del Registro Oficial del Tribunal de Cuentas, habiéndose implantado, recientemente, una nueva aplicación de registro que afecta, tanto a los Registros Presenciales como al Registro Electrónico.

El Proyecto de una nueva aplicación de Registro fue aprobado por la Comisión de Estrategia TIC en sesión de 31 de enero de 2017, habiéndose producido su definitiva implantación el 17 de septiembre de 2018.

El módulo de la nueva aplicación de Registro (de Entrada y Salida) o *«Modulo de Registro»* se encuentra integrado en la *Plataforma de Gestión Electrónica del Tribunal de Cuentas* (AL SIGM) y está preparado para poder ser certificado en la normativa SICRES 3.0 (intercambio registral con el SIR).[34]

La nueva aplicación de Registro afecta tanto al Registro Presencial (de Fuencarral y de Padre Damián), como al Registro Electrónico, a través del que se recibe la documentación enviada telemáticamente al Tribunal de Cuentas. La documentación recibida del exterior a través de las oficinas presenciales del Tribunal de Cuentas será registrada de entrada en Registro

32. Información obtenida en las *Jornadas de Novedades Tecnológicas del Tribunal de Cuentas,* celebradas en la Sede del Tribunal de Cuentas de la calle Fuencarral el 18 de octubre de 2019.

33. Información obtenida del curso de formación TCu37/2019 *La administración electrónica en el Tribunal de Cuentas. Referencia especial al portafirmas electrónico del Tribunal de Cuentas,* celebrada en tres ediciones del 19 de noviembre del 2019 al 14 de enero del 2020.

34. Norma relativa al intercambio registral que garantiza la interoperabilidad entre registros una vez que se cumplan los requisitos del Esquema Nacional de Interoperabilidad (ENI) y del Esquema Nacional de Seguridad (ENS).

General y digitalizada, reflejándose el día, hora, minuto y segundo del registro. Esta digitalización se hará con OCR (reconocimiento de texto) lo que permitirá la realización posterior de búsquedas en el texto, y será estampada con el sello del Tribunal de Cuentas. La documentación digitalizada y estampada se anexará al asiento registral de entrada. Asimismo, Registro General remitirá la documentación original recibida en soporte papel al destinatario de la misma.

Registro General pondrá la documentación digitalizada a disposición de la oficina de Registro interno a la que fuera dirigida a través de la función «Comunicaciones internas» de la aplicación. Conforme a esta funcionalidad, Registro General seleccionará un registro de entrada y lo «comunicará» a una o varias oficinas internas. Estas oficinas o Registros Internos se asimilan a los distintos subregistros que se venían llevando en los Departamentos y Unidades del Tribunal de Cuentas.

Los usuarios a los que se les haya dado permiso, visualizarán en la aplicación de Registro Interno un aviso cuando se les haya distribuido documentación desde Registro General o desde cualquier otro Registro Interno (otro Departamento, Fiscalía, Presidencia, etc.).

Actualmente existen creadas más de 78 oficinas internas de Registro y se encuentran dados de alta más de 209 usuarios.

— **Módulo *«Brahma - Tramitación de expedientes»***

El módulo *«Brahma - Tramitación de expedientes»* responde a la necesidad de dotar al Tribunal de un sistema específico de gestión electrónica de procedimientos de toda índole sustanciados en el órgano. Se encuentra, asimismo, integrado en la *Plataforma de Gestión Electrónica del Tribunal*. Incluye procedimientos de Gerencia, de recursos humanos, de contratación, de celebración de sesiones del Pleno, de la Comisión de Gobierno, de la Sección de Fiscalización y de la Sección de Enjuiciamiento, procedimientos de tramitación y ejecución del programa Anual de Fiscalizaciones y procedimiento de reintegro por alcance (siendo éste el *«Gestor Procesal»,* para la tramitación de procedimientos jurisdiccionales del órgano, al que nos referiremos posteriormente).

Se encuentra interconectado, a través de la *Plataforma de Gestión Electrónica,* con el *«Módulo de Registro»,* desde el cual se remite la documentación en formato digital. Interopera, asimismo, con el módulo *«Thot - Portafirmas electrónico»* para la firma digital de la documentación tramitada, con el módulo *«Ágora - Órganos Colegiados»* y con la plataforma Hermes para la realización de comunicaciones y notificaciones. Está prevista, asimismo, su conexión en un corto horizonte temporal, al módulo de archivo.

— **Módulo *«Ágora - Órganos colegiados»***

El módulo denominado *«Ágora - Órganos Colegiados»,* empleado por vez primera en la Sesión de Comisión de Gobierno 12/2015, de 16 de abril de 2015, permite el acceso al contenido de las sesiones de Pleno, Comisión de Gobierno, Sección de Fiscalización y Sección de Enjuiciamiento, por parte de sus miembros, así como de Directores Técnicos y otro personal a su cargo a los que se haya autorizado el acceso.

La documentación, en formato electrónico, constitutiva de cada uno de los puntos que conforman el orden del día de cada sesión de Pleno, Comisión de Gobierno, Sección de Fiscalización y Sección de Enjuiciamiento, se encuentra a disposición de sus miembros, facilitando

su consulta y descarga en cualquier momento y en cualquier lugar, como herramienta de trabajo y de apoyo para la celebración de la sesión.

El sistema cuenta con un módulo de administración de usuarios, habilitando el acceso a la documentación de las sesiones de los Órganos Colegiados únicamente a las personas autorizadas para ello con el consiguiente permiso.

El módulo *«Ágora - Órganos Colegiados»* es una aplicación de consulta de documentación que no implica de por sí ningún tipo de tramitación electrónica. Ahora bien, la documentación que se muestra en este módulo tiene su origen en los distintos procedimientos internos y son estos los que sí se podrían gestionar de forma electrónica a través de la Plataforma de Gestión Electrónica del Tribunal de Cuentas.

El sistema cuenta con diversos mecanismos que garantizan la seguridad de la información, como la necesidad de acceder al módulo mediante certificado electrónico, la identificación del dispositivo desde el que se accede o el cifrado de las conexiones para salvaguardar la transmisión.

Actualmente, la totalidad de las sesiones del Pleno, de la Sección de Fiscalización y de la Sección de Enjuiciamiento, son convocadas y publicadas electrónicamente mediante esta aplicación.

— **Módulo *«Thot - Portafirmas Electrónico»***
Mediante el módulo *«Thot - Portafirmas Electrónico»,* los usuarios designados, normalmente los miembros del Pleno, podrán «Firmar y enviar», los expedientes gestionados a través de la Plataforma de Gestión Electrónica.

Así, el usuario con permisos suficientes, enviará desde el procedimiento correspondiente un expediente entero o un documento a la firma. Este envío generará un correo electrónico de aviso al destinatario, que accederá al *«Portafirmas»* a través de una página simplificada en la que a su vez se le ofrece la posibilidad de «Consultar firmas pendientes» (en que podrá, respecto de un documento o expediente, firmarlo y enviarlo a un destinatario posterior, únicamente firmarlo o rechazarlo), la posibilidad de «Consultar histórico de firmas» (en que podrá analizar los documentos firmados y los devueltos sin firmar) y por último la posibilidad de «Delegar la firma» (para delegar a un usuario determinado la posibilidad de firmar o de revocar la delegación anterior).

— **Plataforma *Hermes, comunicaciones y notificaciones electrónicas***
En lo relativo a las comunicaciones, *Hermes* se configura como una herramienta para la creación de tramites electrónicos (parametrizador de trámites y formularios) que posibiliten la recepción de información del exterior de forma personalizada y adaptada a las necesidades del usuario interno demandante de la misma.

La herramienta, (antiguo «Tramitador» de la Sede Electrónica, puesta en producción en mayo de 2014 y desarrollada a partir de la plataforma SISTRA con medios propios del Tribunal) permite la creación de formularios electrónicos en los que el usuario exterior, a través de una navegación sencilla y guiada, va cumplimentando los distintos datos que le son solicitados y adjuntando los documentos electrónicos que se determinen por el Tribunal de

Cuentas, permitiendo la remisión de la documentación de forma segura al ser necesario para el envío, entre otras medidas, certificado electrónico reconocido y quedando registradas todas las entradas en el registro electrónico del Tribunal de Cuentas.

En lo relativo a las notificaciones, se está implementando un servicio de notificaciones mediante comparecencia en la Sede Electrónica del Tribunal de Cuentas mediante la herramienta «Notific@» (servicio de notificaciones electrónicas desarrollado por el Ministerio de Hacienda y Función Pública) conforme a lo establecido en el artículo 43 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

— ***«Módulo de Archivo»***

El 1 de octubre de 2017 se adjudicó el contrato para la implantación de un nuevo *«Módulo de Archivo»* en el Tribunal de Cuentas, que ya se encuentra operativo, con la finalidad de culminar el ciclo completo de la vida administrativa de un expediente, tanto en soporte papel como electrónico, desde su creación y tramitación en las diferentes unidades y departamentos del órgano, hasta su archivo para su custodia y conservación o, en caso de considerarse conveniente, para su eliminación. La nueva herramienta permite gestionar sistemas de archivo, describir la documentación conforme a los estándares internacionales de descripción archivística de fondos y de instituciones (normas ISAD-G e ISAAR-CPF) y transferir documentación entre la unidad de archivo y el resto de departamentos y unidades del Tribunal, tanto en soporte papel, como en soporte electrónico.

Los módulos *«Ágora - Órganos colegiados», «Brahma - Tramitación de expedientes», «Módulo de Registro», «Archivo»* y *«Thot - Portafirmas Electrónico»* se encuentran integrados en la *Plataforma de Gestion Electrónica del Tribunal de Cuentas,* herramienta base para la digitalización del organismo mediante la adaptación de la tecnología AL-SIGM en su versión 3.0.1, desarrollada por el Ministerio de Industria, Energía y Turismo (MINETUR), al entorno del Tribunal.[35]

Digitalización de la jurisdicción contable

1. Proyecto de digitalización de la Sección de Enjuiciamiento

Las particularidades del ejercicio de la función jurisdiccional de enjuiciamiento contable del Tribunal de Cuentas exigían un proceso de digitalización adaptado.

Era necesario contar con desarrollos informáticos que satisficieran las necesidades propias de los procedimientos de enjuiciamiento de la responsabilidad contable, —reintegro por alcance, juicio de cuentas y expedientes de cancelación de fianzas— y que atendieran al estricto cumplimiento de la normativa procesal, para garantizar el uso de la informática al servicio de la legalidad.

35. Mediante Acuerdo de la Comisión de Gobierno, en sesión de 20 de marzo de 2014,se aprobó la implantación en el Tribunal de Cuentas de un Sistema Integral de Gestión electrónica de expedientes y la realización de un Proyecto Piloto del sistema AL SIGM que dio lugar a la Plataforma de Gestion Electrónica del Tribunal de Cuentas.

En atención a esta necesidad se procedió a la creación del «Grupo de Trabajo para la Informatización de los Procedimientos de Responsabilidad Contable», integrado por personal del Tribunal, cuya primera reunión se celebró el 21 de enero de 2013, con el objeto de elaborar las estrategias adecuadas de incorporación de las tecnologías de la información a los procedimientos sustanciados en la Sección.

Desde un primer momento se puso de manifiesto la conveniencia de llevar a cabo las actuaciones que fueran necesarias para la obtención de información funcional y técnica, así como la concertación de las visitas oportunas, en relación a la implantación de *LexNet,* como herramienta de notificación, y de una aplicación de gestión procesal que soportara la tramitación electrónica de los procedimientos jurisdiccionales del Tribunal de Cuentas. Durante los meses siguientes se mantuvieron[36] sucesivos contactos con diversos técnicos del Ministerio de Justicia, de la Generalitat de Cataluña y del Gobierno de Canarias, así como con técnicos de varias empresas privadas, para la evaluación de los sistemas de gestión procesal *Minerva-Noj, E-Justicia.cat* y *Atlante II* que se encontraban implantados, respectivamente, en el ámbito del Ministerio de Justicia, en la comunidad autónoma catalana y de la canaria. Tras analizar las ventajas, facilidades de implantación e inconvenientes de unos y otros, se concluyó que la aplicación del sistema *Minerva-Noj* (aplicación de gestión procesal desarrollada por el Ministerio de Justicia), reunía las características exigidas para la tramitación de los procedimientos contables, recomendándose su implantación en la Sección de Enjuiciamiento del Tribunal de Cuentas. Se mantuvieron, asimismo, contactos con personal responsable del Ministerio de Justicia en cuanto a la posibilidad de implantación del sistema *LexNet,* convenientemente adaptado, a la Sección de Enjuiciamiento para la realización de notificaciones electrónicas en el seno de los procedimientos jurisdiccionales de responsabilidad contable.

El Grupo de Trabajo elaboró, fruto de los estudios anteriores, dos informes. Un primer «Informe organizativo, funcional y procedimental de la Sección de Enjuiciamiento del Tribunal de Cuentas», con objeto de compendiar las características de la Jurisdicción Contable a efectos de la posible adaptación de un sistema importado de gestión procesal; y un segundo informe relativo a los «Esquemas de tramitación procedimental (aplicación Minerva)», en cuanto a la conveniencia de la implantación del sistema *Minerva-Noj* en la Sección de Enjuiciamiento.

Finalmente, sin embargo, las negociaciones con el Ministerio de Justica resultaron infructuosas, tanto en lo relativo a la incorporación del sistema *LexNet* como en lo concerniente a la adaptación del sistema *Minerva-Noj,* de gestión procesal, a las necesidades procedimentales de la Sección de Enjuiciamiento, momento en que se concluyó sobre la conveniencia de acometer, por el propio Tribunal, un proyecto de configuración de un gestor o tramitador procesal propio. Nace así el «Proyecto AL-SIGM Enjuiciamiento»[37] para crear, por medio de la herramienta AL-SIGM ya implantada en el Tribunal (*Plataforma de Gestion Electrónica del Tribunal de Cuentas,* integrándose en el módulo «*Brahma - Tramitación de*

36. Las primeras reuniones se celebraron en febrero del año 2013.

37. Cuya dirección fue asumida por personal perteneciente al Departamento Primero de la Sección de Enjuiciamiento.

Expedientes»), un mecanismo de gestión o tramitación procesal electrónica, —*«Gestor Procesal»*—, que satisficiera las necesidades específicas de sustanciación de los procedimientos jurisdiccionales contables.

Para la creación del gestor procesal se acordó la contratación de órganos externos que trabajaran en colaboración con personal informático cualificado del propio Tribunal.

El adjudicatario debía realizar el trabajo de forma presencial en la Sede del Tribunal de Cuentas de la calle Fuencarral y en colaboración directa con el personal técnico de la Subdirección de Tecnologías de la Información y las Comunicaciones.

Las tareas de análisis y programación debían incluir la participación directa de este personal a fin de asegurar el conocimiento en profundidad de los módulos desarrollados para que el Tribunal de Cuentas pudiera hacerse cargo de su mantenimiento posterior.

Se procedió así, a la celebración de un primer contrato para el desarrollo del gestor en los procedimientos de Secretaria de Gobierno, de diligencias preliminares en los Departamentos de instancia y en actuaciones previas y desde entonces se han ido concatenando contratos sucesivos para la ampliación de funcionalidades del aquel.

Recientemente, la Comisión de Gobierno, en reunión de 5 de diciembre de 2019, acordó otorgar la autorización para la contratación de nuevas funcionalidades en la *Plataforma de Gestión Electrónica del Tribunal de Cuentas* para la Sección de Enjuiciamiento, en la que está prevista la implementación del desarrollo del *«Gestor Procesal»* al procedimiento de reintegro por alcance.

2. Características organizativas y procedimentales de la Sección de Enjuiciamiento a efectos de la digitalización

El gestor procesal, para la tramitación electrónica de los procedimientos de responsabilidad contable, debía atender a las especialidades de organización de la Sección de Enjuiciamiento, a los esquemas procedimentales básicos y a los trámites o actuaciones concretas realizadas por cada órgano o unidad.

En particular, la Sección de Enjuiciamiento está integrada por el Presidente de la Sección de Enjuiciamiento y los Consejeros de Cuentas[38], a quienes, como órganos de primera instancia o adscritos a la Sala o Salas del Tribunal, corresponde conocer de los procedimientos jurisdiccionales.[39] Actualmente se estructura en: Presidencia de la Sección de Enjuiciamiento y Tres Departamentos de Instancia.

Además de las funciones jurisdiccionales, corresponde a la Sección de Enjuiciamiento, entre otras actuaciones, preparar la Memoria de las Actuaciones Jurisdiccionales del Tribunal

38. Artículo 24 de la Ley Orgánica 2/1982, de 12 de mayo, del Tribunal de Cuentas.

39. Artículo 25 Ley Orgánica 2/1982, de 12 de mayo, del Tribunal de Cuentas.

y sentar los criterios con arreglo a los cuales deba efectuarse el reparto de asuntos entre las Salas y entre los Consejeros de la Sección de Enjuiciamiento.

La jurisdicción contable se ejercerá por los siguientes órganos:

- **Los Consejeros de Cuentas:** Adscritos cada uno a un Departamento de la Sección de Enjuiciamiento, siendo actualmente tres.

  Cada Consejero está al frente de un Departamento, como órganos de primera o única instancia, asistidos de un Secretario (Director Técnico) cada uno, y con el personal que demanden las necesidades del servicio. En los citados Departamentos se lleva a cabo la tramitación y, en su caso, resolución de los siguientes asuntos:

  – Las diligencias preliminares.[40]
  – Las acciones públicas.[41]
  – Los procedimientos de reintegro por alcance (en primera instancia).[42]
  – Los juicios de las cuentas (en primera instancia).[43]
  – Los expedientes de cancelación de fianzas.[44]
  – Tramitación del recurso de apelación (hasta su remisión a la Sala de Justicia).[45]
  – De los recursos contra las resoluciones dictadas en la tramitación de estos procedimientos.[46]
  – También conocen de los incidentes de recusación promovidos contra los Secretarios y resto de los funcionarios que intervengan en los procedimientos jurisdiccionales de su competencia, por las causas y trámites establecidos en las Leyes Orgánica del Poder Judicial y de Enjuiciamiento Civil.[47]

- **Las Salas del Tribunal de Cuentas** (Formadas por tres Consejeros. Actualmente solo existe una Sala):

  La Sala está integrada por el Presidente de la Sección y dos Consejeros de Cuentas, con la asistencia de un Secretario y con el personal que demanden las necesidades del servicio.

  La Sala conocerá:

  – De las apelaciones contra las resoluciones que ponen fin a la primera instancia dictadas por los Consejeros de Cuentas en los procedimientos de reintegro por alcance, juicios de cuentas, en los expedientes de cancelación de fianzas.[48]

40. Artículo 46 Ley 7/1988, de 5 de abril, de Funcionamiento del Tribunal de Cuentas.
41. Artículo 56 Ley 7/1988, de 5 de abril, de Funcionamiento del Tribunal de Cuentas.
42. Artículo 72 y ss. de la Ley 7/1988, de 5 de abril, de Funcionamiento del Tribunal de Cuentas.
43. Artículo 68 y ss. de la Ley 7/1988, de 5 de abril, de Funcionamiento del Tribunal de Cuentas.
44. Artículo 75 y ss. de la Ley 7/1988, de 5 de abril, de Funcionamiento del Tribunal de Cuentas.
45. Artículo 80.2 Ley 7/1988, de 5 de abril, de Funcionamiento del Tribunal de Cuentas.
46. Artículo 80.1 Ley 7/1988, de 5 de abril, de Funcionamiento del Tribunal de Cuentas.
47. Artículo 53.2 Ley 7/1988, de 5 de abril, de Funcionamiento del Tribunal de Cuentas.
48. Artículo 80.2 Ley 7/1988, de 5 de abril, de Funcionamiento del Tribunal de Cuentas.

- En única instancia, de los recursos que se formulen contra resoluciones dictadas por las Administraciones Públicas en materia de responsabilidades contables en los casos previstos por las leyes.[49]
- De los recursos formulados en las actuaciones previas a la exigencia de responsabilidades contables en vía jurisdiccional y contra las resoluciones que inadmitan las acciones públicas y las diligencias preliminares.[50]
- De los recursos de queja por inadmisión de la apelación acordada por los Consejeros de Cuentas en asuntos propios de su competencia jurisdiccional.[51]
- De los recursos de reposición contra resoluciones de trámite de la propia Sala.[52]
- De la preparación de los recursos de casación.[53]
- De los incidentes de recusación promovidos contra los Consejeros de Cuentas, Secretarios y restantes funcionarios que intervengan en los procedimientos jurisdiccionales de su competencia, por las causas y trámites establecidos en las Leyes Orgánica del Poder Judicial y de Enjuiciamiento Civil, sin perjuicio de lo que dispone el artículo 3.m), de la LFTC (Pleno si afecta a la mayoría).[54]

Los órganos del Tribunal de Cuentas que fueren competentes para conocer de un asunto lo serán también para todas sus incidencias y para ejecutar las resoluciones que dictaren. Asimismo, las resoluciones del Tribunal de Cuentas, son susceptibles del recurso de casación y revisión ante el Tribunal Supremo.

Para el ejercicio de las funciones jurisdiccionales del Tribunal de Cuentas, en cuanto no esté previsto en la Ley Orgánica del Tribunal de Cuentas o en la Ley de Funcionamiento del Tribunal de Cuentas, se aplicarán supletoriamente la Ley reguladora de la Jurisdicción Contencioso-Administrativa y las de Enjuiciamiento Civil y Criminal, por dicho orden.[55]

En la Sección de Enjuiciamiento, orgánicamente integradas en Presidencia de la Sección, se encuentran además:

- La Secretaria de Gobierno: Encargada, entre otras funciones, del turno de reparto de los asuntos, de la elaboración de los Libros de actas, así como de la elaboración de las propuestas de avocación y de los nombramientos de Delgados Instructores.
- Unidad de Actuaciones Previas: Encargada, entre otras funciones, de la tramitación de las Actuaciones Previas a la exigencia de responsabilidades contables en los procedimientos de reintegro por alcance por parte de los Delegados Instructores.[56]

49. Artículo 41.2 de la Ley Orgánica 2/1982, de 12 de mayo, del Tribunal de Cuentas.
50. Artículo 48.1 de la Ley 7/1988, de 5 de abril, de Funcionamiento del Tribunal de Cuentas.
51. Artículo 85.2 Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa.
52. Artículo 79 Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa.
53. Artículo 89 de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa.
54. Artículo 53.2 Ley 7/1988, de 5 de abril, de Funcionamiento del Tribunal de Cuentas.
55. Disposición Final Segunda de la Ley Orgánica 2/1982, de 12 de mayo, del Tribunal de Cuentas.
56. Artículo 47 de la Ley 7/1988, de 5 de abril, de Funcionamiento del Tribunal de Cuentas.

3. La herramienta de tramitación procesal o *«Gestor Procesal»*

Pues bien, la principal dificultad con que se ha encontrado la configuración del *«Gestor Procesal»* se deriva de la propia complejidad estructural e incluso logística de los procedimientos tramitados en la Sección de Enjuiciamiento, en que un mismo expediente ha de desplazarse por las distintas unidades de aquella para la ejecución de los diferentes trámites. En el caso del procedimiento de reintegro por alcance, el expediente parte de Secretaría de Gobierno, en que se turnan los asuntos, pasa por los Departamentos de instancia para la tramitación de diligencias preliminares o acción pública, vuelve a Secretaría de Gobierno para ser turnado al Delegado Instructor, se traslada a la Unidad de Actuaciones Previas para su práctica, vuelve al Departamento de instancia, para la tramitación del procedimiento de reintegro por alcance y finalmente, en su caso, se deriva a la Sala de Justicia para la sustanciación del recurso de apelación en segunda instancia. A ello se une la sustanciación de posibles recursos de los artículos 48.1 y 46.2 de la Ley de Funcionamiento del Tribunal de Cuentas y el recurso del artículo 41.2 de la ley Orgánica, con los correspondientes desplazamientos del expediente. El principal reto lo constituyó la posibilidad de interconexión entre todas las unidades y departamentos, respetando las restricciones de acceso a la información por unas y por otras en las distintas fases del procedimiento pues, por poner un por ejemplo, un mismo expediente no ha de estar visible para el departamento de instancia cuando se están sustanciado las actuaciones previas, o en el transcurso de la sustanciación de un recurso en la Sala de Justicia, el expediente no ha de estar visible o accesible en Secretaría de Gobierno.

Por ello el *gestor* o tramitador procesal se ha concebido de una forma más amplia que una mera unidad para generar documentos electrónicos y crear un expediente digital. Se concibe en una triple dimensión: en primer lugar como una plataforma de trabajo, en segundo lugar, como un gestor documental y en tercer lugar, como un tramitador de expedientes.[57]

Se entiende como una plataforma de trabajo en el sentido de constituir un punto común de conexión a todas las unidades de la Sección de Enjuiciamiento, hasta la fecha compartimentos estancos, permitiendo la interconexión de todas ellas en los términos antes mencionados. Dicha conexión permite la puesta a disposición de toda la Sección, de una misma información relativa al expediente, que una vez incorporada ya consta en el mismo y no ha de ser completada de nuevo por las distintas unidades en la sustanciación de los distintos trámites, evitando duplicidades en la realización del trabajo.

Un gestor documental, pues el expediente está formado por documentos que se van incorporando sucesivamente en el transcurso de los distintos trámites. Se pretende que la mayor parte de los documentos de tramitación —véase, diligencias de ordenación, providencias— se generen desde la propia aplicación de forma automática mediante la formulación de plantillas.

En tercer lugar, es un tramitador de expedientes, pues permite el desarrollo del proceso en sus diferentes trámites mediante la movilidad del mismo.

57. Información obtenida de las «Jornadas sobre novedades tecnológicas del Tribunal de Cuentas» celebrada en fecha 18 de octubre de 2019.

3.1. Aplicación práctica

El modulo que contiene el *«Gestor Procesal»* presenta unas primeras pestañas comunes para las distintas unidades de la Sección y pantallas propias según el departamento o la unidad a la que pertenezca el usuario. Para un usuario perteneciente en la Secretaría de Gobierno, la plataforma le permitirá el acceso a los trámites que han de sustanciarse en ésta, para un usuario perteneciente a la Unidad de Actuaciones Previas, únicamente el acceso a las mencionadas actuaciones y así respecto al personal perteneciente a cada departamento o unidad.

La aplicación habilita diferente posibilidades de perfil de usuario, entre los que se encuentran el de Secretaria de Gobierno y los de receptor de la documentación, de tramitador y de notificador, aplicables a las distintas unidades y departamentos.

Actualmente la aplicación del *«Gestor Procesal»* se encuentra en fase de pruebas en el entorno de Secretaria de Gobierno, en los Departamentos de instancia para la tramitación de diligencias previas y acción pública y en la Unidad de Actuaciones Previas.

Como adelantábamos, se encuentra autorizada la contratación de los desarrollos necesarios para la ampliación de funcionalidades del gestor en lo concerniente a los trámites propios del procedimiento de reintegro por alcance. Resulta deseable que en un futuro no muy lejano, se proceda a la contratación oportuna que permita la implantación del gestor en la Sala de Justicia.[58]

3.2. Interoperabilidad del *«Gestor Procesal»* con otras aplicaciones o módulos

Para la completa digitalización del sistema, el *«Gestor Procesal»* por sí solo, —si bien constituye un determinante motor de impulso para la simplificación y agilización de los procedimientos—, no es suficiente, sino que ha de estar conectado y ser operable con el restante conjunto de aplicaciones informáticas del Tribunal que digitalizan las funciones que pueden tener conexión con los procedimientos de enjuiciamiento, como el *«Módulo de Registro»,* el módulo *«Thot - Portafirmas Electrónico»,* la plataforma *Hermes,* comunicaciones y notificaciones y el *«Módulo de Archivo»*.

Actualmente el *gestor* se encuentra interconectado con los módulos de *registro* y de *portafirmas electrónico.*

El *«Módulo de Registro»* permitirá la digitalización de la entrada y salida de los documentos con destino y origen en la Sección de Enjuiciamiento para los procedimientos jurisdiccionales, en el momento en que el gestor procesal se encuentre plenamente operativo.

La Comisión de Gobierno ha aprobado, hasta la fecha, la creación de diversas oficinas de registros internos para la Sección de Enjuiciamiento entre las que se encuentran las de Presidencia de la Sección de Enjuiciamiento, de la Dirección Técnica de la Presidencia de la Sección de Enjuiciamiento, de Secretaria de Gobierno, de la Sala de Justicia, de la Unidad de Actuaciones Previas, del Departamento Primero de la Sección de Enjuiciamiento, de la Dirección Técnica del Departamento Primero de la Sección de Enjuiciamiento, del Departamento

58. Información obtenida en el curso de formación TCu05/2019 *Tramitación electrónica de los procedimientos de los Departamentos de Instancia de la Sección de Enjuiciamiento del Tribunal de Cuentas,* celebrado en tres ediciones (del 8 al 10 de octubre, del 23 al 25 de octubre y del 19 al 21 de noviembre de 2019).

Segundo de la Sección de Enjuiciamiento, de la Dirección Técnica del Departamento Segundo de la Sección de Enjuiciamiento, del Departamento Tercero de la Sección de Enjuiciamiento y la de la Dirección Técnica del Departamento Tercero de la Sección de Enjuiciamiento.

El módulo *«Thot - Portafirmas Electrónico»,* interconectado asimismo al gestor, permitirá la firma electrónica de documentos procesales de toda índole una vez que este último se encuentre plenamente operativo.

Mediante el *Portafirmas Electrónico* los usuarios designados (Consejeros, Letrados, Secretarios o miembros de la Comisión de Gobierno, entre otros) podrán firmar electrónicamente desde un ordenador o un dispositivo móvil, los expedientes tramitados a través del gestor procesal, cuando se encuentre operativo. Así, el usuario con el permiso adecuado, enviará desde el procedimiento correspondiente un expediente entero o un documento a la firma. Este envío generará un correo electrónico de aviso al destinatario, que podrá acceder al *Portafirmas*.

El *Portafirmas* pone a disposición del «firmante» distintas posibilidades. La posibilidad de «Consultar firmas pendientes», en cuyo caso podrá, respecto a un documento o expediente concreto, firmar y enviar al siguiente destinatario, devolver el documento sin firmar o únicamente firmar sin enviarlo a un destinatario posterior. El *Portafirmas* habilita, asimismo, al «firmante» la posibilidad de consultar el histórico de firmas (con los documentos firmados y enviados o los documentos devueltos sin firmar) y proceder a la delegación de firma si lo estimara procedente, respecto a un usuario determinado con la opción de revocación de la delegación anterior.

4. Otras cuestiones

Recientemente[59] se ha procedido a la mejora y desarrollo de nuevas funcionalidades del buscador de documentación del Sitio Web del Tribunal de Cuentas las cuales han incidido de forma significativa en la función de enjuiciamiento. En particular, en cuanto a la publicación de Sentencias y Autos y a la navegación entre Informes y Sentencias.

En cuanto a la publicación de Sentencias y Autos, el nuevo desarrollo permite que se almacenen las Sentencias y Autos en formato PDF (hasta la fecha se almacenaban en formato HTML). En cuanto a las Sentencias y Autos históricos, se habilitará un proceso automático que convierta los ficheros HTML a PDF.

En cuanto a la navegación entre Informes y Sentencias, teniendo en cuenta que algunos de los Informes de Fiscalización que realiza el Tribunal de Cuentas pueden acabar dando lugar a un procedimiento judicial, que finalmente puede terminar en una Sentencia, se ha habilitado la posibilidad de crear una referencia en el Informe de los Autos o Sentencias a los que hubiera dado lugar.

Se ha procedido también, a la eliminación de la función de buscador por «voces» en que las búsquedas realizadas daban lugar, en muchas ocasiones, a resultados inexactos *o incorrectos*.

59. El contrato se adjudicó el 1 de octubre de 2017.

5. Bibliografía

ARAGUÀS GALCERÀ, Irene. «La Administración electrónica en España: de la "administración en papel" a la "e-administración"» *Revista chilena de derecho y ciencia política,* agosto-diciembre. Vol. 3 N.º 2. Págs. 109-139. 2012. *{https://dialnet.unirioja.es/descarga/articulo/4095025.pdf}*

BOCANEGRA REQUENA, José Manuel y BOCANEGRA GIL, Borja. *La Administración Electrónica en España. Implantación y régimen jurídico.* Atelier. Barcelona, Barcelona, 2011.

CORTÉS ABAD, Oscar. «Las redes sociales en la Administración General del Estado. Factores jurídicos e institucionales.» Tesis doctoral UDC / 2019 {https://ruc.udc.es/dspace/bitstream/handle/2183/24407/CortesAbad_Oscar_TD_2019.pdf}

CORTÉS ABAD, Oscar. «Reflexiones sobre administración pública inteligente.» i-public@. (2007). {http://i-publica.blogspot.com/}

GÓMEZ PUENTE, Marcos. *La Administración electrónica. El procedimiento administrativo digital.* Editorial Aranzadi. Pamplona. 2019.

LOMBARDÍA VILLALBA, Ana. «Nuevas tecnologías y Administración de Justicia.» *Actualidad Jurídica Uría Menéndez* / 30-2011. 2011 *{https://www.uria.com/documentos/publicaciones/3224/documento/art06.pdf}*

TRIBUNAL DE CUENTAS. Plan estratégico 2018-2021 Objetivos estratégicos, objetivos específicos y medidas *{https://www.tcu.es/tribunal-de-cuentas/export/sites/default/.content/pdf}*

Blockchain: instrumento de transparencia y control del sector público

JOSÉ LUIS WANDEN-BERGHE LOZANO y **ELISEO FERNÁNDEZ DAZA**
Profesores de Economía Financiera y Contabilidad de la Universidad de Alicante

RESUMEN

Blockchain es una herramienta para satisfacer la demanda social de transparencia y la mejora del control interno y externo del sector público. Promete ser un avance decidido para que los ciudadanos recuperen la confianza en las instituciones y ayudar al sostenimiento del sistema por una mayor eficiencia en el empleo de los recursos públicos. La revisión de aplicaciones que se están experimentando en todo el mundo, auguran un futuro ilusionante, aun teniendo que superar dificultades en distintos órdenes, como necesidades regulatorias o de carácter técnico.
Es una tecnología de bases de datos distribuidas en donde la información se mantiene inmutable, verificable, consensuada y sin requerir de la existencia de un ente centralizador que intermedie para dar confianza. Es el propio sistema el que genera confianza, con la facultad de incluir smart contracts, a través de los cuales se automatizan procesos, con su consiguiente reducción de tiempos y costes. La función contable y auditora se vería beneficiada por una tercera entrada constituida por los registros en blockchain, dispuestos a mitigar la crisis de confianza que han propiciado algunos escándalos financieros y, a su vez, a automatizar procesos redundantes, redirigiendo los recursos liberados hacia tareas de mas amplios análisis y controles. La extensión de las plataformas y la interoperatividad de las aplicaciones blockchain pueden llevar a un ecosistema que haga real el anhelo de acercarse hacia la auditoría continua y que el sector público gane en transparencia y eficiencia, para una mayor calidad de los servicios públicos.

PALABRAS CLAVE

contabilidad | blockchain | auditoría | sector público | transparencia

ABSTRACT

Blockchain is a tool for meeting the social demand for transparency and the improvement of internal and external control of the public sector.
It promises to be a determined step forward for citizens to regain confidence in institutions and help sustain the system by means of a greater efficiency in the use of public resources.
The revision of applications that are being experienced around the world, envisages an exciting future, even though some different problems, such as regulatory or technical requirements must be overcome. It is a distributed database technology where information remains immutable, verifiable, in consensus, and not requiring a centralized agency in-between, thus creating trust. This trust is produced by the system itself, with the ability include smart contracts which automatize processes, therefore offering reduction in time and costs.
The accounting and auditory function would take advantage of a third entry consisting of Blockchain records, ready to mitigate the crisis of trust that have led to some financial scandals and, in turn, to automate redundant processes, readdressing the released resources to more extensive analysis and control tasks.
The extension of platforms and the interaction of Blockchain applications can lead to a system that makes a real-world yearning to move towards continuous auditing and for the public sector to gain in transparency and efficiency, for higher quality public services.

KEYWORDS

accounting | *blockchain* | *auditing* | *public sector* | *transparency*

1. Introducción

Desde distintos órdenes se señala que la sostenibilidad económica, financiera, social y medioambiental de nuestros gobiernos y sociedades requiere la aplicación de los principios del buen gobierno, y en especial la transparencia y el control de las organizaciones públicas y los gobiernos. La transparencia implica la rendición de cuentas y esta ha de suponer la divulgación de la información, que precisa el control para garantizar la fiabilidad y razonabilidad de las informaciones y la calidad de la gestión desarrollada, haciendo más eficiente el sistema (Montesinos, 2016). Para el logro de tales propósitos se propone en este trabajo la tecnología blockchain como un instrumento tendente a dar transparencia en la información, así como representar una poderosa herramienta de control. Nadie ignora que las nuevas tecnologías de la información y la comunicación están suponiendo una transformación digital de la sociedad y de la economía, que están destinadas a significar un efecto impulsador hacia una mayor transparencia, eficiencia y control del sector público y privado (Wanden-Berghe; Bednàrová; Fernández Daza, 2019). El uso de las tecnologías digitales se extiende por gobiernos y empresas de todo el mundo como un elemento esencial en las estrategias de modernización tanto para la prestación de servicios como para procesos internos (OCDE, 2014). En este contexto, que se ha calificado como la cuarta revolución industrial (Schwab, 2016), caracterizado por la revolución digital y la inteligencia artificial, blockchain es una de las tecnologías mas disruptivas al aportar descentralización de los datos y seguridad en la fiabilidad de la información, al margen de otras propiedades cuando se combina con la inteligencia artificial y otras tecnologías. Lo que inicialmente se enfocó para ser el soporte de transacciones con criptomonedas[1], concretamente con bitcoin, se ha visto que es aplicable a múltiples sectores dada su flexibilidad y aplicabilidad. En pocos años se han multiplicado las aplicaciones de blockchain con soluciones innovadoras en los sistemas de información y de control, que están cambiando la forma de relacionarse entre los entes públicos y privados, así como innovando los modos de colaboración. Tal como señala el observatorio blockchain de la Unión Europea, si 2016 fué el año de la formación sobre esta tecnología y sus usos, 2017 el año de las pruebas de concepto para experimentar, 2018 el año de proyectos a gran escala, ahora hay muy buenas razones para creer que 2019 es el año en que los proyectos se ponen en marcha, con una serie de importantes plataformas en fases avanzadas de producción (EUBlockchain, 2018).

Esta explosiva evolución de las aplicaciones blockchain no está exenta de incertidumbres y desafíos, especialmente ligadas a la falta de regulación, la falta de conocimiento de esta tecnología y de sus posibilidades, así como sobre los costes de la implantación de las aplicaciones y su sostenibilidad (Deshpande, Stewart, Lepetit, y Gunashekar, 2017). Sin embargo, tales dificultades no van a impedir el desarrollo de soluciones blockchain, a la vista del ritmo en que se experimentan y de los resultados que se obtienen.

Este trabajo, por tanto, parte describiendo el fundamento de blockchain, la composición de los bloques y como se enlazan entre ellos formando la cadena con el uso de la criptografía, a la vez que se muestran sus principales propiedades. A continuación se aborda la tipología

1. El diseño de bitcoin lo firma Shatoshi Nakamoto (2008), pseudónimo de la persona o el grupo creador, que se mantiene en el anonimato.

de las redes pues pueden ser públicas, privadas o híbridas o de consenso. El siguiente punto se destina a los smart contracts, programas autoejecutables propios de la inteligencia artificial que han adquirido mucho relieve en las aplicaciones blockchain. Con ello se completan los elementos básicos de blockchain. Tras ello se hace una exploración por iniciativas blockchain que se están llevando a cabo en el sector público, partiendo por una muestra que da signos de cambio en la administración publica que planean optar por aplicar blockchain en los servicios públicos. La revisión de iniciativas se agrupan atendiendo a nuestros propósitos en proyectos que giran en torno a la identidad digital, a los registros en sentido amplio, a la lucha contra el fraude y la corrupción y, especialmente a la contratación pública. El último bloque se centra en estudiar los impactos de blockchain en las prácticas de contabilidad y auditoría y su efecto como herramienta para la transparencia y el control. La cadena de bloques va a implicar una mejora en la calidad de la información ya que los registros son inmutables, verificables, consensuados y, en definitiva, mas confiables. Al mismo tiempo, la disponibilidad de la información es más inmediata y muchos procesos pueden ser automatizados. Con todo ello, se reducen las oportunidades para manipular los datos y resulta más fácil realizar las tareas de control haciendo factible que la gestión pública haga que sus transacciones y el resultado de sus decisiones sean más transparentes y sus mecanismos de control puedan revisar con mayores garantías la ejecución del presupuesto público. Este punto concluye describiendo un proyecto piloto del Tribunal de Cuentas Europeo en materia de auditoría que ha sido seleccionado por el Partenariado Europeo en Blockchain para estudiar su implementación a nivel europeo. Finalmente se incluyen unas consideraciones finales.

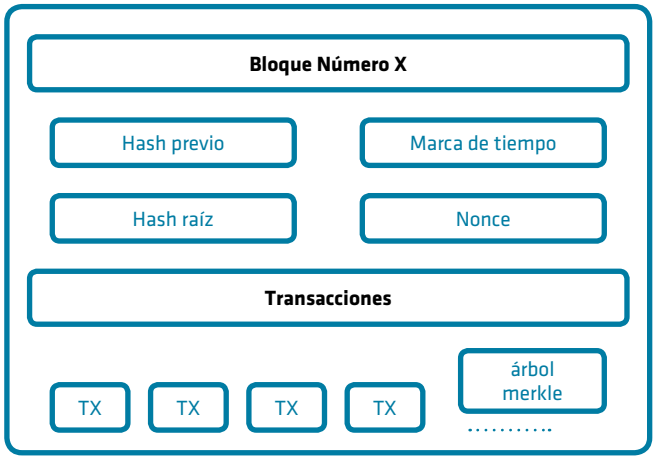
2. Fundamento y características de blockchain

El propósito de Nakamoto (2008) al diseñar la blockchain de bitcoin fué crear un sistema para realizar transacciones entre los miembros de una red, sin necesidad de la existencia de entidades centralizadas. Es el propio software el que garantiza y da fiabilidad a la transacción, apoyándose en una tecnología de bases de datos distribuidas en donde cualquier activo o información puede ser directamente transmitido entre los participantes de la red, sin requerir mediación alguna. La información se mantiene distribuida en nodos (ordenadores) y protegida criptográficamente en una red entre pares o P2P (Peer-to-Peer), donde todos los nodos están conectados y no tienen necesariamente que confiar plenamente entre ellos, pero el mismo sistema permite consensuar la veracidad de los datos compartidos. Así pues, la fiabilidad sobre la transmisión de activos o sobre la información almacenada en la cadena de bloques se logra a través de un protocolo de consenso que hace que todos los miembros puedan confiar en su contenido. Cada participante mantiene una copia de la cadena de bloques y cualquier actualización debe ser validada por la totalidad de la red.

Cada bloque tiene una cabecera y un cuerpo donde están registradas las transacciones que se han realizado, tal como se representa en el gráfico 1. La cabecera del bloque contiene datos identificativos como el número del bloque y el número hash que es el instrumento para enlazar los bloques y formar la cadena. Un bloque se tiene que generar haciendo referencia y consignando el hash del bloque previo. El hash está compuesto por bits que se calculan criptográficamente a partir de los datos de la cabecera y equivale a la huella

dactilar del bloque. También se refleja la marca de tiempo para indicar el momento en que se creó, así como el hash raíz de las transacciones y la forma en que se ha realizado el consenso que es el nonce, representado por otro algoritmo matemático (Wanden- Berghe y Fernández Daza, 2018b). Por otra parte, el bloque incorpora el árbol merkle que contiene todas las transacciones y se representa en forma de árbol, de forma que cada transacción equivaldría a una hoja. El hash de la información contenida en cada hoja, es decir, de cada registro o transacción, se concatena con los diversos valores hash del nivel inferior y se le aplica la función hash que sirven de base para calcular el hash del nivel superior. Este proceso se repite hasta que se llegue a un nivel donde hay un solo nodo, un sólo hash, denominado raíz del árbol (Dolader, Bel y Muñoz, 2017).

GRÁFICO 1
BLOCKCHAIN. ESTRUCTURA BÁSICA DE UN BLOQUE



Fuente: *Wanden-Berghe y Fernández Daza (2018b)*

El sistema se describe en muchas ocasiones como un libro mayor distribuido y posibilita que los miembros de la red puedan acceder a la información registrada, consultar el histórico de transacciones o de datos, hacer el seguimiento ya que cada registro lleva su marca de tiempo y los bloques están encadenados. La inmutabilidad de los registros es una característica central en blockchain que la hace atractiva para muchas aplicaciones e indudablemente también en contabilidad y auditoría. El hecho de replicar la información en múltiples nodos garantiza la integridad de la información y otorga la confianza de que no ha existido manipulación en los registros. Los nodos que almacenan la información en la cadena de bloques son testigos e impiden cualquier alteración en los registros históricos o la inclusión en unos nodos sin que existan en el resto. Toda la información que contienen es idéntica y compartida mediante un protocolo de consenso. Bitcoin y otras critomonedas utilizan como consenso la minería, que consiste en acertijos criptográficos para la prueba de trabajo previa a la inclusión de un nuevo registro en la cadena de bloques. Este protocolo se utiliza en redes en donde los miembros no tienen confianza y ninguna relación entre ellos. Sin embargo, hay otros sistemas de consenso que implican menos empleo de recursos que se emplea en redes privadas o híbridas.

Es importante tener presente que cualquier bien, derecho u obligación, podría estar representado en un token y que la tecnología blockchain facilita la emisión, comercialización y almacenamiento de los mismos. Ello induce a pensar que adicionalmente esta tecnología podría concretar a través de un token algunos intangibles que en la actualidad son de difícil transmisión y reflejo contable y, consiguientemente, cabe la posibilidad de llegar a materializarse por la potencialidad de esta tecnología.

3. Tipología de las redes

No existe una única configuración de red blockchain pues puede variar en función del grado de privacidad, los permisos de acceso para escribir o leer y otros aspectos de carácter técnico. La clasificación mas extendida es la que diferencia entre blockchains públicas, privadas o permisionadas e híbridas, también conocidas como federadas o de consorcio (Buterin, 2015).

- La blockchain pública está abierta totalmente sin restricciones para ser usuario. Cualquiera puede ser miembro y generar un nodo, registrar, leer la información, hacer transacciones y participar en el consenso. Las redes más conocidas de este estilo son Bitcoin[2] y Ethereum[3]. Una configuración de red de este tipo en el ámbito del sector público llevaría a una transparencia total de la información. La seguridad en una red pública se logra con gran número de ordenadores conectados y no restingiendo el acceso (World Bank, 2017).
- Las redes blockchain privadas, en cambio, está limitado el acceso y se requieren ciertas condiciones para ser miembros. Son redes permisionadas, en donde se precisa tener una autorización de un nodo de control para poder participar. Es la configuración que mayoritariamente utilizan las empresas que inician proyectos basados en blockchain (Popper y Lohr, 2017). En las redes privadas no se realiza el consenso por minería y, en consecuencia, no hay costes de recompensa (Atzori, 2015). Un ejemplo de este tipo de redes es Hyperledger[4], muy utilizada para soluciones empresariales, o sirva como ejemplo también Ripple[5] y R3 Corda[6] donde igualmente se realiza una configuración en la que ciertos miembros pueden acceder, escribir información en la cadena de bloques o aprobar la admisión de nuevos miembros. Son redes parcialmente descentralizadas en las que cabe la posibilidad de dar privilegios de anulación de registros a un nodo central aunque, en tal caso, puede socavar la credibilidad de la cadena de bloques (Liu, Wu y Xu, 2019).
- Una situación mixta la protagonizan las redes híbridas, en donde se requiere permiso para el acceso pero la validación la realizan solamente una parte de ellos. A su vez, la información contenida en la cadena de bloques podrá ser configurada tanto de forma pública como privada. Un ejemplo es XDC Network de XinFin[7].

2. https://bitcoin.org
3. https://www.ethereum.org/
4. https://www.hyperledger.org/
5. https://www.ripple.com/
6. https://www.r3.com/
7. https://www.xinfin.org/

Las configuraciones de red pueden ser muy variadas dependiendo de la estructura centralizada o descentralizada, de los permisos para el registro o la lectura de los datos (Jayachandran, 2017), así como por aspectos acerca de la identidad, el anonimato o el pseudoanonimato (Swanson, 2015).

4. Acuerdos autoejecutables: Smart contracts

La tecnología blockchain comenzó como una aplicación de sistema de pago pero, conforme se ha ido conociendo su funcionamiento, se ha extendido a muchas más aplicaciones. Tal como se distingue en Zhao, Fan y Yan (2016) cabe identificar tres generaciones en esta tecnología: Blockchain 1.0 cuyo objeto es realizar transacciones de criptomoneda; Blockchain 2.0 que incorpora smart contracts y otras aplicaciones que amplia su funcionalidad y no se limita a las transacciones con criptomonedas; y Blockchain 3.0, que integra aplicaciones en nuevas áreas de actuación y con un alcance mayor, como por ejemplo en el gobierno digital.

Un smart contract (Szabo, 1994, 1997) es un contrato inteligente que se programa y es autoejecutable. Es un contrato del tipo «if-them», es decir, que si se cumplen las condiciones acordadas se realizará automáticamente una determinada acción. La cadena de bloques ha hecho aumentar el empleo de smart contracts, a pesar de ser un recurso de inteligencia artificial creado en la década de los noventa, al no precisar un tercero para supervisar y ejecutar el contrato, ya que esta tecnología propicia la ejecución automatizada en la medida que las responsabilidades de supervisión se distribuyen entre los nodos participantes (Dai y Vasarhelyi, 2017). Es un acuerdo entre las partes que se programa y almacena en la cadena de bloques de tal forma que cuando verifica que los datos recibidos cumplen las reglas preestablecidas, realiza una acción. En cambio, en el caso que no se cumplan las condiciones se envía un mensaje de error a la red y no se ejecuta el contrato (Rozario y Vasarhelyi, 2018).

Se suele decir que en blockchain el código es la ley y el smart contract es código de programación que se mantiene de forma inalterable y transparente, conteniendo acuerdos entre las partes. Para poder interactuar un smart contract requiere «oracles» que transmiten la información del exterior con el fin de cambiar su estado interno y poder ejecutarse y, por tanto, debe ser un suministrador de información acordado y fiable.

5. Blockchain en el sector público

5.1. Signos de cambio en la administración pública

La administración pública ha creado en lo que llevamos de siglo muchas sedes y registros electrónicos, servicios telemáticos de notificaciones o plataformas de pago electrónico, estableciendo relaciones jurídicas con los ciudadanos en un entorno telemático. Ha avanzado de forma sustancial pero todos estos recursos dependen de una entidad centralizada que controla, custodia y supervisa, planteando importantes implicaciones en lo que se refiere a la falta de cooperación interadministrativa y de control ciudadano de la toma de decisiones públicas. Sin embargo, la irrupción de blockchain parece hacernos prever un cambio trascendental en los fundamentos sobre los que se sostendrá la gobernanza pública (Pereiro, 2019).

Ciñéndonos solo a nuestro entorno más cercano y dejando al margen los numerosos pronunciamientos en el resto del mundo que apuestan por implantar blockchain en la gestión pública, cabe señalar como muy significativa la declaración de 22 estados miembros de la Unión Europea el 10 de abril de 2018 por la que crean la asociación europea de blockchain, con la intención de cooperar, intercambiar experiencias y conocimientos en los ámbitos técnico y reglamentario y con el objetivo de identificar casos de uso, desarrollar especificaciones y preparar el lanzamiento de aplicaciones de blockchain en toda la Unión Europea. La comisaria Mariya Gabriel en el acto de presentación manifiesta: «En el futuro, todos los servicios públicos utilizarán la tecnología blockchain. Blockchain es una gran oportunidad para Europa y los Estados miembros para repensar sus sistemas de información, promover la confianza del usuario y la protección de datos personales, ayudar a crear nuevas oportunidades de negocio y establecer nuevas áreas de liderazgo, beneficiando a los ciudadanos, servicios públicos y empresas. La Asociación lanzada hoy permite a los Estados miembros trabajar conjuntamente con la Comisión Europea para transformar el enorme potencial de la tecnología blockchain en mejores servicios para los ciudadanos»[8]. En este momento, ya son 27 países los que han suscrito la declaración. Al mismo propósito obedece el Observatorio y Foro Blockchain de la Unión Europea que promueve y hace un seguimiento de los desarrollos y es un vehículo de comunicación con la emisión de importantes informes[9]. El 3 de octubre de 2018 el Parlamento Europeo aprueba la resolución sobre las tecnologías de registros distribuidos y las cadenas de bloques para fomentar la confianza con la desintermediación[10], solicitando a la Comisión Europea que evalúe y desarrolle un marco jurídico para solventar posibles problemas legales que puedan plantearse en caso de fraude o delitos, no tanto regulando los nuevos fenómenos, sino eliminando las barreras para su desarrollo.

Los pronunciamientos se suceden y cabe señalar por reciente y significativo que en septiembre de 2019, Alemania ha publicado su estrategia blockchain, por la que crea las condiciones marco para las innovaciones basadas en esta tecnología con la intención de desarrollar un ecosistema dinámico de desarrolladores y proveedores de servicios (Bundesministerium der Finanzen y Bundesministerium für Wirtschaft und Energie, 2019). Y mientras se termina de escribir estas líneas, el 3 de octubre de 2019, el Parlamento de Liechtenstein ha aprobado por unanimidad la Ley sobre tokens y entidades que prestan servicios basados en tecnologías fiables (TVTG), también conocida como la Ley Blockchain[11], por la que crea un marco jurídico que pretende incentivar las soluciones tecnológicas basadas en blockchain.

En España existe dos proposiciones no de ley, una sobre regulación, tributación, comunicación del uso legal de criptomonedas y la tecnología blockchain de 20 de marzo de 2018 y la otra sobre introducción de la tecnología blockchain en la Administración pública de 22 de junio de 2018 que profundiza más en las aplicaciones blockchain pero de forma muy general, apuntando aspectos tan importantes como las concesiones administrativas, la contratación y procesos internos y se postula tendente a un mayor control, trazabilidad y transparencia.

8. https://www.criptonoticias.com/comunidad/adopcion/paises-asociacion-europea-blockchain/

9. https://www.eublockchainforum.eu/

10. http://www.europarl.europa.eu/doceo/document/TA-8-2018-0373_ES.html?redirect

11. https://www.landtag.li

Sin embargo si que existe una realidad de carácter semipúblico que es la red Alastria[12] que es un consorcio multisectorial integrado por más de 300 empresas e instituciones con el fin de establecer una infraestructura semipública que soporte servicios con un estándar de Identidad Digital, que otorgue validez legal en el ámbito español para las administraciones públicas como el sector privado y de acuerdo con la regulación europea.

5.2. Hacia una identificación digital para soluciones blockchain

La verificación y autenticación de identidad es un componente crítico para la prestación de servicios tanto para el sector privado como para el público, y en la era digital se exigen enfoques que aporten más seguridad que los actuales. Nos encaminamos hacia un ecosistema digital donde empresas, personas y administración pública interactúan en plataformas estandarizadas para un propósito mutuamente beneficioso, como intereses comerciales o sociales, innovación o interés común.

De acuerdo con las indicaciones del United States National Institute of Standards and Technology (NIST) la identidad digital debe evitar la dependencia de un único punto de confianza e impedir que una sola parte realice un seguimiento de las transacciones de un usuario, manteniendo al mismo tiempo un rastro auditable que no se puede alterar pero que, a su vez, impida la extracción de datos, protegiendo la identidad con criptografía de última generación (Grassi, Lefkovitz y Mangold, 2015). Tales objetivos de privacidad e integridad de datos, son factibles en un modelo descentralizado basado en blockchain que aproveche las plataformas y estándares tecnológicos, y que esté disponible en un ecosistema de participantes, en código abierto y con licencias para que sea fácilmente adoptado e integración por los desarrolladores de aplicaciones (Wolfond, 2017).

Hay muchos ejemplos de gobiernos que ya han desarrollado soluciones de identidad digital. Estonia tiene un sistema de identificación digital seguro que la mayoría de sus ciudadanos posee y sobre el que ha creado servicios públicos digitalizados. Su proyecto e-Residency permite desde 2014 que personas de cualquier parte del mundo soliciten la residencia electrónica para tener acceso a los servicios, abrir un negocio y actuar como cualquier ciudadano estonio (Sullivan y Burger, 2017). Estonia también lleva más de una década de votaciones en línea a través del proyecto i-Voting[13].

A nivel de ciudades, Dubai presume ser la primera ciudad en estar gestionada totalmente con la tecnología blockchain. En Smart Dubai[14] participan empresas públicas, desarrolladores, empresas locales y nuevas empresas en un proyecto de ámbito tanto público como privado. Cuentan con registros de salud, registro de negocios, testamentos digitales, proyectos de turismo, transferencia de títulos, visados, securización del comercio de diamantes y se extiende por todos los sectores de la ciudad. Otras líneas de actuación se realizan con el proyecto Dubái City Accelerator o el Blockchain Trade Finance sobre el comercio y la gestión de aduanas y el Dubai Trade, registro de licencias, entre otros servicios (Moonesar, Stephens, Batey y Hughes, 2019).

12. https://alastria.io

13. e-Estonia: https://e-estonia.com

14. Smart Dubai: https://www.smartdubai.ae

La ciudad suiza de Zug utiliza una identidad digital a través de uPort sobre la que construye un marco de servicios a los ciudadanos, como la participación ciudadana (evoting) o un ecosistema de negocios que sirve de germen para la puesta en marcha de nuevos proyectos[15]. En Holanda, igualmente están en marcha muchos proyectos pilotos[16] que han dado lugar a prototipos en el dominio público, a la vez que se está trabajando para configurar la cooperación con otros países y organizaciones internacionales (Bhunia, 2018). Finlandia tiene una tarjeta con identificación única que permite pagar impuestos y servicios así como recibir dinero que el Servicio de Inmigrantes finlandés ha aplicado a refugiados sirios (Gray, 2017). En el distrito chino de Chancheng se ha creado una plataforma de identificación digital verificable y se ha iniciando la prestación de algunos servicios públicos en blockchain para optimizar y corregir la alta fragmentación de registros y simplificar la burocracia, intentando que los

5.3. Registros inmutables en sentido amplio

Una de los principales aplicaciones blockchain es la administración y gestión de registros. En los registros de la propiedad o catastros se abre la posibilidad de interactuar entre las partes y minimizar la labor de la administración, tanto en la identificación de los activos como de las transacciones. Cabe mencionar el registro de la propiedad de Suecia que ha completado la tercera fase de su proyecto Lantmäteriet que consiste en un registro permisionado y público que no tokeniza las propiedades sino las transacciones (Chromaway, 2018). En Georgia, la Agencia Nacional de Registro Público de Georgia (NAPR) lleva a cabo un registro de tipo espejo entre el digital y el tradicional desde 2016 (Bitfury, 2017). En el estado de Illinois se está llevando a cabo un proyecto público y tokenizado, cuyo objetivo es mejorar el proceso de transmisión y registro de transacciones (Yarbrough y Mirkovic, 2017). Brasil plantea un proyecto de registro por fases, iniciándose en el ámbito local para posteriormente ir ampliando las áreas geográficas. Es público y se ocupa de registrar las transacciones sobre la propiedad (Lemieux y Lacombe, 2018). Por su parte, el HM Land Registry del Reino Unido se preocupa de digitilizar al máximo el registro y de facilitar el acceso, mejorar la velocidad y la eficacia de los procesos[17].

En otro orden y tipo de registros, están los del ámbito sanitario. En la Unión Europea, MyHealthMyData crea una red de información biomédica en el marco del programa Horizon 2020. En Estonia, e-Health, cuenta con más del 95% de los datos de los pacientes y realiza una prevención sanitaria que apunta a ser más eficiente y a conseguir grandes ahorros económicos. (Priisalu y Ottis, 2017). También hay iniciativas en asuntos de trazabilidad y cadenas de suministro (Nærland, Müller-Bloch, Beck y Palmund, 2017) y en materia de títulaciones y expedientes académicos cada vez son más los organismos que pasan a gestionarlos con blockchain como en Melbourne, Malta, Malasia, entre otros (Angraal, Krumholz y Schulz, 2017; Deloitte, 2018; Yumna, Murad Khan, Ikram, Noreen y Sabeen, 2019).

15. La web de Zug: http://www.stadtzug.ch

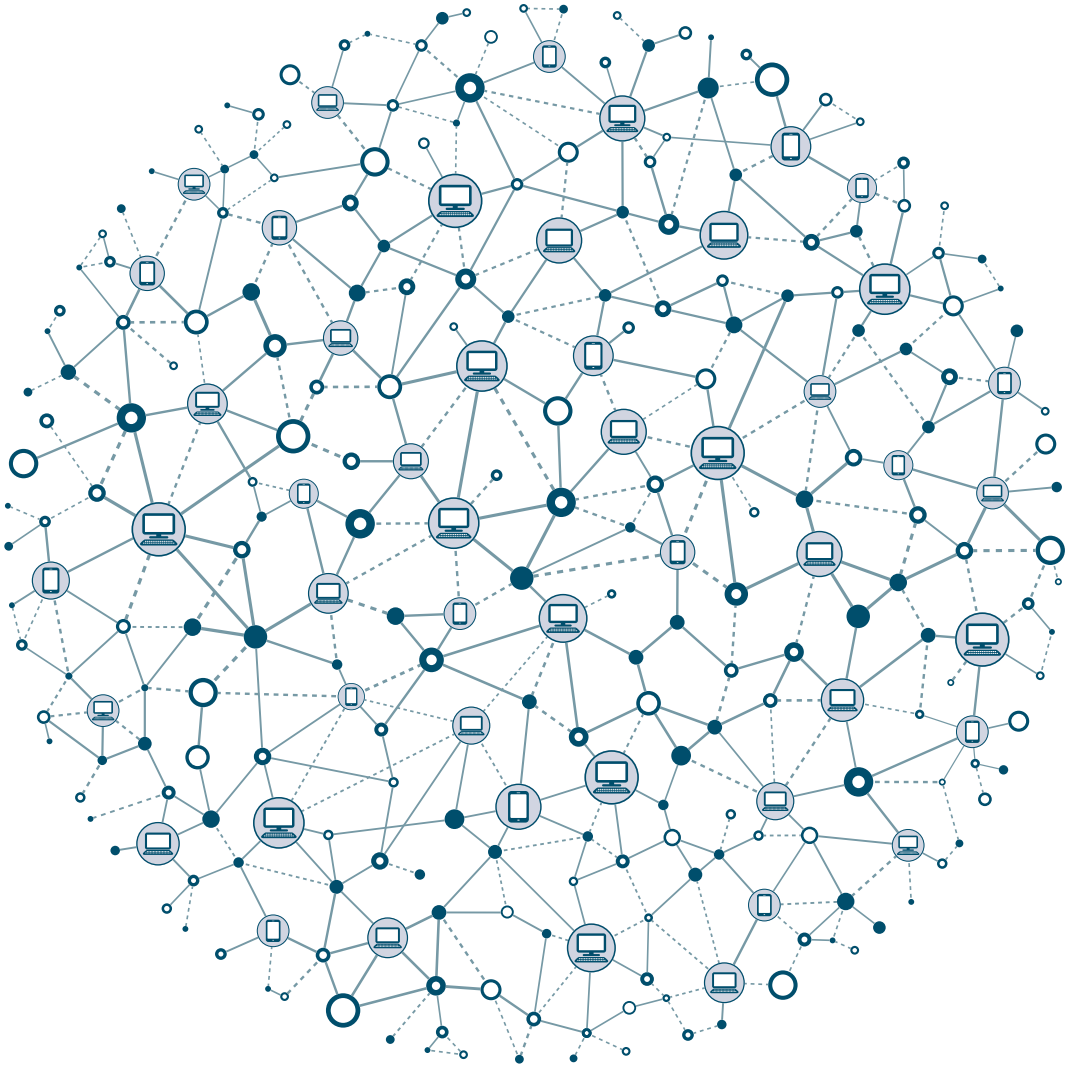
16. Se pueden ver en Blockchain Dutch Coalition (https://dutchblockchaincoalition.org) y el proyecto Blockchainpilots (https://www.blockchainpilots.nl)

17. https://www.gov.uk/get-information-about-property-and-land/search-the-register

5.4. Prevención contra fraudes y corrupción

Muchas aplicaciones persiguen que los ciudadanos tengan más confianza en las cuentas públicas, sea más difícil que se produzcan fraudes y sea un instrumento eficaz contra la corrupción. En Singapur se desarrolla un sistema con bancos locales con el fin de prevenir el fraude y detectar operaciones financieras engañosas (Kshetri, 2017; Higgins, 2017). Otros trabajos se han ocupado por prevenir declaraciones de impuestos fraudulentas (Hyvärinen, Risius y Friis, 2017).

En Europa se está desarrollando un proyecto que utiliza blockchain para combatir el fraude que se realiza en el IVA, muy difícil de reducir por su sistema de recaudación, pues las inspecciones se realizan a posteriori y sobre una muestra, ya que el coste para perseguirlo es elevado. Se estima en 150.000 millones de euros lo que se defrauda anualmente. El blockchain que se está configurando es sobre una red permisionada que contiene un registro de facturas confidencial con sellado del tiempo y plantea automatizar el proceso de recaudación del IVA (EUBlockchain, 2018).



5.5. Contratación pública con blockchain

La relevancia que tiene para los órganos de control interno y externo la fiscalización de la contratación pública hace que nos detengamos en este punto especialmente, pues una parte importante de la inversión pública se canaliza a través de la contratación administrativa y en los últimos años se ha despertado una gran alarma social como consecuencia de prácticas corruptas de gran envergadura (Medina y López, 2006).

Hay varios desarrollos en todo el mundo dirigidos a este fin pero tan sólo hay que mirar en España para encontrar dos interesantes proyectos blockchain relacionados con la contratación pública, que se ponen en marcha a finales de 2018. La Sociedad Informática del Gobierno Vasco (EJIE), hace uso de blockchain en el registro de contratistas y el Gobierno de Aragón sacó a concurso un servicio de registro distribuido de ofertas y evaluación automatizada en procedimientos de contratación pública electrónica.

En síntesis, blockchain permite acreditar los requisitos del contratista y que los miembros de la red de contratación pública, entre los que están otras administraciones públicas, puedan comprobar el cumplimiento de las condiciones y almacenar las garantías que se requieran para concurrir. De forma automática, la plataforma comprobaría y bloquearía en el procedimiento a quienes incurran en causas de incapacidad o incompatibilidad por infracciones o cualquier otro motivo. A través de smart contracts se comprueba la información de los licitadores en su participación en otros contratos públicos, con el fin de detectar incumplimientos, retrasos en la ejecución o cualquier resolución al respecto y evaluar la oferta. Tales ofertas se presentarían con su huella digital con sello de tiempo siguiendo el procedimiento administrativo estipulado, estando todo el contenido registrado con criptografía y de forma inmutable, con su hash correspondiente. La selección final del contratista se realiza por la mesa de contratación o mediante un smart contract tras verificar que el hash de la oferta presentada coincide con el registrado en la red blockchain, a efectos de garantizar que el documento no ha sufrido ninguna modificación. El proceso puede extenderse hasta fases de ejecución del contrato. (Pereiro, 2019; Bernal Blay, 2018; Muñoz Carmona, 2018). De esta forma la contratación pública gana en transparencia y la aplicación de smart contracts en el control y evaluacion de las ofertas puede quitar arbitrariaridad, al margen que es un sistema más ágil, rápido en su gestión y que supone menos costes.

6. Blockchain como herramienta de transparencia y control en el sector público

6.1. La transparencia y el control de las cuentas públicas

La sociedad demanda una actuación pública transparente como mecanismo para desencadenar cambios profundos en distintos ámbitos y redunda en la credibilidad de las organizaciones y del propio sistema. Es uno de los principios básicos del buen gobierno y de la calidad de las instituciones. Por su parte, el control constituye el elemento esencial para garantizar la transparencia y de esa forma alcanzar el objetivo de una mejora de la gestión. A su vez, la transparencia resulta fundamental para el correcto funcionamiento

de las instituciones de control. Ambos abren oportunidades y representan una fortaleza del sistema, generando confianza en los ciudadanos y con ello se facilita y dignifica la labor pública (de la Fuente, 2017).

La tecnología Blockchain puede representar un aporte muy importante para la transparencia de las cuentas públicas por la posibilidad que ofrece de registrar los hechos contables en una tercera entrada directamente en un registro conjunto, inmutable, verificable y distribuido criptográficamente. Este sistema en sí mismo genera confianza porque resulta prácticamente imposible manipular y en paralelo está disponible para ser auditada la información, con la consiguiente reducción de costos y de tiempos. Ian Grigg (2005) denominó «Contabilidad de triple entrada» a un diseño basado en la tecnología de registros distribuidos (DLT) cuando aún no había aparecido blockchain, en el que la tercera entrada contiene el recibo firmado criptográficamente sobre la transacción y ofrece un control por todas las partes de la misma información. Posteriormente, la literatura contable ha resaltado la potencialidad de blockchain para alcanzar ese objetivo (Dai y Vasarhelyi, 2017; Kokina, Mancha y Pachamanova 2017). En el registro de los hechos cada parte realiza su anotación contable por partida doble y, simultáneamente el sistema genera un flujo de datos en blockchain que se almacenan mediante transferencias de tokens que sirven como certificados de propiedad de activos o de obligaciones contraídas entre las partes intervinientes. Todo activo puede ser tokenizado y consiguientemente se le atribuye una identidad digital, puede ser transmitido por la red, se puede hacer su trazabilidad y se puede detallar sus componentes y características. Los tokens pueden ser simplemente medios de pago (criptomonedas) o representar bienes o derechos para el consumo de bienes o servicios (utility tokens), así como participaciones o títulos valores (security tokens)[18].

Las propiedades de blockchain garantizan la prueba de existencia, la identidad, la autoría, la propiedad y el orden temporal de los hechos por el sello de tiempo y autenticación de datos, ya que los documentos y la información que figuran en la cadena de bloques no se pueden borrar ni alterar. En definitiva, son una prueba puesto que la firma criptográfica es una huella digital y los hash enlazan la cadena de seguimiento con una marca de tiempo en cada registro que, para más seguridad, se encuentra descentralizada. Al auditar el presupuesto público, se recopilan evidencias con el fin de saber si los fondos se han empleado para lo que estaban destinados y si se han cumplido las normas y procedimientos. Todo ello estará consignado criptográficamente en los bloques de forma inalterable, facilitando los mecanismos de control.

Por tanto, la visibilidad de las transacciones que la cadena de bloques ofrece a todos los participantes conduce hacia esa transparencia que se demanda con una mayor confianza sobre la veracidad de los registros y, además muchas tareas de revisión, cotejo y validación se pueden automatizar con la ejecución de smart contracts, y el tamaño de las muestras pueda aumentar hasta incluso la población total. Como es sabido, el sistema contable está basado en múltiples mecanismos de control que en la actualidad se realizan en buena parte de forma manual exigiendo esfuerzos duplicados en ocasiones, como en tareas de conciliación (Deloitte 2016) y limitando el campo de observación. Con las soluciones basadas en

18. Esta clasificación de los token es la utilizada en CNMV y Banco de España (2018).

blockchain muchas comprobaciones de auditoría se van a automatizar haciendo más sencilla la conciliación de cuentas y existiendo un flujo transparente de los datos registrados, con la seguridad que concede el sistema. De forma derivada, la aplicación de blockchain puede conducir a que muchos recursos se redirijan hacia tareas de análisis más complejas o en generar nuevos mecanismos de control, o en modelar riesgos como el de crédito (Byström, 2019) y a detectar anormalidades o irregularidades.

El aumento de la muestra y la disponibilidad de la información en tiempo prácticamente real, proporciona una ventana para ver tendencias y observaciones que ayudan a prevenir cualquier tipo de fraude con dinero público (Antipova, 2019). En paralelo, la tecnología blockchain puede reducir la burocracia, aumentar la eficiencia de los procesos administrativos y el nivel de confianza en el mantenimiento de registros públicos (Allessie, Sobolewski y Vaccari 2019).

En la auditoría del sector público, combinar blockchain con otras tecnologías ayuda a analizar el presupuesto y a hacer un uso racional de los fondos públicos pero ello implica ampliar las expectativas de lo que se incluye en una auditoría y ajustar ciertos conocimientos y habilidades de los auditores (Lewis, Neiberline y Steinhoff, 2014). Aún falta un recorrido pero es fácil vislumbrar que el éxito de blockchain pasa por hacerla coexistir e interactuar con otras tecnologías existentes, como las herramientas y técnicas de auditoría asistida por ordenador (CAATT), el big data, la inteligencia artificial y los análisis ADA que los auditores utilizan para evaluar volúmenes crecientes de datos (Abreu, Aparicio y Costa, 2018).

6.2. Proyecto blockchain del Tribunal de Cuentas Europeo

El Tribunal de Cuentas Europeo inició en marzo de 2018 un proyecto piloto para explorar las capacidades y los beneficios de la aplicación de un sistema de registro electrónico basado en la tecnología blockchain. El proyecto, siguiendo a Cordero (2019) y Compellio (2018) para describir su contenido, se preocupó de probar tres casos de uso: auditoría de fondos europeos, contratación pública y protección de las publicaciones. Para ello utilizó el software Compellio que utiliza tecnología blockchain y creó en tres meses la plataforma ECA Registry que utiliza blockchains públicos para aplicar el control por diseño en los procesos de auditoría y, en ese sentido, inducir transparencia hacia empresas, beneficiarios finales, instituciones y ciudadanos de la UE. La plataforma permite a los usuarios registrar documentos digitales en blockchains públicos, verificar su autenticidad y crear una pista de auditoría segura. Actúa como un servicio notarial que permite registrar y relacionar las huellas digitales de los documentos y sus metadatos, realizar el control de plazos, verificar los documentos y cualquier otra información digitalizada e intercambiar bidireccionalmente huellas digitales (hash) con otros sistemas y, con ello evitar problemas de protección de datos.

La plataforma ECA registry calcula la huella digital de cada uno de los documentos o informaciones que van a ser registradas. Esta huella digital recoge toda la información de la transacción y es la que se registra en la cadena de bloques pública, concretamente se registraron en cuatro plataformas públicas, mientras que el documento se conservó en un registro privado, precisamente en ECA registry.

Las especificaciones que se establecieron perseguían obtener resultados rápidos, presentar usos concretos de blockchain en el ámbito de la auditoría, usar una aplicación web que

fuese una interfaz intuitiva para el simple uso del registro, utilizar una plataforma pública de blockchain y permitir la interoperabilidad entre las plataformas públicas de cadena de bloques y los sistemas informáticos internos.

En los casos de la auditoría, se aplicaron a dos casos: 1) Auditoría de fondos financiados por la Unión Europea y 2) Auditoría en el ámbito de la agricultura (promoción del vino). Las evidencias son registradas por el beneficiario en el momento en que se generan y el resto de actores del proceso como coordinadores, agencias regionales, y cualquier otro organismo de control, sólo tenían que acceder al registro para inscribir nuevas informaciones, o para consultar y verificar la información del registro.

El ECA Registry podía integrarse con los sistemas de información existentes en el Tribunal de Cuentas Europeo y con otros organismos de control y facilitar la captura de evidencias fiables introduciendo el concepto de control-por-diseño. Ello permite una importante reducción del coste de la auditoría y aumenta la transparencia, generando confianza.

Con respecto a la prueba piloto en el uso de contratación pública, se ha comprobado cómo la solución del registro, ayuda a tener garantías sobre la integridad de los documentos y el cumplimiento de los plazos. Y el tercer caso, al registro de informes oficiales del Tribunal de Cuentas Europeo que se publican en la web, con el fin de garantizar la autoría y la integridad del contenido, se les asoció un icono que figura al lado del título e indica que la publicación es la original. La plataforma permite, a cualquier usuario, comprobar si el texto es realmente el original o, por el contrario, ha sido alterado. Los resultados obtenidos han llevado a que la aplicación para la auditoría del ECA Registry haya sido seleccionado como uno de los proyectos que el Partenariado Europeo en Blockchain estudiará para su posible implementación a nivel europeo, empleando para tal fin fondos de cohesión. (Cordero, 2019; European Court of Auditors (2018); Compellio, 2018).

7. Consideraciones finales

En nuestra opinión, la sociedad y la economía están decididas a explorar las posibilidades de blockchain y hacer realidad aplicaciones que utilizan esta tecnología para recuperar la confianza de los ciudadanos y alcanzar los objetivos de transparencia, control y eficiencia en el sector público.

Para el logro de toda su potencialidad, debe converger la tecnología y la legislación actual, precisando una regulación y una adecuación sobre aspectos con los que choca en la actualidad, como la protección de datos o el reconocimiento o no de las criptomonedas como activos financieros. Hay que tener presente que tanto la privacidad de los datos como blockchain tienen como propósito aumentar la seguridad sobre los mismos, con lo que es de suponer que las herramientas tecnológicas podrán converger con las legales, manteniendo la privacidad y la integridad de los datos.

En los aspectos técnicos, es preciso establecer estándares de interoperabilidad entre las distintas aplicaciones blockchain, haciéndolas escalables y despejando las dudas de seguridad para hacer posible intercambiar datos entre sí cualquiera que sea la plataforma.

Se están creando sistemas blockchain de forma dispersa, siendo necesario que los responsables públicos se coordinen con el fin de que todos los esfuerzos sean compatibles y confluyan en un ecosistema de transparencia y eficacia, integrando todas las infraestructuras que se están desarrollando.

Finalmente se necesita formar sobre esta tecnología, pues va a implicar un cambio de roles en la profesión contable y auditora que va a exigir nuevos conocimientos que deberían ya estar impartiéndose en los ámbitos profesionales y universitarios. A su vez, conviene revisar el alcance y los objetivos de control y auditoría, dado que la sociedad lo demanda y la tecnología lo permite.

8. Referencias bibliográficas

ABREU, P. W, APARICIO, M., y COSTA, C. J. (2018), *«Blockchain technology in the auditing environment»,* The Institute of Electrical and Electronics Engineers, Inc. (IEEE) Conference Proceedings; Piscataway.

ALLESSIE, D., SOBOLEWSKI, M. Y VACCARI, L. (2019), *«Blockchain for digital government - An assessment of pioneering implementations in public services»,* European Commission.

ANGRAAL, S., KRUMHOLZ, H.M., y SCHULZ, W.L. (2017), *«Blockchain Technology: Applications in Health Care»*. Circulation. Cardiovascular quality and outcomes. 10, 9, Sep.

ANTIPOVA, T. (2019), *«Digital Public Sector Auditing: a look into the future»,* Quality-Access to Success, 20 (S1), January 2019.

BERNAL BLAY, M.A. (2018), *«El desarrollo autonómico de la normativa sobre contratos públicos»,* Revista Aragonesa de Administración Pública, ISSN 1133-4797, N.º Extra 18, (Ejemplar dedicado a La Ley de Contratos del Sector Público), pp. 91-138.

BUNDESMINISTERIUM DER FINANZEN Y BUNDESMINISTERIUM FÜR WIRTSCHAFT UND ENERGIE (2019), Blockchain-Strategie der Bundesregierung - Wir stellen die Weichen für die Token-Ökonomie https://www.bundesfinanzministerium.de/Content/DE/Pressemitteilungen/Finanzpolitik/2019/09/2019-09-18-PM-Block-Anlage.pdf;jsessionid=8AF112BA611BBEDB8023445CBF889E66?__blob=publicationFile&v=7

BHUNIA, P. (2018), «*How the Dutch Government is exploring blockchain use cases through many concurrent pilot projects»,* OpenGov. Disponible en: https://www.opengovasia.com/articles/how-the-dutch-government-is-exploringpotential-uses-of-blockchain-through-many-concurrent-pilot-projects [Consulta: 1 de octubre 2019].

BITFURY (2017), *«The Bitfury Group and Government of Republic of Georgia Expand Historic Blockchain Land-Titling Project»,* Medium. Disponible en: https://medium.com/@BitfuryGroup/the-bitfury-group-and-government-of-republic-ofgeorgia-expand-historic-blockchain-land-titling-4c507a073f6b [Consulta: 2 de octubre 2019].

BUTERIN, V. (2015), *«On public and private blockchains»,* Ethereum.org, Disponible en: *https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/* [Consulta: 2 de octubre 2019].

BYSTRÖM, H. (2019). *«Blockchains, real-time accounting and the future of credit risk modeling»,* The journal Ledger, Vol 4, 2019, pp 44-47.

CHROMAWAY (2018), *«Blockchain and future house purchases. Third phase completed in april 2018»*. Disponible en: https://chromaway.com/landregistry/ [Consulta: 3 de octubre 2019].

CNMV y BANCO DE ESPAÑA (2018), *«Comunicado conjunto sobre "criptomonedas" y "ofertas iniciales de criptomonedas" (ICOs)»,* 8 de febrero de 2018, Disponible en: *http://www.cnmv.es/loultimo/NOTACONJUNTAriptoES%20final.pdf* [Consulta: 2 de octubre 2019].

COMPELLIO (2018), *«Bringing EU Audit into the Blockchain World.»* Disponible en: https://medium.com/@compellio/bringing-eu-audit-into-the-blockchain-worldb5e4d2219649 [Consulta: 3 de octubre 2019].

CORDERO VALDAVIDA, M. (2018), *«Auditoría digital: el reto del siglo XXI»,* Presupuesto y Gasto Público, nº 91, 135-151.

CORDERO VALDAVIDA, M. (2019), *«Blockchain en el sector público, una perspectiva internacional»,* Revista Vasca de Gestión de Personas y Organizaciones Públicas, Núm. 16, 2019. pp. 16-34.

DESHPANDE, A., STEWART, K., LEPETIT, L. y GUNASHEKAR, S. (2017). *«Distributed Ledger Technologies/Blockchain: Desafíos, oportunidades y perspectivas de estándares. Informe general»,* The British Standards Institution (BSI).

DAI, J. y VASARHELYI, M. A. (2017), *«Toward Blockchain-Based Accounting and Assurance»,* Journal of Information Systems, 31(3), June, pp. 5-21.

DE LA FUENTE Y DE LA CALLE, M. J. (2017), *«Reflexiones acerca de la transparencia como instrumento de mejora de la gestión pública»,* Revista Española de Control Externo, vol. XIX, n.º 56 (Mayo 2017), pp. 43-75.

DELOITTE (2016), *«Blockchain technology: A game changer in accounting»,* Disponible en: *https://www2.deloitte.com/content/dam/Deloitte/de/Documents/Innovation/Blockchain_A%20game-changer%20in%20accounting.pdf* [Consulta: 1 de octubre 2019].

DELOITTE (2017a), *«Blockchain Technology, A game-changer in accounting?»* Accesible en: https://www2.deloitte.com/content/dam/Deloitte/de/Documents/Innovation/Blockchain_A%20game-changer%20in%20accounting.pdf [Consulta: 1 de octubre 2019].

DELOITTE (2018), *«Blockchain in Public Sector, Transforming government services through exponential technologies»,* January 2018

DOLADER RETAMAL, C., BEL ROIG J., y MUÑOZ TAPIA, J. (2017), *«La Blockchain: Fundamentos, aplicaciones y relación con otras tecnologías disruptivas»,* Universitat Politécnica de Catalunya, Disponible en: *https://www.mincotur.gob.es/Publicaciones/Publicacionesperiodicas/EconomiaIndustrial/RevistaEconomiaIndustrial/405/DOLADER,%20BEL%20Y%20MU%C3%91OZ.pdf* [Consulta: 1 de octubre 2019].

EUBLOCKCHAIN (2018), *«Blockchain for government and public services»,* The European Union Blockchain Observatory & Forum, Disponible en: *https://www.eublockchainforum.eu/sites/default/files/reports/eu_observatory_blockchain_in_government_services_v1_2018-12-07.pdf* [Consulta: 1 de octubre 2019].

EUROPEAN COURT OF AUDITORS ECA (2018), *«ECA conference on blockchain: opportunities and practical applications for EU expenditure control»,* Luxembourg on 8 November 2018. Disponible en: *https://www.youtube.com/watch?v=v5Ej4LfqQBg&t=3625s* [Consulta: 1 de octubre 2019].

FANNING, K. y CENTROS, D. P (2016), *«Blockchain and its coming impact on financial services»,* Journal of Corporate Accounting & Finance, 27 (5), 53-57.

GARCÍA BLANCO, M. J. (2018), *«El control externo por el Tribunal de Cuentas de los órganos constitucionales y de relevancia constitucional»,* Revista Española de Control Externo, vol. XX, n.º 58 (Enero 2018), pp. 119-153.

GRAY, A. (2017), *«Finland has created a digital money system for refugees»,* World Economic Forum, September 14, 2017.

GRIGG, I. (2005), *«Triple Entry Accounting»,* Disponible en: *http://iang.org/papers/triple_entry.html* [Consulta: 1 de octubre 2019].

GRASSI, P., LEFKOVITZ, N. y MANGOLD, K. (2015), Privacy-Enhanced Identity Brokers. Gaithersburg, MD: National Institute of Standards and Technology (NIST), U.S. Department of Commerce.

HIGGINS, S. (2017), *«IBM: Nine in 10 Government Execs Plan to Invest in Blockchain By 2018»,* Coindesk.

HYVÄRINEN, H., RISIUS, M., y FRIIS, G. (2017), *«A blockchain based approach towards overcoming financial fraud in public sector services»*. Business & Information Systems Engineering, 59, pp. 441–456.

JAYACHANDRAN, P. (2017), *«The difference between public and private blockchain»*. Disponible en: *https://www.ibm.com/blogs/blockchain/2017/05/the-difference-betweenpublic-and-private-blockchain/* [Consulta: 3 de octubre 2019].

KSHETRI, N. (2017), *«Blockchain's roles in strengthening cybersecurity and protecting privacy»,* Telecommunications Policy. (Sep. 2017).

KOKINA, J., MANCHA, R. y PACHAMANOVA, D. (2017), *«Blockchain: Emergent Industry Adoption and Implications for Accounting»,* Journal of Emerging Technologies in Accounting, Vol. 14, Nº. 2, pp. 91-100.

LEMIEUX, V. y LACOMBE, C. (2018), *«Title and code: Real Estate Transaction Recording in the Blockchain in Brazil (RCPLAC-01)»*. Case Study 1 Document Control.

LEWIS A.C., NEIBERLINE C. y STEINHOFF J.C. (2014), *«Digital Auditing: Modernizing the Public Sector Financial Statement Audit Approach»,* Journal of Public Sector Financial Management, Spring 2014, 63, 1, pp 32-37.

LIU, M., WU, K. Y XU, J. (2019), *«How Will Blockchain Technology Impact Auditing and Accounting: Permissionless Vs. Permissioned Blockchain»,* Current Issues in Auditing, August 2019.

MOONESAR, I.A., STEPHENS, M., BATEY, M., y HUGHES, D. (2019), *«Government Innovation and Creativity: A Case of Dubai»,* in (ed.) Future Governments (Actions and Insights - Middle East North Africa, Volume 7) Emerald Publishing Limited, pp. 135-155.

MONTESINOS JULVE, V. (2016), *«Auditoría y sostenibilidad de las entidades públicas: retos y camino a recorrer»,* Revista de la Asociación Española de Contabilidad y Administración de Empresas, n.º 115, pp. 41-43.

MONTESINOS JULVE, V. Y BRUSCA ALIJARDE, M. I. (2019), *«Non-financial reporting in the public sector»,* Revista de contabilidad: Spanish accounting review [RCSAR], Vol. 22, N.º 2, 2019, págs. 122-128.

MEDINA GUIJARRO, J. y LÓPEZ LÓPEZ, J. (2006), *«La fiscalización de la contratación administrativa por el Tribunal de Cuentas»,* C.Documentación Administrativa; Madrid N.º 274-275, pp. 407-424.

MUÑOZ CARMONA, A. (2018), *«Implicaciones jurídicas del uso de blockchain en la Administración pública»,* Trabajo Fin de Master. Universidad de Murcia. Disponible en: *https://digitum.um.es/xmlui/handle/10201/61679* [Consulta: 1 de octubre 2019].

NÆRLAND, K., MÜLLER-BLOCH, C., BECK, R., y PALMUND, S. (2017), *«Blockchain to rule the waves: Nascent design principles for reducing risk and uncertainty in decentralized environments»,* 38th International Conference on Information Systems, Seoul.

OCDE (2014), *«Recommendation of the council on digital government strategies»,* Accesible en: *http://www.oecd.org/gov/digital-government/Recommendation-digitalgovernment-strategies.pdf* [Consulta: 1 de octubre 2019].

PEREIRO CÁRCELES, M. (2019), *«La utilización del blockchain en los procedimientos de concurrencia competitiva»,* Revista General de Derecho Administrativo, n.º 50 monográfico «Derecho Público, derechos y transparencia ante el uso de algoritmos, inteligencia artificial y big data», (Iustel, enero 2019)

POPPER, N. y LOHR, S. (2017), *«Blockchain: A better way to track pork chops, bad peanut butter?»,* New York Times, 4 March., 2017, Accesible en: *https://www.nytimes.com/2017/03/04/business/dealbook/blockchain-ibmbitcoin.html?mcubz=1* [Consulta: 1 de octubre 2019]

PRIISALU, J., y OTTIS, R. (2017), *«Personal control of privacy and data: Estonian experience»,* Health and technology, vol. 7, n.º 4, 2017, pp. 441–451.

ROZARIO, A, y VASARHELYI, M.A. (2018), *«Auditing with Smart Contracts»,* The International Journal of Digital Accounting Research, January, pp. 1-27.

SULLIVAN, C., y BURGER, E. (2017), *«E-residency and blockchain»* Computer Law & Security Review, Vol. 33, n.º 4, págs. 470-481.

SWAN, M. (2015), *«Blockchain: Blueprint for a New Economy»,* O'Reilly Media, Inc.

SWANSON, T. (2015), *«Consensus-as-a-service: a brief report on the emergence of permissioned, distributed ledger systems»*. Disponible en: http://www.ofnumbers.com/wp-content/uploads/2015/04/Permissioneddistributedledgers.pdf [Consulta: 2 de octubre 2019].

SZABO, N. (1994), *«Smart contracts»*. Disponible en: *http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literatre/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html* [Consulta: 2 de octubre de 2019].

SZABO, N. (1997), *«Smart contracts: Formalizing and securing relationships on publicnetworks»,* First Monday, vol. 2, September.

WANDEN-BERGHE, J.L.; BEDNÁROVÁ, M.; FERNÁNDEZ, E. (2019). *La tecnología blockchain y sus implicaciones en el ámbito empresarial.* Asociación Española de Contabilidad y Administración de Empresas (pp. 1-61).

WANDEN-BERGHE, J. L. y FERNÁNDEZ DAZA, E. (2018). *«La Contabilidad de triple entrada y las implicaciones en Blockchain»,* En VV.AA., Blockchain: Aspectos Tecnológicos, Empresariales y Legales (pp. 269-293). Madrid: Aranzadi.

WANDEN-BERGHE, J. L. y FERNÁNDEZ DAZA, E. (2018b). *«Una propuesta de aplicación de la Contabilidad en Blockchain»*, XVIII Encuentro Internacional AECA, Lisboa. Disponible en: https://aeca.es/wp-content/uploads/2014/05/80g.pdf [Consulta: 1 de octubre de 2019].

WOLFOND, G. (2017), «*A Blockchain Ecosystem for Digital Identity: Improving Service Delivery in Canada's Public and Private Sectors»,* Technology Innovation Management Review, October 2017 (Volume 7, Issue 10) pp. 35-40.

WORLD BANK (2017). Distributed Ledger Technology (DLT) and blockchain, 2017.

YARBROUGH, KAREN A., y MIRKOVIC, J. (2017), *«Blockchain Pilot Program. Final Report, Deputy Recorder of Deeds»* (Communications/IT). Cook County, Illinois. Disponible en: http://cookrecorder.com/wp-content/uploads/2016/11/Final-Report-CCRD-Blockchain-Pilot-Program-for-web.pdf [Consulta: 4 de octubre de 2019].

YUMNA, H.,MURAD KHAN, M. IKRAM, M., NOREEN, S., y SABEEN, R. (2019), *«Use of blockchain in Education: A systematic Literature Review»,* Asian Conference on Intelligent Information and Database Systems, ACIIDS 2019: Intelligent Information and Database Systems pp. 191-202.

ZHAO, J. L., FAN, S. y YAN, J. (2016). Overview of business innovations and research opportunities in blockchain and introduction to the special issue.

La tecnología blockchain y su pretendida aplicación a la contratación pública como mecanismo para lograr mayor integridad

JOSÉ LUIS QUINTANA CORTÉS
Abogado. Socio de Rodríguez Castaño Abogados.
Doctorando de la Universidad Carlos III de Madrid

RESUMEN

Este artículo expone de manera sencilla, desde la perspectiva de un jurista, el funcionamiento de la tecnología blockchain o, por su terminología en castellano, de la cadena de bloques, así como sus principales características, atributos y aplicaciones. Además, por su importancia en el futuro del mundo jurídico y las relaciones comerciales, se describen y estudian los *smart contrats*. Todo ello, para poder analizar posteriormente, la aplicación de blockchain al ámbito de las Administraciones Públicas y, más en concreto, al de la contratación de las entidades del sector público. Si bien se tienen en cuenta los límites actuales para su plena implementación, sobre todo los legislativos, se debate y vaticina, proponiéndose algunas pretendidas aplicaciones, como pueden ser los registros de contratistas, las identificaciones o la valoración de las ofertas, la importancia que en el futuro, blockchain y los contratos inteligentes tendrán para garantizar la trazabilidad, inmutabilidad, auditabilidad y transparencia de los procedimientos de contratación pública. También, se estudia la posibilidad de incluir clausulas autoejecutables, *smart contrats,* en los contratos públicos. Ahora bien, nos queda un largo camino que recorrer para poder implementar esta tecnología plenamente en el ámbito que aquí se estudia.

PALABRAS CLAVE

blockchain | *smart contrats* | contratación pública | registros administrativos | integridad

ABSTRACT

In this article we try to describe from a lawyer's perspective how blockchain works, as well as its main characteristics and possibles applications in a simple way. Furthermore, due to their importance in the future of legal world and business relationships, this paper explains smart contrats and its characteristics. Moreover, it analyses how blockchain coul work in government services and administrative procurement, more specially, in public procurement. This analyses considers the existence of regulatory limits — legislative changes are needed to use blockchain technology to some cases—. Also, we propose the application of blockchain technology to public tenders, for example by desinging a bockchain-based contractor´s registry or by issuing a publicly verified bockchain-based indentity credential to contractors —they are just our propossals—. Blockchain can bring to public procurement transparency, inmutability, auditability and integrity. In adiction, it is important to study how smart contrats can be used in the public procurement. However, there is still a long way to go before we will be able to implement some of these ideas.

KEYWORDS

blockchain | *smart contrats* | *public procurement* | *administrative registry* | *integrity*

1. Introducción

La tecnología blockchain —«cadena de bloques» en su traducción al castellano[1]— se ha popularizado en los últimos años, primero, por servir de soporte a *bitcoin* y otras criptomonedas y, después, por ser una de las innovaciones a las que se le vaticina un mayor potencial disruptivo[2] y aplicaciones posibles.

Blockchain no es un fenómeno nuevo. En el año 2008, Satoshi Nakamoto[3] en el artículo *Bitcoin: a Peer-to-peer Electronic cash System*[4] propuso una solución técnica, a través de un red de blockchain, para realizar transacciones de la moneda virtual bitcoin sin la intervención de una entidad compensadora o validadora. En 2009 nacería así bitcoin y la primera red de blockchain.

En la actualidad no paran de surgir proyectos e iniciativas que tratan de aprovechar blockchain en numerosos sectores, a la cabeza de los cuales se encuentran el financiero o el asegurador. La comunidad jurídica muestra también un creciente interés por esta tecnología, principalmente considerando su propósito acreditativo. De igual manera, las Administraciones públicas no quieren —y no deben— quedar descolgadas de este fenómeno.

Entusiasma imaginar cómo serán las relaciones administrativas con la aplicación de blockchain, la robótica, el internet de las cosas (*Internet of Things*, en adelante, IoT) o la inteligencia artificial. Desde luego, aun no puede precisarse de manera clara cuál va a ser el impacto de estas tecnologías, pero ello no debe impedir que abordemos el debate de manera seria. Mostrando, como no podía ser menos, ciertas cautelas.

La primera de ellas es el temor a que se trate tan solo de una moda. En ocasiones, ante fenómenos como este, es difícil separar el sustrato de realidad de la exageración, el impacto imaginado o proyectado del que efectivamente se producirá. GARCÍA MELIÁN[5] en este sentido ha comparado blockchain con lo que los expertos en marketing denominan *hype*, es decir, la técnica de marketing que se basa en la exageración del producto hasta conseguir debido a las numerosas expectativas generadas que los consumidores solo deseen comprarlo.

El anterior fenómeno es especialmente acusado en el ámbito de las Administraciones públicas, pues actualmente resulta difícil encontrar proyectos consolidados que apliquen blockchain más allá de meras declaraciones de intenciones o experimentos para evaluar

1. En el artículo se utilizará indistintamente el término inglés y el castellano, por ser el anglosajón de uso generalizado en nuestro país.
2. La OCDE en «Chapter 2: Future Technology trends Science» *Technology and Innovation* identifica blockchain como una de las diez tendencias tecnológicas claves en el futuro.
3. La identidad de Satoshi Nakamoto es una incognita. Se ha especulado mucho sobre quién es la persona que se encuentra tras este seudónimo.
4. NAKAMOTO, S. (2008): *Bitcoin: a Peer-to-Peer Electronic Cash System*. Disponible en: https://bitcoin.org/bitcoin.pdf
5. GARCÍA MELIÁN, J.C. (2019). «Blockchain y contratación pública estratégica», Contratación Administrativa Práctica n.º 159.

su aplicación a procedimientos administrativos. Además, las instituciones públicas no son tan permeables a las innovaciones tecnológicas como otros sectores.

La segunda es que, en ciertas ocasiones, en vez de utilizar la cadena de bloques para solucionar problemas existentes, se buscan estos —o incluso se crean— para poder aplicarla[6].

La tercera es que, en particular en el ámbito administrativo, las soluciones basadas en blockchain deberán respetar las disposiciones en materia de procedimiento administrativo, v.gr. no podrá automatizarse un trámite y sus consecuencias con un *smart contrat* cuando para que se produzcan estos efectos el administrado tenga derecho a ser oído porque la omisión de la audiencia dará lugar a la nulidad del procedimiento.

No obstante, no pueden usarse de excusa las anteriores llamadas a la cautela. Es necesario introducir en el debate, como se propone en este artículo, las mejoras que blockchain puede ayudar a conseguir en el ámbito de la contratación pública para que las compras del sector público sean más eficientes, más transparente y que se garantice una mayor integridad en un ámbito especialmente abonado para la aparición de prácticas corruptas.

Así, en este trabajo, primero se trata de explicar qué es blockchain desde la perspectiva de un jurista y dirigido también a no técnicos, ya que el conocimiento de la tecnología, de cómo funciona y cuáles son sus posibilidades, permite comprender después no solo las posibles aplicaciones en el ámbito de la compra pública sino también las limitaciones que actualmente existen.

Esta es una materia en la que los juristas tenemos que caminar de la mano de informáticos, matemáticos y expertos en código y programación. Pronostico, al albur de los avances tecnológicos, que en no mucho tiempo el Derecho también se escribirá con bits. La necesidad de asesoramiento de expertos en estas tecnologías no debe disuadirnos a la hora de aproximarnos a estos avances, pues no es un fenómeno nuevo, en multitud de áreas los juristas ya caminamos de la mano de expertos en las mismas.

Posteriormente, se expone por qué aplicar blockchain en la contratación pública, prestando especial atención a los efectos positivos que esto puede tener en la lucha contra la corrupción en las licitaciones públicas.

Finalmente, se analizan ejemplos de posibles aplicaciones de blockchain en los procedimientos de licitación. En este sentido, se toma en especial consideración lo afirmado por BERNAL BLAY[7]: «[l]os casos de uso de blockchain deben ir precedidos *de una revisión de los trámites que se evacúan en los procedimientos sobre los que operan, de una reflexión sobre*

6. A este respecto, véase COLLINS, A. (2017) *«Four reasons to question the hype around blockchain»*. Disponible en: https://www.weforum.org/agenda/2017/07/four-reasons-to-question-the-hype-around-blockchain/ (última consulta: 1 de diciembre de 2019). Este autor, responsable de Riesgos Globales en el Foro Económico Mundial, señala que: *«algunas organizaciones…en vez de poner sus problemas sobre la mesa y reflexionar sobre si la tecnología DLT puede ayudar, están poniendo la tecnología DLT sobre la mesa y buscando problemas a los que podrían aplicar esta tecnología»*. Compruébese, además, que como GARCÍA MEILÁN utiliza el término *hype* para caracterizar el fenómeno de blockchain.

7. BERNAL BLAY, M.A. (2018). *Blockchain, Administración y contratación pública*. Disponible en web: http://www.obcp.es/index.php/mod.opiniones/mem.detalle/id.418/relcategoria.208/chk.5d7064a2b9f6eb58024d2d1d4706c591 (última visita: 01/12/2019).

su necesidad, y valorar las posibilidades de su simplificación. No se trata de llevar a una blockchain todos los datos y documentos que forman parte de los expedientes (el que piense que se trata de eso no ha entendido cómo funciona blockchain)». La contratación pública no es materia para experimentos, de ahí que sea esencial que, primero, se teorice y se pongan sobre la mesa los posibles problemas que de la aplicación de la cadena de bloques a este campo pueden surgir.

2. Entender blockchain[8]

2.1. Un sencillo ejemplo

Habitualmente se recurre a la comparación con los libros de contabilidad para explicar blockchain de manera sencilla.

Desde hace siglos, empresas e instituciones (bancos, Administraciones públicas, etc.) han hecho uso de libros donde anotaban o registraban las transacciones. En estos libros se concentraba la totalidad de la información disponible sobre las transacciones. De tal forma que para realizar y conocer los intercambios realizados los usuarios deben acudir al intermediario que custodia el libro. Más sencillo, si A quiere transferir X a B, dará la orden a la institución que custodia y lleva el libro que comprobará los saldos y verificada la posibilidad de realizarla, posteriormente, si es posible, la registrará en el libro.

Así, para que este sistema funcione es necesaria, según BOUCHER[9], una autoridad central que es «*un intermediario en quien todos los usuarios confían que tiene un control total sobre el sistema e interviene en todas las transacciones*».

El supuesto descrito es el de un registro centralizado, caracterizado porque los usuarios no disponen de una copia del libro y para realizar las transacciones deben recurrir a quien lo tiene, un intermediario de confianza o autoridad central.

Pues bien, blockchain supone un giro copernicano en la concepción de este sistema, puesto que con esta tecnología el libro está distribuido entre todos los usuarios del sistema que registrarán las transacciones siempre que haya un consenso entre la mayoría de ellos y el contenido de dicha transacción concuerde con los registros que poseen. Su singularidad radica en el hecho de que el libro registro se encuentran distribuido entre toda la red de participantes y que, además, todos asumen la llevanza. Aquí no es necesaria ya una autoridad central.

Así, con la tecnología blockchain, como *distributed ledger technology* o *DLT* (tecnología de red o de registro distribuido), mediante un protocolo informático de código abierto la llevanza y custodia de los libros se realiza por los miembros de la red sin la necesidad

8. Para los juristas que quieran profundizar en la cuestión y entender blockchain se recomienda la lectura de GONZÁLEZ MENESES-GARCÍA-VALDECASAS, M. *Enteder blockchain. Una introducción a la tecnología de registro distribuido.* Thomson Reuters-Arazandi. Cizur Menor (Navarra). 2017.

9. BOUCHER, P (2017): «How blockchain could change our lives», *In-deph Analysis,* European Parlamentary Research Service, pág. 5.

de contar con un intermediario de confianza que como en el primer modelo actúe de garante e intermediario en las transacciones.

GONZÁLEZ MENESES[10] señala que blockchain es «*un registro de transacciones único pero llevado de forma descentralizada o distribuida; un libro de contabilidad, un* libro mayor, un ledger —en inglés—, que no lleva un solo sujeto, sino a la vez todos los *usuarios del sistema. Es como si la contabilidad de todos los bancos en cuyas cuentas se refleja todo nuestro dinero y todas las transferencias dinerarias que vamos haciendo la llevásemos directamente todos los clientes de los bancos mediante nuestros propios ordenadores*».

Por supuesto que blockchain es un sistema más complicado que la imagen que acaba de ofrecerse, en el que los algoritmos de consenso, la criptografía de clave asimétrica y los algoritmos de destilación tienen un papel destacado, pero lo aquí expuesto sirve para ilustrar que con esta tecnología cada miembro o nodo de la red posee la cadena de bloques que compone el historial de transacciones y participa en la incorporación de nuevas cadenas.

2.2. Cómo funciona blockchain

PASTOR SEMPERE[11] utilizando, como se ha hecho en el apartado anterior, el símil de un libro mayor de contabilidad define blockchain como «*un libro mayor distribuido (replicado miles o cientos de miles de veces) en el que la información sobre las transacciones de cualquier activo con valor se anota de forma secuencial en bloques para formar una cadena. Cada bloque de información de la cadena está referenciado al anterior, de manera que todos los eslabones guardan relación indirecta con el primero, y toda la cadena se replica en una red mundial de ordenadores, usando además mecanismos de seguridad criptográficos*».

Para comprender el funcionamiento debe atenderse a cómo se incorpora la información en los registros distribuidos mediante la cadena de bloques. Se continua simplificando la explicación en aras de conseguir antes la comprensibilidad que el rigor técnico en la exposición de la tecnología.

En los libros o registros cada una de las transacciones se incorpora como un bloque que se une de manera sucesiva a los ya registrados. Así, los bloques de información quedan vinculados de manera irreversible formando una cadena de bloques, que da nombre a la tecnología. El hecho de que la vinculación sea irreversible, mediante complejos sistemas criptográficos determina que los registros en blockchain sean inalterables por lo que estamos ante un instrumento acreditativo de un elevado potencial[12].

10. GONZÁLEZ MENESES-GARCÍA-VALDECASAS, M. *Enteder blockchain. Una introducción a la tecnología de registro distribuido*. Thomson Reuters-Arazandi. Cizur Menor (Navarra). 2017.

11. PASTOR SEMPERE, M.C. «Criptodivisas: ¿una nueva disrupción jurídica en la Eurozona?». *Revista de Estudios Europeos*. N.º 70. Instituto de Estudios Europeos de la Universidad de Valladolid. Valladolid. 2017 (pág. 294).

12. No obstante, con respecto a la inalterabilidad, y sin que sea objeto de análisis en este artículo, debe plantearse cómo se ejercitará el derecho al olvido, reconocido en el artículo 17 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), por ejemplo en los registros que utilicen la tecnología blockchain y, consecuentemente, tengan este atributo de inalterabilidad.

La integridad del registro distribuido viene dada por dos importantes características: (i) las transacciones se incorporan formando una cadena cronológica de bloques que están unidos tanto a los anteriores como a los posteriores; y (ii) a la existencia de copias del registro distribuidas entre los participantes del sistema.

Para conseguir que el sistema tenga estos caracteres se utilizan algoritmos de destilación que representan matemáticamente, mediante una sucesión alfanumérica denominada *hash*, los ficheros. De esta forma, el algoritmo de destilación funciona de compresor para facilitar la computación y garantiza que aplicando el algoritmo al mismo texto siempre obtendré el mismo *hash*. De manera más sencilla, una pequeña modificación del texto dará lugar a un *hash* distinto y será inmediatamente detectable la alteración.

Esta función, como se expondrá *ut infra* al abordar las aplicaciones de la tecnología en la contratación pública, en la presentación de las ofertas mediante huellas electrónicas basadas en blockchain.

El anterior proceso determina la dificultad de modificación o manipulación de la concatenación de *hash's*, o de la cadena de bloques, porque la modificación de uno determinará la alteración de toda la cadena. En definitiva, se garantiza la no manipulación del registro y su integridad, robusteciendo su propósito acreditativo.

El ejercicio de validar e incorporar los bloques al registro es realizado por los llamados nodos validadores. Así, estos usuarios de la red verificarán para cada una de las transacciones las identidades del emisor y del receptor de la transacción y la capacidad para disponer de lo que se transfiere, es decir, si el emisor tiene lo que traspasa al receptor. Cotejarán así, que la transacción sea coherente con el contenido ya registrado, del que el nodo validador tiene una copia. Una vez validado por este nodo, se someterá a la aprobación del resto de los nodos validadores que volverán a cotejarlo con la copia del registro que ellos tienen. Si la mayoría acepta el bloque, este se incorporará al registro sin que pueda ser destruido o corrompido.

En esta validación se aplican algoritmos de consenso, es decir, fórmulas aptas para conseguir el acuerdo entre la pluralidad de nodos validadores, con el objetivo de que se inscriba en el registro la verificación que tenga mayor consenso entre los participantes en el sistema.

Por otro lado, también debe hacerse referencia a la identificación de los usuarios de la red distribuida. En blockchain, para la identificación se utiliza una criptografía de clave asimétrica. Todos los usuarios tienen una clave pública y una clave privada que se encuentran vinculadas entre sí. La clave pública es conocida por todos los miembros del sistema e identificará a su poseedor ante todos los usuarios del mismo. La clave privada sólo será conocida por su titular, que firmará con ella sus transacciones, convirtiéndose en ese momento en su clave pública para que el resto de los miembros puedan identificarlo. Ambas claves además de asimétricas son unívocas y bidireccionales, la clave pública de un usuario corresponde indefectiblemente a su clave privada.

Lo que acaba de exponerse con respecto a la criptografía asimétrica, cobrará importancia después cuando se comente la posibilidad de crear una identidad digital de los licitadores.

Veamos un ejemplo práctico. Siendo A y B usuarios de una red de blockchain con sus claves criptográficas y un monedero virtual donde almacenan las criptomonedas, de manera muy esquemática y sintética un transacción de bitcoins en blockchain, se realiza como sigue: (i) A, mediante un mensaje encriptado, firmado con una clave privada correlativa a la clave pública que todos los miembros conocen, propondrá que una cantidad de bitcoins que constan en su cuenta pasen a B; (ii) el mensaje encriptado será recibido por los nodos validadores que verificarán, valiéndose de la copia del registro que almacenan, la identidad de A, la disponibilidad de bitcoins y la existencia de B; (iii) si el mensaje de A es coherente con la información disponible en los registros, se calculará el correspondiente *hash*; y (iv) el *hash* se incorporará a la cadena como un nuevo bloque almacenado en el registro del que disponen todos los usuarios.

Finalmente, debe referirse que no todas las redes de blockchain tienen la misma configuración. En este sentido, simplificando, puede distinguirse entre redes públicas y redes privadas. En las redes públicas cualquier usuario puede constituirse en nodo y participar en el proceso de validación y registro de las transacciones. En cambio, en las redes privadas la participación está limitada, solo podrán constituirse como nodos aquellos sujetos que previamente hayan sido acreditados por un órgano gestor de la red[13]. La diferenciación entre ambos tipos y la apuesta por la utilización de una red u otra esta íntimamente relacionado con el debate presente y candente sobre la gobernanza de blockchain.

En cuanto a la utilización por la Administración de una u otra red, PEREIRO CARCELES[14] afirma que «*la Administración escogerá aquella configuración que mejor se adecue a sus circunstancias y al caso de aplicación*». Ahora bien, en estos momentos, las entidades públicas, hasta que la tecnología tenga un mayor grado de madurez y exista un marco jurídico que la regule, apostarán por redes privadas para controlar las validaciones y registros. Es esta una cuestión que va a ser largamente debatida.

2.3. Características de blockchain

Una vez expuesto el funcionamiento de blockchain, deben destacarse las características más relevantes de esta tecnología para su aplicación a los problemas jurídicos.

a) Integridad de los registros en blockchain

La configuración de las redes determinan la integridad de los registros siendo los bloques que se incorporan a la cadena irrevocables e inmutables. Una vez que una determinada transacción se incorpore a la red no será posible ni su alteración ni eliminación como consecuencia de la concatenación de los *hash's*.

Si un nodo altera o elimina una determinada parte de la cadena, modificará su libro registro pero no el resto de copias del mismo, en poder del resto de nodos, con lo que será además bastante fácil la comprobación y detección de estos fraudes.

13. Esta necesaria presencia de un órgano gestor de la red que acredite a los participantes reduce consecuentemente la distribución de la red. No obstante, en el caso de redes con aplicaciones administrativas, lo más adecuado al menos en los primeros estadios de aplicación de la tecnología, será que la Administración asuma esta posición de gestor controlando el proceso de validación y registro.

14. PEREIRO CÁRCELES, M. (2019): «La utilización de blockchain en los procedimientos de concurrencia competitiva». *Revista General de Derecho Administrativo*. N.º 50. Enero 2019.

b) Transparencia y auditabilidad

Dado que todos los usuarios tienen acceso al libro registro todos conocerán el contenido de las transacciones. Además, es también posible en determinadas redes el acceso de usuarios que no son miembros de la misma a los efectos de poder conocer la información almacenada en las cadenas de bloques.

Esto determina que a través de los registros distribuidos de blockchain pueda controlarse la trazabilidad de un determinado procedimiento, ya que en las cadenas de bloques se contendrá toda la información desde las primigenias transacciones hasta las últimas y todas ellas concatenadas.

2.4. *Smart contrats*

En su origen blockchain surge como soporte de bitcoin, como el sistema que verifica y ejecuta las transacciones de esta moneda virtual. Con posterioridad, nuevas criptomonedas, en concreto Etherum, que utilizan este sistema tecnológico, han ampliado las posibilidades de uso más allá de servir de monedero (*wallet*) —de libro registro de transacciones—, introduciendo una mayor complejidad y posibilitando nuevas funciones que trascienden del registro, permitiendo incluir aplicaciones que se ejecutan tal y como se programaron sin que sea necesaria la intervención de un tercero.

Así surgen los llamados *smart contrats* —denominados contratos inteligentes en su traducción al castellano, aunque de nuevo se usará el término inglés debido a su uso generalizado— que podemos describir como cláusulas contractuales autoejecutables programadas en tecnología blockchain.

Su denominación puede inducir a error. Como señalan PORXAS y CONEJERO[15] el *smart contract* «*no es más que un programa autoejecutable*», así estos son tan solo una parte de los contratos propiamente dichos en los que deberán en todo caso concurrir consentimiento, objeto y causa (artículo 1.261 del Código Civil). De tal modo que en la doctrina hay consenso acerca de que no estamos ante un nuevo tipo de contratos sino ante una nueva forma de instrumentarlo, que permite la ejecución de un acuerdo de voluntades, que se traduce a un código informático en una red de blockchain, y se ejecuta de manera automática[16].

Los *smart contrats* son programas autoejecutables en los que usa un código informático y se almacena en una red de blockchain para conseguir la ejecución automática sin la intervención de terceros ni de las partes de un acuerdo de voluntades que reúne todos los elementos exigidos por el Código Civil.

15. PORXAS, N. y CONEJERO, M (2018): «Tecnología blockchain: Funcionamiento, aplicaciones y retos jurídicos relacionados», *Actualidad Jurídica Uría Menéndez*.

16. TUR FAÚNDEZ, C (2018): *Smart contrats, análisis jurídico,* Editorial Reus, Madrid.: *«El Smart contrat jurídicamente relevante es el instrumento creado para la ejecución del contrato legal inteligente e intervendrá normalmente como un tercero inexorable que, de producirse un evento para el que esté programado: a) Podrá recibir fondos de la cuenta de un deudor; b) Podrá cobrar automáticamente de la cuenta de un deudor y transferir los fondos a su propia cuenta o a la del acreedor, con o si intereses; c) Podrá retener fondos en su propia cuenta; d) Podrá recibir información sobre cualquier hecho constatable en el fundo exterior y actuar en consecuencia; e) Podrá ordenar que cualquier mecanismo exterior interconectado al programa: e.i. Se inicie o se detenga; e.ii. Se encienda o se apague; e.iii. se bloquee o desbloquee; f) Podrá ordenar la detención se su propia autoejecución; g) Podrá ordenar su autodestrucción, en cuyo caso jamás volverá a estar operativo en la cadena de bloques».*

Para hacernos una idea, podemos acudir a un ejemplo real: un contrato de compra de cualquier materia prima que será transportada en barco, se programa este acuerdo sobre blockchain, configurando como una cláusula autoejecutable que una vez que el barco alcance una determinada localización se realice el pago por la mercancía. Así, una vez se constata informáticamente la localización vía GPS del barco, se realiza automáticamente el pago sin la intervención ni de las partes ni de un tercero.

Dadas las características de inmutabilidad e inalterabilidad de blockchain, una vez programado el *smart contract* las partes tienen absoluta certeza del cumplimiento del acuerdo sin que deban prestarse más garantías ni hacer necesaria la intervención de terceros.

Asimismo, como señala LEGERÉN-MOLINA[17] «*en ellos la ejecución no depende de la voluntad de las partes, sino que, gracias a los comandos programados, tiene lugar de manera "automática", una vez se dan las condiciones preestablecidas por aquéllas*».

En cuanto a su potencial, coincido con MUÑOZ CARMONA[18] el automatismo y autonomía de la ejecución de los contratos inteligentes aporta una serie de beneficios al tráfico jurídico, en tanto que dan certidumbre. Cumplido el contrato y verificada, de manera objetiva y previamente definida, la realización de la prestación, mediante el uso del llamado IoT, se autoejecuta el *smart contrat*.

Además, las aplicaciones de los *smart contracts* aumentan con el uso de la robótica o el denominado internet de las cosas (*Internet of Thins, IoT*)[19] en la que objetos, utensilios y máquinas están conectados a internet y poseen sensores capaces de recopilar y transmitir gran cantidad de información. Este gran volumen de datos, *Big Data*, puede ser tratado y analizado con inteligencia artificial y contribuir a que las máquinas aprendan y mejoren por sí mismas a través del *machine learning*. Así, todas estas innovaciones y desarrollos tecnológicos harán que los supuestos de aplicación de los *smart contrats* se eleven de manera exponencial.

No obstante lo anterior, actualmente los *smart contrats* padecen serias limitaciones. Pueden implementarse sin problemas a transacciones simples, fácilmente parametrizables y, por consiguiente, traducibles a fórmulas matemáticas y a un código informático. Sin embargo, resulta extremadamente difícil que puedan darse *smart contrats* en aquellos acuerdos de voluntades en los que intervengan un número elevado de contingencias, sea

17. LEGERÉN-MOLINA, A. (2019). «Retos jurídicos que plantea la cadena de bloques». *Revista de Derecho Civil*. Vol. 6, n.º 2.

18. MUÑOZ CARMONA, A. (2018). Implicaciones jurídicas del uso de blockchain en la Administración pública. Trabajo Fin de Master. Universidad de Murcia. Disponible en web: https://digitum.um.es/xmlui/handle/10201/61679 (última visita: 23/11/2019).

19. Téngase en cuenta que los *smart contrats* son denominados por algún autor como contratos programados. De acuerdo con GARCÍA GIL, pueden ser definidos como aquellos capaces de combinar la ejecución automatizada de sus prestaciones y su plena interoperabilidad a través del Internet de las Cosas gracias a la detección, por parte de sistemas dotados de inteligencia artificial insertos en su código, de un complejo estado del mundo cuya evolución permita el paulatino ajuste de las reciprocas obligaciones de las partes que se irían reconfigurando en lo necesario para obtener en cada momento el equitativo reparto del excedente contractual en los términos y proporción que hubiere sido acordado GARCÍA GIL, V. J. (2016): *«De qué hablamos cuando hablamos de 'smart contracts'»*. Disponible en: https://blogs.elconfidencial.com/espana/blog-fide/2018-04-26/smart-contracts_1555216/

necesario un juicio de valor o en su definición esté presente un concepto jurídico indeterminado por las dificultades que ofrece su conversión a un lenguaje matemático o de programación informática.

Lo anterior determina que, nos encontremos, con dificultades para la aplicación de los *smart contrats* en el ámbito de la contratación administrativa donde existen muchas vicisitudes, criterios de valoración sometidos a juicio de valor o tramites procedimentales que no se pueden obviar.

En cuanto a la posibilidad de automatización de decisiones administrativas, tiene cobertura legislativa en el artículo 41 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público[20] (en adelante, LRJSP) que, por tanto, en principio, ampararía, con los límites señalados, la posibilidad de uso de los *smart contrats*.

2.4. Aportaciones de blockchain con importancia para los juristas

La configuración de blockchain no solo resulta disruptiva en el ámbito tecnológico, sino que contiene aportaciones que implementadas en el campo jurídico suponen un giro en la concepción de los tradicionales modelos de confianza de nuestros ordenamientos jurídicos.

A continuación, se resumen las aportaciones que la cadena de bloques realiza y que pueden ser de aplicación en el ámbito jurídico y, como se estudiará a continuación, en la contratación pública. Estas principalmente son:

- La posibilidad de crear un registro íntegro (inmutable e inalterable) en el que aparecerá acreditada la titularidad de los activos, las transacciones realizadas con la inclusión de su fecha o los compromisos contractuales autoejecutables sin que exista posibilidad de modificación, manipulación o modificación.
- Permite la llevanza de estos registros sin la existencia de una autoridad central o tercero de confianza —recuérdese que estamos ante una red distribuida—.
- Se puede compartir de forma segura, mediante una potente encriptación, documentos o información entre los miembros, nodos de la red, cada uno de los cuales tiene una copia de los registros.
- Se garantiza la transparencia de la trazabilidad de los procesos, ya que en los registros puede consultarse todo el historial de transacciones. Si la red es pública, también podrá ser consultada por terceros que no son usuarios, —nodos de la red—.
- Como consecuencia de la evolución de blockchain, se pueden automatizar procesos, decisiones o acuerdos de voluntades a través de los *smart contrats*.

20. El artículo 41 de la LRJSP dispone que: *«1. Se entiende por actuación administrativa automatizada, cualquier acto o actuación realizada íntegramente a través de medios electrónicos por una Administración Pública en el marco de un procedimiento administrativo y en la que no haya intervenido de forma directa un empleado público. 2. En caso de actuación administrativa automatizada deberá establecerse previamente el órgano u órganos competentes, según los casos, para la definición de las especificaciones, programación, mantenimiento, supervisión y control de calidad y, en su caso, auditoría del sistema de información y de su código fuente. Asimismo, se indicará el órgano que debe ser considerado responsable a efectos de impugnación».*

3. Blockchain en la contratación pública

Visto y analizado el potencial disruptivo de la tecnología blockchain, estamos obligados a plantearnos y a abordar los posibles usos de la misma en el ámbito de los procedimientos administrativos y, en particular, de las licitaciones públicas.

Aunque, como ya se ha advertido, actualmente no existen iniciativas consolidadas que utilicen la tecnología blockchain en el sector público. Sin embargo, la Unión Europea está prestando especial atención al impacto que esto pueda tener y la Comisaria de Economía y Sociedad Digital, Mariya Gabriel, señaló en la firma de la Declaración para el establecimiento de un *«European Blockchain Parnertship»* que, *«en el futuro todos los servicios públicos utilizarán la tecnología blockchain»*.

Como ya se ha indicado, las instituciones públicas no son especialmente permeables a los avances tecnológicos, no obstante, las dos leyes que constituyen la clave de bóveda del ordenamiento administrativo, la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante, LPACAP) y la LRJSP, apuestan por la relación electrónica entre los administrados y las administraciones, reconociendo la tramitación electrónica como modo habitual de la tramitación administrativa.

Como destaca PEREIRO CÁRCELES[21] , las sedes electrónicas, los registros electrónicos y de apoderamiento, los servicios telemáticos de notificación o las plataformas de pago electrónico, como están actualmente configuradas, dependen de una entidad centralizada. En cambio, la aplicación de blockchain supondrá la descentralización y distribución de estos sistemas. Me aventuro a vaticinar que en un futuro, no muy lejano, los registros administrativos harán uso de la tecnología de la cadena de bloques no solo para aumentar la transparencia y auditabilidad de su contenido, sino por la necesidad de garantizar la integridad e inmutabilidad de los mismo y mejorar los mecanismos de identificación de los ciudadanos[22].

Así, la utilización de blockchain puede aportar ventajas en: (i) dotar de integridad (inmutabilidad) a los registros públicos; (ii) aumentar la transparencia en las actuaciones administrativas; (iii) aportar un modo seguro y certero de identificación de los ciudadanos en sus relaciones con las Administraciones públicas[23]; (iv) simplificar determinados procedimientos mediante la distribución y descentralización; y, (v) contribuir a la automatización de la actividad administrativa[24, 25].

21. PEREIRO CÁRCELES, M. (2019). Op. Cit.

22. Mantengo mi pronóstico aún después de la aprobación del Real Decreto-ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones que ha establecido que no serán admisibles en ningún caso y, por lo tanto, no podrán ser autorizados, los sistemas de identificaciones basados en tecnologías de registro distribuido y los sistemas de firma basados en los anteriores, en tanto que no sean objeto de regulación específica por el Estado en el marco del Derecho de la Unión Europea. Es tan sólo cuestión de tiempo.

23. A este respecto, téngase en cuenta lo que posteriormente se indicará del Real Decreto-ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones.

24. Artículo 41 de la LRJSP.

25. PEREIRO CÁRCELES, M. (2019). Op. Cit. señala como posibles usos de blockchain en la Administración pública los siguientes: (i) como sistema de identificación; (ii) inmutabilidad de los documentos registrados; (iii) eficacia de los procedimientos: (iv) como mecanismo de transparencia y trazabilidad; y, (v) como mecanismo favorecedor de la interoperabilidad entre administraciones.

Consecuentemente, la introducción de la innovación tecnológica, por ende, también blockchain, en el ámbito de la contratación pública está siendo un objetivo de los países de la Unión Europea para que estas herramientas doten de mayor eficiencia y eficacia a las compras públicas y permitan que exista una mayor transparencia e integridad para luchar contra la corrupción en un campo especialmente abonado para esta.

Al igual que se considera la compra pública como mecanismo estratégico para la consecución de objetivos de las políticas sociales y medioambientales, puede usarse la misma como palanca para la implementación de estas innovaciones en el sector público.

La contratación pública es un campo especialmente azotado por los efectos adversos de la corrupción, alterando la competencia en las licitaciones, reduciendo la eficiencia de las compras públicas y aumentando el gasto público. GIMENO FELIÚ[26] destaca que: «*la importancia económica y social de los contratos públicos aconseja reforzar la visión de compra pública desde la integridad, en tanto la realidad nos presenta como en este escenario concurren numerosos casos de corrupción y de prácticas clientelares, de las que derivan evidentes ineficiencias económicas y, por supuesto, pérdida de legitimación democrática de las instituciones administrativas y políticas*».

En este contexto, es evidente que no puede desdeñarse el potencial de blockchain como instrumento acreditativo, como registro inmutable y transparente, para lograr que los licitadores, o cualquier ciudadano, controlen los procedimientos de licitación, dotando, por ejemplo, de transparencia e inmutabilidad a la presentación de ofertas, o contribuyendo a la valoración automática de las ofertas —siempre que responda a criterios fácilmente traducibles a fórmulas matemáticas que permitan su programación en la red de blockchain—, o la ejecución automática de determinadas clausulas —también siempre que respondan a criterios fácilmente programables—.

Claramente, la necesidad de sencillez es un límite. La contratación pública es una materia compleja y sujeta a mucha casuística. Así, debemos ser cautelosos en la pretendida aplicación de la cadena de bloques. Tenemos ante nosotros una potente solución tecnológica y estamos ávidos de encontrar problemas a los que la misma pueda aplicarse, pero no es este un campo en el que realizar experimentos. Además, la introducción de soluciones basadas en blockchain va a requerir de cambios legislativos, máxime cuando aún carecemos de una regulación de la cadena de bloques que dé cobertura normativa a su implementación.

4. Iniciativas para la utilización de blockchain en la contratación del sector público español

Hasta el momento, como ya se ha señalado, faltan en nuestro país ejemplos de iniciativas públicas en las que el uso de blockchain sea una realidad, salvo el caso de Aragón en cuanto al establecimiento de un registro de ofertas.

Existen declaraciones de intenciones para promover su uso y proyectos para estudiar su posible implementación al registro de contratistas y a la evaluación automatizada de las

26. GIMENO FELIÚ, J.M. (2014): «Decálogo de Reglas para prevenir la corrupción en los Contratos Públicos». *Observatorio de la Contratación Pública*. Disponible en: http://www.obcp.es/opiniones/decalogo-de-reglas-para-prevenir-la-corrupcion-en-los-contratos-publicos

ofertas. En marzo de 2018, el Grupo Parlamentario del Partido Popular promovió en el Congreso de los Diputados una proposición no de ley con el objetivo de instar al gobierno a introducir la tecnología Blockchain en el sector público español[27, 28], ya que, como se expone en la propia proposición: «*[l]a Administración Pública también podría beneficiarse de estas tecnologías. La introducción de Blockchain —en las concesiones administrativas, en la contratación o en procesos internos— propiciará un mayor control, trazabilidad y transparencia en los procesos. Además, la utilización de esta tecnología también puede reportar ingresos extra a la Administración mediante el impulso de nuevos modelos de intercambio de derechos en sectores como el logístico, el turístico o las infraestructuras*.»

No obstante, los términos de la proposición son absolutamente genéricos, podría sustituirse blockchain por cualquier otra innovación tecnológica y la proposición continuaría siendo válida[29]. Una iniciativa ambiciosa en este sentido debe apostar por un planteamiento en el que se estudie el rediseño de los procedimientos para poder implantar la tecnología como las máximas garantías jurídicas para los administrados y con el adecuado soporte normativo. No puede obviarse que la implantación de esta tecnología requerirá modificaciones legislativas, con lo que más que una proposición no de ley habrá de hacerse a través de un proyecto o anteproyecto de ley.

Además, el alcance de una proposición no de ley es muy reducido, en la medida en que se trata de una mera manifestación en la función de control del Gobierno por el Congreso de los Diputados y carece de efectos jurídicos[30].

Ahora bien, durante la elaboración de este artículo, se ha dictado el Real Decreto-ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones (en adelante, RD-Ley 14-2019). Esta es la primera norma en la que se hace referencia a los registros distribuidos, y no es precisamente para potenciarlos, aunque las circunstancias de extraordinaria y urgente necesidad como son, de acuerdo con ALMONACID LAMELAS[31], la preocupación por el hecho de que el desarrollo tecnológico implica una mayor exposición a nuevas amenazas, especialmente las asociadas al ciberespacio, tales como el robo de datos e información, el hackeo de dispositivos móviles y sistemas industriales, o los ciberataques contra infraestructuras lícitas, así lo justifican.

El RD-Ley 14-2019 incorpora una disposición adicional sexta a la LPACAP, que prevé que en las relaciones de los interesados con las Administraciones Públicas no serán admisibles en ningún caso y, por lo tanto, no podrán ser autorizados, los sistemas de identificaciones basados en tecnologías de registro distribuido, es decir, en blockchain, y los sistemas de firma

27. BOCG núm. 321, de 20 de marzo de 2018.

28. Señalar que esta proposición no llegó a ser aprobada al disolverse antes de su aprobación las Cortes Generales.

29. BERNAL BLAY, M.A. (2018) Op. Cit.

30. BERNAL BLAY, M.A. (2018) Op. Cit.

31. ALMONACID LAMELAS, V. (2019): «*Comentarios de urgencia al Real Decreto-ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones*». Disponible en: https://nosoloaytos.wordpress.com/2019/11/05/comentarios-de-urgencia-al-real-decreto-ley-14-2019-de-31-de-octubre-por-el-que-se-adoptan-medidas-urgentes-por-razones-de-seguridad-publica-en-materia-de-administracion-digital-contratacion-del-se/ (última consulta: 01/12/2019).

basados en los anteriores, en tanto que no sean objeto de regulación específica por el Estado en el marco del Derecho de la Unión Europea. Además, establece que cualquier sistema de identificación basado en tecnología de registro distribuido que prevea la legislación estatal deberá contemplar que la Administración General del Estado actuará como autoridad intermedia que ejercerá las funciones que corresponda para garantizar la seguridad pública.

Las restricciones impuestas a los sistemas de identificaciones y firmas basados en tecnologías de registro distribuido en ningún caso suponen una prohibición general. Simplemente, se restringe puntualmente y de forma meramente provisional su uso como sistema de identificación y firma de los interesados cuando estos últimos se interrelacionan con la Administración y mientras no haya más datos o un marco regulatorio ad hoc de carácter estatal o europeo que haga frente a las debilidades que implica su uso para los datos y la seguridad pública.

En suma, por razones de seguridad, se ha producido una prohibición temporal del uso de la tecnología blockchain, en el ámbito de las Administraciones públicas, tanto para el establecimiento de registros como de sistemas de identificación, en tanto que se no realice una regulación de esta tecnología.

En el ámbito autonómico, en concreto en Aragón[32], se puso en marcha en 2018, encontrándose actualmente en pleno funcionamiento, un registro distribuido de ofertas de contratos públicos del Gobierno de Aragón. Este es un sistema de presentación de ofertas en el que se usa la tecnología blockchain como mecanismo para garantizar la integridad de las ofertas y su inmutabilidad, que como hemos visto son dos de las funcionalidades de la cadena de bloques. En el siguiente epígrafe, al hacer referencia a esta posible aplicación, se detallan alguno de los elementos del sistema[33, 34].

5. Propuestas de aplicación práctica de blockchain en la contratación pública

Una vez explicado qué es blockchain, cómo funciona y los posibles beneficios de su aplicación en esta materia, debe abordarse qué trámites del procedimiento de licitación pueden ser mejorados mediante la aplicación de la cadena de bloques y sus características de inmutabilidad, trazabilidad y transparencia.

32. Esta comunidad autónoma es la que más ha avanzado en la aplicación de blockchain en la contratación pública en nuestro país, e incluso me atrevería decir que a nivel europeo.

Además, el Gobierno Aragón aprobó en 2018 el Anteproyecto de Ley de uso estratégico de la contratación pública en Aragón, que decaería al disolverse las Cortes por el final de la legislatura, cuya disposición adicional tercera permitiría la implementación de la tecnología blockchain como medio, por un lado, para asegurar la integridad de los datos y documentos de cualquier expediente, procedimiento o registro de contratación pública y, por otro, para automatizar la tramitación de los citados procedimientos.

33. A juicio de este autor, el sistema implementado en Aragón no se ve afectado por la introducción de la disposición adicional sexta de la LPACAP por el RD-Ley 14/2019, ya que no estamos ni ante un registro —a pesar del nombre— ni ante un sistema de identificación. Este es un sistema para la presentación de ofertas que encuentra cobertura normativa como se verá en la Disposición Adicional Decimosexta, apartado h) de la LCSP.

34. Este proyecto es citado en el documento *«Blockchain for Government And Public Services»* elaborado por The European Union Blockchain Observatory & Forum, diciembre 2018. Disponible en: https://www.eublockchainforum.eu/sites/default/files/reports/eu_observatory_blockchain_in_government_services_v1_2018-12-07.pdf (última consulta: 01/12/2019).

Debe partirse del hecho de que la LCSP ha dado un paso importante en la digitalización de las licitaciones públicas. De acuerdo con lo dispuesto en la Disposición Adicional decimoquinta de la LCSP, actualmente, la presentación de ofertas, salvo que concurra alguno de los supuestos excepcionales recogidos en su apartado 4, debe realizarse a través de medios electrónicos. De esta forma, actualmente la regla general es que en las licitaciones se empleen medios electrónicos, informáticos y telemáticos.

Asimismo, puede destacarse el artículo 63 de la LCSP que obliga a los órganos de contratación a difundir exclusivamente a través de Internet en su perfil de contratante, donde se agrupa la información y documentos relativos a su actividad contractual al objeto de asegurar la transparencia y el acceso público a los mismos[35]. Esta publicación mejora la transparencia del procedimiento ya que el acceso a la información del perfil de contratante es libre sin requerir identificación previa (artículo 63.1 LCSP). Así, se disminuyen notablemente las posibilidades de corrupción o fraude.

Blockchain podrá aplicarse aportando inmutabilidad, trazabilidad y transparencia a las licitaciones en los siguientes puntos:

a) Registro de licitadores

Como ya se ha afirmado, en el futuro, en opinión de este autor, los registros administrativos utilizarán la tecnología blockchain para garantizar la transparencia, inmutabilidad y la trazabilidad de los mismos. En consecuencia, el actual Registro Oficial de Licitadores y Em-

35. De conformidad con los apartados 2 y 3 del artículo 63 de la LCSP, en el perfil del contratante se podrá incluir cualesquiera datos y documentos referentes a la actividad contractual de los órganos de contratación. En cualquier caso, deberá publicarse tanto la información de tipo general que puede utilizarse para relacionarse con el órgano de contratación como puntos de contacto, números de teléfono y de fax, dirección postal y dirección electrónica, informaciones, anuncios y documentos generales, tales como las instrucciones internas de contratación y modelos de documentos, así como la información particular relativa a los contratos que celebre.

Con respecto a la información relativa a cada licitación, al menos deberá publicarse en el perfil, la siguiente información:

a) La memoria justificativa del contrato, el informe de insuficiencia de medios en el caso de co ntratos de servicios, la justificación del procedimiento utilizado para su adjudicación cuando se utilice un procedimiento distinto del abierto o del restringido, el pliego de cláusulas administrativas particulares y el de prescripciones técnicas que hayan de regir el contrato o documentos equivalentes, en su caso, y el documento de aprobación del expediente.

b) El objeto detallado del contrato, su duración, el presupuesto base de licitación y el importe de adjudicación, incluido el Impuesto sobre el Valor Añadido.

c) Los anuncios de información previa, de convocatoria de las licitaciones, de adjudicación y de formalización de los contratos, los anuncios de modificación y su justificación, los anuncios de concursos de proyectos y de resultados de concursos de proyectos, con las excepciones establecidas en las normas de los negociados sin publicidad.

d) Los medios a través de los que, en su caso, se ha publicitado el contrato y los enlaces a esas publicaciones.

e) El número e identidad de los licitadores participantes en el procedimiento, así como todas las actas de la mesa de contratación relativas al procedimiento de adjudicación o, en el caso de no actuar la mesa, las resoluciones del servicio u órgano de contratación correspondiente, el informe de valoración de los criterios de adjudicación cuantificables mediante un juicio de valor de cada una de las ofertas, en su caso, los informes sobre las ofertas incursas en presunción de anormalidad a que se refiere el artículo 149.4 y, en todo caso, la resolución de adjudicación del contrato.

Igualmente serán objeto de publicación en el perfil de contratante la decisión de no adjudicar o celebrar el contrato, el desistimiento del procedimiento de adjudicación, la declaración de desierto, así como la interposición de recursos y la eventual suspensión de los contratos con motivo de la interposición de recursos.

presas Clasificadas del Sector Público terminará por usar blockchain y ser, por tanto, un registro distribuido.

Además, si se incorporan a este registro *smart contrats* —programas autoejecutables—, se podrá de una forma rápida y automatizada comprobar la capacidad de los licitadores, produciéndose la exclusión de aquellos que no poseen la exigida en los pliegos de manera inmediata.

Actualmente, dada la modificación introducida por el RD-Ley 14/2019, no se admite en nuestro ordenamiento este tipo de registro hasta que no sean objeto de regulación específica por el Estado en el marco del Derecho de la Unión Europea. Tendremos, por tanto, que esperar a que se produzca una regulación *ad hoc* de los registros distribuidos en el ámbito de las Administraciones públicas o se levante la prohibición impuesta para que esta propuesta pueda ser una realidad.

b) Identidad de los contratistas

Una de las aplicaciones de blockchain en la que se viene trabajando con más ahínco es la de la creación de una identidad inequívoca y dotada de confianza sobre registros distribuidos. Cabría, de esta forma, implementar en el ámbito de la contratación soluciones de identidad digital[36] gestionadas con la tecnología de la cadena de bloques. Así, en un registro distribuido se acumularían todos los atributos inherentes de una persona —en este caso, de los licitadores— tanto los acumulados por la misma, v.gr. etiquetas, como los que puedan ser asignados, v.gr. prohibiciones de contratar o ejecución de otros contratos.

Las ventajas de esta forma de identificación es que sería inmutable, una vez registrada en la misma una prohibición de contratar no habría forma de que el licitador pudiera ocultarla a los poderes adjudicadores con acceso a la red o pasar desapercibida a estos. Asimismo, los poderes adjudicadores conocerían la trazabilidad, con las fechas concretas, de todos los atributos identificativos del licitador.

Esta forma de identificación contenida en una red de blockchain permitiría a todos los poderes adjudicadores que actúen como nodos de la red comprobar de manera sencilla si un licitador cumple los requisitos exigidos en un determinado contrato. La extensión de esta comprobación dependerá de los atributos con que cuente la identidad registrada en la cadena de bloques. En principio es posible que la misma incorpore datos e informaciones relativos a la capacidad y a la solvencia, tanto económico y financiera, como técnica.

Para garantizar la privacidad, la red que opere sobre registros distribuidos incorporará todos los datos e informaciones públicas en relación con el contratista. v.gr. toda la información disponible sobre los mismos en registros públicos y administrativos. Con respecto a otros datos, el licitador los compartirá con el poder adjudicador en el momento de licitar el contrato, haciéndose constar el nivel de protección de los mismos[37].

36. Estas soluciones de identificación son conocidas por su nombre en inglés *«self-sovereign identity»*. Actualmente no existe una traducción aceptada del término en español, dados los problemas que plantea *«sovereign»* al traducirlo por soberana.

37. Aunque no es objeto de este trabajo no puede dejar de comentarse que en este tipo de soluciones de blockchain se deberá ser especialmente cuidadoso para que las mismas cumplan con todas las obligaciones establecidas en materia de protección de datos.

Con respecto a lo anterior, debe señalarse que la tecnología que aquí se analiza permite mediante la criptografía asimétrica, esto es, mediante el uso de una clave pública y otra privada, que están asociadas entre sí, que el licitador decida con quién comparte determinada información o documentación. Estos datos estarán cifrados, de tal forma que sólo aquellos nodos con los que el licitador comparta la clave privada podrán acceder a ellos[38].

Con respecto a lo anterior, debe destacarse que las iniciativas de *self sovereign identity* también se desarrollan para que los ciudadanos puedan decidir con quién compartir la multitud de datos que poco a poco van generando y que se van almacenando en internet, v.gr. redes sociales.

Esta forma de identificación incluiría en los registros distribuidos toda la información relativa a las prohibiciones de contratar. Así, mediante una sencilla automatización, podría excluirse de manera ágil y rápida a todos aquellos licitadores que estuvieran incursos en algunas de las prohibiciones de contratar.

Lo mismo ocurriría con respecto a la solvencia económica y financiera, para lo cual el licitador tendría, mediante un sistema de criptografía asimétrica, compartir con la Administración la información económica y financiera que considerase.

Asimismo, en relación con la solvencia técnica, en la red debería constar documentación e información relativa a los contratos ejecutados por la empresas, el número de trabajadores y sus currículos o todo aquello que fuera necesario.

También, es aplicable todo lo aquí expuesto al caso de la verificación de las etiquetas, es decir, de acuerdo con el artículo 127 de la LCSP, los documentos, certificados o acreditaciones que confirme que las obras, productos, servicios, procesos o procedimientos de que se trate cumplen determinados requisitos.

Disponiéndose de toda esta información en la red de blockchain, mediante un *smart contrat*, como se ha visto, que accede a todos estos datos se verificará de manera sencilla el cumplimiento de las capacidades y requisitos exigidos en la concreta licitación. Como ya se ha apuntado *ut supra,* el artículo 41 de la LRJSP permite la actuación administrativa automatizada siempre que se establezca previamente el órgano competentes para la definición de las especificaciones, programación, mantenimiento, supervisión y control de calidad y, en su caso, auditoría del sistema de información y de su código fuente y se indique el órgano que debe ser considerado responsable a efectos de impugnación.

Como puede comprobarse, esto no es más que una extensión de la aplicación referida en la letra anterior. De igual manera, actualmente, debido a la reciente introducción de la disposición adicional sexta de la LPACAP, que declara no admisibles los sistemas de identificación basados en registros distribuidos, esta aplicación no es posible, al menos hasta que se regulen estos registros.

38. PONCE DE LEÓN, P.J. (2018). «Blockchain, un nuevo patrón tecnológico». En: VILLAROIG MOYA R. y PASTOR SEMPERE, C. (dirs.). *Blockchain: aspectos tecnológicos, empresariales y legales.* Cizur Menor (Navarra): Thomson Reuters-Aranzadi, pp. 35-77.

c) El uso de blockchain para la presentación de ofertas

Esta aplicación ya es una realidad en Aragón en algunos procedimientos abiertos simplificados abreviados (artículo 159.6 de la LCSP).

Permítanme, antes de continuar con esta posible aplicación, que haga mención al hecho de que con la actual regulación de la LCSP, la tecnología que aquí se expone es aplicable especialmente a los procedimientos abiertos simplificados abreviados, entre otras cosa, porque no se dispone que la apertura del único sobre que debe presentarse se haga en acto público, porque la valoración se hace exclusivamente con una fórmula.

En esta posible aplicación se aprovechan la inmutabilidad, una vez presentada la oferta ya no es modificable, y la transparencia, es por todos conocida la fecha y hora de presentación de la misma, propias de la tecnología blockchain. Desaparecerá cualquier duda sobre la custodia y posible modificación de las ofertas desde que son presentadas hasta que se realiza su valoración.

Esto encuentra una precisa cobertura normativa en la Disposición Adicional Decimosexta, apartado h) de la LCSP, la cual dispone que «*en los procedimientos de adjudicación de contratos, el envío por medios electrónicos de las ofertas podrá hacerse en dos fases, transmitiendo primero la huella electrónica de la oferta, con cuya recepción se considerará efectuada su presentación a todos los efectos, y después la oferta propiamente dicha en un plazo máximo de 24 horas. De no efectuarse esta segunda remisión en el plazo indicado, se considerará que la oferta ha sido retirada*».

En consecuencia, la presentación se hace en dos fases, en la primera, se produce el registro de la huella electrónica[39] y con posterioridad, se envía la oferta. En la primera fase, el licitador una vez que se ha identificado debidamente —bien con un sistema basado también en blockchain o con alguno de los actualmente admitidos en la LPACAP[40]— presenta la oferta en el sistema generándose una huella electrónica, con la terminología propia de la tecnología blockchain, un *hash*. Se generará además en el sistema un registro del momento exacto en que la oferta ha sido presentada, tanto para el órgano de contratación como para el resto de licitadores.

Con posterioridad, el licitador enviará la oferta. Debido a las garantías de inmutabilidad de blockchain, si el licitador ha modificado la oferta esta dará lugar a un hash distinto con lo que quedaría excluido. Durante este periodo, el órgano de contratación no tiene el deber de custodiar las ofertas. En este sentido, la normativa, en concreto el la Disposición Adicional Decimosexta, apartado h) de la LCSP, debería modificarse para establecer que las ofertas podrán mandarse hasta el momento de apertura de las mismas, y no en el plazo de 24 horas.

39. De acuerdo con la Disposición Adicional Decimosexta, apartado h) de la LCSP: «*Se entiende por huella electrónica de la oferta el conjunto de datos cuyo proceso de generación garantiza que se relacionan de manera inequívoca con el contenido de la oferta propiamente dicha, y que permiten detectar posibles alteraciones del contenido de esta garantizando su integridad. Las copias electrónicas de los documentos que deban incorporarse al expediente, deberán cumplir con lo establecido a tal efecto en la legislación vigente en materia de procedimiento administrativo común, surtiendo los efectos establecidos en la misma*».

40. El sistema implementado en Aragón usa estos últimos.

Además de las mejoras que puede traer esta posibilidad en cuanto a la integridad y trazabilidad del procedimiento, técnicamente la presentación sería más rápida y sencilla —en el modelo implementado en este sentido en Aragón el tiempo de presentación es inferior a los dos minutos— y no habría problema en la carga de los archivos por su tamaño.

d) Valoración de las ofertas

Si las ofertas presentadas deben valorarse tan sólo mediante criterios recogidos en una fórmula, esta valoración puede automatizarse mediante un *smart contrat*. De tal forma, que si combinamos lo aquí propuesto con lo que se indica en la letra anterior en referencia a la presentación de ofertas, serían prescindibles trámites como la apertura de los sobre e incluso la intervención de la mesa de contratación en estos supuestos.

Ahondando en el supuesto de los procedimientos abiertos simplificados abreviados, el artículo 159.6.d) de la LCSP dispone que «*[l]a valoración de las ofertas se podrá efectuar automáticamente mediante dispositivos informáticos, o con la colaboración de una unidad técnica que auxilie al órgano de contratación*». Esto determina que a todo lo expuesto *ut supra* en relación con la presentación de ofertas con blockchain pueda ampliarse la aplicación de esta tecnología mediante un *smart contrat* que valore dichas ofertas —todo ello en procedimientos abiertos simplificados abreviados—.

Téngase en cuenta que actualmente encontramos límites a la aplicación de esta propuesta ya que tanto en el procedimiento abierto[41] como en el procedimiento abierto simplificado[42] se dispone la apertura en acto público de los sobres. A mi juicio, en estos casos no podría incorporarse la valoración automática de las ofertas, puesto que la apertura de los sobres no sería pública y estos procedimientos de licitación tendrían por tanto una tacha de invalidez.

Cuando existan criterios de adjudicación cuya cuantificación dependa de un juicio de valor no será posible su automatización ya que estos criterios no son reducibles a un código informático.

e) Ejecución de los contratos

Con el estado actual de la tecnología, el uso de blockchain, en la fase de ejecución, quedaría reducido a la automatización de las prestaciones, como señala MUÑOZ CARMONA[43].

Esta aplicación podría ser de utilidad en los contratos menores del artículo 118 de la LCSP[44]. De tal forma, que a través del *IoT* pudiera verificarse fácilmente la realización de la prestación y automatizarse el pago. Un ejemplo de esta aplicación, en el ámbito de la contratación

41. El artículo 157.4 de la LCSP dispone que *«[e]n todo caso, la apertura de la oferta económica se realizará en acto público, salvo cuando se prevea que en la licitación puedan emplearse medios electrónicos»*.

42. El artículo 159.4.d) de la LCSP establece que *«[e]n todo caso, será público el acto de apertura de los sobres que contengan la parte de la oferta evaluable a través de criterios cuantificables mediante la mera aplicación de fórmulas establecidas en los pliegos»*.

43. MUÑOZ CARMONA, A. (2018). Op. Cit.

44. Téngase en cuenta las dificultades de extender esta automatización a los contratos mayores. ¿Cómo podría realizarse en esos casos las funciones del órgano fiscalizador en cuanto a la comprobación material de la inversión?

privada, se da en contratos de transporte en los que cuando el medio de transporte alcanza la una determinada geolocalización, verificable por medios electrónicos, se realiza automáticamente el pago.

No obstante, como se ha afirmado dado el estado de maduración de la tecnología, la aplicación actual podría darse tan solo en supuestos muy sencillos.

Por otro lado, constituye un freno a la automatización de la fase de ejecución, el hecho de que en los contratos administrativos no hay una igualdad de partes como en la contratación privada. Así, los contratos administrativos tienen importantes peculiaridades derivadas de la presencia de una persona jurídica dotada de *imperium* como son las Administraciones públicas. Y, es que el posible ejercicio por parte de la Administración de las prerrogativas enumeradas en el artículo 190 LCSP hace que difícilmente puedan automatizarse o reducirse a un *smart contract*.

Asimismo, en los casos de cumplimiento defectuoso, es decir, cuando el contratista, por causas imputables al mismo, hubiere incumplido parcialmente la ejecución de las prestaciones definidas en el contrato, la Administración podrá optar, atendidas las circunstancias del caso, por su resolución o por la imposición de las penalidades que, para tales supuestos, se determinen en el pliego de cláusulas administrativas particulares o en el documento descriptivo (artículo 192.2 de la LCSP). Esto, como puede comprenderse, tampoco podrá automatizarse. Incluso, aunque en los pliegos se definiese de manera precisa, objetivándose, cuando la Administración debe optar por la imposición de penalidades y en qué cuantía, es imposible su automatización. De acuerdo con lo que dispone la reciente Sentencia del Tribunal Supremo, Sala Tercera, Sección 4ª, de 21 de mayo de 2019 (nº. de recurso 1372/2017) en la imposición de penalidades debe existir una tramitación mínima, en la que haya una propuesta, un trámite de audiencia y una decisión para evitar la indefensión del penalizado. Esto es, si se automatiza la imposición de la penalidad, no habrá trámite de audiencia y se estará ante una nulidad de pleno derecho conforme a lo dispuesto en el artículo 47.1.e) de la LPACAP, al prescindirse de un trámite esencial para que el contratista pueda defender sus derechos.

Además, en aquellos casos, en que la realización de la prestación objeto del contrato no sea verificable de manera sencilla y mediante mediciones objetivas, resulta imposible automatizar la ejecución. Reitero, los contratos inteligentes o *smart contracts* podrán establecerse cuando pueda configurarse previamente, reduciéndose a un código informático, los presupuestos para considerar debidamente ejecutada la prestación del contrato, para que una vez verificados, haciendo uso del IoT, se produzca el pago por la mera ejecución del código.

6. Conclusión

Blockchain es una tecnología con un enorme potencial para mejorar la eficiencia y la integridad de la contratación pública, no obstante debido a la legislación existente y la escasa maduración de la tecnología, se encuentran importantes límites a su aplicación. En la actualidad, es ideal para procedimientos abiertos simplificados abreviados o para el diseño de sistemas de presentación de ofertas. En el futuro, oiremos hablar mucho de esta innovación en el ámbito de la contratación pública pero para ello se necesitaran cambios normativos y probablemente la regulación de la cadena de bloques.

7. Bibliografía

ALMONACID LAMELAS, V. (2019): *«Comentarios de urgencia al Real Decreto-ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones»*. Disponible en: https://nosoloaytos.wordpress.com/2019/11/05/comentarios-de-urgencia-al-real-decreto-ley-14-2019-de-31-de-octubre-por-el-que-se-adoptan-medidas-urgentes-por- razones-de-seguridad-publica-en-materia-de-administracion-digital-contratacion-del-se/ (última consulta: 01/12/2019).

ANGUIANO JIMÉNEZ, J. M. «Blockchain: Fundamentos y perspectiva jurídica. De la confianza al consenso». *Diario La Ley*. N.º 18. Editorial Wolters Kluwer. Madrid. 2018.

BERNAL BLAY, M.A. (2018). *Blockchain, Administración y contratación pública*. Disponible en: http://www.obcp.es/index.php/mod.opiniones/mem.detalle/id.418/relcategoria.208/chk.5d7064a2b9f6eb58024d2d1d4706c591 (última visita: 01/12/2019).

BOUCHER, P (2017): «How blockchain could change our lives», *In-deph Analysis*, European Parlamentary Research Service.

COLLINS, A. (2017) *«Four reasons to question the hype around blockchain»*. Disponible en: https://www.weforum.org/agenda/2017/07/four-reasons-to-question-the-hype-around-blockchain/ (última visita: 01/12/2019).

FELIU REY, J. (2018): «Smart Contract: Concepto, ecosistema y principales cuestiones de Derecho privado». *La Ley Mercantil*. N.º 47. Wolters Kluwer. Madrid.

GARCÍA GIL, V. J. (2016): *«De qué hablamos cuando hablamos de "smart contracts"»*. Disponible en: https://blogs.elconfidencial.com/espana/blog-fide/2018-04-26/smart-contracts_1555216/ (última visita: 01/12/2019).

GARCÍA MELIÁN, J.C. (2019). «Blockchain y contratación pública estratégica», *Contratación Administrativa Práctica*. N.º 159.

GARCÍA MELIÁN, J.C. (2018). *Blockchain y smart contracts para la transparencia y confidencialidad de los contratos públicos*. Disponible en: https://mymabogados.com/blockchain-en-la-contratacion (última visita: 01/12/2019).

GIMENO FELIÚ, J.M. (2014): «Decálogo de Reglas para prevenir la corrupción en los Contratos Públicos». *Observatorio de la Contratación Pública*. Disponible en: http://www.obcp.es/opiniones/decalogo-de-reglas-para-prevenir-la-corrupcion-en-los-contratos-publicos (última visita: 01/12/2019).

GONZÁLEZ MENESES-GARCÍA-VALDECASAS, M. *Enteder blockchain. Una introducción a la tecnología de registro distribuido*. Thomson Reuters-Arazandi. Cizur Menor (Navarra). 2017.

PASTOR SEMPERE, M.C. (2017): «Criptodivisas: ¿una nueva disrupción jurídica en la Eurozona?». *Revista de Estudios Europeos*. N.º 70. Instituto de Estudios Europeos de la Universidad de Valladolid. Valladolid.

PORXAS, N. y CONEJERO, M (2018): «Tecnología blockchain: Funcionamiento, aplicaciones y retos jurídicos relacionados», *Actualidad Jurídica Uría Menéndez*.

TUR FAÚNDEZ, C: *Smart contrats, análisis jurídico*, Editorial Reus, Madrid, 2018

VILLAROIG MOYA R. y PASTOR SEMPERE, C. (dirs.). *Blockchain: aspectos tecnológicos, empresariales y legales*. Cizur Menor (Navarra): Thomson Reuters-Aranzadi.

Auditoría de la ciberseguridad de los principales ayuntamientos de la Comunidad Valenciana

ANTONIO MINGUILLÓN ROY
Auditor director del Gabinete Técnico de la Sindicatura de Cuentas de la Comunidad Valenciana

CARLOS GARCÍA BURGOS
Auditor de Sistemas de Información de la Sindicatura de Cuentas de la Comunidad Valenciana

JORGE SOLER IRANZO
Auditor de Sistemas de Información de la Sindicatura de Cuentas de la Comunidad Valenciana

RESUMEN

La Sindicatura de Cuentas de la Comunidad Valenciana, en respuesta al imparable crecimiento de los ciberriesgos y las amenazas del ciberespacio que comprometen el buen funcionamiento y la prestación de los servicios públicos a los ciudadanos, ha realizado una auditoría de los controles básicos de ciberseguridad de los quince principales ayuntamientos de la Comunitat Valenciana.

Para ello se ha utilizado metodología basada en las mejores prácticas recogidas en las guías de fiscalización de los OCEX sobre ciberseguridad, que están totalmente alineadas con lo establecido en el Esquema Nacional de Seguridad. Cada informe ha reunido en un análisis la valoración sobre el nivel de madurez de los controles de ciberseguridad implantados por las entidades y su cumplimiento normativo.

Los resultados obtenidos muestran que los ayuntamientos no disponen de controles de ciberseguridad eficaces que garanticen la protección de sus sistemas de información de forma satisfactoria y que el cumplimiento de la legalidad es insuficiente, situación que pone en riesgo a los servicios, datos y activos de información de las entidades auditadas.

Las deficiencias de control identificadas ponen de manifiesto la necesidad de inversiones sostenidas y de un mayor compromiso de los órganos de gobierno con la seguridad de los sistemas de información y las comunicaciones.

PALABRAS CLAVE

Ayuntamientos | ciberseguridad | ciberhigiene | ciberamenazas | ENS

ABSTRACT

The Sindicatura de Cuentas de la Comunidad Valenciana, in response to the unstoppable growth of cyber-risks and cyberspace threats that compromise the proper functioning and provision of public services to citizens, has carried out an audit of the basic cybersecurity controls of the fifteen main municipalities of the Valencian Community.

The methodology employed is based on the best practices contained in the OCEX audit guidelines on cybersecurity, which are fully aligned with the regulatory framework provided by National Security Scheme. Each report holds an analysis that assess the maturity level of cybersecurity controls implemented by the entities and their regulatory compliance.

The results shows that municipalities do not have effective cybersecurity controls able to successfully ensure the protection of their information systems and that legal compliance is inadequate, a situation that puts at risk the services, data and information assets of the audited entities.

The control deficiencies identified highlight the need for sustained investment and greater commitment of governing bodies to the security of information and communications systems.

KEYWORDS

Town halls | *cybersecurity* | *cyber-hygiene* | *cyberthreats* | *ENS*

1. Introducción

Nuestra sociedad y en particular las administraciones públicas están haciendo un uso cada vez más extenso e intenso de las tecnologías de la información y las comunicaciones (TIC). Las Leyes 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, representan la consolidación desde el punto de vista jurídico de esta tendencia en todas las entidades públicas. Como consecuencia de la aplicación de dichas leyes, todas las entidades locales están inmersas en procesos de transformación en la forma de prestación de los servicios a los ciudadanos y de la gestión pública, para un pleno despliegue de la administración electrónica sustentada en sistemas de información cada vez más complejos tecnológicamente e interconectados.

La crisis desencadenada por la epidemia COVID-19 no solo no ha frenado esta tendencia, sino que, entre otras muchas cuestiones, ha puesto de manifiesto que las administraciones públicas han sido capaces de mantener gran parte de su actividad confiando en el buen funcionamiento y la eficacia de los sistemas de información y comunicaciones (SIC). Obligados por el confinamiento decretado por el Gobierno de la Nación para hacer frente a la epidemia, todas las administraciones han recurrido al trabajo en remoto, en sus distintas modalidades técnicas, para mantener su actividad en niveles razonables. Este importante salto cualitativo, impensable en condiciones normales, ha sido posible gracias a unos sistemas de información y comunicaciones ampliamente desarrollados, cuanto más avanzados y basados en las distintas modalidades de computación en la nube, por ejemplo, más resilientes han sido las organizaciones en las actuales circunstancias.

Toda esta situación no ha hecho sino poner en clara evidencia la absoluta dependencia de las TIC que existe actualmente en la gestión pública, el creciente grado de vulnerabilidad de nuestras administraciones frente a los ciberataques y que mantener una adecuada ciberhigiene y un sólido sistema de protección frente a aquellos es más necesario que nunca.

La generalización del trabajo en remoto tiene como contrapartida de su eficiencia un fuerte aumento de la superficie de exposición frente a las ciberamenazas al que las entidades públicas tienen que hacer frente con las dificultades propias de un periodo de crisis. Cuanto mayor sea el uso y la dependencia de las TIC en la gestión pública mayor importancia debe concederse a las cuestiones relativas a la ciberseguridad.

Se han oído y leído muchas advertencias en este sentido durante estas semanas de confinamiento, valgan como ejemplo los comentarios de Alberto Dasca, director de Risk Advisory especializado en ciberseguridad de Deloitte[1]: *«En estas épocas de incertidumbre, causada por el coronavirus, todos utilizamos con mucha más frecuencia la tecnología para contactar con nuestros amigos, familiares o colegas. El cibercrimen se aprovecha del pánico causado por la crisis para incrementar los ciberataques, comprometiendo la seguridad de empresas y usuarios. Desde el área de ciberseguridad de Deloitte estamos observando un incremento de amenazas que facilitan el fraude, los ataques relacionados con malware y el robo de credenciales, utilizando para ello dominios relacionados con el coronavirus.»*

1. DASCA, ALBERTO; «La otra amenaza del coronavirus», *Diari de Tarragona,* 30 de marzo de 2020.

No solo se produce este fenómeno en nuestro país[2], como señalan Pipikaite y Davies[3] *«a medida que la pandemia de coronavirus sigue perturbando los sistemas mundiales de salud, económicos, políticos y sociales, hay otra amenaza invisible en aumento en el espacio digital: el riesgo de ataques cibernéticos que se aprovechan de nuestra mayor dependencia de las herramientas digitales y de la incertidumbre de la crisis…*

En una pandemia de esta escala, con casos de coronavirus registrados en más de 150 países, la dependencia de las comunicaciones digitales se multiplica. Internet se ha convertido casi instantáneamente en el canal para la interacción humana efectiva y la forma principal en que trabajamos, nos contactamos y nos apoyamos mutuamente.

Las empresas y las organizaciones del sector público están ofreciendo o aplicando cada vez más políticas de «teletrabajo», y las interacciones sociales se están limitando rápidamente a las videollamadas, las publicaciones en las redes sociales y los programas de chat. Muchos gobiernos están difundiendo información a través de medios digitales.

En este contexto actual sin precedentes, un ataque cibernético que priva a las organizaciones o familias del acceso a sus dispositivos, datos o Internet podría ser devastador e incluso mortal: en el peor de los casos, los ataques cibernéticos de base amplia podrían causar fallos de infraestructura generalizados que desconecten a comunidades o ciudades enteras, poniendo obstáculos a los proveedores de atención médica, los sistemas públicos y las redes.»

Volviendo a la situación en nuestro entorno más cercano, los **riesgos** para los sistemas de información y comunicaciones que soportan los procesos de la administración electrónica aumentan a medida que las amenazas a la seguridad provenientes del ciberespacio evolucionan continuamente y aparecen ataques nuevos cada vez más sofisticados y destructivos que obligan a los entes públicos a hacerlas frente de forma proactiva y sistemática, estableciendo mecanismos de defensa que en su fundamento están articulados mediante el Esquema Nacional de Seguridad, de aplicación obligatoria para todo el sector público.

Es imperativo que los responsables de los entes públicos gestionen esos riesgos y establezcan controles de ciberseguridad adecuados para mantener los sistemas de información protegidos frente a las amenazas de seguridad.

Abundando en esta idea, en la conferencia inaugural de los XIII Encuentros Técnicos de los OCEX, impartida por Javier Candau, jefe del Servicio de Ciberseguridad del Centro Criptológico Nacional, se destacó que **en los entornos de administración electrónica, en los que todos los entes públicos desarrollan actualmente sus funciones, es una necesidad ineludible adoptar medidas eficaces para hacer frente a las cada vez más ubicuas ciberamenazas,** tal como queda recogida en las concusiones de los Encuentros[4].

2. «Pandemic profiteering how criminals exploit the COVID-19 crisis», EUROPOL, marzo 2020.

3. PIPIKAITE, ALGIRDE; DAVIS, NICOLAS; «¿Por qué la ciberseguridad es más importante que nunca durante la pandemia de coronavirus?», *World Economic Forum,* 27 marzo 2020.

4. Véanse dichas conclusiones en el documento de Conclusiones de los XIII Encuentros Técnicos de los OCEX 2019 o en la *Revista de Auditoría Pública,* n.º 74, noviembre 2019.

2. Ciberriesgos y los auditores públicos

Pero los ciberriesgos, además de afectar directamente a todos los entes públicos, afectan de forma importante a la actividad de los auditores públicos a la hora de abordar la fiscalización de una entidad que opera en un entorno de administración electrónica avanzado, es decir, todos los entes públicos de tamaño mediano o grande.

En la guía de auditoría *GPF-OCEX 5311 Ciberseguridad, seguridad de la información y auditoría externa*, aprobada por la Conferencia de Presidentes de ASOCEX en 2017, ya se destacaba la importancia creciente que las cuestiones relacionadas con la ciberseguridad estaban adquiriendo en la gestión de las administraciones públicas, razón por la que **los auditores públicos deben prestar cada vez más atención a dichas cuestiones.** En el curso de los ya mencionados XIII Encuentros Técnicos de los OCEX se insistió en la necesidad que tienen las instituciones de control externo (ICEX) de incorporar en sus actuaciones la revisión de los controles de ciberseguridad, con el objetivo de evaluar el nivel de protección de la información y de los sistemas de las entidades fiscalizadas frente a las graves consecuencias de las amenazas de ciberseguridad.

La ciberseguridad se ha convertido en uno de los temas más relevantes tanto para los gobiernos, en un nivel más general y amplio, como para los gestores públicos y privados, y por supuesto para los auditores, dada la potencial repercusión que las amenazas a la seguridad de los sistemas de información representan sobre las cuentas que se auditan[5] y sobre la misma continuidad de la actividad y la prestación de servicios públicos.

3. Qué ha auditado la Sindicatura de Cuentas de la Comunidad Valenciana

La Sindicatura de Cuentas no es indiferente ante esta problemática y consciente de la creciente dependencia de los SIC y del riesgo que representan las ciberamenazas, en el Plan Estratégico de la Sindicatura para el periodo 2019-2022, aprobado en diciembre de 2018, se señala **a la ciberseguridad como una de las áreas de alto riesgo y prioritarias para llevar a cabo su tarea fiscalizadora.**

Considerando además que las entidades locales no son ajenas a la problemática planteada por la ciberseguridad, el Consejo de la Sindicatura incluyó en los Programas Anuales de Actuación de 2019 y 2020 la realización de un informe sobre los controles básicos de ciberseguridad (CBCS) de los principales ayuntamientos de la Comunitat Valenciana (CV) para evaluar su preparación frente a este tipo creciente de riesgos.

Conviene destacar que la ley reguladora de la Sindicatura establece que, en el desarrollo de su función fiscalizadora, la Sindicatura de Cuentas está facultada para **verificar la seguridad y fiabilidad de los sistemas informáticos** que soportan la información económico-financiera, contable y de gestión.

5. MINGUILLÓN ROY, ANTONIO; «El control externo y la auditoría de sistemas de información», *Revista Española de Control Externo,* vol. XVIII, n.º 53, mayo de 2016.

Así se han auditado los CBCS de los 15 ayuntamientos de mayor población (superior a los 50.000 habitantes) de la CV. En el siguiente cuadro pueden verse los entes auditados con los datos de población de 2018 y las obligaciones reconocidas netas (ORN) de 2018. Tanto en población como en presupuesto, los ayuntamientos auditados representan casi la mitad de todos los de la CV.

AYUNTAMIENTO	POBLACIÓN	ORN *(mill. euros)*
Valencia	791.413	1.046,1
Alicante	331.577	287,2
Elche	230.625	187,4
Castellón	170.888	172,9
Torrevieja	82.599	64,8
Torrent	81.245	52,7
Orihuela	76.778	72,1
Gandía	73.829	92,9
Paterna	69.156	65,4
Benidorm	67.558	94,7
Sagunto	65.669	64,2
Alcoy	58.977	56,6
San Vicente del Raspeig	57.785	36,9
Elda	52.404	35,6
Villarreal	50.577	53,8
Ayuntamientos auditados	**2.261.080**	**2.383,3**
Total ayuntamientos CV	**4.963.703**	**4.917,0**
Cobertura de la auditoría	**45,6%**	**48,5%**

Fuente: *Ministerio de Hacienda. Liquidaciones de los presupuestos del ejercicio 2018. Datos actualizados 31/07/2019. (https://serviciostelematicosext.minhap.gob.es/SGCAL/CONPREL).*
Las *obligaciones reconocidas netas* es información consolidada obtenida de la Liquidación de cada Entidad local, que recoge la información de la Administración General de la Entidad local y la relativa a sus Organismos Autónomos.

4. Qué son los controles básicos de ciberseguridad

La auditoría realizada ha estado basada en la Guía práctica de fiscalización de los OCEX ***GPF-OCEX 5313 Revisión de los controles básicos de ciberseguridad (CBCS)*** aprobada por la Conferencia de Presidentes de ASOCEX el 12/11/2018. Para mayor detalle sobre los controles de ciberseguridad y la metodología utilizada nos remitimos a esa guía que está accesible en la página web de ASOCEX, y en el Manual de fiscalización de la Sindicatura de Cuentas de la CV[6].

El contenido de la GPF-OCEX 5313, fundamentalmente relacionado con la auditoría de la seguridad de los sistemas de información, **es totalmente coherente con los postulados del ENS, que es de obligado cumplimiento para todos los entes públicos.** Esta alineación ha facilitado la realización de las auditorías de ciberseguridad por la Sindicatura y coadyuva a la implantación del ENS en los entes auditados, ya que prácticamente todos los subcontroles o controles detallados que ha revisado la Sindicatura están exigidos por el ENS.

6. Manual de fiscalización de la Sindicatura de Comptes de la Comunitat Valenciana.

Dada la amplitud del ENS, que está formado por 75 medidas de seguridad, y la gran cantidad de tiempo que requiere su auditoría, se seleccionó una serie limitada de controles para su inclusión en los CBCS. Para seleccionar los más relevantes, en la GPF- OCEX 5313, se atendió al marco conceptual establecido por la prestigiosa organización Center for Internet Security[7], que prioriza y clasifica los controles según su importancia para hacer frente a las ciberamenazas.

Siguiendo esta guía, la auditoría se ha centrado en el análisis de la situación de los ocho CBCS, que debidamente referenciados con el ENS son:

CONTROL		MEDIDA DE SEGURIDAD DEL ENS
CBCS 1	Inventario y control de dispositivos físicos	op.exp.1
CBCS 2	Inventario y control de *software* autorizado y no autorizado	op.exp.1 op.exp.2
CBCS 3	Proceso continuo de identificación y remediación de vulnerabilidades	mp.sw.2 op.exp.4
CBCS 4	Uso controlado de privilegios administrativos	op.acc.4 op.acc.5
CBCS 5	Configuraciones seguras del *software* y *hardware*	op.exp.2 op.exp.3
CBCS 6	Registro de la actividad de los usuarios	op.exp.8 op.exp.10
CBCS 7	Copias de seguridad de datos y sistemas	mp.info.9
CBCS 8	Cumplimiento de la legalidad *(ENS, RGPD/LOPD y Ley 25/2013)*	--

Los CBCS son controles globales formados por varios subcontroles detallados, que en total suman 26.

5. Qué se ha revisado

El objetivo general de las auditorías ha sido proporcionar una evaluación sobre el grado de ciberseguridad y ciber-resiliencia de los principales ayuntamientos de la Comunitat Valenciana y sobre el cumplimiento de la normativa en materia de seguridad de los sistemas de información.

Con esta finalidad el trabajo de auditoría ha consistido en:

- El análisis del diseño y la eficacia operativa de los CBCS implantados en los ayuntamientos.
- La identificación de deficiencias de control interno que puedan afectar negativamente a la integridad, disponibilidad, autenticidad, confidencialidad y trazabilidad de los datos, la información y los activos de los sistemas de información de esas entidades.
- La determinación del nivel de madurez existente en cada uno de los CBCS y a nivel general en cada uno de los ayuntamientos auditados y sus respectivos índices de cumplimiento.
- La identificación de incumplimientos significativos de la normativa sobre seguridad de la información.

7. www.cisecurity.org

Dada la gran amplitud, complejidad y diversidad de los sistemas de información y comunicaciones que los ayuntamientos tienen desplegados, ha sido necesario delimitar y concretar qué parte de estos se iban a analizar. En este sentido, de cada entidad hemos analizado las aplicaciones que soportan dos de los procesos de gestión más relevantes: la gestión contable y presupuestaria y la gestión tributaria y recaudatoria.

Además, por su importancia para el buen funcionamiento de los SIC, en cada ente hemos analizado también una selección de los siguientes tipos de elementos:

- Controlador de dominio.
- Software de virtualización.
- Equipos de usuario.
- Elementos de la red de comunicaciones (*router*, *switches*, punto de acceso a red *wifi*, etc.).
- Elementos de seguridad (*firewall, IPS, proxy* de correo, *proxy* de navegación, servidores de autenticación, infraestructura de generación de certificados, etc.).

Todas nuestras comprobaciones han tenido por finalidad verificar la situación real, basada en las evidencias obtenidas en la entidad, no la teórica recogida en sus normas internas pero no aplicada, y contrastarla con las buenas prácticas recogidas en la GPF-OCEX 5313.

Los resultados de las auditorías muestran la situación real de los ayuntamientos en un periodo que abarca el segundo semestre de 2019 y el primero de 2020, finalizando los últimos informes en pleno aislamiento por la epidemia de COVID-19, haciendo pleno uso de las herramientas de comunicaciones y teletrabajo con total satisfacción[8].

Dado el carácter limitado de la revisión, el objetivo no ha consistido en emitir una conclusión de carácter general sobre la confianza que merecen los controles de ciberseguridad existentes en el conjunto de los sistemas de información de los ayuntamientos auditados. No obstante, la auditoría proporciona información relevante sobre el grado de ciberseguridad y ciber-resiliencia de las entidades y sobre las posibles acciones de mejora que deberían acometer para subsanar las deficiencias observadas y alcanzar los niveles de madurez establecidos como objetivos en las buenas prácticas y en el ENS.

6. Metodología utilizada

La auditoría ha sido realizada por la Unidad de Auditoría de Sistemas de Información de la Sindicatura de Comptes (UASI)[9], siguiendo la metodología establecida en la guía práctica de fiscalización de los OCEX *GPF-OCEX 5313 Revisión de los controles básicos de ciberseguridad* (en el número 73 de la revista Auditoría Pública[10] se hizo una pequeña reseña de esta guía).

Dado que la información utilizada en la auditoría y los resultados detallados de la misma tienen un carácter sensible y pueden afectar a la seguridad de los sistemas de información

8. VPN, correo electrónico, ORVE, Microsoft Teams, TeamMate, etc.

9. El equipo de auditoría ha estado formado por los autores de este artículo.

10. Las nuevas guías prácticas de fiscalización de los OCEX, unas guías de auditoría de la administración electrónica para el siglo XXI.

de las entidades revisadas, los resultados de cada uno de los controles detallados solo se han comunicado con carácter confidencial a los responsables de aquellas para que puedan adoptar las medidas correctoras que consideren precisas. En los informes los resultados se muestran de forma sintética.

7. Cómo se ha medido la eficacia de los CBCS y el estado de la ciberseguridad de los ayuntamientos

La situación de los CBCS se ha evaluado en cada ayuntamiento a tres niveles:

- Subcontrol
- Control principal o CBCS
- Global del ayuntamiento

Los CBCS son controles generales compuestos por varios controles detallados o subcontroles, de los que se ha revisado su **diseño y eficacia operativa real.** El trabajo de auditoría ha consistido básicamente en revisar y evaluar la situación de cada subcontrol en función de los resultados de las pruebas realizadas y las evidencias obtenidas. Los aspectos que se comprueban en cada CBCS se especifican con el máximo detalle en la GPF-OCEX 5313.

Hemos evaluado la situación de los CBCS utilizando el **modelo de nivel de madurez** de los procesos ya que, además de ser un sistema ampliamente aceptado, permite establecer objetivos, medir el grado de cumplimiento con esos objetivos, realizar comparaciones entre distintas entidades y ver la evolución a lo largo del tiempo. Para evaluar el nivel de madurez de cada CBCS se han tenido en cuenta los resultados obtenidos en la revisión de los subcontroles que lo forman y considerando la ponderación o importancia relativa que les asignamos para el cumplimiento del objetivo de control del CBCS.

La metodología utilizada, de acuerdo con la *GPF-OCEX 5313*, está plenamente alineada con lo establecido en la *Guía de seguridad CCN-STIC 804* del Centro Criptológico Nacional, usando una escala, según se resume en el siguiente cuadro.

NIVEL	ÍNDICE	DESCRIPCIÓN
N0 **Inexistente**	0	El CBCS no está siendo aplicado en este momento
N1 **Inicial /ad hoc**	10	El proceso existe, pero no se gestiona. El enfoque general de gestión no es organizado
N2 **Repetible, pero intuitivo**	50	Los procesos siguen una pauta regular cuando los procedimientos se realizan por distintas personas. No hay procedimientos escritos ni actividades formativas
N3 **Proceso definido**	80	Los procesos están estandarizados, documentados y comunicados con acciones formativas
N4 **Gestionado y medible**	90	La Dirección controla y mide el cumplimiento de los procedimientos y adopta medidas correctoras cuando se requiere
N5 **Optimizado**	100	Se siguen buenas prácticas en un ciclo de mejora continua

Consideramos que este modelo proporciona una base sólida para formarse una idea general de la situación en la entidad revisada de los controles de ciberseguridad y el cumplimiento de la legalidad en esta materia.

Como ya hemos dicho, la evaluación del nivel de madurez no se ha basado en los procesos teóricos o en los procedimientos aprobados, sino en la **verificación de su aplicación real** en la práctica.

El ENS asigna una categoría de seguridad a los SIC de los organismos del sector público en función de la valoración del impacto que tendría sobre la organización un incidente que afectara a la seguridad de la información o de los sistemas, teniendo en cuenta las cinco dimensiones de la seguridad[11]. En función de esa categoría, el ENS asigna un nivel de madurez mínimo que deben cumplir los SIC de la entidad en cuestión. Los sistemas auditados en el trabajo que comentamos están clasificados como de categoría MEDIA. En consecuencia, en la auditoría, **hemos analizado si los resultados para cada CBCS obtenidos de acuerdo con el modelo de nivel de madurez alcanzan el nivel mínimo de exigencia requerido en el ENS, que en el presente caso es el N3, *proceso definido* y un índice de madurez del 80%.**

Además, a efectos del ENS, la guía CCN-STIC-824 contempla una serie de indicadores agregados capaces de aportar información resumida sobre el estado de la seguridad en los organismos públicos. Dichos indicadores han sido aplicados a los CBCS ya que permiten sintetizar el estado de las medidas de seguridad de cada ayuntamiento tanto a los efectos del ENS, como de los CBCS.

Estos **índices globales** son:

- El **índice de madurez del ayuntamiento** sintetiza, en tanto por ciento, el nivel de madurez alcanzado por un organismo respecto del conjunto de CBCS.
- El **índice de cumplimiento** del ayuntamiento analiza igualmente el nivel de madurez alcanzado, pero en relación con la exigencia aplicable en cada caso, teniendo en cuenta la categoría del sistema. Es decir, compara el índice de madurez con el nivel mínimo exigido para dicha categoría en el ENS, que en la presente auditoría es *N3* (80%) para todos los casos.

El modelo de madurez proporciona una base sólida para formarse una idea general de la situación en la entidad revisada de los controles de ciberseguridad y el cumplimiento de la legalidad en esta materia.

8. Cumplimiento normativo

Como señalan Benitez y Vaz, *«en un mundo interconectado, y donde la interoperabilidad es ya un mandato, un punto vulnerable debilita todo el sistema. La fragilidad de las entidades locales, sus escasos recursos humanos y presupuestarios y su heterogeneidad hacen de la ad-*

11. Confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad.

ministración local el eslabón más débil de la cadena. De ahí la importancia de cumplir con la normativa vigente y de verificar, desde el control externo, que así se está haciendo»[12].

Por esta razón en este tipo de revisión está incluida, como CBCS 8 la verificación del cumplimiento de diversas normas relacionadas con la seguridad de la información:

SUBCONTROLES	OBJETIVO DE CUMPLIMIENTO
Cumplimiento del ENS	• Política de seguridad y responsabilidades • Declaración de aplicabilidad • Informe de Auditoría (nivel medio o alto) • Informe del estado de la seguridad • Publicación de la declaración de conformidad y los distintivos de seguridad en la sede electrónica
Cumplimiento de la LOPD/RGPD	• Nombramiento del DPD • Registro de actividades de tratamiento • Análisis de riesgos y evaluación del impacto de las operaciones de tratamiento *(para los de riesgo alto)* • Informe de auditoría de cumplimiento *(cuando el responsable del tratamiento haya decidido realizarla)*
Cumplimiento de la Ley 25/2013, de 27 de diciembre de Impulso de la factura electrónica y creación del registro contable de facturas	• Informe de auditoría de sistemas anual del Registro Contable de Facturas (*Artículo 12 apartado 3)*

9. Qué informes se han emitido

Como resultado del trabajo realizado, se han elaborado 15 informes de auditoría de los controles básicos de ciberseguridad[13], uno para cada ayuntamiento. Además, se ha elaborado un informe global de síntesis de los principales hallazgos de las auditorías.

Este artículo pretende ser un breve análisis de los resultados recogidos en esos 15 informes de auditoría. Los datos aportados se han obtenido de esos informes públicos.

Los trabajos de auditoría se iniciaron progresivamente en la primavera de 2019 y finalizaron en la de 2020. Los informes recogen la situación de los CBCS al finalizar el trabajo de campo y emitir el informe de auditoría.

Consideramos como fin del trabajo de campo la fecha en la que los hallazgos de la auditoría, las conclusiones y el borrador previo del informe es, de acuerdo con lo establecido en nuestro Manual de fiscalización, discutido con los responsables de la entidad auditada. Es admitida cualquier evidencia adicional disponible en ese momento y son corroborados los hechos puestos de manifiesto en el informe. **El informe con carácter general refleja la situación en ese momento**, ya que es frecuente que desde que se inicia el trabajo de campo, determinadas deficiencias observadas y señaladas a los gestores sean subsanadas y recogidas de esta forma en las conclusiones y en los indicadores.

12. BENITEZ PALMA, ENRIQUE; VAZ CALDERÓN, CARLOS; «La ciberseguridad en las entidades locales: cómo enfocar una fiscalización externa de cumplimiento de legalidad», *Revista de Auditoría Pública,* n.º 74, 2019.

13. Publicados en la página web de la Sindicatura de Cuentas de la Comunidad Valenciana.

10. Confidencialidad

Dado que la información utilizada en la auditoría y los resultados detallados de la misma tienen un carácter sensible y pueden afectar a la seguridad de los sistemas de información de las entidades revisadas, las comunicaciones de información sensible entre la Sindicatura y las entidades se han realizado por medio canales cifrados, garantizando así la integridad y confidencialidad de los datos.

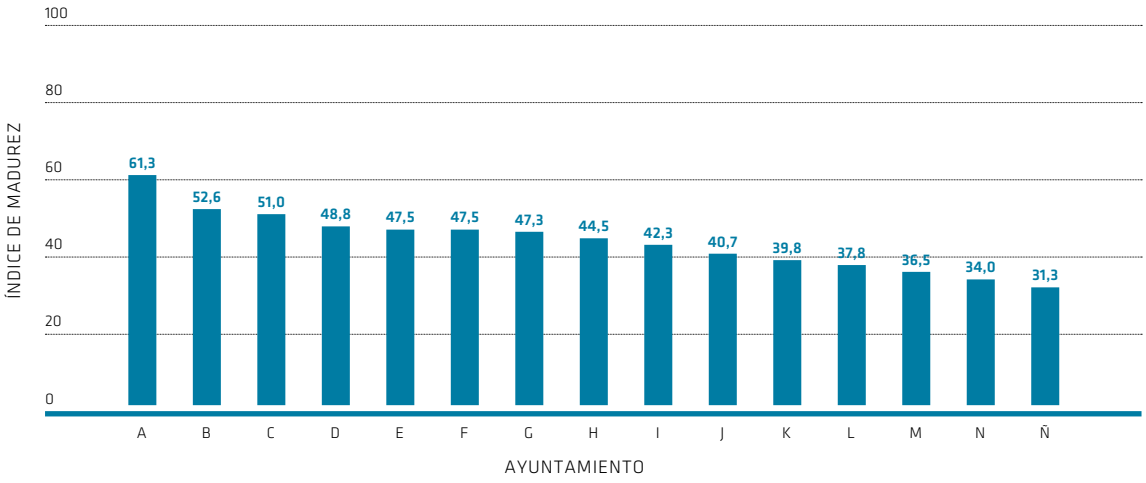
Tal como requiere la GUID 5100[14], se ha tenido en cuenta la sensibilidad y confidencialidad de la información presentada en los informes, toda ella relacionada con la seguridad de los sistemas de información, y una vez elaborados los distintos informes, los resultados al máximo nivel de detalle únicamente se han comunicado con carácter confidencial a los responsables de cada entidad, con el objeto de que puedan adoptar las medidas correctoras que consideren precisas.

11. Algunas observaciones sobre los resultados de las auditorías

En cada informe de auditoría se concluye sobre la situación de los controles de ciberseguridad en los distintos ayuntamientos. En este breve trabajo vamos a extraer alguna conclusión u observación de carácter general.

La **primera observación** que se puede destacar es que **ningún ayuntamiento auditado alcanza el índice de madurez general del 80%, o nivel de madurez N3, que es el nivel mínimo exigido por el ENS.** El índice de madurez medio de los 15 ayuntamientos es el 44,2% muy por debajo del nivel que exige el ENS. Los resultados obtenidos han sido:

GRÁFICO
ÍNDICE DE MADUREZ GENERAL



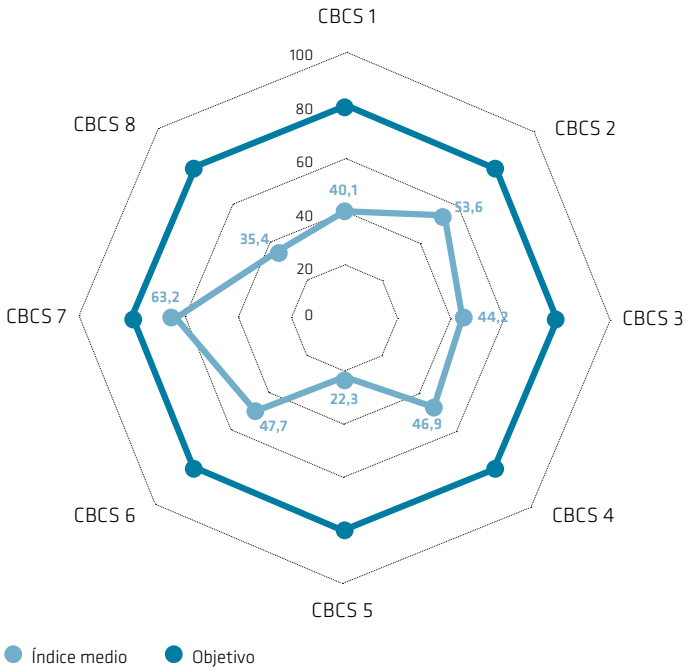
14. Ver párrafo 7.3 de la GUID 5100 Guidance on Audit of Information Systems.

Por tanto, puede deducirse que ningún ayuntamiento dispone de un conjunto de controles de ciberseguridad que garantice la protección de sus sistemas de información de forma satisfactoria.

Podría pensarse que la valoración obtenida guarda relación directa con los recursos disponibles en cada entidad, pero analizando en detalle los datos de los dos ayuntamientos mejor valorados se llega a un resultado sorprendente: el ayuntamiento mejor valorado (61,3%) es el que tiene una relación Obligaciones Reconocidas Netas / Población más favorable (1.402 euros/habitante), resultado que parece lógico; pero el segundo ayuntamiento mejor valorado (52,6%) es el que tiene la peor relación ORN/Población (679 euros/habitante). A falta de análisis posteriores más detallados, nos hace pensar que quizá otros factores «intangibles» sean más relevantes, por ejemplo, la concienciación de los altos órganos de dirección con la importancia de la ciberseguridad y la necesidad de adoptar medidas de ciberhigiene[15].

La segunda observación la podemos hacer respecto de los índices de madurez medios de los CBCS, que en todos ellos, está por debajo del 80% o Nivel 3 requerido por el ENS. Tal como puede apreciarse en el siguiente gráfico:

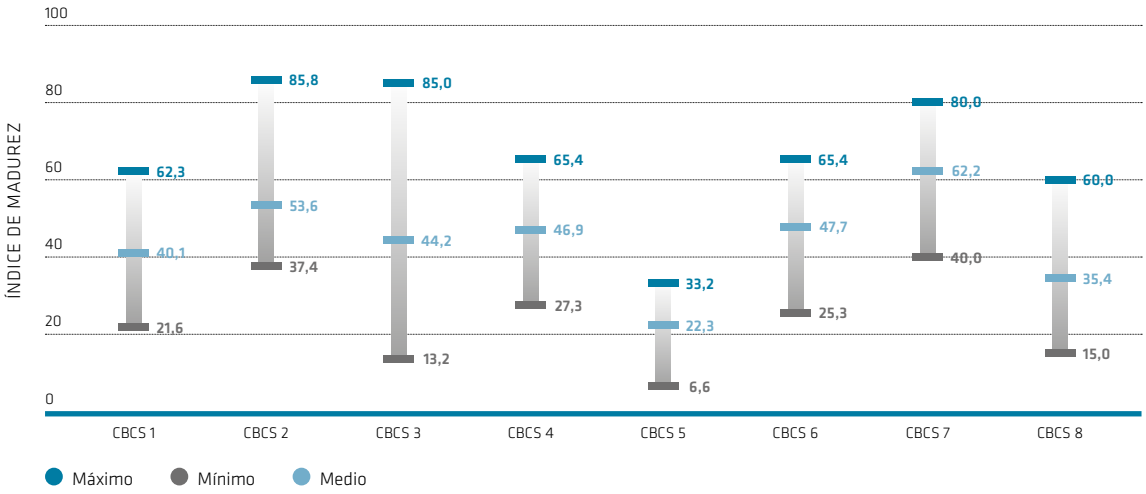
GRÁFICO
ÍNDICE MEDIO DE MADUREZ DE LOS CBCS



15. La European Union Agency for Cybersecurity (ENISA) señala que «la ciberhigiene es un principio fundamental relativo a la seguridad de la información y, como la analogía con la higiene personal, es el equivalente a establecer simples medidas rutinarias para minimizar los riesgos de las ciberamenazas. La suposición subyacente es que las buenas prácticas de ciberhigiene pueden proporcionar inmunidad en las entidades que las aplican» reduciendo los ciberriesgos. *«Review of Cyber Hygiene practices»,* ENISA, diciembre de 2016.

Se puede profundizar en el análisis de los resultados y se observa una situación muy dispar en los 15 ayuntamientos auditados, con grandes diferencias en los resultados obtenidos, tal como puede observarse en el gráfico siguiente que muestra la dispersión de los resultados obtenidos en los índices de madurez de los CBCS.

GRÁFICO
VARIABILIDAD DE LOS ÍNDICES DE MADUREZ



Esta disparidad de resultados, con un marco legal de obligado cumplimiento común, el ENS, quizá sea un indicador de la dispar percepción de la seguridad entre las distintas entidades, dependiendo de aspectos como:

a. El mayor o menor compromiso de los máximos responsables de los ayuntamientos con la seguridad de la información.
b. Los conocimientos, experiencias y perfiles de los profesionales que componen los departamentos fiscalizados. Y relacionado con el punto a) su motivación o desmotivación.

Es interesante observar cómo, en el caso del *CBCS 3 Proceso continuo de identificación y remediación de vulnerabilidades*, hay algún ayuntamiento que ha cumplido sobradamente con los requerimientos y excede en cinco puntos el objetivo del 80%, y sin embargo hay alguno en una situación muy deficiente y solo ha obtenido una valoración de 13,2%.

La situación observada en el CBCS 4 *Uso controlado de privilegios administrativos,* es preocupante por los riesgos derivados de su deficiente situación y valoración, muy inferior al nivel requerido. En parte debido a que en un mismo ayuntamiento, aunque haya casos en los que existe un proceso de control adecuado, en general, éste nunca es considerado de manera integral para todos los sistemas de la entidad, limitando su efectividad y nivel de madurez.

También se observa que en el caso del *CBCS 5 Configuraciones seguras del hardware y software*, los resultados han sido muy deficientes en todos los casos. En general, no existen procedimientos específicos establecidos con el objeto de conferir a las configuraciones un

nivel determinado de seguridad, y la limitada eficacia de los controles existentes depende casi exclusivamente de los conocimientos técnicos del personal del departamento.

Finalmente se observa que el *CBCS 7 Copias de seguridad de datos y sistemas*, es el que ha obtenido la mejor valoración media de todos los CBCS analizados.

12. Principales deficiencias observadas

Las principales deficiencias observadas en los distintos CBCS, presentes en al menos la mitad de los ayuntamientos, han sido:

CBCS 1 Inventario y control de dispositivos físicos

- Ausencia de un procedimiento formalmente aprobado para la gestión del inventario y el control de activos físicos, que incluya las revisiones periódicas de hardware.
- Los controles para restringir el acceso de dispositivos físicos no autorizados a la red corporativa son inefectivos o inexistentes.

CBCS 2 Inventario y control de *software* autorizado y no autorizado

- Ausencia de un procedimiento formalmente aprobado que considere de manera integral el control y la gestión de todo el software de la entidad, aprobando una lista blanca de software autorizado, revisiones periódicas y que describa las medidas implantadas para impedir la ejecución del no autorizado.
- Ausencia de planes de mantenimiento para la gestión del soporte de todo el software utilizado en la entidad.
- Existe un número significativo de equipos con *software* fuera del periodo de soporte por parte del fabricante.

CBCS 3 Proceso continuo de identificación y remediación de vulnerabilidades

- Ausencia de un procedimiento formalmente aprobado para la identificación, priorización, resolución y parcheo de las vulnerabilidades detectadas.
- No existe gestor de parches y actualizaciones de software o su gestión no está correctamente implantada.
- Ausencia de herramientas para realizar escaneos periódicos en busca de vulnerabilidades en la red.

CBCS 4 Uso controlado de privilegios administrativos

- Ausencia de un procedimiento formalmente aprobado para la gestión de usuarios con privilegios de administración que aplique a todos los sistemas de la entidad.
- Existencia de usuarios no nominativos con privilegios de administración en los distintos sistemas, impidiendo la trazabilidad de las acciones en caso de incidentes de seguridad.
- Los administradores de sistemas no utilizan diferentes cuentas con distintos niveles de seguridad dependiendo de las tareas a realizar (tareas de administración del sistema o tareas ofimáticas que no requieren privilegios administrativos), incumpliendo así con la regla de la mínima funcionalidad.

CBCS 5 Configuraciones seguras del *hardware* y *software* de dispositivos móviles, portátiles, equipos de sobremesa y servidores

- Ausencia de procedimientos formalmente aprobados para la aplicación de configuraciones seguras a dispositivos y sistemas, considerando la seguridad por defecto y el criterio de mínima funcionalidad.
- Ausencia de mecanismos que garanticen una monitorización efectiva de cambios no autorizados en la configuración en los sistemas críticos de la entidad.

CBCS 6 Registro de la actividad de los usuarios (mantenimiento, monitorización y análisis de los *logs* de auditoría)

- Carencia de procedimientos formalmente aprobados por el órgano competente que describa la gestión de los registros de actividad de los usuarios, incluyendo los sistemas afectados, la información recabada, el periodo de retención y los mecanismos de protección de dichos registros.
- Los registros de auditoría de los distintos dispositivos y sistemas no están centralizados en herramientas de recolección de logs que faciliten su revisión.

CBCS 7 Copias de seguridad de datos y sistemas

- Ausencia de procedimientos formalmente aprobados por el órgano competente que describa las acciones que deben llevarse a cabo para realizar copias de seguridad de datos y sistemas.
- No se realizan pruebas de recuperación planificadas de los sistemas críticos de la entidad.

13. Cumplimiento legal

Puede apreciarse en los gráficos anteriores que, **en general, el nivel de cumplimiento de la legalidad es bastante insatisfactorio**, tal como refleja el índice medio de cumplimiento del CBCS 8 del 44,2%, que recoge el grado de cumplimiento con varias normas en materia de seguridad de los sistemas de información.

Cabría destacar aquellos incumplimientos que suponen un mayor impacto a efectos de protección de datos de carácter personal y de consecución del requerido nivel de seguridad de los sistemas de información:

- La ausencia de Política de Seguridad aprobada y de cuerpo normativo y procedimental, evidenciando la falta de conciencia y de compromiso de la entidad con la seguridad de la información y la protección de datos personales.
- La ausencia de órganos de gobierno y de los perfiles requeridos por la normativa vigente, particularmente del DPD y del Responsable de Seguridad, carencias que dificultan la toma de decisiones, la unificación de criterios y la implantación homogénea de medidas de seguridad.
- La falta de un registro de actividades del tratamiento, que implica la identificación y consideración de todos los usos de datos de carácter personal, requisitos previo imprescindible para la implantación de medidas y el cumplimiento de obligaciones para con el uso de dichos datos.

La responsabilidad de garantizar un nivel adecuado de cumplimiento de las normas legales recae sobre los máximos órganos de dirección de las entidades locales que deben impulsar las medidas necesarias para subsanar la deficiente situación puesta de manifiesto en los informes.

14. La ciberseguridad no tiene coste cero

Son necesarias inversiones sostenidas y un mayor compromiso de los órganos de gobierno con la seguridad de los sistemas de información. La necesaria mejora de los controles de ciberseguridad requiere de actuaciones e inversiones, tanto en medios materiales como personales, que deben ser adecuadamente planificadas y sostenidas en el tiempo, puesto que cada vez más servicios se prestan utilizando sistemas de información y cada vez las amenazas provenientes del ciberespacio son más persistentes y dañinas.

Si no se priorizan presupuestariamente los controles de seguridad y se refuerza la capacidad de resiliencia de los sistemas de información, las entidades asumen riesgos importantes de perturbaciones en la prestación de servicios a su comunidad y se compromete la confidencialidad e integridad de la información que poseen.

15. Recomendaciones

En los informes se ha incluido un apartado de recomendaciones para mejorar los controles de ciberseguridad. Con ánimo de facilitar esa tarea, en los informes se han clasificado las recomendaciones según criterios combinados de riesgo potencial a mitigar y coste de su implantación; de esta forma los responsables de las entidades pueden establecer acciones basadas en criterios de coste/beneficio.

Además de las recomendaciones señaladas en los informes, se ha comunicado a los responsables de cada ayuntamiento el detalle al máximo nivel de las deficiencias de seguridad reportadas, y otras recomendaciones con una relación de riesgo potencial a mitigar y coste de su implantación menos favorable que las anteriores.

16. A modo de conclusión

La ciberseguridad es una materia de importancia crítica en el mundo de la administración electrónica en el que nos ha tocado vivir y fiscalizar. La total dependencia de las TIC que tienen las administraciones públicas se ha mostrado con toda su crudeza a lo largo de la crisis del coronavirus al poner ante nuestros ojos, desnuda de envoltorios, esa realidad y obligarnos a dar, a todos los agentes del sector público, un acelerado gran salto cualitativo en el trabajo en remoto y en ver la necesidad de utilizar la tecnología para gestionar y prestar servicios a los ciudadanos sin estar ligados a un lugar físico. Esto a su vez ha puesto de manifiesto los graves riesgos de ciberseguridad, y la importancia de tener implantada una sólida protección frente a las ciberamenazas que ampare el conjunto del sistema de información y comunicaciones de cada entidad pública.

Las entidades locales, que prestan servicios fundamentales a los ciudadanos, no escapan a esa creciente ola de dependencia de las TIC y en consecuencia están sujetas a los mismos ciberriesgos que el resto de las administraciones públicas. Por ello la Sindicatura de Cuentas ha realizado sendas auditorías de ciberseguridad de los 15 principales ayuntamientos de la Comunidad Valenciana.

Los resultados no han sido muy alentadores mostrando una situación claramente mejorable en todos ellos, y en algunos muy deficiente. Las auditorías también han mostrado un bajo o muy bajo grado de cumplimiento con la normativa relativa a la seguridad de la información. Muy probablemente esta situación sea extrapolable a la generalidad de las entidades locales de nuestro país.

Las ICEX debemos perseverar en este tipo de auditorías ya que abordan un tipo de riesgo en crecimiento exponencial y con capacidad para afectar no solo a la información económica y presupuestaria de las entidades públicas, sino que puede afectar a su propia capacidad de seguir prestando servicios públicos con normalidad.

Aunque hay que reconocer que no es habitual, reconforta recibir un día el correo electrónico de un responsable TIC de uno de los ayuntamientos auditados con el siguiente mensaje:

> «Buenos días,
>
> Espero que estéis bien, en estos tiempos no podemos más que agradecer el trabajo que hicisteis con la auditoría, ya que nos permitió poner al día, al menos las medidas básicas para tener mayor seguridad en los sistemas, que al final redunda en mayor disponibilidad y capacidad de dar servicio, y desde ese punto inicial ir mejorando paso a paso.
>
> Dudo que, sin la auditoría para focalizar esfuerzos, estuviéramos soportando la situación actual de teletrabajo sin caídas de servicio.
>
> Un saludo, y hasta la próxima.»

Cierras tu portátil con la sensación de haber hecho un buen trabajo y, sobre todo, útil.

17. Bibliografía

BENÍTEZ PALMA, ENRIQUE; VAZ CALDERÓN, CARLOS; «La ciberseguridad en las entidades locales: cómo enfocar una fiscalización externa de cumplimiento de legalidad», *Auditoría Pública*, n.º 74, noviembre 2019.

CENTRO CRIPTOLÓGICO NACIONAL, Guías de seguridad de las TIC CCN-STIC serie 800.

Conclusiones de los XIII Encuentros Técnicos de los OCEX (2019), *Revista de Auditoría Pública*, n.º 74, noviembre 2019.

DASCA, ALBERTO; «La otra amenaza del coronavirus», *Diari de Tarragona*, 2020.

ENISA, «Review of Cyber Hygiene practices», 2016.

EUROPOL, «Pandemic profiteering how criminals exploit the COVID-19 crisis», 2020.

INTOSAI, «Guidance on Audit of Information Systems», 2019.

MINGUILLÓN ROY, ANTONIO; «El control externo y la auditoría de sistemas de información», *Revista Española de Control Externo*, n.º 53, 2016.

MINGUILLÓN ROY, ANTONIO; «La ciberseguridad, el auditor externo y los OCEX», *Revista de Auditoría Pública*, n.º 70, 2019.

MINGUILLÓN ROY, ANTONIO; «Las nuevas guías prácticas de fiscalización de los OCEX, unas guías de auditoría de la administración electrónica para el siglo XXI», *Revista de Auditoría Pública*, n.º 73, 2019.

PIPIKAITE, ALGIRDE; DAVIS, NICHOLAS; «¿Por qué la ciberseguridad es más importante que nunca durante la pandemia de coronavirus?», *World Economic Forum*, 2020.

LEGISLACIÓN Y JURISPRUDENCIA

3C_2019

JAVIER MEDINA GUIJARRO
JOSÉ ANTONIO PAJARES GIMÉNEZ

INTRODUCCIÓN

Siguiendo similar metodología a la de los números anteriores, ofrecemos en esta sección al lector interesado en ello una información de carácter general sobre la legislación y la jurisprudencia más relevante producida en el tercer cuatrimestre del año, en relación con las materias que directa o indirectamente afectan a la actividad económica-financiera del sector público, sin que en el periodo a que se refiere este número de la Revista se hayan publicado en el Boletín Oficial del Estado fiscalizaciones aprobadas por el Pleno del Tribunal de Cuentas.

En la primera parte «Legislación y otros aspectos» constan, sistemáticamente ordenadas, Leyes del Estado y, en su caso, Autonómicas, Decretos u Órdenes ministeriales, y demás Resoluciones. La información que se proporciona consiste en el enunciado de la disposición y en la referencia del periódico oficial donde se publica, para facilitar su consulta.

La segunda parte «Jurisprudencia» recoge, principalmente, las resoluciones dictadas por la Sala de Justicia de la Sección de Enjuiciamiento del Tribunal, figurando una breve descripción de su fundamentación jurídica. También se hace mención, cuando procede, de las sentencias y autos pronunciados por el Tribunal Constitucional y el Tribunal Supremo en materias que afecten al Tribunal de Cuentas, así como de las cuestiones y recursos de inconstitucionalidad que, por su relevancia, merecen citarse.

1. LEGISLACIÓN Y OTROS ASPECTOS

1.1. LEYES ESTATALES Y DISPOSICIONES CON VALOR DE LEY

- **REAL DECRETO-LEY 12/2019, de 11 de octubre,** por el que se adoptan medidas urgentes para paliar los efectos de la apertura de procedimientos de insolvencia del grupo empresarial Thomas Cook. (BOE n.º 246, de 12 de octubre de 2019)

- **REAL DECRETO-LEY 13/2019, de 11 de octubre,** por el que se regula la actualización extraordinaria de las entregas a cuenta para el año 2019 de las comunidades autónomas de régimen común y de las entidades locales, en situación de prórroga presupuestaria, y se establecen determinadas reglas relativas a la liquidación definitiva de la participación de las entidades locales en los tributos del Estado, correspondiente al año 2017. (BOE n.º 246, de 12 de octubre de 2019)

- **REAL DECRETO-LEY 14/2019, de 31 de octubre,** por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones. (BOE n.º 266, de 5 de noviembre de 2019)

- **REAL DECRETO-LEY 15/2019, de 8 de noviembre,** por el que se adoptan medidas urgentes para la organización en España de la XXV Conferencia de Naciones Unidas sobre el Cambio Climático. (BOE n.º 271, de 11 de noviembre de 2019)

- **REAL DECRETO-LEY 16/2019, de 18 de noviembre,** por el que se adoptan medidas relativas a la ejecución del presupuesto de la Seguridad Social. (BOE n.º 278, de 19 de noviembre de 2019)

- **REAL DECRETO-LEY 17/2019, de 22 de noviembre,** por el que se adoptan medidas urgentes para la necesaria adaptación de parámetros retributivos que afectan al sistema eléctrico y por el que se da respuesta al proceso de cese de actividad de centrales térmicas de generación. (BOE n.º 282, de 23 de noviembre de 2019)

- **REAL DECRETO-LEY 18/2019, de 27 de diciembre,** por el que se adoptan determinadas medidas en materia tributaria, catastral y de seguridad social. (BOE n.º 312, de 28 de diciembre de 2019)

1.2. LEYES AUTONÓMICAS Y DISPOSICIONES CON VALOR DE LEY

Comunidad Autónoma de Andalucía

- **LEY 4/2019, de 19 de noviembre,** de Cámaras Oficiales de Comercio, Industria, Servicios y Navegación de Andalucía. (BOE n.º 304, de 19 de diciembre de 2019)

Comunidad Autónoma de Cataluña

- **LEY 7/2019, de 14 de noviembre,** de modificación de la Ley 2/2000, del Consejo del Audiovisual de Cataluña, y de la Ley 11/2007, de la Corporación Catalana de Medios Audiovisuales. (BOE n.º 286, de 28 de noviembre de 2019)

- **LEY 8/2019, de 28 de noviembre,** de modificación de la Ley 7/2011, de medidas fiscales y financieras, y de la Ley 20/2000, de creación del Instituto Catalán de las Industrias Culturales. (BOE n.º 298, de 12 de diciembre de 2019)

Comunidad Autónoma de Extremadura

- **LEY 12/2019, de 11 de octubre,** del Voluntariado de Extremadura. (BOE n.º 261, de 30 de octubre de 2019)

- **LEY 13/2019, de 16 de octubre,** de modificación parcial de la Ley 1/2014, de 18 de febrero, de regulación del estatuto de los cargos públicos del Gobierno y la Administración de la Comunidad Autónoma de Extremadura. (BOE n.º 271, de 11 de noviembre de 2019)

Comunidad Autónoma de las Illes Balears

- **DECRETO-LEY 2/2019, de 4 de octubre,** por el que se establecen ayudas puntuales para paliar los impactos económicos producidos por el concurso de acreedores de la agencia de viajes mayorista Thomas Cook sobre la economía de las Illes Balears. (BOE n.º 273, de 13 de noviembre de 2019)

1.3. REALES DECRETOS Y DECRETOS

- **SENTENCIA de 10 de julio de 2019,** de la Sala Tercera del Tribunal Supremo, que estima parcialmente el recurso contencioso-administrativo número 83/2018 contra el Real Decreto 1072/2017, de 29 de diciembre por el que se modifica el Reglamento general del régimen sancionador tributario, aprobado por el Real Decreto 2063/2004, de 15 de octubre. (BOE n.º 226, de 20 de septiembre de 2019)

- **REAL DECRETO 538/2019, de 20 de septiembre,** por el que se convocan elecciones locales parciales 2019. (BOE n.º 229, de 24 de septiembre de 2019)

- **SENTENCIA de 5 de julio de 2019,** de la Sala Tercera del Tribunal Supremo, que declara estimar el recurso contencioso-administrativo número 535/2017, contra el Real Decreto 529/2017, de 26 de mayo, por el que se modifica el Reglamento del Impuesto sobre el Valor Añadido, aprobado por el Real Decreto 1624/1992, de 29 de diciembre. (BOE n.º 231, de 25 de septiembre de 2019)

- **REAL DECRETO 595/2019, de 18 de octubre,** por el que se modifica el Reglamento del Impuesto sobre la Renta de no Residentes, aprobado por el Real Decreto 1776/2004, de 30 de julio. (BOE n.º 252, de 19 de octubre de 2019)

- **REAL DECRETO 597/2019, de 18 de octubre,** por el que se regula la concesión directa de subvenciones a entidades públicas en el ámbito del Ministerio de Educación y Formación Profesional. (BOE n.º 252, de 19 de octubre de 2019)

- **REAL DECRETO 639/2019, de 8 de noviembre,** por el que se crea el Comité Organizador de la XXV Conferencia de Naciones Unidas sobre el Cambio Climático. (BOE n.º 271, de 11 de noviembre de 2019)

- **SENTENCIA de 25 de septiembre de 2019,** de la Sala Tercera del Tribunal Supremo, que declara estimar parcialmente el recurso contencioso-administrativo 85/2018 contra el Real Decreto 1070/2017, de 29 de diciembre, por el que se modifican el Reglamento General de las actuaciones y los procedimientos de gestión e inspección tributaria y de desarrollo de las normas comunes de los procedimientos

de aplicación de los tributos, aprobado por el Real Decreto 1065/2007, de 27 de julio, y el Real Decreto 1676/2009, de 13 de noviembre, por el que se regula el Consejo para la Defensa del Contribuyente. (BOE n.º 275, de 15 de noviembre de 2019)

- **REAL DECRETO 656/2019, de 18 de noviembre,** por el que se regula la concesión directa de diversas subvenciones en el ámbito del Ministerio de Educación y Formación Profesional para el ejercicio presupuestario 2019. (BOE n.º 278, de 19 de noviembre de 2019)

- **REAL DECRETO 657/2019, de 18 de noviembre,** por el que se regula la concesión directa de subvenciones en materia de turismo para el ejercicio presupuestario 2019. (BOE n.º 278, de 19 de noviembre de 2019)

- **REAL DECRETO 658/2019, de 18 de noviembre,** por el que se regula la concesión directa de determinadas subvenciones en el ámbito del medio ambiente para el ejercicio presupuestario 2019. (BOE n.º 278, de 19 de noviembre de 2019)

- **REAL DECRETO 659/2019, de 18 de noviembre,** por el que se regula la concesión directa de subvenciones a determinadas entidades para la promoción de las artes escénicas y musicales en el año 2019. (BOE n.º 278, de 19 de noviembre de 2019)

- **REAL DECRETO 661/2019, de 18 de noviembre,** por el que se regula la concesión directa de subvenciones para gastos de funcionamiento de fundaciones y asociaciones vinculadas con partidos políticos con representación en las Cortes Generales que realicen actividades de estudio y desarrollo del pensamiento político y social. (BOE n.º 278, de 19 de noviembre de 2019)

- **REAL DECRETO 663/2019, de 18 de noviembre,** por el que se regula la concesión directa de diversas subvenciones en el ámbito de competencias del Ministerio de Ciencia, Innovación y Universidades, para la ejecución de actuaciones en materia de investigación científica, desarrollo tecnológico e innovación. (BOE n.º 278, de 19 de noviembre de 2019)

- **REAL DECRETO 598/2019, de 18 de octubre,** por el que se regula la composición y el funcionamiento de la Comisión Interministerial de coordinación en materia de tratados y otros acuerdos internacionales. (BOE n.º 279, de 20 de noviembre de 2019)

- **REAL DECRETO 716/2019, de 5 de diciembre,** por el que se modifican el Real Decreto 773/2015, de 28 de agosto, por el que se modifican determinados preceptos del Reglamento General de la Ley de Contratos de las Administraciones Públicas, aprobado por el Real Decreto 1098/2001, de 12 de octubre, y el Real Decreto 700/1988, de 1 de julio, sobre expedientes administrativos de responsabilidad contable derivados de las infracciones previstas en el título VII de la Ley General Presupuestaria. (BOE n.º 293, de 6 de diciembre de 2019)

- **REAL DECRETO 748/2019, de 27 de diciembre,** por el que se modifica el Real Decreto 636/2014, de 25 de julio, por el que se crea la Central de Información económico-financiera de las Administraciones Públicas y se regula la remisión de información por el Banco de España y las entidades financieras al Ministerio de Hacienda y Administraciones Públicas. (BOE n.º 312, de 28 de diciembre de 2019)

- **REAL DECRETO 749/2019, de 27 de diciembre,** por el que se aprueba el Reglamento de funcionamiento del Inventario de Entidades del Sector Público Estatal, Autonómico y Local. (BOE n.º 312, de 28 de diciembre de 2019)

1.4. ÓRDENES MINISTERIALES Y CIRCULARES

- **ORDEN HAC/973/2019, de 26 de septiembre,** por la que se fijan las cantidades de las subvenciones a los gastos originados por actividades electorales para las elecciones generales de 10 de noviembre de 2019. (BOE n.º 234, de 28 de septiembre de 2019)

- **ORDEN HAC/1111/2019, de 11 de noviembre,** por la que se regulan las operaciones de cierre de ejercicio 2019 relativas al presupuesto de gastos y operaciones no presupuestarias. (BOE n.º 272, de 12 de noviembre de 2019)

- **ORDEN TMS/1114/2019, de 12 de noviembre,** por la que se regulan las operaciones de cierre del ejercicio 2019 para las entidades que integran el sistema de la Seguridad Social. (BOE n.º 273, de 13 de noviembre de 2019)

- **ORDEN HAC/1170/2019, de 18 de noviembre,** por la que se modifica la Orden HAC/316/2019, de 12 de marzo, de delegación de competencias y por la que se fijan los límites de las competencias de gestión presupuestaria y concesión de subvenciones y ayudas de los titulares de las Secretarías de Estado. (BOE n.º 291, de 4 de diciembre de 2019)

- **ORDEN HAC/1272/2019, de 16 de diciembre,** por la que se publican los límites de los distintos tipos de contratos a efectos de la contratación del sector público a partir del 1 de enero de 2020. (BOE n.º 314, de 31 de diciembre de 2019)

1.5. ACUERDOS, RESOLUCIONES E INSTRUCCIONES

- **RESOLUCIÓN de 4 de septiembre de 2019,** de la Secretaría General del Tesoro y Financiación Internacional, por la que se actualiza el anexo 1 incluido en la Resolución de 4 de julio de 2017, por la que se define el principio de prudencia financiera aplicable a las operaciones de endeudamiento y derivados de las comunidades autónomas y entidades locales. (BOE n.º 214, de 6 de septiembre de 2019)

- **RESOLUCIÓN de 10 de septiembre de 2019,** de la Presidencia de la Agencia Estatal de Administración Tributaria, por la que se modifica la de 21 de septiembre de 2004, por la que se establece la estructura y organización territorial de la Agencia Estatal de Administración Tributaria. (BOE n.º 218, de 11 de septiembre de 2019)

- **RESOLUCIÓN de 17 de septiembre de 2019,** de la Intervención General de la Administración del Estado, por la que se establece el funcionamiento del Registro de cesiones de crédito. (BOE n.º 232, de 26 de septiembre de 2019)

- **INSTRUCCIÓN 9/2019, de 25 de septiembre,** de la Junta Electoral Central, de aplicación a las elecciones al Congreso de los Diputados y al Senado de 10 de noviembre de 2019, de la disposición adicional séptima de la Ley Orgánica 5/1985, de 19 de junio, del Régimen Electoral General, en su redacción dada por la Ley Orgánica 2/2016. (BOE n.º 232, de 26 de septiembre de 2019)

- **INSTRUCCIÓN 10/2019, de 25 de septiembre,** de la Junta Electoral Central, sobre Juntas Electorales competentes y otros extremos en relación con las elecciones locales parciales, convocadas por Real Decreto 538/2019, de 20 de septiembre, a celebrar el 10 y el 17 de noviembre de 2019)

- **CORRECCIÓN DE ERRORES DE LA INSTRUCCIÓN 9/2019, de 25 de septiembre,** de la Junta Electoral Central, de aplicación a las elecciones al Congreso de los Diputados y al Senado de 10 de noviembre de 2019, de la disposición adicional séptima de la Ley Orgánica 5/1985, de 19 de junio, del Régimen Electoral General, en su redacción dada por la Ley Orgánica 2/2016. (BOE n.º 233, de 27 de septiembre de 2019)

- **CORRECCIÓN DE ERRORES DE LA RESOLUCIÓN de 10 de septiembre de 2019,** de la Presidencia de la Agencia Estatal de Administración Tributaria, por la que se modifica la de 21 de septiembre de 2004, por la que se establece la estructura y organización territorial de la Agencia Estatal de Administración Tributaria. (BOE n.º 236, de 1 de octubre de 2019)

- **RESOLUCIÓN de 7 de octubre de 2019,** de la Secretaría General del Tesoro y Financiación Internacional, por la que se actualiza el anexo 1 incluido en la Resolución de 4 de julio de 2017, de la Secretaría General del Tesoro y Política Financiera, por la que se define el principio de prudencia financiera aplicable a las operaciones de endeudamiento y derivados de las comunidades autónomas y entidades locales. (BOE n.º 243, de 9 de octubre de 2019)

- **RESOLUCIÓN de 22 de octubre de 2019,** del Congreso de los Diputados, por la que se ordena la publicación del Acuerdo de convalidación del Real Decreto-ley 12/2019, de 11 de octubre, por el que se adoptan medidas urgentes para paliar los efectos de la apertura de procedimientos de insolvencia del grupo empresarial Thomas Cook. (BOE n.º 260, de 29 de octubre de 2019)

- **RESOLUCIÓN de 22 de octubre de 2019,** del Congreso de los Diputados, por la que se ordena la publicación del Acuerdo de convalidación del Real Decreto-ley 13/2019, de 11 de octubre, por el que se regula la actualización extraordinaria de las entregas a cuenta para el año 2019 de las comunidades autónomas de régimen común y de las entidades locales, en situación de prórroga presupuestaria, y se establecen determinadas reglas relativas a la liquidación definitiva de la participación de las entidades locales en los tributos del Estado, correspondiente al año 2017. (BOE n.º 260, de 29 de octubre de 2019)

- **RESOLUCIÓN de 25 de octubre de 2019,** de la Intervención General de la Administración del Estado, por la que se aprueba la adaptación de las Normas de Auditoría del Sector Público a las Normas Internacionales de Auditoría. (BOE n.º 266, de 5 de noviembre de 2019)

- **RESOLUCIÓN de 5 de noviembre de 2019,** de la Presidencia del Tribunal de Cuentas, por la que se publica el Acuerdo del Pleno, de 31 de octubre de 2019, por el que se aprueba la Instrucción relativa a la fiscalización de las contabilidades de las elecciones a Cortes Generales de 10 de noviembre de 2019. (BOE n.º 268, de 7 de noviembre de 2019)

- **RESOLUCIÓN de 18 de noviembre de 2019,** de la Intervención General de la Administración del Estado, por la que se publica el Acuerdo del Consejo de Ministros, de 15 de noviembre de 2019, por el que se modifica el de 30 de mayo de 2008, por el que se da aplicación a la previsión de los artículos 152 y 147 de la Ley General Presupuestaria, respecto al ejercicio de la función interventora en régimen de requisitos básicos. (BOE n.º 281, de 22 de noviembre de 2019)

- **RESOLUCIÓN de 7 de noviembre de 2019,** de la Intervención General de la Administración del Estado, por la que se publica resumen de la Cuenta General del Estado del ejercicio 2018. (BOE n.º 281, de 22 de noviembre de 2019)

- **RESOLUCIÓN de 27 de noviembre de 2019,** del Congreso de los Diputados, por la que se ordena la publicación del Acuerdo de convalidación del Real Decreto-ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones. (BOE n.º 291, de 4 de diciembre de 2019)

- **RESOLUCIÓN de 27 de noviembre de 2019,** del Congreso de los Diputados, por la que se ordena la publicación del Acuerdo de convalidación del Real Decreto-ley 15/2019, de 8 de noviembre, por el que se adoptan medidas urgentes para la organización en España de la XXV Conferencia de Naciones Unidas sobre el Cambio Climático. (BOE n.º 291, de 4 de diciembre de 2019)

- **RESOLUCIÓN de 27 de noviembre de 2019,** del Congreso de los Diputados, por la que se ordena la publicación del Acuerdo de convalidación del Real Decreto-ley 17/2019, de 22 de noviembre, por el que se adoptan medidas urgentes para la necesaria adaptación de parámetros retributivos que afectan al sistema eléctrico y por el que se da respuesta al proceso de cese de actividad de centrales térmicas de generación. (BOE n.º 291, de 4 de diciembre de 2019)

- **RESOLUCIÓN de 27 de noviembre de 2019,** del Congreso de los Diputados, por la que se ordena la publicación del Acuerdo de convalidación del Real Decreto-ley 16/2019, de 18 de noviembre, por el que se adoptan medidas relativas a la ejecución del presupuesto de la Seguridad Social. (BOE n.º 291, de 4 de diciembre de 2019)

- **RESOLUCIÓN de 3 de diciembre de 2019,** de la Secretaría General del Tesoro y Financiación Internacional, por la que se actualiza el anexo 1 incluido en la Resolución de 4 de julio de 2017, de la Secretaría General del Tesoro y Política Financiera, por la que se define el principio de prudencia financiera aplicable a las operaciones de endeudamiento y derivados de las comunidades autónomas y entidades locales. (BOE n.º 293, de 6 de diciembre de 2019)

- **RESOLUCIÓN de 19 de diciembre de 2019,** del Consejo de la Comisión Nacional del Mercado de Valores, por la que se aprueba el Reglamento de Régimen Interior de la Comisión. (BOE n.º 312, de 28 de diciembre de 2019)

2. JURISPRUDENCIA TRIBUNAL DE CUENTAS. SALA DE JUSTICIA

2.1. SENTENCIAS Y RESÚMENES DOCTRINALES

- **SENTENCIA N.º 15/2019. Recurso de apelación, rollo N.º 8/19, interpuesto contra la Sentencia N.º 9/2018, de 13 de septiembre, dictada en el procedimiento de reintegro por alcance n.º B-225/15-39, del ramo de Comunidades Autónomas (Consejería de Empleo – Ayudas destinadas a Empresas para la financiación de Planes de Viabilidad– .....), Andalucía. Ponente: Excma. Sra. D.ª María Antonia Lozano Álvarez.**

  Resumen de doctrina: La Sala, tras exponer las alegaciones de las partes en sus respectivos escritos de recurso, concluye que la Sentencia impugnada explica minuciosamente las razones por las que la participación de los recurrentes en los hechos generadores de alcance resultan encuadrables en el concepto de responsabilidad contable subsidiaria, tal y como se define en el artículo 43 de la Ley Orgánica 2/1982, de 12 de mayo, del Tribunal de Cuentas.

  La salida injustificada de numerario que se produce desde las arcas públicas a un patrimonio particular bajo la apariencia de una subvención o ayuda, sin que existan los requisitos del derecho de cobro por el perceptor, ni se adopte el procedimiento legalmente previsto, ni quede acreditada la corrección jurídica del destino final dado a los fondos transferidos, se encuadra con claridad en el concepto técnico jurídico de alcance que se recoge en el artículo 72 de la Ley de Funcionamiento del Tribunal de Cuentas.
  En cambio, y a pesar de las alegaciones de los recurrentes, no encaja en el concepto también técnico jurídico de pagos indebidos.

  Tampoco estima la Sala que exista una cuestión prejudicial penal por la que debiera suspenderse este proceso de responsabilidad contable. Ello es así, en primer lugar, porque el planteamiento de esta cuestión se hace en un momento procesal inoportuno. En segundo lugar, porque no se aporta en el recurso argumento ni prueba alguna que pueda sustentar una excepción al principio general de compatibilidad entre la jurisdicción penal y la contable para el enjuiciamiento de unos mismos hechos (artículo 18 de la Ley Orgánica del Tribunal de Cuentas y artículo 49 de la Ley de Funcionamiento del mismo, en relación con el artículo 17.2 de la primera).

  Por lo demás, la compatibilidad entre las actuaciones del presente procedimiento de reintegro por alcance y las seguidas en el proceso concursal no provoca ninguna distorsión en los derechos de los acreedores de la empresa declarada en concurso pues, como tiene dicho la Sala de manera uniforme siempre que se plantea la cuestión de la compatibilidad de jurisdicciones, es en fase de ejecución de sentencia donde se deben adoptar las medidas de coordinación necesarias para que no se produzcan consecuencias antijurídicas en perjuicio de la parte ejecutante ni de la parte ejecutada ni de posibles terceros.

- **SENTENCIA N.º 16/2019. Recurso de apelación n.º 24/19, interpuesto contra la Sentencia n.º 17/2018, de 3 de diciembre, dictada en el procedimiento de reintegro por alcance n.º B-98/13, del ramo Entidades Locales (Ayto. Marbella, -...-"-Inf.Fisc.TCU, Ejerc. 1/01/02 a 21/04/06), MÁLAGA. Ponente: Excmo. Sr. D. José Manuel Suárez Robledano.**

  Resumen de doctrina: Una vez expuestas las alegaciones de las partes, y como cuestión previa, manifiesta la Sala que debe pronunciarse acerca de la excepción de falta de legitimación pasiva de las personas que ostentaron la condición de miembros del Consejo de Administración, en el momento de producirse los hechos enjuiciados en el procedimiento de instancia, y que fue apreciada por la Juzgadora de instancia en la Sentencia recurrida. La concurrencia de dicha excepción procesal ha constituido motivo de recurso. Y la Sala de Justicia considera que resulta procedente declarar la concurrencia de la excepción de falta de legitimación pasiva.

  A la vista, pues, de los hechos acreditados en las actuaciones, la Sala entiende que en el presente caso no cabe otra cosa sino confirmar las conclusiones contenidas en la Sentencia impugnada, de inexistencia de un alcance de los fondos públicos municipales.

- **SENTENCIA N.º 17/2019. Recursos de apelación, rollo n.º 18/19, interpuestos contra la Sentencia 10/2018, de 8 de noviembre, dictada en el procedimiento de reintegro por alcance n.º A-73/17, Sector Público Local**

(Informe de Fiscalización «Análisis de la Gestión de los Fondos Líquidos del municipio de ...., Ejercicio 2012»), Málaga.

Resumen de doctrina: Una vez expuestos por la Sala los distintos argumentos de las partes, y entrando en el fondo de los recursos formulados, analiza si se ha producido el error en la valoración de la prueba por parte de la Consejera de instancia que alegan todos los impugnantes a excepción del Ministerio Fiscal.

La fijación de los hechos y la valoración de los medios de prueba, con base en criterios de crítica racional es competencia del Juez de instancia, pero, como ha reiterado la Sala (entre otras, Sentencias 18/2009, de 22 de julio, y 4/2015, de 2 de julio) el Tribunal de apelación puede valorar las pruebas practicadas en la instancia y corregir la ponderación llevada a cabo por el Juez *«a quo»*. Ello deriva de la naturaleza propia del recurso de apelación, que otorga plenas facultades al Juez o Tribunal *«ad quem»* para resolver cuantas cuestiones se le planteen, sean de hecho o de derecho, por tratarse de un recurso ordinario que representa un *«novum iudicium»,* como en reiteradas ocasiones ha afirmado el Tribunal Constitucional (entre otras, Sentencias 124/83, 23 y 24/85, 145/87 y 295/90). Ello permite a la Sala la posibilidad de aplicar e interpretar normas jurídicas con criterio diferenciado, corrigiendo, enmendando o revocando lo decidido y recurrido e incluso decidir lo mismo con fundamentación diferente, aunque siempre dentro del principio de congruencia y de los límites de las pretensiones de las partes.

La Sala concluye que no se ha producido una errónea valoración de la prueba por parte de la Consejera de instancia y tampoco una infracción de la doctrina vigente sobre la existencia de responsabilidad contable, ni de los artículos 38 y 42 de la LOTCu y 49 de la LFTCu.

- **SENTENCIA N.º 18/2019. Recurso de apelación, rollo n.º 22/19, interpuesto contra la Sentencia N.º 1/2019, de 15 de febrero, dictada en el procedimiento de reintegro por alcance N.º C-115/17, del ramo de Sector Público Estatal (Informe TCu principales inversiones ... , 2005-2012, Irreg. Expte. 231/10. Centro Formación ...), Oviedo. Ponente: Excma. Sra. D.ª María Antonia Lozano Álvarez.**

Resumen de doctrina: El recurso plantea, en primer lugar, una serie de cuestiones de índole procesal, cuales son que no toda la prueba propuesta fue admitida —sobre este particular la Sala de Justicia manifiesta que resulta conforme a derecho y no se ha provocado menoscabo alguno del derecho a la tutela judicial efectiva del apelante ni se ha causado indefensión, material o formal—; que la Sentencia recurrida vulnera el derecho a la tutela judicial efectiva del apelante pues no toma en consideración, sin motivar por qué, las funciones decisivas que en la resolución y liquidación del contrato de obras desarrolló el asesor jurídico —la Sala manifiesta que ello no implica infracción procesal generadora de menoscabo alguno en el derecho a la tutela judicial efectiva—; que el apelante dejó de ser empleado de la actora en febrero de 2012, por lo que no pudo tener acceso a los justificantes —la Sala manifiesta que tal circunstancia no ha menoscabado el derecho a la tutela judicial efectiva del impugnante ni, en particular, su derecho de defensa, pues se realizaron a través de los órganos competentes del Tribunal de Cuentas indagaciones y requerimientos documentales que hubieran resultado difíciles para aquél—; que a la actora incumbía la carga de la prueba de acreditar el daño —la Sala de Justicia comparte el criterio mantenido por el juzgador de primera instancia en su aplicación de las reglas de la carga de la prueba y considera, igualmente, que incumbía al demandado haber aportado la justificación suficiente y adecuada de que los 1.504 euros que se le reclaman se abonaron dentro de la legalidad y para satisfacer una obligación ajustada a derecho—; que la Sentencia de primera instancia se separa del criterio del informe de fiscalización y sigue el punto de vista de la Delegada Instructora de las Actuaciones Previas, pero no motiva las razones —sobre este particular, la Sala considera que la existencia de un alcance está suficientemente motivada en la Sentencia recurrida, cuya argumentación se ajusta a los requisitos de motivación de las Sentencias previstos en la Jurisprudencia Constitucional.

En cuanto al fondo del asunto considera demostrado en el presente proceso que la cifra total que se pagó a la UTE a través del libramiento de pago emitido por el apelante incluía 1.504 euros para los que no existía justificación.

- **SENTENCIA N.º 19/2019. Recurso de apelación, rollo n.º 28/19, interpuesto contra la Sentencia N.º 11/2018, de 2 de octubre, dictada en el procedimiento de reintegro por alcance N.º B-126/17, del ramo de Sector Público Local, Ayuntamiento de ....., Asturias. Ponente: Excma. Sra. D.ª María Antonia Lozano Álvarez.**

  Resumen de doctrina: Tras exponer pormenorizadamente las alegaciones de las partes, la Sala resuelve en primer término la única cuestión procesal suscitada por los apelantes, cual es la petición de suspensión del presente proceso de apelación por concurrir prejudicialidad penal, concluyendo que no precisa de ningún pronunciamiento penal previo para poder conocer y resolver sobre las pretensiones procesales planteadas por las partes en el presente recurso, y que no aprecia la existencia de «elemento previo necesario» ni «cuestión directamente relacionada» con la responsabilidad contable que le impida resolver sobre las cuestiones formales y de fondo que integran el debate procesal de esta segunda instancia.

  A continuación, analiza las pretensiones de las partes relativas a la existencia de un alcance en los fondos públicos, así como los requisitos constitutivos de la responsabilidad contable, y concluye con la procedencia de confirmar los pronunciamientos efectuados en la sentencia de primera instancia.

- **SENTENCIA N.º 20/2019. Recurso de apelación, rollo N.º 32/19, interpuesto contra la Sentencia N.º 9/2019, de 8 de abril, dictada en el procedimiento de reintegro por alcance n.º B-225/15-04, del ramo de Comunidades Autónomas (Consejería de Empleo –Ayudas destinadas a Empresas para la financiación de Planes de Viabilidad– ..., S.L.), Andalucía. Ponente: Excma. Sra. D.ª María Antonia Lozano Álvarez.**

  Resumen de doctrina: Tras exponer pormenorizadamente las alegaciones de las partes, la Sala examina los motivos de los recursos, empezando por los de naturaleza procesal y así, en cuanto a la prejudicialidad penal no puede estimarse, ya que no aprecia la existencia de ninguna cuestión que requiera una previa decisión penal que constituya elemento previo necesario para la declaración de responsabilidad contable y que esté relacionada con ella directamente. En relación con la prescripción, el recurrente alega que la Sentencia apelada fija como *«dies a quo»* para computar el plazo de prescripción las fechas en que se ordenaron los pagos, pero que él no tuvo conocimiento de las actuaciones que se estaban realizando por el Tribunal de Cuentas hasta que se le remitió la demanda formulada por la Junta de Andalucía, habiendo transcurrido por tanto el plazo de prescripción de la responsabilidad contable que se le reclama. La Sala manifiesta a estos efectos, que todas las actuaciones mencionadas forman parte de procedimientos y procesos orientados a investigar los hechos enjuiciados y, por otra parte, tuvieron que ser conocidas por quien tuvo acceso a las citaciones y comunicaciones que se le hicieron llegar formalmente, pero también tuvo que conocer materialmente las actuaciones relativas a la Empresa, ya que era en aquellas fechas administrador de dicha Entidad y encargado de la gestión de la misma. En cuanto a la falta de audiencia del interesado e inválida notificación edictal, tampoco se aprecia irregularidad procesal alguna ni indefensión. En relación con la falta de legitimación pasiva del recurrente, por no haber sido gestor de fondos públicos ni perceptor de los mismos, ya que las ayudas no se le concedieron a él sino a la Empresa, la Sala concluye que la participación del apelante en los hechos tuvo una influencia jurídicamente relevante por lo que concurre su legitimación pasiva en el presente proceso.

  En relación con las cuestiones de fondo, la Sala considera que si la actuación de los recurrentes constituyó o no una estrategia defraudatoria encaminada a un enriquecimiento ilícito a costa de los fondos públicos, no es una cuestión que pueda formar parte del debate procesal de un procedimiento de reintegro por alcance.

2.2. AUTOS

- **AUTO N.º 10/2019. Recurso de Apelación n.º 9/19. Procedimiento de Reintegro n.º B-215/17. Ramo: SECTOR PÚBLICO AUTONÓMICO- (.....) CATALUÑA . Ponente: Excmo. Sr. D. José Manuel Suárez Robledano**

  Resumen de doctrina: La Sala comienza exponiendo que la petición de complemento de Sentencia se fundamenta en dos tipos de alegaciones. En la primera de ellas, el peticionario consideró que se

había omitido un pronunciamiento expreso sobre la falta de responsabilidad contable por alcance respecto al gasto derivado de la elaboración del soporte informático. En la segunda de ellas, volvió a incidir en la vinculación entre los órdenes jurisdiccionales contable y penal, señalando que se habrían omitido unos pronunciamientos respecto a si dicha vinculación ha de ser respecto a sentencias o autos, así como en una supuesta contradicción entre los autos dictados por la Sala de lo Civil y Penal del Tribunal Superior de Justicia de Cataluña y la Sentencia recaída en materia Contable.

Tras analizar las alegaciones vertidas por las partes, la Sala concluye que ambos extremos han sido ampliamente tratados en las sentencias dictadas en primera y en segunda instancia y, por tanto, desestima la solicitud de complemento efectuada.

- **AUTO N.º 11/2019. Recurso del artículo 46.2 de la Ley 7/1988 n.º 26/19. Diligencias Preliminares n.º B-147/18. Sector Público Autonómico (.....), Cataluña. Ponente: Excmo. Sr. D. José Manuel Suárez Robledano.**

Resumen de doctrina: Una vez resumidos los argumentos de las partes, la Sala recuerda el reiterado criterio interpretativo que ha venido elaborando sobre el recurso contemplado en el art. 46.2 LFTCu, contra la resolución de archivo de las actuaciones. Dicho recurso es considerado como un incidente de archivo, cuya finalidad es rechazar *«a limine»* aquellas denuncias que versen sobre hechos que, manifiestamente, no revistan los caracteres de alcance.

A continuación, la Sala pone de manifiesto que no resulta asumible la tesis mantenida por las asociaciones recurrentes, en el sentido de ampliar la acción de responsabilidad contable como consecuencia de los gastos derivados del despliegue policial llevado a cabo por la Administración del Estado, dentro de la llamada «operación Copérnico», por cuanto el debate relativo a los gastos derivados de la partida económica mencionada afecta a la extensión y límites de la propia jurisdicción contable y es susceptible de ser sometido al conocimiento del orden jurisdiccional contencioso-administrativo.

Por ello, la Sala considera plenamente justificado el acuerdo de archivo parcial de las actuaciones adoptado por el Auto objeto de recurso.

- **AUTO N.º 12/2019. Recurso del artículo 48.1 de la Ley 7/1988, de 5 de abril, n.º 27/19. Actuación Previa n.º 182/18. Ramo: SECTOR PÚBLICO LOCAL.- (Ayuntamiento.....) BARCELONA. Ponente: Excmo. Sr. D. Felipe García Ortiz**

Resumen de doctrina: Comienza exponiendo los planteamientos jurídicos realizados por las partes y a continuación alude a la naturaleza jurídica del recurso del artículo 48.1 de la Ley de Funcionamiento del Tribunal de Cuentas —medio de impugnación especial y sumario tendente a impugnar resoluciones similares a las de tipo interlocutorio, dictadas en la fase preparatoria o facilitadora de los procesos jurisdiccionales contables, por medio del cual no se persigue un conocimiento concreto de los hechos objeto de debate en una segunda instancia jurisdiccional sino que, lo que la Ley pretende, es ofrecer un mecanismo de revisión a los intervinientes en la fase de Actuaciones Previas de que se trate de cuantas resoluciones puedan limitar las posibilidades de defensa (Auto de 2 de octubre de 2014)—. Por ello, no ha de entrar la Sala a conocer del fondo del asunto. Los motivos de este recurso no pueden ser otros que los establecidos taxativamente por la ley, es decir, que no se accediera a completar las diligencias con los extremos que los comparecidos señalaren o que se causare indefensión.

En aplicación de lo que antecede, la Sala rechaza los motivos esgrimidos por el recurrente —improcedencia del procedimiento de reintegro por alcance, así como improcedencia de la atribución de responsabilidad contable por alcance— ya que constituyen cuestiones de fondo por completo ajenas a los motivos mencionados.

Por otra parte, aprecia que no se ha producido perjuicio alguno en la posición jurídica y defensa del recurrente, ya que no se le impidió participar en la fase instructora, con independencia de que el mismo pueda legítimamente discrepar de las conclusiones alcanzadas.

- **AUTO N.º 13 /2019. Recurso de apelación n.º 31/19, contra el Auto de 10 de abril de 2019, dictado en el Procedimiento de Reintegro por Alcance n.º B-225/15-27, Ramo Sector Público Autonómico (C.ª de Empleo –Ayudas destinadas a Empresas**

para la Financiación de Planes de Viabilidad– ... .), Andalucía. Ponente: Excma. Sra. D.ª María Antonia Lozano Álvarez.

Resumen de doctrina: Tras exponer pormenorizadamente las alegaciones de las partes, la Sala revisa la adecuación a derecho de la solución a la que llegó el órgano de instancia, favorable a la suspensión del procedimiento contable, al apreciar la existencia de una cuestión prejudicial penal —la posible prescripción de las acciones para la exigencia de responsabilidades contables derivadas de los hechos—, cuya resolución se revela imprescindible para enjuiciar y decidir sobre la responsabilidad contable.

A juicio de la Sala, no concurre en el presente caso elemento alguno que permita soslayar la regla general de compatibilidad de jurisdicciones y sustituirla por la decisión excepcional de suspender el proceso de responsabilidad contable hasta la conclusión del proceso penal que se sigue por los mismos hechos.

Voto particular: El Consejero de Cuentas Excmo. Sr. D. José Manuel Suárez Robledano sostiene que ninguna de las alegaciones manifestadas por las partes apelantes y que han sido asumidas por el criterio mayoritario de esta Sala de Justicia, sirven para combatir la procedencia del Auto recurrido, que se circunscribe al ámbito estricto de la controversia procesal a la que se refiere, no cabiendo apreciar ni en su fundamentación jurídica ni en su parte dispositiva, pronunciamiento alguno que anticipe indebidamente cuestiones sobre la prescripción, propias de la resolución definitiva del procedimiento. Por todo ello, habría resultado procedente desestimar el recurso de apelación interpuesto con expresa imposición de costas.

- **AUTO N.º 14/2019. Recurso del artículo 48.1 de la Ley 7/1988, de 5 de abril, n.º 15/19. Actuación Previa n.º 148/18. Ramo: SECTOR PÚBLICO LOCAL.- (Ayuntamiento .....) MADRID. Ponente: Excmo. Sr. D. Felipe García Ortiz**

Resumen de doctrina: Tras exponer pormenorizadamente las alegaciones de las partes, y hacer referencia a los motivos tasados del recurso del artículo 48.1 LFTCu, así como a la naturaleza de las actuaciones previas aborda las cuestiones relativas a si se ha producido indefensión al recurrente y concluye que no se observa falta de motivación alguna en el Acta de Liquidación Provisional y la decisión contenida en la misma, así como en la Providencia de requerimiento subsiguiente.

En cuanto a la alegación relativa a la pendencia de un procedimiento penal sobre los mismos hechos que se plantean ante esta jurisdicción contable, cabe recordar la reiterada doctrina de esta Sala, (Auto 21/2007, de 6 de marzo, entre otros) conforme a la cual los artículos 18 de la Ley Orgánica 2/82, del Tribunal de Cuentas y 49.3 de la Ley 7/88, de Funcionamiento del Tribunal de Cuentas preceptúan la compatibilidad de la jurisdicción penal y de la contable sobre los mismos hechos.

En cuanto a la solicitud de que se declare el sobreseimiento de actuaciones, no cabe decretar el mismo por la Sala de Justicia, a través del presente recurso, ni tampoco por el órgano instructor en fase de actuaciones previas, debiendo desestimarse la solicitud planteada en este sentido.

Frente a la solicitud de suspensión de actuaciones, y en concreto de la Providencia de requerimiento de pago, depósito o afianzamiento, cabe recordar que la interposición del recurso del artículo 48.1 de la Ley de Funcionamiento del Tribunal de Cuentas, no tiene efecto suspensivo de la eficacia de la resolución impugnada, salvo que concurran circunstancias excepcionales, que en el presente supuesto no concurren.

- **AUTO N.º 15/2019. Recurso de apelación N.º 29/19 formulado por el Procurador de los Tribunales Don Miguel Angel Aparicio Urcía, en nombre y representación de Don I. A. C., contra Auto de 21 de marzo de 2019 dictado en la acción pública N.º C-1/19, del ramo de Sector Público Local, ...Navarra. Ponente: Excmo. Sr. D. José Manuel Suárez Robledano.**

Resumen de doctrina: Tras exponer pormenorizadamente las alegaciones de las partes, la Sala manifiesta que además de no acreditarse debidamente las irregularidades denunciadas, la posible veracidad de las mismas acreditada en un eventual proceso contable, no nos permitiría nunca acceder a lo solicitado por la representación de la parte que ha interpuesto el recurso de

apelación, ya que, atendiendo a los términos en que ha sido planteada la cuestión, no es competencia del Tribunal de Cuentas declarar la mera infracción o aplicación indebida de preceptos contenidos en la Ley de Contratos del Sector Público, desligándolo de la ineludible acreditación de indicios que, según los preceptos de la LOTCu y de la LFTCu y la Jurisprudencia del Tribunal Supremo, permitieran sostener una acción de responsabilidad contable por alcance. Ello representaría la comisión por la Sala de Justicia de un defecto procesal por exceso de jurisdicción.

- **AUTO N.º 16/2019. Recursos de apelación, rollo n.º 30/19, interpuestos contra el Auto de 27 de marzo de 2019, dictados en el procedimiento de reintegro por alcance n.º B-225/15-30, Comunidades Autónomas (C.ª de Empleo –Ayudas destinadas a empresas para la financiación de Planes de Viabilidad– ..., S.L.) Andalucía. Ponente: Excma. Sra. D.ª María Antonia Lozano Álvarez.**

  Resumen de doctrina: Tras exponer pormenorizadamente las alegaciones de las partes, resuelve la cuestión procesal suscitada relativa a la suspensión del proceso por concurrir prejudicialidad penal, concluyendo la Sala que no precisa de ningún pronunciamiento penal previo para poder conocer y resolver sobre las pretensiones planteadas por las partes, y que no aprecia la existencia de *«elemento previo necesario»* ni *«cuestión directamente relacionada»* con la responsabilidad contable que le impida resolver.

  Voto particular: El Consejero de Cuentas Excmo. Sr. D. José Manuel Suárez Robledano sostiene que ninguna de las alegaciones manifestadas por las partes apelantes y que han sido asumidas por el criterio mayoritario de esta Sala de Justicia, sirven para combatir la procedencia del Auto recurrido, que presenta la suficiente justificación, habida cuenta los diferentes plazos en que puede ejercitarse la acción de responsabilidad, según los hechos sean definitivamente declarados como constitutivos de delito, o no, circunscribiéndose la resolución apelada al ámbito estricto de la controversia procesal a la que se refiere, no cabiendo apreciar, ni en su fundamentación jurídica ni en su parte dispositiva, pronunciamiento alguno que anticipe indebidamente cuestiones sobre la prescripción, propias de la resolución definitiva del procedimiento.

- **AUTO N.º 17/2019. Recurso de apelación, rollo n.º 36/19, interpuesto contra el Auto de 18 de marzo de 2019, dictada en el procedimiento de reintegro por alcance n.º B-225/15-31, Comunidades Autónomas (C.ª de Empleo –Ayudas destinadas a empresas para la financiación de Planes de Viabilidad– .... .) Andalucía. Ponente: Excmo. Sr. D. Felipe García Ortiz.**

  Resumen de doctrina: Tras exponer pormenorizadamente las alegaciones de las partes, resuelve la cuestión procesal relativa a la prejudicialidad penal, concluyendo la Sala que no precisa de ningún pronunciamiento penal previo para poder conocer y resolver sobre las pretensiones planteadas por las partes en el presente recurso, y que no aprecia la existencia de *«elemento previo necesario»* ni *«cuestión directamente relacionada»* con la responsabilidad contable que le impida resolver.

  Voto particular: El Consejero de Cuentas Excmo. Sr. D. José Manuel Suárez Robledano sostiene que ninguna de las alegaciones manifestadas por las partes apelantes y que han sido asumidas por el criterio mayoritario de esta Sala de Justicia, sirven para combatir la procedencia del Auto recurrido, que presenta la suficiente justificación, habida cuenta los diferentes plazos en que puede ejercitarse la acción de responsabilidad, según los hechos sean definitivamente declarados como constitutivos de delito, o no, circunscribiéndose la resolución apelada al ámbito estricto de la controversia procesal a la que se refiere, no cabiendo apreciar, ni en su fundamentación jurídica ni en su parte dispositiva, pronunciamiento alguno que anticipe indebidamente cuestiones sobre la prescripción, propias de la resolución definitiva del procedimiento.

- **AUTO N.º 18/2019. Recurso del artículo 48.1 de la Ley 7/88, de 5 de abril, N.º 38/19, Actuaciones Previas N.º 211/18, del ramo de Sector Público Autonómico.- Inf. Fisc. Tcu....., Región de Murcia. Ponente: Excma. Sra. D.º María Antonia Lozano Álvarez.**

  Resumen de doctrina: Tras exponer las alegaciones de las partes, y hacer referencia a los motivos tasados del recurso del artículo 48.1 LFTCu, la Sala manifiesta que la presunta falta de formación contable y presupuestaria del interesado, la ilegalidad o no en su conducta, así como la

solicitud de que la responsabilidad contable se desvíe a los perceptores de subvenciones en lugar de exigirse al gestor público, constituyen cuestiones de fondo que habrán de ventilarse, en su caso, en un momento procesal ulterior.

En cuanto a la alegación del impugnante relativa a la insuficiencia de la documentación en la que la Delegada Instructora fundamentó sus conclusiones la Sala manifiesta que resulta evidente que la Delegada Instructora ha desarrollado una actividad indagatoria suficiente, de acuerdo con el artículo 47.1 de la Ley de Funcionamiento del Tribunal de Cuentas y con los criterios de esta Sala de Justicia, lo que impide que se pueda apreciar la indefensión alegada por el recurrente.

En relación con la alegación relativa a que la ausencia en el procedimiento de los perceptores de las subvenciones constituye una irregularidad procesal determinante de una situación de indefensión para el recurrente, tampoco puede estimarse ya que la Liquidación Provisional impugnada motiva las razones por las que la Instructora considera que la responsabilidad contable del posible alcance detectado debe imputarse.

- **AUTO N.º 19/2019. Recurso del artículo 46.2 de la Ley 7/1988 n.º 39/19. Diligencias Preliminares n.º C-96/19. Sector Público Estatal (.....), Málaga. Ponente: Excmo. Sr. D. José Manuel Suárez Robledano.**

Resumen de doctrina: Tras exponer pormenorizadamente las alegaciones de las partes, la Sala recuerda el criterio interpretativo elaborado sobre el recurso del artículo 46.2 de la LFTCu, a saber, un incidente de archivo cuya finalidad es rechazar *«a limine»* aquellas denuncias que versen sobre hechos que, manifiestamente, no revistan caracteres de alcance. En general, no cabe el archivo *«ex»* artículo 46.2 de la Ley 7/1988, de 5 de abril, de Funcionamiento del Tribunal de Cuentas, si las cuestiones planteadas son inherentes a la gestión de fondos públicos, a infracciones del ordenamiento jurídico presupuestario, y a un posible menoscabo del erario público debido a la adopción de decisiones de gasto y pago, que pudieran haber carecido del suficiente respaldo normativo.

El objeto del presente recurso previsto en el artículo 46.2 de la LFTCu consiste en determinar si procede, o no, el archivo de las Diligencias Preliminares que se iniciaron como consecuencia de presuntas irregularidades en el uso de un coche oficial que, según afirma el Ministerio Fiscal, deberían ser investigadas con arreglo a lo dispuesto en el artículo 47 de la LFTCu.

La Sala manifiesta a estos efectos que las irregularidades apreciadas en su día por la IGAE, dado que parece existir una insuficiente justificación de la afección del uso del medio de locomoción al fin público al que está afectado y, por otro, una duda razonable sobre la naturaleza y adecuado soporte documental del gasto excesivo que gravita sobre dicha utilización, no puede afirmarse que exista una causa patente, clara y descubierta que pueda amparar, sin la práctica de investigación alguna, *«ad limine»,* el archivo de la causa.