



Los sistemas de información y la auditoría informática aplicados a una institución fiscalizadora subestatal: la Sindicatura de Comptes de la Comunidad Valenciana (España)

Information systems and computer auditing applied to a sub-state audit institution: the Sindicatura de Comptes de la Comunidad Valenciana (Spain)

Maria Angeles Abellan¹
Gonzalo Pardo Beneyto²

Resumo

A digitalização é um fenômeno global que afeta todas as atividades humanas. As administrações públicas também incorporaram novas tecnologias de informação e comunicação em suas estruturas e o setor público. A auditoria de computadores é uma ferramenta que permite auditar as administrações públicas e melhorar a prestação de contas. Este artigo examina as principais vantagens e riscos da digitalização e oferece um estudo de caso de uma instituição de auditoria regional na Espanha que implementou a auditoria por computador.

Palavras-chaves: Sistemas de informação. Auditoria por computador. Ciber segurança. Abordagem de risco.

Abstract

Digitization is a global phenomenon that affects all human activities. Public administrations have also incorporated new information and communication technologies into their structures and the public sector. Computer auditing is a tool that allows auditing public administrations and improving accountability. This article examines the main advantages and risks of digitization and offers a case study of a regional audit institution in Spain that implemented computer auditing.

Keywords: Information Systems. Computer audit. Cybersecurity. Risk Approach.

Introducción

La digitalización es un fenómeno que ha afectado a toda la sociedad global, de manera que se ha instalado de forma rápida tanto en el sistema productivo como en las actividades cotidianas de las personas. De hecho, la economía digital es parte de la actividad económica basada en el uso de Internet en numerosos subsectores económicos como el turismo, la salud,

¹ Doutora em Direito, Docente na *Universitat de València*, Espanha.

² Doutor em Direito, Docente na *Universidad de Alicante*, Espanha.

la seguridad, la banca, la logística, la educación, la cultura o el transporte, por citar algunos. Las administraciones públicas no son una excepción y las nuevas tecnologías de la información y la comunicación (TICs) forman parte de sus estrategias modernizadoras en un contexto cambiante y complejo como el que vivimos. Tanto es así que las TICs son un elemento fundamental de los procesos de innovación pública en las instituciones y en los flujos de trabajo dado su potencial transformador. Las administraciones públicas lideran una serie de cambios complejos y este tipo de tecnologías digitales se materializan como su soporte básico.

La revolución digital ofrece numerosos beneficios a la ciudadanía pues agiliza los trámites burocráticos, no requiere presencia física y aporta inmediatez, transparencia, eficiencia, así como menor impacto medioambiental al prescindir del papel. Además, se produce una cierta interacción entre ciudadanía y administración, lo que se genera valor público (Moore, 1998) y se produce un cambio de percepción al orientar las TIC hacia dentro o fuera de la institución (Gil-García, 2012).

La Organización para Cooperación al Desarrollo Económico (OCDE, 2009), el e-gobierno se define como “el uso de las tecnologías de la información y la comunicación y, particularmente, internet como una herramienta para mejorar el gobierno”.

Sin embargo, la implementación del mundo digital en los aparatos político-administrativos conlleva, a su vez, importantes amenazas que hay que combatir para asegurar la seguridad jurídica, la privacidad y la protección de los datos personales de la ciudadanía. En el caso de España, no existe una administración pública que no esté digitalizada en su sentido más amplio del término, es decir, no existen procesos y gestiones administrativos, independientemente del ámbito multinivel o sectorial, que no requiera algún tipo de trámite digital por muy básico que sea. En consecuencia, la transformación digital constituye una de las actividades más importantes del sector público en un entorno absolutamente informatizado como son las fiscalizaciones públicas.

Este artículo profundiza en la fiscalización digital, también conocida como auditoría informática, planteando tanto las ventajas para la rendición de cuentas democráticas como los riesgos inherentes en un mundo de redes interconectadas (Weber, 1998; Hall & Singleton, 2004; Piattini y Del Peso, 2008; Singleton, 2010, 2011). Para ello, hace falta estudiar algunos de los cambios principales producidos en las políticas públicas de implantación de las tecnologías de la información y la comunicación. En este trabajo seguiremos las directrices que han señalado la Organización Internacional de Entidades de Fiscalización Superior (INTOSAI, por sus siglas en inglés) y la Unión Europea en materia digital.

El caso que aquí se documenta es el de la *Sindicatura de Comptes de la Comunidad Valenciana* (España) que es una institución pública fiscalizadora regional que depende del parlamento regional valenciano. La Sindicatura de Comptes vendría a ser un equivalente a una contraloría de nivel regional o subestatal, con funciones de fiscalización y contabilidad de las cuentas públicas delimitadas en su territorio.

Esta institución fiscalizadora se encarga de auditar el gasto público del sector público regional de la Comunidad Valenciana y que, geográficamente, se encuentra al sur de Cataluña con la que comparte rasgos culturales y lingüísticos. La Sindicatura de Comptes tiene atribuidas unas competencias fundamentales, como son las funciones de control y censura de las cuentas públicas del sector público valenciano. La fiscalización de los fondos públicos es *ex post* puesto que el control se realiza sobre la actividad financiera una vez realizada.

La Sindicatura de Comptes de la Comunidad Valenciana ha implementado la auditoría informática para sustituir el soporte físico documental de las fiscalizaciones, por lo que ha entrado de lleno en la transformación digital que se ha mencionado *supra*.

Este estudio nos permite un mejor entendimiento de los elementos relacionados con la rendición de cuentas (*accountability*) como un componente necesario de la democracia representativa, con vocación de control de la gestión pública y como lucha contra el fraude y la corrupción. Si bien las instituciones fiscalizadoras de control externo forman parte del sistema político administrativo, en realidad son poco conocidas por la ciudadanía.

El presente texto se estructura del siguiente modo. En primer lugar, se desarrolla el marco teórico que sustenta este trabajo así como la metodología. A continuación, se abordan las principales tendencias isomórficas en las políticas públicas digitales en el contexto español y de la Unión Europea. En tercer lugar, se plantea la institucionalización de las nuevas tecnologías y la expansión digital en el estudio de caso, con énfasis en las políticas de los sistemas de información adoptadas. Finalmente, se ofrecen unas conclusiones en las que se plantea los inevitables riesgos del entorno digital y la necesidad de establecer defensas eficaces en los sistemas de información.

Referencial teórico

Las bases teóricas que fundamentan este trabajo son el neoinstitucionalismo sociológico y los procesos de isomorfismo normativo, coercitivo y mimético, sin los cuales no se podrían comprender la expansión e implementación de las políticas públicas digitales.

La aplicación del neoinstitucionalismo sociológico en ciencia política y en ciencias de la administración es adecuado para explicar los principales cambios que surgen en las instituciones públicas (Scott, 2008; Olsen, 2009). En concreto y, de cara a este artículo, debemos hacer referencia a tres elementos fundamentales: 1) la importancia del entorno como elemento en el que se gestan las innovaciones, 2) los procesos de adopción de innovaciones en las instituciones y, 3) la finalidad última de los dos puntos anteriores, conseguir legitimidad.

El entorno en el que se insertan las instituciones es fundamental para conocer su evolución, funcionamiento y objetivos. No se debe perder de vista que el mismo condiciona sobremanera su forma de actuar no solo al recibir los insumos que se necesitan para llevar a cabo sus tareas que justifican su existencia, sino que condicionan la toma de decisiones en cuanto a su organización y mejora se refiere (Hodge et al. 2003; Meyer y Rowan, 1977; Brusson, 1986, 1990; Mintzberg, 2012).

Siguiendo dicho razonamiento podemos afirmar, en base al trabajo de DiMaggio y Powell (1983), que el proceso de cambio se produce en las instituciones a través de tres insumos que estandarizan sus dinámicas y funcionamiento: 1) el isomorfismo coercitivo, 2) el isomorfismo normativo y, 3) el isomorfismo mimético. El primero de ellos es el proceso de cambio que se origina por una constricción de instituciones superiores o que tienen un rol de prevalencia sobre la segunda y que se da por cambios en la legislación y sus instrumentos de control. El isomorfismo normativo se entiende como las modificaciones que son auspiciadas por los profesionales y expertos de un sector concreto y en las que se suelen crear redes de aprendizaje e intercambio de información. Por último, debemos hacer referencia al isomorfismo mimético que es la acción de imitar a otro tipo de instituciones en la solución de un problema concreto condicionado por la incertidumbre.

Obviamente, dichos procesos no son automáticos y es en el seno de la organización en la que se toman las decisiones al respecto. Por tanto, toda innovación adoptada tiene una parte estratégica (DiMaggio, 1988, Oliver, 1988) que produce adaptaciones de aquellas modas administrativas presentes en el entorno (Abrahamson, 1996; Czarniawska y Joerges, 1996). Así, el comportamiento de los individuos no será automático, sino que se irá adaptando a los objetivos de la organización y de sus gestores.

Por último, debemos tener en cuenta la legitimidad, que no es otra cosa que “una percepción generalizada o suposición de que las acciones de una entidad son deseables o apropiadas dentro de un sistema socialmente construido de normas, valores, creencias y definiciones” (Suchman, 1995, p. 574). De esta forma, los cambios producidos en una

institución se justifican de acuerdo a estrategias relacionadas con el incremento de la legitimidad y la mejora de la percepción generalizada sobre la misma. Esta forma de proceder no deja de estar relacionada con una necesidad de llevar a cabo cambios en el seno de las instituciones que ha sido abordada desde distintos puntos de vista, pero que coinciden en el mismo punto (Núñez Sabarís, 2016). En última instancia, de lo que trata la institución es que su acción en la sociedad sea reconocida y acatada por la ciudadanía.

Metodología

La presente investigación ha utilizado técnicas e investigación social y ha combinado contenidos de las disciplinas de la ciencia de la administración, ciencia política y teoría de la organización. Asimismo, este trabajo ha necesitado la observación y extracción de datos, la consulta a documentos oficiales, fundamentalmente de la INTOSAI y a fuentes institucionales junto a un repaso a la literatura. Asimismo, se han sistematizado las taxonomías más utilizadas para clasificar el impacto de las tecnologías de la información y la comunicación en las administraciones públicas.

Por otra parte, la estrategia de investigación que se ha seguido es el estudio de caso (*case study*), que considera un único caso. Existen autores que lo rechazan como parte del método comparativo. Morlino (2010, p. 135) sostiene que “el estudio de caso es una estrategia particular de comparación cuya característica es considerar un único caso, lo que permite estudiarlo a fondo”. Para Landman (2012, p. 54), “se consideran comparados los estudios de un solo caso si desarrollan conceptos aplicables a otros casos y/o buscan hacer inferencias de amplio alcance”. En general, el estudio de caso proporciona una descripción contextual y permite enriquecer nuestra comprensión puesto que se centra en explicar al máximo sus características (Levy, 2008; Della Porta, 2013).

Los datos utilizados en este trabajo se han extraído del análisis documental que es una técnica de investigación de la metodología cualitativa (Corbetta, 2003). Se han revisado y estudiado los informes, bases de datos estadísticas, portales de transparencia, legislación multinivel, planes modernizadores sobre gestión pública, boletines oficiales, manuales y normativa de fiscalización y agendas digitales de diversas instituciones nacionales e internacionales. De esta forma, se aporta información fundamentada en los estudios de la Organización para la Cooperación y Desarrollo Económico, de la Unión Europea y de la Organización Internacional de las Entidades Fiscalizadoras Superiores. La investigación documental facilita el estudio y aporta información relevante sobre los acontecimientos del

pasado y permite el seguimiento y secuenciación cronológica hasta la actualidad. Es decir, ofrece un hilo conductor evolutivo que favorece un conocimiento realista de cómo se ha desarrollado un determinado fenómeno social.

Por otro lado, se ha revisitado la bibliografía y se han incluido referencias actuales sobre la auditoría informática y las TICs, que evolucionan rápidamente en nuestra sociedad. Finalmente, se ha analizado la legislación, los protocolos y los reglamentos de servicio y funcionamiento de la Sindicatura de Comptes de la Comunidad Valenciana. Fruto de este análisis, se han obtenido datos empíricos que hemos conectado con el marco teórico utilizado en este trabajo, lo que ofrece una visión de conjunto entre las perspectivas macro y micro del fenómeno digital que se aborda en este artículo.

La tendencia isomórfica de las políticas públicas digitales

En el presente trabajo partimos de la premisa de que las tecnologías de la información y la comunicación son herramientas potentes y transformadoras de la realidad pública, impulsoras del cambio social y que, por esta razón, han de ser estudiadas. Las tecnologías de la información y la comunicación han cambiado la fisonomía de las organizaciones y de los procesos implementando nuevas metodologías que si bien proporcionan muchos beneficios también plantean importantes retos y amenazas para el desempeño público.

La transformación digital se ha materializado en una de las políticas públicas de mayor calado e impacto multisectorial y transversal en la mayoría de países. Y es que las tecnologías de la información y la comunicación se aplican tanto a la elección de los gobernantes, a los procesos políticos y de decisión y a la participación y conformación de las políticas públicas y las decisiones públicas (Remenyi y Wilson, 2007).

A través de diversas denominaciones, desde el último cuarto del pasado siglo hasta el presente, las políticas de transformación digital han estado de forma omnipresentes en las tomas de decisiones gubernamentales.

Esta evolución en el caso español se constata a lo largo de varios hitos que van desde la publicación del *Libro Blanco para la mejora de servicios públicos* (2000), el *Plan Avanza* (2004), el *Informe Reina* (2007), la *Agenda Digital para España* (2013), el *Plan de Transformación Digital de la Administración General del Estado y sus Organismo Públicos* (Estrategia TIC 2015-2020), hasta la actual Secretaría de Estado para el Avance Digital. Todos estos planes son reflejos de la adopción de la legislación y planes europeos sobre la materia mediante procesos de isomorfismo.

El contexto social, económico y político se caracteriza por su dinamismo y complejidad, modificando algunas inercias tradicionales de las administraciones públicas como consecuencia de la digitalización. Pero junto a estas transformaciones también ha aparecido un efecto no deseado pero real y es la percepción de riesgo sistémico procedente de la globalización.

Las administraciones públicas han de procesar una gran cantidad de datos personales y uno de los grandes retos de la actualidad es el abordaje del uso de datos y las implicaciones éticas que conlleva. De hecho, la ética de los datos masivos (*big data*) en las administraciones públicas y su gestión ha de plantearse en esta propuesta como una necesidad democrática de primer orden.

Según Castells (1998, 1999, 2001), vivimos inmersos en una sociedad-red, en la sociedad informacional, que está generando cambios fundamentales en la economía mundial y ha acabado por afectar la creación y distribución de bienes y servicios. La ciudadanía del siglo XXI demanda una administración pública más capacitada para gestionar los recursos públicos y la e-administración legítima y aporta herramientas modernizadoras para la innovación.

La globalización ha creado una tendencia isomórfica de expandir las interconexiones digitales y la economía del conocimiento es un motor de innovación, desarrollo y competitividad que ha materializado en diferentes técnicas de gestión de la calidad (Pardo Beneyto, 2016).

Respecto a los antecedentes de los planes confeccionados por la Unión Europea y de aplicación en sus Estados miembros, podemos hacer referencia a los esfuerzos realizados por Reino Unido, concretamente a planes como *Next Steps*, *Modernizing Government* o el libro Blanco sobre el *Open Government* y Estados Unidos, con documentos como *From Red Tape to Results: Creating a Government that Works better and costs less*, al *Access America* o al *Memorandum sobre Open Government* del presidente Obama. Estas iniciativas sintonizaban con la *New Public Management* y con una tendencia parar reducir el gasto e incrementar la eficiencia (Hood, 1991; Greenwood et al., 2002).

También, se destacan las iniciativas realizadas por Naciones Unidas y, en especial, por la Organización para la Cooperación al Desarrollo Económico para la extensión de las tecnologías de la información. Por su lado, la Unión Europea (UE) puso en marcha la *Agenda Digital* en el marco de la *Europa 2020* para fortalecer un crecimiento inteligente, sostenible e integrador. La Comisión Europea ha dirigido sus esfuerzos para llevar a cabo una transformación digital en la misma línea (Pardo Beneyto, 2018). En esta línea, se ha implementado el *Programa Europa Digital 2021-2027* de la Comisión Europea, cuyo

objetivo general es apoyar la transformación digital de la economía y la sociedad europeas, apoyado en un despliegue a gran escala en todas las áreas de interés público y en el sector privado para completar el mapa de la digitalización.

La administración electrónica representa un proceso isomórfico muy importante para la UE que la considera una máxima prioridad. A través del *Plan de Acción de Administración Electrónica 2016-2020*, la Comisión Europea se propuso como objetivo emprender acciones en torno a tres prioridades: a) modernización de la administración pública apoyada en las TIC's utilizando facilitadores clave (*key enablers*); b) facilitación de la movilidad digital transfronteriza con servicios públicos digitales interoperables (*Enabling Cross-border Mobility*) y, c) accesibilidad de la interacción digital entre ciudadanía, empresas y administraciones para proporcionar servicios públicos de alta calidad (*Facilitation of digital interaction*).

Los principios sustentadores de esta estrategia son los siguientes:

- 1) Digital por defecto, lo que significa que es la opción predominante.
- 2) Principio de una sola vez, que conecta con la reutilización de los datos e implica que el ciudadano no deba presentar documentos cada vez que solicita un servicio público.
- 3) Inclusividad y accesibilidad, lo que supone la reducción de barreras sociales y físicas.
- 4) Apertura y transparencia,
- 5) Visión unitaria de los servicios digitales por encima de las fronteras evitando la fragmentación.
- 6) Interoperabilidad por defecto, entendida como la capacidad de compartir datos y posibilitar el intercambio de información dentro de la UE.
- 7) Confianza y ciberseguridad en el estricto cumplimiento sobre la protección de datos personales, privacidad y seguridad de las TIC's integrándolos en su diseño.

La figura 1 representa la construcción de la arquitectura del Plan Digital de la Comisión Europea.

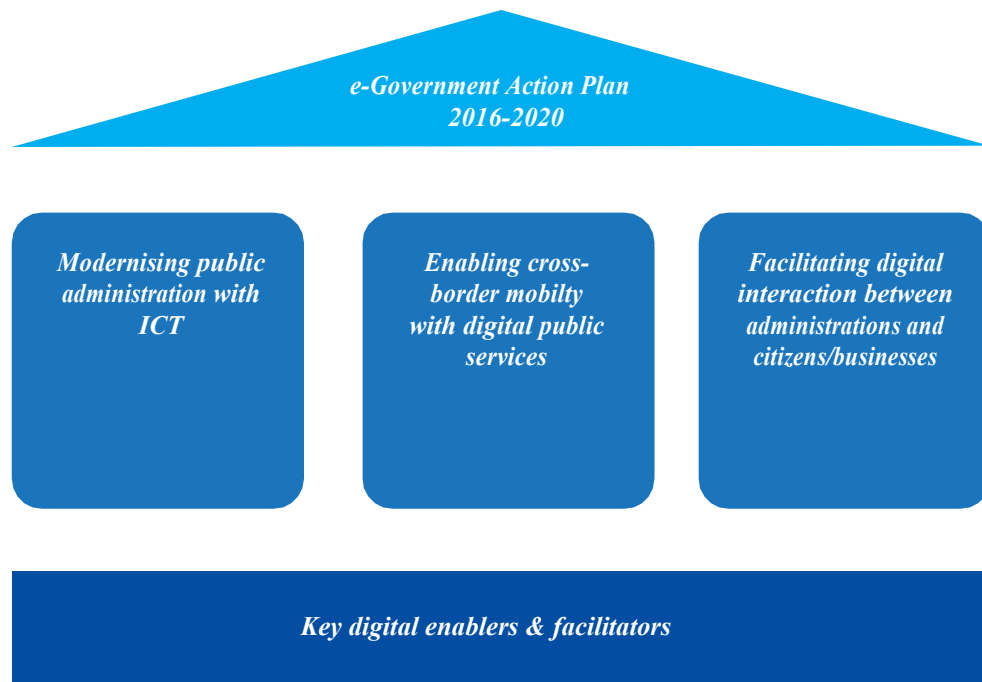


Figura 1. e-Government Action Plan 2016-2020

Fuente: European Commission.

La revolución digital ha supuesto un punto de inflexión en la innovación de las organizaciones públicas ofreciendo a la ciudadanía más posibilidades de interacción y participación. Sin lugar a duda, las nuevas tecnologías son un elemento que, con un buen uso, pueden convertirse en generadores de legitimidad no solo hacia la ciudadanía, sino también para el sistema político y la propia organización.

La institucionalización de la tecnología como adaptación al entorno. El caso de la Sindicatura de Comptes de la Comunidad Valenciana (España)

En este epígrafe vamos a tratar las principales características de la auditoría informática y cómo la ha implementado una institución fiscalizadora regional de España: la Sindicatura de Comptes de la Comunidad Valenciana creada por la Ley de la Generalitat Valenciana 6/1985, de 11 de mayo. Es oportuno contextualizar que la Comunidad Valenciana se creó en 1982 cuando España había realizado su transición a la democracia y pergeñado un nuevo diseño de la distribución territorial del poder con la creación de las comunidades autónomas. De esta forma, el Estado español descentralizado se ha desarrollado durante las últimas cuatro décadas en tres niveles: el Estado central, el sistema autonómico y los entes locales (municipios y provincias). La creación del sistema autonómico, que es donde se ubica la Comunidad Valenciana, aspiraba a institucionalizarse como máxima prioridad. El autogobierno, como parte de un proceso de descentralización política, buscaba la legitimidad

de ejercicio para asegurar su éxito y la fiscalización del sector público autonómico valenciano representaba una prioridad. Por otro lado, en la agenda política de las comunidades autónomas figuraba la puesta en marcha de los servicios y políticas públicas de su competencia. La implementación del Estado de bienestar requería la creación de nuevas estructuras del sector público, en una etapa expansiva de transferencias de las competencias del Estado central a las comunidades autónomas. Estas nuevas estructuras institucionales, con cargo a los presupuestos públicos, debían ser auditadas por el órgano de control externo autonómico (Abellán López, 2018, 2019).

Así pues, desde su creación, la Sindicatura de Comptes de la Comunidad Valenciana, que depende del parlamento regional, ha elaborado auditorías de legalidad, de conformidad financiera y operativa, las cuales requieren una utilización intensiva de las tecnologías de la información. La informatización abrió la posibilidad a la gestión masiva de los datos y a la realización de fiscalizaciones más completas e integrales hasta el punto de que se ha producido lo que Michael Power (1996) denomina “explosión de auditoría”, para referirse al fenómeno intensivo y extensivo de las auditorías.

En este contexto, la auditoría informática se presenta como la herramienta imprescindible para revisar y examinar de manera sistemática y analítica los sistemas de información, los procedimientos, actividades, programas u operaciones que realiza el sector público, lo que permite evaluar el cumplimiento de legalidad, la conformidad financiera, su eficacia, eficiencia y economía en la utilización de los recursos disponibles. Uno de sus objetivos estratégicos fue fortalecer las TIC's aplicadas a las fiscalizaciones, lo que implicaba un rediseño de su estructura organizativa. Las unidades de nueva creación fueron el Gabinete Técnico, la Unidad de Auditoría de Sistemas de Información (UASI) y la Comisión Técnica de Auditoría (CTA). De esta manera, la institución fiscalizadora elaboró un protocolo de políticas de gestión y ciberseguridad de los sistemas de información (SI) en 2009 y que actualizó en 2019, incluye las siguientes directrices de la figura 2.

Principios de política de la seguridad informática de la Sindicatura de Comptes
La seguridad de los SI como proceso integral
Gestión de la seguridad basada en riesgos
Prevención, reacción y recuperación
Líneas de defensa
Reevaluación periódica

La seguridad como hecho diferencial y objetivo en sí mismo
Concienciación, responsabilidad y capacitación permanente del personal

Figura 2. Los principios de los sistemas de información (SI)

Fuente: Elaboración propia a partir de la Sindicatura de Comptes.

De esta forma, el órgano de control externo valenciano ha podido atender las principales demandas en su misión en entornos intensamente informatizados. El rediseño de los circuitos de los sistemas de información se hizo extensivo a todas las áreas funcionales de la Sindicatura de Comptes adoptando un enfoque transversal a todos los procesos y fiscalizaciones. La aspiración de integrar la auditoría de sistemas de información en las fiscalizaciones era una necesidad puesto que todas las actividades, procesos y operaciones se han generalizado en entornos informatizados. El objetivo concreto era tanto proporcionar un soporte sólido a los equipos de fiscalización como dotarse de una infraestructura capaz de revisar los propios sistemas de información. Se partía de la idea de que era necesario auditar los propios sistemas informáticos del sector público para poder pronunciarse objetiva y verazmente sobre la liquidación presupuestaria del gasto público.

Pensemos que el sistema de control externo debe adaptarse a la digitalización incorporando herramientas y metodologías que le permitan acceder a los sistemas de gestión que se pretenden fiscalizar. Dificilmente puede auditarse sin soporte informático la gestión de la receta electrónica, la gestión de la nómina de los empleados públicos, el sistema de control interno de los diferentes entes públicos, la gestión de compras, *e-procurement*, el registro de facturas, la auditoría operativa de indicadores de la e-Administración, etc. El control interno de las administraciones públicas se ha informatizado al 100% y ello conduce necesariamente a que el control externo opere en idénticas condiciones para desarrollar su misión.

Algunas de las áreas de mayor incidencia para la auditoría pública son la contabilidad, el gasto público, los recursos humanos, las subvenciones, la contratación, los tributos y la recaudación cuyo soporte es íntegramente digital. Fiscalizar todas estas áreas requería la implantación de la auditoría informática, también conocida como papeles de trabajo electrónico. Por *papeles de trabajo* se entienden los apuntes contables o documentos que constituyen la prueba, la verificación de las conclusiones o juicios de los auditores públicos. Durante las fiscalizaciones, los auditores constatan evidencias y formulan juicios que vinculan el trabajo de campo con el informe de fiscalización. Estas evidencias son las pruebas materiales, documentales y testimoniales. Cuando hablamos de evidencia informática nos referimos a la información contenida en soporte digital en la que se fundamenta el informe de

fiscalización y que se materializa en apuntes contables, contratos, facturas, confirmaciones, órdenes de pagos electrónicos, etc.

El sistema de papeles de trabajo electrónico ha permitido a la Sindicatura de Comptes ser más eficiente en el proceso documental, en la elaboración de informes y en las revisiones posteriores. La auditoría informática permite que varios auditores o usuarios pueden acceder simultáneamente y, a la vez, ha mejorado la estandarización del trabajo lo que repercute en la mejora de la calidad de las auditorías.

Sin embargo, como en cualquier otra aplicación digital, la auditoría informática no está exenta de riesgos y es necesario conocerlos para establecer defensas. La figura 3 recoge una serie de principios generales de la auditoría del sector público según la Norma ISSAI-100. Las ISSAI (*International Standards of Supreme Audit Institutions*) son las normas internacionales de las Entidades Fiscalizadoras elaboradas por la Organización Internacional de Entidades de Fiscalización Superior, de aplicación mundial que permiten la homogeneidad y la comparabilidad de la información contable. Uno de estos principios de las ISSAI es el denominado riesgo de auditoría, entendido como la valoración de que un error puede cometerse por la falta de evidencia o por la obtención de una evidencia insuficiente o incompleta.



Figura 3. Principios generales de auditoría del sector público

Fuente: Elaboración propia a partir de la Norma ISSAI-100

El riesgo de auditoría también existe en la auditoría informática como se aprecia en la figura 4, en la que se describen las principales características de tales riesgos.

Principales riesgos de la auditoría informática
La ausencia de transacciones, de documentos en soporte papel, como pedidos, albaranes, facturas, cheques, etc.
El riesgo de manipulación de la información o alteración de pruebas visibles
La pérdida generalizada de pistas visibles de auditoría.
La desaparición de los libros de contabilidad tradicionales en papel, y su sustitución por las bases de datos contables.
Concentración de tareas digitales en una sola persona que antes ejecutaban varias y que puede incurrir en la realización de funciones incompatibles.
Posibilidad de acceso a personas no autorizadas
Ejecución automática de tareas que no estén documentadas y que no puedan ser validadas posteriormente
Volumen masivo de datos y transacciones que dificultan la corrección de errores u omisiones en el proceso
La intangibilidad de los elementos de trabajo

Figura 4. Principales riesgos de la auditoría informática

Fuente: Elaboración propia.

Una de las principales responsabilidades de los auditores es asegurar la integridad de los datos, es decir, que la información contable obtenida a través de las aplicaciones informáticas sea idéntica a los datos del sistema fiscalizado.

Auditar organizaciones implica evaluar entidades que tienen toda su gestión informatizada y que su información económica fiscal está almacenada digitalmente. Lo que se fiscaliza es información procesada y guardada en incontables de registros que requieren mecanismos de almacenamiento analítico de los datos. Las organizaciones públicas registran cada vez más información de los ciudadanos, de sus clientes, de los proveedores y de sus empleados. El verdadero reto es enfrentarse tanto a un aumento de la cantidad de información como a la novedad de los datos que se procesan, lo que exige herramientas digitales cada vez más avanzadas para extraer información. Esta situación, cantidad y novedad de los datos, es la que plantea la necesidad de una adecuada regulación legal en materia de privacidad y seguridad.

Por esta razón, la auditoría informática ha adoptado el enfoque de riesgos conocido como Auditoría Basada en el Análisis de Riesgos (ABAR). El diseño de un mapa de riesgos y su evaluación permiten tomar consciencia de las vulnerabilidades de auditoría para minimizarlas. Un enfoque ABAR supone la secuencia progresiva de varias fases como el

análisis de los riesgos de la utilización de las tecnologías de la información, la evaluación de su fiabilidad y la valoración de la eficacia de los controles y procesos.

En este punto, parece conveniente aclarar que la actividad auditora es siempre una actividad de riesgos puesto que no se trata de una mera inercia mecánica, sino que supone una opinión global del resultado del trabajo de fiscalización. Y aunque las nuevas tecnologías permitan examinar en algunos casos un 100% de transacciones para conocer si se adecuan al cumplimiento de legalidad y conformidad financiera, los auditores utilizan el muestreo estadístico sobre los elementos auditables. Dicho de otro modo, implica un juicio profesional fundamentado en evidencias adecuadas extraídas de muestras sobre una determinada parcela de gestión que han de trasladarse al informe de fiscalización de forma transparente. Asimismo, cuando se trata de auditorías operativas, la investigación requiere flexibilidad, imaginación y gran competencia analítica. De lo señalado hasta el momento, se desprende la complejidad de la auditoría informática que ha de integrar la auditoría financiera, la de cumplimiento de legalidad y, en su caso, la auditoría operativa. Los principales esfuerzos se han centrado en hibridar la metodología de la auditoría financiera y la auditoría informática adoptando un enfoque de riesgo.

¿Por qué es importante el enfoque de riesgos? La interconexión global conlleva la emergencia de riesgos digitales, a los que ninguna organización puede ser ajena. La ciberseguridad se ha convertido en una preocupación gubernamental, de gran repercusión mediática que inquieta a políticos, a directivos, gestores, interesa a los auditores y afecta a toda la ciudadanía. Las amenazas y las vulnerabilidades del ciberespacio, que aloja millones de unidades de información sobre nuestros datos, constituye uno de los frentes de batalla más prioritarios de las distintas organizaciones nacionales e internacionales, públicas y privadas. Y es que la información se ha convertido en una materia prima muy valiosa y los datos son una categoría de activo económico muy importante en nuestra economía y sociedad contemporáneas.

Todo esto requiere proporcionar a los auditores públicos una formación muy especializada. Un auditor destinado a las fiscalizaciones informáticas ha de conocer el *software* que apoya su tarea y el que soporta los sistemas que ha de auditar. Porque solo es posible reducir los riesgos de las fiscalizaciones si los auditores están capacitados en técnicas y metodologías adecuadas que les permita detectar los errores, fraudes y anomalías. Los auditores han de estar familiarizados con los entresijos de la organización que han de fiscalizar, con los procedimientos, procesos y gestiones más habituales, la dirección de sus flujos de información, las aplicaciones utilizadas, las interfaces y las diferentes bases de datos

que contengan la información almacenada. Basta pensar en las numerosas bases de datos y ficheros donde se almacena información de cualquier organización pública que registran todas sus operaciones realizadas durante el ejercicio presupuestario. El auditor o auditora público debe ser capaz de extraer y comprender la estructura de los datos del sistema que ha de fiscalizar y debe saber dónde se almacenan y cuáles son los más significativos, desde el punto de vista de la auditoría.

Las contribuciones positivas de las auditorías informáticas a la buena gobernanza son evidentes porque suministran información confiable a la ciudadanía basada en evidencias empíricas, mejoran los procesos de rendición de cuentas y la transparencia, legitima a las organizaciones acciones y crean incentivos para mejorar la toma de decisiones, tanto desde el punto de vista económico financiero como de gestión pública.

Conclusiones

La digitalización se ha desarrollado a velocidad de vértigo en la sociedad y en todo el sistema productivo. Adquirimos bienes y servicios *on line*, trabajamos o buscamos trabajo a través de dispositivos tecnológicos, nos relacionamos con otras personas a través de redes sociales y correo electrónico. La globalización ha posibilitado un mundo interconectado, que ofrece más posibilidades de información pero que tiene su contrapunto en la rapidez y el volumen de información que genera.

Las organizaciones públicas tienen competencias en muchos subsectores económicos como el turismo, la salud, la seguridad, la banca, la logística, la educación, la cultura o el transporte y todos ellos se han visto afectados por las TICs. Los servicios públicos, el Estado de bienestar y las instituciones públicas se han digitalizado de manera intensiva. Por esta razón, la rendición de cuentas públicas ha de utilizar la auditoría informática para fiscalizar el gasto público.

Sin embargo, la auditoría informática también incluye riesgos y por esta razón se ha implementado un enfoque para detectar los riesgos digitales. La ciberseguridad, las amenazas y las vulnerabilidades del ciberespacio, que aloja millones de unidades de información sobre nuestros datos, constituye uno de los frentes de batalla más prioritarios de las distintas organizaciones nacionales e internacionales, públicas y privadas. Y es que la información se ha convertido en una materia prima muy valiosa y los datos son una categoría de activo económico muy importante en nuestra economía y sociedad contemporáneas.

A través del estudio de caso, la Sindicatura de Comptes de la Comunitat Valenciana (España), equivalente a una contraloría regional, se ha ofrecido un ejemplo de implementación de la auditoría de sistemas de información para la mejora de la eficacia y la eficiencia del control externo de las cuentas públicas. La Sindicatura de Comptes ha asumido la incorporación de herramientas disponibles en el ámbito de la fiscalización y la informática, en un lógica isomórfica propia de la globalización.

En la actualidad, la auditoría informática está íntegramente implementada para llevar a cabo las fiscalizaciones y se están desarrollando actuaciones en materia de ciberseguridad. El objetivo es asegurar la integridad de los datos, evitar su manipulación y elaborar estrategias para minimizar las vulnerabilidades y brechas de seguridad. Las principales ciberdefensas son la monitorización y el mapeo sistemático, la capacitación del personal, la gestión diligente y el control de las vulnerabilidades.

De este modo, las auditorías informáticas serán más seguras, de mayor alcance y más eficaces en su cometido fiscalizador. En definitiva, las auditorías informáticas como instrumento de la rendición de cuentas contribuyen a la legitimidad del sistema político.

Bibliografía

- Abellán, M.A. (2019). *Rendición de cuentas y control externo en España: una aproximación a las instituciones fiscalizadoras desde el contexto de la modernización política administrativa*. Madrid: Tirant lo Blanch-Instituto Nacional de Administración Pública (INAP).
- Abellán, M.A. (2018). *La Sindicatura de Comptes de la Comunitat Valenciana 1985-2015. Un estudio dinámico de tres décadas como institución fiscalizadora de autogobierno*. València: Corts Valencianes.
- Abrahamson, E. (1996). Management Fashion. *Academy of Management Review*, 21, (1), 254-285.
- Brunsson, N. (1986). Organizing for inconsistencies: On organizational conflict, depression and hypocrisy as substitutes for action. *Scandinavian Journal of Management Studies*, 2, 165-185.
- Brunsson, N. (1990). Deciding for Responsibility and Legitimation: Alternative Interpretations of Organizational Decision-Making. *Accounting, Organizations and Society*, 15, 47-59.
- Castells, M. (1998). *La Sociedad-Red*. Madrid: Alianza.

- Castells, M. (1999). *La era de la Información. Economía, sociedad y cultura. La Sociedad* Red. Vol. I. México: Siglo XXI.
- Castells, M. (2001). *La galaxia Internet. Reflexiones sobre Internet, empresa y sociedad*. Madrid: Plaza & Janés.
- Corbetta, P. (2003). *Metodología y técnicas de investigación social*. Madrid: McGraw-Hill.
- Czarniawska, B. y Joerges, B. (1996). Travels of ideas, en B. Czarniawska y G. Sevón (Eds.) *Translating Organizational Change*. Berlín: de Gruyter.
- Della Porta, D. (2013). “Análisis comparativo: la investigación basada en casos frente a la investigación basada en variables”, en Della Porta, D. y Keating, M. (Coord.) *Enfoques y metodologías de las Ciencias Sociales*. Madrid: Akal.
- DiMaggio, P. J. (1988). Interest and Agency in Institutional Theory, en L. Zucker (ed.), *Institutional patterns and organizations*. Cambridge, Massachussets: Ballinger.
- DiMaggio, P.J., & Powell, W. (1983). The iron cage revisited: institutional isomorphism and collective rationality in organizational fields. *American Sociological Review*, 48(2), 147-160.
- European Commission (2018). *E-Government Benchmark 2018. Securing eGovernment for all*. Capgemini, IDC, Sogeti & Politecnico di Milano. doi: 10.2759/473144
- Gil-García, J. R. (2012). *Enacting Electronic Government Success*. Nueva York: Springer.
- Greenwood, R., Suddaby, R., & Hinings, C. (2002). Theorizing Change: The Role of Professional Associations in the Transformation of Institutionalized Fields. *The Academy of Management Journal*, 45(1), 58-80. doi:10.2307/3069285
- Hall, J. y T. W. Singleton (2004). *Information Systems Auditing and Assurance Paperback*. UK: South-Wertern College Pub.
- Hodge, B. J., William, P. A., & Gales, L. M. (2003). *Teoría de la Organización. Un enfoque estratégico*. Madrid: Pearson.
- Hood, C. (1991). A Public Management for all Seasons? *Public Administration*, 69, 3-19.
- Landman, T. (2011). *Política comparada. Una introducción a su objeto y métodos de investigación*. Madrid: Alianza editorial.
- Levy, J.S. (2008). “Case Studies: Types, Designs, and Logics of Inference”. *Conflict Management and Peace Science*, 25(1), 1-18.
- Meyer, J. W., y Rowan, B. (1977). “Institutionalized Organizations: Formal Structure as Myth and Ceremony”, *American Journal of Sociology*, 83, 340-363.
- Mintzberg, H. (2012). *La estructuración de las Organizaciones*. Madrid: Alianza.

- Moore, M. H. (1998). *Gestión estratégica y creación de valor en el sector público*. Barcelona: Paidós.
- Morlino, L. (2010). *Introducción a la investigación comparada*. Madrid: Alianza Editorial.
- Núñez Sabarís, A. (2016). “Transformaciones en la gestión pública, condicionantes históricos y tradición administrativa: aportes de la investigación sobre el caso español al debate internacional y la literatura comparada”, en Criado, J.I. (ed.) *Nuevas tendencias en la gestión pública. Innovación abierta, gobernanza inteligente y tecnologías sociales en unas administraciones públicas colaborativas*, 49-67. Madrid. INAP.
- Organización para la Cooperación al Desarrollo Económico (OCDE). (2009). *e-Gobierno para un mejor gobierno*. Madrid: INAP. <https://doi.org/10.1787/9789264062603-es>.
- Oliver, C. (1988). The Collective Strategy Framework: An Application to Competing Predictions of Isomorphism. *Administrative Science Quarterly*, 33(4), 543-561.
- Olsen, J. P. (2009). Change and continuity: an institutional approach to institutions of democratic government. *European Political Science Review*, 1, 3-32.
- Pardo Beneyto, G. (2016). “El uso de las cartas de servicio en la administración local: el caso del Ayuntamiento de Torrent”. *Barataria*, 21, 191-2015.
- Pardo Beneyto, G. (2018). *La Modernización de la Administración Local Municipal: la Innovación y la Reingeniería de Procesos en los Ayuntamientos de Alicante y València (2001-2016)*. Tesis doctoral, Universidad de Alicante.
- Piattini, M., E., Del Peso & M. del Peso (2008). *Auditoría de Tecnologías y Sistemas de Información*. RAMA, S.A. Madrid.
- Power, M. (1996). *The Audit Explosion*. London: Demos.
- Remenyi, D. & Wilson, D. (2007). “e-Democracy: An “e” Too Far?”, en Griffin, D., Trevorrow, P., Halpin, E. (eds.) *Development in e-Government. A critical Analysis*, 89-100. Amsterdam: IOS.
- Scott, W. R. (2008). “Approaching adulthood: the maturing of institutional theory”. *TheorSoc*, 37, 427-442.
- Singleton, T. W. (2010). “Data Extraction, A Hindrance to Using CAATs”. *ISACA Journal*, 6, 1-2.
- Singleton, T. W. (2011). Cómo el auditor de TI puede hacer contribuciones sustanciales a una auditoría financiera. *ISACA Journal*, 1, 1-3.
- Suchman, M. S. (1995). Managing Legitimacy: Strategic and Institutional Approaches. *The Academy of Management Review*, 20(3), 571-610.
- Weber, R. A. (1998): *Information Systems Control and Audit*. Pearson Education.
- Revista de Gestão e Secretariado (GeSec), São Paulo, SP, 11(2), maio/ago., 2020, p. 121-138.

Submetido em: 22.01.2020

Aceito em: 11.04.2020