Revista Española de Documentación Científica
43(3), julio-septiembre 2020, e272
ISSN-L:0210-0614. https://doi.org/10.3989/redc.2020.3.1666

ESTUDIOS / *RESEARCH STUDIES*

La gestión documental en los modelos de gobernanza TIC: presencia y visibilidad de la normativa internacional en el modelo de referencia COBIT

Ricardo Eito-Brun*, Coral Calleja Aliaga**

* Universidad Carlos III de Madrid.
Correo-e: reito@bib.uc3m.es | ORCID iD: http://orcid.org/0000-0003-1219-0510

** Sagardoy Abogados S.L.
Correo-e: cca@sagardoy.com | ORCID iD: http://orcid.org/0000-0001-8919-8727

Recibido: 13-03-2019; 2ª versión: 09-09-2019; Aceptado: 27-09-2019.

Cómo citar este artículo/Citation: Eito-Brun, R.; Calleja Aliaga, C. (2020). La gestión documental en los modelos de gobernanza TIC: presencia y visibilidad de la normativa internacional en el modelo de referencia COBIT. *Revista Española de Documentación Científica*, 43 (3), e272. https://doi.org/10.3989/redc.2020.3.1666

Resumen: La gobernanza y gestión de servicios y sistemas de información disponen de una serie de normas que reúnen las mejores prácticas desarrolladas por instituciones y empresas. Esta experiencia se presenta en la forma de marcos de referencia que definen objetivos, indicadores y procesos, y que se pueden usar como guía para definir los procesos internos y comparar la actuación de las organizaciones con las buenas prácticas de la industria. Entre ellos destacan el modelo COBIT desarrollado por ISACA (*Information Systems Audit and Control Association*) y la norma internacional ISO/IEC 38500, dedicados a la gobernanza TIC.

En este artículo se analiza la presencia de las prácticas de gestión documental en el marco del modelo COBIT y la visibilidad de las normas específicas de gestión de documentos ISO 15489 e ISO 30300 en el mismo.

Palabras clave: Gestión documental; normas técnicas; COBIT; marcos de referencia; gestión de activos y TIC.

Records and document management in the IT Governance frameworks: best practices and standardization (COBIT framework)

Abstract: Organizations have at their disposal different standards that provide guidance for the governance and management of information services and systems. These standards are made up of the best practices developed by public and private organizations. They are also presented in the form of frameworks that define objectives, key process indicators and processes. Entities can use these frameworks and standards as a basis to define their own internal processes and compare them with the best practices in the industry. Among these frameworks, one that is especially relevant is the COBIT model developed by ISACA (Information Systems Audit and Control Association) and international standards like ISO/IEC 38500.

This paper analyses the presence of document management practices and specific standards (in particular ISO 15489 and ISO 30300) within the COBIT framework.

Keywords: Records management; technical standards; COBIT; reference frameworks; information assets management.

1. INTRODUCCIÓN

Los marcos para la gobernanza y gestión de las tecnologías de la información (TIC) surgieron como respuesta a la necesidad de contar con prácticas comunes para la gestión de activos de información, y establecer controles para paliar y mitigar los efectos negativos de los riesgos. El desarrollo de estos marcos y el concepto de gobernanza adquirieron relevancia a partir de la década de los noventa, con la publicación del *Informe Cadbury* (Financial Reporting Council, 1992) y los *Principios de gobernanza corporativa* de la OCDE (1998). Su desarrollo ha sido resultado de una acción progresiva, alineada con los cambios producidos en la sociedad de la información y en las tecnologías (Gelbstein, 2016).

El principal objetivo de la gobernanza de las TIC es la dirección y control del uso actual y futuro de las tecnologías de la información (ISO/IEC 38500, p. 8). La evolución de las tecnologías implica oportunidades y riesgos que obligan a establecer controles para evitar la pérdida o el deterioro de la información, asegurar su fiabilidad, autenticidad y accesibilidad. La gobernanza debe atender al complejo nexo entre datos y tecnologías que constituye la base para asegurar la prestación de servicios y la ejecución de las actividades cotidianas de las organizaciones. En la actualidad, las iniciativas de digitalización vuelven a situar a las TIC y a la información – en cualquiera de sus formas – entre los principales activos de las organizaciones junto al capital humano y el intelectual, y se exige redefinir los procesos de negocio a partir de volúmenes crecientes de datos y de la eclosión de nuevas tecnologías.

La gestión de los activos de información debe considerar riesgos asociados a la privacidad, precisión e integridad de los datos y establecer mecanismos de control y auditoría (Smallwood, 2014). Recae sobre la dirección de las organizaciones cualquier responsabilidad derivada del incumplimiento de la legislación sobre privacidad, protección de datos, retención de información, etc., así como las del incumplimiento de los requisitos de continuidad y sostenibilidad. Solo mediante una planificación y control efectivo de su *información documentada*– si utilizamos la terminología de ISO 9000 – y de las tecnologías, pueden las organizaciones avalar su trayectoria y dar testimonio fiel de sus actividades.

Se han formulado distintas respuestas a estas necesidades, entre ellas el desarrollo de marcos de referencia y normas internacionales. Entre los primeros destaca, por su amplia adopción internacional, las guías y pautas publicadas por ISACA (*Information Systems Audit and Control Association*) en su modelo COBIT (*Control Objectives for Information and related Technology*). Otro referente que debe citarse es la norma internacional ISO/IEC 38500, dedicada en exclusiva a la gobernanza corporativa de las TIC. Sirven de apoyo a ésta otras normas de contenido más técnico como ISO/IEC 27001 e ISO/IEC 20000, orientadas a la gestión de la seguridad de la información y a la gestión de servicios.

Los objetivos de estos referentes para la gobernanza TIC nos llevan a considerar su paralelismo con los estándares para los sistemas de gestión de documentos (SGD) definidos en las normas ISO 15489 e ISO 30301. El propósito y evolución de estas normas ha sido discutido en distintas contribuciones (Bustelo, 2007; Healy, 2010; Joseph y otros, 2012; García-Morales, 2014), así como su aplicación práctica (Dherent, 2006; Grimal-Santos y otros, 2009; García-Alsina, 2012; Oliver, 2014). Su relación con otras normas de gestión también ha sido analizada: Lomas (2010) trató la compatibilidad entre ISO 15489 e ISO 27000; Moro-Cabero y otros (2011) estudiaron la complementariedad de ISO 15489 con ISO 9000, ISO 14000 e ISO 27000, y Conde-Hernad y Gonzalez-Gaya (2013) describieron su uso como base para la gestión de documentos en sistemas de gestión de calidad ISO 9001.

Sin embargo, en la literatura no se encuentra ningún análisis entre las normas de gestión de documentos y su aplicación en el contexto de la gobernanza. En los siguientes apartados se presentan las características de los marcos de referencia para la gobernanza TIC, y un análisis de su complementariedad con las normas de gestión de documentos ISO 15489 e ISO 30301.

El trabajo pretende analizar la complementariedad de estos marcos y normas, y dar respuesta a las siguientes interrogantes:

- Analizar el nivel de cobertura que ofrece el modelo COBIT a los principios y prácticas de gestión documental.
- Evaluar las similitudes y la concordancia entre las prácticas para la gestión de documentos que recoge el modelo COBIT y las normas ISO 15489 y 30301.
- Conocer en qué medida el modelo COBIT hace referencia a la normativa internacional sobre gestión de documentos, y a partir de este punto comprobar si las citadas normas han alcanzado un nivel de visibilidad suficiente en la comunidad dedicada a la gobernanza.

2. ANTECEDENTES: MARCOS DE REFERENCIA PARA LA GOBERNANZA

Las principales referencias para la gobernanza TIC las encontramos en el modelo COBIT y en la norma ISO 38500.

El primero – COBIT - es el marco más popular, y la principal contribución de la organización internacional ISACA, creada en 1967 con el fin de desarrollar guías en el área de auditoría de sistemas de información. Esta surgió en la década de los setenta como una actividad de apoyo a la auditoría financiera y contable, y en respuesta a la informatización de la gestión económica de las empresas. La adherencia a las pautas dictadas por ISACA permite a los profesionales actuar con homogeneidad en los procesos de auditoría. ISACA también ofrece servicios de certificación de habilidades y conocimientos para la planificación, despliegue, control y auditoría de sistemas de información[1]. Las actividades de difusión se materializan a través de publicaciones como *ISACA Journal* y conferencias internacionales. En la actualidad, cuenta con presencia en más de ochenta países y con más de cien mil profesionales asociados procedentes de distintos sectores: finanzas, administración pública, servicios, industria, etc. En España cuenta con tres delegaciones en Barcelona, Madrid y Valencia.

COBIT se publica desde 1996, y proporciona una visión global para la gobernanza de los sistemas de información de las organizaciones, si bien inicialmente se centró en las prácticas de auditoría. Posteriormente, se amplió su alcance para cubrir las áreas de gestión, control y gobierno de las TIC y asegurar que éstas se alinean con las necesidades de las partes interesadas, se planifican, monitorizan y controlan (Smallwood, 2014). La última revisión se ha publicado recientemente: COBIT®2019. Las sucesivas versiones de COBIT añadieron guías y pautas para la autoevaluación, indicadores de desempeño, y evolucionaron el conjunto de procesos para alinearse con otros marcos independientes como Val IT, Risk IT o ITIL. Esta evolución incorporó una perspectiva global para la gestión de la información – no sólo de las TIC - como activo estratégico para asegurar el cumplimiento de las regulaciones, marcos legales y normativos que conforman el contexto en el que opera una organización. Aunque COBIT y las normas de gestión de documentos han tenido un origen y una evolución independientes, se puede observar un aspecto común entre ambas; ISO 15489, que se publicó con posterioridad a COBIT, su primera versión en 2001, recogía en su capítulo 5 la necesidad de "*identificar el marco reglamentario que afecta a las actividades de la organización*" y el que la organización "*debería poder probar a través de sus documentos que realiza sus actividades de acuerdo con el marco reglamentario.*"

COBIT parte de dos principios: la información es un recurso clave para cualquier organización, y la tecnología permite generarla y custodiarla (Anderson, 2012). El modelo facilita definiciones, buenas prácticas y modelos estructurados en torno a cinco principios y siete facilitadores.

Los cinco principios son los siguientes (ISACA, 2012a, p. 13):

- *Satisfacer las necesidades de las partes interesadas*.
- *Tratar las necesidades de la organización de forma integral*, de forma que el gobierno de las TIC esté integrado en el gobierno de la organización y cubra todas las funciones y procesos.
- *Aplicar un solo marco integrado*, que reúna a los distintos modelos y normas usados como referencia en las organizaciones. Dentro de estos modelos se cita COSO *(Internal Control--Integrated Framework)*, ISO/IEC 31000 para la gestión de riesgos, TOGAF para el diseño, planificación e implementación de la arquitectura empresarial y PMBOK (*Project Management Body of Knowledge*) para la gestión de proyectos.
- *Habilitar un enfoque holístico*, que integre los distintos factores que influyen en el cumplimiento de los objetivos de la organización a través de la consecución progresiva de metas en cascada.
- *Separar el gobierno de la gestión o administración*; si el primero evalúa las necesidades de las partes interesadas y define objetivos en el marco de una estrategia, la segunda función establece prioridades y revisa su cumplimiento centrándose en la planificación, ejecución y seguimiento de las actividades alineadas con los objetivos establecidos por el primero (ISACA, 2012a, p. 31). Este principio también se destaca en la norma ISO/IEC 38500, que limita la gobernanza a quienes ostentan la máxima responsabilidad en la empresa: consejo de administración, administradores únicos o figuras equivalentes.

En la nueva versión de COBIT, estos principios se han reformulado ligeramente para hablar de un sistema de gobernanza dinámico y adaptado a las necesidades de la organización.

Junto a estos principios, COBIT define los llamados factores habilitadores, facilitadores o *catalizadores* (este último término es el utilizado en la documentación oficial en español). Se refieren a los factores que permiten alcanzar las metas y los objetivos de la organización. La versión 2019 mantiene los siete catalizadores de la versión anterior, si bien se opta por hablar de *componentes del sistema de gobernanza* que – de forma individual

o conjunta, contribuyen a la misma e interactúan entre sí. Los catalizadores incluyen: 1. Principios, políticas y marcos de referencia, 2. Procesos, 3. Estructuras organizativas, 4. Cultura, ética y comportamiento, 5. Información, 6. Servicios, infraestructura y aplicaciones, y 7. Personas, habilidades y competencias.

La definición de los catalizadores se basa en un esquema con cuatro dimensiones: partes interesadas, metas, ciclo de vida y buenas prácticas, a los que unen mediciones para evaluar si se alcanzan las metas, se aplican las buenas prácticas y si se responde a las expectativas de las partes interesadas. En la versión 5 los catalizadores se desarrollan en distintas guías y documentos, aun no revisados para la nueva versión. En ellos se establecen cuarenta objetivos para la gobernanza TIC, guías de diseño y pautas de implantación, un modelo de calidad de la información y una descripción de los procesos de administración y gobierno de sistemas de información (ISACA, 2013).

En el ámbito de la normativa internacional ISO, la norma UNE/ISO 38500 establece el vocabulario y seis principios para la gobernanza (responsabilidad, estrategia, adquisición, desempeño, cumplimiento y conducta humana), con referencias a la gestión de activos de información y del conocimiento estratégico de las organizaciones. Sin embargo, su nivel de detalle dista del que ofrece COBIT.

3. JUSTIFICACIÓN DEL ESTUDIO Y METODOLOGÍA

Resulta obvio que debe de ser posible establecer cierto paralelismo entre los marcos y normas de gobernanza – y en particular COBIT - y los estándares para gestión de documentos ISO 15489 e ISO 30301. En ambos casos se parte del reconocimiento de la importancia que tienen los datos y la información en las actividades de las organizaciones, y de su valor para demostrar el cumplimiento de requisitos legales, compromisos contractuales y para garantizar la transparencia. ISO 15489 señala "*el papel de los documentos como facilitadores de las actividades y como activos de información*" (p. 5) e ISO 30301 que "*la creación y gestión de documentos es una parte integral de las actividades, procesos y sistemas de las organizaciones*" (p. 6). Sin embargo, los anexos de COBIT que establecen correspondencias con otras normas no incluyen ninguna mención explícita a las normas ISO para la gestión de documentos, aspecto que resulta sorprendente. Sí lo hace con otras normas como ISO 38500, ISO/IEC 31000, ISO/IEC 27000 y para marcos como PRINCE2®, TOGAF® o ITIL®.

Esta limitación lleva a considerar la necesidad de realizar un análisis comparativo entre las normas de gestión de documentos y el marco COBIT, con el fin de establecer paralelismos, áreas de influencia, y establecer una trazabilidad que haga posible su correlación y facilite su uso conjunto. Esta trazabilidad situaría a las normas de gestión de documentos en un contexto más amplio que contribuiría a darles una mayor visibilidad, y con ello a apreciar y extender su valor. Por otra parte, el modelo COBIT se puede beneficiar de un enfoque más preciso para la valoración, control y auditoría de la información no estructurada.

Como parte del estudio se realizó un análisis previo de la bibliografía para encontrar referencias conjuntas a ambos marcos y normas. Se identificaron referencias puntuales en los siguientes documentos publicados por ISACA:

- *Getting started with data governance using COBIT ® 5: Design and Delivery of Data Governance* (ISACA, 2017), donde se remite al anexo A del documento *COBIT® 5: Información catalizadora* (ISACA, 2013) y se señala que éste recoge una comparación entre COBIT y la norma ISO 15489.
- *COBIT® 5: Información catalizadora.* En este documento se recoge un anexo A donde se relaciona COBIT con ISO 15489:2001 y con el modelo DAMA-DMBOK para la gestión de datos. El anexo recoge una tabla con los títulos de los capítulos de la primera versión de ISO 15489 y los relaciona con procesos y características de COBIT.
- El artículo *An Introduction to Digital Records Management* (Hamidovic, 2010) hace referencia a la ISO 15489-1:2001, y describe de forma sucinta las prácticas de gestión documental propuestas en la primera versión de la norma. Otro artículo de ese mismo autor (Hamidovic, 2014) dedicado al cumplimiento con el modelo para comercio-e UNCITRAL (United Nations Commission on International Trade) omite, no obstante, referencias a las normas ISO para gestión de documentos.
- Un artículo más reciente, *Maintaining data protection and privacy beyond GDPR implementation* (Clements, 2018) incluye una mención de unas pocas líneas a ISO 15489, e indica su relevancia para el cumplimiento del artículo 30 de GDPR, que obliga a mantener registros.

Se aprecia – mediante estas referencias – que la visibilidad de las normas de gestión de documentos dista de ser la que podría preverse. Destaca la falta de referencias a la norma ISO 30301, y el hecho de que la única trazabilidad que se ha establecido

se haya hecho respecto a la versión obsoleta ISO 15489-1:2001. Por estos motivos, se reitera la necesidad de un estudio comparativo con el fin de identificar sinergias y mejoras.

La metodología propuesta para hacer este ejercicio se basa en el análisis de distintos textos de referencia, con el fin de establecer la trazabilidad entre los principios, catalizadores y procesos COBIT a los distintos apartados de las normas de gestión de documentos. El estudio se ha acotado a la ISO 15489-1:2016 e ISO 30301:2012. La estrecha relación y la complementariedad que existe entre ellas permiten hablar de un marco normativo común en el que tienen cabida otras normas internacionales de carácter más técnico, como las dedicadas a la gestión de metadatos (ISO 23081), requisitos funcionales (ISO 16175) o directrices para la digitalización (ISO TR 13028) entre otras.

El análisis de los textos se completó con la ayuda de la herramienta Atlas.TI, que permite la codificación y categorización de los datos y su análisis concurrente. Estas técnicas son habituales en las metodologías de investigación cualitativa (Runeson et al., 2012, 64). La codificación se puede completar en distintas etapas: a) codificación abierta, donde se extraen de los datos las categorías y sus códigos relacionados; b) codificación axial, donde se identifican conexiones entre categorías y códigos; y c) codificación selectiva, donde se identifica y describe la categoría principal. En la primera se identifican las palabras, términos o conceptos que aparecen en los documentos y se etiquetan mediante códigos, identificándose *indicadores* (palabras, frases o párrafos) que hacen referencia a eventos o ideas a los que se asignan nombres representativos o *códigos*. Estos se definen como "*ideas descriptivas o explicativas, ítems con significado comprendidos en una palabra, etiqueta o símbolo*." (Birks y Mills 2011, 89).

Los códigos son una forma de referirse a conceptos o patrones que aparecen de forma recurrente en los datos analizados. Constarán de dos o tres palabras que representan un concepto clave (Hoda y otros, 2010). En el proceso de codificación se pueden etiquetar fragmentos literalmente, tal cual figuran en la fuente de información, que reciben el nombre de *códigos in vivo*. La diferencia entre códigos y conceptos es que éstos ofrecen una representación abstracta de un evento, objeto o acción significativa (Hook, 2015).

A partir de la codificación inicial, el análisis procede con la identificación de categorías o grupos de códigos relacionados. Se dice que se produce la saturación de las categorías cuando los nuevos códigos que se identifican en los datos se encuadran en categorías existentes y no se precisa añadir ninguna categoría adicional. Conforme se capturan códigos, se realiza su análisis, de forma concurrente, estableciendo relaciones entre ellos. Cada nuevo código que emerge de los datos se contextualiza con los obtenidos anteriormente, detallándose la relación que existe entre ellos. Este análisis y la interpretación de los datos obligan a comparar casos o incidentes, códigos y categorías de forma continua, con una introspección sistemática por parte del investigador, método que se considera válido para el desarrollo de nuevo conocimiento (Glinz y Fricker, 2015).

En este estudio, se ha aplicado esta técnica para extraer los distintos conceptos presentes en las normas y en los identificados en los documentos publicados por ISACA (véase apartado con la bibliografía) en forma de códigos, apuntando cada uno de ellos a los fragmentos de los documentos donde se definen o mencionan. Por ejemplo, el código "partes interesadas" se identifica en distintos fragmentos de la norma y de los documentos publicados por ISACA, aunque con distintas formas. A partir de este listado de códigos se establecen las similitudes que presentan los dos marcos de referencia y que se describen en el siguiente apartado del artículo.

4. DESARROLLO DEL ESTUDIO, RESULTADOS Y DISCUSIÓN

La realización del estudio basado en técnicas de codificación, partió de la identificación de los principales conceptos y categorías en el modelo COBIT. A partir de ellos se estableció un conjunto inicial de categorías usado como referencia para procesar el contenido de las normas de gestión de documentos. En los siguientes apartados se presentan las conclusiones del estudio, a partir de los principios y de los catalizadores COBIT.

4.1. Análisis a partir de los principios

El estudio de los textos permite obtener las siguientes conclusiones a partir de los principios COBIT.

P1. Satisfacer las necesidades de las partes interesadas

Este principio se relaciona con el concepto de *partes interesadas* presente en ISO 15489, cuyo apartado introductorio señala que los modelos de negocio cambiantes exigen "… *profesionales en gestión de documentos que comprendan y atiendan las necesidades de las partes interesadas tanto internas como externas (…), que pueden provenir del público en general, los clientes, los*

usuarios de los servicios, las personas directamente interesadas, u otros interesados en cómo se crean, capturan y gestionan los documentos.". En sus apartados 7.1 y 7.3 también se hace referencia a la necesaria colaboración con las *partes interesadas* para comprender los procesos de la organización, los documentos que ésta genera, y capturar sus requisitos.

ISO 30301 señala en su capítulo introductorio, que "*El SGD, determina los requisitos de gestión documental y las expectativas de las partes interesadas*.", y como parte de la comprensión de la organización y de su contexto (apartado 4.1) que este debe contemplar "*las relaciones, percepciones, valores y expectativas de las partes interesadas externas.*" La evaluación del desempeño del SGD que se prescribe en el capítulo 9 incluye la satisfacción de los usuarios y de las partes interesadas como uno de los aspectos a medir, analizar y evaluar.

Se identifica otra similitud entre COBIT e ISO 15489 en la clasificación que se hace de las partes interesadas. COBIT explica que - para definir el ciclo de vida de la información y determinar las prácticas a seguir -, es aconsejable clasificar a las partes interesadas en: a) creadores de información, b) custodios y c) consumidores. En el apartado 6.1 de ISO 15489 se mencionan categorías similares: "*personas que crean documentos*", "*personas involucrados en la gestión de documentos*" y "*otros usuarios de las aplicaciones de gestión documental*".

P2. Enfoque holístico

El enfoque holístico de COBIT propone establecer metas y objetivos que se propagarán sistemáticamente a través de todos los niveles de la organización, con el fin de asegurar el cumplimiento de la misión y de los objetivos generales. Esta aproximación es característica de los sistemas de gestión (ISO 9001, ISO 14001, etc.). En todos ellos se parte del estudio del contexto de la organización y de las expectativas de sus partes interesadas para derivar requisitos legales, de negocio o de cualquier otro tipo. La dirección debe establecer esa propagación de objetivos y definir el alcance de los procesos del sistema.

En relación a este principio, ISO 15489 incluye una nota en su introducción, en la que se recoge que las actividades de la organización, que pueden consistir en procesos, actividades u operaciones, dependiendo de su granularidad, es aquello que se ejecuta para alcanzar los objetivos de la organización.

ISO 30301, en su capítulo 6.2 *Objetivos de la gestión documental y planes para alcanzarlos*, indica que "*la alta dirección debe asegurar que se establecen los objetivos (…) y se comunican en los niveles y las funciones pertinentes dentro de la organización*". Estos objetivos se derivan del análisis de actividades y tras identificar en qué áreas son aplicables ciertos reglamentos, buenas prácticas, legislación, etc. También el apartado 4.1 señala la necesidad de comprender la organización y su contexto, factores externos e internos, entorno social, cultural, legal, tecnológico, etc., para alcanzar una visión global e integrada de la organización.

P3. Trato integral de las necesidades de la organización

Ambas normas hacen referencia a la creación y gestión de documentos como una "*parte integral de las actividades, procesos y sistemas de las organizaciones*" (ISO 30301, p. 6) o "*parte integral de la gestión de la organización en cualquier contexto*" (ISO 15489, p. 9). Aunque centradas en la gestión de documentos, se parte de la necesidad de conocer y comprender el contexto de la organización, sus relaciones, estructura, motivación, y el entorno en el que realiza sus actividades. Esta comprensión integral de la organización será la base para establecer los requisitos que debe cumplir la gestión de documentos.

P4. Marco integrado

ISO 30301 se enmarca dentro de las normas internacionales para sistemas de gestión. Esto ya implica su pertenencia a un marco integrado junto a otras normas como ISO 9001, ISO 14001 o ISO 27000, entre otras. Todas estas normas comparten una estructura y requisitos comunes, lo que facilita su uso conjunto en los llamados sistemas de gestión integrados. El capítulo 1 de ISO 30301 señala que "*esta norma internacional puede ser implementada con otras Normas de Sistemas de Gestión*", y se destaca su utilidad para demostrar la conformidad con los requisitos de control de información documentada definidos en las mismas. En su anexo informativo B, también se hace referencia a las normas ISO antes citadas y se incluye la trazabilidad entre los capítulos de esas normas que tratan la información documentada, con los procesos de gestión de documentos definidos en el anexo A de ISO 30301.

ISO 15489 por otra parte, incluye en su bibliografía una referencia a la norma ISO 27001, pero evita en su última revisión las referencias a otras normas de gestión, que sí se citaban en la versión precedente, hoy obsoleta, en el apartado *Normas para consulta*.

P5. Separar la gobernanza de la gestión

Este principio COBIT está presente en ISO 30301, cuyo capitulo introductorio señala, entre los destinatarios de la norma, tanto a la alta dirección "*que toma las decisiones de establecer e implementar un sistema de gestión…*", como a "*aquellos responsables de la implementación del SGD, los profesionales en las áreas de gestión de riesgos, auditoría, gestión de documentos, tecnologías de la información y seguridad de la información*." La gobernanza estaría enmarcada en los requisitos del capítulo 5, referidos al liderazgo y compromiso de la dirección, la definición de una política alineada con la misión y la definición, asignación y comunicación de roles. La gestión estaría enmarcada en los requisitos de los capítulos 6, 7 y 8 dedicados a la planificación, a los procesos de soporte y a la operación del SGD.

Esta distinción entre gobernanza y gestión también se aprecia en el apartado 5.3, donde se distingue entre las responsabilidades de la dirección y las operativas: las primeras se centran en la concienciación y definición de roles y aseguramiento de las competencias, y las segundas en la implementación operacional del SGD y en su mejora continua.

4.2. Análisis a partir de los catalizadores

COBIT establece siete habilitadores o componentes: 1. Principios, políticas y marcos de referencia, 2. Procesos, 3. Estructuras organizativas, 4. Cultura, ética y comportamiento, 5. Información, 6. Servicios, infraestructura y aplicaciones, y 7. Personas, habilidades y competencias. El análisis de las normas para SGD permite identificar una correspondencia con estos componentes.

H1. Principios, políticas y marcos de referencia

Este componente está alineado con un aspecto fundamental de las normas de gestión de documentos. La definición, comunicación y promoción de una política por parte de la alta dirección, adecuada al propósito y basada en la mejora continua es también la base de ISO 30301, que dedica el capítulo 5.2 a este punto. ISO 15489 recoge una aproximación equivalente en su apartado 6.2 *Políticas*, y señala que la gestión de los documentos "*debe ser impulsada y dirigida por la dirección de la organización, quien debe ejercer el liderazgo y garantizar que se dispone de los recursos necesarios para llevarla a cabo y cumplir con los requisitos establecidos en la política y en los marcos normativos"*.

H2. Procesos

COBIT detalla treinta y siete procesos para la gobernanza, que se desarrollan en una guía específica (ISACA, 2012b). Para cada proceso se especifican sus entradas, resultados y actividades, así como la necesidad de establecer indicadores para su control, rendimiento y apreciación del riesgo. De estos treinta y siete procesos, en la correspondencia con ISO 15489-1:2001 que se incluye en el documento *Información catalizadora* (ISACA, 2013), se identificaba un subconjunto con incidencia directa en las prácticas de gestión de documentos y en el diseño, despliegue y operación de una aplicación de gestión documental:

- APO03 Administrar arquitectura empresarial.
- BAI01 Gestionar programas y proyectos.
- BAI02 Gestionar la definición de requisitos.
- BAI03 Gestionar la identificación y construcción de soluciones.
- BAI04 Gestionar la disponibilidad y capacidad.
- BAI05 Gestionar la introducción de cambios organizacionales.
- BAI08 Gestionar el conocimiento.
- BAI09 Gestionar los activos.
- BAI10 Gestionar la configuración.

El enfoque a procesos también es característico de las normas de gestión de documentos, aunque con un alcance más limitado y concreto. ISO 15489 los acota a los de creación, captura y gestión de documentos (apartado 5.3.1), que posteriormente detalla en nueve procesos en su capítulo 9: creación, captura, clasificación e indización, control de acceso, almacenamiento, uso y reutilización, migración o conversión y disposición. Es aquí posible establecer una equivalencia con los procesos del ciclo de vida de la información que se escriben en ISACA (2013, p. 37), donde tras una fase de planificación y diseño se hace referencia a la creación/adquisición, almacenamiento, uso y distribución, monitorización y disposición (archivo o destrucción).

ISO 30301 trata el diseño de procesos de gestión documental en su apartado 8.2, que parte del análisis de los procesos de trabajo organizativos y de los riesgos derivados de fallos en el control y creación de los documentos. El anexo normativo A hace referencia a dos procesos, Creación y Control, y los controles asociados a los mismos (un total de treinta y tres).

Se debe destacar que los procesos definidos en COBIT se orientan al diseño y despliegue de sistemas de información, por lo que también son apli-

cables cuando éste consiste en un sistema para la gestión de documentos. Mientras tanto, los procesos ISO se centran en la operativa del sistema, con la excepción de los procesos ISO 30301 del subconjunto *A.2.5. Establecer las condiciones de administración y mantenimiento de las aplicaciones de gestión de documentos*, vinculados al mantenimiento de la infraestructura técnica. Esto no quiere decir que las normas de gestión de documentos no traten cuestiones relacionadas con la planificación, diseño y despliegue de SGD y de sus elementos técnicos. Así, ISO 30301 en su capítulo 8 establece las fases de planificación, diseño e implementación de los procesos de gestión documental, y el 7 de ISO 15489 presenta los requisitos para una fase de identificación y valoración que comenzará con el análisis para identificar requisitos y guiar su implementación. Se puede concluir que el modelo de procesos COBIT ofrece información más detallada y complementa la definición de los procesos que – en términos demasiado genéricos – ofrecen las dos normas de gestión de documentos.

El concepto de indicadores de procesos de COBIT se relaciona con las prácticas definidas en el capítulo 6.4. *Supervisión y evaluación* de ISO 15489 y al 9.1 de ISO 30301, donde se señala la necesidad de establecer mediciones que deben ser supervisadas para comprobar la adecuación del SGD con las políticas autorizadas y con los requisitos de negocio.

Un aspecto que encontramos en COBIT, pero no en la definición de procesos de las normas ISO, se refiere a la capacidad de los procesos. Este concepto, característico de modelos de evaluación y mejora desarrollados para la industria software (CMMI o ISO/IEC 15504, SPICE), busca caracterizar y representar la predictibilidad de los resultados de los procesos, estableciendo distintos niveles de capacidad o de madurez. COBIT identifican seis niveles de capacidad (incompleto, ejecutado, gestionado, establecido, predecible y optimizado), que se evalúan u obtienen implementando unos atributos y prácticas asociados a cada uno de ellos. Aunque ISO 30301 establece las bases para auditar el cumplimiento de los requisitos, existen diferencias significativas entre el concepto de auditoría y el de evaluación de capacidad. La primera evalúa el grado de cumplimiento respecto a los requisitos establecidos en la norma, mientras que los segundos permiten obtener una valoración de la predictibilidad de los resultados de cada proceso individual y establecer un plan de mejora progresivo a medio-largo plazo, con metas bien definidas. Se trata, por lo tanto, de uno de los aspectos más prometedores en los que COBIT puede influir en las normas de gestión de documentos.

Tabla I. Semántica de los niveles (ISACA 2012a, p. 42)

0 - Incompleto	El proceso no está implementado o no alcanza su propósito.
1 - Ejecutado	El proceso implementado alcanza su propósito.
2 - Gestionado	El proceso está implementado de forma gestionada (planificado, supervisado y corregido) y los resultados de su ejecución están establecidos.
3 - Establecido	El proceso está implementado usando un proceso definido capaz de alcanzar sus resultados.
4 - Predecible	El proceso se ejecuta dentro de los límites definidos para alcanzar sus resultados.
5 - Optimizado	El proceso es mejorado continuamente para cumplir con las metas presentes y futuros.

H3. Estructuras organizativas

La necesidad de establecer una estructura organizativa está presente en el apartado 5.3 de ISO 30301, que establece la necesidad de definir, asignar y comunicar funciones, responsabilidades y competencias en todos los niveles de la organización. Otros sub-apartados de ese mismo capítulo se refieren a la designación de un representante de la dirección, y de un representante a nivel operativo. Se encuentra una referencia similar en el apartado 6.3 de ISO 15489.

H4. Cultura, ética y comportamiento

Este componente se relaciona con algunos apartados de ISO 30301, concretamente con el 4.1 *Comprensión de la organización y su contexto*, en el que se hace referencia al entorno cultural, valores y expectativas de las partes interesadas, entre los aspectos a analizar para comprender la organización. También en el 6.2 se incluye el cumplimiento de la legislación y de códigos de buenas prácticas, conducta y ética entre las fuentes de requisitos para la gestión de documentos, y en el capítulo 4.2 se habla de "*requisitos de otra índole que incluyen compromisos voluntarios de carácter no legislativo hechos por la organización*". Dada la importancia del SGD como un garante de la trazabilidad de las acciones de las organizaciones, los requisitos que establece la norma respecto a la concienciación y la comunicación resultan también relevantes.

ISO 15489 no ofrece referencias explícitas que puedan trazarse a este catalizador, si bien se indica entre los beneficios de la gestión de documentos la capacidad de "*mejorar la transparencia y la rendi-*

ción de cuentas" y "*proteger los derechos y obligaciones de las organizaciones y de los individuos*" (p. 6). En el caso de la ISO 30301, el apartado 7.3 "Concienciación y formación", requiere que el personal sea consciente de la importancia de sus actividades relacionadas con la gestión de información, la necesidad de seguir los procedimientos establecidos y las consecuencias de no hacerlo.

H5. Información

COBIT evita el término documento y adopta un enfoque genérico para referirse a "*toda la información relevante para la empresa, no sólo la información automatizada, y que puede ser estructurada o no estructurada, formalizada o informal*" (ISACA, 2012a, p. 81). La información es el resultado de la transformación de datos generados por los procesos de negocio, a partir de la cual se genera conocimiento y se crea valor.

El modelo COBIT caracteriza la información a partir de tres características o criterios: a) calidad intrínseca, b) calidad contextual, y c) accesibilidad-seguridad. Estos se subdividen a su vez en quince más específicos, que se resumen a continuación:

- Calidad intrínseca
  - Precisión: la información es correcta y se puede confiar en ella.
  - Objetividad: la información es imparcial y no presenta prejuicios.
  - Credibilidad: en qué medida la información se considera verdadera o creíble.
  - Reputación: la información se valora considerando su origen o el contexto en el que se genera.
- Calidad contextual
  - Relevancia: la información es aplicable y útil para realizar cierta actividad.
  - Completitud: no falta información, y ésta ofrece la profundidad y nivel de detalle necesario para realizar cierta actividad.
  - Actualizada: la información está actualizada para permitir realizar la tarea en cuestión.
  - Cantidad adecuada: el volumen de información es adecuado para completar la actividad.
  - Presentación concisa: la información se presenta de forma compacta.
  - Presentación consistente: la información se presenta en un formato homogéneo.
  - Comprensibilidad: la información es fácil de entender.
  - Fácil de utilizar: la información se puede reutilizar y aplicar en diferentes tareas.
- Seguridad-accesibilidad
  - Disponibilidad: la información está disponible cuando se precisa, o se puede recuperar con rapidez y facilidad.
  - Acceso restringido: el acceso a la información está restringido a las personas autorizadas.

Es posible establecer una correspondencia entre estos criterios de calidad de la información y las características que – según el apartado 5.2 de ISO 15489 - deben cumplir los documentos: autenticidad, fiabilidad, integridad y usabilidad. De estos cuatro criterios, solo tres de ellos se mencionan en ISO 30301 (normalmente como parte de los controles del anexo A), y se omite el de fiabilidad, quizás por ser el más complejo de demostrar con medios técnicos. Las cuatro características están presentes en el modelo de calidad de la información de COBIT.

El desarrollo del componente *Información* de COBIT también hace referencia a su ciclo de vida, distinguiendo la planificación, diseño, construcción/adquisición, uso y operación. Este último punto incluye su almacenamiento, distribución y uso, y entre los ejemplos que se mencionan en ISACA (2013, p. 40-41) se encuentran preguntas relativas a su almacenamiento físico, acceso, estructura, tipos de información, retención, canales de acceso, y una distinción entre el valor histórico y operacional de la información. En este punto también resulta posible establecer un paralelismo con los contenidos de ISO 30301 – que distinguen planificación, diseño y operación - y con los nueve procesos de ISO 15489.

H6. Servicios, infraestructura y aplicaciones

Este habilitador remite a las tecnologías y aplicaciones informáticas, también presentes en las normas para gestión de documentos. Estas citan las herramientas tecnológicas que sirven de apoyo al sistema y a los "*elementos técnicos de software, que se puede haber diseñado específicamente para gestionar documentos o con otro propósito…*" (ISO 15489, 3.16).

ISO 30301 incluye la infraestructura técnica entre los recursos necesarios para gestionar y operar el SGD, que según el apartado 7.1, deben ser asignados y mantenidos por la alta dirección. También en el diseño del proceso que se describe en el capítulo 8.2 se señala que – como parte de la especificación del proceso – se deben "*determinar las tecnologías adecuadas para crear y capturar los documentos*" y "*establecer las condiciones que deben regir la administración y mantenimiento de las aplicaciones de gestión documental*."

La norma incluye un apartado dedicado a la implementación de las aplicaciones de gestión documental, el 8.3, cuya adecuación a las necesidades de la empresa deberá ser supervisada regularmente. La efectividad de las aplicaciones de gestión documental y de los recursos de infraestructura técnica son aspectos que se deben medir y evaluar de forma sistemática según los requisitos del capítulo 9 *Evaluación del desempeño del SGD*.

H7. Personas, habilidades y competencias.

Este componente COBIT es otro eje fundamental en las normas de referencia. ISO 15489, en su apartado 6.5 *Competencia y formación*, e ISO 30301 en el capítulo 7.2 hacen una mención explícita a todas la personas que trabajan en la organización y establecen responsabilidades y competencias de dirección y rendición de cuentas. Siguiendo con las pautas habituales en las normas de sistemas de gestión, se exige el desarrollo de competencias con un plan de capacitación para que equipos y personas desempeñen sus funciones correctamente.

ISO 30301 trata en sus capítulos 7.1 *Recursos* y 7.2 *Capacitación*, los requisitos relativos a la asignación de los recursos necesarios (incluyendo, pero no limitado al personal), y al aseguramiento de que éste dispone de las competencias necesarias mediante capacitación y formación. ISO 15489 establece la necesidad de un plan de formación continuo dirigido a todos los miembros de la organización, incluido el personal externo que se vean afectados por la gestión de documentos.

Como resumen de los puntos tratados en los apartados anteriores, la tabla II recoge la trazabilidad entre los principios y los catalizadores COBIT y los apartados de las normas de gestión de documentos en los que se puede identificar una conexión o relación.

Tabla II. Tabla resumen: puntos de conexión y trazabilidad

Principios COBIT	**Apartados de normas ISO 15489 e ISO 30301**
Satisfacer las necesidades de las partes interesadas	ISO 15489, 6.1, 7.1 y 7.3. ISO 30301, 4.1.
Enfoque holístico	ISO 30301, 4.1, 6.2.
Trato integral de las necesidades de la organización	ISO 15489, p. 9 ISO 30301, p. 6
Marco integrado	Referencias a ISO 9001, 14001 27000.
Separar gobernanza de gestión	ISO 30301, 5 (compromiso y liderazgo de la dirección) y requisitos de planificación, procesos de soporte y operación del SGD en apartados 6, 7 y 8.
Catalizadores COBIT	**Normas ISO 15489 e ISO 30301**
Principios, políticas y marcos de referencia	ISO 15489, 6.2. ISO 30301, 5.2.
Procesos	ISO 15489, 5.3.1 y procesos definidos en apartado 9. ISO 30301, 8.2 (diseño de procesos de gestión documental) y anexo normativo A (procesos de Creación y Control)
Estructuras organizativas	ISO 15489, 6.3. ISO 30301, 5.3.
Cultura, ética y comportamiento	ISO 15489, beneficios de la gestión documental destacados en p. 6 ("mejorar la transparencia y la rendición de cuentas" y "proteger los derechos y obligaciones de las organizaciones y de los individuos"). ISO 30301, 4.1, 4.2, 6.2 y 7.3.
Información (características)	ISO 15489, 5.2 (características de la información). ISO 30301, anexo A.
Servicios, infraestructura y aplicaciones	ISO 15489, 3.16 ISO 30301, 7.1, 8.2, 8.3
Personas, habilidades y competencias	ISO 15489, 6.5 ISO 30301, 7.1 y 7.2.

4.3. Gestión de riesgos y auditorías de evaluación del cumplimiento

La norma ISO/IEC 38500 se refiere, en uno de sus principios – Desempeño – a la necesidad de que los administradores evalúen los riesgos que pueden comprometer la integridad y protección de la información que conforma la memoria colectiva. La gestión de riesgos se menciona en la descripción del primer principio de COBIT (*Satisfacer las Necesidades de las Partes Interesadas*), y es junto a la realización de beneficios y la optimización de recursos uno de los objetivos de la gobernanza (ISACA, 2012a, p. 18). COBIT hace referencia a las normas ISO 31000 – dedicada de forma específica a la gestión de riesgos -, y estas prácticas son claves en el entramado regulador de ISACA. Strait (2010) describe el proceso de gestión de riesgos en uno de las pocas publicaciones de ISACA dedicadas a la gestión de documentos. En ella se considera la gestión documental como un conjunto de prácticas para la mitigación de riesgos. Se señala que, en el momento de determinar el alcance del programa de gestión de documentos, se deben identificar los riesgos que se asumen si no se adopta un enfoque de gestión de riesgos, que contará con su propio plan. El documento también señala que el plan de gestión de riesgos necesitará:

- Crear un equipo interdisciplinar.
- Analizar escenarios de riesgo más relevantes y probables que impacten en los objetivos de la organización, y entre ellos los asociados al ciclo de vida de la información.
- Revisar los procesos y la forma en que se recibe y genera información, dónde se almacena, quién accede ella, cómo se distribuye, etc.
- Cuantificar y priorizar los riesgos atendiendo a su probabilidad e impacto en caso de que se materialicen.
- Proponer un plan y estimar un presupuesto.

La gestión de riesgos también se contempla en las normas de gestión de documentos, y han sido revisadas en la literatura de administración empresarial (Andreeva y otros, 2017)

ISO 15489, en su introducción se refiere a: "*f) la importancia de la gestión de riesgos en las estrategias concebidas para la gestión de los documentos, y la gestión de documentos como una estrategia de gestión de riesgos en sí misma.*" En los principios enumerados en el apartado *4 Principios para la gestión de documentos* mencionan: "*d) las decisiones relativas a la creación, captura y gestión de los documentos están basadas en la apreciación del riesgo de las actividades de la organización, en su contexto legal, y social.*", aspecto que se desarrolla ampliamente en el apartado 7. Aquí, como parte de la evaluación de las actividades con el fin de identificar los documentos que se generan y capturan, se incluye el análisis y apreciación de los riesgos derivados de la carencia de documentos y se propone la gestión documental como una medida para evitarlos. En relación a la gestión de riesgos en la gestión documental, se debe considerar también el informe técnico UNE-ISO/TR 18128, que proporciona pautas para la identificación y gestión de riesgos en los procesos y sistemas de gestión documental. Las áreas de incertidumbre que menciona este informe (diseño del sistema, mantenimiento, sostenibilidad y continuidad, interoperabilidad y seguridad) están incluidas en la más amplia lista de perfiles de riesgo que establece COBIT (ISACA, 2018d, p. 24).

Respecto a las directrices ISACA sobre auditoría de datos, Gelbstein (2016) señala que la auditoría proporcionará evidencias sobre: "*datos incompletos, inexactos o inconsistentes, datos que no cumplen con la privacidad o las leyes regulatorias, lagunas en los niveles o procesos de seguridad de datos, la ubicación de las fuentes de datos de la organización, datos no verificados que alguien puede estar usando sin que se sepa, así como lagunas en la responsabilidad sobre los datos*".

El capítulo 9.2 de ISO 30301 establece los requisitos para un sistema de auditoría interna para evaluar y supervisar el cumplimiento de los requisitos de gestión de documentos, aspecto de la norma que ha sido discutido en detalle por Moro-Cabero (2011). Ese apartado de la norma no hace referencia a criterios de auditoria específicos, sino únicamente a la necesidad de definirlos, siendo el conjunto de controles del anexo normativo A la principal referencia para establecer el alcance de las auditorías. ISO 30301 incluye controles similares a los propuestos por COBIT y citados en el párrafo anterior: "*A.1.3.1. Se debe identificar y documentar la información requerida como documento para cada proceso de trabajo…*", "*A.2.2.1 Se deben dictar normas para regular el acceso a los documentos…*", o "*A.2.3.1. Se deben implementar procedimientos para garantizar la integridad/seguridad de los documentos e impedir la utilización no autorizada, la modificación, el traslado, el ocultamiento o la destrucción*". En ISO 15489:2016 las referencias a auditorias dejaron de estar presentes, si bien se mantienen requisitos para la supervisión y evaluación en el capítulo 6.4.

La auditoría es, por tanto, una pieza clave y constituye una actividad necesaria que pone de manifiesto tanto los cumplimientos como las no conformidades con el sistema de gestión, permite valorar riesgos, oportunidades de mejora y puntos débiles.

5. CONCLUSIONES

La información que produce una organización como resultado del desarrollo de su actividad y para dar cumplimiento a sus objetivos, constituye un valioso activo, al servir de respaldo a las actividades y decisiones y al permitir la rendición de cuentas a las partes interesadas desde los puntos de vista empresarial y legal.

Como consecuencia del desarrollo de las TIC, esta información se crea y gestiona mayoritariamente con el soporte de complejas infraestructuras informáticas. La adopción de las TIC ha supuesto ventajas como la agilidad en los procesos, el aumento exponencial de la capacidad de almacenar datos y mayores posibilidades de recuperación y difusión. Pero al mismo tiempo ha generado nuevos riesgos asociados tanto a posibles problemas técnicos como organizativos: exceso de información y de datos, control y acceso a información confidencial o privilegiada, exposición a amenazas y ataques, etc.

Esto ha llevado a las comunidades profesionales a establecer mecanismos que garanticen el control y la calidad de la información, de los procesos que la generan y gestionan, y de las condiciones de los sistemas que permiten recuperarla de forma íntegra y segura, manteniendo su autenticidad, validez y accesibilidad. Si hasta hace pocos años los órganos de gobierno de las organizaciones delegaban en los profesionales informáticos esta labor, progresivamente – y gracias a la labor de organizaciones como ISACA y a los distintos marcos de referencia y normativos, se ha generalizado un enfoque holístico que da cabida a distintos perfiles profesionales con la gestión de riesgos y la continuidad digital como aspectos centrales.

El modelo de referencia propuesto por ISACA sirve de apoyo a los profesionales encargados de verificar que las organizaciones han establecido las medidas necesarias para evitar, mitigar y paliar los riesgos y sus efectos. Sin embargo, aunque existen claras similitudes y paralelismos entre el marco de referencia de ISACA y el marco normativo establecido por las normas UNE/ISO para la gestión de documentos, tal y como se demuestra en este estudio, es evidente la necesidad de una mayor permeabilidad entre estos modelos.

El análisis demuestra que existe un grado significativo de compatibilidad entre los principios y prácticas de gestión de información que define el modelo COBIT con las normas de gestión documental. Existe una base común y ambos modelos comparten en última instancia el objetivo de asegurar el cumplimiento de las obligaciones que establece el contexto en el que desarrolla su actividad la organización (jurídico, reglamentario, normativo, etc.). Cabe señalar, no obstante, que en la formulación actual de COBIT las normas de gestión de documentos no tienen la visibilidad que cabría esperar. Así, ni la lista de objetivos de gobierno y gestión (ISACA, 2018a) ni las guías de diseño e implementación de un sistema de gobierno de la información (ISACA 2018b, 2018c) incluyen a las normas ISO 15489 o ISO 30301 en su lista de normas de referencia. Se debe tener en cuenta que COBIT pretende servir de paraguas a distintas normas relacionadas con el cumplimiento de requisitos normativos (véase ISACA, 2018a anexo C, en el que se hace referencia a 26 normas y marcos). Esto permite concluir que las normas de gestión de documentos no han alcanzado la visibilidad esperada en una comunidad profesional que debería incluirse entre su público objetivo.

COBIT, sin embargo, sí incluye numerosas prácticas de gestión que exigen la generación y gestión de documentos (ISACA, 2018a), por ejemplo:

- *BAI08.01 Identificar, validar y clasificar las diversas fuentes de información internas y externas, incluidos los documentos estratégicos, reportes de incidentes, requeridas para habilitar el gobierno y la gestión.*
- *DSS05.06: Gestionar documentos sensibles y dispositivos de salida.*
- *DSS06.06 Asegurar los activos de información a través de métodos aprobados, incluyendo información en formato electrónico u otros métodos (p.ej. documentos fuente o informes de salida)… de principio a fin.*

Estas prácticas se dividen a su vez en actividades más específicas, en las que encontramos nuevas referencias a la gestión de documentos, sirviendo como ejemplo las siguientes:

- *Considerar los tipos de contenido (procedimientos, procesos, estructuras, conceptos, políticas, reglas, hechos, clasificaciones), artefactos (documentos, registros, vídeo, voz) e información estructurada y no estructurada.*
- *Recopilar, cotejar y validar la información con base a los criterios de validación de la información (p. ej., comprensión, relevancia, importancia, integridad, precisión, consistencia, confidencialidad, vigencia y confiabilidad)*
- *Definir un período de retención adecuado para la documentación de los cambios y la documentación del sistema y del usuario.*
- *Establecer procedimientos para gobernar la recepción, uso, retiro y desecho de documentos sensibles y dispositivos de salida, dentro y fuera de la empresa.*

La complementariedad entre COBIT y las normas de gestión de documentos identifica dos líneas:

a) El conjunto detallado de prácticas, actividades y controles que ofrece COBIT, sirve como referencia para la planificación, diseño, construcción y operación de un sistema de gestión de documentos, contemplándose así muchos aspectos que no están presentes en las normas ISO.

b) Los controles que establece ISO 30301 en su anexo A, dan respuesta a la necesidad de definir los controles de los procesos de negocio que establece COBIT (2018a, p. 270). El componente *Guía de los controles del negocio* del grupo *Políticas y Procedimientos* señala la obligación de garantizar un control adecuado y reducir el riesgo de fraude y errores, identificar controles manuales para proteger documentos, así como controles de supervisión para revisar el flujo de documentos y garantizar su correcto procesamiento. Estos controles deberán incluir la seguridad física, acceso, autenticación, gestión de cambios y las llamadas comprobaciones de edición.

Se puede concluir que, en el contexto actual, en el que asegurar el cumplimiento normativo es una de las obligaciones más relevantes para cualquier organización (Junceda, 2018, López-Arranz, 2019), se debería potenciar la presencia, visibilidad y comprensión de las normas de gestión de documentos en el ámbito de profesionales dedicados al cumplimiento y a la gobernanza de la información y del soporte tecnológico necesarios para garantizarlo.

NOTAS

1. Concretamente, cuenta con cuatro certificaciones personales: Auditor Certificado de Sistemas de Información (CISA), Gestor Certificado de Seguridad de la Información (CISM), Certificado en Gobierno de TI de la Empresa (CGEIT) y Certificado en Riesgos y Controles de los Sistemas de Información (CRISC).

REFERENCIAS

AENOR (2011). *UNE-ISO/IEC 20000-1:2011, Tecnología de la información. Gestión del Servicio. Parte 1: Requisitos del Sistema de Gestión del Servicio (SGS)*. Madrid: AENOR.

AENOR (2011). *UNE-ISO 30301:2011, Información y documentación. Sistemas de gestión para los documentos. Requisitos.* Madrid: AENOR.

AENOR (2013). *UNE-ISO 38500:2013, Gobernanza corporativa de la Tecnología de la Información (TI)*. Madrid: AENOR.

AENOR (2016). *UNE-ISO 15489-1:2016, Información y documentación. Gestión de documentos. Parte 1: Conceptos y principios*. Madrid: AENOR.

AENOR (2017). *UNE-EN ISO/IEC 27001:2017, Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos. (ISO/IEC 27001:2013 incluyendo Cor 1:2014 y Cor 2:2015).* Madrid: AENOR.

Anderson, K.A. (2012). A Case for a Partnership Between Information Security and Records Information Management. *ISACA Journal*, vol. 2, 1-5.

Andreeva, S.; Velikanova, S.; Chernykh, O.; Kozhushkova, N.; Samarokova, I.; Arakcheeva, Z. (2017). The Risk-Based Thinking in Managing Documents as Assets. *International Journal of Economic Perspectives*, 11 (2), 829-837.

Birks, M.; Mills, J. E. (2011). *Grounded Theory: a Practical Guide*. Los Angeles: Sage.

Bustelo, C. (2007). Norma UNE ISO 15489. Gestión de documentos. *Anuario ThinkEPI*, vol. 1, 146-147.

Clements, T. (2018). *Maintaining Data Protection and Privacy beyond GDPR Implementation*. Rolling Meadows, IL: ISACA. 20 p.

Conde-Hernad, J.M.; Gonzalez-Gaya, C. (2013). Methodology for implementing a Document Management System to support ISO 9001:2008 Quality Management Systems. *Procedia Engineering*, vol. 63, 29-35. https://doi.org/10.1016/j.proeng.2013.08.225

Dhérent, C. (2006). Document management at the French National Library. *Records Management Journal*, 16 (2), p. 97-101. https://doi.org/10.1108/09565690610677454

Financial Reporting Council (1992). The Financial Aspects of Corporate Governance. London: GEE, [90 p.] ISBN 085258 9158.

García-Alsina, M. (2012) Contribución de la serie ISO 30300 a la gestión de la documentación judicial. *Ibersid. Revista de Sistemas de Información y Documentación*, vol. 6, 135-143.

García-Morales, E. (2014). Un encaje perfecto: ISO 30300 y sistemas integrados de gestión empresarial. *Anuario ThinkEPI*, vol. 8, 153-155.

Gelbstein, E. D. (2016). IS Audit Basics: The Domains of Data and Information Audits. *ISACA Journal*, vol. 6, 1-4.

Glinz, M.; Fricker, S. A. (2015). On shared understanding in software engineering: an essay. *Computer Science - Research and Development*, vol. 30, 363-376. https://doi.org/10.1007/s00450-014-0256-x

Grimal-Santos, O.; Vaquero-Lorenzo, P.; Vian-del-Pozo, M. J. (2009). El archivo parlamentario de las Cortes de Castilla y León: Implementación de un sistema de gestión documental (aplicación práctica de la norma ISO 15489). *Tabula*, vol. 11, 345-358.

Hamidovic, H. (2010). An Introduction to Digital Records Management. *ISACA Journal* vol. 6, 1-6.

Hamidovic, H. (2014). Electronic Documents Information Security Compliance. *ISACA Journal* vol. 3, 1-3.

Healy, S. (2010). ISO 15489 Records Management: its development and significance. *Records Management Journal*, vol. 20 (1), 96-103. https://doi.org/10.1108/09565691011039861

Hoda, R.; Noble, J.; Marshall, S. (2010). Using grounded theory to study the human aspects of software engineering. En: *Human Aspects of Software Engineering*. ACM, 5. https://doi.org/10.1145/1938595.1938605

Hook, N. (2015). Grounded theory. En: *Game Research Methods*, 309-320. ETC Press.

ISACA (2012a). *COBIT® 5: un marco de negocio para el gobierno y la gestión de las TI de la empresa*. Rolling Meadows, IL: ISACA. 94 p. ISBN: 978-1-60420-282-3.

ISACA (2012b). *COBIT® 5: Procesos catalizadores*. Rolling Meadows, IL: ISACA. 230 p. ISBN: 978-1-60420-285-4.

ISACA (2013). *Información Catalizadora*. Rolling Meadows, IL: ISACA, 102 p. ISBN 978-1-60420-554-1.

ISACA (2017). *Getting Started with Data Governance using COBIT 5: Design And Delivery Of Data Governance*, 20 p. Disponible en: http://www.isaca.org/KnowledgeCenter/Research/ResearchDeliverables/Pages/Getting-Started-with-Data-Governance-Using-COBIT-5.aspx (última consulta 12/07/2019)

ISACA (2018a). *Marco de Referencia COBIT® 2019: Objetivos de gobierno y gestión*. Schaumburg, IL: ISACA, 302 p., ISBN 978-1-60420-790-3.

ISACA (2018b). *Guía de implementación de COBIT® 2019: Implementación y optimización de una solución de gobierno de Información y Tecnología*. Schaumburg, IL: ISACA, 78 p., ISBN 978-1-60420-794-1

ISACA (2018c). *Guía de diseño COBIT® 2019: Diseño de una solución de Gobierno de Información y Tecnología*. Schaumburg, IL: ISACA, 150 p., ISBN 978-1-60420-793-4

ISACA (2018d). *Marco de referencia COBIT® 2019: Introducción y metodología*. Schaumburg, IL: ISACA, 64 p., ISBN 978-1-60420-788-0.

Joseph, P.; Debowski, S.; Goldschmidt, P. (2012) Paradigm shifts in recordkeeping responsibilities: implications for ISO 15489's implementation. *Records Management Journal*, vol. 24 (1), 57-75. https://doi.org/10.1108/09565691211222108

Junceda, J. (2018). Programas de cumplimiento y sector público. Especial mención a las empresas y entes públicos. *Presupuesto y gasto público*, no. 91, 169-178.

Lomas, E. (2010) Information governance: information security and access within a UK context. *Records Management Journal*, vol. 20 (2), 182-198. https://doi.org/10.1108/09565691011064322

López-Arranz, A. (2019). El trabajador con funciones de compliance officer en la empresa, en Europa y España. *Revista de Investigación del Departamento de Humanidades y Ciencias Sociales*, no. 15, 1-20

Moro-Cabero, M. (2011). La relevancia de auditar requisitos de información en el diseño de sistemas de gestión de documentos: métodos tradicionales, enfoques emergentes. *Investigación Bibliotecologica*, vol. 25 (53), 201-230. https://doi.org/10.22201/iibi.0187358xp.2011.53.27475

Moro-Cabero, M.; Martin-Pozuelo, M. P.; Bonal-Zazo, J. L. (2011). ISO 15489 and other standardized management systems: analogies and synergies. *Records Management Journal*, vol. 21 (2), 104-121. https://doi.org/10.1108/09565691111152044

OCDE (1998). *Principles of Corporate Governance*, Paris: OECD Publishing. 45 p.

Oliver, G. (2014). International records management standards: the challenges of achieving consensus. Records Management Journal, vol. 24 (1), 22-31. https://doi.org/10.1108/RMJ-01-2014-0002

Runeson, P.; Höst, M.; Rainer A.; Regnell, B. (2012). *Case study research in software engineering: guidelines and examples*. Hoboken, N.J.: Wiley. https://doi.org/10.1002/9781118181034

Smallwood, R. F. (2014). Information governance, IT governance, data governance: what's the difference? En: *Information Governance: Concepts, Strategies, and Best Practices*. Wiley. ISBN: 978-1-118-21830-3.

Strait, C. (2010). Building a business case for records management. *ISACA Journal*, vol. 6, 1-3.