Actas das I Xornadas Olga Gallego de Arquivos

Transparencia "versus" corrupción: os arquivos e a democracia

Actas das I Xornadas Olga Gallego de Arquivos

Transparencia "versus" corrupción: os arquivos e a democracia

A Coruña 2 e 3 de outubro de 2015

FUNDACIÓN OLGA GALLEGO
2016

Edición:
© 2016, **Fundación Olga Gallego**
©2016, **Os autores**

Deseño e maquetación:
Salgado & Santana

ISBN:
978-84-608-6572-8

Comité organizador

Pedro López Gómez

Isabel Buján Bernárdez

Mª del Mar García Miraz

Olimpia López Rodríguez

Mª Dolores Pereira Oliveira

Gabriel Quiroga Barro

Comité científico

Carlos Amoedo Souto

Javier Barbadillo Alonso

Luis Martínez García

Fernanda Ribeiro

Gestión de riesgos aplicada a la gestión de documentos

una metodología para garantizar una rendición de cuentas confiable

Anahí Casadesús de Mingo

Gestión de riesgos aplicada a la gestión de documentos: una metodología para garantizar una rendición de cuentas confiable

Anahí Casadesús de Mingo

Resumen

La gestión de riesgos aplicada a la gestión de los documentos es un método que garantiza una rendición de cuentas confiable a partir de la mejora en el sistema de gestión de documentos de la organización. Controlando los riesgos asociados a los documentos se controla a la vez la gestión documental y se garantiza la primera fase del proceso de rendición de cuentas: la fase de información. En este artículo se presentan varias metodologías, válidas tanto para organizaciones públicas como privadas, para llevar a cabo una apreciación del riesgo asociado a los documentos: identificación, análisis y evaluación. Se hace especial hincapié en los enfoques a la hora de identificar riesgos, presentando diferentes perspectivas y metodologías y llegando a la conclusión de que emplearlas conjuntamente aporta mejores resultados.

Abstract

Risk management methodology applied to Records management guarantees a reliable accountability from improving records management systems of the organizations. Controlling records risks, the organization controls records management and can both control and guarantee the first phase for accountability: the information phase. This article discusses several methodologies, to private and public bodies, to conduct an assessment of the risk associated to records: identification, analysis and evaluation. An especial emphasis is placed on the different identification approaches, presenting different perspectives and methodologies about it and concluding that using them together brings better outcomes.

Palabras clave

Gestión de riesgos, gestión de documentos, riesgos de la información y los documentos, rendición de cuentas.

Introducción y marco conceptual

En el campo de la gestión documental la gestión del riesgo es un ámbito aún poco estudiado pero que va cogiendo fuerza y apareciendo cada vez más en la implantación de Sistemas de Gestión Documental (SGD) normalizados. Es precisamente en los estándares internacionales donde encontramos mayor trabajo en esta dirección, partiendo de la norma

UNE-ISO 31000:2009 de gestión del riesgo que ha dado lugar al posterior desarrollo de una norma específica de riesgos de gestión documental, la norma UNE-ISO/TR 18128:2014, de apreciación del riesgo en procesos y sistemas de gestión documental. En ambas normas encontramos una definición del término riesgo prácticamente igual: “el efecto[1] de la incertidumbre[2] sobre la consecución de los objetivos”.

La gestión de riesgos de gestión documental puede entenderse como una adaptación del proceso genérico de gestión del riesgo aplicado a la integridad, disponibilidad y confidencialidad de la información y los documentos de una organización con el objetivo de mantener la calidad de dicha información (Pullen y Maguire, 2007). Lemieux fue una de las primeras profesionales en relacionar los riesgos y su gestión con el ámbito de la gestión documental, la información y los documentos. Según Lemieux, los riesgos de la información y los documentos abarcan cualquier amenaza que provenga de alguna insuficiencia en la información y los documentos (Lemieux, 2004) y que podría suponer el incumplimiento de los objetivos de la organización. Es interesante remarcar que Lemieux habla de riesgos de la información y los documentos, no de riesgos de gestión documental, centrando así la atención, el análisis y los controles del riesgo en el objeto y no en el proceso que lo gestiona. Por el contrario, las normas ISO hablan de riesgos de los procesos y sistemas de gestión documental, centrando el análisis en la metodología operacional de trabajo y no tanto en el objeto.

Los documentos, y la información en ellos contenida, afectan a las entradas, procesos, salidas y resultados de la organización y es por ello que necesitan ser gestionados de manera adecuada dentro de cualquier estrategia de gestión del riesgo (Pullen y Maguire, 2007). Una política de gestión documental definida y controlada asegurará que la organización está protegida frente a riesgos como litigios o desastres, y que las prácticas de gestión documental cumplen con los requisitos legales y normativos aplicables (Hugues, 2003; citado en Pullen y Maguire, 2007). Cuanto mejor sea la gestión de documentos en una organización, menor riesgo existirá.

Sin una gestión de documentos efectiva (dentro de la cual se incluye la gestión de riesgos) no será posible proporcionar un acceso de calidad a información fiable y útil (Millar, 2003) para garantizar el proceso de rendición de cuentas. Este proceso normalmente consiste en tres fases. La primera de ellas se relaciona directamente con la gestión documental e implica la obligación de quien rinde cuentas de informar al foro que lo evalúa, proporcionando documentos e información sobre el desempeño de sus tareas, resultados o procedimientos. En la segunda fase el foro puede interrogarle y cuestionar la adecuación de la información proporcionada así como la legitimidad de su conducta. En la tercera fase el foro puede aprobar o desaprobar la conducta de quien rinde cuentas, así como condenar públicamente su comportamiento. Dentro de esta última etapa pueden imponerse sanciones por una mala conducta o actuación. Pero, para que este proceso pueda llevarse a cabo se parte de la necesidad de que exista y esté controlada la documentación sobre el hecho o acontecimiento sobre el que se rinde cuentas y para ello es necesario disponer de SGD adecuados en las organizaciones, que garanticen la conservación, la accesibilidad, la usabilidad y la recuperación pertinente de la información.

1. Un efecto es una desviación, positiva y/o negativa, respecto a lo previsto (UNE-ISO 31000:2009,2.1).

2. La incertidumbre es el estado, incluso parcial, de deficiencia en la información relativa a la comprensión o al conocimiento de un suceso, de sus consecuencias o de su probabilidad (UNE-ISO 31000:2009,2.1).

Gestión del riesgo

Según la norma IEC 31010: 2009, la gestión del riesgo incluye la aplicación de métodos lógicos y sistemáticos para la comunicación y consulta a lo largo del proceso de gestión del riesgo; el establecimiento del contexto para identificar, analizar, evaluar y tratar los riesgos asociados a una actividad, proceso, función o producto; la monitorización y revisión de los riesgos; y la realización de informes y documentación de los resultados de manera apropiada. La gestión del riesgo no es una política más que debería crearse, sino que es la política sobre la cual construir todos los demás procesos de negocio y políticas de la organización (ARMA, 2009). Debe estar integrada en todas las prácticas y procesos de la organización, de manera que sea relevante, eficaz y eficiente (UNE-ISO 31000:2009, 4.3.4).

El proceso de gestión del riesgo, según la norma UNE-ISO 31000:2009 comprende las siguientes actividades (ver Figura 1):

- Comunicación y consulta
- Establecimiento del contexto
- Apreciación del riesgo
- Tratamiento del riesgo
- Seguimiento y revisión
- Registro del proceso de gestión del riesgo (documentar)

De estas actividades, algunas son comunes a cualquier disciplina, como el establecimiento del contexto, la comunicación y consulta, y el seguimiento y revisión, de los cuales se debe establecer un procedimiento o metodología que puede compartirse con cualquier campo de trabajo; y otras son específicas y se relacionan directamente con la actividad de la cual se realiza la gestión del riesgo, en este caso la gestión de documentos. Concretamente los aspectos relacionados con la apreciación y el tratamiento estarán directamente relacionados con la parte operacional de la gestión de documentos y de la información. En este trabajo nos centraremos en el proceso de apreciación del riesgo con el objetivo de mejorar la gestión de documentos como garantía de una rendición de cuentas confiable, basada en documentos íntegros, auténticos, fiables y usables. Para ello es importante tener en consideración los subprocesos de identificación, análisis y evaluación del riesgo (proceso general de apreciación del riesgo).

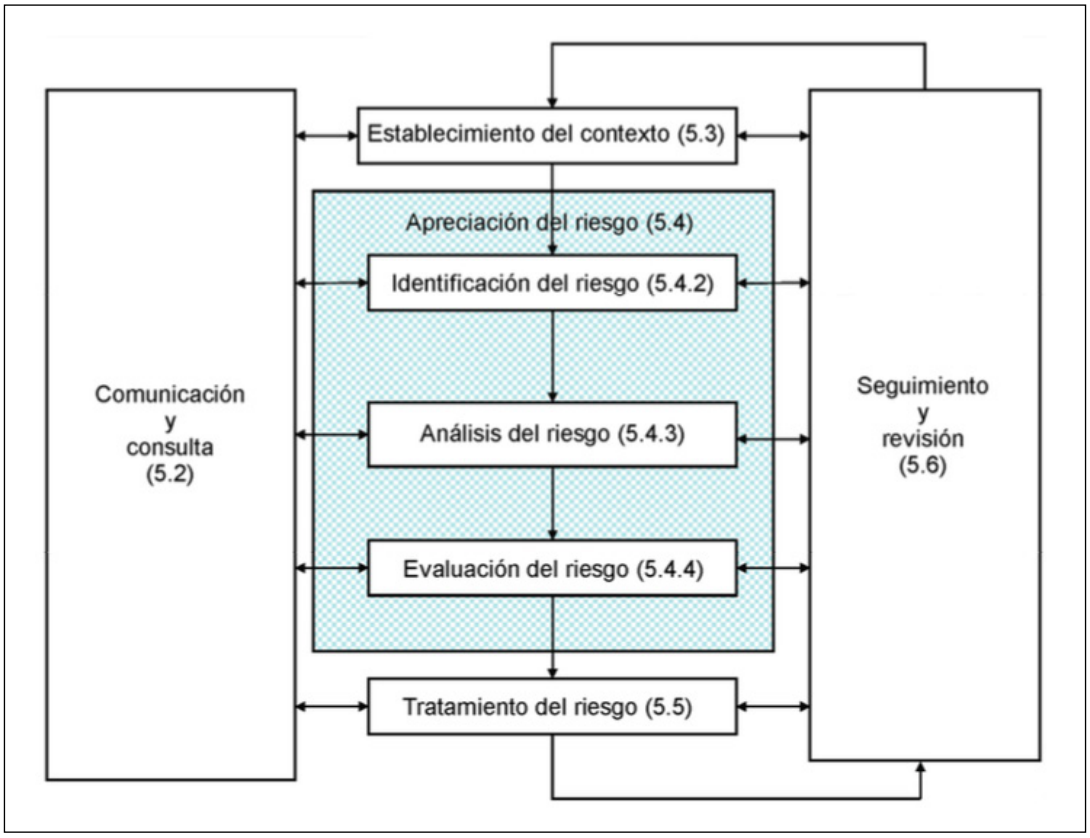

Figura 1 – Proceso de gestión del riesgo (UNE-ISO 31000:2009)

Antes de centrarnos en los aspectos de apreciación del riesgo es importante señalar que dentro del apartado de establecimiento del contexto se incluye la definición de los criterios de riesgo, es decir, aquellos criterios que se aplicarán para evaluar la importancia del riesgo. Los criterios deben reflejar los valores, objetivos y recursos de la organización y pueden derivarse de los requisitos legales o normativos aplicables. Al definir estos criterios debería considerarse una serie de factores, entre los que se encuentran el nivel de riesgo aceptable o tolerable[3]; el método para determinar el nivel de riesgo o para la definición de la probabilidad; y otros.

Los criterios para evaluar los riesgos de gestión documental deberían incluir el tamaño y alcance de los sistemas de gestión de documentos de la organización, el número de usuarios y el uso que se hace del sistema en las operaciones de la organización. Los criterios para evaluar los riesgos que afectan específicamente a los procesos de gestión documental deberían incluir la frecuencia del proceso, cuántos sistemas se usan en el mismo, y su importancia relativa en la creación o gestión de los documentos, el seguimiento de los procesos y el potencial para revertir o remediar los potenciales efectos adversos (UNE-ISO/TR 18128: 2014, 4.2).

3. Determinar el nivel de tolerancia es uno de los aspectos fundamentales en la gestión del riesgo. El nivel de tolerancia al riesgo es la máxima exposición posible al riesgo que se considera aceptable, basándose en los beneficios y costes asociados. El nivel de tolerancia al riesgo debe revisarse de manera periódica teniendo en cuenta los cambios en procedimientos o políticas de la organización así como otros aspectos del contexto interno y externo.

■ Apreciación del riesgo

La apreciación del riesgo es el proceso que comprende la identificación, el análisis y la evaluación del riesgo (ver Figura 2). Se incluye dentro del proceso global de gestión del riesgo (ver Figura 1) y proporciona una mejora en la comprensión de los riesgos que pueden afectar a la consecución de los objetivos, y la adecuación y efectividad necesaria de los controles ya existentes. Las salidas (*outputs*) de la apreciación del riesgo son entradas (*inputs*) para el proceso de toma de decisiones de la organización.

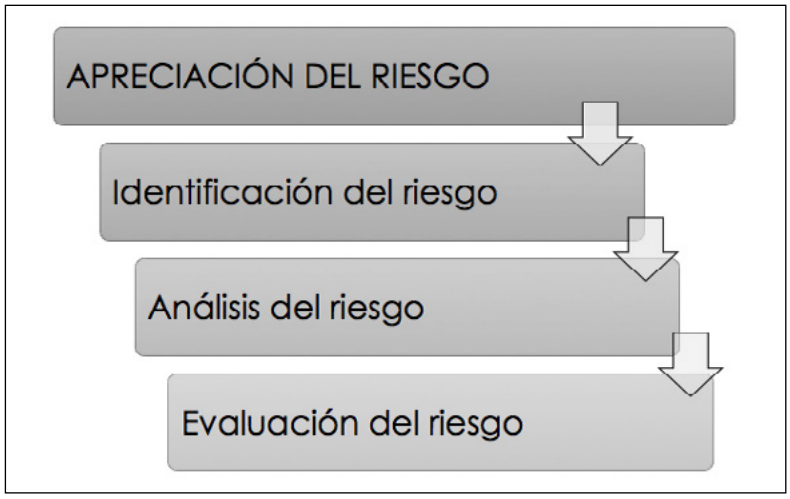

Figura 2 – Proceso de apreciación del riesgo (UNE-ISO 31000:2009)

1. Identificación de riesgos de la información y los documentos

Todas las organizaciones identifican, analizan y controlan los riesgos relacionados con el éxito de su funcionamiento, aunque en la mayoría no se tienen en cuenta los riesgos de la información y los documentos. Sin embargo, cualquier organización crea, recibe, gestiona y conserva documentos en el desarrollo de sus actividades de negocio, que deben ser y debe poder demostrarse que son: auténticos, fiables, íntegros y usables. Dentro del contexto de la gestión de documentos, el riesgo es impulsado o generado por hechos que impactan precisamente en la usabilidad, integridad, confianza y fiabilidad de la información y los documentos (ARMA, 2009). La identificación de riesgos en cualquier organización debería, por tanto, incluir aquellos relacionados con la información y los documentos, así como con los asociados a los sistemas y procesos de gestión documental, con el objetivo de detectar qué podría suceder o qué situaciones pueden darse que puedan afectar a la capacidad de los documentos para satisfacer las necesidades de la organización. El proceso de identificación del riesgo incluye la detección de las causas y el origen del riesgo, las acciones, situaciones o circunstancias que podrían tener un impacto material sobre los objetivos de la organización, así como la naturaleza de ese impacto (UNE-ISO/TR 18128:2014, 5.1). Para ello, en este artículo se explican varias metodologías que pueden resultar útiles y pueden adaptarse a las diferentes necesidades y realidades. La efectividad del proceso de gestión del riesgo dependerá de la capacidad de la organización

de identificar las incertidumbres y eventos potencialmente negativos (Egbuji, 1999) y es por ello que en este artículo centramos la atención en dicho subproceso, desde varias perspectivas.

En primer lugar, Lemieux (Lemieux, 2004) propone dos metodologías distintas para llevar a cabo la identificación de riesgos en una organización: el enfoque basado en hechos y el enfoque basado en requisitos. Ambas metodologías se explican a continuación (ver Figura 3).

Enfoque basado en hechos

Tradicionalmente las organizaciones han identificado y gestionado los riesgos asociados a la información y los documentos que les afectan a partir de un hecho, acontecimiento o amenaza desencadenante. Un ejemplo de ello serían desastres naturales, fallos en el sistema debido a errores humanos, desclasificación no autorizada de documentos, eliminaciones no autorizadas,…

Enfoque basado en requisitos

Consiste en la identificación a partir del análisis de los requisitos aplicables que afectan a la documentación y la información, que pueden derivar de la legislación y normativas en las cuales la organización desarrolla su actividad. El riesgo, a partir de este enfoque, aparece en el momento en que la organización falla en el cumplimiento de dichos requisitos. Para poder trabajar de acuerdo a este enfoque Lemieux identifica tres etapas (ver Figura 3). En una primera etapa las organizaciones necesitarán determinar las características y cualidades de los documentos que mejor se adapten a sus requisitos de negocio, definir estas características y determinar la importancia de cada una. Teniendo identificadas las características de la información y los documentos, en una segunda etapa se debería evaluar el impacto que podría tener en sus objetivos que éstos no cumplieran con los requisitos establecidos. Por último, en la tercera etapa, este análisis debería incluir las posibles amenazas que pueden provocar el incumplimiento con los requisitos definidos, la probabilidad de que esto ocurra y las causas que pueden ocasionarlo.

Este enfoque es el mismo que sigue la normativa internacional ISO. En concreto, la norma UNE-ISO/TR 18128:2014 en el apartado 4.2 afirma que los riesgos se identifican basándose en su potencial para socavar las características generales de los documentos (auténticos, fiables, íntegros y usables). Se parte de los requisitos que deben cumplir los documentos para identificar los riesgos que podrían afectarles.

Ambos enfoques, según Lemieux, tienen ventajas e inconvenientes. Por ejemplo, el enfoque basado en hechos podría conllevar la rápida identificación de estrategias de prevención o mitigación de los riesgos ya que se basa en el reconocimiento directo de un hecho o amenaza desencadenante. En cambio, a la hora de detectar fallos del sistema o de procedimiento es mucho mejor el enfoque basado en requisitos ya que mientras el primero se centra en las amenazas, el segundo va más allá, analizando los procesos de negocio y detectando fallos en los flujos de información. El enfoque basado en requisitos también tiene otras ventajas, ya que empieza por analizar los requisitos de la información y los

documentos con los que necesita cumplir la organización para alcanzar sus objetivos y, por tanto, puede ser un mejor método cuando se vincule la gestión de riesgos a los procesos estratégicos. En conclusión, trabajar en función de uno u otro método dependerá de las necesidades y objetivos de la organización, aunque ambas metodologías pueden ser complementarias y retroalimentarse.

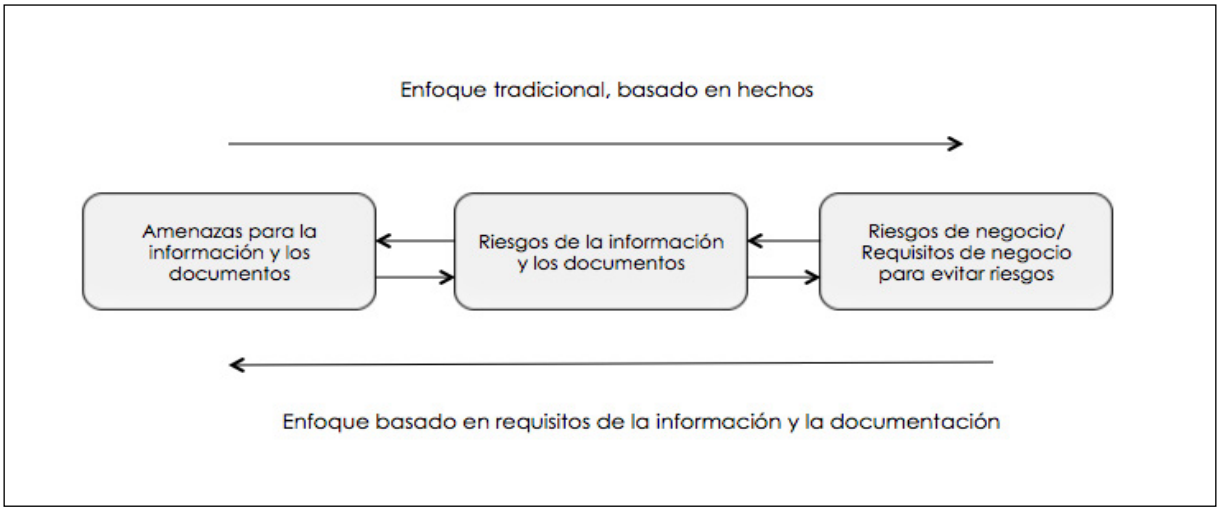

Figura 3: Enfoques para la identificación y gestión de riesgos de información y documentos (Lemieux, 2004)

A la hora de llevar a cabo la identificación de riesgos, independientemente de la metodología o enfoque empleado, existen también diferentes aspectos o ámbitos que pueden tenerse en consideración, que explicamos a continuación.

■ Identificación de riesgos: Cuadrante propuesto por la organización ARMA

La organización ARMA[4] en su publicación sobre “Evaluar y mitigar los riesgos de la información y los documentos” propone un cuadrante (ver Figura 4) en el que incluye cuatro categorías de riesgos de la información y los documentos. Pretende ser un marco de referencia para el establecimiento de sistemas para la evaluación de las amenazas que pueden afectar a la gestión del riesgo, tanto en organizaciones públicas como privadas. En dicha publicación se describe un proceso estructurado, que parte del cuadrante mencionado, para el desarrollo de un sistema de gestión de riesgos.

En el cuadrante se especifican cuatro categorías o tipos de riesgos: riesgos administrativos, riesgos en el control de los documentos, riesgos legales o normativos y riesgos tecnológicos. Cada una de estas categorías está dividida en diferentes áreas relacionadas entre sí, con la categoría superior jerárquicamente y con otras categorías del cuadrante, con lo que el análisis resultante es completo y sólido.

4. Association of Records Managers and Administrators, http://www.arma.org/ (consultado el 25/08/2015).

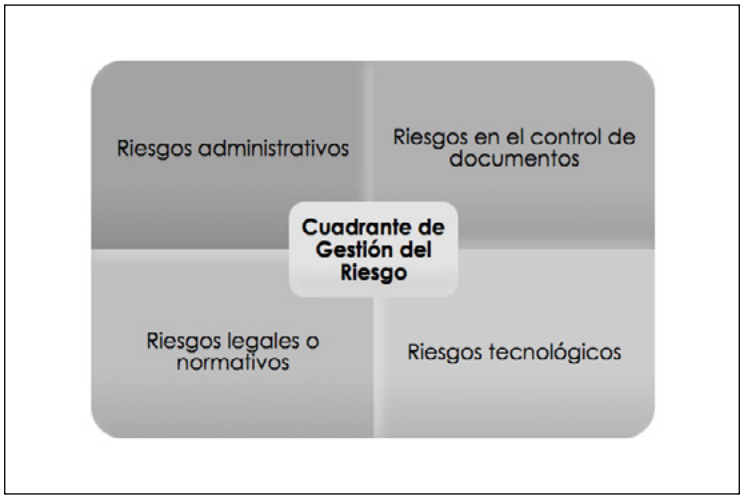

Figura 4: Cuadrante de riesgos (ARMA, 2009)

Riesgos administrativos

Se refiere a las amenazas relacionadas con el SGD de la organización. Se incluyen dentro de esta categoría las áreas de Gobernanza de la Información, Gestión del Cambio y Gestión de Emergencias.

ARMA define la gobernanza de la información como el establecimiento de políticas y procedimientos, así como la ejecución y mejora de ambos para el control y la gestión de la información dentro de la organización. Se debe definir un marco dentro del cual poder gestionar, controlar, hacer accesible y usable la información así como desarrollar los mecanismos para ello. En concreto ARMA indica que, al identificar los riesgos, debe tenerse en cuenta el compromiso constante por parte de todos los niveles de la organización; la capacitación y formación adecuada del personal encargado de la gestión de documentos; la creación de comités consultivos para la toma de decisiones en materia de gestión documental; el desarrollo de políticas y procedimientos de gestión documental; la formación continua en todos los niveles de la organización; la asignación de responsabilidades en materia de gestión documental en todos los niveles de la organización así como la comunicación, información y formación sobre qué implican dichas responsabilidades; por último, el seguimiento y evaluación del cumplimiento con lo anteriormente establecido.

La gestión del cambio en este contexto se relaciona con las posibles modificaciones en la organización que podrían afectar al SGD, ya sean tecnológicas, de contexto, legales,… Cualquier variación en los instrumentos (procedimientos, políticas,…) de gestión documental sólo podrá tener éxito si en la organización existe una adecuada gestión del cambio, por lo que es un aspecto fundamental a tener en cuenta a la hora de identificar riesgos. Dentro de este área se incluyen aspectos de comunicación, formación y de la implementación por fases, de manera progresiva.

Respecto a la gestión de emergencias, ARMA la define como un enfoque planificado para la prevención de desastres referidos a la información y documentación, incluyendo la respuesta a emergencias y la recuperación que sigue a una situación de este tipo. Se hace

hincapié en que los desastres pueden ser tanto naturales (inundaciones, terremotos,…), como técnicos (incendios, robos y otros acontecimientos causados por un error humano) o civiles (conflictos bélicos, terrorismo, vandalismo,…). Desde el enfoque de lo que debería estar planificado se plantea la identificación de posibles amenazas que puedan afectar a los documentos y a la información de cualquier organización.

Riesgos en el control de los documentos

En esta categoría se incluyen los riesgos asociados con los procesos de gestión documental: clasificación, disposición y retención, y almacenamiento de los documentos. Es la categoría más operacional de las que propone ARMA en su cuadrante de riesgos.

La clasificación de los documentos requiere determinar la relación jerárquica de estos, sus características (metadatos) y las normas que define la organización para dar nombre a los documentos, sobre todo de cara a garantizar su usabilidad y la recuperación pertinente de información en un futuro. La clasificación es especialmente importante cuando más de un departamento nutre de contenido un mismo expediente o se gestiona un trámite entre diversas áreas. Los metadatos proporcionan información descriptiva sobre los documentos, dotándoles de contexto y haciéndolos fácilmente recuperables, pero para ello debe existir un mínimo de metadatos obligatorios para la creación y el control de dichos documentos.

Dentro del área de retención y disposición se mencionan tres aspectos: el establecimiento de tablas y políticas de retención, la gestión por terceras partes, y el almacenamiento de los documentos. Las tablas y políticas de retención son necesarias para asegurar una gestión de documentos consistente y para evitar la destrucción prematura o no controlada de documentos. Respecto a la gestión por terceros, es obligación de la organización que externaliza parte de sus procesos asegurarse de que éstos se llevan a cabo siguiendo las directrices y la legislación aplicables, así como realizar auditorías de manera periódica para comprobarlo. En relación con el almacenamiento de documentos ARMA menciona tres aspectos a la hora de identificar riesgos: la evaluación del soporte, la migración, y la disposición o eliminación. La organización debe decidir qué soportes va a utilizar en función de sus necesidades; debe conocer los periodos de conservación de los documentos para poder decidir de manera coherente los soportes, así como establecer los procesos de migración para garantizar el acceso y usabilidad a lo largo del tiempo que sea necesario. Estos procesos deben ser supervisados para asegurar que todos los componentes del documento, incluidos los metadatos, son migrados de modo que se asegura la fiabilidad, autenticidad, integridad y usabilidad de dichos documentos.

Riesgos legales o normativos

Son aquellos relacionados con el cumplimiento legal y normativo o reglamentario en relación a la gestión de información y de documentos, de cualquier tipo de organización ya sea pública o privada y de cualquier sector. Se incluye el cumplimiento legal y normativo, y la pronta respuesta y disponibilidad frente a posibles litigios.

Dentro del área de cumplimiento legal y normativo se especifica que las organizaciones deben identificar aquellos requisitos que afectan a sus actividades y aquellos que afectan a la documentación que generan, reciben y gestionan. Es primordial para evitar posibles

consecuencias de incumplimiento legal. Deben, por tanto, mantener actualizada la información sobre la legislación y normativa que les afecta así como también todo lo referente a las buenas prácticas en su sector.

Respecto a la capacidad de respuesta y disponibilidad frente a posibles litigios o auditorías, se distingue entre la evaluación de dicha disponibilidad y la existencia de un plan para responder frente a litigios. Ambas áreas tienen el objetivo de que la organización esté realmente capacitada para dar respuesta y responder con fiabilidad y pertinencia a cualquier solicitud de información al respecto de un litigio o una auditoría.

Riesgos tecnológicos

Dentro de cualquier SGD existen riesgos asociados con la tecnología, como la seguridad de la información, las comunicaciones electrónicas y el control del software.

Dentro de la seguridad de la información ARMA considera como aspectos clave: la creación de un programa de protección y pérdida de información, el desarrollo de controles de acceso, y la comprensión de las necesidades de confidencialidad. El primero debería ser capaz de identificar contenido sensible de la organización e implementar controles para su creación, recepción, uso y distribución para prevenir cualquier incidente, ya sea interno o externo. El acceso a la información también requiere de controles específicos para garantizar los niveles de confidencialidad; debe existir un equilibrio entre acceso y seguridad.

Respecto a las comunicaciones electrónicas las áreas clave son la creación autorizada de métodos de comunicación, la necesidad de transmisiones seguras y la necesidad de gestionar los contenidos que los métodos de comunicación electrónica crean, transmiten o almacenan. Muchos procedimientos o trámites se inician con una comunicación electrónica y es por ello que deben gestionarse estas comunicaciones como si fueran documentos propios de la organización. Para ello es fundamental conocer las aplicaciones con las que se trabaja, su integración e interoperabilidad (control del software).

■ Identificación de riesgos: áreas de incertidumbre según la UNE-ISO/TR 18128:2014

Otra metodología para la identificación de riesgos, es la propuesta en la norma UNE-ISO/TR 18128:2014 que distingue, en aquello referido a la información y los documentos, entre riesgos de los SGD y riesgos de los procesos documentales. Dentro de estos dos grupos define diferentes áreas de incertidumbre, en su mayoría contextualizadas en entornos digitales o de documentos electrónicos.

Sistemas de Gestión Documental

Se refiere a los riesgos relacionados con los sistemas y aplicaciones que crean o controlan documentos y engloba cinco áreas de incertidumbre: desde el diseño de dichos sistemas, pasando por el mantenimiento, sostenibilidad, continuidad, interoperabilidad y seguridad de los mismos. Pese a centrarse en los sistemas y aplicaciones, estas áreas de incertidumbre se relacionan directamente con las de los procesos documentales o de gestión documental,

sobre todo en aspectos como el diseño o la implementación de dichos procesos en los sistemas o aplicaciones. El diseño del sistema interactúa con la identificación de riesgos para los procesos de gestión documental y, por tanto, una buena documentación de la configuración del sistema es clave para abordar otras áreas de riesgo relacionadas.

La identificación de riesgos en el diseño de sistemas incluye la definición de los documentos que el sistema crea y gestiona, el establecimiento adecuado de los requisitos de conservación, la identificación y documentación de todos los procesos de gestión documental que se gestionan dentro del sistema, la negociación de la dependencia del proveedor y el acceso a su documentación, y la efectividad del diseño del SGD en relación a su adecuación al personal y a la tecnología de la organización.

El mantenimiento del SGD se refiere, sobre todo, a la plataforma tecnológica y a los aspectos que pueden verse afectados por cambios estructurales de la organización, en el negocio y en los sistemas que afecten a los SGD, ya sea por la implementación de nuevos sistemas, por un cambio tecnológico, o por la competencia y fiabilidad del proveedor y del soporte técnico.

La sostenibilidad del SGD depende de que la supervisión de los cambios en el contexto interno y externo de la organización permita que el sistema se mantenga actualizado y sea capaz de responder a dichos cambios cuando sea necesario. El plan de continuidad del SGD se enmarca en el plan de continuidad del negocio y deben establecerse prioridades de actuación y procedimientos para la restauración después de una interrupción del servicio. Otros aspectos a tener en cuenta a la hora de identificar riesgos son: la capacidad del SGD para mantener la usabilidad de los documentos, la capacidad del SGD para importar documentos heredados de otros sistemas de gestión, la migración de documentos a nuevos sistemas, y otros aspectos relacionados.

La interoperabilidad se refiere a la capacidad de los SGD de relacionarse con otros sistemas. En este caso, la identificación de riesgos incluye aspectos como la identificación de las especificaciones requeridas para la interoperabilidad entre los SGD y otros sistemas de gestión, la compatibilidad con normas o especificaciones para el intercambio de documentos o la interoperabilidad entre sistemas, y la gestión de metadatos relacionados con los controles de gestión documental, entre otros.

Respecto a la seguridad del SGD, los riesgos incluyen la adecuación de la política de seguridad de la organización con respecto a los documentos, procesos de gestión documental y SGD, la capacidad de aplicar normas de acceso y los roles y permisos definidos por la organización tanto para el personal interno como para los proveedores o personas que trabajan en nombre de la organización,… Este apartado puede leerse en complementariedad con la serie de normas ISO/IEC 27000, de Sistemas de Gestión de la Seguridad de la Información.

Procesos documentales

Se refiere a los riesgos asociados a los procesos de gestión documental, que engloban procesos de creación de los documentos así como los procesos de control y gestión de documentos. Concretamente analiza los riesgos de las siguientes áreas de incertidumbre:

el diseño de documentos, la creación de documentos y la implementación de sistemas de gestión de documentos, los metadatos, el uso de los documentos y los sistemas de gestión de documentos, el mantenimiento de la usabilidad, y la disposición.

Respecto al diseño de los documentos, debe tenerse en consideración si las actividades de negocio se analizan de manera adecuada para identificar los requisitos de gestión de documentos, si la recogida de dichos requisitos se realiza de forma detallada para cada proceso de negocio, la clasificación y asignación de nombres a los documentos,…

Los procesos de creación de documentos e implementación de SGD engloban la identificación de riesgos para los momentos de creación y captura en los diferentes procesos de negocio, la integración de los procesos de creación y control de documentos en los procesos de negocio de la organización, la definición y asignación de responsabilidades, las especificaciones de los metadatos y los procesos que gestionan el acceso a la documentación.

Respecto a las especificaciones de los metadatos, estas deben ser accesibles para el personal autorizado y deben poder ser actualizadas cuando así lo requieran los procesos de negocio de la organización.

El uso de los documentos y la accesibilidad a los mismos, así como al SGD, debe tener en cuenta a la hora de identificar riesgos, la recuperación pertinente y a tiempo de los documentos, la adecuación de la gestión de permisos para todos los niveles de la organización así como el control de accesos, el mantenimiento de información sobre quién ha accedido o ha modificado documentos a lo largo del tiempo, la gestión de fallos en la seguridad del sistema y el cumplimiento con los procedimientos establecidos.

El mantenimiento de la usabilidad está muy relacionado con el punto anterior. Además de lo anteriormente especificado, debe considerarse el mantenimiento del significado de los metadatos a lo largo del tiempo, la adecuación de los procesos de gestión documental para la preservación de la autenticidad y fiabilidad de los documentos, la correcta gestión del historial de eventos y los aspectos relacionados con la obsolescencia del software (incluyendo la migración) y del hardware.

Por último, debe implementarse y autorizarse la disposición, incluyendo el desarrollo de los procedimientos para llevarla a cabo. La destrucción debe producirse siguiendo la legislación aplicable y debe estar debidamente autorizada y documentada. Del mismo modo, debe garantizarse la conservación de aquellos documentos que deban permanecer usables y accesibles a lo largo del tiempo.

Además de la parte más operacional, descrita anteriormente, esta norma ISO también tiene en cuenta el análisis del contexto de la organización (interno y externo) dentro del cual se enmarcaría la identificación de los riesgos operacionales específicos de los sistemas y procesos de gestión documental. Se analiza el contexto y se determinan unas áreas de incertidumbre en relación con la gestión de documentos.

Contexto externo

El contexto externo se refiere al entorno político, social, macroeconómico y tecnológico así como al entorno físico. Pese a que estos factores están fuera del control de la organización, pueden tener impacto en sus actividades, por lo que deberían tenerse en cuenta. Concretamente se analizan los riesgos de las siguientes áreas de incertidumbre: cambios en el entorno político-social, entornos macroeconómico y tecnológico, entorno físico e infraestructura, y amenazas de seguridad externas. Los cambios en el entorno social y político pueden conllevar modificaciones legales y normativas con un posible impacto en la organización y, como consecuencia, en los requisitos de sus documentos. Algunos ejemplos que pueden afectar a la gestión de los documentos son los relacionados con el acceso a la información, la privacidad, derechos de propiedad intelectual, responsabilidad social corporativa, entre otros. En relación a las amenazas de seguridad externas, la identificación del riesgo debería incluir desde daños en las instalaciones o en la prestación de servicios hasta accesos no autorizados, tanto al SGD como a otros sistemas de gestión de la organización.

Contexto interno

El contexto interno incluye aquellos factores internos no controlados por la persona responsable de los procesos y sistemas de gestión documental, como la estructura o las finanzas de la organización, el despliegue de tecnología, dotación de recursos, la cultura de la organización,… todo lo cual influye en las políticas y en el modo en que se gestionan los documentos. Concretamente analiza los riesgos de las siguientes áreas de incertidumbre: cambios en la organización, cambio tecnológico, personas y competencias, y recursos económicos y materiales.

■ Breve comparativa del sistema ISO/TR 18128 y el sistema ARMA

El sistema de apreciación del riesgo de la norma UNE-ISO/TR 18128:2014 se centra sobre todo en la parte operativa y baja muy al detalle en todos los aspectos referidos a los documentos, su creación, captura y control. En cambio, el sistema de ARMA está más enfocado hacia los riesgos de la gestión y administración de los sistemas que crean, gestionan y controlan documentos, y no baja hasta el detalle al que llega la norma ISO, que está más focalizada en los riesgos propios de los documentos.

El sistema ISO divide la identificación de riesgos en tres grandes áreas: contexto, sistemas y procesos, centrándose así en la parte más operativa de la gestión de documentos y, como hemos dicho, en aquellos aspectos que afectan directamente a los documentos. El sistema ARMA hace una distinción en cuatro bloques: administración, control de documentos, legislación y tecnología, menos operativa y más generalista, incluyendo aspectos que afectan a la gestión del sistema y, por tanto aunque de manera indirecta, también a los documentos.

Consideramos que ambos métodos son perfectamente válidos y que la mejor solución para una gestión global del riesgo dentro de una organización sería la combinación de ambas metodologías, ya que de este modo se contemplarían los aspectos de gestión y administración con los aspectos operativos de la documentación y la información.

2. Análisis de riesgos de la información y los documentos

Los riesgos se analizan para determinar sus consecuencias potenciales y la probabilidad de que ocurran (UNE-ISO/TR 18128:2014, 6.1). El análisis de riesgos siempre tiene en cuenta, por tanto, una combinación de causas o fuentes, probabilidad y consecuencias (ver Figura 5).

Las causas son la base para la prevención, ya que identificando el origen del problema pueden implantarse medidas de corrección y prevención, minimizando y mitigando los riesgos.

La probabilidad puede expresarse de diferentes maneras, pero normalmente es relativa al nivel de riesgo. Los métodos propuestos por los estándares internacionales (UNE-ISO 18128:2014, 6.2 e IEC 31010:2009, 5.3.1) son los cualitativos, semi-cuantitativos y cuantitativos. Los métodos cualitativos pueden combinar consecuencias, probabilidad y nivel de riesgo mediante niveles significativos como “alto”, “medio” y “bajo”. Los métodos semi-cuantitativos utilizan escalas numéricas para las consecuencias y probabilidades y las combinan utilizando una fórmula para determinar el nivel de riesgo. Las escalas pueden ser lineales o logarítmicas, o tener cualquier otra relación; la fórmula utilizada puede variar. Los métodos puramente cuantitativos son los que utilizan valores numéricos para las consecuencias y sus probabilidades, se pueden utilizar (estadísticamente) cuando haya datos disponibles sobre el desempeño de los procesos y sistemas de gestión documental durante un periodo significativo. Para ello es necesario el desarrollo de indicadores y controles que permitan estas mediciones a lo largo del tiempo.

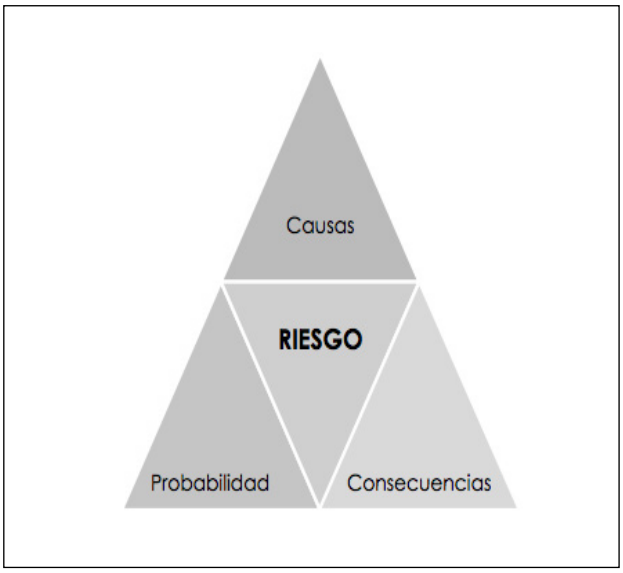

Figura 5 –Factores para el análisis del nivel de riesgo

Las consecuencias se identifican con la pérdida o daño de los documentos que afectan a su usabilidad, autenticidad, completitud e inalterabilidad a lo largo del tiempo y, por consiguiente, pueden fallar en el soporte a las actividades de la organización. Su análisis determina la naturaleza y el impacto que podría tener un evento, situación o circunstancia en particular si ocurriese. Dicho evento puede tener un rango de impacto de magnitudes

diferentes así como afectar a diferentes objetivos y partes interesadas. Los tipos de consecuencias a analizar y las partes interesadas afectadas podrán ser determinadas a partir del análisis del contexto de la organización.

El análisis de las consecuencias puede centrarse en dos aspectos diversos: por un lado, en la severidad y la afectación que supondría dentro de la organización, proceso, o procedimiento analizado; y por otro lado, en los posibles efectos que podrían ocurrir si se da el caso, como por ejemplo pérdida de credibilidad o fiabilidad de la organización, pérdida de clientes, despidos,… Los efectos pueden valorarse junto con la severidad, aunque analizados por separado pueden proporcionar mucha más información para la toma de decisiones.

3. Evaluación de riesgos de la información y los documentos

La evaluación del riesgo es aquella parte de la gestión de riesgos que proporciona un proceso estructurado para identificar cómo los riesgos pueden afectar a los objetivos, y para analizar el riesgo en términos de consecuencias y probabilidades para la toma de decisiones sobre el tratamiento y control más oportuno (IEC 31010:2009, Introducción). El propósito es ayudar a tomar decisiones sobre qué riesgos necesitan tratamiento y con qué prioridad, partiendo de los resultados del análisis (UNE-ISO 18128:2014, 7.1). Las decisiones pueden incluir cuándo un riesgo necesita tratamiento, la prioridad de tratamiento, o cuándo una actividad de control debería llevarse a cabo, entre otras. Tratar o no el riesgo y cómo hacerlo dependerá de los costes y beneficios asociados a correr el riesgo, y los costes y beneficios asociados a implementar acciones de control y de mejora.

La evaluación en relación con la probabilidad y las consecuencias adversas debería dar el suficiente peso a los incidentes excepcionales o sin precedentes cuando tienen un impacto generalizado y grave. Asimismo, el impacto de una acumulación de incumplimientos leves puede ser muy superior a un incidente individual si el resultado es el deterioro de la integridad y fiabilidad de los documentos o del sistema de gestión de documentos.

■ Conclusiones

En este artículo se han presentado varias metodologías para una apreciación del riesgo asociado a los documentos. Es especialmente importante llevar a cabo una identificación de riesgos completa y pertinente, combinando las metodologías propuestas, sin olvidar los enfoques de aproximación a la identificación de Lemieux que mejor se adapten a la realidad en la que opera la organización. Para que la apreciación del riesgo sea completa deben valorarse tanto aspectos puramente operativos como de la administración y gestión de los procesos y sistemas, y para ello una de las mejores alternativas es fusionar las dos metodologías presentadas (ARMA e ISO), ya que permiten la identificación de riesgos de manera global. Pero el proceso no finaliza ahí, sino que a partir de la identificación, análisis y evaluación de los riesgos es que debe realizarse un esfuerzo por parte de la organización y de los responsables de la gestión documental con el objetivo último de mejorar, implantando acciones y controles periódicos, designando responsables, implementando nuevos procesos o revisando los ya existentes para blindar el SGD y que éste pueda servir a la rendición de cuentas.

La identificación y el tratamiento de riesgos que pueden afectar a los documentos, sistemas y procesos de gestión documental son un modo de anticiparse y de asegurar una efectiva y confiable rendición de cuentas a través de la garantía de la integridad, fiabilidad, autenticidad y usabilidad de los documentos. Para ello, el proceso debe ser proactivo, identificando las debilidades del sistema, los riesgos potenciales e implantando controles y tratamientos que mitiguen y reduzcan al máximo la probabilidad de que algo negativo ocurra. Hay que anticiparse, tanto a los posibles errores y pérdidas de información como a la desclasificación de documentos y la provisión de información para los procesos de rendición de cuentas,… en definitiva, se trata de mejorar los SGD desde la base de un amplio conocimiento de sus fortalezas y debilidades, asumiendo que los errores pueden ocurrir (y ocurren) y siendo conscientes de que existen mecanismos y metodologías para reducir las probabilidades de que ocurran.

Las organizaciones pueden anticiparte a la fase de información del proceso de rendición de cuentas disponiendo de un SGD, y decidiendo qué documentos es necesario crear y conservar como evidencia de las decisiones y acciones de la organización. Pero también pueden ir más allá, implantando una política de gestión del riesgo en la que se incluyan los riesgos de los documentos y la información como medida de prevención y previsión para garantizar los procesos de rendición de cuentas.

■ Bibliografía

ARMA International. “Evaluating and Mitigating Records and Information Risks. An ARMA International Guideline”. USA: ARMA International, 2009.

Bovens, Mark. “Two Concepts of Accountability: Accountability as a Virtue and as a Mechanism”. En West European Politics, 2010, vol. 33, n. 5, pp. 946-967.

Egbuji, Angel. “Risk management of organisational records”. En Records Management Journal, 1999, vol. 9 Iss 2, pp. 93-116.

IEC 31010:2009 – Risk Management. Risk assessment techniques. International Standard Organization, 2009.

ISO/IEC 27005: 2008 – Information technology. Security techniques. Information security risk management. International Standard Organization, 2008.

Lemieux, Victoria. “Two Approaches to Managing Information Risks”. En The Information Management Journal, 2004, sept-oct, pp. 56-62.

Lemieux, Victoria. “The records-risk nexus: exploring the relationship between records and risk”. En Records Management Journal, 2010, vol. 20 Iss 2, pp. 199-216.

Meijer, Albert. “Accountability in an Information Age: Opportunities and Risks for Records Management”. En Archival Science, 2001, vol. 1, pp. 361-372.

Meijer, Albert. “Anticipating Accountability Processes”. En Archives and Manuscripts, 2000, mayo, vol. 28, n. 1, pp. 52-63.

Millar, Laura. “The Right to Information – the Right to Records. The Relationship between Record Keeping, Access to Information, and Government Accountability”. International Records Management Trust, 2003.

Pullen, Troy; Maguire, Heather. “The information management risk construct: identifying the potential impact of information quality on corporate risk”. En International Journal of Information Quality, 2007, vol. 1 (4). pp. 412-443.

Roberts, Alasdair. “Dashed Expectations: Governmental Adaptation to Transparency Rules”. En Hood, Christopher; Heald, David (Eds.). Transparency. The Key to Better Governance? New York: Oxford University Press, 2006, pp. 107-125.

UNE-ISO 31000: 2010 – Gestión del riesgo. Principios y directrices. Asociación Española de Normalización y Certificación, 2010.

UNE-ISO/IEC 27001: 2007 – Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI). Requisitos. Asociación Española de Normalización y Certificación, 2007.

UNE-ISO/TR 18128: 2014 – Información y documentación. Apreciación del riesgo en procesos y sistemas de gestión documental. Asociación Española de Normalización y Certificación, 2014.