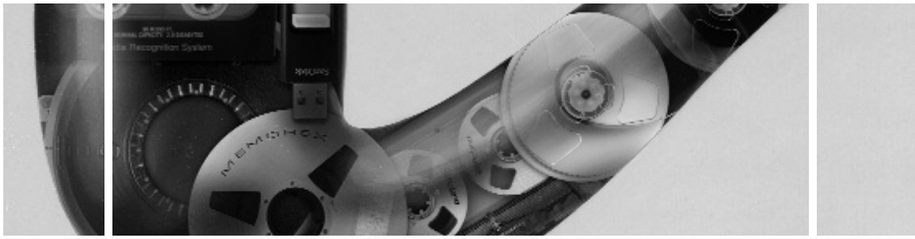
studia



TAMARA MORTE NADAL

El papel del archivero en la gestión del riesgo asociada a la gestión de documentos

The role of the archivist in risk management for records management

Tamara Morte Nadal
tmorte@unizar.es
Facultad de Filosofía y Letras. Universidad de Zaragoza

Citación: Morte Nadal, Tamara (2021). "El papel del archivero en la gestión del riesgo asociada a la gestión de documentos". *Tábula,* n. 24, pp. 21-43

Recibido: 18-1-2020. Aceptado: 2-4-2021
DOI: https://doi.org/xxx

Resumen analítico / Analitic summary

La gestión de riesgos apareció a mediados del siglo XX dentro de las empresas privadas. No obstante, la relación de la gestión del riesgo con la gestión documental es relativamente reciente y la mayoría del conocimiento se concentra en las normativas internacionales. El objetivo de este trabajo es aplicar la metodología de gestión de riesgos asociados con la gestión de documentos en el proceso de implantación de la Administración Electrónica en el Gobierno de Aragón. Se concluye con la necesidad de integrar las materias de gestión de riesgos y de gestión documental en el proceso de implantación de la administración electrónica.

GESTIÓN DE RIESGOS | GESTIÓN DOCUMENTAL | ADMINISTRACIÓN ELECTRÓNICA | GOBIERNO DE ARAGÓN | ESTUDIO DE CASO

Risk management appeared in the mid-20th century within private companies. Nevertheless, the relationship between risk management and records management is relatively recent and most of the knowledge is concentrated in international regulations. The aim of this study is to apply risk management methodology to records management in the process of implementation of electronic Administration in the Government of Aragon. It is concluded the need to integrate the subjects of risk management and document management in the process of implementation of electronic administration.

RISK MANAGEMENT | RECORDS MANAGEMENT | ELECTRONIC ADMINISTRATION | GOVERNMENT OF ARAGON | CASE STUDY

En el año 2018 se produjeron filtrados masivos de información personal provocados por ataques informáticos. El mayor de todos esos ataques se situó en la India. La base de datos del gobierno, Aadhaar, sufrió múltiples filtrados de datos que comprometió la información de los 1.1 billones de ciudadanos registrados. Otros casos parecidos fueron los 150 millones y los 50 millones de usuarios afectados por las aplicaciones MyFitnessPal y Facebook, respectivamente. La vulnerabilidad potencial de la infraestructura tecnológica se ha convertido cada vez más en un problema de seguridad nacional (World Economic Forum, 2019).

En Aragón, el día 28 de mayo de 2019, se produjo un fallo en el hardware del sistema de almacenamiento del Gobierno de Aragón, alojado en el Parque Tecnológico Walqa (Huesca). Este problema en el sistema informático generó problemas en la Administración general, en las páginas web oficiales, en el Boletín Oficial de Aragón, en el sistema informático del Servicio Aragonés de Salud y en el de la Administración de Justicia. El origen del problema fue un fallo eléctrico registrado en la zona, que supuso un bloqueo automático del hardware del centro de datos para salvaguardar los datos y su integridad. Esta incidencia puede suponer para el proveedor del servicio una sanción de alrededor de 100.000 euros (Lahoz y Gabás, 2019).

El crecimiento del volumen de información en soporte electrónico al que se enfrentan las organizaciones y el aumento de los riesgos asociados a este hacen necesario un eficaz control de la información. Porque si la información no dispone de un adecuado sistema de gestión durante todo su ciclo de vida, se puede generar una masa de datos y documentos inmanejable, con el riesgo añadido que supone una pobre conservación. Por su parte, la tecnología debe aportar soluciones que permitan la gestión de los archivos de documentos y de datos. Pero, ante

todo, se debe aplicar un modelo de identificación y gestión de riesgos que incluya las políticas y estrategias de seguridad respecto a la información electrónica (García-Morales, 2013).

Es necesario señalar que la gestión de riesgos aplicada a la gestión documental es un ámbito de estudio poco explorado**,** ya que apenas existen estudios de caso e investigaciones. La mayoría del conocimiento sobre el tema se encuentra en normas ISO. Este trabajo tiene como objetivo presentar una metodología basada en la gestión del riesgo para la identificación de peligros relacionados con la gestión documental; y se basa en un estudio de caso del Servicio de Administración Electrónica (SAE) del Gobierno de Aragón entre los meses de abril y junio de 2019.

Objetivos

El objetivo general de este trabajo es aplicar la metodología de gestión de riesgos asociados con la gestión de documentos en el proceso de implantación de la Administración Electrónica en el Gobierno de Aragón.

Y sus objetivos específicos son:

- Explicar y comprender qué es la gestión del riesgo y la normativa internacional al respecto.
- Analizar las dimensiones y la metodología de la gestión de riesgos aplicada a la gestión de documentos en un entorno electrónico.
- Identificar los riesgos vinculados con la gestión de documentos en el Servicio de Administración Electrónica del Gobierno de Aragón.

El concepto de riesgo y de gestión de riesgos

La norma *UNE-ISO 31000:2018 Gestión del Riesgo. Directrices* (en adelante, ISO 31000) entiende por riesgo el "efecto de la incertidumbre sobre los objetivos", que precisa mediante una serie de aclaraciones (AENOR, 2018). De esta definición se deduce que el concepto de riesgo se amplía para acoger simultáneamente estos sentidos: la incertidumbre que caracteriza a una actividad; la probabilidad de que algo ocurra; o un evento futuro o una circunstancia que puede mejorar o disminuir la capacidad de la organización para conseguir sus objetivos. Este último sentido muestra las dos connotaciones que puede tener el concepto riesgo: la negativa (incertidumbre, amenaza, obstáculo) y la positiva (oportunidad). Cabe mencionar que el riesgo no hace referencia a problemas actuales, sino a problemas potenciales (Popescu y Helerea, 2012) y que precisamente porque la noción

del riesgo se basa en un número infinito de factores, es imposible prevenir completamente un riesgo (Gellert, 2015).

El concepto de riesgo ha ido evolucionando desde su aparición a mediados del siglo XX hasta desarrollar el concepto próximo de gestión de riesgos. De un foco que se situaba en la nación o en la sociedad (ya que estaba muy ligado a los estudios de seguridad e inteligencia), saltó a las empresas y organizaciones en 1963 cuando Robert I. Mehrs y Bob Hedges publicaron "*Risk Management and the Business Enterprise*". No obstante, hasta los años 80 no se comenzaron a crear estándares públicos y guías de mejores prácticas para la gestión de riesgos (Villanueva, 2015).

Las primeras etapas de la gestión de riesgos se orientaron a la identificación de riesgos fortuitos, basándose en experiencias previas y en la determinación del coste de dicho aseguramiento y la transferencia de riesgos a terceros. Con la crisis del petróleo, las subidas del tipo de interés y la volatilidad del mercado de divisas de los años 70 y 80, se centró en las posibles pérdidas derivadas de los eventos de riesgo, especialmente causadas por riesgos asegurables y financieros. Más adelante se abordó de manera más integral, ampliando el foco a los riesgos operacionales y estratégicos, sin olvidar el impacto económico.

En definitiva, se empezó a considerar a las organizaciones como un sujeto que es objeto de riesgos muy heterogéneos y en numerosas ocasiones interrelacionados entre sí. El aumento de la complejidad de los riesgos afrontados (globalización económica, multiculturalidad, la fragmentación y diversidad de los mercados, el avance tecnológico), la presión regulatoria y la necesidad de adoptar una visión global, debido a que el riesgo puede ser multifactorial, forzaron la evolución de los enfoques y técnicas de gestión de riesgos. Esto supuso la implantación y el desarrollo de sistemas globales o integrados de gestión de riesgos en las empresas (*Enterprise Risk Management Systems*, ERP), que abarcan y conectan todas sus áreas convirtiéndose en un elemento esencial de éstas (Villanueva, 2015).

De este modo se ha llegado al concepto actual de gestión de riesgos, definido por la Norma ISO 31000 como "*actividades coordinadas para dirigir y controlar la organización con relación al riesgo*". La gestión de riesgos es considerada como un proceso sistemático de identificación, análisis, acercamiento y control de los riesgos dentro de una organización. Es decir, se trata de una serie de actividades coordinadas para dirigir y controlar a una organización respecto al riesgo, que pueden adaptarse a cualquier organización y contexto (Popescu y Helerea, 2012). Para ello, la gestión de riesgos se dota de un conjunto de técnicas y herramientas que ayudan a tomar las decisiones más apropiadas, teniendo en cuenta la incertidumbre, la posibilidad de futuros sucesos y los efectos sobre los objetivos establecidos.

La gestión del riesgo está basada en unos principios, un marco de referencia y un proceso que se describen en la norma ISO 31000. Estos componentes podrían existir de manera previa en parte o en toda la organización, pero puede ser necesario modificarlos para que la gestión del riesgo sea eficiente, eficaz y coherente

(AENOR, 2018). Necesita del establecimiento de una infraestructura adecuada y de una cultura de gestión de riesgos. En consecuencia, se deben aplicar procesos lógicos y sistemáticos de gestión de riesgos a todos los estados del ciclo de vida de cualquier actividad, función u operación (Popescu y Helerea, 2012).

Normativa sobre gestión del riesgo y el proceso de gestión del riesgo

La ya mencionada ISO 31000 establece una serie de principios y directrices para gestionar de forma eficaz el riesgo, pero no cómo integrar la gestión del riesgo en los procesos de gestión de las organizaciones. El informe técnico *UNE-ISO/ TR 31004:2015 Gestión del riesgo. Orientación para la implementación de la Norma ISO 31000* (en adelante, ISO/TR 31004) es complementario a la ISO 31000. Proporciona una metodología general a las organizaciones sobre cómo implementarla y cómo integrarla en los procesos de gestión de su organización. Otra norma internacional que complementa a la norma ISO 31000 es la norma *ISO/IEC 31010:2011 Gestión de Riesgos: Técnicas de apreciación del riesgo* (en adelante, ISO 31010). Su objetivo es proporcionar directrices para la selección y aplicación de técnicas sistemáticas para la apreciación del riesgo.

Según la ISO 31000, el proceso de gestión del riesgo es la aplicación sistemática de políticas, procedimientos y prácticas a las actividades de comunicación y consulta, establecimiento del contexto y evaluación, tratamiento, seguimiento, revisión, registro e informe del riesgo. Aunque se suele presentar como secuencial, en la práctica se trata de un proceso iterativo (AENOR, 2018). En el apartado 4 nos centraremos en el punto 3, el proceso de evaluación del riesgo.

Proceso de gestión del riesgo	
1. Comunicación y consulta	Comunicación y consultas con las partes interesadas
2. Alcance, contexto, criterios	Establecimiento del alcance, contexto externo e interno de la organización, y de los criterios del riesgo
3. Evaluación del riesgo	3.1 Identificación del riesgo Elaboración de una lista de riesgos exhaustiva 3.2 Análisis del riesgo Comprender la naturaleza del riesgo y su nivel de riesgo 3.3 Valoración del riesgo Toma de decisiones sobre las medidas a tomar, si son necesarias
4. Tratamiento del riesgo	Seleccionar e implementar opciones para abordar el riesgo Preparación e implementación de los planes de tratamiento
5. Seguimiento y revisión	Acciones de seguimiento y revisión periódicas
6. Registro e informe	Documentación del proceso de gestión del riesgo y de sus resultados a través del registro e informe

Tabla 1. Proceso de gestión del riesgo. Resumen. Fuente: ISO 31000

La gestión del riesgo dentro de la gestión de documentos

En la década de los 90 del siglo XX comenzaron a aparecer trabajos que analizaban las interrelaciones entre los procesos de gestión documental y los de gestión de riesgos. Se identificó que muchas de las dificultades de la gestión financiera provenían de la ausencia de métodos de gestión documental para los documentos creados por los sistemas de contabilidad (Mena y del Castillo, 2018a).

En 1998, McKemmish en la *22nd Annual Conference of the Archives and Records Association of New Zealand* declaró que el fracaso de los sistemas de gestión documental generaba riesgos organizacionales y sociales. Lemieux (2001) exploró la relación entre fracasos organizacionales y una pobre o inexistente gestión documental. La misma autora conceptualizó años después los riesgos en los documentos electrónicos en términos prácticos (Lemieux, 2004). Posteriormente, Lemieux (2010) publicó un estado de la cuestión sobre la literatura especializada en la relación entre documentos y riesgos.

McDonald (1995 y 2005) abordó en dos trabajos los riesgos del impacto de las tecnologías en la gestión de los documentos electrónicos en las oficinas. Bearman (2007) en un trabajo posterior presentó los seis puntos críticos en el que los riesgos sobre los procesos de gestión de documentos electrónicos se acentúan: captura, mantenimiento, ingreso, acceso, eliminación y preservación. En una línea similar se encuadra la tesis doctoral de Hay-Gibson (2011) sobre la gestión del riesgo asociada a la gestión de documentos electrónicos en el entorno de la Administración Electrónica, tras señalar que era un ámbito que apenas había sido explorado. También en el ámbito anglosajón se han publicado la mayoría de artículos que relacionan gestión documental con rendición de cuentas y gestión de riesgos (Mena y del Castillo, 2018a).

En España Montserrat García Alsina (2012) fue pionera en indicar la necesidad de diseñar sistemas de gestión documental que incluyan la gestión de los riesgos naturales, humanos o técnicos. Unos años después, Elisa García-Morales (2016) planteó las relaciones entre la gestión de riesgos, la gestión de la seguridad de la información y la gestión documental. Por su parte, Anahí Casadesús (2016) ha presentado la gestión de riesgos aplicada a la gestión de documentos como una forma de garantizar la rendición de cuentas. Esta autora analizó en 2017 las normas de gestión documental desde la perspectiva de la gestión del riesgo, la auditoría de la información y el análisis de procesos. También se debe a Casadesús

(2018) el trabajo más completo sobre la metodología de gestión del riesgo aplicada a la gestión de documentos: una tesis doctoral defendida en la Universidad Autónoma de Barcelona compuesta por un estudio teórico acompañado de un estudio de caso sobre un Ayuntamiento catalán.

Normativa de la gestión del riesgo dentro de la gestión de documentos

Algunas de las organizaciones que han trabajado en la normalización del proceso de gestión del riesgo con relación a la información y los documentos han sido el *UK Institute of Risk Management* (IRM), la *International Standardization Organization* (ISO), *Standards Australia* (SA) y la *Association of Records Managers and Administrators* (ARMA International) (Casadesús, 2018).

Si se analiza la normativa ISO sobre gestión documental, se puede observar que la gestión de documentos es una buena aliada de la gestión de riesgos. En esta normativa se refleja la convicción de que crear y controlar documentos de manera sistemática y verificable contribuye a minimizar los riesgos relacionados con la creación de evidencias de actividades o transacciones organizacionales (Mena y del Castillo, 2018b). Además, están alineadas con los postulados de la gestión de riesgos, ya que asumen en mayor o menor medida la necesidad de identificar y analizar riesgos en su ámbito de acción. Como ejemplo, la norma ISO 30301 dedica a esta materia un apartado completo ("Acciones para hacer frente a riesgos y oportunidades"), donde se muestra cómo la organización debe determinar los riesgos y las oportunidades que necesitan tratamiento, para asegurar que el SGD alcance los resultados esperados, prevenir o reducir los efectos no deseados y lograr la mejora continua (AENOR, 2019).

De acuerdo con la normativa ISO, la gestión de riesgos puede aplicarse a la gestión documental en varios ámbitos: para gestionar los riesgos de un proyecto de implantación de un SGD o de una aplicación para documentos electrónicos; para identificar riesgos de negocio que pueden mitigarse con la creación y gestión de los documentos necesarios; y para gestionar los riesgos a nivel operativo en los procesos y sistemas de gestión documental (Bustelo, 2014). Para apoyar la acción en esta tercera área se cuenta con el informe técnico ISO/TR 18128:2014, adoptado como norma UNE el mismo año 2014, que relaciona las normas ISO 31000 de gestión del riesgo y la norma ISO 30301 de sistemas de gestión de documentos. Este informe, dirigido a los profesionales de la gestión de documentos y a las personas responsables de los documentos en las organizaciones, se centra en la identificación y el control de los riesgos documentales en las organizaciones (Casadesús, 2017). Su objetivo es asistir a las organizaciones en la apreciación de los riesgos relacionados con la implantación y el mantenimiento de sistemas y procesos de gestión documental (AENOR, 2014).

La ISO/TR 18128 adopta un enfoque operativo, ya que se centra en todos los aspectos relacionados con la creación, captura y control de los documentos, atendiendo para su identificación al contexto en el que se produce, los sistemas que se emplean y los procesos que se siguen (Casadesús, 2016). La premisa de la que parte el informe ISO/TR 18128 es que la organización ya ha creado documentos de sus actividades y que ha establecido un mecanismo para la gestión y control sistemático de los mismos. Es importante reseñar que el informe ISO 18128 no abarca el tratamiento del riesgo, puesto que la respuesta ante los riesgos forma parte del programa global de gestión del riesgo (AENOR, 2014).

El proceso de evaluación del riesgo en procesos y sistemas de gestión documental

La evaluación (denominada como apreciación en el informe técnico ISO/TR 18128[1]) del riesgo de los sistemas y los procesos de gestión documental se incluye dentro del proceso general de gestión del riesgo de la organización, como se ha podido observar en la tabla 1. Esta evaluación se realiza mediante tres subprocesos secuenciales: identificación, análisis y evaluación.

En la identificación de riesgos se detecta qué podría suceder o qué situaciones pueden darse, que puedan afectar a la capacidad de los documentos para satisfacer las necesidades y objetivos de la organización. Las potenciales acciones que generan incertidumbre pueden ser tanto externas como internas a la organización (AENOR, 2014).

Es importante contar con información pertinente, apropiada y actualizada. La organización debería identificar los riesgos, tanto si sus fuentes están o no bajo su control. Para ello pueden utilizar técnicas diferentes (AENOR, 2018). Los métodos de identificación del riesgo pueden estar basados en evidencias (listas de verificación, revisiones de datos históricos), enfoques sistemáticos del equipo (un grupo de expertos sigue un proceso sistemático para identificar riesgos) o técnicas de razonamiento inductivo (HAZOP). También se pueden aplicar técnicas de apoyo para mejorar la precisión y la exhaustividad, como la tormenta de ideas o la metodología Delphi (AENOR, 2011). Independientemente de las técnicas empleadas, es importante dar el debido reconocimiento a los factores humanos y de la organización, así como atender a los elementos del "hardware" y del "software".

A continuación, se pasa a la etapa del análisis. En esta etapa se comprende la naturaleza del riesgo y sus características, incluyendo, cuando sea apropiado, el nivel del riesgo. El análisis del riesgo implica una consideración detallada de incertidumbres, fuentes de riesgo, consecuencias, probabilidades, eventos, escenarios, controles y su eficacia. Es importante tener en cuenta que un suceso puede tener múltiples consecuencias y afectar a múltiples objetivos (AENOR, 2018).

Las técnicas de análisis que se utilicen pueden ser cualitativas (por ejemplo, categorías de tipo alto, medio o bajo), cuantitativas (valores numéricos) o una combinación de ambas (AENOR, 2018). Es necesario indicar que todos los niveles de riesgo que se calculen serán estimativos (AENOR, 2011).

El análisis del riesgo proporciona una entrada para la valoración del riesgo, para las decisiones sobre la manera de tratar los riesgos, si es necesario, y sobre la estrategia y los métodos más apropiados para el tratamiento del riesgo (AENOR, 2018). Se establecen dos tipos de consecuencias que puede tener la no prevención de los riesgos identificados en la gestión documental: primarias y secundarias. Las consecuencias primarias de los riesgos son la pérdida o daño de los documentos, que ya no serían usables, fiables, auténticos e íntegros o inalterados. En cambio, las consecuencias secundarias se asocian a pérdidas económicas, de prestigio, de credibilidad, mala reputación, incumplimiento de las obligaciones de transparencia y de rendición de cuentas, despidos de personal… (Casadesús, 2017).

Por último, el tercer subproceso es la valoración. Su propósito es apoyar la toma de decisiones. Implica comparar los resultados del análisis del riesgo con los criterios del riesgo establecidos para determinar si se requieren acciones adicionales. Estas decisiones pueden ser (AENOR, 2018):

- No hacer nada más.
- Considerar opciones para el tratamiento del riesgo.
- Realizar un análisis adicional.
- Mantener los controles existentes.
- Reconsiderar los objetivos.

La norma ISO/TR 18128 aporta información sobre la evaluación de la probabilidad para los eventos de riesgo relacionados con el contexto externo e interno, con los sistemas y con los procesos (AENOR, 2014). Puede haber una frecuencia muy baja o ninguna circunstancia histórica de una situación, pero no se puede asumir que dichos eventos no puedan ocurrir (AENOR, 2014).

Algunos factores a tener en cuenta en esta fase son el número de usuarios y partes interesadas afectadas, el efecto del daño o de la pérdida de los documentos en las operaciones en curso de la organización, las medidas existentes para responder a la interrupción en el acceso, el tiempo y esfuerzo para recobrar o reemplazar los documentos afectados, el impacto de la pérdida o del daño en los derechos o en la capacidad de la organización para cumplir con sus obligaciones, y el impacto de la imagen pública de la organización.

El impacto potencial de los eventos adversos se puede clasificar utilizando los factores identificados como los más relevantes para el tamaño y la naturaleza de las actividades de la organización. Las categorías para evaluar los riesgos son de tipo cualitativo: menor, moderado, mayor y severo (AENOR, 2014).

El proceso de identificación de riesgos en procesos y sistemas de gestión documental: Servicio de Administración Electrónica del Gobierno de Aragón

Aunque la norma ISO/TR 18128 propone una metodología para la evaluación del riesgo para procesos y sistemas de gestión documental, ninguna institución española ha publicado una guía para llevar a cabo la evaluación del riesgo vinculada a la gestión documental. Por lo tanto, a la hora de llevar a cabo este trabajo se partió directamente de la norma UNE ISO 31000, del informe técnico 18128, complementándolo con la norma ISO 31010 y la metodología que desarrolló Anahí Casadesús en su tesis doctoral (2018), "La gestión del riesgo aplicada a la gestión de documentos y su impacto en la rendición de cuentas pública".

Es necesario indicar que en este estudio solo se pudo completar la fase de identificación de riesgos relacionada con la gestión documental. Además, cabe mencionar que antes de realizar la fase de evaluación, se tuvieron que llevar a cabo las dos primeras etapas del proceso general de gestión del riesgo, la comunicación y consulta; y el alcance, contexto y criterios de la organización. Para ambas etapas fue de gran utilidad la técnica de la observación participante, que la investigadora realizó durante los meses de abril a junio de 2019.

El objetivo de la comunicación y la consulta era el de asistir a las partes interesadas a comprender el riesgo, las bases con las que se toman decisiones y las razones por las que son necesarias ciertas acciones (AENOR, 2018). La propia organización tenía conciencia de la importancia de obtener información de calidad que pudiera asistirla en toma de decisiones. También se tuvo en cuenta el contexto interno y externo, el contexto del propio proceso de gestión del riesgo, los roles y las responsabilidades de los miembros del SAE, el alcance y amplitud de las actividades de evaluación del riesgo, la metodología, y los criterios de riesgo (AENOR, 2014). Estos criterios de riesgo debían derivarse de los requisitos legales que el Gobierno de Aragón tenía que cumplir.

A parte de los datos que se tomaron de la observación participante directa, durante ese periodo se llevaron a cabo una serie de entrevistas semiestructuradas al personal del SAE y a la Jefa de Sección del Archivo de la Administración del Gobierno de Aragón, Magdalena Gómez de Valenzuela.

De acuerdo a la norma ISO/TR 18128, para identificar los riesgos relacionados con la gestión documental deben analizarse las siguientes áreas de incertidumbre: contexto, sistemas y procesos. La tabla 2 recoge de modo sumario los diversos elementos que se deben atender para identificar riesgos de acuerdo con estas categorías. Existen diversos métodos para su identificación: los principales métodos se comparan en el anexo B de la Norma ISO 31010 (AENOR, 2014).

Identificación del riesgo en sistemas y procesos de gestión documental		
Contexto	Externo	Contexto político social Económico y tecnológico Entorno físico e infraestructura Seguridad
	Interno	Organización Tecnologías Personas Recursos económicos y materiales
Sistemas de gestión documental	Diseño Mantenimiento Sostenibilidad y continuidad Interoperabilidad Seguridad	
Procesos documentales	Diseño Creación de documentos e implementación de SGD Metadatos Uso de documentos y de SGD Mantenimiento de la usabilidad Disposición	

Tabla 2. Elementos para la identificación de riesgos.
Fuente: elaboración propia

El contexto debería reflejar el entorno especifico de la actividad en la cual se va a aplicar el proceso de la gestión del riesgo (AENOR, 2018). Es importante analizar el entorno (interno y externo) porque la gestión del riesgo ocurre en el contexto de los objetivos y las actividades de la organización, de modo que los factores organizacionales pueden ser una fuente de riesgo. Los elementos que deberían analizarse dentro de los sistemas de gestión documental son su diseño, los problemas de la plataforma tecnológica, su sostenibilidad y continuidad, y los problemas de interoperabilidad y seguridad. Hay que tener en cuenta que los sistemas de gestión documental cambian a lo largo del tiempo, debido a circunstancias económicas, cambios en las actividades y el personal y a cambios en el tamaño y estructura. Por último, la identificación de riesgos en los procesos documentales se centra en la creación de los documentos, en elementos de los propios documentos y en los procesos de control y gestión (AENOR, 2014).

Una vez se han definido estos tres elementos, se tuvieron que seleccionar métodos para la identificación del riesgo. Tomando como referencia la norma ISO 31010, se eligieron la tormenta de ideas y la aplicación de listas de verificación.

La tormenta de ideas permite recopilar un conjunto de ideas que luego son sometidas a clasificación. Por su parte, las listas de verificación son una lista de incertidumbres típicas que es necesario tener en consideración, puesto que se han desarrollado generalmente a partir de la experiencia como resultado de una apreciación previa del riesgo o como resultado de fallos ocurridos en el pasado (AENOR, 2011).

La tormenta de ideas se utilizó en varias sesiones conjuntas con el SAE durante los meses de mayo y junio de 2019. Siguiendo la metodología de Casadesús (2018), la tormenta de ideas tuvo un enfoque basado en amenazas, es decir, posibles amenazas que podrían surgir o que surgieron en algún momento determinado. Esta técnica se apoyó en la información que se obtuvo durante la observación participante y las entrevistas. Posteriormente, se utilizaron dos listas de verificación para que la identificación fuera lo más exhaustiva posible: el *Catálogo de elementos de la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información* (MAGERIT) y la lista de comprobación para identificar áreas de incertidumbre del informe técnico ISO/TR 18128:2014.

Los motivos para la selección de estas técnicas fueron, de acuerdo con la norma UNE-ISO 31010 su facilidad de aplicación, las necesidades de la organización (se necesita una comprensión más general que detallada), el grado de conocimientos técnicos y la experiencia profesional que requerían, las limitaciones que se tenían en el tiempo y la disponibilidad de información y de datos. Se trata de técnicas poco complejas, que no requieren de muchos recursos o capacidades.

Conclusiones y reflexiones

Por temas de protección de datos no se pueden mostrar los resultados de la aplicación de esta metodología, ya que competen al Gobierno de Aragón. No obstante, no se quiere dejar la pasar la oportunidad de hacer una serie de reflexiones sobre la gestión del riesgo aplicada a la gestión de documentos, así como señalar las limitaciones del trabajo que se realizó.

La gestión del riesgo se utiliza ampliamente en los procesos de evaluación de riesgos técnicos, relacionados con de seguridad informática. Pero no sé puede afirmar que la pérdida, destrucción o inadecuada gestión de documentación de una organización no le suponga ninguna consecuencia. Según se infiere de la norma ISO/TR 18128, ignorar la gestión documental podría tener consecuencias legales (por ejemplo, en materia de protección de datos y de transparencia), provocar pérdida de patrimonio documental, afectar a la toma de decisiones, limitar la rendición de cuentas, dañar la imagen pública de la entidad, añadir riesgos de seguridad y disminuir la calidad de los servicios. Por ejemplo, un acceso no autorizado a los datos podría suponer consecuencias a nivel legal por infracción de la

legislación de protección de datos. Tampoco se puede obviar desde la perspectiva de la política de gestión de documentos la relación entre la gestión del riesgo aplicada a los documentos y la capacidad de transparencia de las organizaciones, un requerimiento determinado en gran medida por exigencias y normativas exteriores a estas. Una adecuada gestión documental garantiza los derechos de los ciudadanos y de la propia Administración. Porque si se produce algún fallo el afectado es el ciudadano y, además, la Administración tiene responsabilidades legales y patrimoniales al respecto, puesto que tiene la obligación de garantizar a los ciudadanos el ejercicio de sus derechos. Además, en la actualidad sigue generándose una gran cantidad de papel en las administraciones. Estos documentos también tienen riesgos vinculados con su gestión documental, que pueden coincidir o no con los del soporte digital.

Para finalizar, se recogen algunas limitaciones. En primer lugar, se debe destacar la limitación temporal de la que se dispuso por circunstancias personales de la investigadora, que se encontraba en periodo de prácticas curriculares en el SAE y por lo tanto estaba sujeta a un plan de estudios oficial. Por lo tanto, solo fue posible desarrollar la fase de identificación de riesgos documentales.

La utilización de dos técnicas cualitativas (tormenta de ideas y listas de verificación) implicó que no se contase con datos cuantitativos. Por lo tanto, se tiene en cuenta que ambas técnicas están sujetas a cierta subjetividad. Además, en el caso de las entrevistas, deben tenerse en cuenta los sesgos, tanto del entrevistador como de los entrevistados, que pueden afectar a los resultados. Especialmente cuando se habla de un tema tan delicado en una institución publica como es la seguridad y la protección de la información.

Como recomendaciones generales que pudieron extraerse de la revisión bibliográfica previa al estudio de caso y de la normativa ISO, se sugiere la creación de un modelo de identificación y gestión de riesgos en las organizaciones, que tenga en cuenta el contexto externo e interno de la organización, las políticas de gestión documental y las políticas de seguridad respecto a la información electrónica. Este modelo de gestión de riesgos debe incluir los principios, el marco de referencia y los procesos de la norma ISO 31000.

Además, el compromiso de la alta dirección y de los órganos de supervisión es fundamental en el éxito de la implantación de la gestión de riesgos. Teniendo en cuenta que, según la norma ISO 31000, el comportamiento humano y la cultura de la organización tiene un gran peso en la gestión de riesgos, se recomienda llevar a cabo programas de formación sobre gestión documental para el personal de la organización.

También se considera imprescindible la presencia de un profesional de la gestión documental o archivero desde el inicio del ciclo de vida del documento (esto es, desde el diseño de la aplicación), en el que pueda definir desde la creación de los documentos los metadatos necesarios para garantizar su posterior

recuperación. Asimismo, identificar y gestionar los riesgos relacionados con la gestión de documentos debería ser responsabilidad del profesional de la gestión de estos.

Bibliografía

Asociación Española de Normalización y Certificación. (2011). Gestión del riesgo. Técnicas de apreciación del riesgo (UNE-ISO 31010:2011).

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

Asociación Española de Normalización y Certificación. (2015). Gestión del riesgo. Orientación para la implementación de la Norma ISO 31000 (UNE-ISO/TR 31004:2015).

Asociación Española de Normalización y Certificación. (2018). Gestión del riesgo. Directrices (UNE- ISO 31000:2018).

Asociación Española de Normalización y Certificación. (2019). Información y documentación. Sistemas de gestión para los documentos. Requisitos. (UNE-ISO 30301:2019).

BEARMAN, David (2007). "Moments of Risk: Identifying Threats to Electronic Records". *Archivaria*. n. 62, p. 15-46. <https://archivaria.ca/index.php/archivaria/article/view/12912/14148>. [Consulta: 30/07/2021]

Bustelo Ruesta, C. (15 abril, 2014). "Nuevo informe técnico: ISO 18128. Apreciación del riesgo para procesos y sistemas de gestión documental". [Artículo en un blog]. <http://www.carlotabustelo.com/index.php?option=com_content&view=article&id=225%3A2014-05-30-18-03-31&catid=53%3Anoticias-iso&Itemid=56&lang=es>. [Consulta: 27/05/2021].

CASADESÚS DE MINGO, Anahí. (2016). "Gestión de riesgos aplicada a la gestión de documentos: una metodología para garantizar una rendición de cuentas confiable". Transparencia "versus" corrupción, os arquivos e a democracia: actas das I Xornadas "Olga Gallego" de Arquivos, A Coruña, 2 e 3 outubro 2015, pp. 161-182. <http://fundacionolgagallego.gal/upload/recursos/cat_2/44/transparencia_1_olga gallego_def.pdf> [Consulta: 30/07/2021]

CASADESÚS DE MINGO, Anahí. (2017). "La normalización en gestión documental más allá de los clásicos". *Consultor de los ayuntamientos y de los juzgados: Revista técnica especializada en administración local y justicia municipal*, n. 7, p. 959-968. <https://www.researchgate.net/publication/316829306_La_normalizacion_en_gestion_documental_mas_alla_de_los_clasicos>. [Consulta: 30/07/2021]

CASADESÚS DE MINGO, Anahí. (2018). La gestión del riesgo aplicada a la gestión de documentos y su impacto en la rendición de cuentas pública (Tesis doctoral, Universitat Autònoma de Barcelona). <http://www.tdx.cat/handle/10803/665386>. [Consulta: 30/07/2021]

GARCÍA ALSINA, Montserrat. (2012). "Gestión de riesgos y de documentos: tener o no tener". *Revista de los Estudios de Ciencias de la Información y de la Comunicación*. n. 9.

<https://www.uoc.edu/divulgacio/comein/es/numero09/articles/Article-montsegarcia.html>. [Consulta: 30/07/2021]

GARCÍA-MORALES, Elisa. (2013). *Gestión de documentos en la e-administración*. Barcelona: UOC.

GARCÍA-MORALES, Elisa. (2016). "Riesgos y seguridad de la información: convergencias desde la gestión documental". *Anuario ThinkEPI. n* 10. <https://recyt.fecyt.es/index.php/ThinkEPI/article/view/thinkepi.2016.27>. [Consulta: 30/07/2021]

GELLERT, Raphaël. (2015). "Data protection: a risk regulation? Between the risk management of everything and the precautionary alternative". *International Data Privacy Law*, n. 5, p. 3-19. <http://dx.doi.org/10.1093/idpl/ipu035> [Consulta: 30/07/2021]

HAY-GIBSON, N. (2011). "Risk and Records Management: Investigating Risk and Risk Management in the Context of Records and Information Management in the Electronic Environment". (Tesis doctoral, Northumbria University). <http://nrl.northumbria.ac.uk/3308/2/hay-gibson.naomi_phd.pdf>. [Consulta: 30/07/2021]

Lahoz, A. y Gabás, L.M. (29 mayo, 2019). "Un fallo en el sistema informático de la DGA bloquea sus servicios todo un día". El Periódico de Aragón. <https://www.elperiodicodearagon.com/noticias/aragon/fallo-sistema-informatico-dga-bloquea-sus-servicios-todo-dia_1365684.html>. [Consulta: 30/07/2021]

LEMIEUX, Victoria. (2001). *Competitive viability, accountability and record keeping: a theoretical and empirical exploration using a case study of Jamaican Commercial Bank Failures*. (Tesis doctoral, University College London). <http://discovery.ucl.ac.uk/1317703/1/272289.pdf> [Consulta: 30/07/2021]

LEMIEUX, Victoria. (2004). "Two approaches to managing information risks". *The Information Management Journal*. n. 38, p. 56-62. <https://studylib.net/doc/8735581/two-approaches-to-managing-information-risks>. [Consulta: 30/07/2021]

LEMIEUX, Victoria. (2010). "The records-risk nexus: Exploring the relationship between records and risk". *Records Management Journal*. n. 20, p. 199-216. <https://www.researchgate.net/publication/235296430_The_records-risk_nexus_Exploring_the_relationship_between_records_and_risk> . [Consulta: 30/07/2021]

MCDONALD, John. (1995). "Managing records in the modern office: Taming the wild frontier". *Archivaria*, n. 39. <https://archivaria.ca/index.php/archivaria/article/view/12069> . [Consulta: 30/07/2021]

MCDONALD, John. (2005). "The wild frontier ten years on". En: McLeod, Julie y Hare, Catherine (eds). *Managing Electronic Records*. London: Facet. p.1-17. <http://www.interpares.org/display_file.cfm?doc=ip1-2_dissemination_bc_mcdonald_mer_2005.pdf>. [Consulta: 30/07/2021]

MCKEMMISH, Sue. (Septiembre, 1998). "The smoking gun: recordkeeping and accountability". 22nd Annual Conference of the Archives and Records Association of New Zealand: "Records and Archives Now - Who Cares? Dunedin. <https://bridges.monash.edu/articles/conference_contribution/The_smoking_gun_recordkeeping_and_accountability/4037394>. [Consulta: 30/07/2021]

MENA MUGICA, Mayra Marta y DEL CASTILLO GUEVARA, Jorge. (2018a). "Integración de los enfoques de gestión documental y gestión de riesgos para el tratamiento de la información como evidencia de actos y transacciones organizacionales". *Revista Cubana de Información en Ciencias de la Salud*. n 29. <http://scielo.sld.cu/pdf/ics/v29n2/a07_1213.pdf>. [Consulta: 30/07/2021]

MENA MUGICA, Mayra Marta y DEL CASTILLO GUEVARA, Jorge. (2018b). "Integración de los enfoques de Gestión Documental y Gestión de Riesgos para la identificación y mitigación de riesgos derivados de la información como evidencia de actos y transacciones organizacionales". Congreso Internacional de Información Info´2018. Información y conocimiento: desafíos para el desarrollo sostenible. <https://cutt.ly/Uniedxg>. [Consulta: 30/07/2021]

POPESCU, Maria y HELEREA, Elena. (2012). "Implementation of Risk Management in University Libraries". Proceedings of the International Conference on Innovation within Libraries (BIBLIO), Brasov, p. 73-78.

Villanueva Fernández, Marta. (2015). "La certificación y la gestión de riesgos". *Revista Economía Industrial*, n. 396, p. 73-80. <https://www.mincotur.gob.es/Publicaciones/Publicacionesperiodicas/EconomiaIndustrial/RevistaEconomiaIndustrial/396/VILLANUEVA%20FERN%C3%81NDEZ.pdf>. [Consulta: 30/07/2021]

World Economic Forum. (2019). "The Global Risks Report 2019. 14th Edition". <http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf> [Consulta: 27/05/2021]

Notas

[1] La actualización de la norma ISO 31000 del año 2010 al año 2018 llevó consigo el cambio de "apreciación del riesgo" a "evaluación del riesgo". El informe técnico ISO/TR 18128:2014 todavía mantiene la palabra "apreciación".