Identificación de riesgos en la producción, gestión y mantenimiento de documentos electrónicos

Carlota Bustelo Ruesta

PID_00202503

UOC
Universitat Oberta de Catalunya

Índice

Introducción..... 5

Objetivos..... 6

1. Gestión de riesgos y gestión de documentos..... 7

2. Políticas de gestión de riesgos en las organizaciones..... 9
2.1. Principios de gestión de riesgos 10
2.2. Estructura de soporte 11
2.3. Proceso 11
2.4. Implicaciones de la política de gestión de riesgos en la gestión de documentos 14

3. Riesgos de la no creación de documentos adecuados..... 15

4. Riesgos de la gestión de documentos y sistemas de gestión documental..... 16
4.1. Contexto: factores externos 17
4.2. Contexto: factores internos 18
4.3. Sistemas 20
4.4. Procesos de gestión documental 22

Bibliografía..... 25

Introducción

En este módulo describimos una metodología para identificar, evaluar y gestionar los riesgos de forma que pueda ayudarnos a realizar planteamientos convincentes para la implantación de modelos de gestión documental.

En primer lugar presentamos el nexo entre gestión de riesgos y gestión de documentos. A continuación exponemos los elementos que componen las políticas de gestión de riesgos en las organizaciones, y algunas metodologías para abordar los procesos inherentes. En tercer lugar, se analizan los riesgos que conlleva la falta de ciertos documentos atendiendo al entorno legal y regulatorio. Por último, se detallan los focos de riesgo en las organizaciones, a partir de los cuales se puede proceder a identificar los riesgos potenciales en torno a los documentos.

Objetivos

1. Aprender cómo alinear la gestión de documentos con la gestión de riesgos.

2. Saber diseñar políticas de gestión de riesgos en una organización.

1. Gestión de riesgos y gestión de documentos

La práctica de la gestión de riesgos y la gestión de documentos han sido siempre campos completamente separados, tanto en la investigación y el mundo académico como en la práctica de las organizaciones.

Las pocas prácticas conocidas que unen los dos campos (gestión de riesgos y gestión de documentos) se centran sobre todo en los documentos electrónicos y en los riesgos de los sistemas de información que los gestionan. Es el caso de la **metodología DRAMBORA** (http://www.repositoryaudit.eu/) para evaluar los riesgos de los repositorios digitales.

Ejemplo

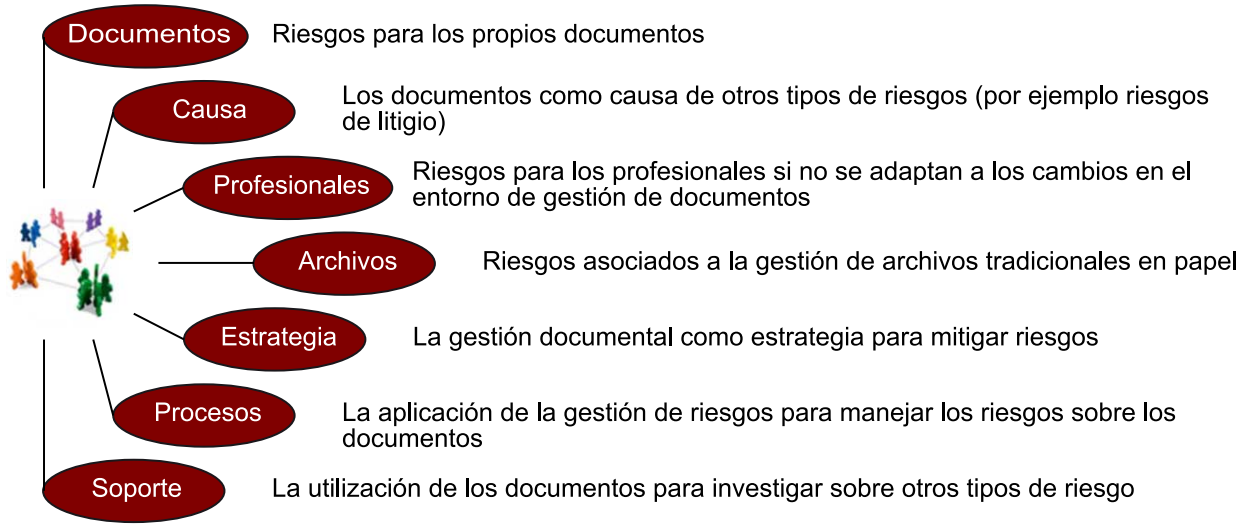
Un ejemplo del concepto de riesgos entre los profesionales de la documentación es un pequeño experimento que se hizo en el entorno del Subcomité Técnico ISO TC46/SC11-Archives/Records Management, con una pequeña muestra de profesionales de la gestión de documentos, preguntándoles que entendían por riesgos en la gestión de documentos. Esto se hizo con motivo de la propuesta de creación de algún tipo de norma sobre el tema de la gestión de riesgos y la gestión documental. La respuesta más común era que asociaba la gestión de riesgos con la "planificación ante posibles desastres" típica de la gestión de archivos en papel, seguida de la identificación de los temas de riesgos con cuestiones informáticas de los departamentos TIC, en las que los riesgos se identifican con la seguridad de la información.

Victoria L. Lemieux (2010) hace un repaso de la bibliografía existente sobre riesgos, donde constata la existencia de diferentes categorías de estos, según autores y sectores: riesgos estratégicos, del entorno, de mercado, operativos, de cumplimiento, riesgos administrativos, de control de documentos, riesgos legales, y riesgos tecnológicos. Al final de su estudio concluye que existen al menos siete tipos de nexos distintos entre documentos y riesgos, procedentes tanto de la existencia o ausencia de documentos como de aspectos que rodean a la gestión documental (figura 1).

Lectura complementaria

Victoria L. Lemieux (2010). "The records-risk nexus: exploring the relationship between records and risk". *Records Management Journal* (vol. 20, núm. 2, pág. 199-216).

Figura 1. Nexo entre riesgo y documentos



Fuente: Traducida y adaptada de Lemieux, 2010.

Actividad

A la hora de establecer la práctica de la gestión de riesgos en relación con la gestión de documentos, no existe una metodología clara para incluir la gestión de riesgos en los procesos y controles documentales.

Después de la lectura del artículo, ¿cuál de las aproximaciones utilizadas os parece más interesante para la alineación de la gestión de riesgos y la gestión documental?

Lectura de Victoria L. Lemieux (2010). "The records-risk nexus: exploring the relationship between records and risk". *Records Management Journal* (vol. 20, núm. 2, pág. 199-216).

2. Políticas de gestión de riesgos en las organizaciones

En un principio, todos tendemos a identificar el concepto de riesgo con el de amenaza. En este sentido, entendemos que todas las actividades de una organización pueden estar sometidas a una serie de amenazas que pueden hacerlas vulnerables. Algunas de las cosas que nos vienen a la mente son accidentes operacionales, enfermedades, incendios u otras catástrofes naturales, etc.

Tradicionalmente, las organizaciones trataron estos riesgos/amenaza mediante estrategias de reacción y soluciones puntuales. Pero a partir de la década de los años noventa del siglo XX, se empieza a imponer el concepto de gestión integral de riesgos, que tiene como base dos principios:

- La ampliación del concepto de riesgo hasta definirlo como "efecto de incertidumbre sobre los objetivos". El efecto puede ser positivo, negativo o una desviación sobre lo esperado.

- El acuerdo generalizado de que los elementos que conforman los riesgos y los factores que determinan el impacto de sus consecuencias son los mismos que intervienen para todos. Por lo tanto, se puede utilizar una misma metodología y estrategia para gestionar cualquier tipo de riesgo.

El modelo de gestión de riesgos generalista se ha plasmado en la norma ISO 31000:2009, si bien hay otros modelos de carácter más específico como COSO ERM (Internal Control - Integrated Framework, del Committee of Sponsoring Organizations en USA) o OHSAS de prevención de riesgos laborales.

Lectura recomendada

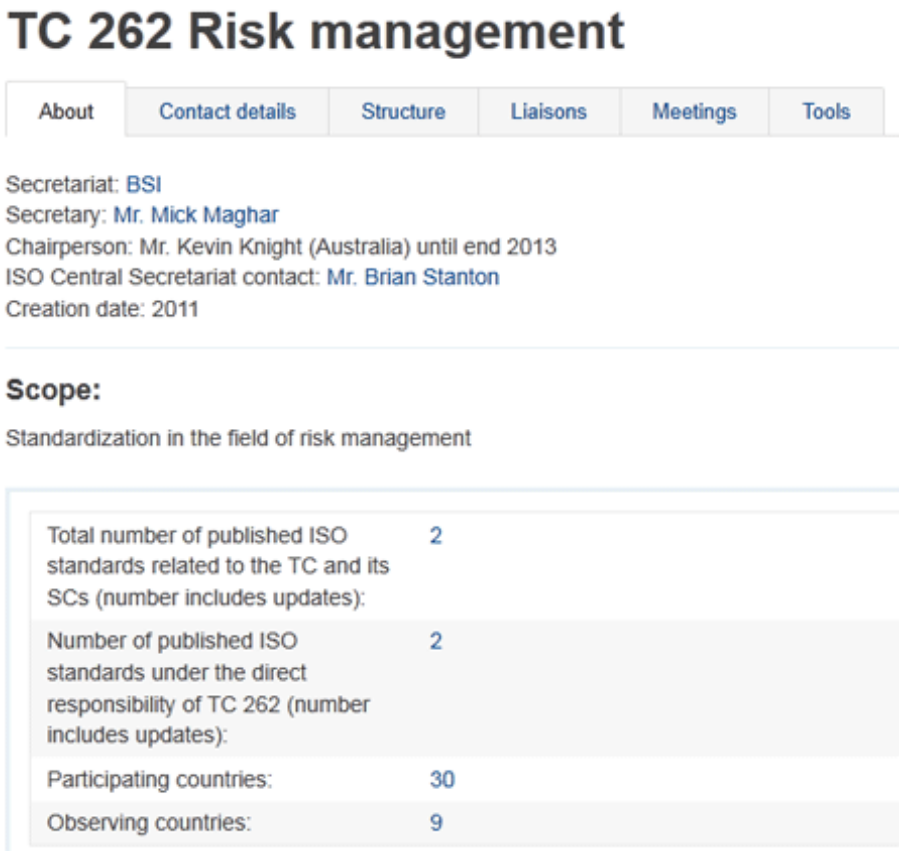
"Además de las propias normas ISO existen algunas guías o manuales sobre la gestión de riesgos que pueden descargarse gratuitamente de Internet. Se recomiendan la guía *A structured approach to Enterprise Risk Management (ERM) and the requirements of ISO 31000*, publicada por AIRMIC, ALARM e IRM, asociaciones integradas en FERMA, Federation of European Risk Management Associations, y que se publica en su web http://www.ferma.eu/wp-content/uploads/2011/10/a-structured-approach-to-erm.pdf"

ISO 31000:2009 Risk management - Principles and guidelines (UNE-ISO 31000:2010, Gestión del riesgo. Principios y directrices).

Podemos tomar como base para el diseño de políticas de gestión de riesgos la norma ISO 31000 porque es fruto del consenso de expertos del ámbito de los distintos países que componen el TC 262. Esta norma trata tres elementos de la gestión de riesgos:

- Los principios de la gestión de riesgos.
- La estructura de soporte.
- El proceso de gestión de riesgos.

Figura 2. Detalle de la composición del Comité Técnico 262 de Gestión de Riesgos



Fuente: http://www.iso.org

2.1. Principios de gestión de riesgos

Con relación al primer elemento, la ISO 31000 detalla los siguientes principios de la gestión de riesgos:

- Crea valor. Contribuye a la consecución de objetivos así como a la mejora de aspectos tales como la seguridad y salud laboral, cumplimiento legal y normativo, protección ambiental, etc.

- Está integrada en los procesos de una organización. No debe ser entendida como una actividad aislada, sino como parte de las actividades y procesos principales de una organización.

- Forma parte de la toma de decisiones. La gestión del riesgo ayuda a la toma de decisiones evaluando la información sobre las distintas alternativas.

- Trata explícitamente la incertidumbre. La gestión del riesgo trata aquellos aspectos de la toma de decisiones que son inciertos, la naturaleza de esa incertidumbre y cómo puede tratarse.

- Es sistemática, estructurada y adecuada. Contribuye a la eficiencia y, consecuentemente, a la obtención de resultados fiables.

- Está basada en la mejor información disponible. Los *inputs* del proceso de gestión del riesgo están basados en fuentes de información como la experiencia, la observación, las previsiones y la opinión de expertos.

- Está hecha a medida. La gestión del riesgo está alineada con el contexto externo e interno de la organización y con su perfil de riesgo.

- Tiene en cuenta factores humanos y culturales. Reconoce la capacidad, percepción e intenciones de la gente, tanto externa como interna, que puede facilitar o dificultar la consecución de los objetivos de la organización.

- Es transparente e inclusiva. La apropiada y oportuna participación de las partes interesadas (*stakeholders*) y, en particular, de los responsables a todos los niveles, asegura que la gestión del riesgo permanece relevante y actualizada.

- Es dinámica, iterativa y sensible al cambio. La organización debe velar para que la gestión del riesgo detecte y responda a los cambios de la empresa.

- Facilita la mejora continua de la organización. Las organizaciones deberían desarrollar e implementar estrategias para mejorar continuamente, tanto en la gestión del riesgo como en cualquier otro aspecto de la organización.

2.2. Estructura de soporte

Con relación al segundo elemento, la estructura de soporte, la ISO 31000 describe un marco o infraestructura para implementar la gestión de riesgos y el proceso en que se soporta. Cada organización debe adaptarlo a sus necesidades, objetivos concretos, contexto, estructura, operaciones, procesos operativos, proyectos, servicios, etc.

En algunos sectores, la función de gestión de riesgos ha sido potenciada en las organizaciones hasta crearse unidades específicas que asumen estas funciones. En el sector financiero estos departamentos son altamente poderosos, pero normalmente lidian solo con los riesgos financieros, que están en el corazón del negocio bancario. En otras organizaciones se ha ampliado la gestión de riesgos a los riesgos operativos, o se han asociado a los riesgos de incumplimiento legal. En otros casos, la gestión de riesgos se identifica exclusivamente con los departamentos TIC y la seguridad de la información.

2.3. Proceso

El último elemento de gestión de riesgos lo constituye el conjunto de actividades que engloba el proceso de gestión de riesgos. Dicho proceso lo describimos siguiendo la norma ISO 31000 y la ISO 31010:2009.

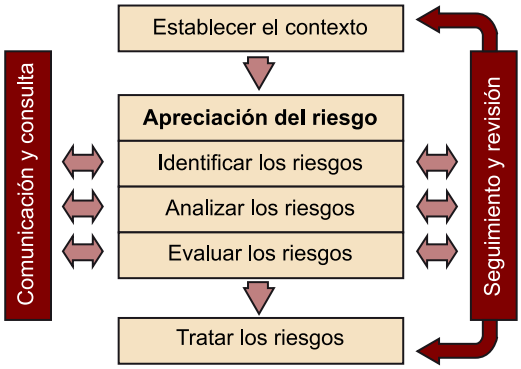
Lecturas recomendadas

La norma ISO 31000 se complementa con la norma ISO 31010:2009, Risk management. Risk assessment techniques, que describe una serie de posible técnicas que pueden ser utilizadas en el contexto del proceso de gestión de riesgos propuestos.

La norma ISO 31010:2009 ha sido traducida y adaptada como norma UNE-EN 31010:2011, Gestión del riesgo. Técnicas de apreciación del riesgo.

El proceso de gestión de riesgos tiene una parte significativa que en español se ha traducido en la versión UNE como **apreciación del riesgo** (en inglés *risk assesment*). Esta apreciación tiene a su vez tres fases: la Identificación, el Análisis y la Evaluación (figura 3).

Figura 3. Esquema de proceso de gestión de riesgos en la ISO 31000



Fuente: UNE-ISO 31000.

El riesgo se identifica con un evento o un cambio en las circunstancias sobre la que se analizan las posibles consecuencias y se evalúa de acuerdo con la probabilidad de que ocurra y la gravedad de sus efectos.

1) Identificación

La identificación de riesgos es el proceso de encontrar, reconocer y registrar los posibles eventos o situaciones que puedan suceder y que afecten a la consecución de los objetivos propuestos.

2) Análisis

El análisis de los riesgos incluye identificar las causas y las fuentes de los riesgos, así como los controles existentes para que no se produzcan.

Cuando se identifican los riesgos lo normal es que se clasifiquen en distintos tipos, si bien no existe una clasificación universalmente aceptada o recomendada por la normas ISO 31000. En cada organización se habrá definido una serie de criterios para evaluar los riesgos, en los que es normal que aparezca el componente de la probabilidad de que el hecho suceda. Los criterios pueden ir desde una simple lista de impacto: alto, medio, bajo a complicadas fórmulas de probabilidad dependiendo de la complejidad, estructura, sector y tamaño de la organización.

3) Evaluar

Los métodos de apreciación de riesgos pueden incluir:

- Métodos basados en la evidencia, como listas de verificación o análisis de datos históricos.

- Equipos de expertos que siguen de forma sistemática un proceso para identificar riesgos mediante un conjunto adecuado de verificaciones y preguntas.

- Técnicas inductivas de razonamiento, como *HAZOP* (*hazard and operability study*).

Otras técnicas de soporte se usan en la apreciación del riesgo incluyendo la lluvia o tormenta de ideas (*brainstorming*) o la metodología DELPHI (de pronósticos y predicciones).

Ejemplo de ficha para registro de riesgos

Category	Description
Risk name	Hardware inaccesible
Risk context	Fallo del hardware y los dispositivos de almacenamiento
Asset type	Sistemas
Risk description	Los dispositivos de almacenamiento donde se encuentran almacenados documentos de conservación permanente no permiten el acceso a la misma cuando se trata de recuperar
Risk impact description	Discontinuidad de servicio de acceso y posible pérdida de información
Risk stakeholder	Departamento de Sistemas
Risk relationships	Relacionado con la obsolescencia del hardware

4) Tratar los riesgos

Una vez que los riesgos han sido evaluados deben establecerse las medidas oportunas para mitigarlos. Estas medidas deben estar en consonancia con la capacidad de la organización y normalmente se aplican a una parte de los riesgos detectados en el proceso de identificación.

2.4. Implicaciones de la política de gestión de riesgos en la gestión de documentos

A la hora de implantar un modelo de gestión de documentos electrónicos es imprescindible saber si en la organización existe algún tipo de procesos de gestión de riesgos, un registro de riesgos o un sistema preventivo, pues de ser así deberíamos tenerlo en cuenta para alinear las estrategias.

En caso de existir un proceso para gestionar riesgos, es conveniente incorporar el componente de gestión de riesgos en el diseño del modelo de gestión documental, ya que dicha integración ayudará a alinear el modelo de gestión documental con los objetivos de la organización.

3. Riesgos de la no creación de documentos adecuados

En general, la creación de los documentos o la información adecuada para soportar las acciones y decisiones de las organizaciones del siglo XXI es una de las áreas de incertidumbre, y por lo tanto, generadora de posibles riesgos.

En el mundo del exceso de información es normal que cuando una organización necesite la evidencia de una acción, dicha evidencia falte o la organización sea incapaz de encontrarla, que es prácticamente lo mismo.

En los casos más graves esto puede producir riesgos legales, ya que no permite aportar pruebas en caso de litigio. En las culturas anglosajonas esta preocupación ha ido tan lejos, que se ha establecido el concepto de *e-discovery*, que se incluye en alguna de las funcionalidades de los sistemas de gestión de contenidos (ECM) que se comercializan en el mercado. *Discovery* se refiere en inglés a la fase de recopilación y aportación de pruebas en un juicio. Cuando se le incluye la *e* delante indica que las pruebas que se van a presentar están en formato electrónico y se requieren una serie de condiciones para que sean aceptadas como tal.

Pero sin llegar a tales extremos, la no creación de las evidencias y documentos de las acciones y decisiones que se toman pueden producir riesgos en la conducción de la propia operativa de las organizaciones, y sin duda, riesgos relacionados con la pérdida del conocimiento de la organización.

En este sentido, podemos concluir que la principal justificación de la creación y control de los documentos en las organizaciones es evitar los riesgos de todo tipo que supone perder la evidencia de las actividades realizadas.

Siguiendo con esta línea argumental, también es fácil observar que muchas de las acciones que se proponen para mitigar riesgos de todo tipo se basan en la creación de documentos y el control de la información. Estos documentos y controles permiten establecer sistemas de alerta y documentar las distintas acciones que se han llevado a cabo.

Algunos especialistas incluso han llegado a decir que toda la gestión de documentos es un sistema de prevención de riesgos. La implantación de un modelo de gestión documental puede verse entonces desde la perspectiva estratégica de acciones para mitigar riesgos de negocio.

4. Riesgos de la gestión de documentos y sistemas de gestión documental

Existe otro nivel de gestión de riesgos que presupone que la organización crea y gestiona documentos de sus actividades y proceso de negocio, y que se centra en el nivel operativo de los propios procesos documentales y de los sistemas donde se crean y gestionan.

En este nivel estamos tratando los riesgos que puede sufrir la organización si los documentos dejan de ser auténticos, fiables, y si los documentos no se mantienen íntegros y usables todo el tiempo que se necesiten.

La idea es aplicar los procesos de la gestión de riesgos, reconocidos y asentados en el campo de la gestión desde hace bastante tiempo, para identificar y evaluar los riesgos asociados a la gestión de los documentos y la información.

La identificación y evaluación de riesgos en el ámbito de la gestión de documentos se postula como una responsabilidad de los profesionales de la gestión de documentos. Así se desprende del borrador del informe técnico ISO PDTR 18028, Information and documentation - Risk assessment for records processes and Systems, cuya publicación puede esperarse para finales del 2012, principios del 2013. Estos profesionales proporcionarían sus hallazgos a los responsables de la gestión de riesgos de la organización, que serían los encargados de incluir esta visión en el programa general de gestión de riesgos.

Se ha realizado un gran esfuerzo por tratar de construir instrumentos útiles para la práctica de la gestión documental, recogiéndose distintas aportaciones de autores que han intentado realizar modelos de gestión de riesgos. A partir de la información recopilada se han intentado establecer cuáles son las posibles **áreas de incertidumbre** en las que pueden producirse riesgos que afecten a las características de los documentos, o cuál es la forma en que estos se gestionan, por si se pudiera incurrir en algún riesgo que vulnere las características de los documentos (autenticidad, fiabilidad, integridad y disponibilidad). Estas áreas de incertidumbre se han clasificado en distintos dominios, estableciéndose las siguientes categorías:

- Contexto externo
- Contexto interno
- Sistemas y procesos de gestión documental

Para cada una de esas categorías se han clasificados las posibles áreas de incertidumbre como una guía de donde se pueden encontrar las fuentes de posibles riesgos en cada organización. Evidentemente, esto no quiere decir que todas

las organizaciones tengan que encontrar riesgos en todas las áreas de incertidumbre listadas. Algunas áreas de incertidumbre se repiten en diferentes tablas pues pueden abordarse desde distintos enfoques.

4.1. Contexto: factores externos

Los factores externos son áreas de incertidumbre que provienen de ámbitos fuera del control de la organización, pero que afectan a los documentos y los sistemas donde se crean y gestionan.

El factor más importante es el **entorno legal y regulatorio** de obligado cumplimiento para las organizaciones, y que constituye el marco en el que las organizaciones deben gestionar sus documentos para que estos puedan contribuir a cumplir con los requisitos legales. Otros factores son el **entorno cultural**, el **entorno macroeconómico nacional o regional**, el **entorno físico** o las amenazas de seguridad en general. Mientras el factor legal y regulatorio, el cultural y el macroeconómico tienen más consecuencias en las políticas y prácticas de cómo se gestionan los documentos, el entorno físico y las amenazas de seguridad tienen más impacto en los sistemas que crean y gestionan documentos, y por lo tanto, están más relacionados con la áreas de incertidumbre agrupadas bajo sistemas.

Ved también

Ver el apartado "Procesos de gestión documental".

Ámbito	Áreas de incertidumbre
Requisitos legales y regulatorios	Cambios en la legislación que afecten a los documentos y a los sistemas que los gestionan
	Cambios en las políticas gubernamentales que afecten a los documentos y a los sistemas que los gestionan
	Nuevas normas o códigos de buenas prácticas que afecten a los documentos y a los sistemas que los gestionan
Cambios en el contexto cultural	Cambio en el clima social y cultural que cambie las actitudes con respecto a la gestión de la información (p. ej., privacidad, derechos de propiedad, o la propiedad de la propia organización)
	Demanda cambiante en los servicios documentales y cambios en las expectativas de los usuarios de los documentos
	Pérdida de reputación o confianza en la habilidad de la organización para proporcionar sus servicios
Entorno macro económico- nacional o regional	Cambio inesperados en la financiación de la organización que afectan al presupuesto para gestionar los documentos
	Cambios en la gestión de prioridades que afectan al presupuesto para gestionar los documentos

Ámbito	Áreas de incertidumbre
	Cambios en la política de personal de la organización que pueden afectar al personal que gestiona los documentos
	Cambios en las soluciones tecnológicas disponibles en la organización que pueden afectar a la gestión de los documentos
	Cambios en el presupuesto de formación y oportunidades que afectan a la capacidad del personal que gestiona documentos
Entorno físico e infraestructura	Grandes desastres naturales o producidos por el hombre que pueden afectar a la pérdida de información
	Fenómenos destructivos medioambientales locales (terremotos, huracanes/ciclones, tsunamis, inundaciones, etc.) que pueden causar daños en los sistemas de información que gestionan los documentos
	Interrupción del suministro de electricidad o otras utilidades principales en la organización
	Planes de recuperación de desastres no probados pueden llevar a la pérdida de información en caso de que se produzca
Amenazas de seguridad externas	Intrusiones no autorizadas a los sistemas de gestión de documentos que llevan a que la información sea alterada o accedida de forma inapropiada
	Vulnerabilidades no identificadas que comprometen la seguridad y que pueden llevar a la degradación de la información (por ej. malware, software espía, parches de seguridad no instalados, etc.)
	Intrusión física en el espacio de almacenamiento de los documentos (depósitos o hardware)
	Ataque ciberterrorista
	Vandalismo físico
	Pérdida del servicio de terceros donde los documentos son gestionados

4.2. Contexto: factores internos

El entorno económico, tecnológico y estructural de las organizaciones cambia y evoluciona para adaptarse a las circunstancias y dar respuesta a las demandas de las distintas partes interesadas. Estos cambios pueden producir áreas de incertidumbre con respecto a los documentos y los sistemas que los gestionan.

Los cambios organizativos y tecnológicos tienen un efecto inmediato en la gestión de los documentos, así como las circunstancias que afecten a los recursos materiales y humanos disponibles en las organizaciones. La tabla siguiente recoge los riesgos identificados.

Ámbito	Áreas de incertidumbre
Cambio organizativo	Decisiones de la alta dirección en fusiones y adquisiciones, reestructuraciones, reducciones, externalización, uso de la nube, etc., que afectan al plan de gestión de documentos (por ejemplo, a la propiedad de los documentos)
	Nuevas políticas internas que modifican el plan de gestión de documentos
	Ausencia o pérdida de conocimiento de que documentos heredados existen y de los procedimientos para recuperarlos y utilizarlos en un cambio organizativo
	Cambio de condiciones en los contratos con terceras partes
	Políticas y procedimientos que no han sido revisados y actualizados y que son ineficientes, inconsistentes o contradictorios con el cambio organizativo.
	Falsa percepción de éxito
Cambio tecnológico	Introducción de nuevas tecnologías y sistemas con problemas de compatibilidad con las plataformas y sistemas anteriores y que suponen la migración de documentos y metadatos. La trasferencia de los controles de acceso, etc.
	Cambios tecnológicos que afectan a la interoperabilidad entre sistemas que crean, guardan o gestionan documentos
	La capacidad de las políticas existentes para cubrir nuevas tecnologías que la organización adopte (p. ej., medios sociales, RFID, GPS, etc.)
	Infraestructura técnica que es incapaz de cumplir los nuevos requisitos resultantes de la evolución natural del plan de gestión de documentos
Recursos: Personal y capacidades	Suficiencia de recursos humanos para crear y controlar documentos y para diseñar y mantener los sistemas de gestión de documentos
	La concienciación del personal en las políticas y procesos de gestión documental
	Suficiencia del compromiso de la alta dirección para apoyar la política de gestión de documentos
	Concienciación en la alta dirección de los riesgos relativos a los documentos y la habilidad de tomar decisiones apropiadas para mitigarlas

Ámbito	Áreas de incertidumbre
	Separación clara de roles administrativos y roles operacionales en las aplicaciones de gestión documental (*front office* separado del *back office*)
	Suficiencia de las capacidades del personal para crear y controlar documentos
	Pérdida de personal clave con habilidades vitales, conocimiento en profundidad de la organización y de la historia corporativa no documentada
	El nivel de habilidades del personal se estanca, deteriora o se convierte en obsoleto
	Incapacidad para evaluar la efectividad o idoneidad del personal
Recursos: Financieros y materiales	Recursos financieros suficientes para cumplir con las metas y compromisos del plan de gestión de documentos
	Suficiencia de los recursos financieros para comprar, actualizar y mantener los sistemas o aplicaciones adecuadas

4.3. Sistemas

En la gestión de los documentos electrónicos los sistemas de información o aplicaciones informáticas que los gestionan son la fuente de varias áreas de incertidumbre en las que se pueden generar riesgos para el mantenimiento de características de los documentos. Muchas de las posibles áreas de incertidumbre no son específicas de los sistemas de gestión documental sino que son comunes a todos los sistemas de información de la organización.

En muchas organizaciones la identificación de riesgos relacionados con los sistemas de información se realiza desde la perspectiva de la seguridad de la información. En muchos casos los riesgos no difieren vistos desde la óptica de la gestión de documentos, pero sí pueden tener una perspectiva más amplia.

Por lo tanto, es normal que algunas de las áreas de incertidumbre descritas en la siguiente tabla y los riesgos que de ellas puedan derivarse sean mitigables con los controles propuestos por las metodologías de seguridad de la información, como por ejemplo la ISO 27001.

Ámbito	Áreas de incertidumbre
Mantenimiento	Cambios frecuentes en el diseño de los sistemas
	El nivel de habilidades de los administradores de sistemas para entender los requerimientos de la gestión documental

Ámbito	Áreas de incertidumbre
	Fiabilidad de los proveedores informáticos y su capacidad para mantener los sistemas al día
	Nivel de documentación existente para los sistemas que crean y gestionan documentos
	Existencia y aplicación efectiva de procedimientos de salvaguardia adecuados y documentados para los sistemas que gestionan documentos
Sostenibilidad y continuidad	Mantenimiento regular de los sistemas de gestión de documentos para que estén en línea con los requisitos documentales de la organización y los desarrollos de la tecnología
	Pruebas de la exhaustividad de los procesos de salvaguardia
	Actualización y pruebas de los procesos de restauración de las salvaguardias
	Existencia de documentación y especificaciones del sistema de forma accesible
	Existencia de procedimientos documentados para el mantenimiento operativo
	Decisiones de implementación documentadas, mantenidas y accesibles a los usuarios cuando se necesiten
	Habilidad de los sistemas que gestionan documentos para mantener la usabilidad de los mismos
	Seguimiento e información a los responsables de gestión documental del rendimiento de los sistemas de gestión documental con respecto a sus objetivos
	Migración de documentos a nuevos sistemas de gestión debidos a los propios requisitos o a cambios en la tecnología
	Habilidad del sistema de gestión de documentos de controlar las decisiones y acciones sobre destrucción de documentos
	Habilidad del sistema de gestión de documentos para apoyar los planes de continuidad proporcionando acceso en caso de desastre, por ejemplo existiendo un espejo del sistema de gestión de documentos
Interoperabilidad	Identificación de todos los sistemas que crean o gestionan documentos en la organización
	Identificación de los requisitos de interoperabilidad entre los sistemas que crean o gestionan documentos
	Utilización de estándares o normas de interoperabilidad

Ámbito	Áreas de incertidumbre
	Mantenimiento de la consistencia en la recuperación de documentos cuando se ha producido un intercambio entre sistemas
	Mantenimiento de los metadatos y de la capacidad de interpretarlos y aplicarlos cuando se ha producido un intercambio entre sistemas
Economía	Recursos financieros y humanos necesarios para el mantenimiento de los sistemas de gestión de documentos
	Duplicidad de funcionalidades cuando se gestionan los documentos en diferentes sistemas de información
	Diseño apropiado de los sistemas de información que crean y gestionan documentos
Seguridad	Concienciación de la organización de la política de seguridad de la información y como afecta a los documentos y a los sistemas que los gestionan
	Restricciones puestas en práctica y documentadas de los usuarios para acceder, crear y cambiar documentos
	Prácticas de almacenamiento de documentos confidenciales fuera de los sistemas oficiales para gestionar documentos
	Control del trabajo de terceras partes que afecte al almacenamiento, acceso, y procesamiento de documentos o de los sistemas que los gestionan
	Fallos o disfunciones en la tecnología que afecten a: - acceso a los sistemas de gestión documental - pérdida de datos - el funcionamiento de los sistemas - el acceso a los documentos - las condiciones de almacenamiento
	Brechas de seguridad por antiguos empleados descontentos que resultan en pérdida o daño de los documentos que se gestionan en los sistemas

4.4. Procesos de gestión documental

Los propios procesos de gestión documental y cómo se diseñan e implementan puede ser una fuente de riesgos para los propios documentos.

En la siguiente tabla se listan las posibles áreas de incertidumbre que pueden encontrarse tanto en el diseño, como en los procesos de creación y control de los documentos (metadatos, uso, usabilidad y disposición).

Ámbito	Áreas de incertidumbre
Diseño de procesos documentales	Extensión y adecuación del análisis para identificar los documentos que deben crearse
	Identificación exhaustiva de los requisitos de los documentos para cada proceso de negocio incluyendo las necesidades de todas las partes interesadas
	Diseño de la estructura y formato de los documentos para que cumplan con los requisitos
	Denominación, control y localización de los metadatos en relación con el propósito para el que se crean
	Puntos de captura de documentos adecuados (integrados y en el tiempo) para los procesos de negocio y los sistemas de gestión documental
	Tecnología apropiada para ser sostenible en el entorno tecnológico y las circunstancia financieras de la organización
Creación de documentos e implementación de sistemas de gestión documental	Integración de la creación y control de documentos con los procesos de negocio
	Responsabilidades en relación con la creación de documentos y las operaciones propias del negocio.
	La gestión de metadatos a lo largo del tiempo
	La gestión de los accesos
	El soporte a los sistemas de gestión de documentos en caso de interrupción del servicio
Metadatos	Las especificaciones técnicas de metadatos (perfiles de aplicación) para los sistemas de gestión documental
	Mantenimiento de las especificaciones técnicas de metadatos en los sistemas de gestión documental
	Metadatos incluidos en las salvaguardias de los sistemas informáticos
	Metadatos buscables
Uso de documentos y de sistemas de gestión documental	Uso de los documentos por el personal interno
	Uso por el personal externo u otros sistemas
	Como se han confeccionado las tablas de seguridad y acceso
	En la seguridad para controlar el acceso
	Controles de seguridad para impedir la modificación de los documentos
	Controles de acceso embebidos en los metadatos

Ámbito	Áreas de incertidumbre
	Forma de recoger la información sobre quien ha accedido y utilizado los documentos
	Capacidad de recuperar, utilizar e interpretar los documentos en su contexto
Mantener la usabilidad	Uso de métodos de encriptación de los documentos
	Versionado e historial de eventos de los documento
	Mantenimiento de los metadatos a lo largo del tiempo
	Aspectos de obsolescencia del hardware y el software relacionados con los documentos y los sistemas de gestión de documentos
Disposición de documentos	Implementación de la disposición
	Documentación e implementación del proceso de destrucción

Reflexión

En este enfoque, que puede ser válido para muchas organizaciones, pueden surgir al menos dos dudas importantes:

- En qué momento se debe producir la identificación y evaluación de los riesgos y cómo incluirlas en los procesos y controles documentales. ¿Es una tarea previa a la implantación de un programa o sistema de gestión de documentos? ¿Es una tarea que se realiza en la auditoría de un programa o sistema ya implantado? ¿Es una tarea rutinaria que debería formar parte de los procesos documentales?

- ¿Cómo encontrar utilidad y aplicación práctica a la identificación y evaluación de riegos relacionados con los documentos, si en la organización no existe un programa reconocido de gestión de riesgos? Si la organización no tiene un programa de gestión de riesgos, ¿merece la pena identificar los riesgos asociados a los documentos? ¿Puede esta identificación y evaluación ayudarnos en el diseño de los procesos documentales?

Bibliografía

AIRMIC, ALARM e IRM (2011). *A structured approach to Enterprise Risk Management (ERM) and the requirements of ISO 31000*. Disponible en línea: http://www.ferma.eu/wp-content/uploads/2011/10/a-structured-approach-to-erm.pdf.

Cowan, J. (2000). "Clinical governance and clinical documentation: still a long way to go?". *British Journal of Clinical Governance* (vol. 5, núm. 3, págs. 179-182).

Cowan, J. (2003). "Risk management, records and the Laming Report". *Clinical Governance: An International Journal* (vol. 8, núm. 3, págs. 271-277).

Egbuji, A. (1999). "Risk management of organisational records". *Records Management Journal* (vol. 9, núm. 2, págs. 93-116).

Groene, O.; Jorgensen, S. J.; Fugleholm, A. M.; Møller, L.; García-Barbero, M. (2005). "Standards for health promotion in hospitals: development and pilot test in nine European countries". *International Journal of Health Care Quality Assurance* (vol. 18, núm. 4, págs. 300-307).

ISO 31000:2009. Risk management - Principles and guidelines (UNE-ISO 31000:2010, Gestión del riesgo. Principios y directrices).

ISO/IEC 31010:2009. Risk management - Risk assessment techniques.

Kolber, M.; Lucado, A. M. (2005). "Risk management strategies in physical therapy: documentation to avoid malpractice". *International Journal of Health Care Quality Assurance* (vol. 18, núm. 2, págs. 123-130).

Lemieux, V. L. (2010). "The records-risk nexus: exploring the relationship between records and risk". *Records Management Journal* (vol. 20, núm. 2, págs. 199-216).

Massingham, P. (2010). "Knowledge risk management: a framework". *Journal of Knowledge Management* (vol. 14, núm. 3, págs. 464-485).

Queensland Government (2002). "Best Practice Guide. Information risk management". Disponible en línea: http://www.qgcio.qld.gov.au/SiteCollectionDocuments/Architecture%20and%20Standards/Information%20Standards/Current/riskmanagementbpg.pdf [Consulta: 15 de octubre del 2012].

Tchankova, L. (2002). "Risk identification - basic stage in risk management". *Environmental Management and Health* (vol. 13, núm. 3, págs. 290-297).

Williams, R.; Bertsch, B.; Dale, B.; Van Der Wiele, T.; Van I., J.; Smith, M.; Visser, R. (2006). "Quality and risk management: what are the key issues?". *The TQM Magazine* (vol. 18, núm. 1, pág. 67-86).