Riesgos y seguridad de la información: convergencias desde la gestión documental

Risks and security of information: convergences from records management

Elisa García-Morales

García-Morales, Elisa (2016). "Riesgos y seguridad de la información: convergencias desde la gestión documental". *Anuario ThinkEPI*, v. 10, pp. 131-133.

http://dx.doi.org/10.3145/thinkepi.2016.27

Publicado en *IweTel* el 21 de enero de 2016

Resumen: La aproximación entre las disciplinas que abordan la gestión de los riesgos, la gestión de la seguridad de la información y la gestión documental es necesaria para que las organizaciones adopten la mejor estrategia en un escenario complejo de transformación digital. Hay muchos puntos de convergencia entre ellas y nuestra experiencia en el sector bancario nos ha demostrado que pueden articularse a través de un programa de gobernanza de la información. Para ello es imprescindible la colaboración entre los distintos profesionales.

Palabras clave: Seguridad de la información; Gestión de riesgos de la información; Gestión documental; Gobernanza de la información.

Abstract: A rapprochement between disciplines that addresses information security management, risk management, and records management is necessary for organizations to adopt the best strategy in a complex scenario of digital transformation. There are many points of convergence between disciplines, and our experience in the banking sector has shown that a program of information governance is necessary to facilitate collaboration between different professionals.

Keywords: Information security management; Information risk management; Records management; Information governance.

1. Introducción

Estamos asistiendo a una interesante aproximación entre ámbitos profesionales poco relacionados entre sí tradicionalmente. En la última *Jornada de gestión de la información* de *Sedic* (2015) participé en un interesantísimo intercambio de puntos de vista entre expertos en seguridad y en gestión de información y documentación.
http://www.sedic.es/xvii_jornadasgestion

En esta misma línea **Roger Poole** (2015) intervenía en el foro profesional de *AIIM*, expresando su confianza sobre un acercamiento de los profesionales de la información y documentación a los aspectos relacionados con la seguridad y protección de datos, especialmente con motivo de la inminente implantación de la reforma sobre privacidad de datos en la UE (*European Commission*, 2015). También he tenido la ocasión de percibir este interés mutuo en mis últimos proyectos de consultoría, trabajando con grupos interdisciplinares en la definición de políticas de gobernanza de la información.

2. Las tensiones y retos de futuro

Un interesante trabajo de la prestigiosa consultora *Gartner* (**Perkins**; **Byrnes**, 2015) compara el panorama de futuro hasta 2020 con la explosión de una estrella desde el núcleo hacia unos bordes que cada vez se expanden más. Siguiendo este símil se plantean dos líneas de tensión principales:

- tensión entre un núcleo en el que predominan los modelos tecnológicos y de información centralizados y unos bordes caracterizados por la multiplicación de dispositivos, aplicaciones, almacenamiento, interacciones y comunicaciones.
- tensión entre un núcleo con acceso y seguridad cerrada y controlada, y unos bordes en los que las exigencias de disponibilidad, transparencia y apertura cada vez son mayores.

La transformación digital sitúa a las organizaciones en un escenario en el que hay que tomar decisiones muy importantes sobre dónde se quieren y deben situar entre el núcleo y el centro de ambas líneas de tensión. Dependiendo de sus características, tamaño, sector al que pertenecen o estrategia de negocio, los modelos a adoptar serán muy distintos. Estas decisiones son cada vez más complejas y hacen imprescindible alinear visiones y planteamientos de todos los ámbitos profesionales relacionados con la gestión de la información.

"El régimen de gestión de riesgos de la información es un factor crítico de éxito y elemento central de cualquier estrategia de ciberseguridad"

3. La gestión de riesgos en el centro de las decisiones

Tal como representa el *CESG* (2015), el régimen de gestión de riesgos de la información es un factor crítico de éxito y elemento central de cualquier estrategia de ciberseguridad. Pero no parece posible aplicar indefinidamente medidas de seguridad del mismo nivel para toda la información de que dispone una organización, por lo que será necesario discriminar en función de sus tipos y ciclos de vida. El balance entre los riesgos asumibles y el valor de la información es inherente a la toma de cualquier decisión relacionada con la gestión y gobierno de la información, y es ahí donde las metodologías de gestión documental y *records management* aportan su utilidad en la apreciación y evaluación de los riesgos relacionados con los diferentes activos de información. La gestión de riesgos de la información actúa como elemento de convergencia entre las disciplinas que protegen a la empresa del potencial daño de seguridad, y las disciplinas que permiten clasificar y mejorar la organización y extracción de valor de la información a lo largo de su ciclo de vida.

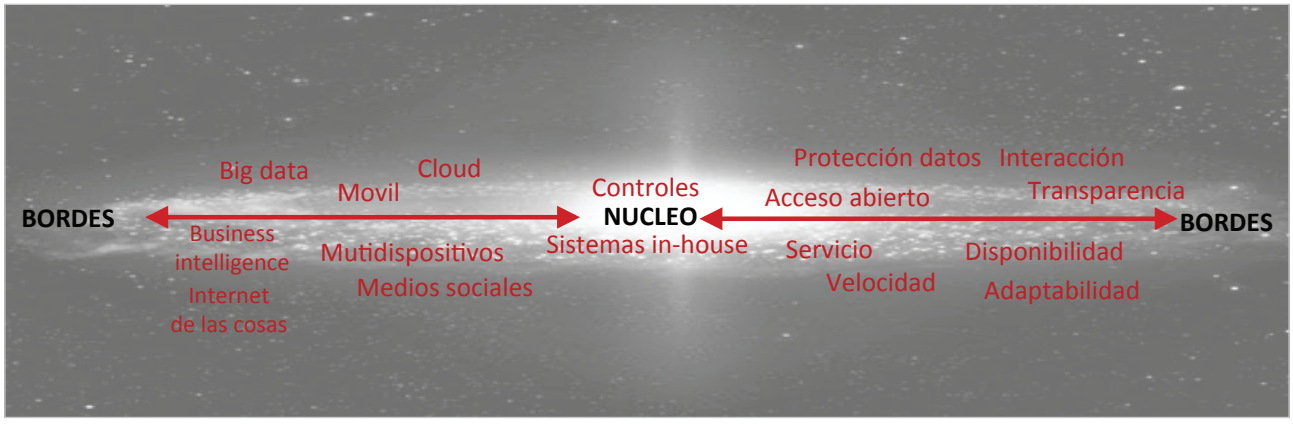
La *ISO 18128* (*Aenor*, 2014), informe técnico desconocido por los responsables de seguridad y de gestión de riesgos, sirve de guía en los trabajos de apreciación de los riesgos operacionales en la gestión de la información y documentos. Los riegos de contexto, en mi experiencia práctica, deben ser evaluados de manera común con todos los ámbitos relacionados con la información.

4. Convergencia en la práctica

A modo ilustrativo, haré referencia a un reciente caso práctico en el sector bancario. Se trata de un proyecto en el que partimos de un planteamiento inicial para abordar la gestión documental con unos requerimientos basados en el empleo de un software ECM (*enterprise content management*) centralizado en un entorno de uso interno restringido; aplicando el símil de las tensiones estaríamos ante un enfoque de núcleo tradicional.

La creación de un equipo de trabajo estratégico integrado por responsables de riesgos, seguridad de la información, cumplimiento normativo, responsabilidad social, I+D, *data management* y organización y procesos, puso rápidamente de manifiesto la necesidad un modelo más transformador, pues la realidad está empujando a la banca a expandirse hacia los bordes. El sector financiero está sujeto a una gran presión reguladora y a potentes dinámicas de cambio de modelo de servicio y relación con los clientes; las tensiones enunciadas han aparecido en prácticamente todas las decisiones que se han tenido que ir adoptando tanto a nivel político como técnico y operacional:

- qué y cómo gestionar la información que residirá en distintas soluciones de almacenamiento en la nube;



- qué contenidos deben permanecer en los sistemas internos en función de sus niveles de riesgos y requerimientos de seguridad;
- cómo abordar el registro de la evidencia de las interacciones con terceras partes a través de canales y/o dispositivos múltiples;
- cómo aplicar una clasificación y calificación de los niveles de seguridad unificada;
- cómo implementar los metadatos como servicio para múltiples aplicaciones;
- etc.

El resultado ha sido la definición de un modelo flexible e integrador de gobierno de la información que aúna los principios de gestión comunes que comparten la gestión de riesgos, la gestión de la seguridad de la información y la gestión para los registros documentales (*records*) entendiendo éstos como datos y documentos. La estrategia de información se articula a partir de la política que marca unos criterios de base que facilitan situarse en el punto adecuado que el banco necesita entre centralización-descentralización y cierre-apertura para cada conjunto o subconjunto de contenidos informativos. El proceso de adopción y transformación se ha planificado a cinco años, lo que, a la velocidad que se mueve el entorno podría parecer un tiempo muy largo. Sin embargo, nuestra experiencia práctica es que las acciones que implican movimientos de cambio en el núcleo pre-existente son por lo general lentas y reactivas. El reto consiste en saber acompasar estas transformaciones con el ritmo al que empujan las necesidades de expansión hacia los bordes y para ello es imprescindible una colaboración cada vez más estrecha entre todos los actores implicados.

5. Bibliografía

CESG (2015). *10 Steps to cyber security*. The UK National Technical Authority for Information Assurance (formerly Communications-Electronics Security Group). *https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility/10-steps-summary*

European Commission (2015). *Agreement on Commission's EU data protection reform will boost digital single market*. Press release, Brussels, 15 December. *http://europa.eu/rapid/press-release_IP-15-6321_en.htm*

Perkins, Earl; **Byrnes, Christian** (2015). *Cybersecurity scenario 2020 phase 2: Guardians for big change*. Gartner. *https://www.gartner.com/doc/3097027/cybersecurity-scenario--phase-*

Poole, Roger (2015). "The basics and (hopefully) some useful information!". *Foro AIIM*, December.

Aenor (2014). *UNE-ISO/TR 18128:2014 IN. Información y documentación. Apreciación del riesgo en procesos y sistemas de gestión documental. http://www.aenor.es/aenor/normas/normas/fichanorma.asp?tipo=N&codigo=N0053363*

Elisa García-Morales
http://www.inforarea.es
garcia-morales@inforarea.com