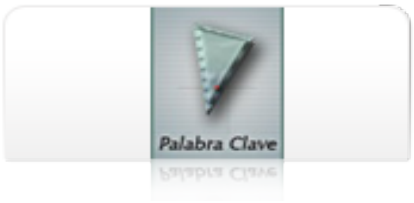

Palabra Clave (La Plata)
E-ISSN: 1853-9912
palabraclave@fahce.unlp.edu.ar
Universidad Nacional de La Plata
Argentina

Corda, María Cecilia; Viñas, Mariela; Coria, Marcela Karina
Gestión del riesgo tecnológico y bibliotecas: una mirada transdisciplinar para su abordaje
Palabra Clave (La Plata), vol. 7, núm. 1, octubre, 2017, pp. 1-18
Universidad Nacional de La Plata
La Plata, Argentina

Palabra Clave (La Plata), octubre 2017, vol. 7, n° 1, e032. ISSN 1853-9912
Universidad Nacional de La Plata.
Facultad de Humanidades y Ciencias de la Educación.
Departamento de Bibliotecología

Gestión del riesgo tecnológico y bibliotecas: una mirada transdisciplinar para su abordaje[1]

Technological risk management: transdisciplinary perspective to think about the libraries

María Cecilia Corda *, Mariela Viñas **, Marcela Karina Coria **

* Facultad Latinoamericana de Ciencias Sociales FLACSO Sede Argentina. Instituto de Investigaciones en Humanidades y Ciencias Sociales (UNLP-CONICET). Facultad de Humanidades y Ciencias de la Educación (FaHCE). Universidad Nacional de La Plata (UNLP), Argentina, ** Instituto de Investigaciones en Humanidades y Ciencias Sociales (UNLP CONICET). Facultad de Humanidades y Ciencias de la Educación (FaHCE). Universidad Nacional de La Plata (UNLP), Argentina | mccorda2003@yahoo.com.ar, marovinas@gmail.com, coria.marcela05@gmail.com

PALABRAS CLAVE

Gestión de bibliotecas

Gestión del riesgo tecnológico

Sistemas de información

Normas nacionales

Estándares internacionales

RESUMEN

El presente trabajo presenta una revisión bibliográfica y de normas nacionales e internacionales sobre la noción de gestión del riesgo tecnológico. El desarrollo tecnológico ha traído como consecuencia el aumento sustancial de los riesgos principalmente en lo referido a problemas derivados en el acceso de la información, ante la posibilidad de pérdida o distorsión de la misma. Se pone el foco en lo que respecta al ámbito específico de bibliotecas, centros de información o documentación. Se rastrearon y analizaron políticas aplicadas en bibliotecas del ámbito nacional. Por último, se delinean algunas consideraciones a tener en cuenta en relación a la gestión del riesgo tecnológico en el campo bibliotecario.

KEYWORDS

Library management

Technological risk management

Information systems

National standards

International standards

ABSTRACT

This paper presents a bibliographical review and of national and international standars about the technological risk management. The technological development has brought as consequence the substantial increase of the risks, principally in connection with information access's problems, in face of the possibility of loss or distortion of the same one. This contribution aims to the specific area of libraries, centers of information or documentation. There were located and analyzed policies applied in libraries of the national area. By last, some considerations about technological risk management in relation with library's ambit are delineated.

Recibido: 26 de mayo de 2017 | Aceptado: 21 de agosto de 2017 | Publicado: 9 de octubre de 2017

Cita sugerida: Corda, M. C, Viñas, M. y Coria, M. K. (2017). Gestión del riesgo tecnológico y bibliotecas: una mirada transdisciplinar para su abordaje. *Palabra Clave (La Plata)*, *7*(1), e032. https://doi.org/10.24215/18539912e032

Introducción

Denominaciones tales como *sociedad de la información*, *sociedad del conocimiento*, *sociedad red*, *era de internet*, entre otras, son muy comunes de leer o mencionar en nuestro ámbito bibliotecario. Sin embargo, poco se analiza o cuestiona sobre los riesgos que ha traído aparejada esta nueva configuración societal.

Autores que reflexionan sobre la denominada modernización reflexiva, tales como Anthoy Giddens (1993, 1998a, 1998b), Scott Lash (1990) y Ulrich Beck (1998, 2002), denuncian los efectos patológicos o perversos del desarrollo del capitalismo tardío y la emergencia de un nuevo tipo societal. El mismo surge, en parte, como consecuencia de la desinstitucionalización (escuelas, familia, iglesias, etc.), con el consiguiente cambio de pautas de organización social. La integración social ya no puede comprenderse como una relación entre actor y sistema, sino como un distanciamiento entre lo objetivo y lo subjetivo.

Beck se diferencia de Lash y Giddens ya que concibe a la reflexividad como autoconfrontación: la individualización no significa atomización, es confrontación a la realidad, es desvinculación seguida de re-vinculación del sujeto como autor de su propia biografía. En el centro del debate se posiciona la problemática de la confianza frente a la imprevisibilidad. Los entornos culturales ya no son tan determinantes, no hay una reglamentación social ante lo que surge una red de relaciones que se entrecruzan, se oponen o se acoplan, creando espacios de mayor libertad. El sujeto se libra de los determinantes de la familia, la clase, el lugar de nacimiento, no está condenado a ser libre, sino a individualizarse, tiene que hallar nuevas certezas y nuevos marcos de confianza en un contexto de otras interdependencias. Es artífice de sus propias convicciones, su propia vida, sus propios compromisos en las distintas fases de su existencia. La familia y el matrimonio dejan de ser las unidades de reproducción, y el individuo ocupa ese lugar, con lo cual se concluye que este sujeto experimenta una sobrecarga ante cualquier fracaso que es tomado como puramente personal.

Estos embates de la modernización reflexiva, consistentes en la transformación de las significaciones colectivas (conciencia de clase) y del optimismo ante el progreso, hacen recaer sobre el individuo la tarea de resignificarlo todo. El hombre es arrojado al mundo del riesgo, una sociedad que resulta del triunfo del capital, no de su crisis, una especie de autodestrucción creativa que da lugar a una nueva sociedad sin que ésta sea el producto de una revolución social.

Ahora bien, en qué momento se puede decir que aparece esta nueva sociedad. Los autores no asientan explícitamente cuándo se genera la transición hacia este nuevo orden; sin embargo, de manera constante hacen referencia al antes y al después, a pesar de que la línea divisoria no esté claramente constituida. Se podría fijar como parámetro la desarticulación que experimenta la sociedad salarial a partir de los años ´70, y las consecuencias que este proceso trajo aparejadas: un nuevo tipo societal conceptualizado, tal como dijimos, como modernización reflexiva, sociedad red, sociedad informacional o del conocimiento, que se caracteriza por profundas transformaciones en las pautas de organización social, que llevan a la desinstitucionalización de los bastiones de la tradición, tales como la escuela, la iglesia, la familia y demás. Dichas instituciones, que prestaban los marcos de confianza que aseguraban las prácticas sociales, dejan paso a una

reflexividad producto del agotamiento de la tradición.

Por su parte, Elliot (1997, p. 21) sostiene que:

> una apertura al mundo social puede significar la oportunidad para la experimentación y la renovación; la transformación personal y la autonomía. Pero igualmente puede significar el riesgo de la confusión personal y cultural, la desintegración de las cosas que parecían sólidas y seguras. De aquí el dilema modernista central: intentar alcanzar alguna especie de equilibrio personal entre seguridad y riesgo, entre oportunidad y peligro.

Es verdad que los autores antes citados piensan las cuestiones en relación a países centrales; no obstante, en nuestras realidades también podemos captar algunas de estas cosas, ya que no nos son ajenas en un mundo globalizado.

Con la aparición y extensión de la tecnología a todos los ámbitos de nuestra vida, nace según Ramírez (2009), y en consonancia con las teorías expuestas, un potencial de riesgo tecnológico doblemente desconocido: por una parte, por su magnitud para la sociedad (al desconocer con certeza el nivel de incidencia que pueda tener) y, por otra, por su alcance (al desconocer el límite espacial y temporal del mismo).

En este marco societal, y pensando en nuestras bibliotecas, centros de información y documentación como instituciones que perviven a pesar de los embates y desafíos que las tecnologías han traído aparejados, ya sea absorbiéndolos, adaptándolos, utilizándolos o ignorándolos, tendríamos que plantearnos si este riesgo se puede gestionar. El interrogante central es si es posible la gestión del riesgo (GRi). Así, en este trabajo nos preguntaremos especialmente por la GRi tecnológico vinculada a los sistemas que atraviesan nuestras unidades de información.

Los interrogantes que nos planteábamos en un trabajo anterior (Corda, Viñas, Coria y Cuervo, 2016) cobran nueva vigencia: ¿La GRi no tendría que implementarse como parte de la gestión antes de dar el paso del cambio en lo tecnológico? ¿Cuántos de estos cambios sólo fueron modas pasajeras? ¿Cuántas pérdidas de tiempo, recursos e inversiones hemos atravesado con la consecuente frustración? ¿Qué evaluación hubo de esos sucesos? ¿Cuáles fueron los aspectos que se replantearon para gestiones futuras?

La GRi debe entenderse como proceso y no como un fin último, además de tener en claro la convicción de que la GRi implica una gestión para reducir el riesgo existente y una gestión para evitar la generación de nuevas vulnerabilidades.

La GRi tecnológico busca evitar las pérdidas de información ante fallas en los sistemas que pueden ser de cualquier tipo (naturales, accidentales, intencionales, etc.), y también considera los fraudes internos o externos (en este sentido, involucra al riesgo legal y al reputacional ante esas amenazas).

Otro enfoque identifica riesgos sobre la infraestructura (nivel físico), los sistemas de información (nivel lógico) y las medidas organizacionales (factor humano).

En cualquier caso, nuestras bibliotecas no pueden permanecer ajenas a esta cuestión, ya que son ellas las que concentran en las organizaciones datos valiosos sobre los acervos documentales, la comunidad usuaria y sus servicios de información y documentación.

Podemos adelantar que la GRi supone entonces la aplicación de un método lógico y sistemático para establecer el contexto interno y externo de la organización, con el fin de identificar, analizar, procesar, monitorear, comunicar y evaluar los riesgos asociados con cualquier actividad, función o proceso, de forma tal que permita a las organizaciones minimizar las pérdidas y maximizar sus beneficios. La GRi debería formar parte de la cultura de gestión de una organización; es decir, debe estar incorporada en la filosofía, las prácticas y los procesos, más que ser considerada como una actividad separada o esporádica. En el presente trabajo justamente nos focalizaremos en un tipo de GRi, la tecnológica, ya que con el correr de los años nuestras unidades han atravesado distintos procesos de informatización y automatización.

Para ello, revisaremos la bibliografía que hemos podido localizar al respecto, además de ciertas experiencias y políticas en torno a la GRi en nuestro ámbito y en referencia especial a aspectos tecnológicos.

Gestión del riesgo: hacia una conceptualización desde distintas matrices

Una GRi, idealmente, debería estudiar los riesgos bajo ciertos parámetros y metodologías, para finalmente poder predecirlos, prevenirlos o controlarlos y así dejen de ser una incertidumbre y los causantes de muchos obstáculos y malos momentos para nuestras organizaciones, para nosotrxs como profesionales, para nuestrxs usuarixs, para la infraestructura de nuestros centros de trabajo, para la colección en el soporte en que se encuentre y para nuestros sistemas informáticos.

Mucha de la bibliografía existente en torno al tema se refiere a catástrofes naturales o causadas por el ser humano; no obstante eso, su alcance es amplio y puede aplicarse a la gestión de las organizaciones en otros contextos que no sean los de la calamidad extrema (incendios, inundaciones, terremotos, saqueos, etc.).

La Organización Panamericana de la Salud (2010), define GRi de la siguiente manera:

> abarca la evaluación y el análisis del riesgo, al igual que la ejecución de estrategias y de acciones específicas para controlar, reducir y transferir el riesgo. Esta es una práctica generalizada de diversas organizaciones para minimizar el riesgo en las decisiones de inversión y para abordar riesgos operativos, tales como la interrupción de los negocios, las fallas en la producción, el daño ambiental, los impactos sociales y los daños como consecuencia de los incendios y de las amenazas naturales (Organización Panamericana de la Salud, 2010, p. 102).

Varela Orol (2009) agrega lo siguiente:

> denominamos gestión del riesgo a la aplicación sistemática de políticas, procedimientos y prácticas de gestión a la tarea de identificar, analizar, evaluar, tratar y controlar los riesgos. Naturalmente, lo primero que es preciso señalar es que un medio libre de riesgos no existe, y que todos los procesos de cambio, al realizar cosas nuevas, implican más riesgos que los procesos habituales, aunque no es menos cierto que cada vez más el mayor riesgo es no hacer cambios. Además a la hora de administrar el riesgo hay que encontrar el equilibrio entre los costes y los beneficios. Por tanto, es preciso definir qué nivel de riesgo es aceptable para una

> organización (Varela Orol, 2009, p. 32).

Por su parte, Rozen (2011) se refiere a la GRi como:

> un sistema compuesto por procesos que permiten en conjunto identificar y administrar en forma adecuada los hechos contingentes (riesgos) a los cuales está expuesto un ente o emprendimiento, a fin de obtener un beneficio y añadir valor como producto de transitar un camino escogido. El objetivo principal de la gestión de riesgos es brindar a las partes interesadas una seguridad razonable (nunca podría ser absoluta) que los riesgos significativos serán identificados, analizados, valorados y serán un input para la toma de decisiones por parte del Management (Rozen, 2011, p. 11).

López Bravo y Montoya (2013) delinean el enfoque de la GRi añadiendo la importancia de la elaboración de políticas organizacionales al respecto:

> es un proceso social complejo, que necesita del planeamiento y aplicación de políticas, estrategias, instrumentos y medidas orientadas a impedir, reducir, prever y controlar los efectos adversos de fenómenos peligrosos sobre la población, los bienes y servicios, y el ambiente. Acciones integradas de reducción de riesgos a través de actividades de prevención, mitigación, preparación para, y atención de emergencias y recuperación post impacto (López Bravo y Montoya, 2013, p. 856).

Además, es importante destacar que se han estudiado los riesgos en el contexto empresarial con énfasis desde especialidades, tales como riesgos laborales, ambientales, relacionados con la calidad, financieros, operacionales, estratégicos, logísticos y de las cadenas productivas, de tecnología de información, entre otros (Bolaño Rodríguez Robaina, Pérez Barnés y Arias Pérez, 2014). Así, estos análisis de riesgos estudian el daño en la especialidad a la que responden. Los autores llaman la atención sobre que es necesario integrar la gestión de todos estos riesgos para favorecer la toma de decisiones en torno a la mejora de su desempeño organizacional, la protección de los diferentes recursos de la empresa (materiales, tecnológicos, humanos, financieros, informacionales), la protección del medio ambiente, y la seguridad en el cumplimiento de lo establecido en las leyes, normas o resoluciones vigentes.

Asimismo, cabe resaltar que, a nivel nacional, IRAM (2015) ha adoptado la norma ISO 31000:2009 (*Risk management*), en la cual define al riesgo como "el efecto de la incertidumbre en la consecución de los objetivos". Esta norma propone que la implementación de la GRI y su sostenibilidad y eficacia requieren de un compromiso organizacional muy fuerte, así como una planificación estratégica que genere niveles de responsabilidad en su cumplimiento efectivo.

En el entorno organizacional, en especial en las bibliotecas, centros de información o documentación, la GRi puede implementarse como proceso teniendo en cuenta los siguientes pasos: 1. Identificar y clasificar los temas clave; 2. Fijar prioridades; 3. Valorar los factores de riesgo; 4. Desarrollar posturas y respuestas (o reacciones); 5. Implementar la acción; 6. Medir los resultados (Cóppola, 2012).

Fernández Sanz y Bernad Silva (2014) señalan que una razón para la crisis en la GRi puede ser el componente subjetivo que tienen los proyectos, y la fuerte dependencia del

punto de vista del observador u observadora. Así, sostienen, mientras es posible cuantificar los costos o avances del proyecto cuyos datos provengan de distintas fuentes, resulta difícil combinar, valorar y dar la credibilidad adecuada a las observaciones de riesgos de diferentes personas o en distintos contextos. Los autores resaltan que existe una abundante normativa sobre cómo identificar y tratar los riesgos. Se dispone además de facilidades como son las taxonomías y las listas de factores de riesgos más conocidos. En la encuesta piloto realizada en España sobre el tema, refieren que los primeros datos parecen ser optimistas sobre el conocimiento de la GRi por parte de los encuestados, la experiencia real de muchos de ellos, y la percepción positiva de su aplicación a los proyectos. Sin embargo, recalcan, llama la atención el contraste entre el buen nivel de conocimiento y el uso de las herramientas disponibles para gestionar los riesgos y las dificultades que parecen existir para acceder a información de proyectos anteriores, así como la aparente falta de disciplina a la hora de documentar los problemas aparecidos durante el desarrollo de un proyecto. Mencionan que falta asumir a la GRi de un modo más sistemático. En lo relativo a los factores de riesgo más frecuentes, la importancia de los requisitos parece ser una constante en todas las categorías que analizaron.

Pérez Moya y Zulueta Véliz (2013) señalan que la GRi incluye subprocesos tales como la planificación, la identificación de los riesgos, el análisis de los riesgos, la definición y la aplicación de actividades para la resolución de eventualidades, la comunicación de los riesgos, el control y la evaluación del proceso de GRi. Los autores se dedicaron a analizar el Centro de Informatización Universitaria dependiente de la Universidad de las Ciencias Informáticas (Cuba). En este centro, los riesgos son monitoreados a través de la plataforma GESPRO (Laboratorio de Gestión de Proyectos). Sugieren la aplicación del método de consulta a expertos, más conocido como método *Delphi*, el cual les ha resultado de utilidad para el estudio llevado a cabo en esa institución académica. Al analizar algunos proyectos llevados adelante, consideran que el principal problema que atentó contra la aplicación de la propuesta fue que la necesidad de gestionar riesgos pasó a un segundo nivel, es decir, se dio una disminución del proceso de seguimiento y control de los riesgos. Asimismo, los autores remarcan que no existían experiencias en la aplicación de métricas, lo que dificultó la recolección de datos para la incorporación e interpretación de estos. En lo que respecta al proyecto Biblioteca, el 73,81% de los riesgos identificados estaban dados por las categorías de negocio, asociados a la gestión y al factor humano.

Nos focalizaremos a continuación en el tema de la GRi tecnológico, para después pasar revista de algunas experiencias en nuestro campo de actuación, las cuales no abundan, aunque no se puede desconocer que hay ciertos avances y ensayos al respecto.

Gestión del riesgo tecnológico: abordaje conceptual

En el trabajo anterior de nuestra autoría ya mencionado, en el que abordamos nociones, recomendaciones, pautas y estándares sobre GRi en el ámbito de las bibliotecas, arribamos a la noción de GRi informático (Corda, Viñas, Coria y Cuervo, 2016, p. 8). Profundizaremos, tal como anticipamos más arriba, sobre este concepto. Puntualmente, intentaremos clarificar algunos conceptos relevantes a la hora de comprender este abordaje específico.

El acelerado crecimiento de las tecnologías de la información y la comunicación de las últimas décadas, sumado a la enorme circulación de información, han generado un sinnúmero de oportunidades, como así también una extensa cantidad de amenazas. Por lo que, en este entorno creciente y complejo, las y los responsables de gestionar las herramientas tecnológicas deben estar capacitados para diagnosticar adecuadamente los riesgos a los cuales se ven expuestos a fin de poder mitigar de manera oportuna las pérdidas que puedan generarse (Sena y Tenzer, 2004, pp. 1-2). En tanto, Mosanlve Pulido, Aponte Novoa y Chaves Tamayo (2014) también se refieren a esta preocupación:

> En la actualidad, la determinación del nivel de inseguridad (visto desde la óptica de vulnerabilidad y riesgo) de la información trasciende los niveles de su uso u operatividad, de forma que es necesario interpretar sus unidades de portabilidad y los medios por los que se transmite, donde se abren nuevas configuraciones al fraude, a la alteración y al uso indebido; esto ha guiado al asentamiento de áreas forenses, cibercrimen e inteligencia sobre la información (Monsalve Pulido, Aponte Novoa y Chaves Tamayo, 2014, p. 67).

El *riesgo informático* refiere a aquella eventualidad que imposibilita el cumplimiento de un objetivo, es decir, todo aquel peligro o daño que puede afectar el funcionamiento directo o los resultados esperados de un sistema informático. Zulueta, Despaigne y Hernández (2009, pp. 7-8) plantean que, si bien se han producido amplios debates sobre una definición adecuada y aun cuando los criterios son variados, hay acuerdo común en que este tipo de riesgo implica dos dimensiones:

Incertidumbre: acontecimiento caracterizado como riesgo: puede, o no, ocurrir.

Efecto en los objetivos: si el riesgo se convierte en una realidad, esto tendrá consecuencias para el proyecto.

Para que un sistema informático pueda definirse como seguro, es necesario que se den cuatro características fundamentales simultáneamente:

- **Integridad**: la información solo puede ser modificada por quien está autorizado.
- **Confidencialidad**: la información solo debe ser legible para las personas interesadas.
- **Disponibilidad**: la información debe estar disponible cuando se necesite.
- **Irrefutabilidad**: la información debe conservar la propiedad de la autoría comprobable.

El riesgo informático posee varios componentes a considerar: seguridad física, control de accesos, protección de los datos y seguridad en las redes, organización y división de responsabilidades, cuantificación de riesgos, políticas hacia el personal, medidas de higiene, salubridad y ergonomía, selección y contratación de seguros, aspectos legales y delitos, estándares de ingeniería, programación y operación, función de los auditores tanto internos como externos, seguridad de los sistemas operativos y de red y plan de contingencia.

A partir de la consulta de la diversa bibliografía sobre la temática, advertimos varios tipos de riesgos informáticos, entre los que podemos mencionar a los siguientes:

Riesgos de integridad: abarcan todos los riesgos asociados con la autorización, completitud y exactitud de la entrada, procesamiento y reportes de las aplicaciones utilizadas en una organización. Estos riesgos aplican en cada aspecto de un sistema de soporte de procesamiento de negocio y están presentes en múltiples lugares y momentos en todas las partes de las aplicaciones.

Riesgos de relación: refieren al uso oportuno de la información creada por una aplicación. Estos riesgos se relacionan directamente a la información de toma de decisiones (información y datos correctos de una persona/proceso/sistema correcto en el tiempo preciso permiten tomar decisiones correctas).

Riesgos de acceso: se enfocan en lo que es el acceso inapropiado a sistemas, datos e información. Estos riesgos suponen tanto los riesgos de segregación inapropiada de trabajo, así como los riesgos asociados con la integridad de la información de sistemas de bases de datos y los riesgos asociados a la confidencialidad de esa información.

Riesgos de utilidad: se centran en tres diferentes niveles de riesgo:

- Los riesgos pueden ser enfrentados por el direccionamiento de sistemas antes de que los problemas ocurran.
- Técnicas de recuperación/restauración usadas para minimizar la ruptura de los sistemas.
- *Backups* y planes de contingencia controlan desastres en el procesamiento de la información.

Riesgos de infraestructura: ocurren cuando en las organizaciones no existe una estructura de información tecnológica efectiva (hardware, software, redes, personas y procesos) para soportar adecuadamente las necesidades futuras y presentes de los negocios con un costo eficiente. Estos riesgos están asociados con los procesos de la información tecnológica que definen, desarrollan, mantienen y operan un entorno de procesamiento de información y las aplicaciones asociadas (servicio al cliente o usuaria/o, pago de aranceles, etc.)

Riesgos de seguridad general: suceden cuando no se tienen en cuenta estándares tales como los de la *International Electrotechnical Commission* (IEC 950), los cuales proporcionan los requisitos de diseño para lograr una seguridad general en vistas de disminuir el riesgo.

El riesgo de origen tecnológico puede incidir sobre las metas y los objetivos organizacionales y ser causa de otro tipo de riesgos al ser intrínseco al uso de tecnología. Por ello, cuestiones tales como el daño, la interrupción, la alteración o la falla derivada del uso de tecnologías pueden implicar pérdidas significativas en las organizaciones, desgranamientos financieros, multas, acciones legales, afectación de la imagen pública de una organización y causar inconvenientes a nivel operativo y estratégico. Por esto,

Ramírez Castro y Ortiz Bayona (2011) proponen una metodología que permite la GRi de origen tecnológico cuya base son los estándares ISO 31000, que ya mencionamos más arriba, e ISO/IEC 27005 (Information Security Risk Management), de los cuales se realizaron las adaptaciones y especificaciones requeridas para este tipo de riesgo. Además se incorporan recomendaciones y buenas prácticas de otras guías y metodologías para GRi. Se trata de una interesante propuesta, ya que permite entender mejor los conceptos definidos en los estándares mencionados para GRi dándole un enfoque hacia lo que son los riesgos tecnológicos.

El nivel de riesgo depende del análisis previo de vulnerabilidades del sistema, de las amenazas y del posible impacto que éstas puedan tener en el funcionamiento de la organización. Gómez Vieites (2013) repasa diferentes metodologías de GRi informático, como por ejemplo, la CRAMM (CCTA Risk Analysis and Management Method) para la evaluación de riesgos en sistemas informáticos. Esta metodología fue desarrollada por la agencia CCTA (Central Computer and Telecommunications Agency) del gobierno del Reino Unido ya en el año 1985.

En vistas de que trabajamos estos conceptos en el ámbito de las bibliotecas y otras unidades de información, es necesario que también abordemos la GRi en sistemas de información. Guerrero Julio y Gómez Florez (2011, p.197) aclaran una diferencia muy importante: en ocasiones se confunde seguridad informática con seguridad de la información y, no obstante, no son sinónimos. La seguridad informática es el conjunto de medidas preventivas y reactivas de las organizaciones y los sistemas tecnológicos que permiten resguardar y proteger la información, buscando mantener la confidencialidad, disponibilidad e integridad de la misma. Mientras que seguridad informática sólo refiere a la seguridad en el medio informático (González Pagés, 2016), la seguridad de la información alude a la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento dentro de una organización. La seguridad de los sistemas de información es la capacidad de las redes o de los sistemas de información para resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de la información almacenada o transmitida, y de los servicios que dichas redes y sistemas ofrecen o hacen accesibles. No obstante, ambas "seguridades" se conocen como parte de la GRi en sistemas de información (Guerrero Julio y Gómez Flores, 2011, p. 198).

Bejarano Lobo (2010) alude a la GRi de proyectos informáticos como el conjunto de procesos concernientes al manejo de la planificación de la GRi, identificación, análisis, respuestas, monitoreo y control del proyecto informático. Los factores de riesgo más comunes en este tipo específico de planificaciones son: el factor humano, el software y el hardware, la comunidad usuaria, la logística, como así también la organización misma del proyecto. Asimismo, la administración de riesgos en el marco de la gerencia de proyectos se conoce como el arte y la ciencia de identificar, analizar y responder a los riesgos a lo largo de la vida de un proyecto, con el propósito de lograr los objetivos del proyecto.

Ahora bien, según Gómez Vieites (2013), un proceso de GRi comprende una etapa de evaluación previa de los riesgos del sistema informático, que se debe realizar con rigor y

objetividad para que cumpla su función con garantías. Para ello, el equipo responsable de la evaluación debe contar con un nivel adecuado de formación y experiencia previa, así como disponer de una serie de recursos y medios para poder realizar su trabajo, contando en la medida de lo posible con el apoyo y compromiso de las autoridades. En el proceso propiamente dicho de GRi, se trata de definir un plan para la implantación de ciertas salvaguardas o contramedidas en el sistema informático que permita disminuir la probabilidad de que se materialice una amenaza, o bien reducir la vulnerabilidad del sistema o el posible impacto en la organización, así como permitir la recuperación del sistema o la transferencia del problema a un tercero (mediante la contratación de un seguro, por ejemplo). Asimismo, la administración de riesgos refiere al proceso interactivo basado en el conocimiento, la valoración y el monitoreo de los riesgos y sus impactos en la organización. Es aplicable a cualquier situación donde un resultado no deseado o inesperado podría ser significativo en el logro de los objetivos, o donde se identifiquen "oportunidades de negocio". No obstante, no basta simplemente con administrar en forma eficaz los riesgos tecnológicos, sino que se debe aprovechar la tecnología para gestionar los riesgos.

De acuerdo con sus operaciones, procesos y estructura, las organizaciones deben definir una *estrategia de protección de activos de información*, que les permita optimizar la efectividad en la administración y el control de sus activos de información. Dicha estrategia debe considerar las amenazas y vulnerabilidades asociadas a cada entorno tecnológico, su impacto en el negocio, los requerimientos y estándares vigentes. Para ello se deben asignar claramente roles y responsabilidades en materia de seguridad, comprometiendo a las autoridades. La estrategia de seguridad debe contemplar el establecimiento de mecanismos de control para la detección, el registro, el análisis, la comunicación, la corrección, la clasificación y la cuantificación de los incidentes y las debilidades en los accesos no autorizados a la información administrada en los sistemas de información. Esta estrategia abarca, además de los recursos informáticos propios de la entidad, a sus grupos de influencia: sistema financiero, clientes o usuarios de todo tipo, proveedores de recursos y sistemas de información, operadores de telecomunicaciones, requerimientos de los organismos de regulación y control, y otros entes externos vinculados directa o indirectamente.

Actualmente, no podemos decir que no existen marcos de trabajo, metodologías y estándares internacionales que aborden la cuestión de la GRi en relación a las tecnologías de información: a ello refieren los trabajos de Fernández Sánz y Bernard Silva (2014), así como el de Ramírez Castro y Ortiz Bayona (2011) y Gómez y otros (2010). El marco para la GRi lo conforman las ya mencionadas normas ISO 31000 e ISO/IEC 2700. Estos estándares proveen lineamientos generales, aunque, señalan Ramírez Castro y Ortiz Bayona (2011), hace falta una guía más precisa que ofrezca pautas sobre la forma de lograr los aspectos de seguridad requeridos; este marco hace referencia a la GRi como concepto global y deja de lado el análisis de riesgos específicos como el tecnológico, lo más cercano a ello es la administración del riesgo operativo que se relaciona de forma tangencial con aquel.

Gestión del riesgo tecnológico en bibliotecas

Al hablar sobre el tema de la GRi en las bibliotecas, Prieto Gutiérrez (2009, pp. 1-2) comenta que la seguridad en las bibliotecas abarca tres campos importantes, que son: la seguridad de las personas, de edificios e instalaciones y del acervo bibliográfico, allí es donde se debe tener en cuenta el riesgo informático. Frecuentemente es tratado de forma independiente, pero su tratamiento en conjunto provoca que se forme un valioso trabajo mejorando la efectividad organizacional.

Hoy en día, las bibliotecas dependen en su gran mayoría de las administraciones locales, provinciales o nacionales. Al estar en edificios que comparten con otras secciones, áreas o departamentos de trabajo, suelen estar obstaculizadas la creación y la puesta en marcha de una unidad central dedicada a la seguridad de las tres áreas indicadas anteriormente. Aquí es donde surge el tema a tener en cuenta: ¿Existe la seguridad en las bibliotecas? El objetivo es gestionar el riesgo a un nivel aceptable, de manera tal que pueda asumirlo la institución sin agravantes (Prieto Gutiérrez, 2009, pp. 1-2).

Autores como Kuna y otros (2008, pp. 1-2) aluden a que un riesgo es una variable del proyecto que pone en peligro o impide el éxito del mismo. Es la probabilidad de que un proyecto experimente sucesos no deseables, como retrasos en las fechas, excesos de costos, o la cancelación directa del mismo. Comenta que se han producido amplios debates sobre la definición adecuada para riesgo de software, y hay acuerdo común en que el riesgo siempre implica dos características principales:

- Incertidumbre: el acontecimiento que caracteriza al riesgo puede o no puede ocurrir; por ejemplo, no hay riesgos de un 100 % de probabilidad.
- Pérdida: las consecuencias no deseadas o las pérdidas si el riesgo se convierte en una realidad.

Hay que pensar en un efectivo proceso de GRi; es un importante componente en todo proyecto de software exitoso y en el cual la Web 2.0 y sus componentes forman parte de ello. El principal objetivo de dicho proceso es posibilitar tanto al proyecto como a las organizaciones el cumplimiento de su misión y de sus propósitos.

La GRi permite definir en forma estructurada, operacional y organizacional, una serie de actividades en los proyectos a lo largo de todas las fases de su ciclo de vida para el desarrollo de software. En la mayor parte de los casos, esto se traduce en la creación de planes tendientes a impedir que los riesgos se transformen en problemas o a minimizar su probabilidad de ocurrencia o impacto (Kuna y otros, 2008, pp. 2-3).

Cuando hablamos del propósito del plan de riesgo, tenemos que identificar los riesgos que se puedan presentar en el desarrollo del proyecto, analizarlos, calcular la exposición y en base a ello priorizarlos para establecer estrategias de control y resolución que permitan ejercer una correcta supervisión de los mismos.

Chávez Flores (2009, pp. 2-5) nos dice que se debe tener en claro que no existe una seguridad en términos absolutos. Sólo se pueden reducir las oportunidades de que un sistema sea comprometido, o minimizar la duración y daños provocados a raíz de un ataque.

Al tratar el asunto de la GRi informático, se está considerando que se encuentran en riesgo tres elementos:

a) Los datos: información guardada en las computadoras. Ellos tienen tres características a proteger: la confidencialidad, la integridad y la disponibilidad;

b) Los recursos: el equipamiento en sí mismo.

c) La reputación: una de las actividades iniciales es el análisis de riesgos, para lo cual se debe realizar un modelado de amenazas. Se trata de una actividad de carácter recurrente.

Un riesgo, podemos ir concluyendo, es, en definitiva, una combinación de activos, vulnerabilidades y atacantes.

Políticas sobre GRi en bibliotecas

En cuanto al rastreo de políticas que efectuamos en relación al tema de la GRi en bibliotecas, detectamos que el Sistema de Bibliotecas de la Universidad Católica de Córdoba (2016, pp. 1-3) diseñó una política de gestión integral de riesgos.

En esa política se tomaron en cuenta los objetivos pensados en conjunción con la misión, la visión y los valores de la universidad; el alcance, previendo el contexto estratégico de la institución, en donde se tomaron en cuenta la identificación, el análisis, la evaluación, el tratamiento y el monitoreo de los riesgos, así como la implementación, el seguimiento y la evaluación de planes para mitigar los riesgos; además, los factores de riesgos internos (riesgos del fondo documental, de servicios y productos, de recursos humanos, de infraestructura en lo que respecta al edificio, de equipamiento tecnológico y de recursos financieros) y riesgos externos (riesgos del medio ambiente, del entorno legal, tecnológico, educativo, cultural, social y económico); los principios básicos de garantizar el acceso a la información, proteger el patrimonio, actuar en caso de riesgos de deterioro documental, garantizar la prestación de los servicios, asegurar el cumplimiento de los objetivos, políticas y plan estratégico, integrar la GRi a la cultura de la organización y proponer una mejora continua. De esta forma se armó el sistema integral de control de riesgos, en donde se pautaron elementos como: nombre del riesgo, evaluación, causas, probabilidad de ocurrencia tomando en cuenta la certeza y la frecuencia de que suceda y el nivel de impacto (alto, medio y bajo). No se dejaron de mencionar, además, las acciones preventivas. Al aplicar todo esto y revisar periódicamente la política de riesgos, cuidando la seguridad informática tal como lo destaca Voutssas (2010, p. 2), se minimizarán los riesgos. El proceso de establecer y observar un conjunto de estrategias, políticas, técnicas, reglas, guías, prácticas y procedimientos tendientes a prevenir, proteger y resguardar de daño, alteración o sustracción de los recursos informáticos de una organización, facilitará que se administre el riesgo.

En otro contexto distinto al argentino, detectamos en el trabajo de Varela Orol (2009, pp.

41-43), el caso de la Biblioteca Pública de San Francisco. En este trabajo se analiza más la GRi sobre los sistemas de información relacionándola con la GRi tecnológico: las actuaciones de esa biblioteca en relación a la información proporcionada por los usuarios (préstamo, préstamo interbibliotecario, servicios virtuales, etc.) y posibles usos de los mismos por parte de la institución (generalmente estadísticos); medidas tomadas para garantizar la confidencialidad en las terminales públicas tanto en el acceso al catálogo como a Internet, como el borrado automático del historial; funciones de acceso al registro personal y posibilidad de borrar por ejemplo perfiles de búsqueda; tratamiento de la información proporcionada mediante correo electrónico o formularios web; información y sus fines sobre los datos recogidos cuando un usuario se conecta a la web de la biblioteca; advertencias sobre la necesidad de revisar las políticas de privacidad de los proveedores de recursos electrónicos a los que se accede a través de la biblioteca.

También la European Library incluye en la política de la biblioteca a la GRi, distinguiendo claramente lo que son datos personales, conservados con fines administrativos por el período requerido, de los no personales, que pueden guardarse indefinidamente con fines de investigación o de toma de decisiones. Esta institución menciona también el uso dado a la información registrada (conocer a la comunidad y sus necesidades y mejorar la accesibilidad del portal); la utilización de las cookies e información de las usuarias y los usuarios (estadísticas de uso, mejora de servicios); el compromiso a usar el nombre y correo electrónico de las personas registradas exclusivamente para contestar sus consultas, advirtiendo además que la biblioteca puede tener que entregar por imperativo legal información registrada a las autoridades judiciales, si es que lo solicitan.

Algunas bibliotecas especifican con exactitud qué tipos de datos tienen registrados y hasta cuando prevén conservarlos. Tal es el caso de la Universidad Libre de Bruselas que, junto a la relación de los tipos de datos registrados (obras prestadas, reservadas, multas pagadas y pendientes), señala la duración de la conservación de los datos de acuerdo con el tiempo que cada tipo de usuario mantenga relación con la organización, indicando también el nombre de la persona de contacto para resolver cualquier asunto referido a la protección de la vida privada por parte de los archivos y las bibliotecas.

Recomendaciones preliminares para la GRi tecnológico en el ámbito de bibliotecas

Algunas recomendaciones puntuales para evitar el riesgo tecnológico en bibliotecas, centros de información y documentación, Podrían orientarse a las siguientes acciones:

• Chequear las normas, las políticas, los procedimientos y los controles de la seguridad informática para perfeccionarlos y mantenerlos actualizados.

• Revisar las normas, las políticas, los procedimientos y los controles de la seguridad de los sistemas de información con los que contemos, para perfeccionarlos y mantenerlos actualizados.

• Consolidar un grupo o comité oficial de seguridad tecnológica con personas, funciones y responsabilidades perfectamente establecidas para trabajar en el tema.

• Migrar periódicamente la información y los sistemas informáticos para que no queden obsoletos.

• Tener respaldos de la información internos y externos en la organización en la que estemos.

• Llevar a cabo estudios estadísticos y efectuar controles periódicos para evaluar los riesgos y actuar en relación a los resultados obtenidos.

Finalmente, es importante recordar que se pueden diseñar entornos de seguridad informática y de información para cualquier tipo de organización, independientemente de su tamaño y complejidad. Lo que tenemos que tener en consideración es que debemos delinear y construir ambientes de preservación a largo plazo tomando en cuenta los estándares nacionales e internacionales, más las experiencias de organizaciones afines a las nuestras, lo cual seguramente redundará en nuestro beneficio y en el de la comunidad usuaria.

Conclusiones

La GRi se presenta como una actividad clave para el resguardo de los activos de información y de los sistemas informáticos de una organización y ha de tomarse como un proceso constante.

La GRi tanto en el aspecto de la información como en la esfera tecnológica es responsabilidad de todas las personas que se desempeñan en el entorno organizacional, por más que existan sectores, comités o departamentos encargados en la materia. Lo esencial es crear y desarrollar una cultura de la seguridad. Tal como lo menciona Varela Orol (2009, p. 32), la GRi consiste en la aplicación sistemática de políticas, procedimientos y prácticas de la gestión a la tarea de identificar, analizar, evaluar, tratar y controlar los riesgos. Si nos centramos en los riesgos tecnológicos que pueden afectar a las bibliotecas, los centros de documentación o información, podemos agrupar a aquellos que se encuentran fuera de la propia organización y tienen que ver con las amenazas del entorno, las lógicas de funcionamiento del mercado tecnológico y financiero, a los que se suman los que están en la propia unidad o en la organización de la que depende.

La GRi tecnológico es importante dado que las organizaciones al usar tecnología en su actividad diaria, y como parte de sus procesos, se encuentran expuestas, y ello puede afectar la actividad propia y ser fuente de pérdidas y daños considerables. Hay que crear conciencia en seguridad para prevenir riesgos y buscar estrategias para obtener el apoyo de todo el personal con el fin de cumplir con los objetivos y asegurar la información y los sistemas que la contienen.

Es necesario que, sin importar el ámbito en el que se encuentra una organización, se aplíquela GRi, ya sea como medida preventiva, como solución a obstáculos que aparezcan con el devenir de su desarrollo, o como política para atemperar las consecuencias cuando los problemas se presenten en esta sociedad del riesgo en la que vivimos.

Notas

1 Este trabajo se inscribe en el marco del Proyecto Promocional de Investigación y Desarrollo PPID/H029UNLP 2017-2018: Gestión del riesgo en el ámbito de bibliotecas universitarias: estudio sobre el sistema bibliotecario de la UNLP.

Referencias bibliográficas

Beck, U. (1998). *La sociedad del riesgo. Hacia una nueva modernidad*. Barcelona: Paidós.

Beck, U. (2002). *La sociedad del riesgo global*. Madrid: Siglo XXI.

Bejarano Lobo, J. F. (2010). *Gestión de riesgos en proyectos informáticos*. En II Seminario Riesgo Operacional en las Actividades Bancaria y Bursátil por Medios Electrónicos. Bogotá, Colombia. Recuperado de http://studylib.es/doc/8162322/gesti%C3%B3n-de-riesgos-en-proyectos-inform%C3%A1ticos (Consultado el 28/03/2017)

Bolaño Rodríguez, Y., Robaina, D. A., Pérez Barnés, A. y Arias Pérez, M. (2014).Modelo de dirección estratégica basado en la administración de riesgos. *Ingeniería industrial, 35*(3), 344-357. Recuperado de http://www.redalyc.org/pdf/3604/360433598010.pdf (Consultado el 13/02/2017)

Cóppola, G. (2012). Gestión del riesgo comunicacional. Puesta en práctica. *Cuaderno, 40*, 33-36. Recuperado de http://fido.palermo.edu/servicios_dyc/publicacionesdc/archivos/373_libro.pdf (Consultado el 15/03/2017)

Corda, M.C., Viñas, M., Coria, M. K. y Cuervo, E. (2016). *Nociones de gestión del riesgo enrelación a las bibliotecas: apuntes conceptuales para su caracterización*. En VII Jornadas de Temas Actuales en Bibliotecología. Mar del Plata, Argentina. Recuperado de http://www.memoria.fahce.unlp.edu.ar/trab_eventos/ev.7765/ev.7765.pdf (Consultado el 13/03/2017)

Chávez Flores, A. (2009). *Seguridad Informática (Informe).* Buenos Aires: CLACSO. Recuperado de https://es.slideshare.net/mariorafaelquirozmartinez/seguridad-informtica-27231511 (Consultado el 28/02/2017)

Elliot, A. (1997). *Sujetos a nuestro propio y múltiple ser: teoría social, psicoanálisis y posmodernidad*. Buenos Aires: Amorrortu.

Fernández Sanz, L. y Bernad Silva, P. (2014). Gestión de riesgos en proyectos de desarrollo de software en España: estudio de la situación. *Revista de la Facultad de Ingeniería de la Universidad de Antioquia*, *70*, 233-243. Recuperado de http://www.redalyc.org/articulo.oa?id=43030033021 (Consultado el 12/02/2017)

Giddens, A. (1993). Bienestar positivo, pobreza y valores de vida. En *Más allá de la izquierda y la derecha: el futuro de las políticas radicales* (pp. 181-204). Barcelona: Cátedra.

Giddens, A. (1998a). Amor, sexo y otras adicciones. En A. Giddens. *Las transformaciones de la intimidad: sexualidad, amor y erotismo en las sociedades modernas* (pp. 67-84). Madrid: Cátedra.

Giddens, A. (1998b). El significado sociológico de la codependencia. En A. Giddens, *Las transformaciones de la intimidad: sexualidad, amor y erotismo en las sociedades modernas* (pp. 85-104). Madrid: Cátedra.

Gómez, R., Pérez, D. H., Donoso, Y. y Herrera, A. (2010). Metodología y gobierno de la gestión de riesgos de tecnologías de la información. *Revista de ingeniería, 31*, 109-118. Recuperado de http://www.scielo.org.co/pdf/ring/n31/n31a12.pdf (Consultado el 13/03/2017)

Gómez Vieites, Á. (2013) Análisis y gestión de riesgos. En Gómez Vieites, A. *Seguridad en equipos informáticos*. Bogotá: Ediciones de la U.

González Pagés, C. (2016). *Seguridad informática en bibliotecas*. Recuperado de http://files.sld.cu/bmn/files/2016/04/Seguridad-Inform%C3%A1tica-en-Bibliotecas-opt.pdf(Consultado el 13/03/2017)

Guerrero Julio, M. L. y Gómez Florez, L. C. (2011). Revisión de estándares relevantes y literatura de gestión de riesgos y controles en sistemas de información. *Estudios gerenciales, 27*(121), 195-215. Recuperado de https://www.icesi.edu.co/revistas/index.php/estudios_gerenciales/article/view/1124 (Consultado el 28/03/2017)

IRAM (2015). *Norma ISO 31000 sobre gestión del riesgo*. Buenos Aires: IRAM.

ISO 31000 (2009). *La gestión del riesgo.* Recuperado de https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-1:v1:en (Consultado el 20/03/2017)

Kuna, H. D. et al. (2008). *Plan de riesgos para la implementación, desarrollo y mantenimiento de componentes de Web 2.0 en bibliotecas, caso de estudio en una biblioteca especializada*. En 6° Jornada sobre la Biblioteca Digital Universitaria JBDU 2008 "Los desafíos de la Web Social". La Plata, Argentina. Recuperado de http://www.amicus.udesa.edu.ar/documentos/6jornada/documentos/pdf/PONENCIA%20MISIONES%20RIESGOS%20Web2.0.pdf (Consultado el 28/02/2017)

Lash, S. (1990). *Sociología del posmodernismo*. Buenos Aires: Amorrortu.

López Bravo, O. y Montoya Rivero, J. (2013). Hacia una cultura de gestión del riesgo desde la formación universitaria en la Universidad Estatal de Bolívar, Ecuador. *Santiago, 132*, 851-859. Recuperado de http://revistas.uo.edu.cu/index.php/stgo/article/download/109/105 (Consultado el 14/03/2017)

Mosanlve Pulido, J. A., Aponte Novoa, F. A. y Chaves Tamayo, D. F. (2014). Estudio y gestión de vulnerabilidades informáticas para una empresa privada en el Departamento de Boyacá (Colombia). *Revista de la Facultad de Ingeniería, 23*(37), 65-72. Recuperado de http://revistas.uptc.edu.co/revistas/index.php/ingenieria/article/view/2791 (Consultado el 13/03/2017)

Organización Panamericana de la Salud. (2010). *Guía para el desarrollo de simulaciones y simulacros de emergencias y desastres*. Ciudad de Panamá: OPS. Recuperado de http://www.paho.org/disasters/index.php?option=com_docman&task=doc_download&gid=1085&Itemid=&lang=es (Consultado el 11/02/2017)

Pérez Moya, O. y Zulueta Véliz, Y. (2013). Proceso para gestionar riesgos en proyectos de desarrollo de software. *Revista cubana de ciencias informáticas*, *2*(7), 206-221. Recuperado de http://rcci.uci.cu/index.php?journal=rcci&page=article&op=view&path%5B%5D=433 (Consultado el 14/03/2016)

Prieto Gutiérrez, J. J. (2009). Seguridad en bibliotecas. *Revista seguritecnia*, 355, 60-64**.** Recuperado de http://eprints.ucm.es/9505/ (Consultado el 28/02/2017)

Ramírez, O. J. (2009). Riesgos de origen tecnológico: apuntes conceptuales para una definición, caracterización y reconocimiento de las perspectivas de estudio del riesgo tecnológico. *Luna azul, 29*, 82-94. Recuperado de http://www.scielo.org.co/pdf/luaz/n29/n29a08 (Consultado el 14/03/2017)

Ramírez Castro, A. y Ortiz Bayona, Z. (2011). Gestión de riesgos tecnológicos basada en ISO 31000 e ISO 27005 y su aporte a la continuidad de negocios. *Ingeniería, 16*(2), 56-66. Recuperado de http://revistas.udistrital.edu.co/ojs/index.php/reving/article/view/3833/5399 (Consultado el 04/04/2017)

Rozen, C. F. (2011). *La gestión de riesgos también puede ser expuesta ante las partes interesadas*. Buenos Aires: UCEMA. Recuperado de http://www.ucema.edu.ar/sites/default/files/publicaciones/2011/revista_temas_de_management_jul_2011.pdf (Consultado el 14/03/2017)

Sena, L. y Tenzer, S. M. (2004). *Introducción al riesgo Informático*. Cátedra *Introducción* a la Computación. Montevideo: Universidad de la República, Facultad de Ciencias Económicas y de Administración. Recuperado de http://www.academia.edu/14745302/Estructura_del_documento_de_riesgos_inform%C3%A1ticos (Consultado el 13/03/2017)

Universidad Católica de Córdoba, Sistema de Bibliotecas. (2016). *Política de gestión integral de riesgos 2016*. Córdoba: Universidad Católica de Córdoba. Recuperado de http://www2.ucc.edu.ar/biblioteca/archivos/File/2016%20Politica%20de%20Gestion%20de%20riesgos.pdf (Consultado el 05/03/2017)

Varela Orol, C. (2009). La gestión de la tecnología en las bibliotecas. *Boletín de la Asociación Andaluza de Bibliotecarios*, *24*(94-95), 27-45. Recuperado de http://www.redalyc.org/pdf/353/35313092003.pdf (Consultado el 28/02/2017)

Voutssas, M. J. (2010). Preservación documental digital y seguridad informática. *Investigación bibliotecológica*, *24*(50), 127-155. Recuperado de http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0187-358X2010000100008&lng=es&tlng=es (Consultado el 28/02/2017)

Zulueta, Y., Despaigne, E. y Hernández, A. (2009). La gestión de riesgos en la producción de software y la formación de profesionales de la informática: experiencias de una universidad cubana. *REICIS. Revista española de innovación, calidad e ingeniería del software, 5*(3), 6-20. Recuperado de http://www.redalyc.org/articulo.oa?id=92217181003(Consultado el 05/03/2017)