TENDÊNCIAS ATUAIS E PERSPETIVAS FUTURAS EM ORGANIZAÇÃO DO CONHECIMENTO

ATAS DO III CONGRESSO ISKO ESPANHA-PORTUGAL
XIII CONGRESSO ISKO ESPANHA

Universidade de Coimbra, 23 e 24 de novembro de 2017

Com a coordenação de

Maria da Graça Simões, Maria Manuel Borges

TÍTULO
Tendências Atuais e Perspetivas Futuras em Organização do Conhecimento: atas do III Congresso ISKO Espanha e Portugal - XIII Congresso ISKO Espanha

COORDENADORES
Maria da Graça Simões
Maria Manuel Borges

EDIÇÃO
Universidade de Coimbra. Centro de Estudos Interdisciplinares do Século XX - CEIS20

ISBN
978-972-8627-75-1

ACESSO
https://purl.org/sci/atas/isko2017

OBRA PUBLICADA COM O APOIO DE

PROJETO UID/HIS/00460/2013

COMPUTAÇÃO EM NUVEM E SISTEMAS DE GESTÃO DOCUMENTAL: AVALIAÇÃO DE RISCOS E RECOMENDAÇÕES

Ariovaldo Veiga de Almeida[1], Maria Cristina Vieira de Freitas[2]

[1]*Universidade de Coimbra, 0000-0001-9563-2657, ari@student.uc.pt*
[2]*Universidade de Coimbra, 0000-0002-8849-8792, cristina.freitas@fl.uc.pt*

RESUMO Atualmente, as informações são geradas numa velocidade espantosa. Segundo estudo da empresa *International Data Corporation* (IDC) estima-se que até o ano 2020 o crescimento de informações digitais deve chegar a 40000 *exabyte* e que aproximadamente 40% do total de informações geradas estarão armazenadas na Nuvem. Assim sendo, os sistemas de informação passam a gerir uma grande quantidade de dados armazenados localmente ou na Nuvem, intensificando-se os riscos de perda ou extravio de informações. Este estudo, de natureza exploratória e descritivo-prescritiva, tem como objetivo identificar características essenciais e modelos de serviços na Nuvem, bem como fatores associados à gestão de riscos na sua implementação e na sua utilização. Como resultado, identificamos os principais riscos e formas de os mitigar, balizados por diretrizes internacionais, concluindo que as boas práticas recomendadas pelas normas analisadas não configuram manuais de procedimentos, devendo, cada organização, avaliar de forma detalhada e específica as suas próprias necessidades técnicas e econômicas, na adoção de serviços em Nuvem, amparando-se em estudos de custos, riscos e benefícios.

PALAVRAS-CHAVE *Armazenamento de dados, Gestão de riscos, Computação em Nuvem, Sistemas de gestão documental.*

ABSTRACT Currently, the information is generated at an astounding speed. According to a study done by International Data Corporation (IDC), it is estimated that, by the year 2020, the growth of digital information should reach 40,000 exabytes and that approximately 40% of the total information generated will be stored in the Cloud. As such, information systems manage a large amount of data stored locally or in the Cloud, intensifying the risks of loss of information. This exploratory and descriptive-prescriptive study aims to identify essential characteristics and service models in the Cloud, as well as factors associated with risk management in its implementation and use. As a result, based on international guidelines, we identify the main risks and ways to mitigate them, concluding that the good practices recommended by the standards analyzed do not configure a procedure to be followed, each organization should evaluate in detail its own technical and economic needs in adopting cloud services, based on analyses of cost, risk, and benefits studies.

KEYWORDS *Data storage, Risk management, Cloud computing, Document management systems.*

INTRODUÇÃO

Atualmente, o crescimento das informações digitais é muito significativo, com a estimativa de se tornar 50 vezes maior em 2020 (Luo, Wu, Gopukumar & Zhao, 2016; Machovec, 2014; Madrid, 2013; Sosa-Sosa & Hernandez-Ramirez, 2012).

Um número crescente de organizações públicas ou privadas possui Sistemas de Gestão Documental (SGD), usados para produzir, gerir e armazenar documentos e informações, mediados por tecnologias computacionais. Estes sistemas são considerados estratégicos, pois simplificam e flexibilizam a forma como a infraestrutura computacional e de armazenamento de dados é disponibilizada, trazendo benefícios nos custos de implementação, administração, manutenção e escalabilidade. Como garantia do seu bom funcionamento, as organizações devem implementar formas eficazes de controlo, para que os documentos, bem como as informações, permaneçam confiáveis, compreensivos, sistemáticos, íntegros e usáveis pelo tempo que forem requeridos (Antonio et al., 2014; Bushey, Demoulin, & McLelland, 2015; Ferreira, 2012; Machovec, 2014; Noh, 2015; Pires, 2016; Poulo, 2013; Shaw, 2013; Sosa-Sosa & Hernandez-Ramirez, 2012; Wilson, 2012).

Neste contexto, releva a segurança. Segundo Bernstein (1996 cit. por Massingham, 2010, p. 465) "[...] o risco é uma escolha e não destino" e "[...] mesmo quando não podemos eliminar o risco, devemos, pelo menos, antecipá-lo e, assim, colocarmos em ação processos que possam reduzir o seu impacto". Ainda, segundo Massingham (2010), tragédias como o ataque terrorista às torres do *World Trade Center* ou a fraude fiscal da empresa Enron®, ocorridas em 2001, ou, ainda, desastres naturais, como o tsunami ocorrido no Oceano Índico, em 2004, aumentam em nós a consciência do risco e das suas consequências.

Os riscos associados à inacessibilidade, vazamento, roubo, extravio ou perda de informações devem ser avaliados e fazer parte da política de segurança das organizações, pois afetam diretamente o funcionamento e a prestação de contas, colocando em risco, no limite, a sua existência (Ali, Khan, & Vasilakos, 2015; Borglund, 2015; Chaves, 2011; Chou, 2015; Dias, Rodrigues, & Pires, 2012; Massingham, 2010; Ostrzenski, 2013; Popovic & Hocenski, 2010; Vurukonda & Rao, 2016; Zissis & Lekkas, 2012).

Partindo destes pressupostos, este estudo centra-se numa revisão teórica de textos recentemente publicados, o que lhe confere uma perspetiva atualizada do problema, procurando responder aos seguintes objetivos: i) identificar características e modelos de serviços na Nuvem, ii) bem como fatores relacionados à gestão de riscos na sua implementação e utilização, especialmente nos SGD; iii) apresentar um leque mínimo de boas práticas e de orientações a adotar, para mitigar esses mesmos riscos, amparando-se em modelos de referência internacionalmente válidos.

METODOLOGIA

Trata-se de um estudo de revisão, baseado numa abordagem exploratória e descritivo-prescritiva, de cunho tendencial, apoiada numa amostra intencional de textos científicos e de documentos normativos, recolhidos por meio de pesquisa bibliográfica e documental. Os documentos recuperados foram publicados, na sua maioria, no período de 2011 a 2017. As consultas foram realizadas em múltiplas

bases de dados disponibilizadas no Portal agregador de conteúdos B-On[1]. Para complementar esses resultados, recorreu-se a outros estudos disponíveis e com elevados índices de citação, no Google *Scholar*[2]. Resumidamente, as buscas foram realizadas do seguinte modo (figura 1):

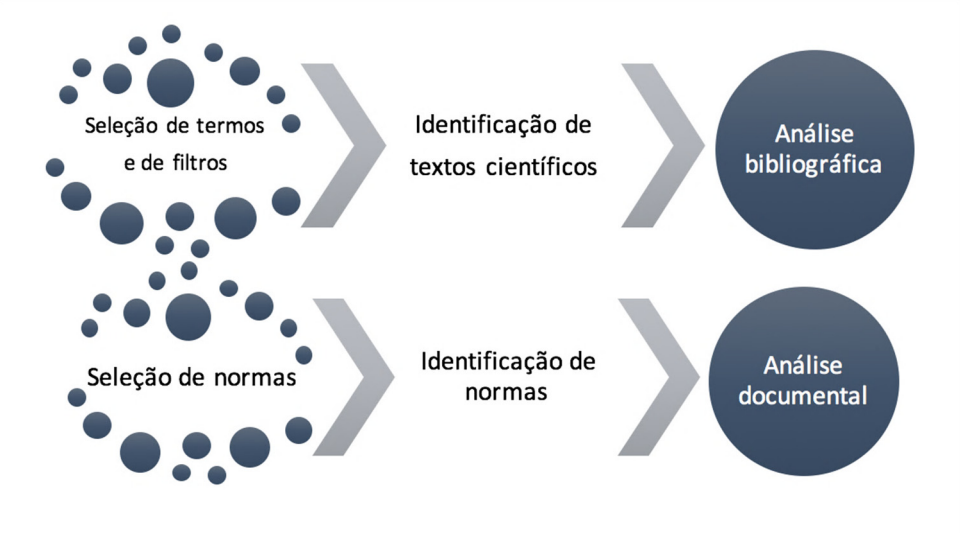

Figura 1. Procedimentos de busca adotados.

Fonte: Elaboração nossa.

Os termos de busca utilizados, isoladamente ou de forma combinada, foram: "*records management*", "*Cloud storage*", "*risk management*", "*archives*" e "*documentation*". Os filtros utilizados foram: Biblioteconomia e Ciência da Informação (área); Inglês e Português (idioma); Revistas acadêmicas, texto integral e revisto por especialistas (fontes). Feitas estas diligências, foram recuperados 220 artigos, dos quais foram selecionados 38 para compor a revisão, com base na leitura das seguintes secções: resumo, introdução e conclusão.

Entre as várias organizações internacionais preocupadas com criação de normas e de procedimentos para mitigar os riscos do uso de serviços de Nuvem, neste estudo, foram avaliados os documentos disponibilizados por apenas três delas, escolhidas pela sua abrangência e atuação, à escala mundial, bem como pelas citações contabilizadas nos vários documentos utilizados na pesquisa bibliográfica. Deste modo, as normas técnicas foram identificadas em portais de instituições credenciadas, a saber: i) *International Organization for Standardization* (ISO), ii) *National Institute of Standards and Technology* (NIST) e iii) *Cloud Security Alliance* (CSA).

Terminada a fase de recolha de dados, passou-se à fase de análise, que, neste estudo, limitou-se à reflexão das ideias principais contidas nos textos pesquisados, que ajudaram a responder aos objetivos de pesquisa delineados, gerando-se, assim, os tópicos incluídos nos resultados, discussão e conclusão.

[1] Disponível em: http://www.b-on.pt.
[2] Disponível em: https://scholar.google.com.

RESULTADOS

A COMPUTAÇÃO E O ARMAZENAMENTO DE DADOS NA NUVEM: CARACTERÍSTICAS, MODELOS E IMPLICAÇÕES

Em computação, o termo "Nuvem" terá sido usado pela primeira vez em 1996, pela empresa Compaq® (Regalado, 2011) num plano de negócios da empresa. Academicamente, estima-se que tenha sido empregue primeiramente pelo Prof. Ramnath Chellappa da Escola de Negócios da *Emory Universisty*, no encontro do *Institute For Operations Research and the Management*, em 1997 (INFORMS, 1997). A computação em Nuvem, entretanto, terá raízes mais antigas. Em 1961, o Prof. John McCarthy, pioneiro cientista de computação, já havia abordado o conceito de "*Utility Computing",* segundo o qual a computação seria adquirida num sistema *pay per use*, de forma semelhante aos outros serviços consumidos diariamente e pagos regularmente (tais como: energia elétrica, água e gás).

Algumas tentativas de descrever o fenómeno têm falhado por não considerar variáveis como diversas tecnologias, configurações e modelos de serviços e de implementação que podem ser usados. Nesse sentido, o NIST, em 2011, publicou um modelo conceitual de Nuvem (Meel & Grance, 2011, p2-3) (figura 2), explicitando cinco características essenciais, três modelos de serviços e quatro modelos de implementação, culminando, no ano seguinte, com as recomendações e chamadas de atenção para aspetos como: oportunidades e riscos, pontos fortes e pontos fracos (Badger, Patt-corner, & Voas, 2012), sendo estes os componentes típicos da Análise *SWOT*[3].

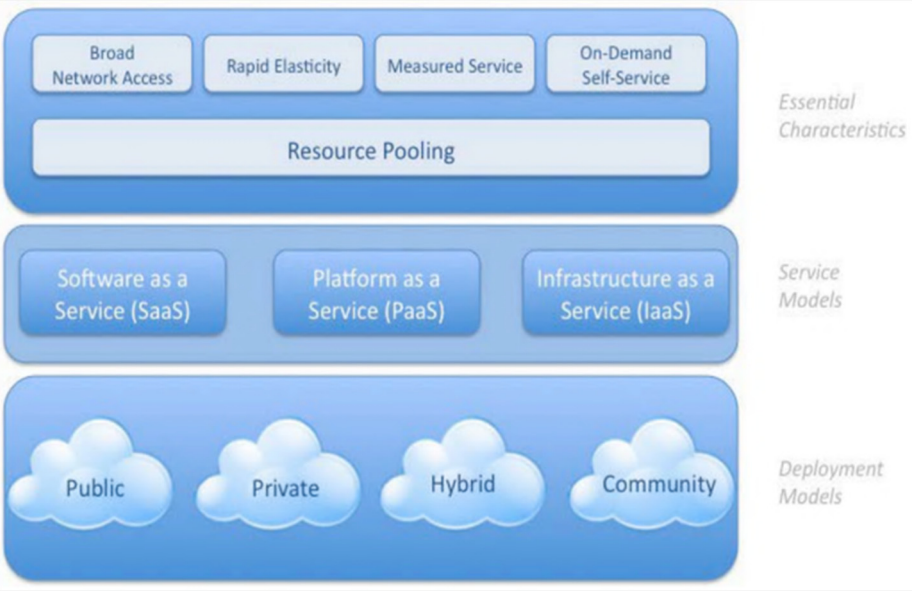

Figura 2. Modelo conceitual de computação em Nuvem, segundo o NIST (2011).

Fonte: (Archer et al., 2011, p.13)

Como vemos na figura 2, as cinco características essenciais da computação em Nuvem apresentadas pelo NIST, de 2011, são: a disponibilidade imediata, o autosserviço, o amplo acesso à rede, a

[3] Análise SWOT (*Strengths, Weaknesses, Opportunities e Threats*) ferramenta estrutural da administração utilizada para avaliar os ambientes, sendo usada como base para a gestão e planejamento estratégico de uma empresa.

possibilidade de adquirir um conjunto de recursos agregados, a rápida elasticidade e a mensurabilidade dos serviços. A estas, a instituição CSA, através do relatório publicado em 2011 (Archer et al., 2011), acrescenta uma sexta característica, que corresponde à segregação de serviços (*Multi-Tenency*). Ainda, segundo a mesma diretriz do NIST, de 2011, são três as categorias ou modelos básicos de serviços oferecidos pela computação em Nuvem: o software como serviço, a plataforma como serviço e a infraestrutura como serviço. Finalmente, a mesma diretriz identifica quatro modelos básicos de implementação de uma infraestrutura de computação em Nuvem: privado, público, comunitário e híbrido.

À medida que a computação em Nuvem se torna mais madura e passa a ser utilizada pelas organizações, gerir as oportunidades e os desafios de segurança e, assim, minimizar os riscos, apresenta-se como crucial para o desenvolvimento dos seus processos de negócio.

Ao contrário do que usualmente acontece num ambiente computacional tradicional, a migração para a Nuvem implica perda da barreira de proteção da infraestrutura. Com a sua adoção, a segurança passa a concentrar-se nos aplicativos e na forma como são manipulados os dados, que precisarão de uma segurança própria que os acompanhe e os proteja. Isso implicará o seu completo isolamento, já que precisam ser mantidos em segurança, para que fiquem resguardados quando vários clientes usarem os recursos compartilhados pela infraestrutura.

Assim que migram seus ambientes de computação para a Nuvem, com suas respetivas identidades, infraestrutura e informações, as instituições se veem na iminência de abrir mão de certos níveis de controlo. No caso das Nuvens públicas, a migração exige um modelo de segurança de informação que concilie a capacidade de expansão e de multialocação de recursos computacionais, sendo necessário confiar nos sistemas e nos provedores, para além de executar verificações periódicas nos sistemas. Fazem parte desse processo de confiança e de verificação: o controlo dos acessos, a segurança dos dados, a gestão e a monitorização contínua de eventos e de informações. Também é importante que a virtualização e a criptografia permitam níveis alternativos de separação entre corporações, utilizadores e comunidades de interesse. Em resumo, trata-se de todos os elementos de segurança que são compreendidos por um departamento específico, implantados com a tecnologia existente e com possibilidade de extensão para a Nuvem.

Assim, a adoção da Nuvem exige um olhar acurado para os riscos que o uso desses serviços pode acarretar. Num tal sentido, as organizações devem empregar práticas de gestão de segurança e de controlo apropriadas à computação em Nuvem, essenciais para operar e manter uma solução segura de um serviço desse porte e com essas características. As atividades de segurança e de privacidade implicam, como vimos, monitorizar os ativos do sistema de informações da organização e avaliar a implementação de políticas, padrões, procedimentos e diretrizes, usados para estabelecer e preservar a confidencialidade, a integridade e a disponibilidade dos recursos nos sistemas de informação.

A PERSPETIVA NORMATIVA DA GESTÃO DE RISCOS NAS ORGANIZAÇÕES E NOS SISTEMAS DE GESTÃO DOCUMENTAL

O risco é definido como um evento ou uma sucessão de eventos não esperados, que afetam as organizações e os seus sistemas, manifestando-se pela perceção dos seus efeitos (ISO 18128-2014, 2014). Num tal sentido, e de acordo com (Massingham, 2010, p.469) os riscos podem ser classificados pelos seguintes parâmetros (figura 3):

Table Risk consequence

Description	*Definition*
Catastrophic	Failure would prevent the organization from meeting the primary operational requirements
Critical	Failure would significantly degrade the organization's ability to perform its primary mission
Major	Failure would result in temporary loss of one or more significant capabilities within the organization
Minor	Failure would result in temporary degradation or loss of one or more capabilities within the organization

Figura 3. Tabela de classificação de riscos.

Fonte: Massingham, (2010, p. 469).

Note-se que, sendo mais graves, os riscos considerados catastróficos e críticos, pelo impacto sistémico, inibem as organizações do exercício da sua missão, podendo, no limite, decretar o seu encerramento. Assim sendo, é importante identificar e avaliar, o quanto antes, esses tipos de riscos, escolhendo-se as formas de os controlar e mitigar.

No campo normativo, destacam-se pelo menos dois dispositivos elaborados pela ISO e diretamente relacionados à gestão de riscos. O primeiro, de caráter geral – ISO 31000:2009: *Risk management: principles and guidelines –,* oferece princípios e orientações, bem como elenca os processos envolvidos na gestão dos riscos organizacionais. O seu uso estende-se aos diversos tipos de instituições, independentemente do tamanho, da atividade ou do setor de atuação. Essa norma oferece os requisitos necessários à identificação de oportunidades e de ameaças, para além de apoiar as organizações em tarefas de alocação e de uso efetivo de recursos no tratamento dos riscos. Os seus principais pontos, conforme (Lark, 2015), podem ser visualizados no esquema a seguir (figura 4):

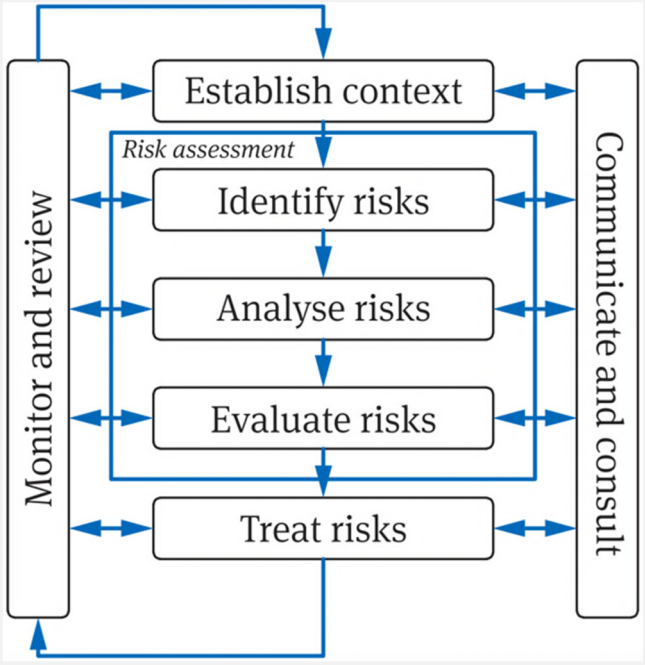

Figura 4. Processo de gestão de riscos segundo a norma ISO 31000:2009.

Fonte: (Lark, 2015, p.14)

Note-se que o processo preconizado pela norma segue um fluxo que inicia com o estabelecimento de um contexto de definição do risco a ser avaliado e prossegue com a sua identificação, análise, avaliação e tratamento. Em cada passo do processo, estão previstas, por um lado, atividades de avaliação periódica, por meio de monitorização e de revisão, e, por outro, atividades de comunicação e de consultoria. Dito diagrama demonstra, ademais, a complexidade e a necessidade de conectividade e de continuidade entre as diversas fases do processo, bem como o seu caráter proativo e reativo.

E, porque há riscos que não se evitam, mas que se controlam, segundo essa mesma norma, a sua gestão deve ir além da adoção de medidas preventivas. Trata-se, pois, de uma tomada de consciência dos riscos que, sendo ou não evitáveis, afetam a organização, de modo monitorizar a sua evolução nos diversos aspetos envolvidos (físicos, ambientais, financeiros e sociais). Num tal sentido, a avaliação deve responder às seguintes questões (figura 5):

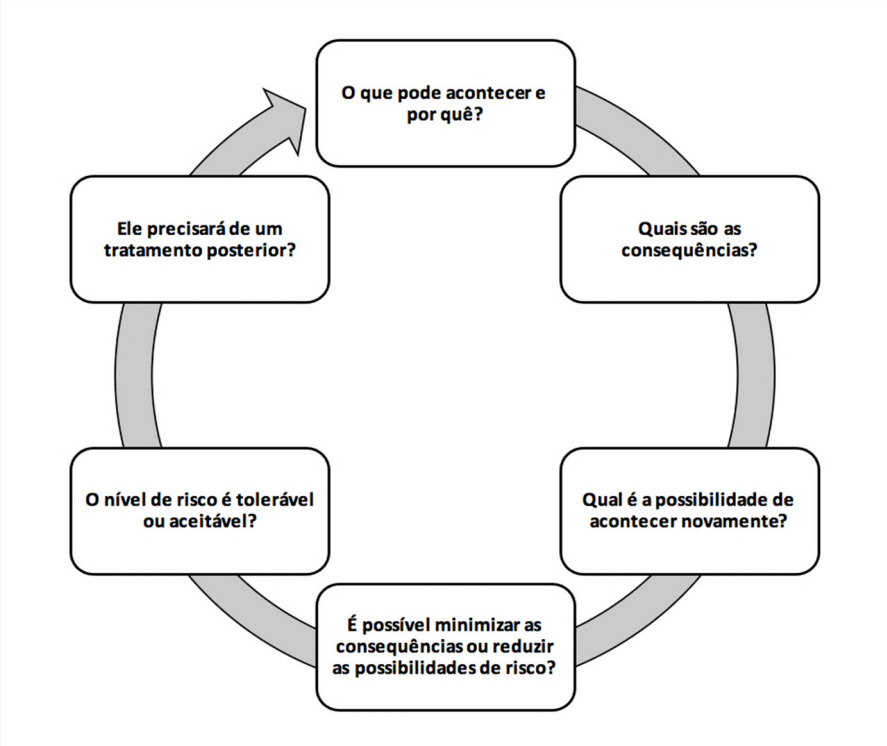

Figura 5. Monitorização dos riscos.

Fonte: Elaboração própria, com base em: (ISO31000-2009, 2009).

Com um caráter específico e de aquisição mais recente, é a norma ISO/TR18128:2014: *Information and documentation: risks assessement for records processes and systems*. Publicada em forma de relatório técnico, trata-se de uma transposição de conceitos e de procedimentos utilizados na norma ISO 31000:2009 para o âmbito da gestão documental. Portanto, esta norma tem como objetivo apoiar diretamente os responsáveis pelos documentos de arquivo, em tarefas de identificação, análise e avaliação dos riscos relacionados aos sistemas[4] e aos processos de gestão da documentação produzida

[4] Na aceção dada pela norma ISO 18128:2014, sistema é qualquer aplicação que cria ou armazena os documentos de arquivo, assegurando que os mesmos, ao serem produzidos, usados e geridos pela organização continuem a atender às suas necessidades de negócio pelo tempo que forem necessários.

e acumulada pelas organizações[5], independentemente do suporte ou do formato. Pelo seu teor, oferece subsídios e diretrizes que contribuem para a implementação de um método de análise eficaz na identificação dos riscos relacionados a esses processos e sistemas, incluindo os fatores externos e os internos suscetíveis de ser encontrados em vários ambientes organizacionais, bem como os seus potenciais efeitos e as formas de os mitigar (ISO 18128-2014, 2014), como podemos visualizar na figura 6.

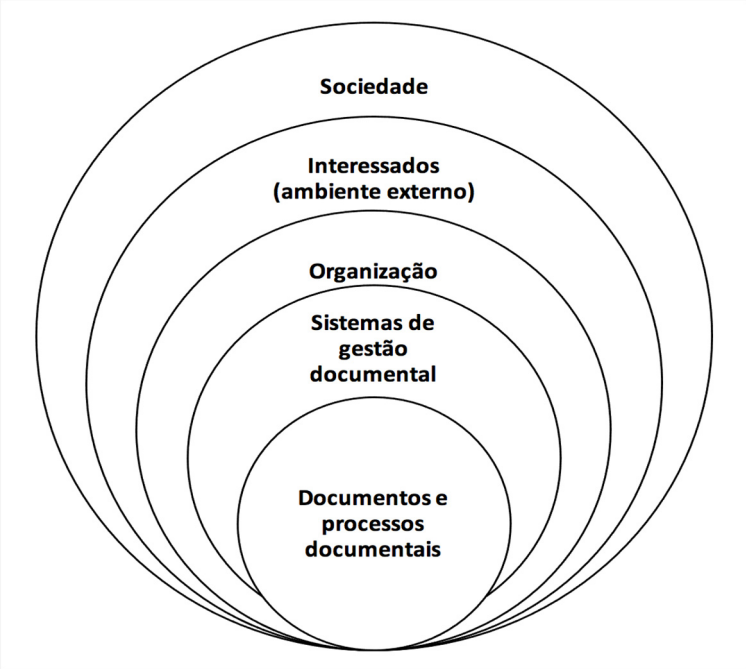

Figura 6. Camadas de intervenção no processo de gestão de riscos nos SGD.

Fonte: Adaptado de ISO 18128:2014 (p. 10).

Saliente-se que a responsabilidade pela identificação e pela gestão dos riscos, nesse caso, recai sobre o profissional da respetiva área (i.é., os arquivos organizacionais), sendo esta uma atividade distinta daquelas em que são identificados e avaliados outros tipos de riscos, que também afetam o bom funcionamento da organização.

Quanto aos impactos, a consequência mais grave associada a um evento de risco em sistemas dessa natureza será a perda ou a danificação irremediável dos documentos, tornando-os inutilizáveis, não confiáveis, inautênticos ou incompletos e, como tal, falhando o próprio sistema em atender aos propósitos da organização. Dada a gravidade, ditada pela extensão da perda, sugere-se que as análises de riscos a realizar nesses sistemas sejam incorporadas às pautas prioritárias das organizações. Os benefícios mais evidentes desta medida seriam um maior e melhor controlo dos documentos, com garantias de preservação da sua integridade, ao longo do tempo, bem como da sua qualidade e do seu uso efetivo, cumprindo-se assim os objetivos para os quais os mesmos são criados (ISO 18128:2014, p. 2).

[5] Esta norma pode ser usada por qualquer organização pública, privada ou comunitária, associação, grupo ou indivíduo que produza e/ou detenha arquivos.

Porquanto, no contexto dos arquivos, a computação em Nuvem oferece tanto atrativos - inovação, desenvolvimento de serviços, eficiência, economia, escalabilidade e flexibilidade, entre outros - quanto riscos associados a aspetos tais como: segurança, privacidade, integridade, autenticidade, acessibilidade e preservação de informação. Quanto a esta última, refira-se a pouca transparência no que toca à continuidade comercial dos serviços prestados pelas empresas da área. Porquanto, para minimizar os riscos e maximizar os benefícios, devem adotar-se procedimentos estandardizados e recomendados (Mckemmish, 2013, p.19). Nesse sentido, quer o cliente, quer o fornecedor dos serviços devem conciliar os seus interesses e requisitos, aquando da implementação de processos de arquivo em Nuvem (Stancic, Rajh, & Brzica, 2015, p214-216). Ainda, uma estrutura simples e eficaz, nesse processo, poderia ser a seguinte (figura 7):

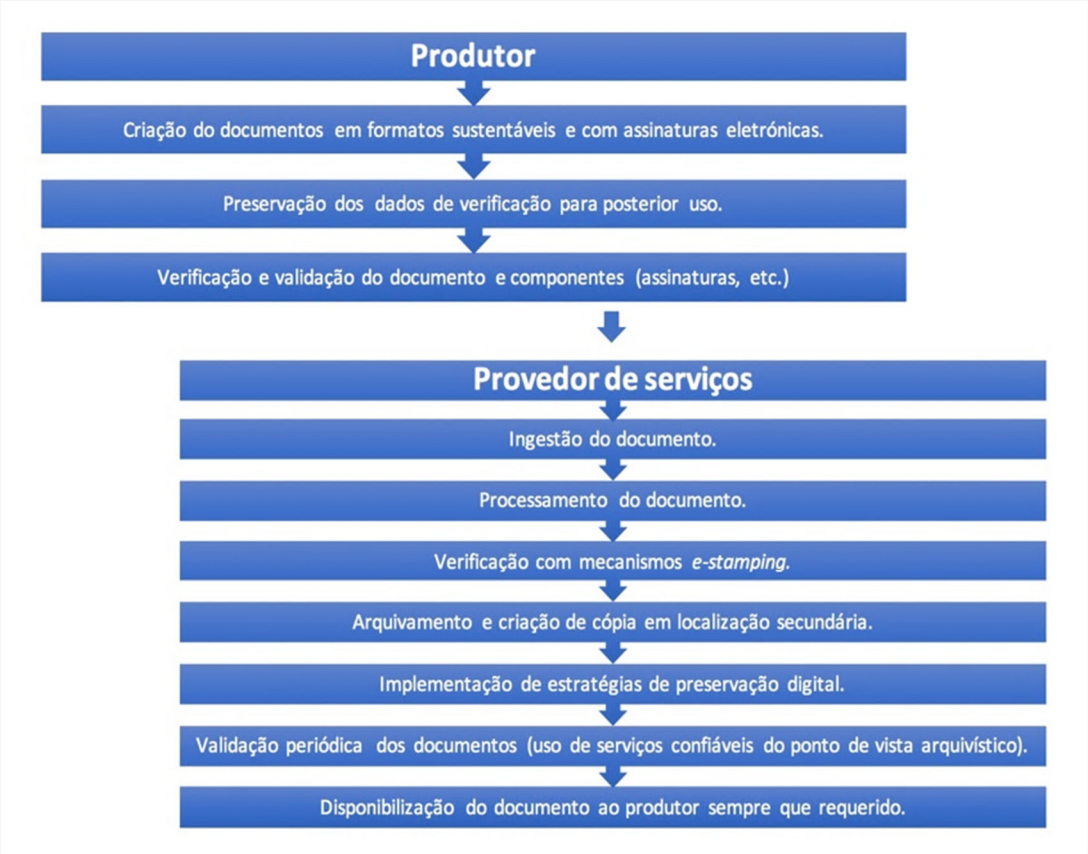

Figura 7. Processo de fornecimento de serviços em Nuvem para arquivos.

Fonte: Elaboração nossa, a partir de Stancic, Rajh e Brzica (2015, p.214-216).

Por seu turno, o Projeto *InterPARES Trust* (2017), de envergadura internacional e com um incontestável prestígio no meio arquivístico, e não só, torna-se num ponto de referência obrigatório para quem pretende desenvolver projetos de migração de arquivos para a Nuvem. Para além de desenvolver o conceito de confiança (*Trust*) e de elencar uma série muito ampla de requisitos necessários à sua obtenção, em níveis aceitáveis e nesses tipos de sistemas, o Website desse megaprojeto internacional recolhe, organiza, descreve e divulga, a toda a comunidade interessada, um vasto leque de projetos de pesquisa e de programas desenvolvidos internacionalmente e que se apresentam como casos de sucesso ou modelos a ser seguidos e/ou adaptados, porque levam consigo a aprovação do *InterPares Trust.* Vale dizer que muitas dos resultados e das recomendações desse projeto, que vem sendo desenvolvido há

vários anos (entre 2013 e 2018) encontram-se espelhados nas normas e noutros documentos citados por este estudo.

O CONTROLO DE RISCOS NA PERSPETIVA DAS ORIENTAÇÕES INTERNACIONAIS

Recomendações do NIST

Em 2011, O NIST elaborou as *Guidelines on security and privacy in public cloud computing*, identificando os desafios à segurança e à privacidade na computação em Nuvem pública. Esse documento é voltado às diversas categorias de profissionais: decisores, profissionais de segurança, auditores, administradores de sistemas e de redes, utilizadores de serviços, entre outros. Devido à natureza evolutiva do tema, o próprio NIST recomendou o uso combinado desse documento com recursos complementares.

Quanto às recomendações, elas podem ser sumariadas do seguinte modo (figura 8):

Figura 8. Recomendações do NIST (2011) para a segurança na computação em Nuvem.

Fonte: Elaboração nossa.

Recomendações da CSA

A CSA é uma organização mundial, sem fins lucrativos, que visa promover as boas práticas de segurança em Computação em Nuvem. Fundada em 2008, é uma organização que conta com profissionais da indústria com conhecimentos especializados em Nuvem, associações, governos e

membros corporativos e individuais, e visa oferecer pesquisas, treinamento, certificação, eventos e produtos relacionados especificamente à segurança na Nuvem (CSA, 2017).

As principais recomendações da CSA estão contidas no documento *CSA Security guidance for critical areas of focus in Cloud Computing*, publicado em 2009, e revisado em 2011 (Archer et al., 2011). Trata-se de uma ampla compilação de ideias de mais de setenta peritos internacionais da indústria, embora reconhecendo a abrangência do tema e a inviabilidade de incluir num único documento todos os possíveis cenários e variações.

O guia serve como sustentação na avaliação dos riscos na implementação da computação em Nuvem, incluindo decisões de segurança. Apresenta uma lista de verificação muito simples, em cinco etapas, usada para avaliar a tolerância de um cliente ao mover seus ativos para um dos vários modelos de computação em Nuvem, conforme se observa na figura 9:

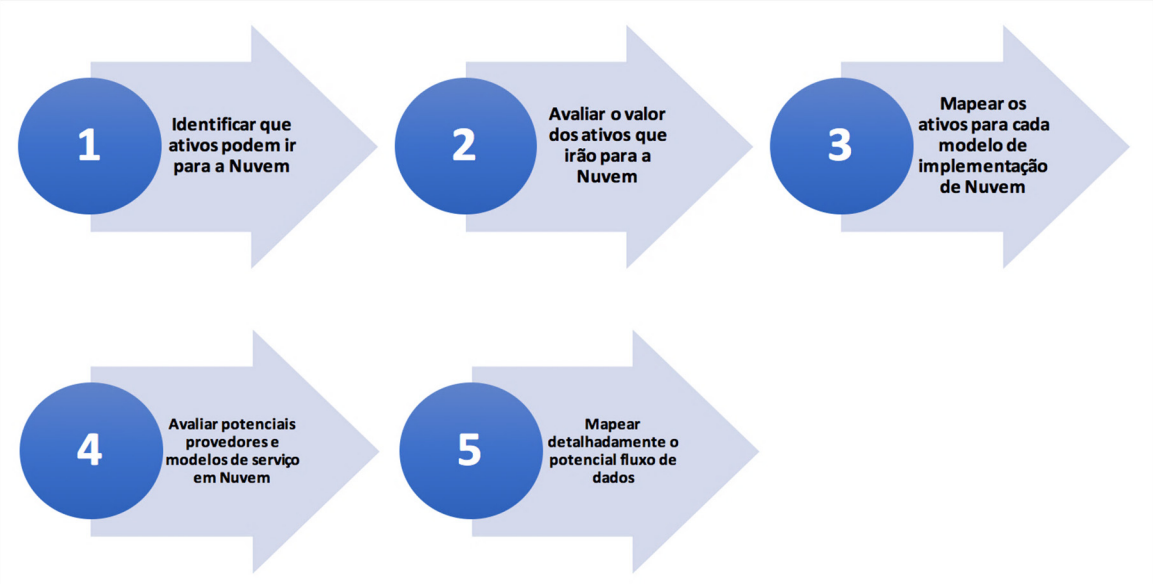

Figura 9. Recomendações da CSA (2011) para a segurança na computação em Nuvem.

Fonte: Elaboração nossa, a partir de (Archer et al., 2011).

DISCUSSÃO E CONCLUSÃO

Segundo Massingham (2010), mesmo quando não podemos eliminar o risco, devemos, pelo menos, tentar antecipá-lo e, assim, colocarmos em ação processos que possam reduzir o seu impacto negativo. Essa colocação se aplica à decisão das organizações na adoção ou não da Nuvem. Da mesma forma que Massingham (2010) menciona que o risco é uma escolha e não um destino, as organizações atualmente possuem muitas escolhas e diversas orientações sobre como devem implementar os seus sistemas computacionais. Atualmente, a adoção da Nuvem é uma excelente opção para as organizações, em geral, devido aos custos envolvidos, aos modelos de serviços e à sua simplicidade de utilização.

As organizações podem optar pela utilização da Nuvem Privada (dentro da própria organização), pela Nuvem Pública (fora da organização), ou por uma mistura delas; mas, como é bom de ver, dependendo da escolha adotada, os riscos serão diferentes, sendo necessário avaliá-los e medi-los.

Um dos principais pontos de discussão, em relação à adoção, ou não, de serviços em Nuvem, prende-se com a capacidade de implementação de um sistema paralelo de medição de riscos. Num tal sentido, são imprescindíveis as normas técnicas e as orientações internacionalmente reconhecidas, das quais trouxemos alguns muito bons exemplos para este estudo. Como vimos, elas oferecem princípios, regras e modelos simples, mas aplicáveis em variados casos, contextos e processos de negócio. Entretanto, e dado o seu caráter geral, ditos dispositivos não proporcionam métodos de análise específicos, sendo esta, naturalmente, uma sua limitação. Com isso, quer-se dizer que uma dada organização pode possuir diversos sistemas e aplicações, devendo, por isso, avaliar, para cada um deles, a viabilidade da adoção da Nuvem, e tomar as suas próprias decisões em função dos riscos observados.

Os processos e os SGD beneficiam-se de princípios e de instruções normativas específicas, dada sua importância para as organizações, quer no registo das suas atividades, quer na prestação de contas e na preservação da memória organizacional. Ditos sistemas fazem parte desse modelo de tecnologias de informação, possuindo, em muitos casos, versões específicas para a Nuvem, escolhidas pela fácil implementação, pelos custos acessíveis e pela escalabilidade. Apesar dessas vantagens, aqui também os riscos são inerentes ao processo e é preciso identificá-los, avaliá-los e tratá-los (pela mitigação ou pela erradicação), adotando medidas de segurança e de monitorização contínua desses sistemas, em tarefas de avaliação periódica.

As organizações devem, pois, empregar práticas de segurança e controlo apropriadas à computação em Nuvem, sem as quais não conseguem manter uma solução confiável de serviço. Avaliar e controlar os riscos nesses sistemas é, desse modo, um desafio e uma meta a atingir. Tanto os indicadores qualitativos quanto os quantitativos podem aplicar-se, devendo ser cuidadosamente ponderados em relação às garantias técnicas, gestionárias e operacionais, tomando-se as medidas necessárias para os reduzir a um nível aceitável.

Pelo exposto, conclui-se que a decisão pela adoção ou não da Nuvem como modelo é inerente a cada organização e deve estar diretamente relacionada com o seu modelo de negócios, para além de aspetos como: custos, administração, localização geográfica, políticas de *compliance*, entre outros aspetos.

As normas referenciadas nesse estudo ajudam na avaliação e análise de riscos trazendo recomendações que são fontes de grande importância para as organizações, porém, a decisão de seus gestores na adoção ou não de serviços de Nuvem deve ser baseada, não somente em fatores financeiros, mas ter em conta os seus objetivos de negócio e os riscos associados às suas próprias decisões.

REFERÊNCIAS BIBLIOGRÁFICAS

Ali, M., Khan, S. U., & Vasilakos, A. V. (2015). Security in cloud computing: Opportunities and challenges. *Information Sciences*, *305*, 357–383. https://doi.org/10.1016/j.ins.2015.01.025

Antonio, R., Monteiro, A., Guimarães, B., Meneses, É., Ledesma, F., Nunes, H., … Ferreira, S. (2014). A Gestão Documental na Governança da Informação. *APDSI*, 357. Retrieved from http://www.apdsi.pt/uploads/news/id844/Gestão Documental 2014_20141111.pdf

Archer, J., Boehme, A., Cullinane, D., Kurtz, P., Puhlmar, N., & Reavis, J. (2011). *CSA Security Guidance for Critical Areas of Focus in Cloud Computing V3.0*. Retrieved from http://www.cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf

Badger, L., Patt-corner, R., & Voas, J. (2012). NIST Cloud Computing Synopsis and Recommendations Recommendations. *Nist Special Publication*, *800*(146), 81. https://doi.org/2012

Borglund, E. A. M. (2015). What About Trust in the Cloud? Archivists' Views on Trust. *Canadian Journal of Information and Library Science-Revue Canadienne Des Sciences De L Information Et De Bibliotheconomie*, *39*(2), 114–127.

Bushey, J., Demoulin, M., & McLelland, R. (2015). Cloud Service Contracts: An Issue of Trust / Les contrats de service d'informatique en nuage: Une question de confiance. *Canadian Journal of Information and Library Science*, *39*(2), 128–153. Retrieved from https://muse.jhu.edu/journals/canadian_journal_of_information_and_library_science/v039/39.2.bushey.html

Chaves, S. (2011). *A Questão dos Riscos em Ambientes de Computação em Nuvem*. Universidade de São Paulo.

Chou, D. C. (2015). Cloud computing risk and audit issues. *Computer Standards & Interfaces*, *42*, 137–142. https://doi.org/10.1016/j.csi.2015.06.005

CSA. (2017). About CSA. Retrieved January 23, 2017, from https://cloudsecurityalliance.org/about/

Dias, J. M. F., Rodrigues, R. de C. M. C., & Pires, D. F. (2012). A Segurança De Dados Na Computação Em Nuvens Nas Pequenas E Médias Empresas. *Revista Eletrônica de Sistemas de Informação E Gestão Tecnológica*, 56–69. Retrieved from http://periodicos.unifacef.com.br/index.php/resiget/article/view/287

Ferreira, O. (2012). *O Nivel de implementacao de Cloud computing nas empresas portuguesas*. Universidade Portucalense Infante D.Henrique.

INFORMS. (1997). Prof. Ramnath Chellappa. Retrieved January 23, 2017, from http://www.bus.emory.edu/ram/

InterPARES Trust. (n.d.). Retrieved July 16, 2017, from https://interparestrust.org/trust/about_research/studies

ISO. (2014). Are you in control of your records? Retrieved January 24, 2017, from http://www.iso.org/iso/news.htm?refid=Ref1830

ISO31000-2009. (2009). ISO31000:2009 - Risk management: Principles and guidleines. Retrieved from http://www.iso.org/iso/home/standards/iso31000.htm

ISO 18128-2014. (2014). ISO/TR18128:2014 - Information and documentation -- Risk assessment for records processes and systems Abstract. Retrieved from http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=61521

Lark, J. (2015). *ISO 31000 - Risk management - a practical guide for SMEs* (Vol. 22). https://doi.org/10.1093/rpd/ncr142

Luo, J., Wu, M., Gopukumar, D., & Zhao, Y. (2016). Big Data Application in Biomedical Research and Health Care: A Literature Review. *Biomedical Informatics Insights*, 1–10. https://doi.org/10.4137/BII.S31559.TYPE

Machovec, G. (2014). Consortia and Next Generation Integrated Library Systems. *Journal of Library Administration*, *54*(5), 435–443. https://doi.org/10.1080/01930826.2014.946789

Madrid, M. M. (2013). A study of digital curator competences: Asurvey of experts. *International Information and Library Review*, *45*(3–4), 149–156. https://doi.org/10.1016/j.iilr.2013.09.001

Massingham, P. (2010). Knowledge risk management: a framework. *Journal of Knowledge Management*, *14*(3), 464–485. https://doi.org/10.1108/13673271011050166

Mckemmish, S. (2013). Recordkeeping and Archiving in the Cloud . Is There a Silver Lining ? *INFuture*, 17–29. Retrieved from http://infoz.ffzg.hr/INFuture/2013/papers/1-02 McKemmish, Recordkeeping and Archiving in the Cloud.pdf

Meel, P., & Grance, T. (2011). *NIST Definition of Cloud Computing*. Retrieved from http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

Noh, Y. (2015). Imagining Library 4.0: Creating a Model for Future Libraries. *Journal of Academic Librarianship*, *41*(6), 786–797. https://doi.org/10.1016/j.acalib.2015.08.020

Ostrzenski, V. (2013). Cloud Computing and Risk : A look at the EU and the application of the Data Protection Directive to cloud computing. *Infopreneurship Journal*, *1*(1), 29–38. Retrieved from http://www.infopreneurship.net

Pires, I. (2016). *Os arquivos organizacionais e a normalização da gestão de documentos eletrónicos : análise de normas nacionais e internacionais (2001-2016)*. Universidade de Coimbra. Retrieved from https://estudogeral.sib.uc.pt/bitstream/10316/32941/1/DISSERTACAO APROVADA 09-09 ISABEL .pdf

Popovic, K., & Hocenski, Z. (2010). *Cloud computing security issues and challenges*. *MIPRO, 2010 Proceedings of the 33rd International Convention*.

Poulo, L. B. N. (2013). *Cloud Computing for Digital Libraries*. University of Cape Town.

Regalado, A. (2011). Who Coined Cloud Computing. *MIT Technology Report*. Retrieved from https://www.technologyreview.com/s/425970/who-coined-cloud-computing/

Shaw, A. K. (2013). Cloud Computing for Libraries: An Economic Strategy. *International Conference on Academic Libraries*, *1*(2), 162–167. Retrieved from http://eprints.rclis.org/19359/1/023_12_Amit Kumar Shaw_34.pdf%0A

Sosa-Sosa, V. J., & Hernandez-Ramirez, E. M. (2012). A file storage service on a cloud computing environment for digital libraries. *Information Technology and Libraries*, *31*(4), 34–45. https://doi.org/10.6017/ital.v31i4.1844

Stancic, H., Rajh, A., & Brzica, H. (2015). Archival Cloud Services: Portability, Continuity, and Sustainability Aspects of Long-term Preservation of Electronically Signed Records. *Les Services D'archivage Dans Un Nuage Informatique: Portabilité, Continuité et Durabilité: Aspects de La Conservation À Long Terme Des Documents Signés Électroniquement.*, *39*(2), 210–227. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,uid&db=lls&AN=109028640&site=ehost-live&scope=site

Vurukonda, N., & Rao, B. T. (2016). A Study on Data Storage Security Issues in Cloud Computing. *Procedia Computer Science*, *92*, 128–135. https://doi.org/10.1016/j.procs.2016.07.335

Wilson, K. (2012). Introducing the Next Generation of Library Management Systems. *Serials Review*, *38*(2), 110–123. https://doi.org/10.1016/j.serrev.2012.04.003

Zissis, D., & Lekkas, D. (2012). Addressing cloud computing security issues. *Future Generation Computer Systems*, *28*(3), 583–592. https://doi.org/10.1016/j.future.2010.12.006