DOI: 10.5433/1981-8920.2017v22n1p215

RECOMENDAÇÕES PARA CERTIFICAÇÃO OU MEDIÇÃO DE CONFIABILIDADE PARA REPOSITÓRIOS ARQUIVÍSTICOS DIGITAIS CONFIÁVEIS COM ÊNFASE NO ACESSO

RECOMENDACIONES PARA LA CERTIFICACIÓN O MEDICIÓN DE CONFIABILIDAD PARA REPOSITORIOS ARCHIVÍSTICOS DIGITALES CONFIABLES CON ÉNFASIS EN EL ACCESO A LA INFORMACION

Paula Regina Ventura Amorim Gonçalez*

RESUMO:
Introdução:
Considerando as diretrizes da Norma ISO 16363:2012 (*Space data and information transfer systems -- Audit and certification of trustworthy digital repositories*) e o texto da Resolução 39 do CONARQ para certificação de Repositório Arquivístico Digital Confiável (RDC-Arq), verificar quais as recomendações técnicas devem ser utilizadas como base para que um repositório arquivístico digital seja considerado confiável. **Objetivo:** Identificar requisitos para a criação de Repositórios Arquivísticos Digitais Confiáveis com ênfase no acesso à Informação a partir da Norma ISO 16363:2012 e da Resolução 39 do CONARQ. **Metodologia:** Para o desenvolvimento do estudo, a metodologia consistiu em uma investigação teórica de nível exploratória, descritivo e documental visto que, está fundamentada na Norma ISO 16363:2012 e na Resolução 39 do CONARQ. Pela perspectiva da abordagem do problema o estudo é qualiquantitativo, pois, os dados foram coletados, tabulados, e analisados a partir da interpretação de seus conteúdos. **Resultados:** Apresenta-se um conjunto de Recomendações de *Checklist* para medição e/ou certificação de confiabilidade para RDC-Arq com um recorte focado na identificação de requisitos com ênfase no acesso à informação. **Conclusões:** O direito à informação bem como o acesso à informação confiável é uma premissa para Repositórios Arquivísticos Digitais, assim, o conjunto de recomendações é dirigido a arquivistas que atuam em Repositórios Digitais e desejam verificar os requisitos necessários para avaliação de confiabilidade do Repositório Digital ou ainda guiar o profissional da informação na coleta de requisitos para certificação de confiabilidade do repositório.

Palavras-chave: Repositórios Arquivísticos Digitais. Certificação confiabilidade. Medição de confiabilidade. RDC-Arq. Repositórios confiáveis

*Doutora em Ciência da Informação pela Universidade Estadual Paulista (UNESP), professora colaboradora da Universidade Estadual de Londrina. E-mail paulaventuramorim@gmail.com

1 INTRODUÇÃO

As instituições arquivísticas são desafiadas a constante atualização no uso das tecnologias de Informação e Comunicação (TIC) para organizar, preservar e disponibilizar de maneira confiável seu acervo documental que é gerado em grandes quantidades e em diferentes suportes.

Adequando-se a essa realidade, arquivos de todo mundo passaram a disponibilizar informações e documentos arquivísticos no ambiente Web, assim, disseminam as informações por eles custodiadas ao tornarem acessível a busca, a consulta, o uso e o reuso da informação, pois tais ambientes possibilitam que os usuários acessem os documentos e informações arquivísticas que satisfaçam suas necessidades informacionais de forma rápida, simples e dinâmica.

Segundo Castells (2006, p.225) “a era da informação é a nossa era, é um período histórico caracterizado por uma revolução tecnológica centrada nas tecnologias digitais de informação e comunicação” está alicerçada na estrutura social dos computadores em rede, a Internet, caracterizada como espaços e lugares que ligam e interligam as atividades humana e que, apesar de ser um instrumento relacionado à atividade econômica, o maior fluxo de informação se concentra no uso social e pessoal e não no comercial.

Nesse contexto, os arquivos digitais, podem contribuir para o ensino e a pesquisa e atender às necessidades informacionais da sociedade, oferecendo serviços com foco no atendimento dos diferentes grupos de usuários. Assim, os serviços gerados por Repositórios Arquivísticos Digitais, motivados pelas tecnologias, podem ter suas rotinas racionalizadas ao se utilizarem de sistemas de automação que agilizem o processo de recuperação e transmissão da informação, tornando-os acessíveis a todo cidadão.

A partir do ano de 2014 arquivos públicos brasileiros que se utilizam dos ambientes digitais devem cumprir as exigências da Resolução 39 do CONARQ, que estabelece diretrizes para implementação e implantação de repositórios arquivísticos, para o arquivamento e a manutenção de documentos.

Nesse cenário, tendo como diretrizes as orientações da Resolução 39 do CONARQ e da Norma ISO 16363:2012 (*Space data and information transfer systems -- Audit and certification of trustworthy digital repositories*), analisamos o conjunto de atributos essenciais para a implantação de Repositórios Arquivísticos Digitais Confiáveis (RDC-Arq) identificando e categorizando as recomendações, para que o arquivista possa mensurar o nível de confiabilidade de um Repositório e adequá-lo para certificação.

2. NORMA ISO 26363:2012 - *SPACE DATA AND INFORMATION TRANSFER SYSTEMS - AUDIT AND CERTIFICATION OF TRUSTWORTHY DIGITAL REPOSITORIES*

O escopo do referencial normativo prescrito pela ISO 16363:2012 é ser uma ferramenta que viabiliza a auditoria, a avaliação e a certificação dos repositórios digitais. A norma aponta, ainda, a documentação básica necessária, para que seja possível o cumprimento do processo de auditoria, bem como os requisitos para os auditores, balizando dessa maneira, o processo de certificação.

A ISO também estabelece metodologias adequadas que irão determinar a consistência e a sustentabilidade nos repositórios digitais. Geralmente os critérios são bem abrangentes, embora alguns tenham explicações insuficientes ou ausentes podem gerar diferentes interpretações. É importante ressaltar que nem todos os critérios serão aplicáveis a todos os repositórios.

A norma contém cento e cinco critérios que abrangem três áreas: Infraestrutura organizacional; Gerenciamento de objetos digitais e Infraestrutura; e gestão de riscos de segurança. Os critérios incluem elementos como: governança; estrutura organizacional; mandato ou finalidades; âmbito; funções e responsabilidades; enquadramento da política; sistema de financiamento; questões financeiras incluindo ativos; contratos licenças e passivos; e transparência (CONSULTATIVE COMMITTEE FOR SPACE DATA SYSTEMS, 2011).

As métricas normativas que estão relacionadas com a Infraestrutura Organizacional fazem a descrição da arquitetura técnica, processos e recursos necessários para que um repositório digital seja sustentável. Os critérios são

divididos em: Governança e viabilidade organizacional; Estrutura organizacional e de pessoal; Responsabilidade processual e preservações no âmbito da política; Sustentabilidade financeira; Contratos licenças e ativos. (CONSULTATIVE..., 2011)

As normas relacionadas à Gestão de objetos digitais avaliam a responsabilidade de gestão dos objetos digitais de um repositório, incluindo os aspectos organizacionais e as técnicas relacionadas com tal responsabilidade como: funções do repositório, processos e procedimentos para a ingestão, gerenciamento, preservação e acesso aos objetos digitais.

Toda preocupação com a auditoria para a certificação de confiabilidade de um Repositório Digital se justifica, quando percebemos a importância dessas ações em nossos dias em que o documento digital é produzido em grande escala. Assim as interfaces dos repositórios possibilitam não somente o acesso rápido e confiável, como também por meio de boas práticas, conectam seus serviços e coleções às comunidades usuárias.

3 RESOLUÇÃO 39 DO CONARQ

A Resolução 39, datada de 29 de abril de 2014, estabelece diretrizes para a implementação de repositórios confiáveis para a transferência e recolhimento de documentos arquivísticos dos órgãos e entidades integrantes do Sistema Nacional de Arquivos (SINAR).

As Diretrizes para Implementação de Repositórios Digitais Confiáveis de Documentos Arquivísticos foram elaboradas por uma equipe constituída por dezessete membros da Câmara Técnica de Documentos Eletrônicos do CONARQ (CTDE), pertencentes a diferentes instituições arquivísticas de diferentes localidades do Brasil.

As diretrizes são baseadas no modelo *Open Archival Information System* (1999), no relatório da *Research Library Group* (RLG) e da *Online Computer Library Center* (OCLC) - *Trusted Digital Repositories Atributes and Responsibilities* (2002) e no documento *Trustworthy Repository Audit & Certification: Criteria and Checklist* (TRAC) (2007) apresentados anteriormente.

Na apresentação das diretrizes, ao tratar do aumento da produção dos documentos arquivísticos em formatos digitais, há a seguinte consideração:

> A produção crescente de documentos arquivísticos em formato digital desafia as organizações produtoras e as instituições de preservação na busca de soluções para a preservação e o acesso de longo prazo. Os documentos digitais sofrem diversas ameaças decorrentes da fragilidade inerente aos objetos digitais, da facilidade de adulteração e da rápida obsolescência tecnológica (CONSELHO NACIONAL DE ARQUIVOS, 2014, p. 4).

Nota-se que, assim como no cenário mundial, essa é uma preocupação emergente no Brasil onde se buscam meios para a salvaguarda dos documentos arquivísticos em formato digital. A resolução explicita tal preocupação na descrição do objetivo de:

> Indicar parâmetros para repositórios arquivísticos digitais confiáveis de forma a garantir a integridade, a autenticidade (identidade e integridade), a confidencialidade, a disponibilidade, o acesso e a preservação, tendo em vista a perspectiva da necessidade de manutenção dos acervos documentais por longos períodos de tempo ou até mesmo permanente. (CONSELHO NACIONAL DE ARQUIVOS, 2014, p. 5).

No dia 04 de setembro de 2015, a Câmara Técnica de Documentos Eletrônicos, por meio da Resolução nº 43, altera a redação da Resolução nº 39, de 29 de abril de 2014, ajustando o texto: onde se lia “Diretrizes para Implementação de Repositórios Digitais Confiáveis de Documentos Arquivísticos”, lê-se “Diretrizes para a implementação de Repositórios Arquivísticos Digitais Confiáveis RDC-Arq”.

Mudança essa bastante pertinente, visto que repositórios arquivísticos se diferenciam dos demais repositórios pela especificidade de seus materiais e pelo cumprimento de requisitos que obrigatoriamente assegurem o armazenamento e o acesso em longo ou permanente prazo.

Vale destacar que a modificação de 2014, na redação das diretrizes, ocorreu somente na nomenclatura. A redação foi modificada para Repositórios Arquivísticos Digitais Confiáveis e acrescentada a sigla RDC-Arq.

Os Repositórios Arquivísticos Digitais são compostos essencialmente de fontes primárias de informações (cartas, processos, registros) produzidas diretamente por um indivíduo ou organização, ao invés de fontes secundárias como as encontradas em bibliotecas (livro, periódicos etc.). Os arquivos custodiam registros únicos que não podem ser encontrados ou consultados em outro local a não ser nos arquivos (RAMALHO, 2007).

Para que sejam cumpridos os requisitos, a fim de que o repositório digital seja considerado confiável, o CONARQ pautou-se na ISO 16.363:2012, conforme apontamentos na resolução. Os requisitos apresentados nas diretrizes da resolução 39 do CONARQ estão organizados em três conjuntos: infraestrutura organizacional; gerenciamento do documento digital e tecnologia, estrutura técnica e segurança.

Nesse momento, cabe um alerta sobre alguns apontamentos rapidamente citados na Resolução do CONARQ para a instalação dos Repositórios Arquivísticos Digitais Confiáveis RDC-Arq. Conforme relatam as normas, nacional e internacional vigente, as interfaces dos repositórios podem potencializar e aumentar sua capacidade de satisfazer as necessidades informacionais de seus usuários ao conectar seus serviços e coleções à comunidade.

A partir da análise categorização e cotejamento das recomendações das normas citadas nas seções dois e três, apresentamos a seguiras recomendações para que o arquivista possa mensurar a confiabilidade de um repositório arquivístico visando sua certificação ou grau de confiabilidade.

4. RECOMENDAÇÕES PARA CONSTRUÇÃO DE RDC-ARQ, FUNDAMENTADOS NO ACESSO À INFORMAÇÃO

Baseados na premissa de que os ambientes informacionais dos Arquivos permanentes tratam, custodiam, preservam e propiciam o acesso às informações e aos documentos, para que repositórios digitais existam e tenham a característica de confiabilidade, faz-se imprescindível manter a integralidade, a proveniência e a preservação dos documentos. Ao contrário, os recursos

arquivísticos deixariam de ser elemento ou prova de algum evento ocorrido, e, por conseguinte, não seriam confiáveis.

A Norma ISO 16363 (2012, p. 14, tradução nossa) aponta, em sua justificativa de criação, que: “[...] as alegações de confiabilidade são fáceis de fazer, mas até o momento, difíceis de justificar ou objetivamente provar. Então estabelecer critérios mais claros detalhando o que é um repositório confiável ou não se tornou vital.”

Assim, a participação do arquivista na construção de um Repositório Digital assegurará a manutenção das características do recurso arquivístico, mesmo com as mudanças ocorridas nos suportes, no acesso, na agilização do processo de descrição e de transferência da informação, criados a partir do uso das tecnologias que potencializam o acesso e a disseminação da informação.

Nesse contexto, considerando a Lei de Acesso à Informação, a preocupação está na construção de Repositórios Arquivísticos Digitais Confiáveis que mantenham as características do recurso para serem elementos de prova, ofereçam acesso remoto, gerenciem conteúdo, preservem, utilizem metadados como parte do processo da Curadoria Digital, visando à preservação, à recuperação, à segurança e à confiabilidade, considerando que o ambiente arquivístico contém especificidades quanto ao grau de sigilo e acesso.

A partir da análise exploratória da Norma ISO 16363:2012 que faz a certificação de Repositórios Digitais, da Resolução 39 do Conarq, que faz recomendações para que um Repositório Arquivístico Digital Confiável, da legislação vigente no Brasil e dos estudos de Camargo (2010), no Quadro 1, a seguir, apresentam-se recomendações que auxiliam o Arquivista no pedido de certificação ou na medição de confiabilidade de um RDC-Arq.

As recomendações sublinhadas foram adicionadas às Diretrizes propostas pela ISO 16363:2012 e pelo CONARQ, visto que este estudo tem como proposta o Acesso à Informação. Assim, dizem respeito ao conhecimento por parte do arquivista, às leis referentes a arquivos e acesso vigentes no país, Curadoria Digital, à Acessibilidade e à Usabilidade.

Quadro 1 - Recomendações de *checklist* para medição e/ou certificação de confiabilidade para RDC-Arq com ênfase no Acesso à Informação

Seção	Tópico	Item	Descrição do item	S	N
ORGANIZAÇÃO E INFRAESTRUTURA	1. Política de Arquivo	1.1	Estar em conformidade com a lei em vigência que dispõe sobre a política nacional de arquivos públicos e privados e dá outras providências, hoje Lei n. 8.159 (BRASIL, 1991).		
		10.12	Estar em conformidade com a Lei de Acesso à Informação Lei 12.527 (BRASIL, 2012).		
	2. Governança e viabilidade organizacional	2.1	Ter uma declaração de missão que reflita um compromisso com a preservação, a gestão e o acesso à informação digital por longo prazo (ISO, 2012).		
		2.2	Ter como missão o compromisso com a preservação, o gerenciamento e o acesso de longo prazo dos documentos digitais. Essa missão é claramente identificada por todos os interessados no repositório e envolve: mandato legal, contexto organizacional e requisitos regulatórios (CONARQ, 2014).		
		2.3	Ter um Plano Estratégico de Preservação que defina a abordagem do repositório no apoio a sua missão em longo prazo (ISO, 2012).		
		2.4	Ter um plano adequado de sucessão, planos de contingência e/ou acordos judiciais, no caso de o repositório parar sua atividade ou a instituição governamental, ou financiamento mudar substancialmente o seu âmbito (ISO, 2012).		
		2.5	Ter um plano de sucessão formal, planos de contingência e/ou acordos estabelecidos para garantir a continuidade do serviço, no caso de o repositório parar de operar ou de a instituição responsável e/ou financiadora mudar seu escopo (CONARQ, 2014).		
		2.6	Controlar seu ambiente organizacional para determinar quando executar o seu plano de sucessão, planos de contingência e/ou acordos judiciais (ISO, 2012).		
		2.7	Ter uma política para o recolhimento do documento, especificando o tipo de informação que irá preservar, manter, gerenciar e fornecer acesso (ISO, 2012).		
	3. Estrutura Organizacional	3.1	Identificar e estabelecer as funções que necessita realizar e nomear pessoas com qualificações e experiência adequadas para cumprir esses deveres (ISO, 2012).		
		3.2	Ter uma equipe dotada de qualificação e formação necessárias e em número suficiente, para garantir todos os serviços e funcionalidades pertinentes ao repositório. Além disso, manter um programa de desenvolvimento profissional contínuo (CONARQ, 2014).		
		3.3	Identificar e estabelecer os deveres que precisa executar (ISO, 2012).		
		3.4	Ter um número adequado de pessoas em sua equipe, para apoiar todas as funções e serviços (ISO, 2012).		
		3.5	Colocar em prática um programa de desenvolvimento profissional ativo que forneça a qualificação da equipe, competências e oportunidades de desenvolvimento (ISO, 2012).		

Seção	Tópico	Item	Descrição do item	S	N
ORGANIZAÇÃO E INFRAESTRUTURA	4. Regulamentação de responsabilidades políticas de preservação	4.1	Definir a sua base de conhecimento, sua Comunidade-Alvo e ter essas definições acessíveis (ISO, 2012; CONARQ, 2014).		
		4.2	Ter políticas de preservação, para garantir que seu Plano Estratégico de Preservação será cumprido (ISO, 2012).		
		4.3	Possuir políticas e definições, acessíveis publicamente que demonstrem como os requisitos do serviço de preservação serão contemplados (CONARQ, 2014).		
		4.4	Possuir mecanismos de revisão, atualização e desenvolvimento contínuo de suas políticas de preservação, à medida que o repositório cresce, e a tecnologia e, as práticas da comunidade evoluem (ISO, 2012; CONARQ, 2014).		
		4.5	Documentar permissões legais – por meio de acordos de custódia, normas de procedimentos e outros – que isentem de responsabilidade, no caso de alterações passíveis de ocorrer em estratégias de preservação digital (CONARQ, 2014).		
		4.6	Ter sua história documentada, bem como as alterações de operações e procedimentos de *software* e *hardware* (ISO, 2012).		
		4.7	Fazer o registro histórico de mudanças de procedimentos e de *software* e *hardware* (CONARQ, 2014).		
		4.8	Comprometer-se com a transparência e com a responsabilidade em todas as ações de apoio à exploração e gestão do repositório que afetem a preservação de conteúdos digitais ao longo do tempo (ISO, 2012).		
		4.9	Relacionar o registro histórico acima referido, com suas estratégias de preservação digital e descrever os potenciais efeitos dessas mudanças sobre os documentos digitais (CONARQ, 2014).		
		4.10	Demonstrar que está sistematicamente avaliando a satisfação das expectativas dos produtores e dos usuários, buscando atendê-las (CONARQ, 2014).		
		4.11	Comprometer-se em definir, coletar, rastrear e fornecer medidas para a integridade da informação (ISO, 2012).		
		4.12	Estar comprometido com a definição, coleta, auditoria e fornecimento (sob demanda) de mecanismos de controle da integridade dos documentos digitais sob sua custódia (CONARQ, 2014).		
		4.13	Possuir com um calendário para fazer regularmente a autoavaliação de seu funcionamento e renovar sua certificação externa (ISO, 2012).		
		4.14	Adotar a Curadoria Digital como um processo para o ciclo de vida dos documentos em que a preservação seja parte desse processo.		
	5.Sustentabilidade Financeira	5.1	Dispor de sistemas de planejamento de negócios de curto e longo prazo, para que seja mantido ao longo do tempo (ISO, 2012).		
		5.2	Demonstrar a capacidade de obter recursos financeiros estáveis e contínuos para sustentar, por meio de prestação de serviço, parcerias, doações, verba da própria instituição, dentre outros (CONARQ, 2014).		

Seção	Tópico	Item	Descrição do item	S	N
ORGANIZAÇÃO E INFRAESTRUTURA	5. Sustentabilidade Financeira	5.3	Possuir práticas e procedimentos que sejam transparentes (em conformidade com as normas e práticas contábeis relevantes) e auditados por terceiros de acordo com os requisitos legais territoriais financeiros (ISO, 2012).		
		5.4	Ter transparência dos procedimentos para obtenção dos recursos e auditoria dos mesmos, de acordo com o sistema jurídico no qual o repositório se insere (CONARQ, 2014).		
		5.5	Realizar revisão e ajustes anuais (CONARQ, 2014).		
		5.6	Ter um compromisso contínuo para analisar e informar sobre riscos financeiros, benefícios, investimentos e despesas (incluindo ativos, licenças e passivos) (ISO, 2012).		
		5.7	Comprometer-se com os ciclos de planejamento, com o equilíbrio dos riscos, benefícios, investimentos e gastos (CONARQ, 2014).		
	6. Contratos, licenças e passivos	6.1	Ter e manter contratos adequados ou contratos de depósito para materiais digitais que ele gerencie e/ou preserve para o qual forneça acesso (ISO, 2012).		
		6.2	Possuir contratos de depósito que especifiquem todos os direitos de preservação necessários, transferindo-os e documentando-os (ISO, 2012).		
		6.3	Ter especificados todos os aspectos relevantes de aquisição, manutenção, acesso e retirada em acordos escritos com os depositantes e outras partes relevantes (ISO, 2012).		
		6.4	Ter seus contratos, licenças e passivos pelo repositório claros e mensuráveis; delinear papéis, responsabilidades, prazos e condições e ser facilmente acessíveis ou disponíveis aos interessados. Esses contratos, licenças e passivos podem envolver tanto a relação entre o repositório e os produtores de documentos digitais, como a relação entre o repositório e fornecedores de serviços. Esses mesmos instrumentos devem especificar todos os direitos e obrigações do repositório sobre os documentos digitais a ele confiados, em especial, no que diz respeito à propriedade intelectual e a restrições de uso (CONARQ, 2014).		
		6.5	Ter registrado as políticas que indiquem quando ele aceita a responsabilidade de preservação de conteúdo de cada conjunto de objetos, de dados apresentados (ISO, 2012).		
		6.6	Ter políticas para lidar com a responsabilidade e os desafios à propriedade e aos direitos (ISO, 2012).		
		6.7	O repositório deve rastrear e gerenciar direitos de propriedade intelectual e as restrições à utilização de conteúdo do repositório como exigido pelo contrato de depósito, contrato ou licença (ISO, 2012).		
	7. Acessibilidade	7.1	Fornecer alternativas de não-texto de modo que possa ser mudado para outro tipo como braile, discurso ou símbolos. (CAMARGO, 2010).		
		7.2	Fornecer alternativas sincronizadas para multimídia (CAMARGO, 2010).		
		7.3	Criar várias maneiras de apresentação do índice (CAMARGO, 2010).		

Seção	Tópico	Item	Descrição do item	S	N
GERENCIAMENTO DO DOCUMENTO DIGITAL	7. Acessibilidade	7.4	Utilizar toda a funcionalidade disponível do teclado (CAMARGO, 2010).		
		7.5	Oferecer opção de modificação de tamanho de fonte (CAMARGO, 2010).		
		7.6	Oferecer opção de modificação de fundo de página (CAMARGO, 2010).		
	8. Usabilidade	8.1	Exibir o nome do Repositório e/ou logotipo ou slogan (CAMARGO, 2010).		
		8.2	Incluir um link da homepage para uma Seção "Sobre Nós" (CAMARGO, 2010).		
		8.3	Incluir um link "Fale Conosco" (CAMARGO, 2010).		
		8.4	Empregar padrões e estilo com consistência (CAMARGO, 2010).		
		8.5	Disponibilizar para os usuários uma caixa de busca (CAMARGO, 2010).		
		8.6	Usar texto com muito contraste e cores de pano de fundo (CAMARGO, 2010).		
		8.7	Evitar rolagem horizontal (CAMARGO, 2010).		
		8.8	Usar raramente menus suspensos (CAMARGO, 2010).		
		8.9	Informar se o *website* ficar paralisado ou não estiver funcionando (CAMARGO, 2010).		
		8.10	Reduzir o tempo das respostas (CAMARGO, 2010).		
		8.11	Oferecer cursor com comportamento padronizado (CAMARGO, 2010).		
		8.12	Dar enfoque no conteúdo (CAMARGO, 2010).		
		8.13	Possibilitar retorno à página principal (CAMARGO, 2010).		
		8.14	Possibilitar o acesso às informações por meio de poucos comandos (CAMARGO, 2010).		
		8.15	Utilizar mensagens de erro com vocabulário neutro (CAMARGO, 2010).		
		8.16	Evitar caracteres especiais e adequar à fonte em relação ao assunto (CAMARGO, 2010)		
	9. Recepção: Aquisição de Conteúdo	9.1	Identificar as informações de conteúdo e as propriedades de informação que o repositório preservar (ISO, 2012).		
		9.2	Ter um procedimento(s) para identificar as propriedades de informações que irá preservar (ISO, 2012).		
		9.3	Ter um registro da informação de conteúdo e as propriedades de informação que irá preservar (ISO, 2012).		
		9.4	Identificar as propriedades do documento que serão preservadas (ex.: o conteúdo, *layout*, tabela de cor, resolução da imagem, canais de som etc.)(CONARQ, 2014).		
		9.5	Especificar claramente a informação que precisa ser associada com informação de conteúdo específico no momento do seu depósito (ISO, 2012).		
		9.6	Especificar claramente a informação que deve estar associada ao documento (metadados associados) no momento da sua submissão (CONARQ, 2014).		
		9.7	O repositório deve ter as especificações adequadas que permitam o reconhecimento e a análise do *SIP* (ISO, 2012).		

Seção	Tópico	Item	Descrição do item	S	N
GERENCIAMENTO DO DOCUMENTTO DIGITAL	9. Recepção: Aquisição de Conteúdo	9.8	O repositório deve ter mecanismos para verificar adequadamente a identidade do produtor de todos os materiais (ISO, 2012).		
		9.9	Ter mecanismos para autenticar a origem dos documentos que estão sendo admitidos no repositório, de forma a garantir sua proveniência (CONARQ, 2014).		
		9.10	Ter um processo de ingerir que verifique cada *SIP* para integralidade e exatidão (ISO, 2012).		
		9.11	Ter procedimentos para verificar a integridade do *SIP* o que pode ser feito por procedimentos automatizados e/ou checagem humana (CONARQ, 2014).		
		9.12	O repositório deve ter controle suficiente sobre os Objetos Digitais para preservá-los(ISO, 2012; CONARQ 2014).		
		9.13	Fornecer ao produtor/depositante respostas adequadas em pontos acordados durante os processos de recepção (ISO, 2012)		
		9.14	Fornecer ao produtor/depositante relatórios do andamento dos procedimentos durante todo processo da admissão (CONARQ, 2014).		
		9.15	Ter registros das ações e processos de administração que sejam relevantes para aquisição de conteúdo (ISO, 2012).		
		9.16	Ter registros de todas as ações e processos administrativos que ocorram durante o processo de admissão e sejam relevantes para a preservação (CONARQ, 2014).		
		9.17	Demonstrar em que momento a responsabilidade pela preservação do documento submetido (*SIP*) é formalmente aceita pelo repositório (CONARQ, 2014).		
	10. Admissão: criação do pacote de arquivamento	10.1	Ter para cada *AIP* ou classe de *AIP* preservados pelo repositório uma definição associada que seja adequada para analisar o *AIP* e estar apto para as necessidades de preservação em longo prazo (ISO, 2012).		
		10.2	Descrever minuciosamente as diferentes classes de informação e como os *AIPs* são implementados nos casos em que a especificidade dessas classes exija ações de preservação diferentes (por exemplo, a imagem *TIFF* que é processada por um sistema pode necessitar de ações de preservação diferentes das ações necessárias à imagem *TIFF* que é apresentada ao olho humano) (CONARQ, 2014).		
		10.3	Ser capaz de identificar qual definição se aplica a qual *AIP* (ISO, 2012).		
		10.4	Ter uma definição de cada *AIP* adequada para a preservação a longo prazo, permitindo a identificação e análise de todos os componentes requeridos do *AIP* (ISO, 2012).		
		10.5	Descrever cada classe de informação (texto estruturado, imagem matricial, banco de dados, imagem em movimento e outras) a ser preservada pelo repositório, e como ela está implementada. Essa descrição deve apontar as componentes chaves do *AIP*: o documento arquivístico, sua informação de representação (informação estrutural e semântica) e as várias categorias de informação descritiva de preservação (fixibilidade, proveniência e contexto), e ainda como esses componentes se relacionam (CONARQ, 2014).		

Seção	Tópico	Item	Descrição do item	S	N
GERENCIAMENTO DO DOCUMENTO DIGITAL	10. Admissão: criação do pacote de arquivamento	10.6	O repositório deve ter uma descrição de como os *AIPs* são construídos a partir *SIP* (ISO, 2012).		
		10.7	Descrever como os *AIPs* são construídos a partir dos *SIPs,* ou seja, apontar todas as transformações pelas quais passarão os documentos, os metadados submetidos e os metadados a serem adicionados no momento da formação do *AIP* (CONARQ, 2014).		
		10.8	Documentar a disposição final de todos os *SIP* (ISO, 2012).		
		10.9	Ser capaz de demonstrar se os *SIPs* foram aceitos e transformados em *AIPs* integralmente ou em parte, ou ainda se foram recusados (CONARQ, 2014).		
		10.10	Seguir os procedimentos documentados (se um *SIP* não está incorporado um *AIP* ou descartado) e deve indicar por que o *SIP* não foi incorporado ou descartado (ISO, 2012).		
		10.11	No caso de o documento já possuir um identificador único a ele atribuído no *SIP*, o repositório deverá mantê-lo no *AIP*, ou criar outro identificador que deverá ser associado, de maneira persistente, ao *SIP* (CONARQ, 2014).		
		10.12	Ter e usar uma convenção que gere identificadores únicos persistentes para todos os *AIPs* (ISO, 2012).		
		10.13	Identificar exclusivamente cada *AIP* dentro do repositório (ISO, 2012).		
		10.14	Possuir identificadores exclusivos (ISO, 2012).		
		10.15	Ceder e manter identificadores persistentes do *AIP* e seus componentes, de modo a ser exclusivo dentro do contexto do repositório (ISO, 2012).		
		10.16	Atribuir aos *AIPs* identificadores que sejam únicos, persistentes e visíveis aos gestores e auditores, de acordo com padrões reconhecidos (por ex.: *Handle System*, DOI, URN, PURL) (CONARQ, 2014).		
		10.17	A documentação deve descrever todos os processos utilizados para alterações nesses identificadores (ISO, 2012).		
		10.18	O repositório deve ser capaz de fornecer uma lista completa de todos esses identificadores e fazer verificações pontuais para duplicações (ISO, 2012).		
		10.19	O sistema de identificadores deve ser adequado para conter atuais e previsíveis necessidades futuras do repositório como números de objetos (ISO, 2012).		
		10.20	O repositório deve ter um sistema de serviços de ligação/resolução de confiança, a fim de encontrar o objeto identificado como exclusivo, independentemente da sua localização física (ISO, 2012).		
		10.21	O repositório deve ter acesso a ferramentas e recursos necessários para fornecer informações ao Representante autorizado sobre todos os objetos digitais que ele contém (ISO, 2012).		
		10.22	O repositório deve ter ferramentas ou métodos para identificar o tipo de todos os objetos apresentados como dados de arquivo (ISO, 2012).		
		10.23	O repositório deve ter ferramentas ou métodos para determinar quais representações das informações são necessárias para fazer todo o dado compreensível para sua comunidade alvo (ISO, 2012).		

Seção	Tópico	Item	Descrição do item	S	N
GERENCIAMENTO DO DOCUMENTO DIGITAL	10. Admissão: criação do pacote de arquivamento	10.24	O repositório deve ter acesso à representação da informação necessária (ISO, 2012).		
		10.25	O repositório deve ter ferramentas ou métodos para garantir que as representações das informações sejam requisitos persistentes e associados aos objetos de dados relevantes (ISO, 2012).		
		10.26	Ter acesso a ferramentas amplamente reconhecidas para apoiar o monitoramento dos componentes digitais dos documentos, tais como diretórios de formatos de arquivo (ex.: *PRONOM* – base de dados com registro de formatos, mantida pelo arquivo nacional do Reino Unido) e registros de outras informações de representação (CONARQ, 2012).		
		10.27	O repositório deve ter processos documentados para a aquisição da Preservação da Descrição da Informação (PDI) para informação de conteúdos associados e adquirir PDI de acordo com os processos documentados (ISO, 2012).		
		10.28	Registrar, em um banco de dados local, a informação de representação dos documentos admitidos, quando essa informação não estiver disponível nas ferramentas mencionadas anteriormente (CONARQ, 2012).		
		10.29	O repositório deve ter processos documentados para a aquisição de PDI (ISO, 2012).		
		10.30	Registrar metadados de preservação associados aos documentos admitidos de maneira a apoiar sua integridade, localização, legibilidade e proveniência, dentre outros (CONARQ, 2012).		
		10.31	Assegurar que as informações de conteúdo do *AIP* sejam compreensíveis para a sua Comunidade alvo no momento da criação do *AIP* (ISO, 2012).		
		10.32	Ter um processo documentado para testar compreensibilidade de suas comunidades designadas das Informações do conteúdo dos *AIP* na sua criação (ISO, 2012).		
		10.33	Executar o processo de teste para cada classe de Informações do conteúdo dos *AIP* (ISO, 2012).		
		10.34	Se falhar o teste de compreensibilidade, o repositório deve pôr as informações de conteúdo do *AIP* até o nível necessário para compreensão (ISO, 2012).		
		10.35	Ter procedimentos para testar se os documentos são compreensíveis pela comunidade alvo e, em caso negativo, adequá-los às necessidades dessa comunidade (ex.: documentos voltados para deficientes visuais) (CONARQ, 2012).		
		10.36	Verificar cada *AIP* para a integralidade e exatidão no ponto em que é criado (ISO, 2012).		
		10.37	Verificar a completude e a correção de cada *AIP* no momento em que é gerado, isto é, no momento em que o *SIP* é convertido em *AIP* (CONARQ, 2012).		
		10.38	Fornecer um mecanismo independente para verificar a integridade do repositório de recolha/conteúdo (ISO, 2012).		
		10.39	Ter um mecanismo independente para verificar a integridade do conjunto do seu acervo, ou seja, verificar que todos os documentos previstos foram, de fato, admitidos no repositório justificando possíveis lacunas (CONARQ, 2012).		

Seção	Tópico	Item	Descrição do item	S	N
GERENCIAMENTO DO DOCUMENTO DIGITAL		10.40	Ter registros contemporâneos de ações e processos de administração que sejam relevantes para a criação do *AIP* (ISO, 2012).		
		10.41	Documentar todas as ações relevantes à preservação dos documentos que estão relacionadas à criação do *AIP* (CONARQ, 2012).		
	11. Preservação	11.1	Documentar estratégias de preservação relevantes para as suas participações (ISO, 2012).		
		11.2	Preservar estratégias bem definidas e periodicamente atualizadas, apontando e detalhando cada procedimento a ser adotado, como, por exemplo, a normalização de formatos (CONARQ, 2012).		
		11.3	Ter mecanismos em vigor para monitorar a preservação do meio (ISO, 2012).		
		11.4	Ter mecanismos para o monitoramento e a notificação quando a informação sobre a representação dos documentos for inadequada para seu público alvo (ISO, 2012).		
		11.5	Ter mecanismos para monitoramento e notificação quando alguma informação de representação dos documentos no repositório estiver se tornando obsoleta ou inviável (ex.: um formato de arquivo que esteja entrando em desuso, um suporte que esteja no final de sua vida útil) (CONARQ, 2012).		
		11.6	Ter mecanismos para mudar seus planos de preservação como resultado das suas atividades de monitorização (ISO, 2012).		
		11.7	Ter mecanismos de mudanças do plano de preservação como resultado do monitoramento (CONARQ, 2012).		
		11.8	Ter mecanismos para criar, identificar ou recolher qualquer representação da informação necessária (ISO, 2012).		
		11.9	Apresentar provas de eficácia das suas atividades de preservação (ISO, 2012).		
		11.10	Fornecer evidências sobre a eficácia do plano de preservação (CONARQ, 2012).		
	12. Preservação do AIP	12.1	Ter especificações para saber como os *AIP* são armazenadas até o nível de *bit* (ISO, 2012).		
		12.2	Utilizar as estratégias previstas no planejamento da preservação que podem ser várias e devem ser registradas nos metadados de preservação (CONARQ, 2012).		
		12.3	O repositório deve preservar as informações de conteúdo do *AIP* (ISO, 2012).		
		12.4	Atender minimamente a dois aspectos da preservação digital – os cuidados com armazenamento (controle dos suportes, dos formatos e da localização de cópias) e a eventual necessidade de migração (atualização de suportes e conversão de formatos) (CONARQ, 2012).		
		12.5	O repositório deve monitorar ativamente a integridade da *AIP* (ISO, 2012).		
		12.6	Monitorar constantemente a integridade dos *AIPs* por meio do registro de metadados de fixidade e de *logs* de checagem dessa integridade (por exemplo, *checksum*) (CONARQ, 2012).		

Seção	Tópico	Item	Descrição do item	S	N
GERENCIAMENTO DO DOCUMENTO DIGITAL	12. Preservação do AIP	12.7	O repositório deve ter registros contemporâneos de ações e processos de administração que sejam relevantes para o armazenamento e preservação dos *AIP (*ISO, 2012).		
		12.8	Preservar o documento digital (informação de conteúdo do *AIP*) originalmente admitido no repositório e daquele resultante da última migração (CONARQ, 2012).		
		12.9	Ter procedimentos para todas as ações tomadas em *AIP (*ISO, 2012).		
		12.10	Ser capaz de demonstrar que as ações tomadas em *AIP* foram compatíveis com a especificação dessas ações *(*ISO, 2012).		
		12.11	Registrar todas as ações de preservação realizadas nos *AIPs* (CONARQ, 2012).		
	13. Gestão da informação	13.1	Especificar os requisitos mínimos de informação para permitir ao público alvo descobrir e identificar o material de seu interesse *(*ISO, 2012).		
		13.2	Ter metadados mínimos que permitam a busca e localização dos documentos e sejam identificadores conhecidos pela comunidade-alvo de usuários (ex.: número de matrícula do servidor público, título de livro numa biblioteca, número de processo) (CONARQ, 2012).		
		13.3	Fazer a captura ou criar informações mínimas descritivas e garantir que ele esteja associado com o *AIP (*ISO, 2012).		
		13.4	Fazer a captura ou criação de metadados mínimos pelo repositório durante o processo de admissão e associação desses metadados ao *AIP* correspondente (CONARQ, 2012).		
		13.5	Manter ligação bidirecional entre cada *AIP* e sua informação descritiva *(*ISO, 2012).		
		13.6	O repositório deve manter as associações entre seus *AIP* e sua informação descritiva ao longo do tempo *(*ISO, 2012).		
		13.7	Integridade referencial entre os *AIPs* e sua informação descritiva (metadados), ou seja, todo *AIP* deve ter uma informação descritiva, e toda informação descritiva deve apontar para um *AIP* (CONARQ, 2012).		
		13.8	Manter a permanência da integridade referencial, mesmo no caso de quebra temporária da relação entre *AIP* e seus metadados descritivos. Nesse caso, o repositório deve ser capaz de restaurar a relação rompida (CONARQ, 2012).		
	14. Gestão do Acesso	14.1	O repositório deve cumprir políticas de acesso *(*ISO, 2012).		
		14.2	Divulgar para a comunidade de usuários as opções disponíveis de acesso aos documentos e de entrega dos mesmos (CONARQ, 2012).		
		14.3	Registrar e analisar todas as falhas de gerenciamento de acesso e anomalias *(*ISO, 2012).		
		14.4	Implementar uma política de registro dos acessos ocorridos que esteja de acordo com as necessidades de controle desses acessos, tanto da parte do repositório como dos produtores dos documentos nele admitidos (CONARQ, 2012).		

Seção	Tópico	Item	Descrição do item	S	N
GERENCIAMENTO DO DOCUMENTO DIGITAL	14. Gestão do Acesso	14.5	Seguir políticas e procedimentos que permitam a difusão de objetos digitais que sejam rastreáveis aos originais com provas que sustentem a sua autenticidade *(*ISO, 2012).		
		14.6	Conceder acesso a cada *AIP* para os usuários autorizados e da forma devida (ex.: autorização de "somente leitura", ou acesso a um número limitado de itens por período), em conformidade com o acordo estabelecido entre o repositório e o produtor/depositante (CONARQ, 2012).		
		14.7	Documentar e implementar políticas de acesso (identificação e autenticação de usuários), em conformidade com os acordos estabelecidos entre o repositório e o produtor/depositante. Essas políticas de acesso podem variar desde a isenção da necessidade de identificação de usuário até o controle rígido da identificação e autenticação do usuário (CONARQ, 2012).		
		14.8	Registrar de falhas no controle de acesso (como, por exemplo, um acesso indevidamente negado) e uso desse registro para avaliar eventuais falhas no sistema de segurança (CONARQ, 2012).		
		14.9	Demonstrar que o processo que gera o *DIP* atende completamente à requisição do usuário (ex.: se o usuário pediu um conjunto de documentos, receberá o conjunto completo; se ele pediu um documento, receberá apenas esse único documento) (CONARQ, 2012).		
		14.10	Demonstrar que o processo que gera o *DIP* está correto em relação ao pedido do usuário (ex.: se o repositório oferece imagens nos formatos JPG e PNG, o usuário deve receber, dentre esses, o formato que solicitou) (CONARQ, 2012).		
		14.11	Demonstrar que todos os pedidos de acesso resultam em uma resposta de aceitação ou rejeição (CONARQ, 2012).		
		14.12	Garantir a autenticidade dos *DIPs* por meio da entrega de cópias autênticas dos originais ou da viabilidade de rastreamento auditável da relação entre o *DIP* e o objeto original. Para isso, um repositório deve ser capaz de demonstrar o processo de construção do *DIP* a partir de um *AIP* (CONARQ, 2012).		
INFRAESTRUTURA E SEGURANÇA NA GESTÃO DE RISCOS	15. Técnicas de Gestão de risco e infraestrutura	15.1	Identificar e gerir os riscos às suas operações de preservação e objetivos associados à infraestrutura do sistema *(*ISO, 2012).		
		15.2	O repositório deve empregar tecnologias de notificação de monitoramento de sistemas relacionadas ao tempo (obsolescência) *(*ISO, 2012).		
		15.3	Dispor de procedimentos para monitorar e receber notificações quando forem necessárias mudanças de tecnologia de *hardware (*ISO, 2012).		
		15.4	Dispor de procedimentos para monitorar e receber notificações quando forem necessárias mudanças de tecnologia de *hardware (*ISO, 2012).		
		15.5	Adotar uma tecnologia de *hardware* e *software* apropriada para os serviços que presta, procedimentos para o recebimento e monitoramento de notificações e para a avaliação da necessidade de mudanças na tecnologia utilizada (CONARQ, 2012).		

Seção	Tópico	Item	Descrição do item	S	N
INFRAESTRUTURA E SEGURANÇA NA GESTÃO DE RISCOS	15. Técnicas de gestão de risco e infraestrutura	15.6	Ter procedimentos, compromisso e financiamento para substituir *hardware* quando a avaliação indicar a necessidade de fazê-lo *(*ISO, 2012).		
		15.7	Ter tecnologias de *software* adequadas aos serviços que presta a sua comunidade alvo *(*ISO, 2012).		
		15.8	Dispor de procedimentos para monitorar e receber notificações quando são necessárias mudanças de *software (*ISO, 2012).		
		15.9	Dispor de procedimentos para avaliar quando as mudanças são necessárias para *software* atual *(*ISO, 2012).		
		15.10	Ter procedimentos, compromisso e financiamento para substituir *software* quando a avaliação indicar a necessidade de fazê-lo *(*ISO, 2012).		
		15.11	Ter suporte de *hardware* e *software* adequado para a funcionalidade de *backup* suficiente para preservar o conteúdo do repositório e acompanhamento de funções de repositório *(*ISO, 2012).		
		15.12	Ter mecanismos efetivos para a detecção de corrupção ou perda de *bits* (CONARQ, 2012).		
		15.13	Registrar e reportar à sua administração todos os casos de corrupção ou perda de dados. Devem ser tomadas medidas para reparo/substituição de dados corrompidos ou perdidos *(*ISO, 2012).		
		15.14	Relatar os incidentes de corrupção ou perda de dados eventualmente ocorridos e adotar medidas para reparação ou substituição desses mesmos dados (CONARQ, 2012).		
		15.15	Ter um processo para gravar e reagir à disponibilidade de novas atualizações de segurança baseados na avaliação do risco/benefício *(*ISO, 2012).		
		15.16	Definir processos para mídia de armazenamento e / ou alteração de *hardware* (ex: *refreshing*, migração) *(*ISO, 2012).		
		15.17	Ter previsão de procedimentos de atualização de suporte (*refreshing*) e de migração decorrentes do cumprimento do prazo de vida do suporte ou da obsolescência dos componentes de *hardware* (CONARQ, 2012).		
		15.18	Identificar e documentar processos críticos que afetem sua capacidade de cumprir com as suas responsabilidades obrigatórias *(*ISO, 2012).		
		15.19	Ter documentação da gestão de mudanças capaz de identificar alterações em processos críticos que afetem a capacidade de o repositório cumprir com suas responsabilidades obrigatórias (CONARQ, 2012).		
		15.20	O repositório deve dispor de procedimentos para monitorar e receber notificações quando forem necessárias mudanças de *software (*ISO, 2012).		
		15.21	Adequar os processos do *hardware* e do *software* do sistema de *backup* às necessidades do repositório (CONARQ, 2012).		
		15.22	Ter um processo de gestão de mudança documentado que identifique alterações em processos críticos que potencialmente afetem a capacidade de o repositório cumprir suas responsabilidades obrigatórias *(*ISO, 2012).		

Seção	Tópico	Item	Descrição do item	S	N
INFRAESTRUTURA E SEGURANÇA NA GESTÃO DE RISCOS	15. Técnicas de gestão de risco e infraestrutura	15.23	O repositório deve gerir o número e a localização das cópias de todos os objetos digitais (ISO, 2012).		
		15.24	Gerenciar o número de cópias de todos os documentos mantidos no repositório e a localização de cada uma delas (CONARQ, 2012).		
		15.25	Ter mecanismos para garantir várias cópias de objetos digitais sincronizados (ISO, 2012).		
		15.26	Ter mecanismos para garantir o sincronismo entre as cópias de um mesmo documento, ou seja, garantir que as mudanças intencionais feitas em uma cópia sejam propagadas para todas as outras (CONARQ, 2012).		
		15.27	Ter seu funcionamento com base num sistema operacional e outros softwares de infraestrutura que tenham um bom suporte do mercado e da comunidade de usuários (CONARQ, 2012).		
		15.28	Ter previsão de procedimentos para testar o efeito de mudanças críticas no sistema (CONARQ, 2012).		
		15.29	Fazer a ponderação entre riscos e benefícios nas decisões de atualização de *software* de segurança (CONARQ, 2012).		
	16. Tecnol. Apropriadas	16.1	Ter adotado uma tecnologia de *hardware* e *software* apropriada para os serviços que presta, procedimentos para o recebimento e monitoramento de notificações e para a avaliação da necessidade de mudanças na tecnologia utilizada (CONARQ, 2012).		
	17. Gestão de riscos de segurança	17.1	Manter uma análise sistemática dos fatores de risco de segurança associados com os dados, os sistemas, o pessoal e as instalações físicas (ISO, 2012).		
		17.2	Fazer a análise sistemática de dados, sistemas, pessoas e instalação física (CONARQ, 2012).		
		17.3	Implementar controles para tratar adequadamente cada um dos riscos de segurança definidos (ISO, 2012).		
		17.4	Adotar procedimentos de controle para tratar adequadamente as necessidades de segurança (CONARQ, 2012).		
		17.5	A equipe repositório deve delinear funções, responsabilidades e autorizações relacionadas com a implementação de mudanças dentro do sistema (ISO, 2012).		
		17.6	Delinear papéis, responsabilidades e autorizações relativas à implementação de mudanças no sistema (CONARQ, 2012).		
		17.7	Ter adequada preparação para desastres escrito e plano(s) de recuperação, incluindo pelo menos um *backup off-site* de todas as informações preservadas, juntamente com uma cópia fora do local do plano (s) de recuperação (ISO, 2012).		
		17.8	Possuir plano de prevenção de desastres e de reparação, que inclua, ao menos, um *backup off site* de tudo o que é mantido no repositório (documentos, metadados, trilhas de auditoria etc.), inclusive do próprio plano de reparação (CONARQ, 2012).		

Fonte: Elaborado pela autora

A análise da Norma ISO 16363:2012 e da Resolução 39 do CONARQ, gerou orientações que auxiliarão os arquivistas no que diz respeito a melhores práticas no que tange à confiabilidade dos Repositórios Arquivísticos Digitais, tanto para sua certificação, como para a medição de confiabilidade, quesito capital para um repositório do domínio arquivístico brasileiro.

Como nossa ênfase está no acesso à informação, as recomendações propostas são dirigidas aos Arquivistas. Após a análise exploratória das normas, foi feita a categorização e o cotejamento entre os dois documentos, após esse processo, foi proposta a ampliação de três tópicos e vinte e cinco requisitos, objetivando o acesso a um maior número de usuários às informações custodiadas e disponibilizadas pelos Repositórios Arquivísticos Digitais Confiáveis RDC-Arq.

Para melhor visualização dos tópicos e dos itens sugeridos, eles estão sublinhados nas Recomendações de *checklist* para medição e/ou certificação de confiabilidade para RDC-Arq com ênfase no Acesso à Informação.

O primeiro tópico sugerido foi denominado de: Política de Arquivo e está inserido na seção: Organização e Infraestrutura. Como estamos trabalhando com Arquivos permanentes, é fundamental que o arquivista tenha conhecimento das Leis vigentes no Brasil, o item 1.1 recomenda que o repositório deverá estar em conformidade com a Lei em vigência que dispõe sobre a política nacional dos arquivos públicos e privados, que no dia de hoje é Lei Nº 8.159, de 8 de janeiro de 1991, e o item 2.2 recomenda que o RDC-Arq deve estar em conformidade com a da Lei Nº 12.527 Lei de Acesso à Informação que regulamenta o direito constitucional de acesso às informações públicas.

Já no tópico quatro - Regulamentação de Responsabilidades políticas de preservação- é feita a recomendação do item 4.17, em que o RDC-Arq deve adotar a Curadoria Digital como um processo para o ciclo de vida dos documentos, e que a preservação seja parte desse processo, por entendermos que o modelo do Ciclo de Vida proposto pela *Digital Curation Centre,* subsidia as atividades realizadas pelo arquivista, visto que foi idealizado a partir de consultas com profissionais e especialistas, em todas as fases de seu ciclo o

que garante uma sequência lógica desde o recebimento do documento, sua avaliação, seleção ou descarte dos dados, seguido de arquivamento e de ações subsequentes como a preservação, o armazenamento, o acesso até a transformação ou reavaliação dos dados.

Todo processo de Curadoria permite que os curadores identifiquem potenciais pontos fracos nas políticas do repositório ou ainda *gaps* na cadeia de arquivo, além de identificar as preocupações com a comunidade que poderiam fazer parte das rotinas de trabalho, bem como identifica outros interessados como fonte ou utilizadores.

Ao se fazer arquivamento dos dados tanto os preserva, quanto agrega valores a eles, pois, ao arquivar o dado, visando sua preservação, poderá ser feita a adição de metadados administrativos que descreverá a cadeia curadora; possibilitará a transformação dos dados para outro formato e ainda eles serão colocados num contexto mais amplo, e, para sua gestão, serão adicionadas anotações ou então serão desenvolvidos relacionamentos com outros conjuntos de dados.

Apesar do requisito acessibilidade ser mencionado na Norma ISO 16363:2012, como parte do requisito 4. Gerenciamento do Objeto Digital, item 4.2 Admissão: criação do pacote de arquivamento, subitem 4.2.7 “O repositório deve assegurar que as informações de conteúdo da *AIP* são compreensíveis para a sua comunidade-alvo no momento da criação da *AIP;* e da Resolução 39 do CONARQ, requisito 4. Gerenciamento do Documento Digital, item: “Ter procedimentos para testar se os documentos são compreensíveis pela comunidade alvo e, em caso negativo, adequá-los às necessidades dessa comunidade (ex.: documentos voltados para deficientes visuais)”. Entendemos que a criação de um tópico contendo recomendações de maneira mais específica, auxiliará o arquivista na criação do Repositório Digital e atenderá um maior número de pessoas com necessidades especiais ou com mobilidade reduzida.

Diante do exposto, para o desenvolvimento de um ambiente informacional digital devem ser considerados os diferentes cenários em que o usuário poderá acessá-lo, como situações em que o usuário tem dificuldades

para ler, ouvir, ou compreender o conteúdo que se apresenta no *site* do repositório digital, ou ainda em casos que o usuário faz uso de dispositivos que apresentam interfaces não convencionais. Outro fato a ser considerado é que o usuário poderá utilizar *browsers* ou sistemas operacionais diferentes e como também poderá ter restrições no que se refere à velocidade de conecção com a Internet (FREIRE; FORTES, 2004).

Nesse cenário foi proposto com o intuito de minimizarem as barreiras de acesso a inserção do tópico de número sete – Acessibilidade - seguido da adição de seis recomendações, as quais elencamos da seguinte maneira: 7.1 Fornecer alternativas de não texto de modo que possa ser mudado para outro tipo de braile, discurso ou símbolos; 7.2 Fornecer alternativas sincronizadas para multimídia; 7.3 Criar várias maneiras de apresentação do índice; 7.4 Utilizar toda a funcionalidade que está disponível no teclado; 7.5 oferecer opção de modificação de tamanho de fonte e 7.6 Oferecer opção de modificação de fundo de página, para a certificação de confiabilidade de um Repositório Arquivístico Digital.

A partir de uma acessibilidade ótima, podemos ter também usabilidade que, segundo Silvino e Abrahão (2003, p. 13) "[...] é aferida pelos critérios ergonômicos e de funcionalidade e indica o grau de facilidade que a página oferece ao ser acessada". Dentre os problemas mais recorrentes no que tange à usabilidade, estão: interação usuário sistema ineficiente, dificuldade em acessar a informação desejada, interfaces complicadas e não intuitivas.

Nessa perspectiva, tendo como base os estudos de Camargo, (2010) sobre acessibilidade e usabilidade, foi feita a inserção do tópico de número 8 – Usabilidade - seguido da proposta da recomendação de dezesseis itens que facilitarão a interação do usuário com a interface de um repositório Arquivístico Digital e consequentemente a satisfação das necessidades informacionais dos usuários. São eles: 8.1 Exibir o nome do Repositório e/ou logotipo ou slogan; 8.2 incluir um *link* da *homepage* para uma Seção "Sobre Nós"; 8.3 Incluir um *link* "Fale Conosco"; 8.4 Empregar padrões e estilo com consistência; 8.5 Disponibilizar para os usuários uma caixa de busca; 8.6 Usar texto com muito contraste e cores de pano de fundo; 8.7 Evitar rolagem horizontal; 8.8 Usar

raramente menus suspensos; 8.9 Informar se o *website* ficar paralisado ou não estiver funcionando; 8.10 Reduzir o tempo das respostas; 8.11 Oferecer cursor com comportamento padronizado; 8.12 Dar enfoque no conteúdo; 8.13 Possibilitar retorno à página principal; 8.14 Possibilitar o acesso às informações por meio de poucos comandos; 8.15 Utilizar mensagens de erro com vocabulário neutro e 8.16 Evitar caracteres especiais e adequar a fonte em relação ao assunto.

Buscamos com a inserção do tópico usabilidade e dos 16 itens, aumentar usabilidade do ambiente digital e, por conseguinte, a qualidade da ambiência, visto que, a usabilidade é que indica o grau de facilidade que uma página da *Web* oferece ao ser acessada, o que contribui para que mais usuários tenham acesso aos documentos custodiados pelo Repositórios Arquivísticos Digitais Confiáveis, pois ao fazerem o acesso, encontrarão páginas intuitivas, fáceis e fluídas e assim poderão satisfazer suas necessidades informacionais.

Nesse momento, vale destacar que ferramentas estão disponíveis na *Web* com a proposta de avaliar a acessibilidade, como é o caso da ferramenta DaSilva[1] o primeiro avaliador de acessibilidade em português para *Website* e o avaliador de usabilidade e desempenho de *Websites ErgoList*[2].

5 CONSIDERAÇÕES FINAIS

O direito à informação bem como o acesso à informação confiável é uma premissa para Repositórios Arquivísticos Digitais. Nesse cenário, analisar o conjunto de atributos essenciais para a implantação de Repositórios Arquivísticos Digitais Confiáveis (RDC-Arq), a partir das diretrizes da Norma ISO 16363:2012 (*Space data and information transfer systems -- Audit and certification of trustworthy digital repositories*) e da Resolução 39 do CONARQ “Diretrizes para a implementação de Repositórios Arquivísticos Digitais Confiáveis RDC-Arq” para criação de um conjunto de recomendações para a

[1] Disponível em: <http://www.dasilva.org.br/>
[2] Disponível em: <http://labiutil.inf.ufsc.br/ergolist/>

certificação de Repositórios Arquivísticos Confiáveis se constituiu como o escopo deste trabalho.

Pudemos observar que os estudos dos Repositórios Arquivísticos Digitais Confiáveis ainda são poucos na vertente da certificação, pois as discussões, na área da Ciência da Informação, são mais frequentes no que se refere à Curadoria Digital e à utilização de *software.*

Apresentamos um conjunto de informações – *Checklist* - dirigidas aos Arquivistas que atuam em Repositórios Digitais e desejam verificar os requisitos necessários para avaliação de confiabilidade do Repositório Digital ou ainda guiar o profissional da informação na coleta de requisitos para a certificação de confiabilidade do repositório.

Como a ênfase do trabalho se dá no acesso à informação, além dos requisitos sugeridos pela Norma ISO 16363:2012 e da Resolução 39 do CONARQ, foi adicionado a esse conjunto de informações um requisito pertinente à Legislação vigente no Brasil, um requisito pertinente à Curadoria Digital, visto que o DCC disponibiliza *Checklist* para cada fase do Ciclo de Vida dos Dados.

Foi incluído o tópico Acessibilidade com seis recomendações, para que o Repositório atinja um maior número de usuários, Nesse momento, faz-se importante ressaltar os apontamentos sobre o usuário feitos por Baranauska e Mantoan (2001, p. 14), ao ponderarem sobre os aspectos da acessibilidade nas páginas da Web, consideram “[...] a variedade de contextos de interação que podem estar relacionadas a diferentes tipos e situações dos usuários com o sem deficiência [...]” e complementam que “Entre esses cidadãos encontram-se também a população idosa.” O que também é partilhado por Winckler e Pimenta (2002, p. 2), quando pontuam que “[...] recomendações para acessibilidade não limita a utilização da interface apenas à pessoa com necessidades especiais”.

Também foi acrescentado o tópico Usabilidade com dezesseis itens, pois a interface é a porta de entrada para que as necessidades informacionais do público alvo sejam atendidas. Assim, faz-se necessária uma interface adequada ao sistema, bem como à satisfação do usuário.

Os requisitos que compõem a Norma ISO e a Resolução 39 do Conarq são elementos essenciais para a implantação de Repositórios Arquivísticos Digitais Confiáveis (RDC-Arq) no que diz respeito ao uso e ao acesso à informação por conectar serviços e coleções visando às comunidades-alvo.

No final de nosso trabalho, as verificações realizadas nos conduziram a reflexões sobre o papel dos Arquivistas, frente à demanda de criação de Repositórios Arquivísticos Digitais Confiáveis, ao trabalho em equipes multidisciplinares, ao conhecimento sobre o processo de Curadoria Digital e consequentemente com o Ciclo de Vida dos Dados. Sendo isso, uma imposição do mercado de trabalho, considerando que o ciberespaço rompe a distância física, temporal e as barreiras geográficas.

REFERÊNCIAS

BARANAUSKAS, Maria Cecilia Calani; MANTOAN, Maria Teresa Eglér. Acessibilidade em ambientes educacionais: para além das guidelines. **Educação Temática Digital**, Campinas, v. 2, n. 2, p. 13-22, 2001. Disponível em: <http://dx.doi.org/10.20396/etd.v2i2.1068>. Acesso em: 23 set. 2016.

CAMARGO, Liriane Soares de Araújo de. **Metodologia de desenvolvimento de ambientes informacionais digitais a partir dos princípios da Arquitetura da Informação**. 2010. 287 f. Tese (Doutorado em Ciência da Informação)-Faculdade de Filosofia e Ciências, Universidade Estadual Paulista, Marília, 2010.

CASTELLS, Manuel. Inovação, liberdade e poder na era da utopia tecnológica. In: MORAES, Dênis de (Org.). **Sociedade midiatizada**. Rio de Janeiro: Mauad X, 2006. p. 225-231.

CONSULTATIVE COMMITTEE FOR SPACE DATA SYSTEMS. **Reference model for an Open Archival Information System (OAIS)**: recommended practice CCSDS 650.0-M-2. Washington, DC: CCSDS, 2012. Disponível em: <https://public.ccsds.org/pubs/650x0m2.pdf>. Acesso em: 15 mar. 2016.

CONSELHO NACIONAL DE ARQUIVOS (Brasil). Resolução nº 39, de 29 de abril de 2014. **Diário Oficial da União**, Poder Executivo, Brasília, DF, 30 abr. 2014. Disponível em: <http://www.conarq.arquivonacional.gov.br/legislacao/ resolucoes-do-conarq/281-resolucao-n-39,-de-29-de-abril-de-2014.html>. Acesso em: 3 jun. 2014.

CONSELHO NACIONAL DE ARQUIVOS (Brasil). Resolução nº 43, de 04 de setembro de 2015. **Diário Oficial da União**, Poder Executivo, Brasília, DF, 8 set. 2015. Disponível em: <http://www.conarq.arquivonacional.gov.br/ legislacao/resolucoes-do-conarq/335-resolucao-n-43,-de-04-de-setembro-de-2015.html>. Acesso em: 15 set. 2015.

FREIRE, André Pimenta; FORTES, Renata Pontin de Mattos. Avaliação e re-engenharia da interface de uma aplicação Web de acordo com normas de acessibilidade. In: SIMPÓSIO SOBRE FATORES HUMANOS EM SISTEMA COMPUTACIONAIS, VI, 2004, Ribeirão Preto, Anais... Ribeirão Preto, 2004, p. 181 – 184.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **ISO 16363:2012**: Space data information transfer systems -- Audit and certification of trustworthy digital repositories. Genebra, 2012.

RAMALHO, José Carlos. Repositórios digitais. In: TERTÚLIA EM INTELIGÊNCIA ARTIFICIAL, 3., 2007, Porto. **Apresentações...** Porto: Universidade do Minho, 2007.

SILVINO, A. M. D; ABRAHÃO, J.I. Navegabilidade e Inclusão Digital: Usabilidade e Competência. RAE-eletrônica, v. 2, n. 2, jul-dez/2003. Disponível em:< http://www.scielo.br/scielo.php?pid=S1676-56482003000200002&script=sci_abstract&tlng=pt> Acesso em: 05 OUT. 2016.

Title

Recommendations for certification or measurement of reliability for reliable digital archival repositories with emphasis on access

Abstract:
Introduction: Considering the guidelines of ISO 16363: 2012 (Space data and information transfer systems -- Audit and certification of trustworthy digital repositories) and the text of CONARQ Resolution 39 for certification of Reliable Digital Archival Repository (RDC-Arq), verify the technical recommendations should be used as the basis for a digital archival repository to be considered reliable. **Objective:** Identify requirements for the creation of Reliable Digital Archival Repositories with emphasis on access to information from the ISO 16363: 2012 and CONARQ Resolution 39. **Methodology:** For the development of the study, the methodology consisted of an exploratory, descriptive and documentary theoretical investigation, since it is based on ISO 16363: 2012 and CONARQ Resolution 39. From the perspective of the problem approach, the study is qualitative and quantitative, since the data were collected, tabulated, and analyzed from the interpretation of their contents. **Results:** We presented a set of Checklist Recommendations for reliability measurement and/or certification for RDC-Arq with a clipping focused on the identification of requirements with emphasis on access to information is presented. **Conclusions:** The right to information as well as access to reliable information is a premise for Digital Archival Repositories, so the set of recommendations is directed to archivists who work in Digital Repositories and wish to verify the requirements necessary to evaluate the reliability of the Digital Repository or still guide the information professional in collecting requirements for repository reliability certification.

Keywords: Digital Archival Repositories. Certification reliability. Reliability measurement. RDC-Arq. Reliable repositories.

Titulo

Recomendaciones para la certificación o medición de confiabilidad para repositorios archivísticos digitales confiables con énfasis en el acceso a la información

Resumen:
Introducción: Considerando las directrices de la norma ISO 16363:2012 (*Space data and information transfer systems -- Audit and certification of trustworthy digital repositories*) y el texto de la Resolución 39 del CONARQ para certificación de Repositorios Archivísticos Digitales Confiables (RDC-Arq), verificar cuales de las recomendaciones técnicas deben ser utilizadas como base para que un repositorio archivístico digital sea considerado confiable. **Objetivo:** Identificar los requisitos para la creación de Repositorios Archivísticos Digitales Confiables con énfasis en el acceso a la Información a partir de la Norma ISO 16363:2012 y de la Resolución 39 del CONARQ. **Metodología:** Para el desarrollo del estudio, la metodología consistió en una investigación teórica a nivel exploratorio, descriptivo y documental, la cual está fundamentada en la Norma ISO 16363:2012 y en la Resolución 39 del CONARQ. Por la perspectiva del abordaje del problema, el estudio es cuali-cuantitativo, porque los datos fueron recolectados, tabulados y analizados a partir de la interpretación de sus contenidos. **Resultados:** Se presenta un conjunto de Recomendaciones de *Checklist* para la medición y/o certificación de la confiabilidad para RDC-Arq con un recorte centrado en la identificación de requisitos con énfasis en el acceso a la información.
Conclusiones: El derecho a la información así como el acceso a la información confiable es una premisa para Repositorios Archivísticos Digitales, por esto, el conjunto de recomendaciones es dirigido a archivistas que actúan en Repositorios Digitales y desean verificar los requisitos necesarios para evaluación de confiabilidad del Repositorio Digital o para guiar al profesional de la información en la colecta de requisitos para certificación de confiablidad del repositorio.

Palabras clave: Repositorios Archivísticos Digitales. Certificación de confiablidad. Medición de confiablidad. RDC-Arq. Repositorios confiables.

Recebido: 12.02.2016
Aceito: 25.03.2017