Notas de tradução

[1] [NT] No original em inglês, *authoritative copy*.
[2] [NT] Pesquisa Internacional sobre Documentos Arquivísticos Autênticos Permanentes em Sistemas Eletrônicos.
[3] [NT] A terceira fase do projeto iniciou-se em 2007, com previsão de conclusão em 2012.
[4] [NT] No original em inglês, COP Model – *Chain of Preservation Model*.
[5] [NT] No original em inglês, BDR Model – *Business Driven Recordkeeping Model*.
[6] [NT] No original em inglês, MADRAS – *Metadata and Archival Description Registry and Analysis System*.

InterPARES 2 Project

International Research on Permanent Authentic Records in Electronic Systems*

Informações para contato

Projeto InterPARES
School of Library, Archival and Information Studies
University of British Columbia
Vancouver, BC V6T 1Z3 Canadá
Tel: +1 (604) 822-2694
Fax: +1 (604) 822-1200



Dr. Luciana Duranti, Diretora do Projeto
+1 (604) 822-2587
luciana.duranti@ubc.ca

Randy Preston, Coordenador do Projeto
+1 (604) 822-2694
interpares.project@ubc.ca

A maior parte do financiamento para o Projeto InterPARES foi fornecida pelo Social Sciences and Humanities Research Council, do Canadá, e pelas National Historical Publications and Records Commission e National Science Foundation, dos Estados Unidos. O financiamento complementar foi fornecido pela Hampton Fund Research Grant, pelo Vice President Research Development Fund, pela Decania de Artes e pela Escola de Biblioteconomia, Arquivologia e Ciência da Informação da Universidade de British Columbia.

Para mais informações, acesse nosso site: www.interpares.org

Tradução e revisão: Arquivo Nacional e Câmara dos Deputados
Editoração: Câmara dos Deputados

* [NT] Pesquisa Internacional sobre Documentos Arquivísticos Autênticos Permanentes em Sistemas Eletrônicos.

Dpd

Diretrizes do produtor

A ELABORAÇÃO E A MANUTENÇÃO DE MATERIAIS DIGITAIS: DIRETRIZES PARA INDIVÍDUOS

Elementos de preservação

		5 Mg Migração	6 Pr Proteção							
	8 Md Metadados	9 Cs Cópia de segurança	10 It Integridade	11 Ac Acurácia	12 Ff Forma fixa	13 Au Autenticidade				
			16 Io Interoperabilidade	17 Co Consciência	18 Ob Obsolescência		20 Fx Fixidez			
		25 Cc Custódia Confiável	26 Og Organização	27 Cf Confiabilidade		29 At Autenticação	30 Ce Conteúdo estável			
				34 As Acessibilidade			37 Id Identidade			

In
Introdução

Introdução

A maior parte das informações de hoje é produzida e armazenada de forma digital. As vantagens do meio digital já são familiares a todas as pessoas. Os documentos podem ser produzidos rapidamente, além de editados e revisados com facilidade. Com a internet, eles podem ser distribuídos mundialmente quase na velocidade da luz. Podem, também, ser manipulados de tal forma que permite serem usados para múltiplas finalidades. O meio digital também resolve os problemas de armazenamento em longo prazo relacionados a grandes conjuntos de documentos arquivísticos em papel.

As vantagens da era digital, contudo, têm seu custo. Apenas recentemente, as pessoas começaram a compreender completamente os muitos problemas inerentes ao meio digital. Por exemplo, a informação digital só pode ser acessada utilizando um computador e este deve ser equipado com os programas necessários para ler as cadeias de bits contidas em disco ou fita. A facilidade de reprodução e a proliferação de cópias tornam ainda mais difícil identificar uma versão completa ou final de um documento digital. A facilidade de distribuição da informação na internet dificulta a preservação dos direitos de propriedade intelectual. Finalmente, todos os materiais digitais são vulneráveis a vírus e a simples falhas tecnológicas, bem como o acelerado desenvolvimento de novos programas e equipamentos pode torná-los inacessíveis rapidamente.

Com todos esses problemas, não é de se estranhar que algumas pessoas tenham saudades da tangibilidade confortável do papel. Ainda que, por um longo período, nossos sistemas para produzir e manter informações continuem a ser híbridos – ou seja, contendo tanto o papel quanto os materiais digitais – a revolução digital é claramente um caminho sem volta. Consequentemente, todas as pessoas deveriam estar cientes dos riscos que atingem os materiais digitais e saber a melhor forma de minimizá-los.

Estas diretrizes foram desenvolvidas para pessoas que produzem materiais digitais no curso de suas atividades profissionais e pessoais, com o objetivo de ajudá-las a tomar decisões conscientes a respeito de elaborar e manter estes materiais, a fim de assegurar sua preservação pelo tempo que seja necessário. Eles também podem ser úteis para pequenas organizações ou grupos de pessoas, tais como consultórios médicos, grupos de pesquisa, ou equipes de pesquisa científica.

Estas diretrizes podem ser aplicadas a vários tipos de publicações, documentos e dados digitais, mas elas são especialmente importantes para documentos arquivísticos digitais. Documentos arquivísticos são aqueles que você elabora, recebe e usa em suas atividades, e que mantém porque pode precisar deles depois, ou porque quer ter um registro confiável do que você fez. Portanto, você precisa ser especialmente cuidadoso com a manutenção e a preservação desses documentos. Estas diretrizes aplicam-se aos documentos arquivísticos que precisam ser armazenados por apenas um pequeno período, bem como àqueles que requerem manutenção em longo prazo. A observância destas diretrizes ajudará a assegurar o acesso aos documentos que merecem ser preservados por um longo período em um repositório arquivístico, quando estes forem entregues aos cuidados de uma entidade arquivística confiável.

Definições

De
Definições

Antes de apresentar as recomendações para orientar a produção e a manutenção de materiais digitais, será necessário e útil esclarecer o significado de alguns dos termos usados neste documento.

No escopo destas diretrizes, um **documento arquivístico** é definido como qualquer documento produzido (isto é, elaborado ou recebido e salvo para ações futuras ou referência) por uma pessoa física ou jurídica no curso de uma atividade prática como um instrumento e subproduto de tal atividade. Uma **publicação** é definida como um documento destinado à disseminação ou distribuição para o público em geral. Todos os documentos arquivísticos e publicações são documentos e contêm dados. Um **documento** é a informação afixada em um meio sob uma forma fixa; **informação** é um conjunto de dados destinados à comunicação através do tempo ou espaço; e **dados** são as menores partes significativas e indivisíveis da informação.

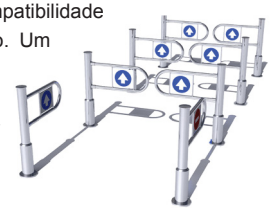
Estas diretrizes objetivam fornecer recomendações para a produção e manutenção de materiais digitais confiáveis em geral, e de documentos arquivísticos em particular, que possam ser precisa e autenticamente mantidos e preservados ao longo do tempo. Para facilitar sua aplicação, contudo, os termos “confiabilidade”, “acurácia”, “autenticidade” e “autenticação” precisam ser definidos.

Para os propósitos destas diretrizes, **confiabilidade** é a credibilidade do material digital enquanto conteúdo ou declaração de um fato. É a responsabilidade do autor dos materiais, seja ele uma pessoa física ou a pessoa jurídica que um indivíduo representa. Ela é estabelecida com base na completeza e acurácia do material, e no grau de controle exercido no processo de sua produção. **Acurácia** é o grau de precisão, correção, verdade e ausência de erros e distorções existentes nos dados contidos nos materiais. Para assegurar a acurácia, deve-se exercer controle sobre os processos de produção, transmissão, manutenção e preservação dos materiais. Com o tempo, a responsabilidade pela acurácia é passada do autor para o responsável pela manutenção (*keeper*) e, mais tarde, para o preservador em longo prazo dos materiais (se for aplicável). **Autenticidade** refere-se ao fato de que os materiais são o que eles dizem ser e que não foram adulterados ou corrompidos de qualquer outra forma. Assim, com relação aos documentos arquivísticos em particular, a autenticidade refere-se à confiabilidade dos documentos enquanto tais. Para assegurar que a autenticidade possa ser presumida e mantida ao longo do tempo, deve-se definir e conservar a identidade dos materiais e proteger sua integridade. A autenticidade é colocada em risco cada vez que os materiais são transmitidos através do tempo e do espaço. Ao longo do tempo, a responsabilidade pela autenticidade é passada do responsável pela manutenção (*keeper*) para o preservador dos materiais em longo prazo. **Autenticação** é a declaração da autenticidade, resultante da inserção ou da adição de elementos ou afirmações nos materiais em questão, e as normas que a regulam são estabelecidas pela legislação. Ou seja, é um meio de assegurar que os materiais sejam o que eles se propõem a ser em um dado momento. Medidas de autenticação digital, como o uso de assinaturas digitais, garantem que os materiais são autênticos apenas quando recebidos, e não podem ser repudiados; porém, tais medidas não asseguram que eles permanecerão autênticos depois disto.

As
Acessibilidade

1. Selecione *hardwares*, *softwares* e formatos de arquivo que ofereçam as melhores expectativas de garantia de que os materiais digitais permanecerão facilmente acessíveis ao longo do tempo

O acesso a materiais digitais depende de um *software* apropriado. *Softwares* que não forem compatíveis com versões anteriores (compatibilidade descendente ou reversa) ou com versões posteriores (compatibilidade ascendente) dificultam o acesso aos documentos ao longo do tempo. Um *software* destinado a uma tarefa específica também precisa trabalhar de maneira eficiente com outros que sirvam para outras tarefas e sistemas (interoperabilidade). A observância dos seis pontos a seguir pode ajudar a garantir que seu *software* e seu *hardware* mantenham a acessibilidade.



A. Escolha um *software* que apresente os materiais como eles aparecem originalmente. Teoricamente, os materiais deveriam manter a mesma aparência ao longo do tempo para serem completamente inteligíveis e acessíveis. Certifique-se de que o novo *software* será capaz de ler os seus materiais mais antigos no formato em que você os mantém, e de mostrá-los na tela com a mesma forma documental em que eram apresentados originalmente. Em outras palavras, o novo *software* deve ter compatibilidade descendente com o *software* antigo.

B. Escolha os *softwares* e *hardwares* que permitam compartilhar materiais digitais com facilidade. O *software* deve ser capaz de aceitar e gerar os arquivos em vários formatos diferentes. A habilidade para interagir facilmente com outra tecnologia é chamada de **interoperabilidade**. Isto tornará mais simples acessar seus materiais e também movê-los para outros sistemas.

C. Use *softwares* aderentes a padrões. Esta é uma das melhores coisas que você pode fazer para assegurar que o seu material durará. Padrões endossados por organizações nacionais e internacionais são os melhores. São os chamados **padrões de direito** (*de jure*). Se não existirem estes tipos de padrões para o seu material, você ainda pode garantir sua longevidade, adotando *softwares* que sejam amplamente usados. Na falta de um padrão oficial, tais *softwares* são comumente considerados um **padrão de fato** (*de facto*). *Softwares* de código aberto, isto é, *softwares* não proprietários, disponibilizados gratuitamente, são os preferíveis (veja a subseção G na próxima página).

<< Padrão de direito >>

Padrão adotado por órgãos oficiais de padronização, sejam eles nacionais (Associação Brasileira de Normas Técnicas – ABNT), multinacionais (Comitê Europeu de Normalização – CEN) ou internacionais (Organização Internacional para Padronização – ISO). Para padrões de arquivos de computador, dois padrões de direito recentes são o PDF/A (padrão PDF para arquivamento) e ODF (OASIS Formato de documento aberto).

<< Padrão de fato >>

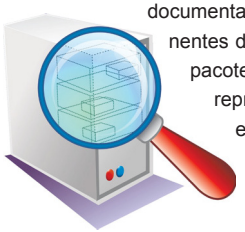
Padrão que não foi adotado por nenhum órgão oficial de padronização, mas que é amplamente usado e reconhecido pelos usuários como tal. Formatos de arquivos de computador bem conhecidos e amplamente usados que são considerados padrões de fato incluem PDF, TIFF, DOC e ZIP.

As
Acessibilidade

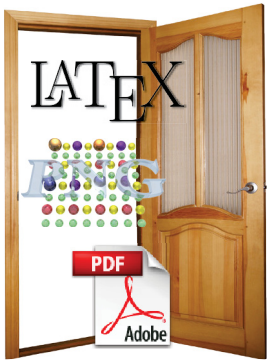
D. Mantenha as especificações do *software*. Este tipo de documentação (por exemplo, o manual do proprietário ou qualquer outra descrição mais detalhada do *software* que você possa ter) será essencial, com o avanço da tecnologia no futuro, para acessar os materiais ou para migrá-los para um novo ambiente computacional. É particularmente importante documentar integralmente qualquer software que você construa.

E. Se você personalizar o *software*, certifique-se de que documentou as mudanças que fez. Forneça informações detalhadas sobre as mudanças realizadas e descreva claramente as alterações produzidas nas características e formas de apresentação do material, assim como os resultados que você está tentando atingir ao personalizar o *software*. Uma boa maneira para fazer isso é incluir a informação sob a forma de comentários no código-fonte do *software*. A informação não será perdida, já que é parte do arquivo, e será muito útil para quem precisar fazer ajustes posteriormente, à medida que a tecnologia avance.

F. Documente a construção do seu sistema para garantir a acessibilidade a ele. Você deve documentar a estrutura e as funções do seu sistema. Isto significa identificar os componentes de *hardware* e *software*, inclusive os periféricos, o sistema operacional e os pacotes de *software*. Tal documentação identificará como os pacotes de *software* representam a informação e como eles a processam e a comunicam entre si e para os usuários. As especificações básicas assegurarão que, no futuro, outros entendam o contexto no qual você está trabalhando agora, fornecendo as informações necessárias para a atualização do sistema quando o *hardware* e o *software* evoluírem.

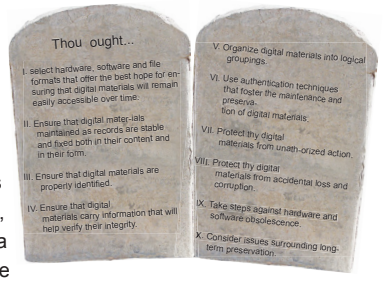


G. Sempre que possível, escolha formatos independentes de plataforma, amplamente utilizados, não proprietários e não comprimidos, com especificações disponibilizadas gratuitamente. Estes são frequentemente chamados de "formatos abertos", o que significa que suas especificações são publicadas e disponibilizadas gratuitamente. Contudo, também pode significar que os formatos são amplamente utilizados e/ou livres de patentes ou *royalties* e da possibilidade de tais direitos serem cobrados no futuro. Deve-se ressaltar que os formatos abertos não são necessariamente o mesmo que formatos produzidos por *softwares* de código aberto. Este termo descreve o *software* para o qual o código-fonte é disponibilizado gratuitamente e pode ser modificado. O *software* de código aberto – não proprietário ou livre – nem sempre produz formatos não proprietários. Diferencie formatos de arquivo, formatos de encapsulamento (*wrapper* ou *container*) e formatos de marcação (*tagged format*), tais como arquivos XML, e certifique-se de que a versão, a codificação e outras características estejam corretas e completamente especificadas. Para arquivos XML, certifique-se de que os arquivos estejam bem formados e válidos, além de acompanhados pelas DTDs ou esquemas necessários. Se não for conveniente para você seguir esta recomendação, consulte um arquivo que receba materiais digitais e escolha entre os formatos que ele recomenda para preservação em longo prazo. Se for possível, não comprima seus materiais digitais, já que isto pode causar problemas para sua preservação em longo prazo. Se você precisar comprimi-los, escolha as técnicas de compressão com menor perda e que estejam de acordo com os padrões internacionais aceitáveis.



Fx
Fixidez

2. Certifique-se de que os materiais digitais mantidos como documentos arquivísticos são estáveis e fixos tanto no conteúdo quanto na forma



Uma das grandes vantagens dos materiais digitais é a facilidade com que a informação pode ser editada, revisada ou atualizada. Mas isto também significa que informações importantes podem ser mudadas ou até mesmo perdidas, acidentalmente ou intencionalmente. Este é um problema particularmente importante para os documentos arquivísticos, porque uma de suas características é que seu conteúdo não foi alterado e é inalterável. Isto implica que a informação e os dados contidos nos documentos arquivísticos não podem ser sobrescritos, alterados, apagados ou expandidos. Um sistema que contém informações ou dados fluidos e em constante mudança não contém documentos arquivísticos até que alguém decida elaborá-los e salvá-los com **forma fixa** e **conteúdo estável**.

<< Fixidez >>

Qualidade de um documento arquivístico que assegura a forma fixa e o conteúdo estável.

Enquanto a ideia de conteúdo estável é relativamente simples, o conceito de forma fixa é mais complexo. Essencialmente, ele significa que a mensagem transmitida por um documento arquivístico digital (ou outro objeto digital) pode ser exibida com a mesma apresentação documental que tinha na tela quando foi elaborada ou recebida e salva pela primeira vez. As cadeias de bits que compõem o documento digital e determinam sua apresentação digital (isto é, seu formato de arquivo) podem mudar, mas sua apresentação documental não pode. Um exemplo simples é quando um documento produzido no Microsoft Word é posteriormente salvo como um arquivo PDF. Embora a apresentação digital do documento tenha mudado – de um arquivo ".doc" do Microsoft Word para um formato ".pdf" do Adobe Acrobat –, sua apresentação documental, também chamada **forma documental**, não mudou e, portanto, podemos dizer que o documento tem uma forma fixa.

<< Forma fixa >>

Qualidade de um documento arquivístico que assegura a mesma aparência ou apresentação documental cada vez que o documento é recuperado.

<< Conteúdo estável >>

Característica de um documento arquivístico que torna a informação e os dados nele contidos imutáveis e exige que eventuais mudanças sejam feitas por meio do acréscimo de atualizações ou da produção de uma nova versão.

Em alguns casos, os materiais digitais podem ser apresentados de muitas maneiras diferentes – em outras palavras, a informação que eles transmitem pode assumir diferentes formas documentais. Por exemplo, dados estatísticos podem ser apresentados como gráfico circular, de barra ou tabelas. Contudo, as variações possíveis dessas formas são geralmente limitadas pelo sistema. Em tais casos, podemos dizer que cada apresentação documental tem conteúdo estável e forma fixa, já que a informação é selecionada a partir de um armazenamento fixo de dados dentro do sistema, cujas regras determinam a forma da(s) sua(s) apresentação(ões) documental(is).

Fx
Fixidez

Uma situação similar ocorre quando a seleção tanto do conteúdo quanto da forma é feita a partir de um amplo conjunto de informações fixas, que é apenas parcialmente acessado cada vez que um usuário consulta o sistema. Se a mesma *query* sempre produz um mesmo resultado para o conteúdo e a forma documental, este resultado pode ser descrito como tendo conteúdo estável e forma fixa. Assim, se você, enquanto autor do documento arquivístico, estabelece regras fixas para a seleção de seu conteúdo e de sua forma documental que permitam apenas uma gama conhecida e estável de variações – isto é, que lhe dotem de **variabilidade limitada** –, então você pode afirmar que seu material tem conteúdo estável e forma fixa.

<< Variabilidade limitada >>

Qualidade de um documento arquivístico que assegura que suas apresentações documentais são limitadas e controladas por regras fixas e um armazenamento estável do conteúdo, da forma e da composição, de modo que a mesma interação, pesquisa, busca ou atividade por parte do usuário sempre produza o mesmo resultado.

A preocupação com a apresentação documental de materiais digitais é particularmente importante para manter e avaliar a confiabilidade e a acurácia dos documentos arquivísticos. No futuro, atualizações, conversões ou migrações de dados podem resultar em mudanças na forma documental. Portanto, é recomendável estabelecer primeiramente a forma dos documentos associados com cada atividade ou procedimento, e depois identificar as características essenciais (isto é, os elementos **extrínsecos** e **intrínsecos**) de cada apresentação ou forma documental. Isto o ajudará a ficar atento a mudanças futuras que impliquem em perda de identidade e integridade do documento, especialmente se você trabalhar com arte digital, na qual uma descrição certificada das características essenciais por parte do artista ajuda no reconhecimento dos direitos de propriedade intelectual ligados ao referido trabalho.

<< Forma documental >>

Regras de representação de acordo com as quais o conteúdo de um documento arquivístico, seu contexto administrativo e documental, e sua autoridade são comunicados. A forma documental possui tanto elementos extrínsecos quanto intrínsecos.

<< Elementos extrínsecos >>

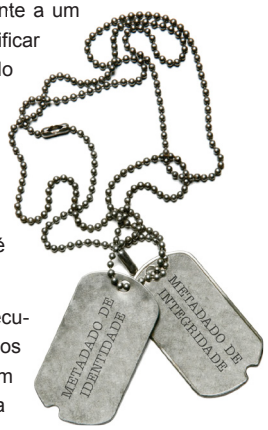
Elementos de um documento arquivístico que constituem sua aparência externa, inclusive as características de apresentação, como fonte, gráficos, imagens, sons, *layouts*, *hyperlinks*, resoluções de imagens etc., assim como selos, assinaturas digitais, carimbos de tempo e sinais especiais (marcas d'água digitais, logotipos, timbres etc.).

<< Elementos intrínsecos >>

Elementos de um documento arquivístico que expressam a ação da qual ele participa e seu contexto imediato, inclusive os nomes das pessoas envolvidas na sua produção, o nome e descrição da ação ou assunto ao qual ele pertence, a(s) data(s) de produção e transmissão etc.

Id
Identidade

3. Certifique-se de que os materiais digitais estão identificados adequadamente



Atribuir um nome com significado pertinente a um arquivo de computador ajuda a identificar seu conteúdo e torna mais fácil localizá-lo. No entanto, a identificação completa dos documentos é mais complexa do que apenas nomear arquivos. Ela é fundamental para diferenciar documentos uns dos outros, para distinguir versões diferentes de um único documento, e para fornecer evidências da identidade de um documento arquivístico desde o momento de sua produção até sua preservação de longo prazo.

A informação sobre os materiais digitais que apoia sua identificação e recuperação é comumente chamada de **metadado**. A maioria dos aplicativos de *softwares* reconhece automaticamente todos os materiais digitais com algum dado sobre sua identidade, porque esta informação é necessária para localizar documentos de forma eficaz. Sem os metadados, seria praticamente impossível encontrar um documento sem abrir e ler toda uma pasta ou vários diretórios. Os metadados descrevem as propriedades ou atributos dos materiais digitais. No caso de documentos arquivísticos, entretanto, essas propriedades (ou atributos) também são necessárias para manter e avaliar sua autenticidade, e é por isso que é importante assegurar que todas as que são essenciais estejam registradas e corretas.

<< IDENTIDADE >>

Conjunto de características de um documento ou de um documento arquivístico que o identifica de forma única e o distingue dos demais. A identidade de um documento, junto com sua integridade, constitui-se em um componente de autenticidade (veja também a Recomendação 4).

As propriedades ou atributos que expressam a identidade dos materiais digitais são chamados de **metadados de identidade**. São elas:

A. Nomes das pessoas envolvidas na produção dos materiais digitais, que incluem:

- o **autor** – a(s) pessoa(s) física(s) ou jurídica(s) responsável(eis) por emitir os materiais;
- o **redator** – a(s) pessoa(s) física(s) ou cargo(s) responsável(eis) por articular o conteúdo dos materiais;
- o **originador** – a pessoa física, cargo ou unidade administrativa responsável pela conta de correio eletrônico ou pelo ambiente tecnológico onde os materiais são gerados e/ou a partir do qual são transmitidos (Nota: A identificação do originador é importante apenas em casos em que a pessoa, cargo ou unidade administrativa responsável por produzir fisicamente e/ou transmitir os materiais não é o autor nem o redator; ela também é essencial quando o fato de o nome do originador aparecer nos materiais, ou de estar associado a eles, coloca em questão o verdadeiro autor e/ou redator dos mesmos. Isto é mais comumente percebido em casos de mensagens de correio eletrônico nas quais o nome do originador aparece no cabeçalho e/ou nos anexos que foram, de fato, de autoria ou redigidos por outra pessoa, mas fisicamente manifestados e/ou transmitidos em nome de tal pessoa pelo originador);
- o **destinatário** – a(s) pessoa(s) física(s) ou jurídica(s) para quem os materiais são destinados; e
- o **receptor** – a(s) pessoa(s) física(s) ou jurídica(s) para quem os materiais podem ter sido enviados como cópia ou cópia oculta.

B. Nome da ação ou assunto – em outras palavras, o título ou assunto.

Id
Identidade

C. Forma documental – em outras palavras, se é um relatório, uma carta, um contrato, uma tabela, uma lista etc.

D. Apresentação digital – em outras palavras, o formato, o *wrapper*, a codificação etc.

E. Data(s) de produção e transmissão, que podem ser:

- a **data cronológica** escrita nos materiais, ou a data na qual os materiais foram compilados;
- as **datas de transmissão e/ou recebimento**; e
- a **data de arquivamento** – em outras palavras, a data na qual os materiais foram associados com uma pasta ou diretório de computador, ou outro esquema ou plano de classificação (veja a Recomendação 5).

F. Expressão do contexto documental – por exemplo, um código de classificação, ou nome da pasta/diretório de computador, ou uma unidade de arquivamento equivalente dentro do esquema ou plano de classificação ao qual os materiais estão associados, e o nome do grupo mais amplo de documentos ao qual os materiais pertencem (veja também a Recomendação 5).

G. Indicação de anexos – se aplicável.

H. Indicação de direitos autorais ou outros direitos intelectuais – se aplicável.

I. Indicação da presença ou remoção de uma assinatura digital – se aplicável. (Ver recomendação 6, seção Autenticação dependente de tecnologia).

J. Indicação de outras formas de autenticação – se aplicável.

Isto poderia incluir, por exemplo, a presença de uma **corroboração** (menção explícita aos meios usados para validar o documento arquivístico); um **atestado** (validação de um documento por aqueles que participaram de sua emissão, e por testemunhas da ação ou da sua "assinatura"); uma **subscrição** (nome do autor ou redator aparecendo na parte inferior do documento) ou uma **qualificação de assinatura** (menção ao título, capacidade e/ou endereço da pessoa ou pessoas signatárias do documento).

K. Indicação da minuta ou número da versão – se aplicável.

L. Existência e localização de materiais duplicados fora do sistema digital – se aplicável.

Se existem múltiplas cópias de um documento, você deve indicar qual é a **cópia autoritária**.[1] Se o documento for certificado pelo autor como uma "reprodução aprovada" de um trabalho (por exemplo, uma obra de arte digital), a indicação da existência de tal certificação é necessária. Se o documento englobar material com direitos autorais registrados por autor(es) diferente(s), a indicação da liberação de tais direitos (ou a falta dela), com as datas relacionadas, é exigida.

<< CÓPIA AUTORITÁRIA >>

Manifestação de um documento arquivístico considerada pelo produtor como sendo o seu documento arquivístico oficial e que está comumente sujeita a controles de procedimentos que não são exigidos para outras manifestações.

It
Integridade

4. Certifique-se de que os materiais digitais carregam informações que ajudarão a verificar sua integridade

Enquanto os metadados de identidade ajudam a distinguir os materiais digitais uns dos outros, outro grupo de metadados permite aos usuários inferir que os materiais são os mesmos desde que foram produzidos (embora não seja possível verificar ou demonstrar isso, pois seria necessária uma comparação com cópias dos materiais mantidas em outros lugares). Estes metadados podem ser chamados de **metadados de integridade**. Os materiais digitais possuem **integridade** se estiverem intactos e não corrompidos, isto é, se as mensagens que eles devem comunicar para atingir seus objetivos estiverem inalteradas. Isto significa que a integridade física dos materiais digitais (por exemplo, o número adequado de cadeias de bits) pode ser comprometida desde que a articulação do conteúdo e os pré-requisitos de sua **forma documental** (veja a Recomendação 2) permaneçam os mesmos. O conteúdo e os dados são considerados inalterados se forem idênticos ao valor e à apresentação (isto é, a posição na tela) do conteúdo e dos dados da primeira manifestação salva do material. Os atributos que se relacionam à integridade dos materiais digitais dizem respeito à manutenção dos materiais, incluindo a responsabilidade por seu uso apropriado, tais como supervisão e documentação de quaisquer transformações tecnológicas ou transferências dos materiais para outros sistemas. Os **metadados de integridade** são:

<< Integridade >>

Qualidade de ser completo e inalterado em todos os aspectos essenciais; junto com a identidade, é um componente da autenticidade.

A. Nome da pessoa ou unidade administrativa que utiliza os documentos – a pessoa ou unidade que utiliza os materiais para conduzir as atividades.

B. Nome da pessoa ou unidade com responsabilidade primária por manter os materiais – pode ser o mesmo que a pessoa/unidade que utiliza os documentos.

C. Indicação de anotações acrescentadas aos materiais, se aplicável.

D. Indicação de quaisquer mudanças técnicas nos materiais ou nos aplicativos responsáveis por gerenciar e prover acesso aos materiais – por exemplo, mudanças de codificação, *wrapper* ou formato; atualização de uma versão para outra; conversão de vários componentes digitais inter-relacionados em apenas um componente (por exemplo, embutindo, diretamente nos materiais, os componentes digitais que eram apenas conectados a eles, tais como áudio, vídeo e elementos gráficos ou de texto, como fontes).

E. Código de restrição de acesso – indicação da pessoa, cargo ou unidade autorizada a ler os materiais, se aplicável.

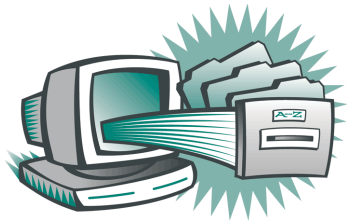
F. Código de privilégios de acesso – indicação da pessoa, cargo ou unidade autorizada a fazer anotações nos materiais, apagá-los ou removê-los do sistema, se aplicável.

G. Código de documento vital – quando aplicável: indicação do grau de importância do documento arquivístico para dar continuidade à atividade para a qual foi produzido ou à atividade da pessoa/unidade que o produziu (Nota: Aplica-se apenas a comunidades de práticas específicas, como na área médica ou jurídica, que devem identificar os documentos vitais para a continuidade de seus negócios em caso de desastre, e que exerceriam, portanto, medidas de proteção especial sobre tais documentos.).

H. Destinação planejada – por exemplo, a remoção de materiais do sistema ativo para armazenamento fora do mesmo; transferência para os cuidados de um **custodiador confiável** (veja a Recomendação 10); eliminação prevista em tabela de temporalidade.

5. Agrupe os materiais digitais de forma lógica

Og
Organização



A gestão e a recuperação dos materiais digitais podem ser incrementadas se você puder tratá-los em grandes grupos, em vez de um por um. Portanto, é importante que você os agrupe de alguma maneira lógica. As categorias escolhidas podem refletir o modo como você trabalha, suas atividades, procedimentos, áreas temáticas ou algum tipo de organização estrutural. Separar os seus documentos arquivísticos de outros materiais digitais é um primeiro passo importante. A organização pode ser baseada nos diferentes tipos de documentos ou na quantidade de tempo pela qual certos tipos de materiais devem ser mantidos. Esses agrupamentos podem estar relacionados entre si de uma forma hierárquica ou horizontal, de acordo com as suas necessidades. De forma geral, esta estrutura deve ser equivalente à organização de seus documentos em papel (ou em outros suportes), para que, quando necessário, os documentos relacionados à mesma atividade ou assunto, ou que sejam do mesmo tipo, possam ser facilmente identificados e recuperados como parte de um mesmo agrupamento conceitual.

<< Plano de classificação >>

Plano para a identificação sistemática e o arranjo das atividades e documentos arquivísticos em categorias, de acordo com convenções logicamente estruturadas, métodos e regras de procedimento.
(veja também a Recomendação 3)

Seu esquema de organização deve ser registrado em um documento que mostre todos os agrupamentos de materiais, descreva-os de forma breve e indique como eles estão relacionados. Neste documento, chamado de **plano de classificação**, cada grupo de documentos pode ter um nome ou código que deve remeter a cada documento pertencente a ele, não importando o meio ou a localização: assim, os documentos relacionados a cada conjunto compartilharão tal código ou nome, seguido por um número que indica a sequência em que se encontram. Este identificador deve ser registrado entre os **metadados de identidade** dos seus documentos arquivísticos digitais e na face dos seus documentos de papel pertencentes ao mesmo grupo, devendo ser único para cada documento.

<< Metadados de identidade >>

Propriedades ou atributos que expressam a identidade de um objeto digital que deve ser mantido como documento arquivístico. (veja também a Recomendação 3).

A identificação do tempo necessário à manutenção dos grupos de documentos facilitará sua gestão enquanto forem utilizados com regularidade, e ajudará a garantir que os documentos que precisam ou merecem preservação de longo prazo sejam logo identificados e recebam a proteção necessária para assegurar sua permanência. Será mais fácil e eficiente definir um prazo de guarda – período que você quer ou precisa manter os materiais – para um grupo de materiais, em vez de itens individuais. Partindo de itens individuais, é muito mais trabalhoso assegurar a manutenção destes itens pelo tempo necessário, ou a eliminação do que não é mais necessário. Mesmo que você pense que, dentro de um grupo, alguns documentos devem ser mantidos por mais tempo que outros, você não apenas poupará tempo mantendo todo o conjunto, como também terá a informação mais completa quando precisar consultá-los. Contudo, para alguns tipos de documentos, você pode produzir subgrupos dentro de cada grupo, levando em conta o prazo de guarda.

At
Autenticação

6. Utilize técnicas de autenticação que favoreçam a manutenção e a preservação dos materiais digitais

A autenticidade dos materiais digitais é ameaçada sempre que eles são transmitidos através do espaço (isto é, quando enviados a um destinatário ou entre sistemas ou aplicativos) ou do tempo (quando os materiais estão armazenados, ou quando o *hardware* ou *software* usado para armazená-los, processá-los ou comunicá-los é atualizado ou substituído). Como a guarda de materiais digitais, para ação e referência futuras, e sua recuperação pressupõem inevitavelmente que eles atravessem fronteiras tecnológicas marcantes (entre subsistemas: de exibição para armazenamento e vice-versa), a inferência da autenticidade dos materiais digitais deve ser apoiada pela evidência de que estes foram mantidos utilizando tecnologias e procedimentos administrativos que garantam a continuidade de sua identidade e de sua integridade, ou que, pelo menos, minimizem os riscos de modificações desde quando os documentos foram guardados pela primeira vez até o ponto em que eles forem acessados subsequentemente.

<< AUTENTICAÇÃO >>

Declaração de autenticidade de um documento arquivístico, num determinado momento, resultante da inserção ou do acréscimo de um elemento ou afirmação por parte de uma pessoa investida de autoridade para tal.

Autenticação independente de tecnologia

Presunção de autenticidade. Uma presunção de autenticidade é uma inferência que é estabelecida a partir de fatos conhecidos sobre a forma como um documento foi produzido e mantido. A adoção e a aplicação consistente das recomendações apresentadas neste documento fornecem a melhor evidência para apoiar tal presunção. As recomendações são cumulativas: quanto maior o número de recomendações seguidas e maior o grau de satisfação de cada uma delas, maior a presunção de autenticidade. A implementação bem-sucedida das recomendações apresentadas neste documento baseia-se no estabelecimento e na aplicação contínua e efetiva de políticas e procedimentos administrativos (veja a referência aos Recursos de Preservação do Projeto InterPARES, item 3, “Arcabouço de políticas”, ao final deste documento). Preferencialmente, você deve se esforçar para implementar, sempre que possível, técnicas de autenticação apoiadas em políticas e procedimentos administrativos independentes de tecnologia e/ou neutros.

Autenticação dependente de tecnologia

Técnicas de autenticação dependentes de tecnologia, tais como a criptografia, são usadas para fornecer um mecanismo tecnológico que garanta a autenticidade dos materiais digitais. Uma destas técnicas criptográficas é a assinatura digital, que pode ser utilizada quando documentos são transmitidos entre pessoas, sistemas ou aplicativos, para declarar sua autenticidade em um dado momento. Tais tecnologias foram reconhecidas como tendo valor legal ou regulatório por alguns órgãos, como a Comissão Europeia e a Securities and Exchange Commission (SEC), dos EUA.

Atenção! As assinaturas digitais podem ficar obsoletas e, em virtude do seu objetivo e de sua funcionalidade inerente, não podem ser migradas junto com os documentos aos quais estão anexadas quando da atualização de versões ou mudança de *software*. De fato, a vida das assinaturas digitais e outras tecnologias de autenticação pode ser muito mais curta do que até mesmo o tempo de manutenção de um documento temporário, devido ao fato de a tecnologia de autenticação mudar rapidamente. A não ser que o desenvolvimento da tecnologia da assinatura digital permita que tais informações codificadas de autenticação sejam preservadas ao longo do tempo com o documento, você deve, quando receber um documento com uma assinatura digital anexada, desanexá-la sempre que possível e adicionar informações aos metadados de integridade para indicar que o documento foi recebido com tal assinatura, e que esta foi verificada, desanexada e apagada.

7. Proteja os materiais digitais de ações não autorizadas

Pr
Proteção

A acurácia e a autenticidade dos materiais digitais não podem ser presumidas se existir qualquer oportunidade de modificá-los sem deixar vestígios. Você tem que ser capaz de demonstrar que seria impossível para qualquer pessoa modificar ou manipular os seus materiais digitais sem que fosse identificada. A segurança inclui restringir o acesso físico a lugares onde os computadores são mantidos, assim como restringir o acesso aos materiais digitais nos próprios computadores; esta última medida pode ser implementada de diversas formas, como o uso de senhas e/ou autenticação biométrica para entrar no sistema.

Também é importante estabelecer uma estrutura para permissões de acessos (também chamada de privilégios de acesso – veja a discussão sobre os **metadados de integridade** na Recomendação 4) para todos os usuários do sistema. Por exemplo, alguns usuários podem apenas ser autorizados a ler os materiais, enquanto outros podem ter permissão para modificá-los. Em qualquer caso, deverá ser impossível modificar qualquer documento, uma vez que este tenha sido arquivado de acordo com o esquema ou **plano de classificação** (veja as Recomendações 3 e 5), e apenas o responsável pela manutenção deve ser capaz de transferir ou apagar materiais do sistema. Além disso, o sistema deve manter uma trilha de auditoria para rastrear o acesso aos materiais, assim como controlar a administração e uso dos privilégios de acesso.

Esta recomendação pode parecer muito rígida para indivíduos que estejam trabalhando em suas casas, ou até mesmo para aqueles que atuam em pequenos escritórios ou comunidades de prática. Mas é importante lembrar que, se você não puder demonstrar que seria impossível que alguém modificasse ou manipulasse seus materiais digitais sem ser identificado, sua certeza de que os seus documentos são acurados e autênticos “de fato” torna-se irrelevante. Neste sentido, pode ser útil manter cópias *offline*, pelo menos dos materiais mais importantes, além de estabelecer alguma rotina segundo a qual os materiais armazenados *offline* sejam aleatoriamente confrontados com seus originais *online* periodicamente.

Cs
Cópia de segurança

8. Proteja os materiais digitais de perdas acidentais e corrupção

Os computadores não são infalíveis, e inúmeros fatores podem causar a corrupção ou outras formas de perda acidental dos documentos ou dados. A melhor maneira de se prevenir contra tais eventos é fazer cópias de segurança com regularidade e frequência. Se você armazená-las em outro local, ainda consegue proteção adicional contra fogo ou roubo de equipamento. Muitas técnicas, pacotes de *software* e serviços de *backup* (ou cópias de segurança) estão disponíveis, inclusive algumas que produzem automaticamente as cópias de segurança e depois as transmitem para um local seguro.

A. Desenvolva uma política ou rotina rigorosa que assegure que seu sistema faça cópias de segurança diariamente. Seu sistema é tão bom quanto sua última cópia de segurança. Assim, você precisa se certificar de que são feitas cópias de segurança frequentemente, ao menos uma vez por dia, utilizando métodos aprovados, que assegurarão que você e/ou suas atividades serão capazes de se recuperar rapidamente se algo der errado. Tais cópias de segurança regulares devem ser eliminadas alternadamente, segundo uma estratégia ou programação que seja a mais apropriada às suas exigências, uma vez que estas cópias não contêm documentos arquivísticos, mas existem apenas para recuperação caso haja uma falha no sistema. Observe que falamos aqui de um ***backup* do sistema** abrangente, que inclui o sistema operacional, os aplicativos de *softwares* e todos os materiais digitais do seu sistema. Se você precisar ter uma cópia de segurança dos seus materiais digitais, além da cópia do sistema, para o caso de seu computador ser roubado ou de alguns de seus documentos serem corrompidos, então você deve copiar esses materiais para outro computador, um disco rígido externo ou outra mídia portátil, e guardar essas cópias de segurança em um local longe do computador que tenha as cópias "originais".

B. Escolha e instale a melhor tecnologia de cópias de segurança para o seu caso. Pesquise a tecnologia e os serviços disponíveis e escolha aqueles que funcionarem melhor para a sua situação específica. Existem muitos sistemas diferentes, desde os que cobrem operações individuais aos capazes de copiar sistemas muito amplos. O sistema de cópias de segurança precisa dispor de uma trilha de auditoria, caso ele falhe entre uma cópia e outra e você precise recuperar os documentos ou materiais digitais produzidos nesse intervalo.

Ob
Obsolescência

9. Previna-se contra a obsolescência de *softwares* e *hardwares*

A velocidade com a qual os *hardwares* e *softwares* ficam obsoletos impõe sérios desafios à manutenção e preservação em longo prazo do material digital. Uma estratégia para solucionar este problema é eliminar a dependência do *hardware*, por meio da transferência das funcionalidades do *hardware* para o *software* (isto é, usar um aplicativo para simular as ações de uma parte do *hardware*). Esta é uma forma mais estável de manter a função quando o *hardware* ficar obsoleto.

As rápidas transformações do ambiente tecnológico tornam necessário que os indivíduos e unidades administrativas atualizem regularmente tanto seus sistemas digitais como todos os documentos dentro destes sistemas e aqueles que foram armazenados em outras mídias de armazenamento, tais como CD, DVD ou fita. Em outras palavras, quando partes do ambiente tecnológico em que você está trabalhando começam a se tornar obsoletas, elas devem ser atualizadas para a tecnologia mais avançada disponível, de acordo com suas exigências e obrigações particulares, e todos os materiais digitais dentro e fora do sistema devem ser migrados para essa nova tecnologia. Quando substituir o *hardware*, é importante que o novo tenha capacidades ao menos iguais às do anterior. Por exemplo, um monitor novo precisa mostrar um documento gráfico de maneira que a forma documental original seja mantida. Planejar atualizações regulares de tecnologia, de acordo com um sistema de rodízio, assegurará que sua tecnologia não se torne ultrapassada e também ajudará a prevenir gastos expressivos e inesperados.

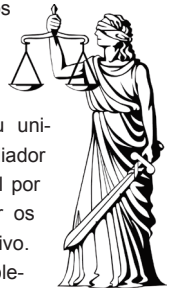
Documentos digitais produzidos ou mantidos em sistemas que estão se tornando obsoletos algumas vezes precisam ser preservados por um longo tempo, mas não se espera que sejam acessados frequentemente. Se estes documentos forem textuais e precisarem ser lidos em sequência, ao invés de aleatoriamente, você pode convertê-los da sua forma digital para microfilme, produzido a partir de um computador. Isto os protegerá de perdas acidentais ou corrupção melhor do que qualquer outra medida. Outra boa medida de proteção é a duplicação – produzir uma segunda cópia de grupos de documentos vitais e mantê-la em outro computador, ou num segundo disco rígido, ou em DVD, em outro local de trabalho ou com outra pessoa, ou ainda em armazenamento remoto. Quando documentos digitais ou outras entidades são removidos de um sistema ativo para armazenamento externo em mídia magnética ou óptica, por exemplo, é essencial que a documentação sobre o sistema e os documentos digitais (como os metadados dos documentos arquivísticos) sejam também removidos e mantidos com eles. Para informações mais detalhadas sobre os tipos de documentação em questão, veja a Recomendação 1, subseções D, E e F.

Co
Consciência

10. Considere os aspectos relacionados à preservação em longo prazo

Embora o foco deste documento seja a produção e manutenção de todos os tipos de materiais digitais enquanto necessários regularmente para o produtor, é importante considerar a melhor maneira de preservar aqueles mais relevantes por um longo período de tempo. De forma geral, apenas uma pequena porcentagem dos materiais precisa ser preservada por longo prazo, mas a habilidade de prover um cuidado contínuo e por um longo período para os materiais, especialmente os digitais, está frequentemente além da capacidade ou interesse das pessoas e pequenas organizações. Existem custos reais – tanto financeiros quanto humanos – na guarda dos materiais em longo prazo, mas tais esforços de preservação são essenciais para constituir e manter nosso patrimônio cultural, para prestação de contas e para fornecer informações para o processo da tomada de decisão.

Para começar esse processo, você deve identificar alguém que se encarregará dos seus materiais digitais, uma vez que eles não sejam mais necessários para propósitos pessoais e profissionais com regularidade. Esta pessoa teria o papel de **custodiador confiável**. Um custodiador confiável é um profissional – ou um grupo de profissionais, como um arquivo ou uma sociedade histórica comunitária – que tem formação em manutenção e preservação de documentos, e que preferencialmente não tem relação com o conteúdo dos documentos ou interesse em permitir que outros os manipulem ou destruam. No caso de pequenas organizações ou unidades administrativas, o custodiador pode ser a pessoa responsável por manter, organizar e armazenar os documentos durante seu uso ativo. No caso de indivíduos que implementam a manutenção de seus próprios documentos, a pessoa encarregada da preservação pode ser um arquivista ou um bibliotecário, seja de um centro de documentação ou simplesmente um profissional da área. Em todos os casos, uma estratégia de preservação deve ser definida o mais cedo possível, porque os materiais digitais que não se tornarem logo objetos de preservação e não forem cuidados de forma proativa não serão preservados. A aderência estrita a estas diretrizes, portanto, facilitará a preservação em longo prazo.



<< CUSTODIADOR CONFIÁVEL >>

Preservador que pode demonstrar que não tem razões para alterar ou permitir que outros alterem os documentos arquivísticos preservados, e é capaz de implementar todos os requisitos para a preservação de documentos arquivísticos autênticos.

Conclusão

Co
Conclusão

Este documento descreveu uma série de atividades para que indivíduos e pequenas organizações consigam produzir e manter materiais digitais que possam ser presumidos autênticos, acurados e confiáveis. Para os indivíduos, o desafio pode parecer grande, mas a alternativa – a perda de documentos ou o surgimento de dados corrompidos e incorretos – seria um problema ainda maior ao longo do tempo. Pequenas organizações se beneficiarão ao fazer uma designação clara da pessoa ou pessoas responsáveis por supervisionar a manutenção dos documentos digitais da organização. Saiba, contudo, que nem todas as recomendações apresentadas neste documento precisam ser aplicadas em cada circunstância; você deve ser capaz de selecionar e adotar as medidas que respondem a seus problemas específicos no contexto em que você trabalha. Também pode haver casos nos quais sejam necessárias medidas adicionais, devido a exigências legais ou regulatórias do seu campo de atuação, ou devido às características da atividade e, portanto, dos documentos que ela produz. Em tais casos, pode ser preciso consultar especialistas, que podem ser os arquivistas dos arquivos nacionais, estaduais ou municipais, bem como associações arquivísticas locais. Indivíduos, unidades administrativas e pequenas organizações não devem hesitar em contatar tais especialistas para pedir conselhos sobre assuntos relacionados à produção e manutenção de seus documentos digitais.

O Projeto InterPARES

A sociedade preserva sua memória na sua arte e arquitetura, em seus livros e outros materiais impressos, e nos registros de suas ações feitos sob a forma de documentos. Os documentos arquivísticos são únicos e participam ou resultam das atividades de indivíduos e organizações, constituindo a fonte primária de conhecimento sobre essas atividades. Cada vez mais, são gerados em forma digital e sua preservação é complicada pela rapidez com que os *hardwares* e *softwares* ficam obsoletos, pela fragilidade da mídia de armazenamento digital e pela facilidade com que a informação digital pode ser manipulada. Uma parte da memória documental da nossa sociedade produzida e preservada digitalmente já foi comprometida. Já é visível que a ameaça virou realidade e se alastrou, embora ainda falte quantificar adequadamente as informações digitais de valor que foram perdidas, ou cuja recuperação tornou-se muito cara. Além disso, já que destacamos tal ameaça, devemos lembrar que os documentos preservados têm pouco valor se não pudermos assegurar que eles são autênticos, isto é, que eles podem ser confiáveis enquanto fontes. Por séculos, a autenticidade dos documentos baseou-se em elementos tais como selos e assinaturas, em mecanismos de controle dos procedimentos para gerar, transmitir, usar e manter os documentos, e numa cadeia de custódia ininterrupta. O uso de tecnologia digital para produzir documentos reconfigurou os elementos formais tradicionais por meio dos quais eles eram reconhecidos como autênticos, permitiu que os controles procedimentais fossem ignorados e tornou menos preciso o conceito de custódia física.

O Projeto InterPARES (*International Research on Permanent Authentic Records in Electronic Systems*)[2] foi lançado em 1999 para tratar desses assuntos. Este projeto multidisciplinar, que concluiu sua pesquisa em 2006, envolveu mais de cem pesquisadores de mais de vinte países em cinco continentes e foi constituído de duas fases.[3]

InterPARES 1 (1999-2001) foi conduzido do ponto de vista do preservador e fez pesquisas sobre a preservação de documentos arquivísticos administrativos autênticos produzidos e mantidos em bases de dados e sistemas de gestão de documentos, e que não eram mais necessários para atender aos propósitos de seu produtor.

InterPARES 2 (2002-2007) tomou como perspectiva o ponto de vista do produtor do documento arquivístico, com o objetivo de desenvolver teoria e métodos capazes de garantir a confiabilidade, a acurácia e a autenticidade dos documentos digitais, desde sua produção até sua preservação. O foco do projeto foi em documentos complexos, tipicamente produzidos em sistemas digitais interativos, experienciais e dinâmicos, produzidos no curso de atividades artísticas, científicas e de governo eletrônico. O InterPARES 2 também buscou desenvolver a consciência sobre assuntos tais como propriedade intelectual e privacidade dos dados, por meio de um diálogo contínuo com indivíduos e organizações.

Recursos de Preservação do Projeto InterPARES

Este conjunto de diretrizes é apenas um dos muitos recursos tratados em ambas as fases do projeto InterPARES, que apoiam o entendimento da natureza dos documentos arquivísticos digitais e o desenvolvimento de métodos para sua produção confiável e para sua manutenção e preservação de forma acurada e autêntica. Essas ferramentas inestimáveis podem ser usadas por indivíduos, organizações e órgãos governamentais como diretrizes e instrumentos para lidar com os problemas apresentados por seus materiais digitais. Estas diretrizes também servem para fornecer informações para as atividades dos órgãos de padronização nacionais e internacionais. Alguns dos recursos-chave são descritos a seguir, e uma lista mais abrangente pode ser encontrada no *site* do InterPARES na internet, em: www.interpares.org.

1. Requisitos de autenticidade. Este recurso do InterPARES 1 é composto de dois conjuntos de exigências para avaliar e manter a autenticidade dos documentos arquivísticos digitais; um deles destinado a produtores de documentos e o outro, a preservadores. O primeiro conjunto, conhecido como **Requisitos de Referência para a Autenticidade**, contém as exigências que apoiam a presunção de autenticidade dos documentos arquivísticos digitais de um produtor, antes que eles sejam transferidos para a custódia do preservador. O segundo conjunto, conhecido como **Requisitos de Base para a Autenticidade**, é composto por exigências que apoiam a produção de cópias autênticas dos materiais digitais transferidos para a custódia do preservador e mantidos em seu sistema de preservação.

2. Modelo de análise. Este recurso do InterPARES 1 propicia a decomposição do documento digital em suas quatro partes constituintes necessárias: a forma documental, as anotações, o suporte e os contextos (isto é, tudo o que envolve a ação da qual o documento participa, o que inclui seus contextos administrativo, de procedimento, documental, tecnológico e de proveniência). O modelo define cada parte e cada elemento da forma, explica seu propósito e indica se, e até que ponto, tal parte ou elemento é útil para avaliar a autenticidade do documento. Em um nível mais básico, o modelo serve como uma lista com definições que ajudam os usuários a determinar, até mesmo, se eles estão lidando com um documento arquivístico de fato.

3. Arcabouço de políticas. Este recurso do InterPARES 2 é composto de dois conjuntos complementares de princípios para a produção e preservação de documentos digitais autênticos que, juntos, ajudam a estruturar a relação entre os produtores e os preservadores, fornecendo um guia para estabelecer um arcabouço intelectual abrangente, dentro do qual eles podem desenvolver ambientes com políticas consistentes e integradas que conduzam à preservação efetiva e coordenada dos documentos digitais.

4. Diretrizes para produtores. Este documento.

5. Diretrizes para preservadores. Este recurso do InterPARES 2 fornece recomendações concretas para qualquer organização responsável pela preservação a longo prazo de documentos digitais.

6. Dois modelos de gestão de documentos arquivísticos. Estes modelos do InterPARES 2 descrevem, de forma gráfica e narrativa, todas as atividades e ações importantes e específicas que devem ser tomadas, bem como as entradas, saídas, mecanismos de capacitação e restrições ou controles, com o objetivo de produzir, gerenciar e preservar documentos arquivísticos digitais confiáveis e autênticos. Desta forma, ambos os modelos caracterizam os dados e a informação que deve ser reunida, armazenada e utilizada para apoiar os vários processos de gestão ao longo da vida do documento.

Modelo da Cadeia de Preservação.[4] O modelo da Cadeia de Preservação, baseado na tradicional abordagem do "ciclo de vida dos documentos", apresenta as perspectivas específicas nas situações do produtor, do gestor e do preservador dos documentos.

Modelo de Manutenção de Documentos Orientada pelas Atividades do Produtor.[5] O modelo de Manutenção de Documentos Orientada pelas Atividades do Produtor, baseado na abordagem do *records continuum*, adota a perspectiva do produtor de documentos arquivísticos.

7. Base de dados de terminologia. Este recurso do InterPARES 2 contém três instrumentos de terminologia: Glossário, Dicionário e Ontologias. O **Glossário** é uma lista de termos autorizados e definições que são fundamentais para nosso entendimento dos ambientes de produção, manutenção e preservação de documentos em evolução. O **Dicionário** é usado para facilitar a comunicação interdisciplinar. Ele contém múltiplas definições para termos de diversas disciplinas. Ao usar esta ferramenta, os usuários podem ver como a Arquivologia utiliza a terminologia em comparação com a Ciência da Computação, a Biblioteconomia e a Ciência da Informação, as Artes etc. As **Ontologias** identificam as relações explícitas entre conceitos de documentos arquivísticos. Isto é útil para comunicar as nuances da Diplomática no ambiente digital interativo, experiencial e dinâmico.

8. Sistema de Análise e Registro de Descrição Arquivística e Metadados (MADRAS).[6] Este recurso *online* interativo do InterPARES 2 é um repositório de esquemas destinado a ajudar na identificação dos conjuntos de metadados, ou das combinações de elementos de diferentes conjuntos, que servem para atender a várias necessidades de manutenção e preservação a longo prazo dos documentos. Em resposta a uma demanda do usuário, o MADRAS fornece recomendações sobre como cada esquema pode ser expandido ou revisado para atender às necessidades de confiabilidade, autenticidade e preservação dos documentos digitais produzidos dentro do domínio, comunidade ou setor do usuário.