Dpd

Diretrizes do produtor

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

Elementos de preservação

6 Pr Proteção				
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
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

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.

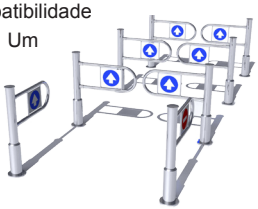
Estas diretrizes objetivam fornecer recomendações para a produção e manutenção de materiais digitais confiáveis em geral, e de documentos arquivísticos em particular, que possam ser precisa e autenticamente mantidos e preservados ao longo do tempo. Para facilitar sua aplicação, contudo, os termos "confiabilidade",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

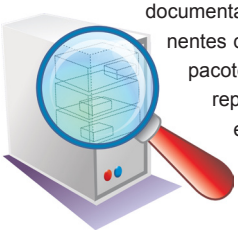
<< Padrão de fato >>

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.

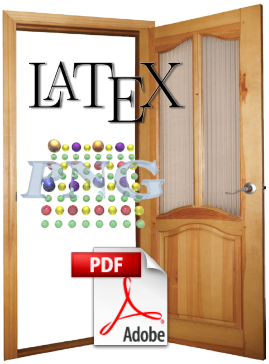
D. Mantenha as especificações do *software*. Este tipo de documentação (por exemplo, o manual do proprietário ou qualquer outra descrição mais detalhada do *software* que você possa ter) será essencial, com o avanço da tecnologia no futuro, para acessar os materiais ou para migrá-los para um novo ambiente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

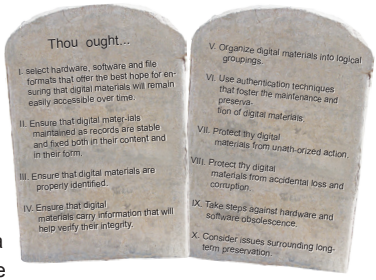


G. Sempre que possível, escolha formatos independentes de plataforma, amplamente utilizados, não proprietários e não comprimidos, com especificações disponibilizadas gratuitamente. Estes são frequentemente chamados de "formatos abertos", o que significa que suas especificações são publicadas e disponibilizadas 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).

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 >>

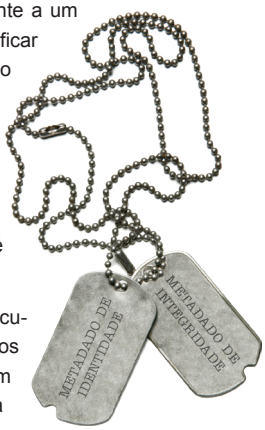
Elementos de um documento arquivístico que constituem sua aparência externa, inclusive as características de apresentação, como fonte, gráficos, imagens, sons, *layouts*, *hyperlinks*, resoluções de imagens etc., assim como selos, assinaturas digitais, carimbos de tempo e sinais especiais (marcas d'água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

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.

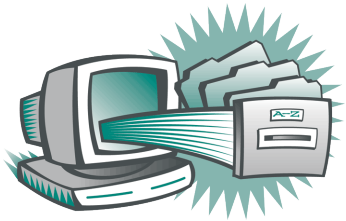
F. Código de privilégios de acesso – indicação da pessoa, cargo ou unidade autorizada a fazer anotações nos materiais, apagá-los ou removê-los do sistema, se aplicável.

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.

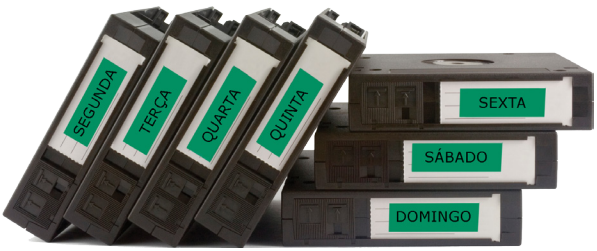
Cs
Cópia de segurança

8. Proteja os materiais digitais de perdas acidentais e corrupção

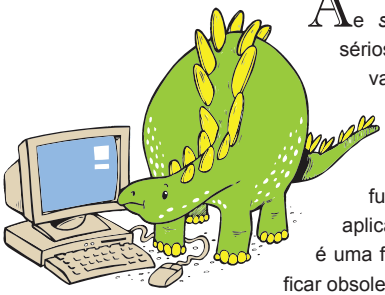
Os computadores não são infalíveis, e inúmeros fatores podem causar a corrupção ou outras formas de perda acidental dos documentos ou dados. A melhor maneira de se prevenir contra tais eventos é fazer cópias de segurança com regularidade e frequência. Se você armazená-las em outro local, ainda consegue 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.



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

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.

Re
Recursos

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.

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.

5 Mg Migração

8 Md Metadados

9 Cs Cópia de seguran

25 Cc Custódia Confiáv

Dpv

Diretrizes do preservador

A PRESERVAÇÃO DE DOCUMENTOS ARQUIVÍSTICOS DIGITAIS: DIRETRIZES PARA ORGANIZAÇÕES

In
Introdução

Introdução

Estas diretrizes foram desenvolvidas com o propósito de fornecer recomendações concretas a vários grupos responsáveis pela preservação a longo prazo de documentos arquivísticos digitais. O objetivo não é ser abrangente, mas sim enfatizar algumas áreas especialmente importantes para a preservação de documentos arquivísticos digitais autênticos, e que a prática já demonstrou serem muitas vezes negligenciadas na pressa de incluir documentos arquivísticos digitais em repositórios de arquivo.

Como já é amplamente conhecido, os documentos digitais devem ser geridos cuidadosamente durante toda a sua existência, a fim de garantir sua acessibilidade e legibilidade ao longo do tempo, mantendo intactos sua forma, seu conteúdo e suas relações até quando for necessário para a continuidade de sua credibilidade como documentos de arquivo. Também já se sabe bem que a gestão de documentos arquivísticos digitais deve ser realizada a partir de uma vasta compreensão de todas as fases ou estágios da existência desses documentos, desde quando são gerados, passando pela sua manutenção por parte do produtor e pela sua avaliação, destinação e preservação a longo prazo como registros autênticos das ações e assuntos que integram. Do ponto de vista da preservação a longo prazo, todas as atividades para gerenciar os documentos, no curso de sua existência, estão ligadas, como em uma cadeia, e são interdependentes. Se um elo se rompe, a cadeia não pode executar sua função. Se certas atividades e ações não são realizadas com os documentos, sua integridade (ou seja, suas confiabilidade e autenticidade) e sua preservação estão em risco.

Estas diretrizes enfocam o elo de preservação da cadeia de preservação e estão organizadas de acordo com a sequência de atividades apresentadas no modelo[1] da **Cadeia de Preservação** (CP)[2] do InterPARES, que mostra os vários passos sequenciais para a produção, manutenção e preservação de documentos autênticos. O código alfanumérico, que aparece entre parênteses ao lado do título de cada seção destas diretrizes, constitui uma referência cruzada à respectiva atividade de preservação apresentada no modelo CP.

As diretrizes foram elaboradas de forma a responder às necessidades de preservação de organizações ou de programas cujos documentos arquivísticos têm que ser guardados e consultados durante longos períodos, bem como às necessidades das instituições arquivísticas responsáveis pela preservação a longo prazo de documentos arquivísticos de terceiros e pela continuidade de sua acessibilidade ao público-alvo. Nos dois casos, de organizações e de instituições arquivísticas, tanto os recursos humanos e financeiros como o conhecimento técnico especializado são frequentemente limitados.

Instituições, organizações e programas com atribuições de preservação devem também consultar o **Arcabouço de Princípios para o Desenvolvimento de Políticas, Estratégias e Padrões para a Preservação a Longo Prazo de Documentos Arquivísticos Digitais** (*Framework of Principles for the Development of Policies, Strategies and Standards for the Long-term Preservation of Digital Records*, também conhecido como **Arcabouço de políticas**)[3], desenvolvido pelo Domínio Transversal de Políticas do InterPARES 2[4], que complementa estas diretrizes. Muitas recomendações contidas aqui também podem ser aplicadas à preservação de entidades digitais que não sejam documentos arquivísticos, como publicações, dados ou documentos não arquivísticos.

Definições

Antes de apresentar as recomendações para orientar o leitor na preservação de documentos digitais, será necessário, e de grande ajuda, esclarecer o significado de alguns termos usados neste documento.

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

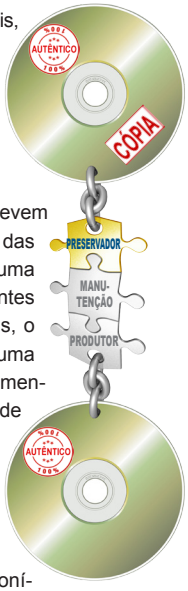
Estas diretrizes têm como objetivo fornecer recomendações para a manutenção e preservação, de forma acurada e autêntica, dos documentos arquivísticos digitais ao longo do tempo. Para facilitar a sua aplicação, contudo, os termos “acurácia”, “autenticidade” e “autenticação” precisam ser definidos.

Para os propósitos destas diretrizes, **acurácia** é o grau de precisão, correção, verdade e ausência de erros e distorções existente 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 documentos arquivísticos (se for aplicável). **Autenticidade** refere-se ao fato de que os documentos arquivísticos 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 documentos arquivísticos e proteger sua integridade. A autenticidade é colocada em risco sempre que os documentos arquivísticos 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 em longo prazo dos documentos arquivísticos. **Autenticação** é a declaração da autenticidade, resultante da inserção ou da adição de elementos ou afirmações nos documentos arquivísticos em questão, e as normas que a regulam são estabelecidas pela legislação. Ou seja, é um meio de assegurar que os documentos arquivísticos 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 documentos arquivísticos são autênticos apenas quando recebidos e não podem ser repudiados; porém, tais medidas não asseguram que eles permanecerão autênticos depois disto.

Ge
Gestão

1. Gerencie a estrutura da cadeia de preservação (A1)

Este aspecto envolve a definição dos requisitos estruturais, bem como o desenho, a implementação e a manutenção de uma estrutura de cadeia de preservação. Uma **Estrutura de Cadeia de Preservação** inclui todos os elementos de política, estratégia, metodologia, entre outros necessários para o gerenciamento de documentos digitais.



1.1. Defina o escopo e os objetivos. Os responsáveis pela preservação devem definir o escopo e os objetivos do seu programa de preservação digital. No campo das artes, por exemplo, podem querer preservar o registro da(s) representação(ões) de uma obra, ou podem escolher realizar uma preservação mais complexa dos componentes de uma obra de arte que propiciam a sua reprodução ou reexecução. Nas ciências, o preservador poderá optar por preservar apenas o relatório final dos resultados de uma experiência ou guardar os dados brutos, normalizados e/ou agregados, a fim de documentar a metodologia usada e o resultado obtido, bem como assegurar a disponibilidade dos dados para usos futuros. Os responsáveis pela preservação devem também levar em consideração a identidade dos usuários eventuais dos arquivos. Usuários tecnicamente sofisticados normalmente exigem menos assistência no acesso a materiais digitais, mesmo os de grande complexidade, ao passo que o público em geral pode exigir mecanismos de acesso mais amigáveis para usuários e materiais transformados em alguns poucos formatos mais simples, porém largamente disponíveis. O escopo do programa de preservação ajudará a definir as estratégias (consultar a **Seção 4** e o **Apêndice C**, **Seção B**) que um preservador possivelmente precisará seguir.

Ao definir o programa de preservação digital, os preservadores devem se basear em experiências anteriores. A fim de desenvolver políticas e estratégias adequadas, devem consultar o Arcabouço de Políticas do InterPARES 2 para orientação aplicável aos níveis organizacional, setorial, nacional, internacional e supranacional. Com relação às funções do programa de preservação, os responsáveis por ela devem consultar o padrão *ISO Open Archival Information System* (OAIS)[5] e seguir o modelo de Cadeia de Preservação do InterPARES 2 para uma adaptação do padrão OAIS especificamente direcionado para documentos arquivísticos digitais. O planejamento deve também refletir a Lista de Auditoria para a Certificação de Repositórios Digitais (*Audit Checklist for Certifying Digital Repositories*)[6], de autoria da Força-Tarefa sobre Repositórios Digitais do National Archives and Records Administration (NARA) e do Research Libraries Group (RLG).

1.2. Adquira recursos. A preservação digital exige recursos substanciais em termos de financiamento, capacidades tecnológicas e conhecimento especializado. Uma organização responsável pela preservação digital tem várias opções, que incluem: a) **adquirir novos recursos**, b) **redistribuir recursos existentes** e/ou c) **alavancar outros recursos**.

Independentemente da(s) opção(ões) escolhida(s), um pré-requisito fundamental é que os recursos sejam sustentáveis. Recursos eventuais, como doações, são mais indicados para tarefas finitas específicas, tais como o estabelecimento do programa de preservação ou processamento de um determinado conjunto de documentos arquivísticos, mas uma fonte confiável de recursos sustentáveis constitui uma condição *sine qua non* para qualquer programa de preservação.

A **aquisição de novos recursos financeiros** exigirá um planejamento sólido e um plano de comunicação compatível para convencer as fontes de financiamento e as partes interessadas de que o programa deve ser financiado. Uma estratégia viável para um programa novo pode ser começar com

poucos recursos e se planejar a partir dos êxitos de curto prazo para tentar convencer as fontes de financiamento a aumentar gradualmente os recursos para o programa. Uma estratégia de incremento deve avaliar se as fontes de financiamento poderão ser influenciadas mais facilmente pelo sucesso a curto prazo em metas básicas do programa ou em áreas de maior relevância para elas. Por exemplo, as fontes podem ser mais influenciadas por demonstrações de capacidade tecnológica do que por um plano sólido e abrangente para a avaliação de documentos arquivísticos digitais.

Para a maioria das organizações, a **redistribuição de recursos** para a preservação digital pode levar a escolhas dolorosas. Assim como na procura de novos financiamentos, talvez seja melhor uma abordagem incremental. Além disso, é possível fazer ajustes ao plano enquanto este se desenvolve, com base na experiência ganha durante cada fase da implementação. Quando for implantar um programa de preservação digital numa instituição de grande porte, é melhor considerar a preservação digital como parte de um plano estratégico geral do que colocá-la como uma iniciativa especial.

Mesmo quando um preservador tem êxito na captação de recursos ou consegue redirecionar os existentes para a preservação digital, é pouco provável que tenha recursos suficientes para enfrentar todos os desafios. Portanto, os responsáveis pela preservação devem investir em oportunidades para **alavancar recursos externos**. Há vários caminhos para se fazer isso. Por exemplo, em vez de tentar contratar técnicos especialistas de forma permanente ou treinar pessoal em todos os conhecimentos e habilidades técnicas necessárias, os preservadores podem contratar especialistas externos como consultores ou para realizar tarefas específicas. Não se deve descartar a possibilidade de contratação tanto para a realização de tarefas básicas quanto *ad hoc*. Num nível básico, os preservadores devem avaliar a possibilidade de usar um provedor de serviços de informática em vez de adquirir um sistema de preservação exclusivo. As opções *ad hoc* incluem a contratação de empresas especializadas para a realização de tarefas, tais como recopiar a partir de mídias digitais obsoletas ou converter formatos raros. Outra opção seria participar – ativa ou passivamente – em comunidades de código aberto que desenvolvem tecnologias necessárias à preservação digital (por exemplo, FEDORA[7], *Global Registry of Digital Formats*[8]).

Finalmente, em uma organização em que faltam recursos para dar suporte a um programa de preservação digital, os preservadores devem investigar a possibilidade de estabelecer consórcio ou parcerias colaborativas, com o objetivo de desenvolver e financiar um programa que obedeça a um padrão mínimo aceitável.

1.3. Concentre-se nos documentos arquivísticos digitais. Os preservadores devem assegurar que os recursos de preservação digital tenham como objetivo principal a proteção de cópias oficiais de documentos digitais, em vez de preservar **cópias digitalizadas** de documentos analógicos remanescentes. Tal lógica baseia-se na idéia de que a maioria dos documentos analógicos sobreviverá sem digitalização, enquanto que os documentos arquivísticos digitais se perderão sem um programa de preservação digital.

> **<< 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.

1.4. Ofereça orientação. Como a cadeia de preservação de documentos arquivísticos digitais começa na produção, os preservadores devem fornecer orientações sobre a produção e manutenção de documentos arquivísticos digitais. Dependendo do mandato do preservador, isto poderá, por exemplo, ser direcionado especificamente para empregados na instituição de preservação ou, no caso dos arquivos nacionais, para outras instituições governamentais. Em outros casos, as orientações devem ser amplamente disseminadas para grupos de interesses específicos ou o público em geral, com o objetivo de atingir a(s) pessoa(s) ou organização(ões) cujos documentos estejam sob a responsabilidade do preservador.

1.5. Dê o bom exemplo. Os preservadores devem estabelecer, dentro da sua organização, um ambiente de elaboração e manutenção de documentos de tal forma que os seus próprios documentos arquivísticos de controle, produzidos no curso da sua função de preservação, sejam produzidos e mantidos de maneira a satisfazer os padrões dos **Requisitos de Referência** para Apoiar a Presunção de Autenticidade de Documentos Arquivísticos Digitais, do InterPARES 1 (consultar o **Apêndice A** para uma versão mais resumida).[9] Além de se tratar de um requisito essencial para qualquer organização que se dedique à preservação a longo prazo, o desenvolvimento deste tipo de ambiente interno oferecerá:

- ❒ um treinamento prático para arquivistas sobre as tecnologias que eles recomendam para os produtores de documentos;
- ❒ o precioso ponto de vista do usuário a respeito das soluções reais de manutenção de documentos arquivísticos e sobre como estas realmente funcionam num ambiente operacional cotidiano;
- ❒ um campo de testes onde as atualizações e as inovações possam ser introduzidas e avaliadas; e
- ❒ um protótipo de trabalho que possa ser usado em demonstrações.

1.6. Desenvolva procedimentos. Os preservadores devem estabelecer controles sobre a transferência, manutenção e reprodução de documentos arquivísticos. Estes controles devem incluir os procedimentos e sistema(s) usados para a transferência de documentos dentro da própria organização ou programa e para a sua manutenção e reprodução, de uma forma que satisfaça os **Requisitos de Base** para Apoiar a Produção de Cópias Autênticas de Documentos Arquivísticos Digitais, do InterPARES 1 (consultar o **Apêndice B** para uma versão resumida).[10] Estes procedimentos devem incorporar controles adequados e eficazes para garantir a **identidade** e a **integridade** dos documentos arquivísticos, e devem especificamente:

- ❒ manter a custódia ininterrupta dos documentos arquivísticos;
- ❒ implementar e monitorar procedimentos de segurança e controle;
- ❒ garantir que o conteúdo dos documentos arquivísticos e as anotações e elementos da forma documental não sofram alterações após a reprodução.

<< IDENTIDADE >>

Conjunto de características de um documento ou documento arquivístico que o identifica como único e o distingue dos demais. Junto com a integridade, é um componente da autenticidade.

<< INTEGRIDADE >>

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

1.7. Implemente estratégias de manutenção. Embora se preste muita atenção ao desenvolvimento de estratégias complexas de preservação de longo prazo, elas não podem ser aplicadas se os documentos arquivísticos para os quais são previstas não estiverem corretamente mantidos e protegidos nos sistemas de manutenção e/ou preservação que os contêm. Uma versão completa das oito principais estratégias de manutenção está disponível no **Apêndice C**, **Seção A**. De forma resumida, incluem:

A1. Distribuição clara de responsabilidades
A2. Provisão de infraestrutura técnica adequada
A3. Implementação de um plano para manutenção, suporte e substituição do sistema
A4. Implementação de um plano para a transferência regular de documentos arquivísticos para novas mídias de armazenamento
A5. Adesão a condições adequadas de armazenamento e manuseio voltadas para mídias de armazenamento
A6. Redundância e *backup* regular das entidades digitais
A7. Estabelecimento de um sistema de segurança
A8. Planejamento para situações de emergência

2. Avalie documentos para preservação permanente (A4.2)

Av
Avaliação

Nos casos em que, tal como recomendado pelo modelo de Cadeia de Preservação do InterPARES 2, for adotada uma tabela de temporalidade, as decisões sobre a destinação dos documentos arquivísticos serão tomadas regularmente como parte da gestão de um sistema de manutenção de documentos. Em alguns casos, avaliações poderão ser conduzidas quando for determinado que documentos arquivísticos em um sistema de longa duração necessitam alcançar uma destinação.[11] A seguir, oito aspectos importantes do processo de avaliação serão discutidos.

2.1. Avalie logo. Dadas as dificuldades técnicas envolvidas na preservação de documentos digitais, a identificação de quais documentos precisam ser preservados a longo prazo deve ser feita o mais cedo possível. Fazer a avaliação, estabelecer métodos de transferência e mesmo identificar potenciais estratégias de preservação com o produtor dos documentos aumentará a probabilidade de sucesso. Este processo poderá também dar ao preservador uma oportunidade de oferecer orientação sobre a produção e manutenção de documentos (consultar a **Seção 1.4**).

Preservadores profissionais, como os arquivistas, são frequentemente estimulados a participar na concepção de aplicativos de computador desenvolvidos pelas organizações com as quais eles mantêm um relacionamento produtor-preservador. Esta abordagem ajudará a integrar as práticas adequadas de manutenção e preservação de documentos. Os preservadores que integraram equipes de desenvolvimento de sistemas aprenderam que esta é uma prática que consome bastante tempo, e que requer uma compreensão bem mais detalhada dos fluxos de trabalho e procedimentos internos da organização do que aquela que um arquivista normalmente adquire durante o processo de avaliação. Além disso, as especificações do sistema raramente são uma descrição correta do aplicativo que será posteriormente implementado. Ainda terá de ser feita uma avaliação logo que o sistema estiver em operação e satisfizer os requisitos organizacionais. Poderá ser mais razoável para os arquivistas contribuírem para o *design* do sistema como parte da função de orientação discutida na **Seção 1.4**. O compartilhamento de estratégias, princípios e diretrizes de alto nível desenvolvidos pela arquivística pode provar ser uma meta mais realista.[12]

2.2. Localize múltiplos proprietários. Nos casos em que os componentes intelectuais de uma entidade digital têm múltiplos proprietários, estes devem ser identificados durante o processo de avaliação a fim de se estimar as ramificações de tal situação na preservação a longo prazo. Isto pode ocorrer, por exemplo, nos casos em que instituições governamentais de vários níveis contribuem com recursos de dados e partilham o acesso a eles. Outro exemplo são os sites da Internet que acessam e usam recursos localizados fora do seu âmbito de controle. Embora acordos de acesso sejam negociados com frequência nestas circunstâncias, eles raramente incluem dispositivos relativos à preservação de longo prazo de todos os componentes digitais significativos.

2.3. Verifique a autenticidade.

A verificação de autenticidade sempre fez parte do processo tradicional de avaliação de arquivos. Na primeira instância, baseava-se na confirmação da existência de uma cadeia de custódia ininterrupta desde o momento da produção do documento até a sua transferência para a entidade arquivística responsável pela sua preservação a longo prazo. Os períodos em que os documentos não estiveram submetidos a algum tipo de medida de proteção pelo seu produtor, ou por uma instituição posterior a ele que tivesse interesse em manter a acurácia e completeza dos documentos, podem causar muitas dúvidas sobre a autenticidade dos mesmos.

A verificação da autenticidade também dependia do conhecimento do arquivista a respeito das práticas de manutenção de documentos, tanto historicamente quanto em relação aos tipos de documentos e procedimentos administrativos de um produtor em particular. O quadro geral para esta verificação foi originalmente codificado pela diplomática.[13] Um terceiro método, usado com menor frequência para confirmar a identidade e a integridade dos documentos, baseia-se na comparação. Documentos de um fundo arquivístico são comparados a cópias encaminhadas e mantidas por fontes externas no curso normal do trabalho do produtor.

Os documentos arquivísticos produzidos e mantidos usando tecnologia digital apresentam dificuldades adicionais, e os arquivistas ainda não desenvolveram práticas padronizadas para verificar a autenticidade neste ambiente. Essas questões relacionam-se ao fato de que as entidades digitais são facilmente duplicadas, distribuídas, renomeadas, reformatadas ou convertidas, como também podem ser facilmente falsificadas sem deixar rastro. Os exemplos seguintes ilustram a extensão da perda para arquivistas, historiadores, juristas e outros que precisam de documentos arquivísticos autênticos para o seu trabalho:

- o suporte físico em que os documentos digitais são armazenados perdeu muito da sua importância para a confirmação da data de um documento ou do seu lugar de elaboração. Qualquer pessoa com acesso a equipamento obsoleto, ainda em funcionamento, e a mídias de armazenamento tem a capacidade de copiar arquivos digitais para, por exemplo, uma fita magnética de 9 faixas ou disquetes de 5 1/4";
- o carimbo de data em qualquer arquivo digital pode ser modificado se o relógio do sistema for ajustado;
- poucas instituições compreenderam o que os seus funcionários fariam, quando lhes fosse confiado um *software* de processamento de texto. Formulários de documentos típicos, tais como memorandos e correspondência com cabeçalho, desapareceram sob o massacre de formulários de documentos novos e individualizados, que rapidamente acrescentaram cores personalizadas, gráficos e mesmo efeitos sonoros, bem como a atribuição de novos significados a letras maiúsculas, cores e ao desenvolvimento de *emoticons*. O grau de erosão das práticas mais comuns de produção de documentos variou enormemente com relação a tipos e dimensões de organizações privadas e governamentais;
- a introdução de redes de e-mail permitiu que os documentos circulassem entre os funcionários por muitos caminhos novos, em vez de seguirem as rotas de distribuição consolidadas, segundo os procedimentos tradicionais da organização; e
- as reduções drásticas de pessoal nas atividades de gestão de documentos e arquivos na maioria das organizações, alimentadas por uma premissa de que os objetos digitais de alguma forma não precisavam ser geridos, acabaram com os acervos dos arquivos correntes que deixaram de receber documentos produzidos e transmitidos em forma digital.

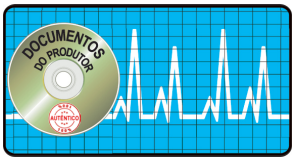
Ao avaliar os documentos produzidos num ambiente digital, a verificação de sua autenticidade deve ser um processo mais aberto e visível, realizado e documentado pelo preservador. A cadeia de custódia ininterrupta, o conhecimento de práticas de manutenção de documentos e a verificação podem ainda oferecer algumas garantias de autenticidade. Também deve ser acrescentada a verificação da conformidade com cada uma das exigências dos Requisitos de Referência para a Autenticidade, listados na **Seção 2.4**.

2.4. Documente a verificação de autenticidade.

O relatório de avaliação deve documentar os controles estabelecidos pelo produtor para garantir a identidade e a integridade dos documentos arquivísticos, e, consequentemente, a presunção da sua autenticidade. Tais controles incluem cada um dos Requisitos de Referência para Apoiar a Presunção de Autenticidade (consultar o **Apêndice A**). Resumindo, essas exigências incluem:

A.1 Expressão dos atributos de documento arquivístico e da ligação com documento arquivístico (por exemplo, os metadados de identidade e integridade)
A.2 Privilégios de acesso
A.3 Procedimentos de proteção contra perda e corrupção de documentos arquivísticos
A.4 Procedimentos de proteção contra deterioração das mídias e mudanças tecnológicas
A.5 Definição de formas documentais
A.6 Autenticação de documentos arquivísticos
A.7 Identificação de documento arquivístico autoritário
A.8 Remoção e transferência de documentação pertinente

2.5. Monitore documentos identificados para preservação de longo prazo.



Uma vez que a avaliação estiver completa, os documentos arquivísticos identificados para preservação devem ser monitorados em intervalos regulares até que sejam transferidos para o responsável pela preservação. A monitoração inclui confirmar com o produtor que nada mudou no que diz respeito a como as classes de documentos identificadas para transferência ou recolhimento estão sendo criadas ou mantidas; ou confirmar que, caso tenham ocorrido mudanças, estas não afetaram a natureza e os atributos dos documentos, além de seu valor, sua autenticidade ou a viabilidade da sua preservação.

Muitas mudanças dentro de uma organização podem afetar a sobrevivência continuada dos documentos digitais. A possibilidade dos documentos serem destruídos em um instante é bem maior do que no caso dos documentos tradicionais. Este risco é, de alguma forma, contrabalançado pela tendência de duplicar material de maneira descontrolada. Infelizmente, se a produção de cópias não for controlada, é pouco provável que se perceba quando a última cópia de um documento for destruída.

O cenário mais simples poderia envolver uma atualização no sistema, tanto do *hardware* como do *software*, que afetará a capacidade dos arquivos para aceitar os documentos arquivísticos. Uma atualização pode também resultar num redesenho do sistema, mesmo em menor escala, que poderia eliminar a capacidade de separar os documentos temporários dos que deveriam ser removidos para a transferência para o responsável pela preservação.

Um segundo cenário poderia envolver mudanças no mandato ou nas funções de uma organização. Isto pode facilmente levar a mudanças na forma como os aplicativos de computador são utilizados, e na natureza e quantidade de dados que eles contêm. As pessoas responsáveis pelo redesenho do sistema podem não conhecer os requisitos para a transferência dos documentos existentes para o preservador designado, antes de o sistema ser modificado. Sem intervenção, mesmo a documentação sobre o aplicativo original e as fitas de *backup* serão conduzidas inexoravelmente até uma data prevista de eliminação.

Finalmente, o colapso generalizado de práticas adequadas de gestão de documentos na maioria das organizações significa que os documentos são mal identificados e incorretamente armazenados em locais inseguros. Administradores e mesmo profissionais de gestão de documentos podem não entender os detalhes da infraestrutura técnica, enquanto que o pessoal de TI pode não estar familiarizado com a história da organização ou com a importância relativa de documentos mais antigos em diversos repositórios de dados. Discos rígidos podem ser apagados, contas de usuários e todos os arquivos que eles contêm podem ser removidos, fitas e discos podem ser reciclados ou destruídos e tecnologias obsoletas de reprodução podem ser eliminadas para satisfazer exigências operacionais cotidianas de velocidade e eficiência, desconsiderando o impacto de tais ações nos documentos de uma organização ou nos acordos de transferência pré-existentes, concebidos para garantir sua preservação a longo prazo.

2.6. Atualize a avaliação. Os processos de avaliação também precisam ser atualizados em intervalos regulares, embora maiores do que os intervalos em que os documentos identificados para transferência precisam ser monitorados. As informações obtidas durante uma visita de monitoramento podem fornecer o primeiro indício de que uma nova avaliação é necessária. Mudanças dentro das organizações e dentro dos seus sistemas de produção e manutenção de documentos são inevitáveis. Os mandatos e responsabilidades organizacionais podem mudar, bem como a forma como estas responsabilidades são desempenhadas, e os dados acumulados em sistemas existentes podem ter novos usos, o que pode aumentar seu valor a longo prazo. No nível mais simples, os sistemas que inicialmente não continham documentos arquivísticos podem ser atualizados para fazê-lo. Isto é especialmente verdade durante o período de sistemas "híbridos" de manutenção de documentos, em que os sistemas de documentos no suporte papel coexistem com os estágios iniciais de sistemas eletrônicos de informação, de documentos ou de documentos arquivísticos.

2.7. Identifique todos os componentes digitais. Documentos arquivísticos em papel mantidos em um sistema de manutenção tradicional normalmente se apresentam como um pacote bem amarrado, em que o conteúdo do documento está firmemente fixado em seu suporte, e o próprio documento está arquivado contextualmente com os outros documentos a ele relacionados. Este sistema contínuo começou a sucumbir com a introdução da tecnologia quando, por exemplo, os negativos fotográficos tiveram que ser processados para produzir fotos impressas, e quando imagens em movimento surgiram a partir de múltiplas camadas de som e imagem, combinadas e recombinadas para produzir a composição final exibida nos cinemas e na televisão.

<< COMPONENTE DIGITAL >>

Objeto digital que é parte de um ou mais documentos arquivísticos digitais, incluindo quaisquer metadados necessários para ordenar, estruturar ou manifestar seu conteúdo e forma, requerendo uma determinada ação de preservação.

A tecnologia digital desmantelou ainda mais o documento arquivístico numa série de componentes. Para extrair com sucesso documentos digitais do sistema em que foram produzidos, ou mesmo de um sistema de manutenção secundário, o preservador deve garantir que todos os componentes digitais essenciais sejam identificados e que as relações implícitas sejam explicitadas nos metadados antes que o todo seja transferido. Um dos exemplos mais comuns de componente digital é a biblioteca de fontes, que podem ser escolhidas pelo produtor, em qualquer quantidade, para serem usadas na apresentação de um documento gerado por um processador de texto. No Windows, estes dados são armazenados em arquivos ".dll" (*dynamic link library*, ou "biblioteca de ligação dinâmica"). Para que o preservador possa reproduzir o documento arquivístico de forma a refletir as intenções originais do produtor, tanto o componente digital que contém o texto quanto o que contém a fonte têm que ter sido preservados, assim como deve ter sido estabelecida a ligação entre eles, de tal maneira que o *software* que tenta exibir o conteúdo do arquivo de texto possa encontrar a biblioteca de fontes correta.[14]

2.8. Determine a viabilidade da preservação. Embora não faça parte da verificação do valor dos documentos, o processo de avaliação tem de ser completado por uma investigação cuidadosa dos requisitos técnicos para a preservação. Diferentes estratégias de preservação (ver **Apêndice C**, **Seção B**) podem variar bastante em termos de custo e podem produzir resultados muito diversos. Um documento textual do qual se retirou toda a formatação pode ser aceitável numa situação em que o preservador está interessado em veicular apenas o conteúdo do documento. No entanto, quando o significado é expresso pela forma documental e pelas características de apresentação do documento arquivístico, uma solução de preservação mais complexa será necessária.

A determinação da viabilidade da preservação é essencial para a entidade preservadora entender claramente o custo da entrada e da preservação dos documentos com que está se comprometendo. Não se trata de uma nova atividade; é simplesmente a extensão para a esfera digital da identificação dos recursos necessários para preservar, por exemplo, documentos arquivísticos em papel que tiverem mofo, ou rolos de filme que estiverem retorcidos. A conjuntura atual da preservação digital significa, contudo, que os custos de preservação devem ser vistos como recorrentes. Recopiar dados de um suporte físico para outro será uma atividade necessária tantas vezes quantas o formato selecionado se tornar obsoleto. A conversão de formatos de arquivo será necessária quando a obsolescência lógica ameaça tornar o conteúdo ilegível. Além disso, os documentos digitais arquivísticos considerados para preservação a longo prazo podem exigir medidas complexas demais para o ambiente tecnológico e para o nível de conhecimento da organização preservadora, o que poderá implicar num adiamento da transferência ou recolhimento.

3. Receba os documentos arquivísticos selecionados para preservação permanente (A4.3)

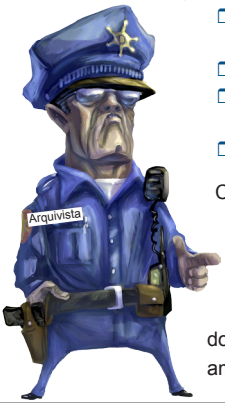
Re
Receber

A atividade desempenhada pelo preservador de receber documentos arquivísticos selecionados e todas as atividades de preservação que se seguem têm como objetivo a autenticidade e a acessibilidade contínuas desses documentos arquivísticos. Este movimento dos documentos arquivísticos que passam da custódia do produtor (ou do sucessor legítimo) para a custódia do preservador é um ponto crítico na cadeia de preservação e tem de ser feito com muito cuidado, a fim de assegurar que nada de errado aconteça no processo de transferência ou recolhimento.

3.1. Desenvolva um plano compartilhado para a transferência. Uma transferência ou recolhimento realizada com êxito, do atual custodiador dos documentos (seja ele o produtor original ou o sucessor legítimo) para a organização ou o programa que assume a responsabilidade pela preservação a longo prazo, exige um plano acordado entre ambas as partes. Tornar a acessar sistemas obsoletos ou extrair documentos arquivísticos inativos de sistemas operacionais são atividades que irão certamente envolver gastos com recursos humanos destinados ao processo de cópia e, potencialmente, ao de programação também. Além disso, é possível que *softwares* e *hardwares* especiais sejam necessários. Os formatos lógico e físico (ou virtual) usados para recebimento devem ser acordados por ambas as partes. Em regra, o plano de transferência ou recolhimento deve ser desenvolvido quando se confirmar a viabilidade técnica do recebimento e da preservação. Se as duas partes não chegarem a um acordo quanto ao processo de transferência ou recolhimento, a decisão de avaliação pode ter que ser revista. Mais uma vez, neste período caracterizado pela manutenção híbrida de documentos arquivísticos, podem ainda existir opções com relação ao suporte papel e ao suporte microfilme. Como alternativa, o preservador deve encorajar o produtor de documentos arquivísticos a adotar atualizações no sistema de arquivos que permitam transferências ou recolhimentos regulares com mais facilidade.

3.2. Aplique procedimentos padronizados. Os controles sobre a transferência ou recolhimento de documentos arquivísticos digitais, da custódia do produtor para a custódia do preservador, devem incluir:

- ❒ estabelecimento, implementação e monitoramento de procedimentos para registrar a transferência ou recolhimento de documentos arquivísticos;
- ❒ verificação da autoridade para transferência ou recolhimento;
- ❒ exame dos documentos arquivísticos para determinar se correspondem aos documentos arquivísticos que foram selecionados para transferência/recolhimento; e
- ❒ entrada dos documentos arquivísticos.



Como parte do processo de transferência ou recolhimento, deve ser verificada a autenticidade dos documentos arquivísticos do produtor, que foi estimada durante o processo de avaliação. Isto inclui a verificação de que os metadados de identidade e integridade foram transferidos junto com seus respectivos documentos e permanecem vinculados a eles. Também se deve verificar se os documentos estão acompanhados de qualquer documentação relevante sobre o ambiente técnico-administrativo em que foram produzidos e mantidos.

3.3. Mantenha o formato lógico mais antigo disponível. O **formato lógico** no qual os documentos arquivísticos foram originalmente produzidos, ou no qual eram mantidos pelo produtor à época da transferência, deve, quando possível, ser mantido pelo preservador, juntamente com quaisquer cópias de referência ou de preservação geradas após o recebimento. Caso as estratégias de preservação escolhidas, tais como uma solução de conversão específica, venham a falhar com o tempo, a guarda continuada do formato lógico inicial irá permitir ao preservador reiniciar essencialmente o processo de preservação com a cópia "mais autoritária" dos documentos, devido à aplicação de uma estratégia diferenciada de preservação. Durante os longos períodos em que o preservador mantém os documentos arquivísticos, a experiência pode mostrar que outras estratégias de preservação são mais estáveis ao longo do tempo, ou podem ser transmitidas com mais facilidade a longo prazo. Alternativamente, novos métodos de preservação poderão ter sido desenvolvidos após o recebimento e o processamento inicial dos documentos.

<< FORMATO LÓGICO >>

Arranjo organizado de dados em suportes eletrônicos que garante que as estruturas de controle de arquivos e dados sejam reconhecíveis e recuperáveis pelo sistema operacional do computador hospedeiro. Dois formatos lógicos comuns para arquivos e diretórios são o ISO 9660, para *CD-ROMs*, e o *Universal Disk Format* (UDF), para DVDs.

3.4. Evite duplicatas. Devido à facilidade de replicar documentos arquivísticos digitais, os preservadores devem implementar procedimentos que assegurem que os documentos arquivísticos digitais de uma série específica sejam transferidos por um determinado produtor para o preservador apenas uma vez. Informações acuradas sobre identidade são um primeiro passo importante para evitar a duplicação por parte do produtor e do preservador. Além disso, se o preservador fornecer cópias de referência ao produtor, após a transferência dos documentos, estas devem ser claramente identificadas e marcadas como tais, a fim de evitar retransferências acidentais.

3.5. Documente todo o processamento. Os processos iniciais adotados durante e imediatamente após o recebimento podem ou não estar relacionados à preservação em si. Confirmar a identidade do material transferido, verificando a existência de vírus, e confirmar se os arquivos recebidos estão completos torna mais provável que estes se mantenham inalterados. A conversão de arquivos, a renomeação de entidades digitais e o encapsulamento de arquivos são atividades mais invasivas. Nos dois casos, os preservadores devem documentar todo o processamento dos documentos arquivísticos digitais e seus efeitos, enquanto estiverem sob a sua custódia (ver **Apêndice B**, **Requisito B.2**). Essa documentação deve incluir informações, tais como:

- ❒ por que razão certos processos foram aplicados aos documentos;
- ❒ quais documentos foram processados;
- ❒ a data em que o processo ocorreu;
- ❒ os nomes das pessoas que realizaram e documentaram os vários estágios do(s) processo(s);
- ❒ o impacto do processo realizado sobre a forma, o conteúdo, a acessibilidade e o uso do documento; e
- ❒ a descrição de qualquer dano, perda ou outros problemas enfrentados como resultado do processamento, inclusive de qualquer efeito nos elementos que expressam a identidade e a integridade dos documentos.

Caso o preservador produza cópias dos documentos recebidos, é importante lembrar que, tal como discutido na **Seção 1.5**, estas cópias devem ser produzidas em um ambiente que satisfaça as exigências relevantes[15] dos Requisitos de Referência para Apoiar a Presunção de Autenticidade, do InterPARES 1.

4. Preserve os documentos arquivísticos recebidos (A4.4)

Pr
Preservação

O preservador de documentos arquivísticos é a entidade responsável pela custódia física e legal dos documentos do produtor, bem como por sua preservação (isto é, proteger e garantir acesso contínuo aos documentos). Seja ele uma organização externa ou uma unidade interna, o papel do preservador designado deve ser o de **custodiador confiável** dos documentos do produtor. As cópias autênticas dos documentos arquivísticos do produtor são mantidas pelo custodiador confiável num **sistema confiável de preservação** (veja o **Apêndice C**), que deve incluir na sua concepção um sistema de descrição e de recuperação. Este sistema confiável de preservação também deve ter regras e procedimentos para a produção contínua de cópias autênticas, à medida que o sistema existente se torne obsoleto e a tecnologia se atualize.

4.1. Descreva os documentos arquivísticos. As informações sobre os documentos arquivísticos e seus contextos, coletadas durante as fases de avaliação e processamento, devem fazer parte da descrição arquivística dos fundos ou séries a que os documentos arquivísticos pertencem (ver **Apêndice B**, **Requisito B.3**). Devem também incluir informações sobre direitos de propriedade intelectual ou questões de privacidade.

A descrição arquivística dos fundos ou séries contendo documentos arquivísticos digitais deve incluir – além de informações relativas aos contextos jurídico-administrativo, de proveniência, de procedimentos e documental – informações sobre as mudanças sofridas por eles desde a sua produção. A descrição deve também incluir uma visão geral dos processos de transferência e preservação, com base na documentação discutida na **Seção 3.5** e na explicação dos relacionamentos entre componentes digitais discutida na **Seção 2.7**.

<< Custodiador confiável >>

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

4.2. Identifique ramificações legais das ações de preservação. Quando se escolhe uma estratégia de preservação, devem-se examinar as suas implicações legais. Por exemplo, a conversão de formato, a partir de um ambiente proprietário, poderá envolver o preservador em ações ilegais. Nos Estados Unidos, a Lei de Direitos Autorais do Milênio Digital (*Digital Millennium Copyright Act*) considera como crime a produção de mecanismos que possam contornar medidas de proteção de direitos autorais. Internacionalmente, o Tratado de Direitos Autorais da Organização Mundial da Propriedade Intelectual (*World Intellectual Property Organization Copyright Treaty - WIPO WCT*) contém disposições que incluem a proteção de direitos autorais sobre *softwares*, bem como sobre obras digitais, e que introduzem penalidades criminais pela infração, que vai desde a cópia não autorizada de material colocado num *site* da Internet até a remoção ou alteração de controles de gestão de direitos sobre obras digitais. A maioria dos pacotes de *software* inclui também algum tipo de restrição semelhante, com as quais os usuários devem concordar durante o processo de instalação.

4.3. Confirme a eficácia da estratégia de preservação escolhida. Tal como discutido na **Seção 2.8**, existem agora diversas estratégias de preservação disponíveis. Teoricamente, a estratégia de preservação selecionada deve ser testada nos documentos arquivísticos antes da sua transferência formal para o preservador, a fim de garantir que o seu desempenho esteja de acordo com o esperado. De forma mais realista, a maioria das organizações ou programas responsáveis pela preservação só pode financiar este tipo de teste excepcionalmente. Assim como os preservadores tradicionais testam cuidadosamente tratamentos propostos antes de aplicá-los em larga escala aos documentos arquivísticos analógicos, os preservadores digitais devem estar constantemente alertas para o impacto que cada processo de preservação possa ter nos documentos, e garantir que ele seja a escolha apropriada para preservar documentos arquivísticos autênticos. Falhas no aplicativo de *software* e variações no funcionamento das versões ao longo do tempo podem resultar em consequências inesperadas, quando aplicadas a um novo grupo de documentos.

Parte desse processo inclui uma consciência constante da necessidade de rastrear a presença e o desempenho de todos os componentes digitais. Uma mudança num componente pode ter resultados inesperados num segundo componente ou pode afetar as funções de relacionamento entre dois componentes essenciais do documento arquivístico ou sua capacidade de interagir. Um relacionamento diferente que pode ser afetado é aquele entre os membros de um grupo de documentos, tal como um dossiê ou uma série, e a apresentação desse conjunto na ordem correta (por exemplo, alfabética, cronológica ou hierárquica). Se a ordem original se perder, medidas corretivas terão que ser tomadas.

4.4. Manter um armazenamento adequado. É um princípio de preservação arquivística amplamente aceito que a manutenção de um ambiente de armazenamento adequado e coerente (umidade relativa e temperatura) para o material que está sendo armazenado é a contribuição mais eficaz, em termos de custo, para a preservação dos documentos arquivísticos a longo prazo. Os fabricantes de meios de armazenamento magnéticos ou ópticos geralmente fazem recomendações quanto às melhores condições possíveis de armazenamento. O ambiente deve ser constantemente monitorado e as leituras, verificadas com regularidade. Esta recomendação é uma das oito estratégias de manutenção obrigatórias delineadas na **Seção 1.7** e discutidas no **Apêndice C**, **Seção A**.

5. Dê acesso aos documentos arquivísticos (A4.5)

Sa
Saída

Como já foi observado anteriormente, a acessibilidade contínua (isto é, o uso) é uma parte integrante do processo arquivístico. Consequentemente, oferecer acesso aos documentos arquivísticos preservados é um componente essencial da cadeia de preservação. O acesso deve ser gerenciado pelo preservador com o mesmo senso de responsabilidade e o mesmo grau de competência técnica e profissional empregados na avaliação, recebimento/transferência, descrição e armazenamento dos documentos arquivísticos.

5.1. Explique como as cópias de referência foram feitas. O relacionamento entre os documentos recebidos do produtor e quaisquer cópias produzidas pelo preservador terá que ser claramente descrito e facilmente acessado pelos usuários (veja o **Apêndice B**, **Requisito B.2.b**). Também se devem documentar como as medidas de controle do processo de reprodução em vigor foram estabelecidas e implementadas, e como são monitoradas a fim de assegurar que o conteúdo dos documentos arquivísticos reproduzidos não sofra alterações no curso da reprodução. Cópias de documentos arquivísticos no sistema de preservação do preservador podem não ser reconhecidas como autênticas, caso o preservador as tenha feito para outros fins, além da preservação; por exemplo, pode-se fazer, para propósitos de acesso, uma cópia da qual foram removidos os identificadores pessoais.

Documentar o processo de reprodução dos documentos arquivísticos e seus efeitos é um meio essencial de comprovar que ele é transparente (isto é, livre de simulação ou engano). Esta transparência é necessária para a satisfação efetiva do papel do preservador como custodiador confiável dos documentos arquivísticos. Ela também fornece aos usuários dos documentos arquivísticos uma ferramenta fundamental para a avaliação e interpretação dos mesmos, por meio da demonstração da autenticidade contínua dos documentos arquivísticos e da apresentação do seu histórico completo, do qual o histórico de reprodução constitui uma parte vital.

5.2. Explique os requisitos técnicos para o acesso. Tal como mencionado na **Seção 1.1**, os diversos preservadores prestam serviços de referência a diferentes tipos de usuários. Isto afetará os formatos de referência e os mecanismos de referência adotados pela organização ou programa de preservação, exigindo métodos mais simples voltados para o público em geral, que podem nem possuir um computador, ou que possuem uma máquina muito simples com alguns *softwares* básicos. Para satisfazer as necessidades destes usuários, o preservador pode ter que realizar processamentos adicionais ou criar ferramentas especiais para apoiar os pesquisadores. Os usuários mais afeitos à tecnologia, tais como estatísticos fazendo análises de dados ou peritos contábeis conduzindo investigações sobre fraudes, são mais capazes de aplicar seus próprios recursos de *software* a cópias de documentos arquivísticos.

Co
Conclusão

Conclusão

Este documento apresentou uma série de diretrizes para instituições, organizações e programas responsáveis pela preservação de documentos arquivísticos digitais que podem ser presumidos como autênticos e acurados, enquanto estiverem sob a custódia do preservador. Nos casos de preservadores individuais e pequenas organizações dedicadas à preservação de documentos, o desafio parece ser grande, mas a alternativa – a perda de documentos arquivísticos ou o surgimento de documentos corrompidos e falsos – seria um problema ainda maior a longo prazo. Pequenas organizações se beneficiarão ao fazer uma indicação clara da pessoa ou pessoas responsáveis por supervisionar a preservação dos documentos arquivísticos digitais da organização. Tenha em mente, contudo, que nem todas as recomendações apresentadas neste documento precisam ser aplicadas em todas as circunstâncias; cada preservador deve ser capaz de selecionar e adotar as medidas que respondem a seus problemas específicos no contexto em que trabalha. Também pode haver casos em que serão necessárias medidas adicionais, devido a exigências legais ou regulamentares, específicas da jurisdição administrativa ou cultural do preservador. Em tais casos, pode ser preciso consultar especialistas na área do direito. Indivíduos, empresas e pequenas organizações responsáveis pela preservação não devem hesitar em contatar esses especialistas para pedir conselhos sobre quaisquer questões relacionadas à preservação de documentos arquivísticos digitais sob sua custódia e seu controle.

Referências citadas

1 Disponível em: http://www.interpares.org/ip2/ip2_models.cfm
2 [NT] No original em inglês, *COP model (Chain of Preservation model)*.
3 Disponível em: http://www.interpares.org/public_documents/ip2(pub)policy_framework_booklet.pdf
4 [NT] No original em inglês, *Policy Cross-Domain*.
5 ISO 14721: 2003, disponível em: http://www.iso.org
6 Disponível em: http://www.worldcat.org/arcviewer/1/OCC/2007/08/08/0000070511/viewer/file2433.html / O *link* para o *site* do *NARA*/ *RLG Digital Repository Task Force* é: http://www.oclc.org/programs/ourwork/past/repositorycert.htm. O documento *Audit Checklist for Certifying Digital Repositories* foi revisado e expandido, e a nova versão foi nomeada como *Trustworthy Repositories Audit & Certification: Criteria and Checklist* (TRAC), disponível em: http://www.crl.edu/content.asp?l1=13&l2=58&l3=162&l4=91
7 Ver em http://www.fedora-commons.org/
8 Ver em http://hul.harvard.edu/formatregistry
9 Ver: Authenticity Task Force, "Appendix 2: Requirements for Assessing and Maintaining the Authenticity of Electronic Records". In: *The Long-term Preservation of Authentic Electronic Records: Findings of the InterPARES Project*, Luciana Duranti, ed. (San Miniato, Itália: Archilab, 2005), 204-219. Disponível em: http://www.interpares.org/book/interpares_book_k_app02.pdf.
10 Ibidem.
11 [NT] No Brasil, as tabelas de temporalidade contemplam prazos de guarda e as ações de destinação, diferentemente dos *records schedules*, que são aplicados nos países de língua inglesa e podem somente prever os prazos de guarda.
12 Muitos aspectos relacionados à criação de programas eficazes de preservação digital foram estudados em anos recentes. Entre os *sites* de internet que contêm informações úteis ou exemplos estão: o Projeto InterPARES, em http://www.interpares.org; *Model Requirements for the Management of Electronic Documents and Records* (MoReq), em http://www.digitaleduurzaamheid.nl/bibliotheek/docs/moreq.pdf; *Metadata Encoding and Transmission Standard* (METS), em http://www.loc.gov/standards/mets/; *Electronic Records from Office Systems* (EROS), do Arquivo Nacional do Reino Unido, em http://www.nationalarchives.gov.uk/electronicrecords/advice/guidelines.htm; e o manual DIRKS (*Designing and Implementing Recordkeeping Systems*), da Austrália, em http://www.naa.gov.au/recordkeeping/dirks/dirksman/dirks.html
13 Ver a discussão sobre diplomática na obra de Luciana Duranti e Kenneth Thibodeau (2006), *The Concept of Record in Interactive, Experiential and Dynamic Environments: the View of InterPARES*, Archival Science 6(1): 15-21.
14 Uma descrição mais detalhada de "componente digital", com mais exemplos ilustrando o conceito, está disponível em: "Appendix 6: How to Preserve Electronic Records", In: *The Long-term Preservation of Authentic Electronic Records*, op. cit., 293-328.
15 O Requisito A.5 ("Estabelecimento de formas documentais"), em que o produtor estabelece a forma documental do documento arquivístico, normalmente não se aplicaria ao preservador, a não ser que a forma documental original do documento arquivístico tenha se perdido e o preservador tenha que indicar um substituto para permitir o acesso.

Apêndice A
Requisitos de Referência para Apoiar a Presunção de Autenticidade dos Documentos Arquivísticos Digitais*

Rr
Requisitos de Referência

Os requisitos de referência são as condições que servem como base para o preservador verificar a autenticidade dos documentos arquivísticos digitais do produtor. A satisfação desses requisitos de referência dará ao preservador a capacidade de inferir a autenticidade de documentos arquivísticos, com base na forma como eles foram produzidos, utilizados e mantidos pelo produtor. Dentre os requisitos de referência, o Requisito A.1 identifica a informação-chave sobre um documento digital – o contexto imediato de sua produção e a maneira como ele foi utilizado e mantido –, que estabelece sua identidade e prepara o terreno para demonstrar sua integridade. Os Requisitos A.2-A.8 identificam os tipos de controles procedimentais sobre produção, utilização e manutenção do documento arquivístico, que apoiam a presunção de sua integridade.

<< Conjunto de Requisitos A >>

A fim de apoiar a presunção de autenticidade, o preservador deve comprovar:

REQUISITO A.1: Expressão dos atributos do documento arquivístico e sua ligação com o documento arquivístico
O valor dos seguintes atributos está explicitamente expresso e inextricavelmente ligado a todos os documentos arquivísticos. Estes atributos podem ser distinguidos em duas categorias: a primeira diz respeito à identidade dos documentos arquivísticos, e a segunda à integridade dos mesmos.

A.1.a Identidade do documento arquivístico:
- **A.1.a.i** Nomes das pessoas que participaram da formação do documento arquivístico, ou seja:
  - nome do autor[a]
  - nome do redator[b] (se for diferente do autor)
  - nome do originador[c] (se for diferente do autor ou do redator)
  - nome do destinatário[d]
- **A.1.a.ii** Nome da ação ou assunto
- **A.1.a.iii** Data(s) de produção e transmissão, ou seja:
  - data cronológica[e]
  - data de recebimento[f]
  - data de arquivamento[g]
  - data(s) de transmissão[h]
- **A.1.a.iv** Expressão de relação orgânica[i] (por exemplo, código de classificação, identificador de arquivo)
- **A.1.a.v** Indicação de anexos

A.1.b Integridade do documento arquivístico:
- **A.1.b.i** Nome da unidade responsável pela execução da ação contida no documento[j]
- **A.1.b.ii** Nome da unidade que tem a responsabilidade principal (se diferente do anterior)[k]
- **A.1.b.iii** Indicação de tipos de anotação acrescentada ao documento arquivístico[l]
- **A.1.b.iv** Indicação de modificações técnicas[m]

REQUISITO A.2: Privilégios de acesso
O produtor definiu e efetivamente implementou privilégios de acesso com relação à produção, modificação, anotação, remanejamento e destruição de documentos arquivísticos.

Apêndice A (cont.)

<< Conjunto de Requisitos A (cont.) >>

REQUISITO A.3: Procedimentos de proteção: perda e corrupção de documentos arquivísticos
O produtor estabeleceu e efetivamente implementou procedimentos para evitar, descobrir e corrigir a perda ou corrupção de documentos arquivísticos.

REQUISITO A.4: Procedimentos de proteção: meios e tecnologia
O produtor estabeleceu e efetivamente implementou procedimentos para garantir a identidade e a integridade contínuas dos documentos arquivísticos, face à deterioração dos meios e das mudanças tecnológicas.

REQUISITO A.5: Estabelecimento de formas documentais
O produtor estabeleceu as formas documentais dos documentos arquivísticos associadas a cada procedimento, de acordo com os requisitos do sistema legal ou os requisitos do produtor.

REQUISITO A.6: Autenticação de documentos arquivísticos
Para o caso de o sistema jurídico ou as necessidades da organização exigirem autenticação, o produtor estabeleceu regras específicas com relação a quais documentos arquivísticos devem ser autenticados, bem como por quem e por que meios a autenticação deve ser feita.

REQUISITO A.7: Identificação do documento arquivístico autoritário
Para o caso de existirem cópias múltiplas do mesmo documento arquivístico, o produtor estabeleceu procedimentos que identificam qual documento é o autoritário.

REQUISITO A.8: Remoção e transferência de documentação relevante
Para o caso de transferência de documentos do arquivo corrente para o intermediário ou recolhimento do arquivo intermediário para o permanente, envolvendo sua remoção do sistema eletrônico, o produtor estabeleceu e efetivamente implementou procedimentos para determinar qual documentação tem que ser removida e transferida para o preservador juntamente com os documentos arquivísticos.

* Extraído de: Authenticity Task Force, "Appendix 2: Requirements for Assessing and Maintaining the Authenticity of Electronic Records". In: *The Long-term Preservation of Authentic Electronic Records: Findings of the InterPARES Project*, Luciana Duranti, ed. (San Miniato, Itália: Archilab, 2005), 204-219. Disponível em: http://www.interpares.org/book/interpares_book_k_app02.pdf. Nota: este excerto não inclui o comentário existente na versão integral.

a O nome da pessoa física ou jurídica com autoridade e capacidade para emitir o documento arquivístico, ou em cujo nome ou sob cujo comando ele foi emitido.

b O nome da pessoa física ou jurídica com autoridade e capacidade para articular o conteúdo do documento arquivístico.

c O nome da pessoa física ou jurídica a quem foi atribuído o endereço eletrônico no qual o documento foi gerado e/ou do qual ele foi enviado.

d O nome da(s) pessoa(s) física(s) ou jurídica(s) a quem o documento arquivístico é dirigido ou para quem ele foi intencionado.

e A data – e possivelmente a hora – da compilação de um registro incluído no documento arquivístico pelo autor ou pelo sistema eletrônico em nome do autor.

f A data – e possivelmente a hora – em que o documento arquivístico é recebido pelo destinatário.

g A data – e possivelmente a hora – em que o documento arquivístico é oficialmente incorporado ao arquivo do produtor.

h A data e a hora em que o documento sai do espaço em que foi gerado.

i A relação orgânica é o relacionamento que vincula cada documento arquivístico, de forma incremental, ao anterior e ao seguinte e a todos aqueles que participam da mesma atividade. É originária (i.e., passa a existir quando um documento é elaborado ou recebido e retido), necessária (i.e., existe para todos os documentos) e determinada (i.e., é caracterizada pela finalidade do documento).

j A unidade administrativa (ou funcionário) com competência formal para realizar a ação com que o documento está relacionado ou para o assunto a que o documento diz respeito.

k A unidade administrativa (ou funcionário) a quem foi dada competência formal para manter o documento arquivístico autoritário, ou seja, o documento arquivístico considerado pelo produtor como sendo o seu documento oficial.

l Anotações são acréscimos feitos a um documento arquivístico depois de concluído. Portanto, não são consideradas elementos de sua forma documental.

m Modificações técnicas são quaisquer mudanças nos componentes digitais do documento, tal como definido pela *Preservation Task Force*. Essas modificações incluem mudanças na forma como alguns elementos do documento arquivístico são codificados digitalmente, bem como mudanças nos métodos (*software*) utilizados para reproduzir o documento arquivístico, a partir dos componentes digitais armazenados; isto é, quaisquer mudanças que possam levantar dúvidas quanto ao fato de o documento reproduzido ter permanecido como era antes da modificação técnica. A indicação de modificações pode se referir a documentação adicional externa ao documento que explique com mais detalhe a natureza dessas modificações.

Apêndice B
Requisitos de Base para Apoiar a Produção de Cópias Autênticas dos Documentos Arquivísticos Digitais*

Rb
Requisitos de Base

Os requisitos de base delineiam as condições mínimas necessárias para possibilitar ao preservador atestar a autenticidade das cópias de documentos arquivísticos digitais de guarda permanente. Diferentemente dos requisitos de referência, todos os requisitos de base devem ser atendidos antes que o preservador possa atestar a autenticidade das cópias digitais sob sua custódia. O cumprimento destes requisitos possibilitará ao preservador certificar que as cópias dos documentos arquivísticos são autênticas. Tradicionalmente, o preservador oficial dos documentos arquivísticos era a pessoa a quem havia sido confiada a tarefa de emitir cópias autênticas desses documentos. Para desempenhar tal papel, o preservador precisava simplesmente atestar que a cópia estava em conformidade com o documento arquivístico reproduzido. Se considerarmos os documentos arquivísticos digitais e as dificuldades relativas à sua preservação, o caminho mais prudente seria o preservador produzir e manter a documentação relativa à maneira como ele manteve os documentos ao longo do tempo, e também como ele os reproduziu para apoiar sua atestação de autenticidade.

<< Conjunto de Requisitos B >>

O preservador deve ser capaz de demonstrar:

REQUISITO B.1: Controles sobre a transferência, manutenção e reprodução de documentos arquivísticos
Os procedimentos e o(s) sistema(s) usado(s) para transferir documentos para o programa de preservação ou instituição arquivística, bem como os procedimentos e sistemas usados para mantê-los e reproduzi-los, constituem controles adequados e eficazes para garantir a identidade e a integridade dos documentos. Além disso, esses procedimentos e sistemas asseguram especificamente que:

B.1.a A custódia contínua dos documentos seja mantida;
B.1.b Os procedimentos de segurança e controle sejam implementados e monitorados; e
B.1.c O conteúdo do documento arquivístico, suas anotações e seus elementos da forma documental permaneçam imutáveis após a reprodução.

REQUISITO B.2: Documentação do processo de reprodução e seus efeitos
A atividade de reprodução foi documentada, e esta documentação inclui:

B.2.a A data da reprodução dos documentos arquivísticos e o nome da pessoa responsável;
B.2.b A relação entre os documentos arquivísticos recebidos do produtor e as cópias produzidas pelo preservador;
B.2.c O impacto do processo de reprodução na forma, no conteúdo, na acessibilidade e no uso dos documentos arquivísticos; e
B.2.d A informação, documentada pelo preservador, de que uma cópia de um documento arquivístico não reproduz total e fielmente os elementos que expressam a sua identidade e integridade; esta documentação deve estar facilmente acessível ao usuário.

REQUISITO B.3: Descrição arquivística
A descrição arquivística dos fundos que contêm documentos arquivísticos digitais inclui – além da informação sobre seus contextos jurídico-administrativo, de proveniência, de procedimentos e documental – informações sobre mudanças sofridas pelos documentos arquivísticos digitais do produtor desde quando foi inicialmente produzido.

* Extraído de: Authenticity Task Force, "Appendix 2: Requirements for Assessing and Maintaining the Authenticity of Electronic Records". In: *The Long-term Preservation of Authentic Electronic Records: Findings of the InterPARES Project*, Luciana Duranti, ed. (San Miniato, Itália: Archilab, 2005), 204-219. Disponível em: http://www.interpares.org/book/interpares_book_k_app02.pdf. Nota: este excerto não inclui o comentário existente na versão integral.

Es
Estratégias

Apêndice C
Estratégias de preservação e manutenção dos documentos arquivísticos digitais*

Este apêndice inclui uma lista de estratégias de preservação extraídas, em sua maior parte, da obra *Diretrizes para a preservação do patrimônio digital*, da UNESCO (no original, *Guidelines for the Preservation of Digital Heritage*[n]), que oferece um quadro para a descrição de estratégias de preservação de documentos arquivísticos digitais, que pode ser utilizado para proteger e manter a acessibilidade de cópias autênticas de documentos arquivísticos digitais ao longo da cadeia de preservação.

<< Estratégia de manutenção >>

Conjunto coerente de objetivos e métodos para a proteção e manutenção da acessibilidade de cópias autênticas de documentos arquivísticos digitais ao longo dos estágios iniciais na cadeia de preservação.

<< Estratégia de preservação >>

Conjunto coerente de objetivos e métodos para a manutenção, ao longo do tempo, dos componentes digitais e das informações a eles relacionadas, e para a reprodução dos documentos arquivísticos autênticos e/ou agregações arquivísticas relacionados a esses componentes e informações.

A lista completa de estratégias possíveis adotadas pelo InterPARES 2 está conceitualmente dividida em duas grandes categorias: a) **estratégias de manutenção**, e b) **estratégias de preservação**.

A. Estratégias de manutenção. As estratégias de manutenção são o requisito mínimo necessário para proteger e manter a acessibilidade de cópias autênticas de documentos arquivísticos digitais. Existem oito estratégias principais de manutenção (ver página seguinte). Todas são necessárias para garantir que os componentes digitais dos documentos existirão por tempo suficiente para que as estratégias de preservação possam ser aplicadas.

B. Estratégias de preservação. Além das estratégias de manutenção, todos os preservadores de documentos arquivísticos são responsáveis por estabelecer um **sistema de preservação confiável** para expressar uma ou mais estratégias de preservação. Doze estratégias de preservação foram listadas a seguir, na **Seção B**, divididas em quatro grandes grupos. É bem possível que, na prática, um preservador apoie duas ou mais estratégias de preservação, além das oito estratégias de manutenção listadas abaixo, na **Seção A**.

<< Sistema de preservação confiável >>

Sistema que compreende todas as regras – e as ferramentas e mecanismos usados para implementá-las –, que orienta a manutenção e o uso intelectual e físico permanente dos documentos arquivísticos sob a custódia do preservador, e que oferece uma probabilidade circunstancial de os documentos que se encontram no sistema serem autênticos.

* Adaptado de: Kevin Glick, *Electronic Records Preservation Strategies* (relatório não publicado, 2006).

n Colin Webb (2003), *Guidelines for the Preservation of Digital Heritage*. Preparado pela Biblioteca Nacional da Austrália para a Divisão de Sociedade de Informação, Unesco, relatório n. CI-2003/WS/3. Disponível em: http://unesdoc.unesco.org/images/0013/001300/130071e.pdf

Apêndice C (cont.)

A. Estratégias de manutenção

Em Estratégias de manutenção

A1. Atribuição clara de responsabilidades. Deve ser atribuída a uma pessoa ou unidade administrativa, de forma não ambígua, a responsabilidade de gerir o armazenamento e a proteção de documentos arquivísticos. Trata-se de uma responsabilidade técnica que exige um conjunto de habilidades específicas, recursos determinados e um plano adequado. Esta estratégia pode ser realizada por meio da contratação de um funcionário competente exclusivamente dedicado a esta tarefa, ou com a designação de um funcionário ou unidade administrativa já existente para desenvolver tal tarefa durante uma parcela do seu tempo.

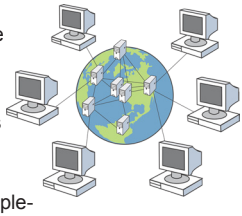
A2. Fornecimento da infraestrutura técnica adequada. Inclui todos os recursos físicos e administrativos que possibilitam os processos de manutenção de documentos arquivísticos (edificações, *hardwares*, redes de computadores e os funcionários auxiliares necessários para mantê-los).

A3. Manutenção, suporte e substituição do sistema. A implementação de um plano para manutenção, atualização e/ou substituição de *hardware* e *software*.

A4. Transferência regular de dados para novos meios de armazenamento. A implementação de um plano para copiar dados de um meio de armazenamento para outro a fim de evitar o impacto da deterioração dos suportes. Estas transferências devem ser feitas de forma sistemática.

A5. Adote condições adequadas para meios de armazenamento. A taxa de deterioração dos meios pode ser dramaticamente reduzida pela adoção de condições ambientais adequadas. Por exemplo, calor excessivo, umidade e poeira colocam em perigo os meios de armazenamento.

A6. Redundância e localização geográfica. A duplicação de entidades digitais e o armazenamento de cópias múltiplas resultantes em meios físicos diferentes as protegem de problemas nos suportes. O armazenamento em diferentes locais físicos também as protege de condições ambientais adversas, fogo, enchentes, entre outros.



A7. Segurança do sistema. Devem ser implementados controles para assegurar que os componentes digitais dos documentos arquivísticos estejam expostos apenas a usuários e/ou processos autorizados. Tais controles devem incluir restrições de acesso físico a locais onde os computadores estão guardados, bem como restrições de acesso aos documentos arquivísticos digitais nos próprios computadores. Esta última restrição poderá ser posta em prática de diversas formas, incluindo o uso de senhas e/ou autenticação biométrica para se acessar o sistema.

A8. Planejamento em caso de desastre. As estratégias descritas acima são concebidas para minimizar perdas acidentais de dados e maximizar a longevidade dos suportes, porém, mesmo com condições perfeitas de armazenamento e excelentes protocolos de utilização, acidentes ainda podem acontecer. Um plano de recuperação de desastres deve conter procedimentos detalhados para restaurar um sistema danificado e para orientar a recuperação efetiva dos sistemas de manutenção e/ou preservação de documentos arquivísticos após um acidente.

Apêndice C (cont.)
B. Estratégias de preservação

B1. Uso de padrões. O uso de padrões amplamente disponíveis e utilizados aumenta a probabilidade de estabilidade e de um suporte mais duradouro. Esses padrões podem ser ***de jure***, se forem acordados de maneira formal, ou ***de facto***, se forem adotados em larga escala pela indústria. Os padrões podem ser aplicados a muitos aspectos de um sistema de preservação, incluindo métodos de codificação, formatos de arquivo, meios físicos de armazenamento etc. A obediência aos padrões pode também simplificar a aplicação e/ou maximizar a eficácia de estratégias de preservação posteriores. A padronização pode ser aplicada **prospectivamente**, limitando os formatos nos quais os documentos arquivísticos digitais podem ser transferidos para o preservador, ou **retrospectivamente**, convertendo arquivos recebidos em outros formatos para formatos padronizados.

B1.1. Formatos autodescritivos (preservação de objeto persistente, marcação). Análise e marcação de documentos arquivísticos de forma que as funções, relacionamentos e estrutura dos elementos específicos possam ser descritos. A reapresentação do conteúdo pode ser feita sem aplicativos de *software* específicos, podendo ser realizada por meio de diferentes aplicativos à medida que a tecnologia se modifica.

B1.2. Encapsulamento. Ato de juntar um documento arquivístico e os meios que dão acesso a ele, normalmente num ***wrapper*** que descreve o que ele é, de forma que possa ser compreendido por uma vasta gama de tecnologias (tal como um documento XML). O *wrapper*, muitas vezes, inclui metadados que descrevem ou remetem às ferramentas adequadas.

B1.3. Restrição da gama de formatos a serem geridos (normalização). O armazenamento de documentos arquivísticos num número limitado de formatos.º A seleção de formatos aceitáveis pode continuar a incluir novos formatos proprietários ou novas gerações de formatos proprietários existentes, ou pode se restringir a formatos não proprietários, a fim de dar um passo adiante na padronização. Um exemplo desta abordagem é chamado de **codificação durável**, que recomenda codificar os documentos arquivísticos para que estejam de acordo com padrões conhecidos de processamento de dados, podendo atingir até um nível de codificação de bits como ASCII ou Unicode UTF-8, e objetos como XML.

B1.4. Conversão. Transferência de códigos digitais de uma geração de *hardware* ou *software* para outra. Diferentemente da **atualização**, que copia a cadeia de dados de um suporte para outro, a conversão implica transformar a forma lógica de um objeto digital para que o objeto conceitual possa continuar a ser corretamente exibido ou apresentado pelo novo *hardware* ou *software*. O método de conversão mais comumente proposto envolve a transformação permanente de um formato lógico em outro, de acordo com as mudanças tecnológicas, de forma que todos os objetos convertidos possam ser apresentados com a tecnologia predominante. Também é possível propor um modelo de "conversão sob demanda" ou de "conversão no ponto de acesso". Esta abordagem é discutida a seguir na **Seção B2.4** (Visualizadores).

<< Padrão de direito >>

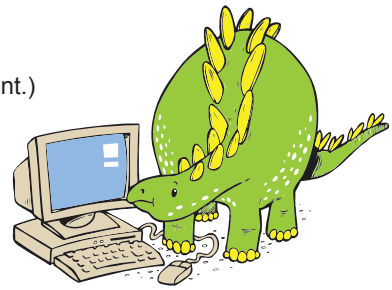
Padrão adotado por órgãos oficiais de padronização, sejam eles nacionais (p. ex. Associação Brasileira de Normas Técnicas – ABNT), multinacionais (por exemplo, Comitê Europeu de Normalização – CEN) ou internacionais (por exemplo, Organização Internacional para Padronização – ISO). Para padrões de arquivos 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.

Apêndice C (cont.)

B. Estratégias de preservação (cont.)



B2. Dependência tecnológica. Estas estratégias continuam a se basear no *hardware* e/ou *software* original, sem alterar os documentos arquivísticos.

B2.1. Preservação da tecnologia. Manutenção do *software* e do *hardware* originais com os quais os documentos foram apresentados.

B2.2. Confiança na compatibilidade descendente ou reversa. Confiança na capacidade de alguns *softwares* de interpretar corretamente e apresentar componentes digitais de documentos produzidos com versões anteriores dos mesmos *softwares*. Nesta estratégia, a apresentação está limitada a uma conversão temporária para fins de visualização ou para fins de cópias não destinadas a arquivo, enquanto a conversão altera permanentemente os documentos para o formato da versão atual do *software*.

B2.3. Reengenharia de *software*. Transformação do *software* à medida que a tecnologia muda. É semelhante à transformação dos formatos de documentos, discutidos anteriormente em **B1.4.** e **B2.2.** Pode incluir desde a recompilação do código-fonte para uma nova plataforma até a recodificação do *software*, a partir do zero, para outra linguagem de programação.

B2.4. Visualizadores e conversão no ponto de acesso. O uso de ferramentas de *software* ou métodos de transformação que oferecem acessibilidade temporária quando necessário, usando a cadeia de dados original.

B2.5. Emulação. Uso de um *software* que faz uma tecnologia se comportar como outra. Em outras palavras, o ato de fazer com que tecnologias futuras se comportem tal como o ambiente de origem de um documento arquivístico digital preservado, de modo que o documento original possa ser apresentado em sua manifestação original, a partir de cadeias de dados originais ou convertidas.

B3. Abordagens não digitais. Ato de copiar os documentos digitais para meios analógicos relativamente estáveis, tais como papel ou microfilme, transferindo o ônus da preservação para uma cópia analógica, no lugar do objeto digital. Esta abordagem destrói qualquer funcionalidade oferecida pelo *software*, como a manuseabilidade.

B4. Restauração de dados (arqueologia digital). Recuperação de documentos arquivísticos como *bits* a partir de suportes físicos, seguida de passos para restaurar a inteligibilidade dos documentos recuperados. É mais frequentemente empregada na recuperação de dados de suportes degradados, danificados ou falhos, mas os métodos de restaurar a inteligibilidade têm sido usados para resgatar documentos em formatos obsoletos.

o Para uma análise detalhada das questões e tendências atuais na seleção de formatos de arquivo, encapsulamento, marcação e codificação, juntamente com recomendações para desenvolver e implementar políticas para a escolha de formatos de arquivo digital para preservação a longo prazo, consulte: Evelyn Peters McLellan (2006), *Selecting Digital File Formats for Long-Term Preservation: InterPARES 2 General Study 11 Final Report*. Disponível em inglês em: http://www.interpares.org/display_file.cfm?doc=ip2_file_formats(complete).pdf, e em francês em: http://www.interpares.org/display_file.cfm?doc=ip2_formats_fichiers_numériques.pdf

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.

5 Mg Migração

8 Rr Requisitos de referência

9 Id Identificaçã

25 Cc Custódia Confiáv