Biblios
ISSN 1562-4730 (online)

Autenticidade de documentos arquivísticos digitais: análise de um processo de afastamento

Marcelo Lopes Kroth
Daniel Flores

Universidade de Federal de Santa Maria – UFSM, Brasil

CASE REPORT

Resumo

Objetivo. Apresenta uma análise dos aspectos que envolvem a presunção de autenticidade de um documento arquivístico nato digital, utilizando o processo de afastamento produzido na Universidade Federal de Santa Maria como estudo de caso.
Método. A pesquisa teve como base a metodologia utilizada no Projeto InterPARES. Foram analisados os contextos jurídico-administrativo, de proveniência, de procedimentos, documental e tecnológico, considerando a Resolução Nº 37, de 19 de dezembro de 2012 do Conselho Nacional de Arquivos, que Aprova as Diretrizes para a Presunção de Autenticidade de Documentos Arquivísticos Digitais.
Resultados. O caso analisado trata-se de um sistema informatizado utilizado no processo de afastamento dos servidores docentes e técnico-administrativos em educação. Mais de dezessete mil processos já foram produzidos exclusivamente em meio digital desde que o sistema entrou em operação, no final de 2012.
Conclusões. A informatização dos processos contribuiu para a transparência ativa, conforme a Lei nº 12.527/2011, e também reduziu o tempo de trâmite do processo, porém a falta de observância de alguns requisitos de gestão arquivística que recai sobre os documentos nato digitais pode gerar incertezas a respeito da autenticidade, bem como, o risco de perda de parte da memória da universidade em longo prazo.

Palavras-chave

Autenticidade; Documentos digitais; Gestão de documentos; Preservação digital; Universidade Federal de Santa Maria

Authenticity of Digital Records: Analysis of a Leave of Absence Process

Abstract

Objective. It presents an analysis of the issues surrounding the authenticity of presumption of a born digital record, using the leave absence process produced at the Federal University of Santa Maria as a case study.
Method. The research was based on the InterPARES Project methodology. The contexts analyzed were legal and administrative, provenance, procedures, documentation and technology, considering a resolution that approves the Guidelines for the Presumption of Archival Digital Document Authenticity.
Results. The case analyzed it is a computerized system used in the leave of absence process of teachers and technical and administrative staff in education. More than seventeen thousand documents have produced exclusively in digital media since the system came into operation in late 2012.
Conclusions. The computerization contributed to the active transparency and reduced the time processing of the process, but the lack of compliance with some archival management requirements that falls on the digital born documents can generate uncertainty about the process authenticity, as well as the risk of losing part of long-term university's memory.

Keywords

Authenticity; Digital preservation; Digital records; Records management; Universidade Federal de Santa Maria

1 Introdução

Os documentos produzidos por entidades públicas, no exercício de suas funções e atividades são instrumentos fundamentais para a tomada de decisão, comprovação de direitos individuais e coletivos e para o registro da memória social. A Lei nº 8.159, de 8 de janeiro de 1991, dispõe sobre a política nacional de arquivos públicos e privados e explicita as responsabilidades com relação aos documentos:

> Art. 25 - Ficará sujeito à responsabilidade penal, civil e administrativa, na forma da legislação em vigor, aquele que desfigurar ou destruir documentos de valor permanente ou considerado como de interesse público e social (BRASIL, 1991).

A Lei nº 8.159, ainda, considera arquivos "os conjuntos de documentos produzidos e recebidos por órgãos públicos, instituições de caráter público e entidades privadas, em decorrência do exercício de atividades específicas, bem como por pessoa física, qualquer que seja o suporte da informação ou a natureza dos documentos". A mesma lei também conceitua a gestão de documentos como "o conjunto de procedimentos e operações técnicas referentes à sua produção, tramitação, uso, avaliação e arquivamento em fase corrente e intermediária, visando a sua eliminação ou recolhimento para guarda permanente" (BRASIL, 1991).

Mais recentemente, foi publicada a Lei nº 12.527, de 18 de novembro de 2011 (BRASIL, 2011), conhecida como Lei de Acesso à Informação, que dispõe sobre os procedimentos a serem observados pela União, Estados, Distrito Federal e Municípios com a finalidade de garantir o acesso a informações previsto na Constituição Federal de 1998. O §2º do Art. 216 da Constituição destaca que "cabem à administração pública, na forma da lei, a gestão da documentação governamental e as providências para franquear sua consulta a quantos dela necessitem" (BRASIL, 1998).

A Lei de Acesso à Informação estabelece que os órgãos e entidades públicas devem divulgar na internet, independentemente de solicitações, informações de interesse geral ou coletivo. Com o acesso prévio à informação, o cidadão não precisa acionar os órgãos e entidades públicas, gerando benefícios tanto para ele, quanto economia de tempo e recursos para a administração pública. Dessa forma, a disponibilização de documentos públicos na internet redefine os horizontes de acesso à informação em direção à essência dos arquivos.

Anteriormente, a disponibilização das informações era uma atividade apenas dos arquivos permanentes quando um documento já estava "arquivado", pautadas pelo princípio de que a circulação de informações representava riscos. Portanto, dominava a cultura do sigilo que, muitas vezes, prevalece na gestão pública. Hoje, o acesso à informação sob a guarda de órgãos e entidades públicas é direito fundamental do cidadão. A boa gestão dessas informações passou a ser responsabilidade de todos os envolvidos desde a produção, tramitação, utilização e guarda dos documentos.

A utilização dos recursos tecnológicos para produção, disseminação e acesso aos documentos é fundamental para que os objetivos previstos na Lei de Acesso à Informação, porém ainda causa algumas preocupações aos profissionais da informação. Algumas das razões são a obsolescência tecnológica, decorrente da rápida evolução das Tecnologias de Informação e Comunicação (TICs), a fragilidade do suporte digital e a falta de observância dos princípios da teoria arquivística pelos gestores de TIC responsáveis pelos sistemas de informação. Tudo isso coloca em risco o patrimônio produzido por uma nova forma de registro do documento, o documento digital e consequentemente o documento arquivístico digital (INNARELLI, 2015).

Segundo o CONARQ (2012), documento arquivístico é o documento produzido ou recebido por uma pessoa física ou jurídica, no decorrer das suas atividades, qualquer que seja o suporte, e retido para ação ou referência. Por sua vez, o documento digital é a informação registrada, codificada em dígitos binários, acessível e interpretável por meio de sistema computacional. Finalmente, o documento arquivístico digital é o documento digital reconhecido e tratado como um documento arquivístico.

Os documentos digitais são produzidos e incorporados aos sistemas de informação das instituições com pouca ou nenhuma preocupação arquivística. Na maioria das vezes, os documentos digitais são gerenciados e preservados por profissionais da área de tecnologia da informação, fato que pode levar à perda de autenticidade e contexto dos documentos arquivísticos digitais ou à perda parcial ou total do documento (INNARELLI, 2015).

O Projeto InterPARES (*International Research on Permanent Authentic Records in Electronic Systems*) (InterPARES, 2012) tem desenvolvido conhecimento teórico-metodológico essencial para a preservação de longo prazo de documentos arquivísticos digitais autênticos. Um dos resultados do projeto foi concluir, de forma empírica, que é impossível preservar os documentos digitais devido à sua construção inata, só sendo possível preservar a capacidade de reproduzi-los (DURANTI, 2010). A reprodução de documentos digitais tornou-se o único meio que os usuários humanos podem confiar para acessá-los novamente após a primeira vez que são salvos, independentemente de quanto tempo eles vão existir. Assim, a preservação da capacidade de reproduzir, tornou-se a pedra angular da preservação digital (XIE, 2011). Neste cenário, a presunção de autenticidade dos documentos arquivísticos digitais deve se apoiar na evidência de que eles foram mantidos com uso de tecnologias e procedimentos administrativos que garantam a sua identidade e integridade; ou que, pelo menos, minimizem os riscos de modificações dos documentos a partir do momento em que foram salvos pela primeira vez e em todos os acessos subsequentes (CONARQ, 2012).

Além disso, essa presunção baseia-se na confirmação da existência de uma cadeia de custódia ininterrupta - linha contínua de custodiadores de documentos arquivísticos pela qual se assegura que esses documentos são os mesmos desde o início, não sofreram nenhum processo de alteração e, portanto, são autênticos (CONARQ, 2012), desde o momento da produção do documento até a sua transferência para a instituição arquivística responsável pela sua preservação no longo prazo. Caso essa cadeia de custódia seja interrompida, o tempo em que os documentos não estiveram sob a proteção do seu produtor ou sucessor pode causar dúvidas sobre a sua autenticidade (CONARQ, 2012).

A presunção de autenticidade dos documentos arquivísticos digitais possui dois componentes: integridade, que é a capacidade de um documento arquivístico transmitir exatamente a mensagem que levou à sua produção de maneira a atingir seus objetivos; e identidade, que é o conjunto dos atributos de um documento arquivístico que o caracterizam como único e o diferenciam de outros documentos arquivísticos (CONARQ, 2012).

Para garantir a integridade dos documentos digitais, é fundamental a observância dos conceitos de forma fixa, conteúdo estável, forma documental armazenada ou manifestada, assim como a fixidez da informação em seu suporte de forma indissociável. A utilização da forma documental manifestada é uma das características do documento arquivístico que mais impactam na percepção humana quanto à sua confiabilidade. Talvez por isso, tem-se orientado a escolha do formato PDF/A (formato de arquivo que assegura o acesso em longo prazo de documentos eletrônicos) para a produção de documentos arquivísticos digitais, por sua baixa exigência de recursos tecnológicos para sua apresentação e sua perspectiva de perenidade (SANTOS, 2012). Para a verificação de fixidez são utilizados algoritmos de *hash* a criação de um código a partir de um objeto digital. Se o código criado em um ponto é idêntico ao código criado pelo mesmo algoritmo em um momento posterior, isso indica que o objeto não se alterou durante esse ínterim (PREMIS, 2015).

Outra grande preocupação é a preservação dos documentos a longo prazo, observando os impactos das mudanças tecnológicas, incluindo o suporte a novas mídias de armazenamento e formato de dados e ainda uma comunidade de usuários em constante transformação. Nesse contexto, os repositórios digitais vêm desempenhando um papel importante na construção de um espaço arquivístico digitais responsável pela guarda confiável de documentos digitais.

Segundo o CONARQ (2014), um repositório digital de documentos arquivísticos (RDC-Arq) é um repositório digital que armazena e gerencia documentos arquivísticos digitais nas fases corrente, intermediária e permanente. Como tal, esse repositório deve ser capaz de gerenciar os documentos e seus metadados (dados estruturados que descrevem o documento) de acordo com as práticas e normas da Arquivologia, especificamente relacionadas à gestão documental, descrição arquivística multinível e preservação; e resguardar as características do documento arquivístico, em especial a autenticidade e a relação orgânica entre os documentos.

O RDC-Arq deve seguir o Modelo OAIS (*Open Archival Information System*) (CCSDS, 2002), que descreve um quadro conceitual para um sistema completo e universal de guarda permanente de documentos digitais, especificando como devem ser preservados desde o momento em que são inseridos no repositório digital até o momento em que ficam disponíveis para acesso pelo usuário final (FLORES; HEDLUND, 2014).

No processo de empacotamento OAIS (SIP – Pacote de Submissão, AIP – Pacote de Arquivamento e DIP – Pacote de Disseminação), para o recolhimento, os documentos arquivísticos podem ser compostos por um ou mais objetos

digitais, que por sua vez são objetos conceituais. Um objeto conceitual pode ser representado em diversos formatos lógicos (PDF, PDF/A, etc.), podendo cada um destes ser suportado por inúmeras representações físicas, que são o suporte físico dos bits (FERREIRA, 2006; ROGERS, 2015).

No final de 2012, a Universidade Federal de Santa Maria (UFSM) informatizou o processo de afastamento dos servidores docentes e técnico-administrativos em educação, gerando um volume considerável de documentos natos digitais, reduzindo o tempo de trâmite do processo.

Esse artigo apresenta o estudo acerca da presunção de autenticidade e preservação de um documento arquivístico nato digital produzido na UFSM, onde se buscou identificar o seu contexto de produção, através da diplomática contemporânea, com a finalidade contextualizar o documento dentro das atividades do órgão produtor e da sua estrutura funcional. O texto está estruturado em 4 seções, sendo a Seção 1 de cunho introdutório, a Seção 2 identifica a metodologia utilizada, a Seção 3 relata o estudo de caso envolvendo o processo de afastamento dos servidores e, por fim, a Seção 4 apresenta as considerações finais.

2 Metodologia

O método de pesquisa utilizado para chegar aos objetivos propostos foi o de estudo de caso clássico (YIN, 2005). Os contextos analisados foram: o contexto jurídico-administrativo, o contexto de proveniência, o contexto de procedimentos, o contexto documental e contexto tecnológico, considerando a Resolução Nº 37, de 19 de dezembro de 2012, que Aprova as Diretrizes para a Presunção de Autenticidade de Documentos Arquivísticos Digitais e inspirado nos estudos de caso realizados pelo Team Brasil referente à fase 3 do projeto InterPARES.

O Projeto InterPARES, organizado através de uma ação colaborativa de diversos países, incluindo o Brasil, por meio de uma equipe denominada Team Brasil coordenada pelo Arquivo Nacional, propôs-se a desenvolver conhecimento para a preservação de registros autênticos criados e/ou mantidos em formato digital, assegurando sua longevidade e sua autenticidade. Em colaboração com o Ministério da Saúde, a Universidade Estadual de Campinas (UNICAMP), a Câmara dos Deputados e o Sistema de Arquivos do Estado de São Paulo (SAESP) o projeto Team Brasil desenvolveu, nove estudos de casos sobre a análise diplomática e o contexto em que documentos arquivísticos ou sistemas de manutenção de documentos se inseriam.

Foram definidos no âmbito do projeto cinco tipos de contexto associados aos documentos arquivísticos: o contexto jurídico-administrativo é o sistema legal e organizacional ao qual a instituição produtora pertence; o contexto de proveniência se refere à entidade produtora, seu mandato, estrutura e funções; o contexto de procedimentos compreende os procedimentos relativos às atividades no curso das quais o documento é produzido; o contexto documental é definido como o fundo arquivístico ao qual o documento pertence e sua estrutura interna; e o contexto tecnológico é definido como as características dos componentes tecnológicos de um sistema informatizado no qual os documentos são criados (InterPARES, 2012).

3 Resultados: apresentação e discussão

Nesta seção serão analisados os cinco contextos definidos pelo Projeto InterPARES (jurídico-administrativo, de procedimentos, de proveniência, documental e tecnológico) no qual o documento foi produzido e usado ao longo do tempo, fundamentais para constatação da sua identidade e integridade.

3.1 Contexto Jurídico-Administrativo

Segundo o projeto InterPARES (2012), o contexto jurídico-administrativo é o sistema legal e organizacional ao qual a instituição produtora pertence. A Universidade Federal de Santa Maria (UFSM), idealizada e fundada pelo Prof. Dr. José Mariano da Rocha Filho, foi criada pela Lei n. 3.834- C, de 14 de dezembro de 1960, com a denominação de Universidade de Santa Maria. A UFSM é uma Instituição Federal de Ensino Superior constituída como Autarquia Especial vinculada ao Ministério da Educação, localizada no centro geográfico do Estado do Rio Grande do Sul. A estrutura acadêmico-administrativa da UFSM, por meio da Portaria n. 156, de 12 de março de 2014, está constituída pela Administração Superior, as Unidades Universitárias, além das Unidades de ensino médio, técnico e tecnológico. As diretrizes da Instituição são traçadas por órgãos deliberativos da Administração Superior: o Conselho Universitário (CONSU), o Conselho de Ensino Pesquisa e Extensão (CEPE), o Conselho de Curadores e a Reitoria (PRADEBON; FLORES, 2014).

3.2 Contexto de Proveniência

O contexto de proveniência se refere à entidade produtora, seu mandato, estrutura e funções; o contexto de procedimentos compreende os procedimentos relativos às atividades no curso das quais o documento é produzido (InterPARES, 2012). De acordo com o Art. 23 do Regimento Geral da Universidade Federal de Santa Maria de 2011, compete à Pró-Reitoria de Gestão de Pessoas (PROGEP) propor e implementar a política de gestão de pessoas no âmbito da UFSM, por meio do planejamento, organização, coordenação, controle e avaliação dos planos, programas e processos voltados ao seu desenvolvimento global. Além disto, compete também, dentre outras atribuições: assegurar o desenvolvimento dos servidores em suas respectivas carreiras para os propósitos de capacitação e qualificação; analisar processos referentes a concessões, licenças e benefícios dos servidores. Um dos documentos produzidos pela PROGEP, mais especificamente pelo Núcleo de Educação e Desenvolvimento (NED) da Coordenadoria de Ingresso, Mobilidade e Desenvolvimento (CIMDE), é a Portaria de Afastamento dos Servidores Docentes ou Técnicos-Administrativo em Educação (TAE).

3.3 Contexto de Procedimentos

Segundo InterPARES (2012), o contexto de procedimentos compreende os procedimentos relativos às atividades no curso das quais o documento é produzido. Até o final de 2012 os processos de afastamento eram feitos em papel, enviando o formulário com os detalhes do afastamento do servidor, bem como toda a documentação adicional necessária à Divisão de Protocolo do Departamento de Arquivo Geral (DAG) para autuação do processo. A partir no final de 2012, com o início da operação do sistema informatizado, o servidor docente ou técnico-administrativo em educação da Universidade Federal de Santa Maria deve iniciar o processo de afastamento única e exclusivamente via Web através do Portal de Afastamentos. O acesso pode ser feito através do Portal do RH ou acessando o endereço do portal diretamente no navegador. A identificação do servidor é feita através de *login* (matrícula SIAPE) e senha, que é única para todo o sistema de gestão da universidade.

O número do processo de afastamento segue o padrão da Portaria SLTI/MP nº 3, de 16 de maio de 2003, que define os procedimentos para a utilização do Número Único de Protocolo (NUP). O número é composto por dezessete dígitos (00000.000000/0000-00), de maneira análoga aos processos produzidos em outros suportes, respeitando o seguinte formato: código da unidade protocolizadora (5 dígitos); sequencial numérico dos processos autuados (6 dígitos); ano de formação do documento (4 dígitos); e dígitos verificadores (2 dígitos). Segundo a Portaria, os processos autuados pelos órgãos públicos federais integrantes do Sistema de Serviços Gerais (órgãos e unidades da Administração Federal direta, autárquica e fundacional) devem adotar a sistemática do NUP, visando a integridade do número atribuído ao documento, na unidade protocolizadora de origem (BRASIL, 2003).

Após o preenchimento das informações relativas ao afastamento, o processo segue para análise da chefia imediata e, caso deferido, segue para a direção do órgão em que o servidor está lotado, também para análise. Após a autorização da direção do órgão, o processo segue para a Coordenadoria de Ingresso, Mobilidade e Desenvolvimento (CIMDE), que revisa as informações e documentação integrantes no processo de afastamento e, caso não encontre nenhuma divergência, encaminha para o Gabinete do Reitor (autoridade máxima da instituição) para autorizar a emissão da portaria de afastamento do servidor.

No instante em que o Gabinete do Reitor autoriza o afastamento, os dados da autorização são registrados no banco de dados, quais sejam: usuário que deferiu o afastamento (reitor, vice-reitor ou diretor em exercício), data e hora da autorização.

Depois que a autoridade máxima da universidade autorizou o afastamento, o processo retorna para a CIMDE para a escolha do modelo e revisão do texto da portaria. Com isso o processo pode seguir para a Secretaria Administrativa da Pró-Reitoria de Gestão de Pessoas (SEADM) onde a portaria recebe a numeração e é gerado o objeto digital no formato PDF.

Figura 1. Informações sobre o afastamento.

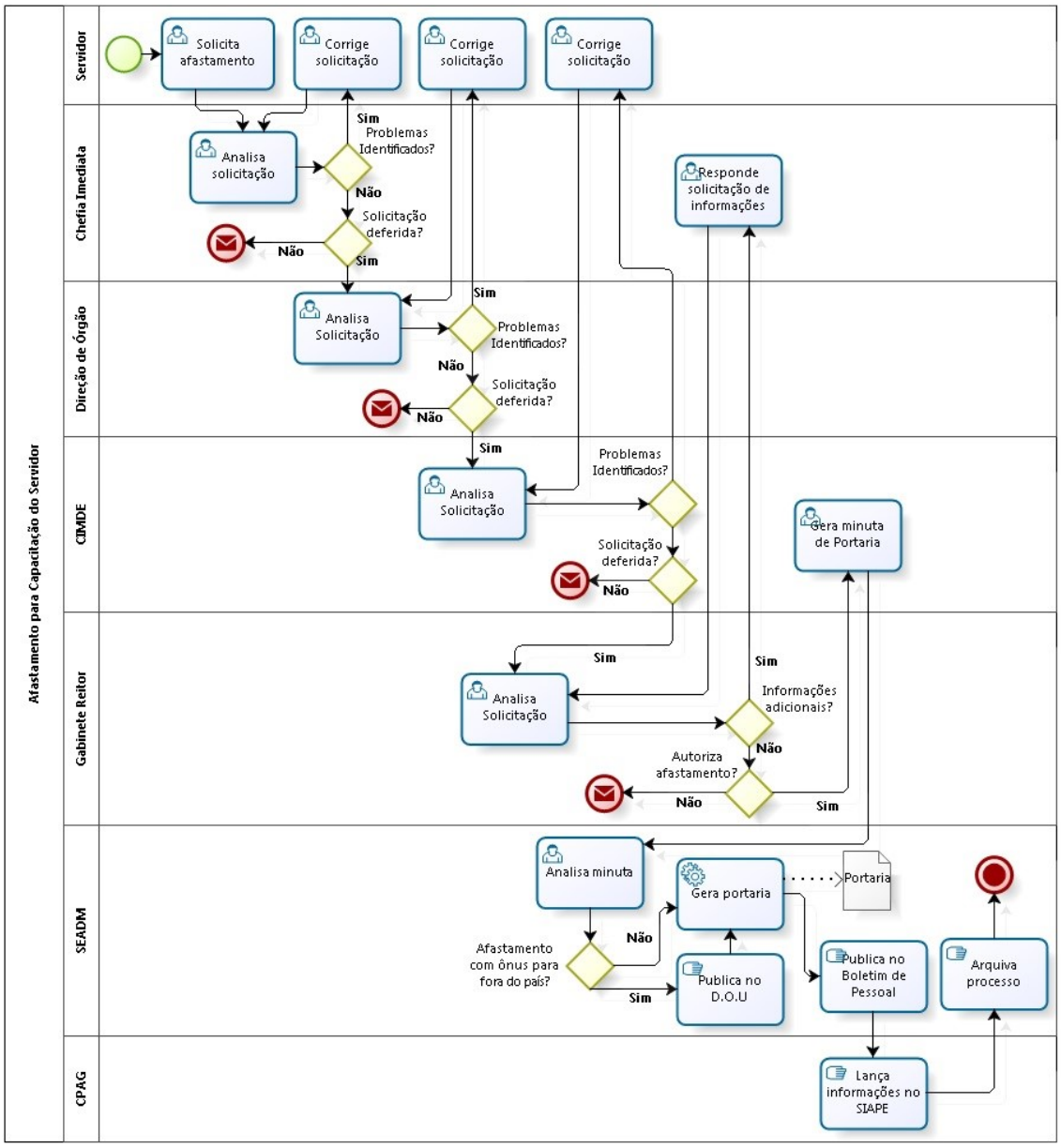
Fonte: Portal de Afastamento da UFSM (UFSM, 2016c).

Após a emissão da portaria de afastamento do servidor, o processo é finalizado na Coordenadoria do Sistema de Pagamentos (CPAG) que providencia o pagamento ao servidor conforme o ônus do afastamento, caso exista (Figura 1).

O processo de afastamento segue um fluxo de procedimentos e autorizações, a partir da solicitação feita pelo próprio docente ou técnico administrativo em educação, conforme a natureza do afastamento, que pode ser de três tipos (UFSM, 2016a):

- Processo de Afastamento Eventual: Afastamento por curto período para atividades relacionadas ao trabalho, tais como atividades com alunos (banca, orientações, viagens), participar de comissões e ministrar cursos.
- Processo de Afastamento para Qualificação: Afastamento de servidor para realização de cursos de educação formal, em nível de pós-graduação lato sensu e stricto sensu (especialização, mestrado, doutorado e pós-doutorado).
- Processo de Afastamento para Capacitação: Afastamento para participação em ações de capacitação e aperfeiçoamento, tais como seminário, congresso, conferência, curso, visita técnica, estágio ou intercâmbio (Figura 2).

Figura 2. Fluxo do Processo de Afastamento para Capacitação.



Fonte: Portal de Processos de UFSM (UFSM, 2016b).

3.4 Contexto Documental

O contexto documental é o fundo arquivístico ao qual o documento pertence e sua estrutura interna (InterPARES, 2012). O Departamento de Arquivo Geral, criado em 17 de janeiro de 1990, na 438º Sessão do Conselho Universitário, como órgão suplementar central da UFSM vinculado à Pró-Reitoria de Administração, tem por finalidade coordenar o sistema de arquivos na UFSM. Em conformidade com a Política dos Fundos Documentais da Instituição o documento arquivístico aqui estudado está incluso ao Fundo I "Pró-Reitoria de Gestão de Pessoas" (CASTANHO; *et al.*, 2000).

3.5 Contexto Tecnológico

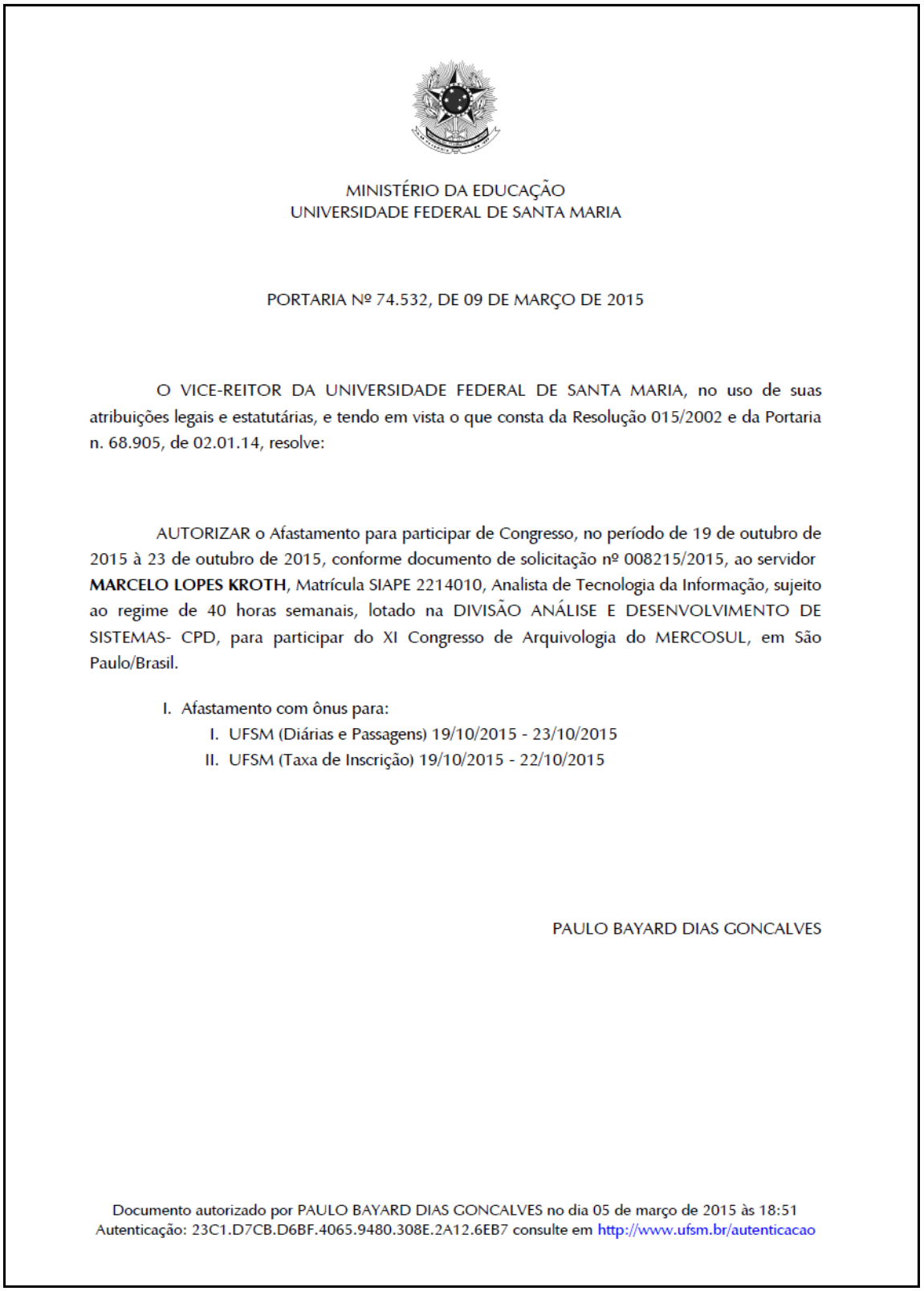
Por fim, o contexto tecnológico que, segundo o projeto InterPARES (2012), são as características dos componentes tecnológicos de um sistema informatizado no qual os documentos são criados. O sistema responsável pela elaboração da Portaria de Afastamento do Servidor na UFSM é o Sistema de Informações Educacionais (SIE). O SIE é um sistema de gestão integrado, onde existe um subsistema específico para os processos de afastamento integrado ao sistema de gestão de pessoas e demais sistemas administrativos (Figura 3).

Figura 3. Metadados da Portaria de Afastamento.

Fonte: Portal de Afastamento da UFSM (UFSM, 2016c).

A portaria é produzida a partir de registros no sistema resultante do processo de afastamento. Os dados do afastamento são mantidos em tabelas no banco de dados institucional e são agrupados para formar o processo de afastamento.

Figura 4. Portaria de Afastamento Digital.



MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DE SANTA MARIA

PORTARIA Nº 74.532, DE 09 DE MARÇO DE 2015

O VICE-REITOR DA UNIVERSIDADE FEDERAL DE SANTA MARIA, no uso de suas atribuições legais e estatutárias, e tendo em vista o que consta da Resolução 015/2002 e da Portaria n. 68.905, de 02.01.14, resolve:

AUTORIZAR o Afastamento para participar de Congresso, no período de 19 de outubro de 2015 à 23 de outubro de 2015, conforme documento de solicitação nº 008215/2015, ao servidor **MARCELO LOPES KROTH**, Matrícula SIAPE 2214010, Analista de Tecnologia da Informação, sujeito ao regime de 40 horas semanais, lotado na DIVISÃO ANÁLISE E DESENVOLVIMENTO DE SISTEMAS- CPD, para participar do XI Congresso de Arquivologia do MERCOSUL, em São Paulo/Brasil.

I. Afastamento com ônus para:
   I. UFSM (Diárias e Passagens) 19/10/2015 - 23/10/2015
   II. UFSM (Taxa de Inscrição) 19/10/2015 - 22/10/2015

PAULO BAYARD DIAS GONCALVES

Documento autorizado por PAULO BAYARD DIAS GONCALVES no dia 05 de março de 2015 às 18:51
Autenticação: 23C1.D7CB.D6BF.4065.9480.308E.2A12.6EB7 consulte em http://www.ufsm.br/autenticacao

Fonte: Portal de Afastamento da UFSM (UFSM, 2016c).

Cada etapa do processo requer autorização das chefias envolvidas e o resultado final é um arquivo no formato PDF de forma fixa e conteúdo estável, com autenticação, contendo as informações sobre a data, hora e a autoridade responsável pela autorização, apesar de ser produzida pela PROGEP (Figura 4).

As chefias das unidades responsáveis estão automaticamente autorizadas pelo sistema de gestão. Outros

servidores que não possuam chefia também podem ter autorização para encaminhar, dar despachos ou autorizar afastamentos, porém este tipo de permissão deve ser feito manualmente no sistema e não existe uma política formalizada na instituição para concessão deste modelo de autorização. Depois de autorizado o afastamento do servidor, o processo tramita internamente na PROGEP até ser gerada a Portaria de Afastamento do Servidor.

A autenticação é realizada através de um código gerado com base em um algoritmo de *hash* utilizando as informações contidas no documento. Pode ser consultada a autenticação através do Sistema de Autenticação de Relatórios (UFSM, 2016d).

É importante salientar que o conceito de autenticação é diferente de autenticidade. A autenticidade é a qualidade de o documento ser verdadeiro, isto é, ser exatamente aquele que foi produzido, ao passo que autenticação é a declaração da autenticidade feita em um dado momento por uma pessoa autorizada para tal. Enquanto declaração, a autenticação não garante necessariamente a autenticidade do documento, na medida em que se pode declarar como autêntico algo que não é. Da mesma forma, um documento pode ser considerado autêntico sem que nele conste uma autenticação (CONARQ, 2012).

Como forma de garantir a manutenção da autenticidade, é fundamental registrar que é obrigatória a adoção de um sistema de gestão, ou seja, um SIGAD nas idades correntes e intermediárias e a adoção de um RDC-Arq na idade permanente, mantendo assim, tanto a cadeia de custódia como a cadeia de preservação na interoperabilidade que será necessária no momento de recolhimento dos documentos arquivísticos, devidamente empacotados de acordo com o Modelo OAIS (em SIP – Pacote de Submissão de acordo com o Modelo, CCSDS, 2002), do SIGAD ao RDC-Arq. Há que se ressaltar que o RDC-Arq também pode ou deve ser adotado nas idades correntes e intermediárias quando nos deparamos com documentos que tenham ao menos uma das características: - documentos de longa temporalidade de guarda no arquivo corrente ou intermediário; - documentos complexos como websites, e-mails ou que apresentem muitos componentes digitais estrutura do documento; e – documentos sensíveis, que tenham uma análise arquivística e sejam considerados complexos ou específicos para a sua manutenção em um Sistema de Gestão Arquivística de Documentos – SIGAD nas idades correntes e intermediária (considerando neste caso também os sistemas de negócio que incorporaram as funcionalidades de um SIGAD, ou seja, um SIGAD de Negócio).

O sistema de gestão mantém automaticamente os registros sobre a utilização das aplicações, armazenando as informações sobre os usuários, data e hora que as aplicações foram acessadas. Além disso, o sistema possui um mecanismo de auditoria onde é possível sinalizar quais campos do banco de dados devem gerar log com as atualizações realizadas (login do usuário, data e hora da operação, conteúdo do campo antes da alteração e conteúdo alterado). Os dados armazenados no SIE e o próprio sistema são gerenciados pela unidade de tecnologia da informação da universidade que é o Centro de Processamento de Dados (CPD). Sendo que os backups de segurança são acondicionados em local distinto do prédio.

Uma análise que se pode realizar é o fato de considerar que as informações que compõem o processo de afastamento ainda estão em forma documental diplomática armazenada, ou seja, estão em tabelas no banco de dados da instituição, estas ainda estão sujeitas a alterações, muito diferente da adoção da forma documental diplomática manifestada, onde as alterações são sensivelmente reduzidas (e em caso de acontecimento, serão devidamente documentadas e registradas com metadados específicos e sob a égide do sistema), e onde já existe a garantia implícita da forma fixa e conteúdo estável. Não obstante às políticas de segurança da informação e controles de acesso ao banco de dados institucional, as informações podem sofrer atualizações feitas pelo próprio sistema de gestão da instituição como resultado da atividade cotidiana da universidade.

Como citado anteriormente, e para garantir que as informações que compõem o processo não sejam modificadas de forma inadvertida, poderia ser utilizada a estratégia de manifestação diplomática do processo (geração de um PDF/A) a cada ação realizada, ainda assim, não se teria a garantia que as informações permaneceriam inalteradas a cada geração, todavia contribuiria sobremaneira além de garantir a forma fixa e conteúdo estável. Outra alternativa seria o registro das informações, mesmo que no mesmo banco de dados, em forma de metadados associados ao processo com mecanismos de isolamento do sistema de gestão, então a manifestação do processo poderia ser feita utilizando os metadados produzidos e com o registro de versionamento de documentos e a incorporação de metadados que registrem as alterações e garantam a retroagibilidade em caso de uma adulteração indevida.

4 Conclusões

Desde o final de 2012, após a informatização do processo de afastamento dos servidores docentes e técnico-administrativos em educação na Universidade Federal de Santa Maria, já foi produzido um volume considerável de documentos nato digitais, reduzindo o tempo de trâmite do processo, porém sem a devida preocupação sobre alguns aspectos importantes acerca de presunção de autenticidade, além dos riscos de perda da memória da universidade em longo prazo.

As informações que compõem o processo de afastamento estão em tabelas no banco de dados da instituição, que estão sujeitas a alterações e demandam de uma intervenção arquivística no tocante à manifestação diplomática, alterando a forma documental diplomática de armazenada para manifestada. Não obstante às políticas de segurança da informação e controles de acesso ao banco de dados institucional, as informações podem sofrer atualizações feitas pelo próprio sistema de gestão da instituição como resultado da atividade cotidiana da universidade. Para garantir que as informações que compõem o processo não sejam modificadas de forma inadvertida, poderia ser utilizada uma estratégia de manifestação do processo (geração de um PDF/A) a cada ação realizada, ainda assim, não se teria a garantia que as informações permaneceriam inalteradas a cada geração. Outra alternativa seria o registro das informações, mesmo que no mesmo banco de dados, em forma de metadados associados ao processo com mecanismos de isolamento do sistema de gestão, então a manifestação do processo poderia ser feita utilizando os metadados produzidos.

A portaria produzida como resultado do processo de afastamento, que é gerada em formato PDF, possui forma fixa e conteúdo estável, apesar de não ser um formato para acesso em longo prazo (PDF/A). A utilização do formato PDF não chega a ser um problema, pois, atualmente, pode ser convertido em PDF/A sem prejuízo do objeto conceitual, pois não utiliza recursos que não são compatíveis com o formato PDF/A. Além do que, o subsistema poderia ser ajustado para produzir originalmente PDF/A, sem nenhum impacto no funcionamento do restante do processo de afastamento.

A manutenção da cadeia de custódia e de preservação não é garantida, pois não existem políticas nem ações de preservação dos documentos digitais do processo de afastamento, principalmente no arquivo permanente, que exige que o recolhimento do documento em um RDC-Arq na forma manifestada ou na forma armazenada, juntamente com o manifestador.

Sendo assim, o processo de afastamento do servidor docente e técnico administrativo em educação, não possuindo fixidez, pode gerar incertezas acerca da autenticidade dos documentos digitais produzidos. Além disso, a falta de políticas e ferramentas de preservação em longo prazo (RDC-Arq) para os documentos digitais pode comprometer parte da memória da universidade que atualmente já está sendo produzida de forma digital.

Referências

BRASIL. Constituição da República Federativa do Brasil de 1998. 1998.

BRASIL. Lei nº 12.527, de 18 de novembro de 2011. Regula o acesso a informações. 2011.

BRASIL. Lei nº 8.159, de 8 de janeiro de 1991. Dispõe sobre a política nacional de arquivos públicos e privados e dá outras providências. 1991.

BRASIL. Portaria Nº 3, de 16 de maio de 2003. 2003.

CASTANHO, Denise Molon et al. Uma política de arranjo documental para a Universidade Federal de Santa Maria. Santa Maria: Universidade Federal de Santa Maria, Departamento de Documentação, Curso de Arquivologia, 2000.

CCSDS. Reference model for an Open Archival Information System (OAIS). Magenta Book. 2002. Disponível em: <https://public.ccsds.org/pubs/650x0m2.pdf>. Acesso em: 30 set. 2016.

CONARQ. Diretrizes para a Implantação de Repositórios Digitais Confiáveis de Documentos Arquivísticos. Rio de Janeiro: Arquivo Nacional. 2014.

CONARQ. Diretrizes para a Presunção de Autenticidade de Documentos Arquivísticos Digitais. Rio de Janeiro: Arquivo Nacional. 2012.

DURANTI, L. From digital diplomatics to digital records forensics. Archivaria vol. 68, pp. 39 a 66. 2010.

FERREIRA, M. Introdução à Preservação Digital: Conceitos, estratégias e actuais consensos. 2006. Disponível em:

<https://repositorium.sdum.uminho.pt/bitstream/1822/5820/1/livro.pdf>. Acesso em: 30 set. 2016.

FLORES, D.; HEDLUND, D. A Preservação do Patrimônio Documental Através da Produção de Instrumentos de Pesquisa Arquivísticos e da Implementação de Repositórios Arquivísticos Digitais. Série Patrimônio Cultural e Extensão Universitária, IPAHN, p. 33, 2014. Disponível em: <http://portal.iphan.gov.br/uploads/publicacao/SerPatExt_n3_m.pdf>. Acesso em: 11 nov. 2015.

INNARELLI, H. C. Gestão da preservação de documentos arquivísticos digitais: proposta de um modelo conceitual. Tese (Doutorado) – Programa de Pós-Graduação em Ciência da Informação, - Escola de Comunicação e Artes, Universidade de São Paulo, São Paulo, 2015.

InterPARES. InterPARES Project. Canadá, 2012. Disponível em: <http://www.interpares.org>. Acesso em: 20 jul. 2015.

PRADEBON, D. R. S.; FLORES, D. Preservação para a futuridade do acesso ao documento arquivístico digital. Informação Arquivística, 129–135. 2014.

PREMIS. PREMIS Data Dictionary for Preservation Metadata. Version 3.0. 2015. Disponível em: <http://www.loc.gov/standards/premis/v3/premis-3-0-final.pdf>. Acesso em: 30 set. 2016.

ROGERS, C. Diplomatics of born digital documents – considering documentary form in a digital environment. Records Management Journal, 25(1), 6–20. 2015.

SANTOS, V. B. Preservação de documentos arquivísticos digitais. Ciência da Informação, v. 41, n. 1, p. 114–126, 2012.

UFSM. Autenticação de relatórios. UFSM – Autenticação de Relatórios. 2016a Disponível em: <https://portal.ufsm.br/autenticacao/consulta.html>. Acesso em: 10 ago. 2016.

UFSM. Portal de Afastamentos Ajuda. 2016b. Disponível em: <https://portal.ufsm.br/afastamento/helpMenu.html>. Acesso em: 10 ago. 2016.

UFSM. Portal de Afastamentos da UFSM. 2016c. Disponível em: <https://portal.ufsm.br/afastamento>. Acesso em: 10 ago. 2016.

UFSM. Portal de Processos da UFSM. 2016d. Disponível em: <http://coral.ufsm.br/processos/ProcessosPROGEP/#diagram/7b8d9fa5-57f2-42af-8fc2-042e8d0c2c6b>. Acesso em: 10 ago. 2016.

XIE, S. Building Foundations for Digital Records Forensics: A Comparative Study of the Concept of Reproduction in Digital Records Management and Digital Forensics. The American Archivist, vol. 74, n. 2, pp. 576 a 599. 2011.

YIN, Robert. K. Estudo de caso: planejamento e métodos. Tradução de Daniel Grassi. 3. ed. Porto Alegre: Bookman. 2005.

Dados dos autores

Marcelo Lopes Kroth
Mestre em Informática pela UFSM, membro da Comissão de Estudos da Gestão de Documentos Arquivísticos Institucionais (Gedai/UFSM) e pesquisador no grupo de pesquisa CNPq Gestão Eletrônica de Documentos Arquivísticos-Ged/A.
marcelo.tuco@ufsm.br

Daniel Flores
Doutor em Metodologías y Líneas de Investigación en Biblioteconomía y Documentación - Universidad de Salamanca/España. Professor Adjunto do Departamento de Documentação da Universidade Federal de Santa Maria.
dfloresbr@gmail.com

Recebido - Received: 2016-09-30

Aceitado - Accepted: 2018-02-03