Publicação da Associação Nacional de Entidades Promotoras de Epreendimentos Inovadores

locus científico

Volume 10 | Número 01 | Dezembro de 2025
ISSN 1981-6804

Códigos do Tempo: o desafio da guarda segura de softwares registrados em ICTs brasileiras

Helton Luiz de Oliveira, Alex Fernandes de Oliveira

anprotec

Códigos do Tempo: O Desafio da Guarda Segura de Softwares Registrados em ICTs Brasileiras

Helton Luiz de Oliveira[1], Alex Fernandes de Oliveira[2]

Resumo

Este artigo analisa os desafios técnicos, jurídicos e institucionais enfrentados pela Universidade Federal de Uberlândia (UFU) no processo de preservação de seus softwares registrados no Instituto Nacional de Propriedade Industrial (INPI). O estudo destaca a lacuna existente entre as limitações administrativas e tecnológicas desta universidade para cumprir a exigência legal de garantir a preservação dos códigos-fonte por 50 anos. Consequentemente, essa situação gera insegurança administrativa e jurídica quanto a garantia de prova de seus softwares registrados, visto que a perda ou corrompimento dessas informações ao longo dessa temporalidade fragiliza seus processos de propriedade intelectual. Para isso, são abordados aspectos referentes às alternativas de preservação, como cofres digitais, uso de blockchain, políticas de migração periódica e estratégias arquivísticas de preservação digital a longo prazo, todas tendo em vista garantir a soberania tecnológica e memória institucional. Com o apoio da Fundação de Amparo à Pesquisa do Estado de Minas Gerais FAPEMIG, no qual registramos agradecimento, foi desenvolvido esse estudo de caso sobre a atuação das unidades administrativas desta universidade no enfrentamento a problemática apontada. Como resultado, foi identificado a necessidade de construção de um ambiente de preservação digital para garantia do acesso aos softwares registrados nesta instituição, mas também que possa ser replicado nas demais ICTs do país.

Palavras-chave: Software; Preservação Digital; Registro; Propriedade intelectual; Soberania tecnológica; Repositório Arquivístico Digital Confiável; RDC-Arq

Abstract

This article analyzes the technical, legal, and institutional challenges faced by the Federal University of Uberlândia (UFU) in the process of preserving its software registered with the National Institute of Industrial Property (INPI). The study highlights the gap between the administrative and technological limitations of this university in complying with the legal requirement of ensuring the preservation of source codes for 50 years. Consequently, this situation generates administrative and legal uncertainty regarding the guarantee of proof of its registered software, since the loss or corruption of this information over this period of time weakens its intellectual property processes. To this end, aspects related to preservation alternatives are addressed, such as digital vaults, use of blockchain, periodic migration policies, and long-term archival strategies for digital preservation, all with a view to ensuring technological sovereignty and institutional memory. With the support of the Minas Gerais State Research Support Foundation FAPEMIG, for which we express our

[1] Helton Luiz de Oliveira, Universidade Federal de Uberlândia. E-mail: helton.oliveira@ufu.br
[2] Alex Fernandes de Oliveira, Universidade Federal de Uberlândia. E-mail: alex.oliveira@ufu.br

gratitude, this case study was developed on the performance of the administrative units of this university in addressing the problem identified. As a result, the need to build a digital preservation environment was identified to guarantee access to the software registered in this institution, but also that it can be replicated in other ICTs in the country.
Keywords: Software; Digital Preservation; Registry; Intellectual Property; Technological Sovereignty; Reliable Digital Archival Repository; RDC-Arq

Introdução

Vivemos uma era em que o software deixou de ser apenas um conjunto de códigos estáticos. Hoje, ele é um organismo dinâmico, frequentemente desenvolvido de forma colaborativa, com atualizações contínuas, múltiplas versões, integração com bibliotecas externas e funcionalidades hospedadas em nuvem.

Nesse cenário, o modelo tradicional de registro de software junto ao Instituto Nacional da Propriedade Industrial (INPI), baseado no depósito do código-fonte embaralhado, começa a mostrar suas limitações. O próprio Manual do INPI (2022) reconhece isso ao recomendar o uso de hash digital e assinatura digital ICP-Brasil para comprovar autenticidade e integridade do código, sem necessidade de armazená-lo diretamente.

No universo das Instituições Científicas, Tecnológicas e de Inovação (ICTs), o software tornou-se peça-chave em pesquisas, serviços e inovação. Embora o registro de programas de computador ainda seja uma das formas mais acessíveis de proteção da propriedade intelectual, emergem questões fundamentais: como preservar com segurança o código-fonte original de um software registrado há 20 ou 30 anos? Como garantir seu acesso, privacidade e validade jurídica nas próximas décadas?

Essa inquietação revela uma lacuna normativa crítica. Não há diretrizes nacionais claras sobre como as instituições públicas devem assegurar a guarda desses ativos digitais ao longo do tempo. Trata-se de um vazio que envolve dimensões técnicas, jurídicas e arquivísticas e que se evidencia na prática de universidades como a UFU, cujo caso serve como ponto de partida desta reflexão.

Autores como Christine Borgman (2007) e Marc Rosenberg (2001) já alertavam para os riscos da obsolescência digital e a necessidade de curadoria contínua dos ativos informacionais. Mesmo no exterior, Philip Goldstein (EDUCAUSE) destaca o papel das universidades como guardiãs do conhecimento tecnológico, ressaltando a urgência de soluções que garantam longevidade e autenticidade do código-fonte.

Além disso, a definição tradicional de software como “conjunto de instruções codificadas” torna-se insuficiente. Hoje, um software pode significar um algoritmo em Python, um app mobile, um sistema embarcado, uma IA treinada ou um script conectado a uma API. Ainda assim, o INPI adota uma abordagem documental e centralizada, que não dialoga com a fluidez dos ecossistemas digitais contemporâneos baseados em repositórios online, integração contínua e versões distribuídas.

Diante desse contexto, este artigo propõe uma análise crítica sobre a lacuna normativa brasileira quanto à guarda de softwares registrados em ICTs públicas. O objetivo é evidenciar os riscos jurídicos, operacionais e patrimoniais dessa ausência de diretrizes, à

luz de marcos legais e experiências institucionais. A pergunta que guia a reflexão é: a guarda segura de software é apenas uma questão técnica e jurídica ou representa um novo campo de disputa pela soberania tecnológica das universidades públicas brasileiras?

Metodologia

Nessa pesquisa, discute-se os desafios contemporâneos e futuros do registro, preservação e acesso aos programas de computador no contexto das ICTs, com foco na experiência da Universidade Federal de Uberlândia (UFU), e tendo a legislação vigente e as práticas do INPI como pressupostos de análise. O artigo analisa a lacuna entre o que a lei exige (preservação e acesso por 50 anos) e o que a realidade técnica permite, articulando a atuação entre unidades administrativas desta universidade, a Diretoria de Inovação e Transferência de Tecnologia (DIRTC) órgão responsável pela gestão da propriedade intelectual nessa universidade e a Divisão de Documentação (DIDOC), órgão responsável pela guarda oficial de bens documentais da instituição.

O artigo se configura como estudo de caso que busca debater e tecer caminhos seguros para o processo de preservação e acesso dos cerca de 200 (duzentos) CDs, Disquets e Pendrives que contém o registro original dos sofwares desenvolvidos pelos diversos programas de pesquisa desta universidade, e que são registrados no INPI. Acrescenta-se nessa problemática, o fato de que há um crescimento médio desse acervo de aproximadamente 4 (quatro) registros/mês, o que torna esse cenário ainda mais preocupante para essa instituição, visto que essas mídias têm um baixo prazo de vida útil.

Assim, tendo como base a literatura sobre a obsolescência digital, preservação de documentos digitais e repositórios digitais, a pesquisa buscou descrever e qualificar as caraterísticas de preservação e acesso destes registros, bem como a capacidade serviço de arquivo dessa instituição para lidar com esse desafio.

Tem como ponto de partida um expediente de trabalho disponibilizado pela DIDOC - a Assistência Técnica Arquivística, que se destina a atender quaisquer unidades acadêmica ou administrativa desta instituição para avaliação, destinação e preservação de seus documentos de arquivo. Neste caso, essa assistência técnica também buscou o envolvimento do Centro de Tecnologia da Informação (CTI), visto que este é o órgão responsável pela avaliação, implantação e manutenção dos suportes e ambientes digitais destinados à preservação destes softwares.

O desenvolvimento das atividades dessas unidades está registrado no processo nº 23117.009965/2024-31, que pode ser acessado através do módulo de Pesquisa Pública do Sistema Eletrônico de Informações SEI-UFU![3]. A partir das informações desse processo, foram refinados artigos na Plataforma Google Scholar e Resoluções do Arquivo Nacional, os

[3] Disponível em: https://www.sei.ufu.br/sei/modulos/pesquisa/md_pesq_processo_pesquisar.php?acao_externa=protocolo_pesquisar&acao_origem_externa=protocolo_pesquisar&id_orgao_acesso_externo=0 acesso em 19 maio 2025.

quais foram utilizados para direcionar a discussão desenvolvida, bem como responder os questionamentos levantados.

Discussão

1. Análise internacional comparativa

Como universidades de ponta tratam a guarda de software científico?

Em instituições como o MIT, Stanford e Oxford, a preservação de softwares produzidos internamente já é considerada uma vertente essencial da preservação digital institucional. Essas universidades investem em estruturas que integram repositórios institucionais, cofres digitais, sistemas de versionamento e hash de verificação para garantir autenticidade e acesso contínuo.

No MIT, iniciativas como o **MIT SuperCloud** (https://supercloud.mit.edu/studentprojects/) oferecem infraestrutura segura para o armazenamento e processamento de dados acadêmicos. A universidade também estimula o uso de repositórios próprios, evitando a dependência de soluções externas.

A Stanford University adota estratégias de emulação, como discutido no **Software Preservation and Emulation Symposium** (https://www.softwarepreservationnetwork.org/software-preservation-and-emulationstanford-a-symposium/)., permitindo que softwares antigos permaneçam acessíveis mesmo diante da evolução tecnológica.

Oxford, por sua vez, desenvolveu o **Oxford Common File Layout (OCFL)**, um modelo de estruturação voltado à integridade e preservação de longo prazo dos dados. Esse modelo pode inspirar abordagens robustas para instituições brasileiras.

Há esforços globais além das universidades?

Sim. A **Software Heritage Foundation**, com sede na França, mantém um arquivo aberto e universal de código-fonte. Ela permite que pesquisadores e instituições arquivem softwares de maneira acessível e verificável, reforçando o código como patrimônio científico.

Essas práticas mostram que a guarda de software vai além do cumprimento legal: trata-se de um compromisso com a memória tecnológica. Mesmo em contextos de menor recurso, como o das ICTs brasileiras, é possível adaptar e construir políticas próprias com base nessas referências. Protocolos conjuntos ou consórcios regionais de preservação digital podem fortalecer as iniciativas locais.

Mesmo tecnologias disruptivas preservam seus códigos?

Sim. O software que originou o Bitcoin, atribuído a Satoshi Nakamoto, permanece preservado em repositórios públicos como o GitHub, com versionamento aberto e controle comunitário. Isso evidencia que até mesmo soluções descentralizadas reconhecem o valor da preservação como legado digital.

Quais aprendizados são aplicáveis ao Brasil?

Diante do avanço internacional, universidades brasileiras podem adotar protocolos como o OCFL e explorar estratégias de emulação e versionamento. A colaboração com iniciativas como a Software Heritage Foundation pode garantir segurança jurídica, visibilidade e longevidade aos softwares acadêmicos nacionais.

2. A realidade brasileira e os caminhos para preservação segura

O que dizem as leis brasileiras e quais são os desafios na prática?

Apesar das boas referências internacionais, a realidade brasileira impõe uma série de desafios específicos para a guarda segura e legalmente válida de softwares desenvolvidos nas instituições públicas de ciência e tecnologia. De acordo com a Lei do Software, os direitos patrimoniais sobre um programa de computador duram 50 (cinquenta) anos, contados de 1º de janeiro do ano subsequente ao da sua publicação, ou na ausência desta, da sua criação.

> Art. 2º O regime de proteção à propriedade intelectual de programa de computador é o conferido às obras literárias pela legislação de direitos autorais e conexos vigentes no país, observado o disposto nesta lei.
> § 2º Fica assegurada a tutela relativa aos direitos do programa de computador pelo prazo de cinquenta anos, contados a partir de 1º de janeiro do ano subsequente ao da sua publicação, ou na ausência desta, da sua criação (LEI 9.609/1998).

Essa exigência, embora clara em termos legais, se torna complexa em termos arquivísticos e tecnológicos, visto que não há orientações sobre como deve ser garantido a guarda do código-fonte de forma confiável durante esse prazo.

Além disso, a Lei de Acesso à Informação (Lei nº 12.527/2011) e a Lei Geral de Proteção de Dados (Lei nº 13.709/2018) trazem camadas adicionais de exigências quanto à transparência, à segurança e à confidencialidade dos dados digitais. O desafio da guarda segura do software registrado envolve, portanto, uma conciliação entre normas que demandam acesso público e aquelas que exigem restrição e proteção.

A inexistência de uma orientação nacional, clara, voltada especificamente à preservação digital de softwares em instituições públicas faz com que cada ICT tenha que criar seus próprios protocolos, nem sempre alinhados com as melhores práticas jurídicas e arquivísticas. Isso gera um campo fértil para litígios futuros ou para a perda de direitos por má gestão da guarda destes documentos.

Portanto, pensar juridicamente a guarda de softwares é reconhecer que ela transita entre a proteção autoral, a responsabilidade civil da instituição, a transparência pública e o direito à memória, tendo em vista que no cenário atual as universidades precisam desenvolver políticas robustas que articulem esses pilares com os avanços tecnológicos disponíveis.

Soluções como a preservação destes registros em datacenters[4] terceiros vulgarmente denominados "nuvem" -, mesmo oferecendo a praticidade da guarda segura e redundância, se mostram extremamente arriscada, pois questões referentes à localização dos servidores, à soberania dos dados e à privacidade precisam ser consideradas, especialmente quando se trata de códigos que podem ter aplicação comercial ou estratégica. Além disso, a guarda de softwares registrados deve contemplar a possibilidade de acesso restrito, controle institucional e rastreabilidade, o que exige a construção de soluções internas ou híbridas, com armazenamento em servidores locais de alta segurança e planos de migração periódica.

Assim, as ICTs brasileiras enfrentam o desafio de adotar abordagens mais robustas, com políticas e planos institucionais para criação de ambientes de preservação digital que tenham como pressupostos: a criação de "cofres digitais" com criptografia, acesso auditável e rastreabilidade; utilização de blockchain para registro de hash dos códigos, garantindo autenticidade sem expor o conteúdo; e a definição de formatos-padrão de longo prazo para armazenamento (ex: PDF/A, XML, ASCII estruturado);

No caso em análise, coube ao serviço de arquivo, inicialmente, caracterizar esses registros, oficialmente, como documentos de arquivo[5], visto que fazem parte do fluxo processual estabelecido pela própria DIRTC, bem como por ser também uma antiga exigência do Instituto Nacional da Propriedade Intelectual (INPI), que requeria a entrega de CD contendo o código fonte do programa de computador desenvolvido na instituição, atendendo assim à seguinte orientação:

> A manutenção da integridade da documentação técnica serão feitas pelo titular de direito e serão fundamentais para uso futuro como prova digital, ou seja, a informação do resumo hash e a descrição do algoritmo no formulário eletrônico e-Software serão fundamentais para uma validação deste documento no judiciário. Um perito técnico poderá inequivocamente assegurar ao judiciário se houve ou não a alteração no documento, bem como a autoria do software. Para comprovar a autoria de um programa de computador

[4] Datacenter: corresponde a um local físico que armazena máquinas de computação e seus equipamentos de hardware relacionados. Ele contém a infraestrutura de computação que os sistemas de TI exigem, como servidores, unidades de armazenamento de dados e equipamentos de rede. É a instalação física que armazena os dados digitais de qualquer empresa (Amazon). Disponível em: https://aws.amazon.com/pt/what-is/data-center/ acesso em 19 maio 2025

[5] Segundo o art. 2º da Lei 8.159/1991, considera-se documento de arquivo os 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.

> (software) será necessária à apresentação do objeto protegido, como o código fonte ou partes deste código, em juízo. Sendo assim, o Certificado de Registro expedido pelo INPI conferirá segurança jurídica aos negócios do titular de direito do software. É recomendável fazer cópias de segurança em um dispositivo de armazenamento, do titular de direito, adequado para manter a longevidade do arquivo (INPI, 2017).

Foi estabelecido também que os suportes de registros dos softwares (CDs, Disquetes e Pendrives) estão sujeitos à degradação física e à obsolescência de leitura, colocando em risco a integridade do material registrado, o que exige desta instituição providências para que estes documentos não sejam perdidos ou corrompidos ao longo do tempo de guarda exigido pela legislação pertinente.

A partir desta análise, o serviço de arquivo identificou que a melhor maneira para preservação destes documentos é sua migração para os formatos digitais recomendados[6] e sua incorporação a um Repositório Arquivístico Digital Confiável (RDC-arq), ambiente de preservação a longo prazo de documentos digitais ou digitalizados, capaz de fornecer confiabilidade aos documentos formadores do acervo universitário digital.

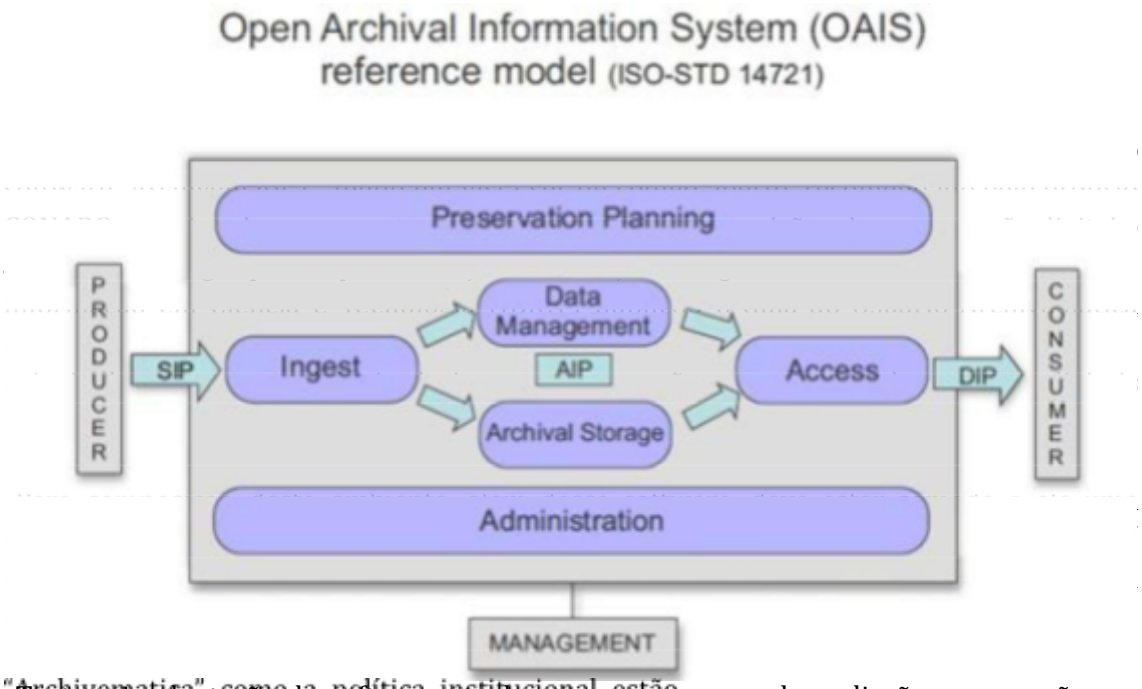
Esse apontamento se baseia na orientação técnica intitulada "Diretrizes para implementação de repositórios digitais confiáveis de documentos arquivísticos", publicada pela Resolução nº 51, de 25 de agosto de 2023, do Conselho Nacional de Arquivos (CONARQ), órgão colegiado da autoridade máxima em termos de arquivos do Poder Executivo Federal - o Arquivo Nacional.

Resumidamente, o objetivo dessa publicação é orientar as instituições / entidades / organizações na construção de ambientes que permitam o armazenamento e gerenciamento de materiais digitais, na qual se captura, armazena, preserva, e acessa objetos arquivísticos digitais.

Esta orientação é decorrente da norma ABNT NBR 15472:2007 "Sistema Aberto de Arquivamento de Informação – SAAI", que por sua vez é a tradução da recomendação internacional ISO 14721/2003, que estabelece o modelo conceitual para definição de um Repositório Digital, identificando o ambiente, os componentes funcionais, suas interfaces internas e externas, e os objetos de dados e informações.

Esse modelo, denominado OAIS (Open Archival Information System), objetiva preparar a instituição para preservar e tornar as informações digitais acessíveis, buscando abordar questões relativas à preservação de longo prazo, independentemente da área de aplicação - documentos de arquivos; documentos de bibliotecas, documentos de museus etc. conforme figura abaixo:

[6] E-ping: define um conjunto mínimo de premissas, políticas e especificações técnicas na TIC na interoperabilidade de serviços do governo eletrônico. Disponível em: https://eping.governoeletronico.gov.br/#apresentacao acesso em 19 maio 2025



"Archivematica", como a política institucional estão

Tanto a implantação do software atualmente, em processo de avaliação e aprovação nas instâncias competentes desta universidade, tendo como peso político institucional as três unidades envolvidas na problemática e cientes de que a construção desse ambiente é fundamental para garantir a preservação e acesso seguro da propriedade intelectual desta universidade.

Conclusão

O registro de programas de computador no INPI é, por si só, um avanço na proteção da propriedade intelectual desenvolvida nas universidades e ICTs. Contudo, ao assumir a

guarda de longo prazo do código-fonte, estas instituições se deparam com o paradoxo silencioso de ter que cumprir a exigência legal de preservação pelo prazo estabelecido na legislação não tendo orientações sobre como realizar tal tarefa, visto que os suportes físicos e sistemas de leitura que geralmente são utilizados evoluem constantemente ou desaparecem em ciclos de vida cada vez mais curtos.

A experiência da Universidade Federal de Uberlândia mostra que essa não é uma questão puramente teórica, visto que o trabalho conjunto entre a Diretoria de Inovação e Transferência de Tecnologia (DIRTC) e a Divisão de Documentação (DIDOC) tem enfrentado o desafio real de identificar, migrar e preservar acessíveis estes softwares, tendo assim a necessidade de criar diretrizes institucionais e práticas seguras de

[7] Cadeia de Custódia: pode ser entendida como o ambiente no qual perpassa o ciclo de vida dos documentos. Em outras palavras, ela define quem é o responsável por aplicar os princípios e as funções arquivísticas à documentação (FLORES, ROCCO e SANTOS, 2016).

preservação e acesso, as quais respeitem a privacidade e a integridade dos arquivos, e sem depender exclusivamente
de paliativos internos ou serviços de terceiros "nuvens".

O futuro aponta para abordagens híbridas, como o uso de blockchain para registro de integridade, cofres digitais criptográficos e, como apontado no caso em análise, para a estratégia do Repositório Digital Arquivístico Confiável (RDC-arq), que, até então, se mostra suficiente para responder as questões aqui levantadas.

Para além destes aspectos, este artigo buscou também incentivar que as demais ICTs brasileiras assumam, com coragem e planejamento, a missão de garantir que o conhecimento que hoje é código não se torne, amanhã, um arquivo corrompido ou um patrimônio perdido. Assim, recomenda-se que outros estudos de casos sejam realizados, visto que a construção de uma orientação nacional passará, invariavelmente, pela construção de um arcabouço de estudos e implementações de ambientes de preservação digital a longo prazo, que hoje não é, nem de longe, realidade das instituições brasileiras.

Agradecimentos

Este trabalho foi realizado com anuência e apoio da Diretoria de Inovação e Transferência de Tecnologia (DIRTC) e da Divisão de Documentação (DIDOC) da Universidade Federal de Uberlândia, às quais os autores deste artigo agradecem a pronta liberação dos dados necessários a escrita do artigo. Registramos também um agradecimento especial pelo apoio recebido da FAPEMIG Fundação de Amparo à Pesquisa do Estado de Minas Gerais.

Referências

ARQUIVO NACIONAL. Conselho Nacional de Arquivos (CONARQ). Resolução nº 51, de 25 de agosto de 2023. Rio de Janeiro, 2023. Disponível em: https://www.gov.br/conarq/ptbr/legislacao-arquivistica/resolucoes-do-conarq/resolucao-conarq-no-51-de-25-deagosto-de-2023 acesso: 20 maio 2025

BRASIL. Presidência da República. Lei nº 9.609, de 19 de fevereiro de 1998. Dispõe sobre a proteção da propriedade intelectual de programa de computador. Diário Oficial da União: seção 1, Brasília, DF, 20 fev. 1998.

BORGMAN, C. L. (2007). Digital libraries and the continuum of scholarly communication. Journal of the American Society for Information Science and Technology, 58(6), 885-896. https://doi.org/10.1002/asi.20664

FLORES, D. BRITO ROCCO, B. C. SANTOS, H. M. Cadeia de custódia para documentos arquivísticos digitais. Acervo. Rio de Janeiro. V. 29, N. 2, P. 117 132, Jul Dez, 2016.

MINISTÉRIO DA ECONOMIA, Instituto Nacional de Propriedade Intelectual (INPI). Manual do Usuário Para Registro Eletrônico de Programas de Computador. Rio de Janeiro, v. 1.6.8,

p. 2 50, 2022. Disponível em: https://www.gov.br/inpi/pt-br/servicos/programas-decomputador/arquivos/manual/manual-e-software-2022.pdf acesso em 20 maio 2025

MINISTÉRIO DA ECONOMIA, Instituto Nacional de Propriedade Intelectual (INPI). E-RPC - Registro Eletrônico de Programa de Computador. Rio de Janeiro, 2017. Disponível em: https://www.gov.br/inpi/pt-br/assuntos/arquivos-programa-decomputador/ApresentaoeSoftware.pdf acesso em: 20 maio 2025

MINISTÉRIO DE CIÊNCIA, TECNOLOGIA E INOVAÇÃO. Instituto Brasileiro de Informação em Ciência e Tecnologia (IBICT). Guia do Usuário Archivematica. Brasília, 136 f. 2016. Disponível em: http://livroaberto.ibict.br/bitstream/123456789/1063/4/ManualArchivematica.pdf acesso em 20 maio 2025

ROSENBERG, M. Digital preservation: A critical issue in the electronic age. 2001, Library Trends, 49(4), 626-638.

SOFTWARE HERITAGE FOUNDATION. Software preservation for software citation. Software Heritage Foundation, 2018. Disponível em: https://www.softwareheritage.org/2018/06/25/software-preservation-for-softwarecitation/ acesso em 12 maio 2025

SOFTWARE PRESERVATION NETWORK. Software Preservation and Emulation Symposium - Stanford University. Software Preservation Network, 2018. Disponível em: https://docs.softwareheritage.org/ acesso em 12 maio 2025