



UNIVERSIDADE FEDERAL DO RIO DE JANEIRO – UFRJ
ESCOLA DE COMUNICAÇÃO – ECO
INSTITUTO BRASILEIRO DE INFORMAÇÃO EM CIÊNCIA E TECNOLOGIA – IBICT
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA INFORMAÇÃO – PPGCI

As instituições estão prontas para receber um Repositório Arquivístico Digital Confiável (RDC-Arq)? Mapeamento das atividades que antecedem a implementação.

Dissertação de Mestrado

Março de 2025



Tiago de Araujo Cardoso

As instituições estão prontas para receber um Repositório Arquivístico Digital Confiável (RDC-Arq)? Mapeamento das atividades que antecedem a implementação.

Dissertação de mestrado apresentada ao Programa de Pós-Graduação em Ciência da Informação do convênio entre o Instituto Brasileiro de Informação em Ciência e Tecnologia (Ibict) e a Escola de Comunicação da Universidade Federal do Rio de Janeiro (Eco-UFRJ), como requisito parcial à obtenção do título de mestre em Ciência da Informação.

Orientador: Prof. Dr. Tiago Emmanuel Nunes Braga.

Rio de Janeiro

2025

CIP - Catalogação na Publicação

551i de Araujo Cardoso, Tiago
As instituições estão prontas para receber um Repositório Arquivístico Digital Confiável (RDC-Arq)? Mapeamento das atividades que antecedem a implementação. / Tiago de Araujo Cardoso. -- Rio de Janeiro, 2025.
100 f.
Orientadora: Tiago Emmanuel Nunes Braga.
Dissertação (mestrado) - Universidade Federal do Rio de Janeiro, Escola da Comunicação, Instituto Brasileiro de Informação em Ciência e Tecnologia, Programa de Pós-Graduação em Ciência da Informação, 2025.
1. Repositório Arquivístico Digital Confiável.. 2. Preservação Digital. . 3. Autenticidade de Documentos Arquivísticos. . 4. Integridade. . 5. Acessibilidade e Interoperabilidade. . I. Nunes Braga, Tiago Emmanuel , orient. II. Título.

TIAGO DE ARAUJO CARDOSO

**As instituições estão prontas para receber um Repositório Arquivístico Digital
Confiável (RDC-Arq)? Mapeamento das atividades que antecedem a
implementação**

Dissertação de mestrado apresentada ao Programa de Pós-Graduação em Ciência da Informação do convênio entre o Instituto Brasileiro de Informação em Ciência e Tecnologia (Ibict) e a Escola de Comunicação da Universidade Federal do Rio de Janeiro (Eco-UFRJ), como requisito parcial à obtenção do título de mestre em Ciência da Informação.

Rio de Janeiro, 10/03/2025

TIAGO EMMANUEL NUNES BRAGA:04481447605 Assinado de forma digital por TIAGO
EMMANUEL NUNES BRAGA:04481447605
Dados: 2025.04.04 09:41:51 -03'00'

Prof. Dr. Tiago Emmanuel Nunes Braga (Orientador) IBICT

Documento assinado digitalmente
 **FABIO CASTRO GOUVEIA**
Data: 08/04/2025 17:10:16-0300
Verifique em <https://validar.iti.gov.br>

Prof. Dr. Fabio Castro Gouveia (Membro interno) IBICT/Eco-UFRJ

Documento assinado digitalmente
 **BRENDA COUTO DE BRITO ROCCO**
Data: 08/04/2025 17:35:28-0300
Verifique em <https://validar.iti.gov.br>

Prof^ª. Dr^a Brenda Couto de Brito Rocco (Membro externo) DEPA/UFRJ

Pessoas livre de limitações, entusiasmadas e inspiradas por fazer mais têm capacidade absolutamente infinita de melhorar.

(Jack Welch).

AGRADECIMENTOS

Em primeiro lugar, agradeço a Deus, fonte de toda sabedoria e força, por me guiar em cada etapa desta jornada, iluminando meu caminho mesmo nos momentos mais desafiados

Aos meus pais, Solon e Maria, meu eterno reconhecimento pelo amor incondicional, pelos valores que me ensinaram e pelo exemplo de dedicação e persevera

À minha esposa Thais, companheira incansável, agradeço pelo apoio, paciência e incentivo em todos os momentos. Sua presença foi fundamental para que eu pudesse chegar até aqui

Ao meu filho Benício, razão do meu sorriso e da minha motivação diária, dedico este trabalho com todo o meu amor, na esperança de que ele inspire sua própria trajetória de conquistas.

Agradeço imensamente ao Prof. Dr. Tiago Emmanuel Nunes Braga, meu orientador e Diretor do IBICT, pelo apoio, dedicação e orientação ao longo do desenvolvimento desta dissertação. Sua expertise, paciência e incentivo foram fundamentais para a construção deste trabalho. Sou grato pelas valiosas discussões, pelos direcionamentos precisos e pelo compromisso com a excelência acadêmica, que me inspiraram a aprimorar cada etapa do estudo.

Meu sincero reconhecimento também ao IBICT, pela estrutura, suporte oferecido e pelas portas sempre abertas para me receber, fatos que contribuíram significativamente para a realização desta pesquisa.

Força, fé e foco!
(Tiago Cardoso).

RESUMO

Este trabalho abordou a implementação de Repositórios Digitais Confiáveis (RDC-Arq) no Brasil, com foco nas condições organizacionais e técnicas necessárias para a criação e gestão desses sistemas. O objetivo principal foi investigar as práticas atuais e os desafios enfrentados pelas instituições brasileiras na implementação do RDC-Arq, analisando questões como o mapeamento de setores envolvidos, a alocação de recursos financeiros e humanos, a infraestrutura tecnológica e a digitalização de arquivos físicos. A metodologia adotada foi qualitativa, utilizando análise documental e estudos de caso de instituições que já implementaram ou estão em processo de implementação do RDC-Arq. A pesquisa também incluiu consulta e validação de propostas com profissionais envolvidos na implementação de modelos de preservação digital. Os resultados revelaram que, embora muitas instituições já tenham identificado a necessidade de implementar o RDC-Arq e alocado recursos humanos para o projeto, a falta de orçamento específico e a infraestrutura tecnológica insuficiente são obstáculos significativos. A digitalização de documentos físicos ainda representa um desafio importante para muitas instituições. A conclusão do estudo aponta para a necessidade de maior planejamento estratégico, alocação adequada de recursos e melhorias na integração tecnológica para garantir a efetividade e sustentabilidade do RDC-Arq. A pesquisa contribui para a compreensão dos desafios enfrentados pelas instituições brasileiras e oferece diretrizes para a implementação bem-sucedida de repositórios digitais confiáveis.

Palavras-chave: repositórios digitais, preservação digital, RDC-Arq, infraestrutura tecnológica, digitalização.

ABSTRACT

This study addressed the implementation of Reliable Digital Repositories (RDC-Arq) in Brazil, focusing on the organizational and technical conditions required for the creation and management of these systems. The main objective was to investigate current practices and challenges faced by Brazilian institutions in implementing RDC-Arq, analyzing issues such as mapping the sectors involved, allocation of financial and human resources, technological infrastructure, and digitization of physical archives. The methodology adopted was qualitative, using documentary analysis and case studies of institutions that have already implemented or are in the process of implementing RDC-Arq. The research also included interviews with professionals involved in the implementation of digital preservation models. The results revealed that, although many institutions have already identified the need to implement RDC-Arq and allocated human resources to the project, the lack of specific budget and insufficient technological infrastructure are significant obstacles. Digitization of physical documents still represents a significant challenge for many institutions. The conclusion of the study points to the need for greater strategic planning, adequate allocation of resources, and improvements in technological integration to ensure the effectiveness and sustainability of RDC-Arq. The research contributes to the understanding of the challenges faced by Brazilian institutions and offers guidelines for the successful implementation of reliable digital repositories.

Keywords: digital repositories, digital preservation, RDC-Arq, technological infrastructure, digitalization.

LISTA DE ILUSTRAÇÕES

Figura 1 – Interseção entre Repositório Arquivístico Digital, Repositório Digital Confiável e Repositório Digital.....	24
Figura 2 – Ciclo de Vida dos Documentos Arquivísticos Digitais e Cadeia de Custódia Digital Arquivística.....	36

LISTA DE SIGLAS

ONU - Organização das Nações Unidas
OMS - Organização Mundial da Saúde
CNPJ - Cadastro Nacional da Pessoa Jurídica
CPF - Cadastro de Pessoas Físicas
DNA - Ácido Desoxirribonucleico
RNA - Ácido Ribonucleico
ECG - Eletrocardiograma
MRI - Ressonância Magnética
AVC - Acidente Vascular Cerebral
HIV - Vírus da Imunodeficiência Humana
CPU - Unidade Central de Processamento
RAM - Memória de Acesso Aleatório
HTML - Linguagem de Marcação de Hipertexto
URL - Localizador Uniforme de Recursos
Hz - Hertz
m/s - Metro por Segundo
Hz - Hertz
PDF - Formato de Documento Portátil
USB - Barramento Serial Universal
GPS - Sistema de Posicionamento Global
Wi-Fi - Wireless Fidelity
IP - Protocolo de Internet
IT - Tecnologia da Informação
RPG - Jogo de Interpretação de Papéis
NGO - Organização Não Governamental
GPS - Sistema de Posicionamento Global
AI - Inteligência Artificial
API - Interface de Programação de Aplicações
SaaS - Software como Serviço
BI - Inteligência de Negócios
SEO - Otimização para Motores de Busca (Search Engine Optimization)
TIC - Tecnologias da Informação e Comunicação

SUMÁRIO

1 APRESENTAÇÃO DO TEMA.....	9
2 JUSTIFICATIVA.....	13
3 OBJETIVOS.....	16
3.1 OBJETIVO GERAL.....	16
3.2 OBJETIVOS ESPECÍFICOS.....	16
4 REFERENCIAL TEÓRICO.....	17
4.1 CONCEITO DE RDC-ARQ.....	17
4.2 DEMANDA SOCIAL PARA IMPLEMENTAÇÃO DE RDC-ARQ.....	18
4.2.1 EXPERIÊNCIA DE ADOÇÃO DE RDC-ARQ.....	20
4.3 PRESERVAÇÃO DIGITAL.....	21
4.4 AUTENTICIDADE DOS DOCUMENTOS ARQUIVÍSTICOS NO RDC-ARQ.....	23
4.5 INTEGRIDADE E SEGURANÇA DA INFORMAÇÃO NO RDC-ARQ.....	30
4.6 ACESSIBILIDADE E INTEROPERABILIDADE DOS DOCUMENTOS NO RDC-ARQ.....	36
4.7 COORDENAÇÃO DE DOCUMENTOS DIGITAIS VISANDO ENVIO PARA UM RDC-Arq.....	42
4.8 LGPD E SUAS CARACTERÍSTICAS.....	43
4.9 PRESERVAÇÃO DIGITAL A LONGO PRAZO.....	46
4.10 NORMAS E CERTIFICAÇÕES PARA O RDC-ARQ.....	52
4.11 DOCUMENTAÇÃO E REGISTRO DE PROCESSOS.....	57
5 METODOLOGIA.....	63
6 RESULTADOS E DISCUSSÃO.....	65
6.1 REQUISITOS OPERACIONAIS.....	65
6.2 REQUISITOS ARQUIVÍSTICOS.....	66
6.3 OBRIGATORIEDADES DE IMPLEMENTAÇÃO.....	66
7 CONCLUSÃO.....	76
REFERÊNCIAS.....	79
APÊNDICE A.....	82
FORMULÁRIO PARA MAPEAMENTO DE REQUISITOS QUE ANTECEDEM A IMPLEMENTAÇÃO DE UM RDC-ARQ.....	82

1 APRESENTAÇÃO DO TEMA

O avanço das tecnologias digitais e o aumento exponencial da produção de dados têm imposto novos desafios para a preservação documental, exigindo o desenvolvimento de métodos eficazes para garantir a integridade, autenticidade e acessibilidade de documentos ao longo do tempo. A necessidade de manter registros digitais confiáveis e acessíveis para futuras gerações transcende questões técnicas, impactando diretamente setores estratégicos, como o governo, a saúde, a educação e o setor jurídico. Nesse contexto, o conceito de Repositório Arquivístico Digital Confiável (RDC-Arq) emergiu como uma solução essencial para enfrentar as particularidades e demandas dessa era digital.

Em meio à crescente dependência de registros digitais, muitas organizações enfrentam dificuldades para preservar adequadamente seus documentos, que podem facilmente se perder, sofrer adulterações ou se tornar inacessíveis devido a falhas tecnológicas e à obsolescência de formatos. Segundo Gava e Flores (2020), o RDC-Arq propõe uma estrutura normativa e técnica que visa criar condições de preservação digital a longo prazo, garantindo que os documentos arquivísticos sejam confiáveis e permaneçam disponíveis, sem comprometimentos de sua autenticidade ou integridade. A implementação do RDC-Arq, dessa forma, apresenta-se como uma necessidade para todas as instituições que gerenciam documentos digitais, especialmente em setores onde autenticidade e a transparência são fundamentais.

A preservação de documentos digitais apresenta desafios únicos, uma vez que esses registros não possuem as mesmas características físicas dos documentos analógicos e dependem inteiramente de sistemas tecnológicos para serem acessados e interpretados. Diferente de um documento impresso, que pode ser armazenado e consultado sem recursos tecnológicos específicos, um documento digital requer uma infraestrutura técnica para garantir sua continuidade e acessibilidade. Andrade e Chagas (2021) destacam que o RDC-Arq atua como um modelo de gestão capaz de lidar com essa fragilidade, proporcionando um ambiente seguro onde os documentos podem ser preservados em conformidade com diretrizes e normas de preservação digital reconhecidas internacionalmente.

Além de atender a uma demanda técnica, a criação de repositórios digitais confiáveis responde a uma demanda social e jurídica cada vez mais evidente. A crescente digitalização de processos judiciais, administrativos e educacionais, por exemplo, faz com que os documentos digitais assumam um papel de prova e evidência que antes era ocupado pelos documentos físicos. A Lei nº 12.527/2011 estabelece diretrizes para garantir o acesso à

informação pública no Brasil, assim como a General Data Protection Regulation (GDPR) na União Europeia, estabeleceram que cidadãos têm o direito de acessar informações confiáveis e de conhecer os registros arquivísticos mantidos por instituições públicas. Nesse sentido, o RDC-Arq não apenas facilita o cumprimento de obrigações legais, mas também promove a transparência e a confiança na gestão pública e privada, pois assegura que os registros digitais sejam mantidos de forma íntegra e autêntica.

O conceito de repositório digital confiável envolve a adoção de práticas de preservação digital baseadas em normas e certificações internacionais. A ISO 16363, por exemplo, fornece diretrizes para a auditoria e certificação de repositórios digitais confiáveis, estipulando critérios que orientam a preservação de documentos arquivísticos digitais. Flores (2021) enfatiza que a adoção dessas normas garante que os repositórios digitais possam ser auditados e monitorados, permitindo uma preservação transparente e segura dos documentos arquivísticos. Além disso, o RDC-Arq, ao se basear em normas amplamente reconhecidas, permite a integração e a interoperabilidade entre diferentes sistemas e plataformas, facilitando o intercâmbio e o compartilhamento de documentos arquivísticos entre instituições.

A implementação de um RDC-Arq apresenta benefícios significativos para instituições e para a sociedade em geral. Em setores como o judicial e o governamental, por exemplo, a autenticidade de documentos digitais é fundamental para a tomada de decisões e para a prestação de contas à sociedade. A adoção de práticas e políticas que assegurem a preservação de documentos arquivísticos digitais evita problemas jurídicos e administrativos decorrentes da perda de dados ou da adulteração de informações. Como discutido por Braga *et al.* (2022), a adoção de um RDC-Arq é uma medida estratégica para fortalecer a governança documental e para assegurar que os documentos digitais sejam preservados em conformidade com os requisitos legais e éticos de cada setor.

A complexidade envolvida na criação e manutenção de um RDC-Arq demanda uma estrutura organizacional que integre recursos humanos e tecnológicos. A preservação digital confiável exige conhecimentos específicos, que vão desde a gestão de documentos até a cibersegurança. Andrade e Chagas (2023) sugerem que a implementação de um RDC-Arq requer o treinamento e a capacitação de profissionais, que devem ser capazes de lidar com as particularidades dos documentos digitais e com os desafios específicos da preservação digital a longo prazo. A presença de uma equipe capacitada é essencial para garantir que os processos de preservação sejam realizados de forma eficiente e que o repositório funcione em conformidade com as normas de preservação digital.

O RDC-Arq também precisa de uma infraestrutura tecnológica adequada para assegurar a integridade, autenticidade e acessibilidade dos documentos ao longo do tempo. Conforme Gava e Flores (2021), a infraestrutura de um repositório digital confiável deve incluir sistemas de backup, redundância de dados e controles de acesso rigorosos. Esses elementos não apenas evitam a perda de dados, mas também garantem que os documentos arquivísticos digitais sejam preservados em conformidade com os requisitos de segurança e acessibilidade. A criação de um RDC-Arq implica, portanto, em um investimento em tecnologia e em um planejamento cuidadoso para que o repositório digital atenda às demandas de preservação e aos requisitos arquivísticos.

O desenvolvimento de um RDC-Arq está alinhado com as demandas sociais e tecnológicas contemporâneas, respondendo ao desafio de assegurar a autenticidade dos documentos arquivísticos digitais. A transformação digital tem impulsionado a criação de registros eletrônicos, e o RDC-Arq surge como um mecanismo essencial para preservar esses registros e garantir que eles continuem acessíveis e autênticos ao longo do tempo. Santos e Flores (2020) ressaltam que a preservação digital confiável não é apenas uma questão técnica, mas também um compromisso com a preservação da memória institucional e com a transparência das ações governamentais e corporativas. O RDC-Arq, nesse sentido, contribui para a construção de uma cultura de preservação digital que prioriza a integridade e autenticidade dos registros arquivísticos.

A ausência de um repositório digital confiável pode comprometer a segurança e a acessibilidade dos documentos digitais, gerando problemas significativos para as instituições que dependem desses registros. Em um cenário onde a perda ou a adulteração de documentos pode gerar consequências legais e financeiras, o RDC-Arq se apresenta como uma solução que mitiga riscos e promove a continuidade e a segurança da informação. Faria e Silva (2023) destacam que o investimento em um repositório digital confiável é uma medida preventiva que evita custos futuros decorrentes de falhas na preservação e de possíveis prejuízos causados pela perda de documentos essenciais.

O Conselho Nacional de Arquivos (CONARQ), por meio da Resolução CONARQ nº 51, definiu os requisitos para a implementação do Repositório Arquivístico Digital Confiável (RDC-Arq). Essa normativa tem como objetivo garantir a preservação, a proteção, a integridade e a acessibilidade dos documentos arquivísticos digitais ao longo do tempo. O RDC-Arq é fundamental para a gestão documental em ambientes digitais, garantindo que informações essenciais sejam mantidas de forma segura e confiável, independentemente das mudanças tecnológicas.

Entre os requisitos definidos pela Resolução, destacam-se a necessidade de mecanismos de segurança da informação, controle de acesso, gestão de metadados, preservação digital ativa e auditabilidade dos processos. Além disso, a normativa enfatiza a importância de políticas institucionais claras para a gestão de documentos digitais, o uso de formatos de arquivo padronizados e sustentáveis, bem como a adoção de procedimentos de backup e recuperação de dados. Esses visam não apenas proteger o conteúdo digital, mas também garantir seus requisitos de autenticidade e usabilidade ao longo do tempo.

A Resolução CONARQ nº 51 estabelece os requisitos essenciais para a implementação bem-sucedida de um Repositório Digital Confiável para Arquivos (RDC-Arq) , definindo critérios técnicos e funcionais que visam garantir a preservação, a proteção, a integridade e o acesso contínuo aos documentos digitais ao longo do tempo. Entre esses requisitos, destacam-se aspectos como segurança da informação, gestão de metadados, controle de acesso, preservação digital ativa e auditabilidade dos processos, fundamentais para a autenticidade de documentos em um repositório.

No entanto, a Resolução não aborda de forma detalhada as orientações institucionais prévias necessárias antes do início do processo de implementação do RDC-Arq. Questões estratégicas, como a definição de políticas de gestão documental, a capacitação de equipes técnicas, a avaliação da infraestrutura tecnológica existente e o engajamento da alta administração são fundamentais para criar um ambiente propício à adoção do repositório, mas não estão contempladas nos requisitos normativos. Esses aspectos de pré-implementação são cruciais para o sucesso da RDC-Arq, pois garantem que uma organização esteja estruturada e alinhada para enfrentar os desafios tecnológicos, administrativos e culturais envolvidos no processo.

Sendo assim, é sistematizado o seguinte problema de pesquisa: Antes da implementação de um RDC-Arq, é essencial observar diversas etapas que garantam a efetividade, segurança e conformidade do sistema. Quais são as principais etapas que devem ser seguidas pelas instituições antes de se iniciar a implementação de um RDC-Arq?

2 JUSTIFICATIVA

A implementação de um RDC-Arq é justificada pela necessidade de preservar documentos arquivísticos digitais de forma que sua autenticidade e integridade sejam asseguradas em longo prazo. Em um contexto de produção contínua de registros eletrônicos, a preservação digital confiável torna-se uma prática essencial para todas as instituições que gerenciam documentos digitais com valor histórico, jurídico ou administrativo. Como apontam Santos e Flores (2020), a preservação digital é um compromisso com a memória institucional e com a transparência, uma vez que garante que os registros arquivísticos digitais possam ser acessados e validados em qualquer momento.

A justificativa para a criação de RDC-Arq também se fundamenta na necessidade de cumprir requisitos legais e regulamentares. No Brasil, a Lei de Acesso à Informação (Lei nº 12.527/20) e a Lei Geral de Proteção de Dados (Lei nº 13.709/2018) exigem que documentos arquivísticos digitais sejam preservados e disponibilizados de forma segura e confiável. Gava e Flores (2021) destacam que o RDC-Arq permite que as instituições atendam a essas exigências, oferecendo uma estrutura confiável para a preservação digital de documentos. Dessa forma, o RDC-Arq se apresenta como uma solução que atende tanto às demandas de transparência e accountability quanto às obrigações legais das instituições.

O RDC-Arq também é justificado pela necessidade de garantir que os documentos arquivísticos digitais não sejam afetados pela obsolescência tecnológica. Em um ambiente onde as tecnologias evoluem rapidamente, muitos documentos digitais correm o risco de se tornarem inacessíveis, caso não sejam preservados de forma adequada. Andrade e Chagas (2021) observam que a implementação de um RDC-Arq é uma medida preventiva contra a obsolescência, uma vez que permite que os documentos arquivísticos digitais sejam preservados de maneira independente das tecnologias originais de criação e armazenamento. Essa independência tecnológica é essencial para garantir a continuidade da informação e para evitar a perda de documentos importantes.

A justificativa para o RDC-Arq também inclui a segurança da informação, uma vez que a preservação digital confiável reduz os riscos associados à perda e adulteração de documentos digitais. Como discutem Santos e Mazuco (2020), a segurança da informação é um requisito fundamental para a preservação digital, e o RDC-Arq oferece uma estrutura que protege os documentos arquivísticos digitais contra acessos não autorizados e contra falhas que possam comprometer sua integridade. A implementação de um RDC-Arq, nesse sentido, é uma medida estratégica que promove a continuidade e a autenticidade dos documentos

digitais, assegurando que eles sejam preservados em conformidade com os padrões de segurança.

Finalmente, o RDC-Arq é justificado pelo valor histórico e cultural dos documentos arquivísticos digitais. Muitos registros arquivísticos possuem um valor documental que vai além de seu uso administrativo ou jurídico, contribuindo para a construção da memória coletiva e para a preservação da história institucional. Chaves (2023) destaca que a preservação de documentos arquivísticos digitais é uma forma de preservar o patrimônio cultural, garantindo que futuras gerações possam acessar informações sobre o passado e compreender a evolução das instituições. A implementação de um RDC-Arq, assim, atende à necessidade de preservar documentos de valor histórico, assegurando que esses registros continuem acessíveis e íntegros.

Tendo em vista a obrigatoriedade do RDC-Arq e a complexidade dos sistemas informacionais de gestão documental, é natural que surjam dificuldades institucionais no processo de sua implementação. A integração entre diferentes sistemas, a adequação de processos preexistentes e a necessidade de garantir a segurança e a autenticidade dos documentos digitais representam desafios significativos para as organizações.

O próprio Conselho Nacional de Arquivos (CONARQ) reconhece essa complexidade ao prever a atuação conjunta de dois grupos de atores essenciais: aqueles responsáveis pela gestão documental e aqueles responsáveis pela gestão dos ativos tecnológicos. Enquanto o primeiro grupo assegura a aplicação das diretrizes arquivísticas e a conformidade com as normativas de preservação digital, o segundo é fundamental para garantir a infraestrutura tecnológica necessária ao funcionamento do RDC-Arq, incluindo aspectos relacionados à segurança da informação, interoperabilidade e manutenção dos sistemas.

Todavia, para que o processo de implementação do RDC-Arq seja eficaz e sustentável, é indispensável o envolvimento ativo da alta administração das instituições. O apoio da alta gestão não se limita ao fornecimento de recursos financeiros e humanos; trata-se de uma participação estratégica, que inclui o patrocínio institucional do projeto, a definição de prioridades, a articulação entre diferentes áreas e o estímulo a uma cultura organizacional orientada à preservação digital. O engajamento da alta administração também é fundamental para superar resistências internas, promover a conscientização sobre a importância do RDC-Arq e garantir que a gestão documental e tecnológica esteja alinhada aos objetivos institucionais de longo prazo.

Assim, a implementação do RDC-Arq deve ser vista como um esforço multidisciplinar e intersetorial, que demanda não apenas competências técnicas, mas também liderança,

comprometimento institucional e uma visão estratégica que considere a preservação digital como um ativo fundamental para a governança da informação no setor público e privado.

A pesquisa propõe-se a identificar os passos preparatórios essenciais para a implementação de um RDC-Arq, considerando tanto os desafios institucionais quanto as exigências técnicas e normativas. Ao mapear as etapas críticas do processo, bem como os papéis e responsabilidades dos diferentes atores envolvidos — desde a gestão documental e tecnológica até o engajamento da alta administração —, a pesquisa visa oferecer um roteiro estruturado que auxilie as instituições a superar barreiras comuns, como a falta de alinhamento entre áreas, a escassez de recursos ou a resistência a mudanças. Com isso, espera-se que as organizações possam avançar de forma mais rápida e eficiente na implementação do RDC-Arq, reduzindo o retrabalho, otimizando a alocação de recursos e promovendo uma maior maturidade na gestão da informação digital. Além disso, os resultados da pesquisa poderão subsidiar a formulação de políticas institucionais e estratégias de capacitação, fortalecendo a governança da preservação digital em diferentes contextos organizacionais.

3 OBJETIVOS

3.1 OBJETIVO GERAL

O propósito central desta pesquisa é identificar e analisar detalhadamente as fases preliminares à implementação de um RDC-Arq.. Esse mapeamento busca estabelecer diretrizes e boas práticas que contribuam para a efetividade do processo, assegurando a preservação digital de documentos arquivísticos de maneira segura, autêntica ao longo do tempo.

3.2 OBJETIVOS ESPECÍFICOS

- ☐ Avaliar os normativos relacionados à implementação de RDC-Arq;
- ☐ Mapear os aspectos preparatórios que poderão contribuir para o sucesso de implementação de um RDC-Arq;
- ☐ Preparar instrumento de avaliação das preparações preliminares necessárias às instituições que almejam implementar um RDC-Arq.

4 REFERENCIAL TEÓRICO

4.1 CONCEITO DE RDC-ARQ

O conceito de RDC-Arq é fundamentado na necessidade de preservar documentos arquivísticos digitais de forma que sua autenticidade, integridade e acessibilidade sejam mantidas ao longo do tempo. A proposta do RDC-Arq vai além do simples armazenamento de arquivos digitais; ela visa criar uma estrutura confiável, baseada em normas internacionais, que permita que os documentos arquivísticos possam ser acessados e utilizados futuramente sem que haja questionamentos quanto à sua veracidade. Braga *et al.* (2022) descrevem o RDC-Arq como um repositório que cumpre critérios rigorosos de preservação digital, alinhados com padrões estabelecidos pela ISO 16363, que orienta a certificação e auditoria de repositórios digitais confiáveis.

O RDC-Arq se diferencia de outros modelos de repositórios digitais pela ênfase na preservação da autenticidade e integridade dos documentos arquivísticos. Diferente de um sistema de backup ou de um simples banco de dados, o RDC-Arq incorpora práticas e políticas que garantem que os documentos não sejam alterados ao longo do tempo e que sua origem e contexto sejam preservados. Andrade e Chagas (2021) apontam que um dos principais objetivos do RDC-Arq é assegurar que os documentos arquivísticos possam ser verificados em qualquer momento, fornecendo evidências que comprovem sua autenticidade e integridade.

A implementação de um RDC-Arq envolve a criação de uma infraestrutura tecnológica e organizacional robusta, capaz de suportar os requisitos específicos de preservação digital de documentos arquivísticos. Segundo Gava e Flores (2020), essa infraestrutura inclui sistemas de segurança da informação, mecanismos de controle de acesso e processos de auditoria que garantem que os documentos arquivísticos sejam protegidos contra acessos não autorizados e contra falhas de integridade. A combinação desses elementos permite que o RDC-Arq ofereça um ambiente seguro e confiável para a preservação de documentos arquivísticos digitais, assegurando que as informações permaneçam disponíveis e verificáveis ao longo do tempo.

O conceito de RDC-Arq também abrange aspectos de governança e gestão documental, uma vez que a preservação digital de documentos arquivísticos exige um conjunto de políticas e procedimentos que assegurem que os documentos sejam tratados conforme suas características e necessidades específicas. Santos e Flores (2022) ressaltam que a

implementação de um RDC-Arq requer uma abordagem holística, que integre práticas de gestão documental com tecnologias de preservação digital, promovendo a continuidade da informação em longo prazo. Essa integração entre gestão e tecnologia é essencial para que o RDC-Arq possa cumprir seu papel de preservar documentos arquivísticos de forma confiável.

A criação de um RDC-Arq também exige o envolvimento de profissionais capacitados, que possam administrar o repositório digital e lidar com os desafios específicos da preservação digital. Segundo Andrade e Chagas (2023), a implementação de um RDC-Arq não se limita à instalação de uma infraestrutura tecnológica; ela envolve o desenvolvimento de uma cultura institucional voltada para a preservação digital e a capacitação de profissionais que compreendam a importância dos documentos arquivísticos e saibam aplicar as melhores práticas de preservação. A presença de uma equipe qualificada é um fator determinante para o sucesso de um RDC-Arq, pois garante que o repositório seja gerenciado de forma eficiente e em conformidade com as normas de preservação digital.

4.2 DEMANDA SOCIAL PARA IMPLEMENTAÇÃO DE RDC-ARQ

A demanda social para a implementação de repositórios digitais confiáveis tem se intensificado nos últimos anos, especialmente devido ao crescimento da produção de registros eletrônicos em ambientes institucionais. O movimento em prol da transparência e da accountability tem impulsionado a necessidade de que documentos arquivísticos digitais sejam preservados de maneira confiável, garantindo que o acesso a informações públicas e privadas seja mantido de forma segura e verificável. Como observam Braga, Holanda e Pignataro (2022), a implementação de RDC-Arq atende a uma demanda social essencial, que busca garantir a preservação dos registros arquivísticos digitais para fins de consulta e auditoria.

A legislação relacionada ao acesso à informação e à proteção de dados pessoais também contribui para a crescente demanda pela criação de RDC-Arq. No Brasil, a Lei de Acesso à Informação (Lei nº 12.527/20) e a Lei Geral de Proteção de Dados (Lei nº 13.709/2018) reforçam a obrigação das instituições públicas e privadas de preservarem e disponibilizarem informações de forma segura. A criação de um RDC-Arq, nesse contexto, é uma medida que permite que as instituições cumpram com esses requisitos legais e ofereçam um serviço de preservação digital que assegure a autenticidade e integridade dos documentos arquivísticos. Gava e Flores (2021) apontam que o RDC-Arq é uma resposta adequada para as

exigências legais e sociais, garantindo que os registros arquivísticos digitais sejam preservados em conformidade com os direitos dos cidadãos.

No setor judicial, por exemplo, documentos arquivísticos digitais são frequentemente utilizados como provas, sendo essencial que esses registros sejam preservados de maneira íntegra e acessível. Santos e Mazuco (2020) discutem que, em processos judiciais, a autenticidade dos documentos é um requisito fundamental, e a implementação de um RDC-Arq é uma medida que assegura que as provas digitais possam ser aceitas e verificadas em qualquer momento, sem riscos de adulteração.

A crescente conscientização da sociedade sobre o valor da informação digital também influencia a demanda por RDC-Arq. O valor social da informação digital vem crescendo, especialmente no que se refere ao direito à memória e ao acesso à informação. Com o avanço da transformação digital, cidadãos têm se conscientizado sobre a importância de preservar registros digitais que documentem ações governamentais, decisões judiciais e outros eventos de interesse público. Como discutem Santos e Flores (2022), a sociedade percebe a necessidade de que documentos digitais não sejam apenas armazenados, mas também preservados de forma confiável para garantir que futuras gerações possam ter acesso a esses registros. Essa demanda social reflete o desejo de uma sociedade que valoriza a transparência e o acesso à informação como direitos fundamentais.

Além do setor público, o setor privado também está sujeito a pressões para adotar práticas de preservação digital confiável. Empresas que armazenam registros de clientes, contratos digitais, e-mails corporativos e outros documentos arquivísticos estão cada vez mais conscientes dos riscos associados à perda ou adulteração de dados digitais. Andrade e Chagas (2023) apontam que o RDC-Arq pode ser implementado em empresas privadas como uma medida de segurança, protegendo informações corporativas e garantindo que os documentos arquivísticos possam ser acessados e utilizados como evidências, caso necessário. Nesse sentido, a demanda social por preservação digital confiável se estende a diferentes setores, fortalecendo a implementação do RDC-Arq como uma prática padrão de preservação.

A importância do RDC-Arq também se torna evidente em contextos onde há uma alta rotatividade de tecnologias e formatos digitais. A obsolescência tecnológica é uma realidade para todas as instituições que produzem e mantêm documentos digitais, e o RDC-Arq atua como uma solução que assegura a continuidade desses registros, independentemente das mudanças tecnológicas. Como observam Chaves (2023) e Andrade e Chagas (2021), a adoção de um repositório digital confiável é uma resposta à necessidade de preservar documentos arquivísticos digitais em um ambiente de constante evolução tecnológica. Sem um RDC-Arq,

muitos documentos arquivísticos digitais poderiam se tornar inacessíveis, comprometendo a continuidade do conhecimento e da memória institucional.

A sociedade, portanto, demanda que as instituições assumam a responsabilidade pela preservação digital de documentos que possuem valor histórico, cultural e jurídico. Esse movimento reforça o papel do RDC-Arq como uma infraestrutura essencial para a preservação de documentos arquivísticos digitais em longo prazo. Santos e Flores (2020) defendem que a implementação de RDC-Arq promove a preservação de informações essenciais e contribui para a construção de uma sociedade mais transparente e comprometida com a memória e o conhecimento. A demanda social por RDC-Arq, assim, reflete o reconhecimento de que a preservação de documentos digitais é uma responsabilidade compartilhada entre as instituições e a sociedade.

4.2.1 Experiência de adoção de RDC-ARQ

Diversas instituições em diferentes partes do mundo já implementaram repositórios digitais confiáveis, oferecendo exemplos valiosos de práticas e estratégias para a preservação digital arquivística. Andrade e Chagas (2023) analisam experiências internacionais que servem como referência para a implementação de RDC-Arq, destacando o trabalho de instituições como a Library and Archives Canada e o National Archives and Records Administration (NARA) nos Estados Unidos. Essas instituições foram pioneiras na implementação de repositórios digitais confiáveis, adotando práticas de preservação que são hoje reconhecidas como referências globais em preservação digital.

No Brasil, algumas instituições têm avançado na implementação do RDC-Arq, como é o caso do Arquivo Nacional e do Tribunal de Justiça do Distrito Federal e Territórios (TJDFT). Essas instituições adotaram práticas de preservação digital baseadas em normas internacionais, como a ISO 16363, e têm investido na criação de uma infraestrutura de repositório digital confiável para preservar documentos arquivísticos digitais. Braga (2023) destaca que o modelo Hipátia, desenvolvido pelo IBICT, tem se mostrado uma alternativa viável para a implementação de RDC-Arq no Brasil, oferecendo uma estrutura que facilita a preservação e a gestão de documentos arquivísticos digitais em longo prazo.

O Projeto Hipátia, desenvolvido pelo Instituto Brasileiro de Informação em Ciência e Tecnologia (IBICT), representa uma experiência inovadora no contexto brasileiro. Esse projeto foi concebido com o objetivo de criar uma solução de preservação digital que atenda aos requisitos arquivísticos necessários para a implementação de um RDC-Arq. Segundo

Braga (2021), o modelo Hipátia oferece um conjunto de ferramentas e práticas que facilitam a preservação digital e garantem a autenticidade e a integridade dos documentos arquivísticos digitais. Esse modelo tem sido aplicado em diversas instituições, consolidando-se como uma solução eficaz para a preservação digital arquivística.

Outra experiência relevante de adoção de RDC-Arq é observada no setor judicial, especialmente com a digitalização de processos judiciais e a criação do Processo Judicial Eletrônico (PJe). O PJe foi desenvolvido com o objetivo de substituir processos físicos por documentos arquivísticos digitais, promovendo uma gestão documental mais eficiente e acessível. Pignataro *et al.* (2023) analisam o uso do Archivematica como uma ferramenta para o gerenciamento dos documentos arquivísticos digitais no PJe, apontando que essa plataforma tem sido eficaz na preservação e na organização dos documentos judiciais digitais. A experiência do PJe demonstra como o RDC-Arq pode ser adaptado para atender às necessidades específicas de diferentes setores, promovendo a autenticidade dos documentos arquivísticos digitais.

Essas experiências de adoção de RDC-Arq evidenciam que a implementação de repositórios digitais confiáveis exige planejamento e investimento em infraestrutura e capacitação. Gava e Flores (2021) ressaltam que a criação de um RDC-Arq não é um processo simples, uma vez que envolve desafios técnicos e organizacionais. As experiências internacionais e nacionais indicam que, para que um RDC-Arq seja eficaz, é necessário que as instituições adotem uma abordagem holística que inclua práticas de gestão documental, políticas de segurança da informação e estratégias de preservação digital. Essas experiências são valiosas para guiar instituições que buscam implementar RDC-Arq, oferecendo insights sobre as práticas e tecnologias que podem garantir a preservação e a acessibilidade de documentos arquivísticos digitais ao longo do tempo.

4.3 PRESERVAÇÃO DIGITAL

Atualmente, vivemos na era digital, um período recente na trajetória da humanidade, mas de impacto profundo e transformador. O fascínio pelas novas tecnologias muitas vezes desvia nossa atenção para as inúmeras possibilidades que elas oferecem. A facilidade de criar, editar, compartilhar e armazenar documentos em formato digital pode nos levar à falsa impressão de que sua preservação também é simples (Reagan, 2009).

Um dos grandes desafios é equilibrar a capacidade de produção com a preservação de preservação, já que essas duas dimensões tendem a ser inversamente proporcionais (Conway,

2001; Sayão, 2006). Grande parte da produção intelectual atual é nativa digital e, em muitos casos, armazenada sem os cuidados básicos necessários para garantir sua conservação ao longo do tempo. Termos como dark age, blank spot e amnésia digital (Brand; Sanders, 1999; Reagan, 2009; Sayão, 2006) são frequentemente usados para descrever o risco de perda da memória coletiva, representando um possível "vazio" na história da humanidade correspondente à nossa era, em razão da demora em adotar práticas práticas de preservação digital. Além da escolha das estratégias adequadas, é fundamental considerar fatores tecnológicos, organizacionais, sociais, legais e econômicos (Sayão, 2006), considerando-os um longo prazo para garantir a sustentabilidade e continuidade dos processos de preservação.

Diferentemente dos documentos analógicos, que podem sobreviver por séculos ou milênios e ainda assim serem legíveis, os documentos digitais não se mantêm acessíveis por acaso. Para os registros analógicos, a conservação do suporte físico é, muitas vezes, suficiente para proteger o conteúdo. Um exemplo disso é uma fotografia ou uma carta, que, mesmo exposta a condições ambientais desfavoráveis (como calor ou umidade), pode apresentar sinais de proteção, mas ainda assim permitir a leitura do seu conteúdo. Existem numerosos exemplos históricos que ilustram isso, como pergaminhos, tabuletas de argila, a pedra de Roseta e manuscritos medievais, que resistiram ao tempo sem cuidados especiais, preservando informações valiosas de civilizações antigas.

No ambiente analógico, é possível separar claramente as ações de preservação e de acesso. O processo de preservação pode focar tanto no conteúdo quanto no próprio objeto físico. Em alguns casos, preservar significa proteger o objeto de manipulação para garantir sua integridade, mesmo que isso limite ou proíba o acesso direto ao item.

No entanto, essa separação não existe no ambiente digital, onde a preservação e o acesso estão intrinsecamente ligados (Conway, 2001). Enquanto, no contexto analógico, o livro físico é o próprio veículo do conteúdo, no mundo digital a mídia de armazenamento não representa o documento em si. O documento digital é intangível, e preservar apenas o suporte físico (como discos rígidos ou CDs) não garante a integridade do conteúdo. Além disso, mesmo quando hardware e software são mantidos em bom estado, é impossível isolar completamente o acesso ao documento, já que sua preservação está diretamente relacionada à capacidade de acessá-lo.

O êxito de um processo de preservação digital está diretamente ligado à participação ativa tanto dos criadores dos documentos quanto daqueles responsáveis por seu armazenamento e/ou disseminação. Atualmente, diversas instituições — além de bibliotecas, arquivos e museus — assumiram o papel de guardiãs do patrimônio digital (Sayão, 2006).

Com isso, diferentes grupos vêm se dedicando a estudar, discutir e propor soluções para garantir uma preservação digital eficiente.

Embora existam várias alternativas disponíveis, ainda não se pode falar em um “conjunto de conhecimentos plenamente estabelecido” (Sayão, 2006, p. 118). Isso pode ser explicado, em parte, pelo fato de que ainda não houve tempo suficiente para avaliar de forma conclusiva a eficácia das estratégias atualmente em uso. O patrimônio digital é extremamente variado, e cada categoria de documento apresenta características e necessidades específicas.

A maioria das abordagens de preservação tem como foco principal o enfrentamento da obsolescência tecnológica, além de buscar soluções para os desafios relacionados à curta vida útil das mídias, dos hardwares e dos softwares que sustentam esses documentos.

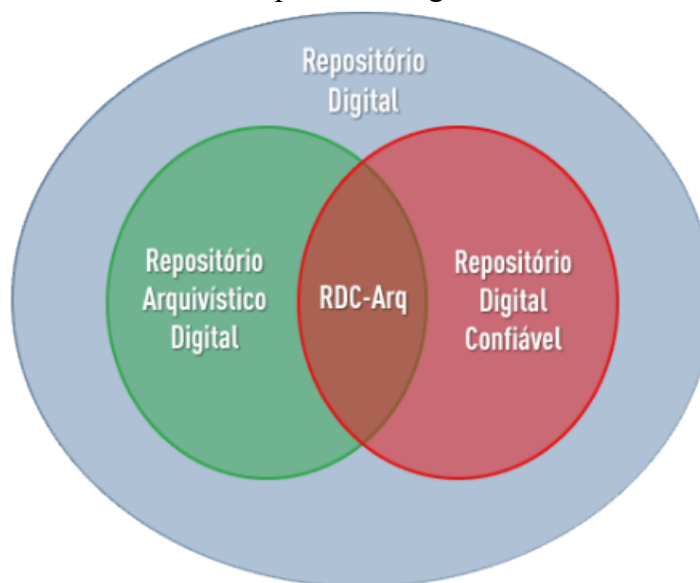
4.4 AUTENTICIDADE DOS DOCUMENTOS ARQUIVÍSTICOS NO RDC-ARQ

A autenticidade dos documentos arquivísticos digitais é um dos elementos mais significativos na construção de um Repositório Arquivístico Digital Confiável (RDC-Arq), pois garante que os documentos mantenham sua veracidade ao longo do tempo, independentemente das mudanças tecnológicas. De acordo com Gava e Flores (2020), a autenticidade está intimamente ligada à capacidade de preservar o documento exatamente como ele foi criado, sem modificações ou adulterações que possam comprometer sua integridade. Isso é particularmente relevante para ambientes institucionais, onde os documentos arquivísticos são frequentemente utilizados como evidências legais e históricas. A implementação de um RDC-Arq visa assegurar que os documentos arquivísticos sejam preservados com registros detalhados sobre sua criação, permitindo que futuros usuários possam verificar a autenticidade desses registros.

Para que a autenticidade seja mantida, o RDC-Arq deve adotar diretrizes internacionais específicas, como a ISO 16363, que estabelece práticas e critérios para auditoria e certificação de repositórios digitais confiáveis. Andrade e Chagas (2021) enfatizam que a adoção dessa norma oferece uma estrutura robusta para a criação de registros detalhados sobre a origem, o uso e a preservação dos documentos arquivísticos. Esses registros são fundamentais, pois fornecem dados sobre o contexto em que os documentos foram criados e as circunstâncias que envolveram sua produção. A certificação de um repositório digital segundo essa norma fortalece a autenticidade do RDC-Arq e permite uma verificação eficaz, independentemente de alterações tecnológicas ao longo do tempo.

O conceito de RDC-Arq se encontra na interseção entre as características de um Repositório Arquivístico Digital e de um Repositório Digital Confiável. A imagem a seguir ilustra como esses três conceitos se inter-relacionam, destacando que o RDC-Arq incorpora os elementos essenciais tanto do ponto de vista arquivístico quanto dos requisitos de autenticidade digital, formando um sistema robusto para a preservação de documentos digitais.

Figura 1 - Interseção entre Repositório Arquivístico Digital, Repositório Digital Confiável e Repositório Digital



Fonte: Gava e Flores (2020).

A interseção representada na imagem destaca a complexidade e a complementaridade entre os aspectos arquivísticos e tecnológicos que definem um RDC-Arq. Esse modelo demonstra que, para atingir a autenticidade necessária, o repositório deve combinar rigorosas práticas de gestão documental com tecnologias avançadas de segurança e preservação digital, garantindo que os registros arquivísticos permaneçam acessíveis, íntegros e autênticos ao longo do tempo.

Entre as ferramentas utilizadas para assegurar a autenticidade, estão as tecnologias de criptografia e os mecanismos de hash, que permitem a detecção de qualquer modificação feita nos documentos após sua inserção no repositório. Mori *et al.* (2020) discutem a implementação de blockchain como uma solução inovadora para o controle de autenticidade no RDC-Arq, criando uma cadeia de custódia digital imutável que registra todas as interações e alterações realizadas nos documentos. Esse processo descentralizado e transparente amplia a segurança e a autenticidade, uma vez que todas as alterações ficam permanentemente registradas, permitindo auditorias frequentes e facilitando a validação de autenticidade.

A verificação de autenticidade no RDC-Arq deve ser um processo contínuo e integrado ao próprio funcionamento do repositório, garantindo que as verificações ocorram de forma automatizada e sem interrupções. Andrade e Chagas (2023) argumentam que as ferramentas de controle e verificação devem ser configuradas para operar automaticamente sempre que um documento for acessado ou atualizado, oferecendo uma camada extra de proteção contra adulterações. Esse modelo de verificação contínua facilita a detecção precoce de possíveis irregularidades e aumenta a segurança dos documentos arquivísticos armazenados, além de reforçar a autenticidade.

Além das verificações técnicas, a autenticidade de um documento arquivístico digital também é garantida pelo controle rigoroso de acesso e pela administração cuidadosa dos documentos. Santos e Mazuco (2020) observam que o acesso controlado é essencial para evitar que usuários não autorizados façam alterações ou consultas indevidas aos documentos arquivísticos. O RDC-Arq deve, portanto, adotar políticas claras de controle de acesso, utilizando autenticação multifator e permissões de usuário específicas, que limitem o acesso aos documentos com base nas funções e nas responsabilidades de cada colaborador. Essas práticas garantem que somente usuários autorizados possam interagir com os documentos arquivísticos, reduzindo os riscos de adulteração e mantendo a autenticidade dos registros.

A preservação da autenticidade também envolve o registro de metadados que documentem todas as atividades realizadas sobre cada documento ao longo de sua vida útil. Gava e Flores (2021) destacam a importância de metadados padronizados e completos para a garantia de autenticidade, uma vez que esses dados permitem que se rastreie o histórico completo do documento, desde a sua criação até seu descarte. Os metadados devem incluir informações sobre o autor, o contexto de criação, a data de criação e as ações realizadas no documento, como modificações, acessos e transferências. Esses registros são indispensáveis para que o RDC-Arq mantenha um histórico preciso e confiável, essencial para a validação da autenticidade dos documentos arquivísticos.

A implementação de RDC-Arq que se baseie na autenticação multifator e no controle de metadados favorece a rastreabilidade dos documentos. Andrade e Chagas (2023) observam que o controle rigoroso das operações realizadas sobre o documento é fundamental para garantir que ele se mantenha íntegro e autêntico ao longo de seu ciclo de vida. Isso significa que qualquer alteração ou interação com o documento, seja um acesso ou uma modificação, deve ser registrada e documentada de forma a permitir a verificação a qualquer momento. A rastreabilidade é um recurso que permite que os documentos arquivísticos digitais sejam

tratados como ativos autênticos e imutáveis, assegurando que sua integridade seja mantida independentemente das mudanças no ambiente digital.

A preservação da autenticidade exige um ambiente controlado, onde as ferramentas de monitoramento e de controle de integridade operem continuamente. Como discutem Mori *et al.* (2020), a configuração de alertas automáticos é uma prática recomendada para que o repositório possa reagir rapidamente em caso de alteração ou tentativa de adulteração dos documentos arquivísticos. Esses alertas são acionados automaticamente sempre que uma modificação suspeita é detectada, permitindo que a equipe do RDC-Arq tome medidas imediatas para evitar qualquer comprometimento da autenticidade do documento.

A prática de auditorias periódicas é outro fator que fortalece a autenticidade no RDC-Arq, pois possibilita que uma entidade externa avalie a conformidade dos processos e verifique a integridade dos documentos arquivísticos. A auditoria periódica é uma prática que assegura que o RDC-Arq continue operando conforme os requisitos internacionais de preservação digital e autenticidade, permitindo a validação contínua dos documentos. De acordo com Andrade e Chagas (2021), a auditoria funciona como uma revisão dos processos de preservação, verificando se os protocolos estão sendo seguidos corretamente e se os documentos arquivísticos permanecem autênticos e íntegros.

As auditorias também permitem que o repositório detecte e corrija falhas nos processos de preservação antes que elas comprometam a autenticidade dos documentos arquivísticos. Santos e Flores (2022) indicam que auditorias regulares são indispensáveis para identificar vulnerabilidades no sistema, principalmente no que se refere ao controle de acesso e à verificação de autenticidade. As auditorias podem ser realizadas de forma interna ou por meio de entidades externas, promovendo uma avaliação independente que assegura a objetividade e a autenticidade dos resultados.

O uso de ferramentas de blockchain no RDC-Arq para fins de autenticação e rastreamento é uma prática que garante um registro imutável de todas as ações realizadas sobre os documentos. Mori *et al.* (2020) argumentam que o blockchain pode fornecer uma camada adicional de segurança e autenticidade para os repositórios digitais confiáveis, assegurando que as transações e interações com os documentos arquivísticos fiquem registradas de forma descentralizada e permanente. Essa tecnologia é particularmente útil em repositórios que lidam com grandes volumes de documentos arquivísticos, uma vez que permite a validação de autenticidade de forma escalável e segura.

O blockchain também contribui para a transparência dos processos de preservação digital, facilitando a auditoria e a verificação de autenticidade em grandes volumes de

documentos. Andrade e Chagas (2021) apontam que a transparência proporcionada pelo blockchain aumenta a confiança dos usuários no RDC-Arq, pois assegura que todos os registros de interações com os documentos estão acessíveis e podem ser verificados independentemente. Esse recurso é valioso para instituições que precisam garantir a autenticidade dos documentos arquivísticos em setores onde a autenticidade dos registros é crítica, como no setor jurídico e governamental.

A implementação de políticas de controle e governança documental também é fundamental para assegurar a autenticidade dos documentos arquivísticos digitais no RDC-Arq. Santos e Mazuco (2020) sugerem que as políticas de governança devem ser claras e objetivas, definindo responsabilidades e funções específicas para a administração dos documentos e para o controle de acessos. Essas políticas orientam a equipe do repositório sobre as práticas recomendadas de preservação e autenticidade, promovendo uma cultura de responsabilidade e segurança dentro da organização.

Os requisitos de autenticação multifator, rastreamento de histórico e auditorias periódicas configuram o ambiente ideal para que a autenticidade dos documentos arquivísticos digitais seja mantida. Conforme indicam Andrade e Chagas (2023), esses elementos asseguram que os documentos arquivísticos digitais mantidos no RDC-Arq possam ser verificados a qualquer momento e em qualquer contexto, possibilitando que sejam utilizados como evidências confiáveis e autênticas. Isso é especialmente importante em instituições que dependem da preservação da memória e da história, onde os documentos arquivísticos representam fontes valiosas de informação e testemunho histórico.

A autenticidade dos documentos arquivísticos no RDC-Arq é um compromisso institucional que exige um esforço contínuo de monitoramento, auditoria e verificação. Santos e Flores (2020) destacam que a autenticidade não é um processo estático, mas uma prática que deve ser revisada e atualizada conforme as mudanças tecnológicas e operacionais ocorrem. Ao implementar políticas e tecnologias que garantam a autenticidade dos documentos arquivísticos digitais, o RDC-Arq se estabelece como um repositório confiável que preserva o valor documental e histórico de registros que sustentam o funcionamento e a memória institucional.

Para assegurar a autenticidade dos documentos arquivísticos, o RDC-Arq deve utilizar práticas avançadas de verificação que validem não apenas o conteúdo do documento, mas também seu contexto original, garantindo que todas as informações relacionadas à sua criação e uso estejam devidamente preservadas. Andrade e Chagas (2021) ressaltam que a autenticidade depende de processos que comprovem a autoria e o propósito de cada

documento, assegurando que sua interpretação permaneça fiel ao contexto original de criação, o que é fundamental em setores onde documentos arquivísticos servem como provas legais ou históricas.

A implementação de assinaturas digitais é uma prática que fortalece a autenticação dos documentos, pois associa um identificador único ao documento, que comprova sua origem e integridade ao longo do tempo. Gava e Flores (2020) observam que, ao utilizar assinaturas digitais, o RDC-Arq garante que os documentos possam ser autenticados de forma contínua, independentemente de mudanças tecnológicas, pois as assinaturas permanecem vinculadas ao documento, independentemente de seu formato.

Além das assinaturas digitais, o RDC-Arq pode adotar práticas de autenticação baseada em biometria para determinados processos, como a criação ou ingestão de documentos que possuem alto valor jurídico. Embora seja uma prática menos comum, Andrade e Chagas (2021) destacam que a biometria oferece uma camada adicional de segurança, que pode ser utilizada em ambientes sensíveis onde a autenticidade do documento deve ser garantida com um nível elevado de precisão. Essa prática é especialmente relevante em instituições jurídicas e governamentais.

O uso de tecnologias de blockchain também oferece uma forma eficaz de fortalecer a autenticidade dos documentos arquivísticos, especialmente quando são necessários registros imutáveis. Mori *et al.* (2020) discutem que o blockchain permite que o RDC-Arq registre todas as ações realizadas em um documento, criando uma trilha de auditoria permanente e inalterável. Esse registro descentralizado e criptograficamente seguro promove a confiança no RDC-Arq e assegura que qualquer modificação no documento seja detectada e registrada.

A adoção de políticas de versionamento é outra prática que garante a autenticidade dos documentos arquivísticos ao longo do tempo. Andrade e Chagas (2023) argumentam que, ao manter versões registradas de cada documento, o RDC-Arq permite que as alterações realizadas ao longo de sua existência sejam rastreadas, preservando a autenticidade do conteúdo original e documentando as modificações subsequentes. Isso é especialmente importante em ambientes colaborativos, onde múltiplos usuários interagem com os documentos ao longo do tempo.

A criação de registros de preservação autenticados, que documentam todas as atividades realizadas nos documentos arquivísticos desde sua criação, fortalece a autenticidade no RDC-Arq. Gava e Flores (2021) concluem que esses registros, que detalham todas as operações, fornecem uma base confiável para futuras auditorias, garantindo que a autenticidade dos documentos seja preservada mesmo diante de mudanças tecnológicas ou

institucionais. Essa prática assegura que cada documento mantido no RDC-Arq possa ser validado de forma confiável, promovendo a segurança e a credibilidade dos registros arquivísticos.

A autenticação dos documentos no RDC-Arq não é apenas um processo técnico, mas também envolve a criação de políticas de controle que determinam critérios claros para a criação, modificação e transferência de documentos. Andrade e Chagas (2021) destacam que essas políticas garantem que os documentos arquivísticos mantenham seu valor probatório e histórico, pois definem padrões que asseguram a legitimidade das ações realizadas sobre cada registro. O estabelecimento de diretrizes formais permite que o RDC-Arq atue de forma consistente, resguardando a autenticidade dos documentos de maneira sistemática.

Para reforçar a autenticidade, o RDC-Arq pode adotar sistemas de controle de acesso baseados em perfis de usuário, onde cada ação realizada nos documentos é vinculada a um responsável específico. Essa prática promove uma camada extra de responsabilidade individual sobre a manutenção da autenticidade dos registros, como observado por Gava e Flores (2020). Associar cada modificação a um usuário específico garante uma rastreabilidade precisa, de modo que qualquer alteração possa ser investigada, proporcionando uma verificação contínua de quem interage com os documentos e em quais circunstâncias. Andrade e Chagas (2023) sugerem que o uso de tecnologias de somente leitura ou de bloqueio de edição para certos tipos de documentos críticos pode impedir que ocorram mudanças indesejadas. Essa prática protege o valor probatório dos documentos e reforça a confiança dos usuários no repositório, promovendo um ambiente onde a autenticidade é constantemente resguardada.

A integridade no RDC-Arq depende não apenas de ferramentas e sistemas, mas também de uma cultura institucional que valorize a segurança da informação. Andrade e Chagas (2021) afirmam que a criação de uma cultura de segurança fortalece a adesão dos funcionários aos protocolos de integridade e evita que ações humanas comprometam a preservação dos documentos. Treinamentos regulares e a conscientização da equipe sobre as melhores práticas de segurança garantem que todos compreendam a importância de seguir os protocolos rigorosamente.

Para prevenir ameaças cibernéticas, o RDC-Arq pode implementar sistemas de criptografia que protejam os dados em trânsito e em repouso, garantindo que o conteúdo dos documentos arquivísticos permaneça seguro em todas as fases de seu ciclo de vida. Chaves (2023) observa que a criptografia de ponta a ponta cria uma barreira contra tentativas de interceptação ou manipulação durante a transferência de documentos, além de proteger o

conteúdo armazenado nos servidores. Essa camada extra de segurança assegura que a integridade dos documentos seja mantida em todas as interações e movimentações.

A integridade dos documentos também pode ser fortalecida com a adoção de rotinas de controle de qualidade que verificam a consistência dos dados arquivados no RDC-Arq. Andrade e Chagas (2023) sugerem que, ao realizar verificações periódicas de qualidade, a equipe do repositório pode identificar erros de armazenamento ou corrupção de dados de forma precoce, permitindo que sejam aplicadas ações corretivas antes que os documentos seja comprometido. Essas rotinas reforçam a autenticidade do RDC-Arq, pois garantem uma supervisão contínua sobre os registros.

A criação de políticas de preservação da autenticidade que incluam critérios para arquivamento e retenção dos documentos também fortalece o compromisso do RDC-Arq com a autenticidade a longo prazo. Andrade e Chagas (2021) enfatizam que a definição de critérios específicos sobre quais documentos devem ser mantidos de forma permanente e quais podem ser descartados permite que o repositório gerencie seu acervo de forma estruturada, mantendo o valor probatório e histórico dos registros preservados. Essa organização garante que os documentos mais relevantes sejam protegidos com medidas adicionais de autenticidade.

O RDC-Arq pode adotar uma política de atualização contínua das práticas de preservação, acompanhando inovações tecnológicas e metodológicas que aprimorem a autenticação dos documentos arquivísticos. Gava e Flores (2020) apontam que a pesquisa e o desenvolvimento de novas tecnologias podem contribuir para a implementação de ferramentas que validem a autenticidade de maneira cada vez mais precisa e ágil. Esse compromisso com a inovação é fundamental para que o RDC-Arq acompanhe as mudanças tecnológicas e mantenha a autenticidade dos documentos em um cenário de evolução constante

4.5 INTEGRIDADE E SEGURANÇA DA INFORMAÇÃO NO RDC-ARQ

A integridade dos documentos arquivísticos digitais é outro pilar essencial para a efetividade de um RDC-Arq. Garantir que os documentos arquivísticos permaneçam intactos e completos ao longo de todo o ciclo de preservação é um desafio constante, especialmente em um contexto onde ameaças à segurança digital, como ciberataques e falhas técnicas, são uma preocupação contínua. De acordo com Braga *et al.* (2022), a integridade dos documentos é mantida por meio de políticas rigorosas de segurança da informação, que incluem práticas como backups regulares, auditorias frequentes e replicação de dados em locais geograficamente distintos. Essas práticas de segurança evitam a perda de dados e asseguram

que os documentos arquivísticos digitais sejam mantidos em sua forma original, independentemente de eventuais problemas que possam surgir.

A certificação de repositórios digitais confiáveis conforme a ISO 16363 destaca a importância de monitoramentos constantes e verificações de integridade para que um RDC-Arq cumpra sua função com excelência. Andrade e Chagas (2023) discutem que auditorias periódicas não são apenas recomendadas, mas essenciais para a manutenção da integridade, permitindo identificar quaisquer irregularidades e assegurar que os processos de preservação estejam de acordo com as melhores práticas. Essas auditorias têm um papel fundamental na verificação da validade dos registros, possibilitando a rápida detecção de alterações não autorizadas e garantindo que o repositório continue alinhado aos padrões de preservação digital.

Além de auditorias e backups, o RDC-Arq deve incorporar ferramentas avançadas de segurança digital que previnam acessos não autorizados, minimizando as chances de comprometimento dos documentos arquivísticos. Santos e Mazuco (2020) propõem uma abordagem de segurança abrangente que abarca medidas físicas, lógicas e administrativas, assegurando proteção em todas as camadas do repositório. No aspecto lógico, o uso de autenticação multifator e criptografia de dados são práticas recomendadas, permitindo que os documentos arquivísticos estejam protegidos contra acessos não autorizados. No nível administrativo, políticas de controle de acesso são fundamentais para que apenas usuários devidamente autorizados possam interagir com os registros, garantindo que a integridade dos documentos não seja ameaçada.

A integridade dos documentos arquivísticos digitais também é assegurada pela redundância de dados, um método que permite que os documentos sejam armazenados em múltiplos locais e dispositivos, evitando a perda de informações em caso de falhas técnicas. Gava e Flores (2021) destacam que a replicação geograficamente distribuída é uma estratégia eficaz para prevenir a perda de dados, pois oferece uma rede de proteção que permite a rápida recuperação dos documentos em situações de desastres naturais ou incidentes de segurança. Esse tipo de redundância também facilita o acesso contínuo aos documentos arquivísticos, mantendo a integridade dos registros em todos os pontos de armazenamento.

A utilização de criptografia e autenticação multifator no RDC-Arq fortalece as barreiras de segurança contra ameaças externas e internas. Andrade e Chagas (2023) enfatizam que a criptografia é essencial para assegurar que os documentos arquivísticos estejam protegidos contra acessos não autorizados, uma vez que essa tecnologia torna as informações ilegíveis para qualquer pessoa sem a chave de acesso apropriada. A autenticação

multifator, por sua vez, aumenta a proteção, pois exige que os usuários passem por múltiplos níveis de verificação para acessar o repositório. Esses procedimentos asseguram que os documentos arquivísticos digitais sejam mantidos em um ambiente seguro e confiável.

O RDC-Arq deve, ainda, adotar políticas de segurança rigorosas que definam claramente as responsabilidades de cada usuário e as permissões de acesso a diferentes níveis de informação. Santos e Mazuco (2020) sugerem que a implementação de políticas de controle de acesso, que regulem quem pode visualizar, modificar ou eliminar documentos, é um componente essencial para garantir que apenas pessoas autorizadas possam interagir com os documentos arquivísticos. Essas políticas permitem que o RDC-Arq opere com segurança, prevenindo modificações não autorizadas que possam comprometer a integridade dos documentos.

A prática de auditorias periódicas complementa as políticas de controle de acesso e permite que o RDC-Arq detecte possíveis ameaças ou falhas nos processos de segurança. Segundo Andrade e Chagas (2021), a realização de auditorias regulares ajuda a manter a integridade dos documentos arquivísticos digitais ao monitorar o cumprimento dos protocolos de segurança e identificar vulnerabilidades antes que elas comprometam os registros. As auditorias são também uma oportunidade para que o RDC-Arq revise suas práticas de segurança e faça atualizações que acompanhem as mudanças tecnológicas e as novas ameaças de segurança digital.

A integridade dos documentos arquivísticos digitais também é promovida pelo uso de algoritmos de verificação, como checksums e hashes, que garantem a integridade dos arquivos ao detectar quaisquer alterações no conteúdo. Mori *et al.* (2020) argumentam que os checksums são uma ferramenta valiosa para a preservação de documentos arquivísticos digitais, pois permitem que o RDC-Arq verifique automaticamente a integridade de cada documento. Em caso de discrepâncias, o sistema pode emitir um alerta, permitindo que a equipe de segurança aja imediatamente para restaurar o documento à sua forma original.

O RDC-Arq pode ainda contar com sistemas de monitoramento contínuo, que acompanham em tempo real a integridade dos documentos e o estado geral do repositório. De acordo com Gava e Flores (2021), o monitoramento em tempo real é uma prática recomendada para repositórios digitais confiáveis, pois permite que o RDC-Arq reaja rapidamente a qualquer ameaça ou falha técnica, minimizando o impacto sobre a integridade dos documentos. O monitoramento contínuo também proporciona maior segurança para a equipe de preservação, que pode agir de forma proativa para assegurar a integridade dos registros arquivísticos.

A implementação de sistemas de backup é outra medida que fortalece a integridade dos documentos arquivísticos digitais. Andrade e Chagas (2023) sugerem que os backups devem ser feitos regularmente e armazenados em locais separados para prevenir a perda de dados em caso de falhas no sistema principal. Esses backups oferecem uma camada adicional de proteção, permitindo que o RDC-Arq recupere os documentos arquivísticos em sua forma original, independentemente de eventuais problemas de segurança ou falhas técnicas.

A replicação de dados, aliada aos backups regulares, configura uma infraestrutura segura e robusta para a preservação digital, prevenindo a perda de informações valiosas. Santos e Mazuco (2020) apontam que a replicação de dados oferece maior resiliência ao RDC-Arq, uma vez que os documentos arquivísticos podem ser recuperados de qualquer local de armazenamento, mesmo em caso de falhas no sistema principal. Essa prática assegura a continuidade dos processos de preservação e fortalece a integridade dos registros, protegendo os documentos contra uma ampla gama de ameaças.

A redundância de dados também é uma medida preventiva contra o comprometimento dos documentos arquivísticos digitais, permitindo que os registros sejam armazenados em múltiplos locais para minimizar os riscos de perda. Andrade e Chagas (2021) discutem que a redundância é uma prática comum em repositórios digitais confiáveis, pois garante que os documentos arquivísticos possam ser recuperados mesmo em casos de falhas de hardware ou desastres naturais. Essa prática de replicação contribui para que o RDC-Arq opere com integridade, protegendo os registros contra ameaças externas e oferecendo um ambiente seguro para a preservação de documentos.

A adoção de práticas de segurança digital robustas também assegura que o RDC-Arq opere com um nível elevado de confiabilidade, fortalecendo a integridade dos documentos arquivísticos. Como observam Gava e Flores (2021), as práticas de segurança digital, quando integradas à preservação arquivística, criam um ambiente controlado onde os documentos permanecem inalterados e íntegros ao longo do tempo. Essas práticas são particularmente relevantes em instituições que trabalham com documentos sensíveis, onde a integridade dos registros é uma exigência operacional.

As medidas de controle de integridade no RDC-Arq são reforçadas pela criação de alertas automáticos que informam a equipe de preservação sobre possíveis falhas ou alterações suspeitas nos documentos. Mori *et al.* (2020) afirmam que esses alertas automáticos são fundamentais para que o RDC-Arq mantenha um controle eficiente sobre a integridade dos documentos, permitindo uma resposta rápida em caso de ameaças. A

implementação desses alertas configura um ambiente proativo, onde a equipe do repositório pode agir imediatamente para evitar compromissos na integridade dos documentos.

O RDC-Arq precisa também assegurar a proteção física dos documentos arquivísticos digitais, implementando sistemas que protejam o hardware e os dispositivos de armazenamento. Santos e Mazuco (2020) ressaltam que a segurança física é um componente essencial para a integridade dos documentos, pois protege a infraestrutura de armazenamento contra danos e interferências externas. Medidas como controle de temperatura e acesso restrito às áreas de armazenamento garantem que o RDC-Arq ofereça um ambiente seguro e controlado para a preservação digital.

A resiliência do RDC-Arq é reforçada pela integração de práticas de segurança em todos os níveis do repositório, desde a infraestrutura de hardware até o software utilizado para o controle e monitoramento dos documentos. Andrade e Chagas (2023) argumentam que a integração de segurança cria um ambiente onde todos os aspectos da preservação digital são protegidos, promovendo a integridade e a confiabilidade dos documentos arquivísticos. Essa abordagem integrada é crucial para que o RDC-Arq funcione com eficiência e segurança, assegurando que os documentos arquivísticos digitais sejam preservados de maneira confiável.

A integridade dos documentos arquivísticos digitais no RDC-Arq é resultado de uma combinação de políticas, tecnologias e práticas de segurança que protegem os registros contra ameaças e falhas. Santos e Flores (2022) concluem que a integridade é uma responsabilidade coletiva dentro do RDC-Arq, onde todos os profissionais envolvidos na preservação digital compartilham o compromisso de manter os documentos íntegros e confiáveis. A prática constante de auditorias, o uso de tecnologias de verificação e o monitoramento contínuo asseguram que o RDC-Arq seja um repositório seguro e confiável para a preservação de documentos arquivísticos digitais ao longo do tempo.

A integridade dos documentos arquivísticos no RDC-Arq é mantida não apenas pelo controle físico dos dispositivos de armazenamento, mas também por meio de práticas de segurança que garantem que o acesso aos dados seja restrito a usuários autorizados. Chaves (2023) observa que o RDC-Arq deve estabelecer protocolos claros de controle de acesso, assegurando que apenas pessoas qualificadas possam modificar ou consultar documentos críticos. Isso evita a adulteração de informações e garante que os documentos arquivísticos mantidos pelo RDC-Arq permaneçam íntegros.

O uso de sistemas de detecção de intrusões é uma prática recomendada para repositórios digitais que desejam garantir a integridade dos documentos arquivísticos. Andrade e Chagas (2021) destacam que esses sistemas monitoram o acesso e as operações

realizadas no RDC-Arq, emitindo alertas em caso de atividades suspeitas. Essa vigilância proativa ajuda a identificar tentativas de violação de segurança e a proteger os documentos arquivísticos contra modificações não autorizadas.

O RDC-Arq também deve implementar práticas de controle de versão, permitindo que alterações feitas em documentos arquivísticos sejam rastreadas e revertidas, se necessário. Gava e Flores (2021) argumentam que o controle de versão oferece uma camada adicional de segurança, permitindo que os administradores do RDC-Arq rastreiem o histórico completo de um documento e revertam modificações indesejadas. Esse recurso é essencial para a manutenção da integridade dos documentos, especialmente em repositórios que lidam com um grande volume de dados e usuários.

A criação de logs detalhados de atividades é outra prática que contribui para a integridade e segurança da informação no RDC-Arq. Segundo Andrade e Chagas (2023), os logs permitem que os administradores do repositório acompanhem todas as ações realizadas nos documentos arquivísticos, identificando padrões de comportamento suspeitos ou acessos não autorizados. Esses registros são importantes para auditorias e verificações de conformidade, pois garantem que o RDC-Arq funcione de forma segura e em conformidade com as normas de preservação digital.

Os backups periódicos são indispensáveis para garantir a integridade dos documentos arquivísticos, pois oferecem uma camada de proteção contra perda de dados em caso de falhas técnicas ou incidentes de segurança. Mori *et al.* (2020) afirmam que o RDC-Arq deve estabelecer uma rotina de backups regulares, armazenando cópias dos documentos em locais geograficamente distintos. Essa prática assegura que os documentos arquivísticos possam ser recuperados em caso de desastres ou ataques, mantendo sua integridade e acessibilidade.

O uso de protocolos de comunicação segura é essencial para que o RDC-Arq assegure que as transferências de dados sejam realizadas de forma protegida. Chaves (2023) observa que o uso de protocolos como HTTPS e VPNs reduz o risco de interceptação de dados, garantindo que as informações transmitidas entre o RDC-Arq e outros sistemas permaneçam seguras. A adoção de práticas de comunicação segura assegura que a integridade e a confidencialidade dos documentos arquivísticos sejam mantidas durante todo o ciclo de preservação.

A implementação de estratégias de redundância de armazenamento, com a replicação dos documentos em diferentes locais, é uma prática essencial para a integridade no RDC-Arq. Andrade e Chagas (2021) sugerem que essa abordagem reduz o risco de perda de dados devido a falhas de hardware ou a desastres naturais, garantindo que cópias adicionais estejam

disponíveis em caso de necessidade. A redundância de armazenamento permite que o RDC-Arq recupere documentos com rapidez e eficiência, protegendo a integridade dos registros mesmo em situações adversas.

O RDC-Arq pode utilizar práticas de segmentação de rede para proteger o acesso aos dados arquivísticos, isolando os documentos mais sensíveis em áreas de acesso restrito. Chaves (2023) observa que a segmentação impede que usuários não autorizados acessem registros confidenciais, fortalecendo a integridade dos dados armazenados. Essa prática é especialmente útil para repositórios que lidam com informações confidenciais ou que precisam atender a regulamentos de privacidade, assegurando que a segurança dos documentos arquivísticos seja mantida em todas as áreas do RDC-Arq.

4.6 ACESSIBILIDADE E INTEROPERABILIDADE DOS DOCUMENTOS NO RDC-ARQ

A acessibilidade é um princípio fundamental na preservação digital, especialmente no contexto de um RDC-Arq, onde os documentos arquivísticos digitais devem estar disponíveis para consulta e utilização sempre que necessário. Garantir a acessibilidade implica não apenas preservar os documentos, mas também disponibilizá-los de forma fácil e eficiente para os usuários autorizados, conforme Chaves (2023). Um RDC-Arq eficiente deve proporcionar ferramentas de pesquisa e recuperação ágeis, que permitam a localização dos documentos com rapidez e precisão. A acessibilidade também envolve a criação de interfaces intuitivas para facilitar o acesso aos documentos arquivísticos por profissionais e pesquisadores, independentemente de sua familiaridade com o sistema.

O ciclo de vida dos documentos arquivísticos digitais abrange as fases corrente, intermediária e permanente, representando a gestão integrada dos registros ao longo de seu tempo de retenção. A imagem a seguir ilustra o fluxo dos documentos dentro da cadeia de custódia digital arquivística e sua transição para o ambiente de preservação, demonstrando como o RDC-Arq desempenha um papel central na preservação e no acesso aos documentos arquivísticos digitais em longo prazo.

Figura 2 - Ciclo de Vida dos Documentos Arquivísticos Digitais e Cadeia de Custódia Digital Arquivística.



Fonte: Gava e Flores (2020).

A representação destaca a interligação entre os sistemas de gestão documental e as plataformas de preservação e acesso, evidenciando o papel do RDC-Arq como um ponto crítico na transição entre as fases do ciclo de vida documental. Essa integração assegura que os documentos arquivísticos sejam preservados com integridade e autenticidade, enquanto permanecem acessíveis para fins administrativos, jurídicos ou históricos, conforme necessário.

A acessibilidade no RDC-Arq não se limita ao acesso aos documentos, mas também à capacidade de compreendê-los e interpretá-los em qualquer contexto. Isso significa que os documentos arquivísticos devem ser armazenados em formatos que possam ser facilmente acessados e visualizados por diferentes plataformas e dispositivos. Para isso, a escolha de formatos amplamente reconhecidos e padronizados é essencial para evitar problemas de compatibilidade e obsolescência tecnológica. Andrade e Chagas (2023) enfatizam que a adoção de formatos abertos, como PDF/A para documentos de texto e TIFF para imagens, aumenta a longevidade dos documentos e permite que eles sejam visualizados em diferentes dispositivos e sistemas operacionais sem perda de qualidade ou acessibilidade.

A interoperabilidade é outro aspecto crucial que complementa a acessibilidade no RDC-Arq. A interoperabilidade garante que os documentos arquivísticos possam ser acessados, compreendidos e compartilhados entre diferentes sistemas, plataformas e instituições, independentemente das tecnologias utilizadas originalmente para sua criação. Shintaku, Braga e Oliveira (2021) apontam que a interoperabilidade é fundamental para evitar

que os documentos arquivísticos fiquem restritos a uma única plataforma ou software, promovendo a integração do RDC-Arq com outros sistemas e repositórios digitais. A utilização de protocolos e padrões de interoperabilidade, como o OAI-ORE, permite que os documentos arquivísticos digitais sejam trocados e acessados por outros repositórios, ampliando a acessibilidade e a usabilidade dos registros.

O protocolo OAI-ORE é especialmente relevante para a interoperabilidade no RDC-Arq, pois facilita o compartilhamento de metadados e permite que os documentos arquivísticos sejam agregados e integrados a partir de múltiplas fontes. Segundo Shintaku *et al.* (2023), o uso desse protocolo assegura que o RDC-Arq possa compartilhar seus documentos com outros sistemas e repositórios, ampliando o alcance dos documentos arquivísticos digitais. Essa interoperabilidade é particularmente importante para instituições que colaboram em projetos de preservação digital ou que compartilham acervos digitais com outras organizações, permitindo que os documentos arquivísticos sejam acessados por uma rede mais ampla de usuários.

A adoção de padrões internacionais de metadados é outra prática essencial para garantir a interoperabilidade e a acessibilidade dos documentos arquivísticos no RDC-Arq. Os metadados são informações estruturadas que descrevem os documentos e facilitam sua recuperação e interpretação. Gava e Flores (2021) destacam que a padronização dos metadados permite que os documentos arquivísticos digitais sejam facilmente localizados e compreendidos, mesmo em plataformas e contextos distintos. A utilização de padrões amplamente reconhecidos, como o Dublin Core, possibilita que os documentos arquivísticos sejam interpretados de forma consistente, independentemente do sistema ou plataforma onde estejam armazenados.

A interoperabilidade no RDC-Arq também envolve a capacidade de integração com outros sistemas de gestão de documentos, como sistemas de gestão de conteúdo (CMS) e sistemas de informações gerenciais. Andrade e Chagas (2023) sugerem que a integração com esses sistemas facilita o compartilhamento e o gerenciamento de documentos arquivísticos em múltiplos contextos, permitindo que o RDC-Arq funcione como um núcleo de preservação digital que interage com outras plataformas. Essa integração aumenta a acessibilidade dos documentos arquivísticos, pois permite que eles sejam acessados de forma ágil e eficiente em diferentes contextos institucionais e operacionais.

A interoperabilidade técnica, que permite que o RDC-Arq se conecte a outros sistemas por meio de APIs (Interfaces de Programação de Aplicações), é um elemento fundamental para assegurar a continuidade do acesso aos documentos arquivísticos digitais. Segundo

Santos e Mazuco (2020), o uso de APIs permite que o RDC-Arq seja acessado por outros sistemas de forma automatizada, facilitando a troca de dados e a integração de documentos arquivísticos com outras bases de dados e plataformas. Essa interoperabilidade técnica assegura que os documentos arquivísticos estejam acessíveis de forma contínua e integrada, promovendo a eficiência e a usabilidade dos registros.

A criação de interfaces amigáveis e intuitivas é essencial para facilitar a acessibilidade dos documentos arquivísticos digitais no RDC-Arq. Chaves (2023) argumenta que o desenvolvimento de interfaces de usuário acessíveis facilita a navegação e a recuperação de documentos arquivísticos, permitindo que os usuários encontrem rapidamente as informações de que precisam. As interfaces devem ser projetadas para atender às necessidades de diferentes perfis de usuários, incluindo profissionais de arquivologia, pesquisadores e o público em geral, promovendo uma experiência de acesso inclusiva e satisfatória.

Além de interfaces intuitivas, o RDC-Arq deve implementar ferramentas avançadas de busca e filtragem que permitam aos usuários localizar documentos arquivísticos com precisão e rapidez. Andrade e Chagas (2023) destacam que as ferramentas de busca avançada são fundamentais para a acessibilidade, uma vez que possibilitam que os usuários filtrem os resultados com base em critérios específicos, como data, autor, tipo de documento e palavras-chave. Essas ferramentas melhoram a experiência de acesso ao RDC-Arq, permitindo que os documentos arquivísticos sejam localizados de forma eficiente e contribuindo para uma recuperação de informações mais precisa.

A acessibilidade também envolve a preservação das condições de legibilidade e interpretabilidade dos documentos arquivísticos digitais. Isso significa que o RDC-Arq deve adotar práticas que garantam que os documentos possam ser visualizados e interpretados da forma correta, independentemente de alterações tecnológicas. De acordo com Andrade e Chagas (2021), a preservação da legibilidade envolve a escolha de formatos padronizados e o uso de práticas de migração de formatos, que assegurem que os documentos arquivísticos possam ser acessados mesmo diante de mudanças nos sistemas operacionais e softwares utilizados.

A adoção de padrões de metadados robustos permite que os documentos arquivísticos digitais mantenham um contexto claro e detalhado para os usuários futuros, facilitando a interpretação correta das informações. Como observam Gava e Flores (2021), os metadados contextualizam o documento, fornecendo informações sobre sua origem, criação, alterações e uso, o que é essencial para garantir que o documento seja compreendido de forma precisa.

Essa prática fortalece a acessibilidade dos documentos no RDC-Arq, pois garante que as informações estejam sempre disponíveis de maneira clara e completa.

A criação de relatórios e documentação de acessibilidade também é uma prática recomendada para o RDC-Arq, pois permite que a equipe de preservação identifique e resolva quaisquer problemas que possam comprometer o acesso aos documentos arquivísticos digitais. Santos e Mazuco (2020) recomendam a realização de relatórios regulares sobre o estado de acessibilidade do repositório, permitindo que a equipe de preservação ajuste as práticas e procedimentos conforme necessário. Esses relatórios ajudam a manter o RDC-Arq atualizado e asseguram que a acessibilidade dos documentos arquivísticos seja preservada ao longo do tempo.

A acessibilidade e interoperabilidade no RDC-Arq são elementos que ampliam o valor e a usabilidade dos documentos arquivísticos digitais. Ao adotar práticas de acessibilidade e interoperabilidade, o RDC-Arq promove a preservação digital de forma eficiente e abrangente, garantindo que os documentos arquivísticos possam ser acessados e utilizados por diferentes usuários e plataformas. Como concluem Andrade e Chagas (2023), a acessibilidade e a interoperabilidade são fatores que fortalecem a missão do RDC-Arq de preservar documentos arquivísticos de forma confiável e acessível, contribuindo para a preservação do patrimônio digital e para a construção de uma memória institucional duradoura.

A acessibilidade dos documentos arquivísticos no RDC-Arq deve ser planejada para atender diferentes públicos e níveis de acesso, garantindo que as informações sejam disponibilizadas de acordo com as permissões definidas para cada usuário. Andrade e Chagas (2021) destacam que, ao estabelecer políticas claras de acessibilidade, o RDC-Arq consegue assegurar que os documentos sejam acessados de forma eficiente e segura, atendendo às necessidades institucionais e promovendo o uso adequado dos registros arquivísticos.

A criação de camadas de acesso personalizadas, onde diferentes usuários têm permissões específicas de visualização, edição ou exclusão, é uma prática recomendada para o RDC-Arq. Chaves (2023) sugere que essas camadas de acesso ajudam a proteger documentos sensíveis, enquanto permitem que usuários autorizados acessem as informações necessárias. Essa estrutura de acessibilidade controlada também favorece a segurança dos documentos, pois limita a exposição de informações críticas a um público restrito.

O uso de metadados estruturados é uma prática que facilita a recuperação de documentos arquivísticos, permitindo que os usuários localizem as informações de forma rápida e precisa. Andrade e Chagas (2023) afirmam que a inclusão de metadados padronizados, como título, autor, data de criação e palavras-chave, aumenta a acessibilidade

dos documentos no RDC-Arq, uma vez que os usuários podem buscar registros específicos por meio de critérios bem definidos. A estruturação dos metadados também promove a interoperabilidade, permitindo que os documentos sejam compreendidos e interpretados em diferentes sistemas.

A interoperabilidade é fortalecida pelo uso de APIs (Interfaces de Programação de Aplicações), que permitem que o RDC-Arq se conecte a outros sistemas e compartilhe dados de forma automatizada. Gava e Flores (2021) sugerem que o uso de APIs facilita a troca de informações com outras plataformas digitais, promovendo uma integração que aumenta a acessibilidade e a usabilidade dos documentos arquivísticos. Essa prática é especialmente importante para instituições que trabalham em colaboração com outras entidades e precisam compartilhar dados de forma eficiente.

A utilização de tecnologias de indexação avançada é uma prática que melhora a acessibilidade no RDC-Arq, permitindo que os usuários localizem documentos com base em diversos critérios de busca. Andrade e Chagas (2023) destacam que a indexação avançada facilita o acesso a grandes volumes de documentos, organizando as informações de maneira estruturada e acessível. A implementação de um sistema de busca eficaz permite que o RDC-Arq ofereça uma experiência de acesso mais intuitiva e eficiente para os usuários.

A criação de diretórios e guias de navegação contribui para a acessibilidade no RDC-Arq, pois orienta os usuários na busca e na localização de documentos arquivísticos. Chaves (2023) argumenta que a criação de uma estrutura de diretórios clara e organizada facilita o acesso aos registros e permite que os usuários naveguem pelo repositório com maior facilidade. Essa prática promove uma experiência de uso satisfatória, assegurando que os documentos arquivísticos sejam acessados e interpretados de forma adequada, independentemente do nível de familiaridade dos usuários com o sistema.

A acessibilidade no RDC-Arq pode ser aprimorada com a criação de guias e tutoriais que orientem os usuários a explorar e utilizar o repositório de maneira mais eficiente. Andrade e Chagas (2021) recomendam que o RDC-Arq disponibilize materiais educativos que abordem desde o uso básico até as funcionalidades avançadas do sistema, permitindo que usuários de diferentes níveis de habilidade possam acessar os documentos sem dificuldades. Esse suporte técnico promove uma experiência de uso positiva e amplia o acesso a informações arquivísticas essenciais.

Para garantir a interoperabilidade, o RDC-Arq pode adotar padrões de metadados específicos para cada tipo de documento, facilitando a comunicação entre diferentes sistemas e plataformas. Gava e Flores (2021) apontam que a padronização de metadados promove uma

integração mais fluida entre o RDC-Arq e outros repositórios, permitindo que os documentos arquivísticos digitais possam ser compreendidos em múltiplos contextos e aplicações. Essa prática é essencial para manter a integridade dos dados e assegurar que os documentos possam ser transferidos e interpretados corretamente em diferentes ambientes.

O RDC-Arq também pode se beneficiar de parcerias com outras instituições para ampliar a interoperabilidade e acessibilidade dos documentos. Andrade e Chagas (2023) sugerem que a colaboração entre diferentes repositórios permite o desenvolvimento de práticas conjuntas e de tecnologias compatíveis, promovendo uma rede de acesso que vai além dos limites de um único sistema. Essas parcerias permitem que os documentos arquivísticos do RDC-Arq sejam acessíveis e interoperáveis em uma escala mais ampla, contribuindo para a disseminação e o uso mais eficaz dos registros digitais.

A inclusão de funcionalidades de acessibilidade, como suporte a pessoas com deficiência visual ou auditiva, amplia a acessibilidade no RDC-Arq e permite que mais usuários interajam com os documentos arquivísticos. Andrade e Chagas (2021) ressaltam que o RDC-Arq pode incorporar tecnologias de leitura de tela e descrições em áudio para facilitar o acesso por usuários com necessidades específicas. Ao adotar essas práticas inclusivas, o repositório demonstra um compromisso com a acessibilidade universal, assegurando que todos os usuários tenham acesso equitativo às informações preservadas.

Para fortalecer a interoperabilidade, o RDC-Arq pode implementar APIs e outros serviços de integração que facilitem a conexão com sistemas de terceiros, promovendo a troca e o compartilhamento de informações de forma ágil e segura. Gava e Flores (2021) apontam que as APIs permitem uma comunicação fluida entre diferentes plataformas, o que torna o RDC-Arq mais flexível e adaptável a novos contextos de colaboração. A interoperabilidade técnica facilita o compartilhamento de documentos e metadados, assegurando que o RDC-Arq seja parte ativa de uma rede global de repositórios digitais.

4.7 COORDENAÇÃO DE DOCUMENTOS DIGITAIS VISANDO ENVIO PARA UM RDC-Arq.

A gestão de documentos digitais é um processo fundamental para a organização, preservação e acesso eficiente à informação no ambiente digital. No contexto de um Repositório Digital Confiável para Arquivamento (RDC-Arq), essa gestão adquire uma importância ainda maior, pois envolve práticas rigorosas externas para a integridade, integridade, autenticidade e preservação a longo prazo dos documentos digitais.

Um RDC-Arq foi projetado para garantir que os documentos arquivados permaneçam seguros e compreensíveis ao longo do tempo, independentemente de mudanças tecnológicas. Para isso, a gestão de documentos de documentos digitais deve abranger todas as fases do ciclo de vida da informação, desde a criação, captura e classificação até o armazenamento, uso, preservação e eventual descarte.

Entre os principais aspectos da gestão de documentos digitais em um RDC-Arq estão:

- Políticas de Preservação Digital: Definição de diretrizes que garantem a manutenção da atualização, integridade e acessibilidade dos documentos ao longo do tempo;
- Metadados e Descrição: Uso de metadados padronizados para descrever o conteúdo, a estrutura, o contexto e o histórico dos documentos, facilitando a recuperação e o entendimento futuro;
- Segurança da Informação: Implementação de medidas de segurança para proteger os documentos contra acessos não autorizados, perdas, alterações indevidas e ameaças cibernéticas;
- Interoperabilidade: Adoção de padrões abertos que permitem a troca de informações entre diferentes sistemas e garantem a continuidade do acesso, mesmo com a evolução das tecnologias;
- Gestão de Riscos: Identificação e mitigação de riscos relacionados à obsolescência tecnológica, falhas de hardware/software e desastres físicos;
- Auditorias e Certificações: Realização de auditorias regulares para verificar a conformidade com normas internacionais, como a ISO 16363, que definem critérios para a confiabilidade de repositórios digitais.

A gestão de documentos eficaz de documentos digitais em um RDC-Arq não se limita a questões tecnológicas; envolve também aspectos organizacionais, legais e de governança da informação. A adoção de boas práticas contribui para a transparência institucional, a proteção da memória organizacional e o suporte à tomada de decisões baseadas em evidências documentais confiáveis.

4.8 LGPD E SUAS CARACTERÍSTICAS

Embora recentemente aprovada e organizada entre as leis de direitos individuais de cada cidadão, a Lei Geral de Proteção de Dados Pessoais, a Lei nº 13.709 de 2018, tem como fundamento: à privacidade; à autodeterminação informativa; à liberdade de expressão, de informação, comunicação e de opinião; à inviolabilidade da intimidade, da honra e da imagem; ao desenvolvimento econômico e tecnológico e a inovação; à livre iniciativa, livre concorrência e defesa do consumidor e o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais (Brasil, 2018).

Isabela Curi (2021) nos diz, ao abordar sobre esta lei, que ela estabelece “claramente os direitos do titular de dados pessoais, seja para apagar informações tornadas públicas por empresas ou corrigi-las”, e continua, “entre os pesquisadores, muitos veem similaridade entre ela e a General Data Protection Regulation, a GDPR, em vigência na Europa”.

A partir disso, devido à lei, qualquer pessoa é considerada proprietária dos seus próprios dados “e não mais as organizações que realizaram a coleta das informações. Com isso, tendem a ser reduzidos à vulnerabilidade, o uso inadequado e até mesmo o vazamento” (Cubos, 2022). Vê-se isso como grande importância desta legislação, já que ela confere às pessoas essa segurança tanto na esfera física quanto digital de seus dados pessoais. Ainda mais, percebe-se que ela está atenta a intensidade da evolução da globalização

Esta lei tem como foco, também, conforme Luke Mewes (2021, p. 47) “construir um mecanismo nacional sólido e organicamente atuante na regulação do tratamento de dados pessoais, mediante a aplicação concreta de preceitos já constituídos na ordem jurídica brasileira”, no entanto, havia uma carência “até então de uma eficácia visível em detrimento das práticas constantemente vivenciadas na chamada sociedade digital, por intermédio de ferramentas tecnológicas não raramente lesivas às liberdades individuais”, conforme (Mewes, 2021, p. 47).

Um dos pontos mais importantes também a ser comentado, é que há uma diferença entre dados pessoais e informações pessoais. Isso porque, segundo Mewes (2021, p. 50) “a informação é um produto da interpretação e sistematização dos dados. Inversamente, dados são a matéria-prima da informação”. Não somente isso, como continua o autor, mas também “ainda que as informações pessoais possuem maior afinidade com aspectos da privacidade do indivíduo, enquanto dados pessoais são mais especificamente ligados à proteção de dados em si”.

Bioni (Wikipedia, 2022), nos diz que “a LGPD cria um conjunto de novos conceitos jurídicos (e.g. "dados pessoais", "dados pessoais sensíveis"), estabelece as condições nas quais os dados pessoais podem ser tratados define um conjunto de direitos para os titulares

dos dados”, e continua ele, “gera obrigações específicas para os controladores dos dados e cria uma série de procedimentos e normas para que haja maior cuidado com o tratamento de dados pessoais e compartilhamento com terceiros”.

Portanto, percebe-se que a Lei Geral de Proteção de Dados, ratificada em 2022 pelo Governo Brasileiro, procura tanto trazer mais segurança para a pessoa física em seus dados pessoais, quanto observar quais desses dados têm o dever de serem, não apenas publicizados pelas empresas, mas também monetizados.

Diante do exposto, com o relevante advento da Blockchain que “das inúmeras vantagens que os sistemas descentralizados oferecem, recorrentemente surgem incertezas quanto à segurança da informação” (Mewes, 2021, p. 17). Com isso, é interessante questionar, juntamente com Luke Mewes (2021, p. 17): “como construir um ambiente paritário de intercâmbio de dados livre de fraudes e abusos na ausência de uma autoridade central para fiscalizá-lo?”

A partir disso, é necessário compreender a suma relevância de relacionar e integrar tanto a LGPD quanto Blockchain. Inicialmente, compreendemos que a importância da Legislação para a sociedade, uma vez que “diante da progressiva invasão à vida privada dos indivíduos no tocante às relações cibernéticas, com o advento da Internet e consolidação da chamada sociedade da informação, exigiu-se uma proteção cada vez mais robusta aos usuários” (Mewes, 2021, p. 68).

Tal Lei se vê como resposta dessa exigência devido a tais fatos ocorridos. Ainda mais, conforme Lucas Mewes (2021, p. 68) “tanto a Blockchain quanto a LGPD podem ser vistas como respostas a uma necessidade de combater o abuso e a centralização de poder que as tecnologias propiciaram a poucos e grandes membros da sociedade digital”.

Aparentemente ambos temas sejam incompatíveis e não podem se integrar, e até mesmo “há quem diga que a LGPD até mesmo inviabilizaria o uso do blockchain por alguns motivos, porque não seria possível cumprir aqueles direitos descritos na LGPD para os titulares de dados” (Curi, 2021).

No entanto, uma das bases da LGPD é a descentralização da identidade digital, isto porque “se garante a privacidade de dados nas transações - não se sabe quem enviou o numerário, por exemplo - e se realiza a "devolução" dos dados aos usuários” (Curi, 2021). Portanto, a autora comenta, ao continuar, que “a descentralização do gerenciamento de identidade devolve ao titular o controle de sua própria identidade, uma das bases da LGPD”.

Relacionado a isto, também se vê uma “possibilidade de tratamento de dados pessoais numa blockchain, o que atrairia a incidência da Lei Geral de Proteção de Dados Pessoais

(MEWES, 2021, p. 72). Ainda mais, há a possibilidade da compatibilização do exercício completo “dos direitos do titular de dados com a tecnologia blockchain; bem como é que esta pode até mesmo contribuir com a gestão do ciclo de vida e morte dos dados, dentro de uma organização, pública ou particular, assim como com o cumprimento da lei” (Curi, 2021).

Da mesma forma, alguns fatores da tecnologia Blockchain podem contribuir com a gestão dos dados dentro das empresas, reforçando assim o devido cumprimento das normas da Lei Geral de Proteção de Dados Pessoais. Isto porque, mais especificamente, pode-se perceber que o risco de informações vazadas e ou corrompidos em Blockchain é demasiado reduzido.

Assim, em consonância com a LGPD, tal tecnologia tem uma possibilidade sumamente relevante de ser uma associada tanto no tratamento e quanto compartilhamento dos dados pessoais. Do mesmo modo, esse meio tecnológico permite o fornecimento da integridade para os dados, como também apaga quaisquer duplicações de informações, aumentando, assim, a segurança. Ao fazer isso, permite a possibilidade de facilidade do rastreamento de quaisquer informações.

4.9 PRESERVAÇÃO DIGITAL A LONGO PRAZO

A preservação digital a longo prazo é um dos maiores desafios enfrentados pelas instituições que implementam um RDC-Arq, uma vez que implica em garantir que documentos arquivísticos digitais permaneçam acessíveis e utilizáveis, independentemente das mudanças tecnológicas. Andrade e Chagas (2021) destacam que o rápido avanço das tecnologias pode comprometer a legibilidade dos documentos arquivísticos se o repositório não adotar políticas eficazes de preservação digital. Assim, para que a preservação digital a longo prazo seja possível, é fundamental implementar práticas como migração de formatos, emulação de sistemas antigos e encapsulamento de dados, que garantem que os documentos arquivísticos possam ser interpretados e acessados, mesmo em um cenário de obsolescência tecnológica.

A migração de formatos é uma prática central para a preservação a longo prazo, pois permite que os documentos arquivísticos digitais sejam transferidos de um formato obsoleto para um formato atual, que possa ser facilmente acessado e interpretado. Segundo Braga *et al.* (2022), a migração periódica é essencial para garantir que os documentos arquivísticos não fiquem presos em formatos que se tornam inviáveis com o tempo. No entanto, a migração deve ser planejada cuidadosamente, considerando as características dos documentos e a

compatibilidade entre os formatos antigos e os novos. Esse processo precisa ser realizado de forma controlada e com a geração de metadados que registram as mudanças, assegurando que o conteúdo e a integridade dos documentos sejam mantidos.

A emulação é outra prática que pode ser adotada para preservar documentos arquivísticos digitais, permitindo que sistemas antigos sejam replicados para que os documentos possam ser acessados em seu ambiente original. Como explicam Andrade e Chagas (2023), a emulação é uma estratégia que evita a necessidade de migração para novos formatos, pois simula o ambiente computacional onde o documento foi originalmente criado e armazenado. Essa prática é particularmente útil para documentos que dependem de softwares específicos para serem interpretados corretamente, como bases de dados e documentos multimídia. A emulação, ao reproduzir o ambiente original de uso dos documentos, garante que eles possam ser acessados com suas características originais, preservando a autenticidade e o contexto de criação.

Além da migração e da emulação, o encapsulamento de dados é uma estratégia que contribui para a preservação digital a longo prazo, pois agrupa o documento arquivístico com seus metadados e informações técnicas necessárias para interpretação futura. De acordo com Gava e Flores (2021), o encapsulamento cria um "pacote" completo que inclui o documento e todos os dados necessários para sua leitura, independentemente do software utilizado originalmente. Essa prática é valiosa para documentos que possuem um ciclo de vida longo e que precisam ser preservados com toda a sua estrutura contextual. O encapsulamento assegura que os documentos arquivísticos digitais possam ser compreendidos de forma completa, mesmo em um futuro onde os softwares originais não estejam mais disponíveis.

A preservação digital a longo prazo exige uma infraestrutura robusta que garanta a integridade e acessibilidade dos documentos arquivísticos ao longo do tempo. Faria e Silva (2023) analisam os custos operacionais envolvidos na manutenção de um RDC-Arq e concluem que, embora seja um investimento significativo, a preservação digital é uma necessidade para evitar a perda de informações valiosas. O investimento em servidores seguros, backups regulares e uma equipe de TI especializada é imprescindível para que o repositório funcione de maneira eficiente e que os documentos arquivísticos sejam preservados em conformidade com as normas internacionais de preservação.

A gestão de obsolescência tecnológica é um dos maiores desafios para a preservação digital a longo prazo, uma vez que os dispositivos e softwares utilizados para armazenamento e acesso aos documentos mudam com frequência. Andrade e Chagas (2021) sugerem que o RDC-Arq deve monitorar continuamente a evolução tecnológica para antecipar possíveis

problemas de obsolescência e planejar a migração de dados antes que os formatos se tornem inacessíveis. Essa gestão proativa permite que o repositório mantenha a acessibilidade dos documentos, mesmo diante de rápidas mudanças no ambiente tecnológico.

O RDC-Arq deve contar com uma política de preservação digital que inclua práticas de revisão periódica dos formatos e tecnologias utilizadas, de forma a assegurar que os documentos arquivísticos sejam sempre acessíveis e interpretáveis. Segundo Braga *et al.* (2022), a revisão periódica é essencial para evitar a perda de acesso a documentos valiosos, permitindo que o repositório avalie continuamente suas práticas e faça ajustes conforme necessário. Essa política de revisão também permite que o RDC-Arq acompanhe a evolução das melhores práticas de preservação digital, aplicando inovações tecnológicas que fortaleçam a preservação dos documentos.

As políticas de preservação digital a longo prazo devem ser fundamentadas em normas internacionais, como a ISO 14721 (Modelo de Referência OAIS), que estabelece diretrizes para a preservação digital confiável. Andrade e Chagas (2021) argumentam que o uso de normas internacionais aumenta a confiabilidade e a consistência das práticas de preservação, pois garante que o repositório esteja em conformidade com padrões amplamente reconhecidos. A adoção dessas normas facilita a certificação do RDC-Arq e assegura que os documentos arquivísticos sejam preservados de forma estruturada e verificável.

A implementação de práticas de preservação digital a longo prazo também depende da capacitação dos profissionais envolvidos no RDC-Arq. Gava e Flores (2021) ressaltam que a preservação de documentos arquivísticos digitais requer habilidades específicas, que incluem o conhecimento técnico em TI e a compreensão das práticas de gestão documental. Profissionais capacitados são essenciais para que o RDC-Arq funcione de forma eficiente, uma vez que eles podem gerenciar a infraestrutura de preservação e implementar as práticas de preservação digital de maneira correta.

A preservação digital a longo prazo exige que o RDC-Arq adote práticas de segurança da informação que protejam os documentos arquivísticos contra ameaças cibernéticas, como hackers e malwares. Santos e Mazuco (2020) discutem que a segurança digital é uma condição necessária para a preservação confiável dos documentos, pois evita que os registros sejam adulterados ou destruídos por ataques externos. A implementação de sistemas de firewall, autenticação multifator e monitoramento contínuo são práticas que asseguram que o repositório funcione de maneira segura e que os documentos arquivísticos sejam protegidos contra ameaças digitais.

Os custos operacionais da preservação digital a longo prazo podem ser mitigados por meio de parcerias e colaborações institucionais. Faria e Silva (2023) sugerem que o compartilhamento de infraestrutura entre diferentes instituições permite que o RDC-Arq reduza os gastos com armazenamento e manutenção, oferecendo um ambiente mais sustentável para a preservação digital. Essas parcerias facilitam o compartilhamento de recursos e conhecimentos, promovendo práticas de preservação mais eficientes e colaborativas.

A adoção de tecnologias emergentes, como o armazenamento em nuvem, pode também contribuir para a preservação digital a longo prazo no RDC-Arq, uma vez que permite que os documentos arquivísticos sejam armazenados em locais de alta segurança e com acesso redundante. Andrade e Chagas (2023) observam que o armazenamento em nuvem oferece flexibilidade e escalabilidade para a preservação digital, uma vez que permite que o repositório aumente sua capacidade conforme necessário e garanta a acessibilidade contínua dos documentos. Contudo, é essencial que o RDC-Arq adote práticas de controle rigorosas para garantir a segurança dos dados em nuvem e evitar acessos não autorizados.

A preservação digital a longo prazo no RDC-Arq é um processo dinâmico que requer uma abordagem multidimensional, integrando práticas de migração, emulação, encapsulamento, políticas de revisão e gestão de obsolescência. Como concluem Andrade e Chagas (2021), a implementação dessas práticas permite que o RDC-Arq preserve a autenticidade, integridade e acessibilidade dos documentos arquivísticos digitais, assegurando que eles permaneçam confiáveis e acessíveis para futuras gerações.

A preservação digital a longo prazo no RDC-Arq deve levar em conta as particularidades de cada tipo de documento, adotando estratégias de preservação específicas para arquivos de diferentes naturezas e formatos. Andrade e Chagas (2021) recomendam a criação de políticas de preservação personalizadas, que definam os métodos de preservação mais adequados para cada categoria documental, promovendo a longevidade dos registros e assegurando que cada tipo de documento receba o tratamento necessário para sua conservação.

O RDC-Arq deve, ainda, manter uma infraestrutura flexível que permita a atualização periódica de seus sistemas e formatos de arquivo. Gava e Flores (2021) afirmam que, ao adotar uma infraestrutura flexível, o RDC-Arq consegue responder rapidamente às inovações tecnológicas e ajustar suas práticas de preservação conforme necessário. Essa flexibilidade é essencial para a continuidade da preservação digital a longo prazo, pois permite que o repositório se adapte a novas demandas e desafios tecnológicos.

A utilização de tecnologias de armazenamento escalável também contribui para a preservação digital a longo prazo, pois permite que o RDC-Arq aumente sua capacidade conforme o volume de documentos arquivísticos cresce. Andrade e Chagas (2023) sugerem que o armazenamento escalável facilita a preservação de grandes volumes de dados, evitando problemas de sobrecarga e assegurando que o RDC-Arq tenha capacidade suficiente para abrigar todos os documentos arquivísticos com segurança.

A criação de políticas de retenção e descarte controlado é uma prática que auxilia na preservação digital a longo prazo, pois define quais documentos devem ser mantidos e quais podem ser descartados após determinado período. Segundo Chaves (2023), essa prática permite que o RDC-Arq preserve apenas os documentos realmente essenciais, otimizando os recursos de armazenamento e promovendo uma gestão documental eficiente e sustentável. A preservação digital a longo prazo também depende da colaboração entre instituições, especialmente para o compartilhamento de boas práticas e tecnologias. Gava e Flores (2021) sugerem que as parcerias institucionais permitem que o RDC-Arq troque informações sobre técnicas de preservação, favorecendo a implementação de metodologias eficazes que promovam a longevidade dos documentos.

A colaboração entre instituições também permite que o RDC-Arq adote práticas testadas e aprimoradas em diferentes contextos, o que fortalece a resiliência do repositório frente a novos desafios. Andrade e Chagas (2023) observam que o compartilhamento de conhecimento e tecnologia com instituições parceiras proporciona ao RDC-Arq acesso a ferramentas inovadoras de preservação, reduzindo o risco de obsolescência tecnológica. Esse intercâmbio institucional ajuda a fortalecer a infraestrutura de preservação digital, permitindo que o RDC-Arq acompanhe as melhores práticas e evite a perda de dados devido a lacunas tecnológicas.

A criação de políticas de recuperação de desastres e planos de contingência é outra prática fundamental para assegurar a preservação a longo prazo no RDC-Arq. Santos e Mazuco (2020) destacam que esses planos permitem que o repositório reaja rapidamente em caso de incidentes, como falhas de hardware ou desastres naturais, reduzindo os danos aos documentos arquivísticos digitais. Essas políticas de contingência são indispensáveis para a continuidade do repositório, pois asseguram que os documentos arquivísticos possam ser recuperados com integridade e acessibilidade, mesmo após eventos inesperados.

A implementação de controles periódicos de qualidade é essencial para que o RDC-Arq verifique continuamente a eficácia de suas práticas de preservação a longo prazo. Andrade e Chagas (2021) argumentam que, ao realizar revisões e testes regulares, o

repositório consegue identificar possíveis pontos de falha e adotar melhorias que assegurem a preservação duradoura dos documentos arquivísticos. Esses controles periódicos permitem que o RDC-Arq ajuste suas estratégias e responda rapidamente a qualquer problema que possa comprometer a integridade dos registros.

A inovação em métodos de preservação digital, como o uso de inteligência artificial (IA) para análise e controle de documentos, também desponta como uma prática relevante para a preservação digital a longo prazo. Gava e Flores (2021) sugerem que a IA pode ser usada para monitorar a integridade e a conformidade dos documentos no RDC-Arq, automatizando processos de verificação e identificando padrões de uso que orientem a adaptação das práticas de preservação. A adoção de IA ajuda a otimizar recursos e oferece uma camada adicional de precisão na análise e controle dos documentos.

A preservação digital a longo prazo no RDC-Arq também pode ser beneficiada pela implementação de técnicas de duplicação segura dos dados, conhecidas como “espelhamento” dos documentos arquivísticos em locais distintos. Andrade e Chagas (2023) recomendam que o RDC-Arq mantenha cópias idênticas dos documentos em diferentes locais de armazenamento, o que permite maior resiliência e recuperação em casos de perda parcial. Essa prática é especialmente importante para registros críticos, pois assegura que os documentos sejam acessíveis mesmo diante de falhas em uma das unidades de armazenamento.

A preservação a longo prazo no RDC-Arq deve incluir uma análise periódica dos custos e da sustentabilidade das práticas de preservação. Faria e Silva (2023) observam que o investimento em preservação digital deve ser planejado a longo prazo, com uma análise contínua de custos para que a sustentabilidade do repositório seja garantida. Esse planejamento financeiro assegura que o RDC-Arq disponha de recursos necessários para manter suas operações e que as práticas de preservação sejam sustentáveis, mesmo em períodos de restrição orçamentária. Dessa forma, a sustentabilidade financeira é integrada às políticas de preservação, permitindo que o RDC-Arq continue preservando documentos arquivísticos digitais de maneira confiável e duradoura.

A preservação digital a longo prazo no RDC-Arq deve considerar também o impacto ambiental das práticas de armazenamento digital, adotando estratégias que minimizem o consumo de energia e o uso de recursos. Gava e Flores (2021) destacam que o uso de tecnologias sustentáveis pode reduzir os custos operacionais e o impacto ambiental, permitindo que o RDC-Arq contribua para práticas de preservação digital mais ecológicas.

Isso inclui o uso de data centers eficientes e a escolha de dispositivos de armazenamento que consomem menos energia sem comprometer a integridade dos documentos arquivísticos.

Além da infraestrutura, a preservação a longo prazo também requer uma visão estratégica que considere o ciclo de vida completo dos documentos arquivísticos. Andrade e Chagas (2023) observam que o RDC-Arq deve implementar políticas de revisão periódica dos documentos, decidindo quais registros precisam de preservação permanente e quais podem ser descartados após cumprirem sua função. Esse planejamento assegura que o repositório opere de forma sustentável e que os documentos mais importantes recebam atenção contínua em termos de preservação.

Para assegurar que a preservação digital a longo prazo seja eficaz, o RDC-Arq pode investir em pesquisas e inovações que contribuam para o aprimoramento das práticas de preservação. Andrade e Chagas (2021) sugerem que a instituição pode destinar recursos para o desenvolvimento de tecnologias e metodologias que melhorem a preservação e o acesso aos documentos, promovendo inovações que assegurem que o RDC-Arq permaneça atualizado. Essa abordagem proativa permite que o repositório se adapte a novas necessidades de preservação, ampliando sua capacidade de manter documentos arquivísticos no futuro.

A preservação digital a longo prazo no RDC-Arq pode ser reforçada com a criação de uma política de atualização tecnológica periódica, que avalie continuamente a eficiência dos equipamentos e softwares utilizados. Andrade e Chagas (2023) sugerem que a implementação de uma política de atualização contínua permite que o RDC-Arq acompanhe as inovações tecnológicas e substitua ferramentas que se tornem obsoletas. Esse monitoramento frequente é essencial para que o repositório se mantenha atual e continue preservando documentos com alta qualidade, mesmo em um cenário de mudanças tecnológicas rápidas.

A criação de um fundo de financiamento específico para a preservação digital garante que o RDC-Arq disponha de recursos a longo prazo para investir em melhorias de infraestrutura e capacitação de pessoal. Faria e Silva (2023) observam que um fundo específico permite que o repositório planeje e implemente atualizações tecnológicas sem depender de orçamentos anuais variáveis, assegurando a sustentabilidade financeira da preservação digital. Esse fundo cria uma base sólida para a continuidade do RDC-Arq, promovendo a segurança e a eficiência das práticas de preservação.

4.10 NORMAS E CERTIFICAÇÕES PARA O RDC-ARQ

A conformidade com normas e certificações internacionais é essencial para que um RDC-Arq possa garantir a autenticidade e a integridade dos documentos arquivísticos digitais. Normas como a ISO 14721 (Modelo de Referência OAIS) e a ISO 16363 (Auditoria e Certificação de Repositórios Digitais Confiáveis) fornecem diretrizes fundamentais para a criação, manutenção e operação de repositórios digitais, assegurando a consistência dos processos de preservação e a qualidade dos documentos preservados. Andrade e Chagas (2021) destacam que essas normas fornecem um modelo teórico que orienta a organização e os procedimentos do RDC-Arq, promovendo a preservação digital de documentos com autenticidade e integridade ao longo do tempo.

A ISO 16363, especificamente, é amplamente utilizada para certificar repositórios digitais confiáveis, pois fornece critérios abrangentes que cobrem aspectos técnicos, administrativos e de segurança. Esta norma oferece uma estrutura detalhada para auditoria, possibilitando que o RDC-Arq passe por processos de verificação externa, onde uma entidade independente avalia se o repositório segue as melhores práticas e se cumpre com os requisitos necessários para ser considerado confiável. Flores (2021) ressalta que a certificação de acordo com a ISO 16363 aumenta a confiança dos usuários e das instituições parceiras, pois garante que o RDC-Arq foi auditado e atendeu aos padrões internacionais, promovendo a transparência e segurança do processo de preservação digital.

A certificação de repositórios digitais confiáveis também reforça a sustentabilidade e a governança do RDC-Arq, pois exige que a instituição mantenha políticas claras de preservação e segurança. Andrade e Chagas (2023) observam que a certificação exige um compromisso de longo prazo por parte das instituições, que precisam demonstrar a capacidade de manter o repositório digital funcionando de forma consistente e sustentável. Esse compromisso inclui práticas de gestão documental e de recursos, que asseguram a continuidade dos serviços oferecidos pelo RDC-Arq e garantem que ele continue operando mesmo em cenários de mudança tecnológica ou de reorganização institucional.

O modelo OAIS, que é a base para a norma ISO 14721, é uma estrutura de referência que orienta a organização de repositórios digitais confiáveis e define os papéis e funções envolvidos no processo de preservação digital. Gava e Flores (2021) apontam que o modelo OAIS oferece um conjunto de conceitos que auxiliam na criação de um sistema organizado para a preservação digital, permitindo que o RDC-Arq funcione de maneira integrada e estruturada. O modelo divide o processo de preservação em etapas, como ingestão, armazenamento, gestão e acesso, o que facilita o planejamento e a execução de práticas que garantam a autenticidade e a acessibilidade dos documentos arquivísticos.

A implementação de normas e certificações em um RDC-Arq fortalece a confiança dos usuários e das instituições parceiras, promovendo a interoperabilidade e o reconhecimento internacional do repositório digital. Como observam Santos e Flores (2020), a conformidade com normas reconhecidas internacionalmente permite que o RDC-Arq seja integrado a outros repositórios digitais e facilite a troca de documentos arquivísticos com instituições de diferentes países. A interoperabilidade, promovida pela adesão a normas globais, assegura que os documentos arquivísticos digitais possam ser acessados e compreendidos em contextos internacionais, ampliando o valor e a utilidade dos registros preservados.

Além das normas ISO, outras diretrizes e frameworks podem ser aplicados ao RDC-Arq para complementar os requisitos de preservação e segurança. A norma NDSA *Levels of Digital Preservation*, por exemplo, fornece uma estrutura prática que auxilia as instituições a implementarem diferentes níveis de proteção e controle para seus documentos digitais. Andrade e Chagas (2021) recomendam a utilização dessa norma como uma forma de fortalecer o plano de preservação do RDC-Arq, permitindo que o repositório digital adote medidas de segurança e integridade que se ajustem às características específicas de seus documentos e às necessidades da instituição.

A certificação ISO 16363 é um processo complexo que exige uma avaliação minuciosa dos processos e das práticas de preservação digital adotados pelo RDC-Arq. Como explicam Gava e Flores (2021), essa certificação exige que o repositório digital mantenha uma documentação completa de todas as atividades relacionadas à ingestão, armazenamento e acesso aos documentos, promovendo uma abordagem transparente e verificável. A documentação detalhada não apenas facilita o processo de auditoria, mas também contribui para a continuidade das operações do RDC-Arq, uma vez que permite que a equipe de preservação tenha um registro histórico de todas as atividades realizadas.

A adoção de normas e certificações também representa um compromisso ético da instituição que mantém o RDC-Arq, pois garante que os documentos arquivísticos digitais sejam preservados em conformidade com os mais elevados padrões de qualidade e segurança. Andrade e Chagas (2023) argumentam que a certificação não apenas atesta a confiabilidade do repositório, mas também assegura que ele opera de forma responsável e comprometida com a preservação a longo prazo dos documentos. Esse compromisso ético reforça a confiança dos usuários e promove a responsabilidade institucional, mostrando que o RDC-Arq está alinhado com as melhores práticas de preservação digital.

A adesão a normas e certificações é uma estratégia que fortalece a governança do RDC-Arq e assegura que ele opere com transparência e eficácia. Santos e Mazuco (2020)

destacam que a governança de um repositório digital confiável deve incluir políticas claras e bem definidas sobre os processos de preservação, auditoria e segurança, garantindo que os documentos arquivísticos digitais sejam mantidos em um ambiente seguro e controlado. A certificação permite que o RDC-Arq demonstre sua conformidade com esses requisitos, promovendo a confiança e a credibilidade entre as instituições e os usuários finais. A conformidade com normas e certificações torna-se um pilar essencial para a preservação digital no RDC-Arq, assegurando que ele opere de forma consistente, sustentável e ética ao longo do tempo.

A adesão a normas e certificações internacionais permite que o RDC-Arq mantenha uma referência de qualidade e autenticidade, criando uma base sólida que respalda sua atuação. Essas normas, como a ISO 16363 e o modelo OAIS, estabelecem não apenas diretrizes técnicas, mas também práticas de governança, segurança e gestão da informação, o que possibilita uma operação mais integrada e organizada do repositório. Segundo Andrade e Chagas (2021), essa base normativa promove uma maior responsabilidade institucional, uma vez que exige que o RDC-Arq estabeleça e mantenha procedimentos documentados que sigam critérios reconhecidos mundialmente.

A adoção de normas e certificações também fortalece a transparência do RDC-Arq, pois facilita o acesso a auditorias externas, que atestam a conformidade das operações com os padrões internacionais. Essas auditorias, realizadas por entidades independentes, não apenas reforçam a credibilidade do repositório, mas também oferecem uma visão externa que permite identificar áreas de melhoria. Gava e Flores (2021) observam que as auditorias externas impulsionam o desenvolvimento contínuo do RDC-Arq, assegurando que o repositório evolua para atender novas demandas de preservação digital.

As normas internacionais incentivam a implementação de uma estrutura sólida de governança e gestão de riscos, elementos essenciais para que o RDC-Arq opere com eficiência em ambientes complexos. Andrade e Chagas (2023) ressaltam que, ao seguir padrões de certificação, o repositório passa a monitorar constantemente suas práticas de preservação e a identificar proativamente quaisquer ameaças à integridade e autenticidade dos documentos. Essa estrutura preventiva é valiosa, pois garante que o RDC-Arq esteja preparado para responder rapidamente a incidentes que possam comprometer a preservação de longo prazo dos documentos arquivísticos.

O alinhamento com padrões como a ISO 14721 (modelo OAIS) também promove a interoperabilidade com outros repositórios e sistemas de preservação digital, uma vez que esses padrões são amplamente reconhecidos e adotados em diferentes países. Isso permite que

o RDC-Arq compartilhe documentos arquivísticos com outras instituições e colabore em projetos internacionais de preservação digital. Conforme argumentam Santos e Flores (2020), a interoperabilidade baseada em normas globais facilita o acesso aos documentos arquivísticos por diferentes sistemas, ampliando o alcance e a utilidade dos registros preservados.

A certificação também auxilia no estabelecimento de políticas de preservação digital que sejam escaláveis e sustentáveis, permitindo que o RDC-Arq gerencie com maior eficácia os recursos humanos e tecnológicos envolvidos no processo de preservação. Flores (2021) sugere que, ao implementar práticas de governança e controle baseadas em normas certificadoras, o repositório adquire uma visão estratégica que possibilita um planejamento de longo prazo. Essa visão orienta as decisões institucionais, permitindo que o RDC-Arq se ajuste de forma planejada a novas demandas ou aumentos no volume de documentos, sem comprometer a qualidade da preservação.

Normas e certificações contribuem para a credibilidade do RDC-Arq junto ao público e aos stakeholders, promovendo uma imagem de transparência e compromisso com a preservação responsável. Andrade e Chagas (2021) ressaltam que, ao demonstrar conformidade com padrões internacionais, o RDC-Arq reforça sua legitimidade como instituição de preservação digital, o que é fundamental para fortalecer parcerias e obter apoio financeiro. Essa credibilidade é uma vantagem estratégica que facilita a atração de investimentos e parcerias, assegurando a continuidade do repositório e a preservação de documentos arquivísticos ao longo do tempo.

O RDC-Arq também pode se beneficiar da integração de normas e certificações específicas do setor, além das internacionais, para atender às regulamentações locais e às necessidades institucionais específicas. Andrade e Chagas (2021) destacam que a combinação de padrões globais com requisitos locais permite que o RDC-Arq opere de forma eficaz dentro de seu contexto, assegurando a preservação conforme as exigências regionais e as melhores práticas internacionais. Essa adaptação torna o repositório mais versátil e melhor alinhado às demandas de preservação locais.

A obtenção de múltiplas certificações pode proporcionar ao RDC-Arq um reconhecimento mais abrangente e consolidar sua posição como repositório de referência em preservação digital. Gava e Flores (2021) sugerem que, ao buscar certificações de diferentes entidades de auditoria, o RDC-Arq amplia sua legitimidade, mostrando um compromisso contínuo com a conformidade e a transparência. Esse reconhecimento facilita a criação de parcerias e amplia a confiabilidade do repositório perante a comunidade e os stakeholders.

A adesão a normas e certificações também impulsiona a inovação e a atualização contínua no RDC-Arq, pois essas certificações exigem práticas e tecnologias de ponta que promovem a eficiência e a modernização do repositório. Andrade e Chagas (2023) observam que a conformidade com as normas certificadoras estimula o RDC-Arq a incorporar soluções tecnológicas avançadas que melhorem o armazenamento, a integridade e a segurança dos documentos arquivísticos digitais, assegurando que o repositório esteja sempre em linha com as melhores práticas globais.

A participação do RDC-Arq em fóruns e conferências internacionais de preservação digital ajuda a atualizar e aprimorar as práticas de conformidade com normas e certificações. Andrade e Chagas (2021) destacam que essa participação permite que o repositório conheça as práticas mais recentes e troque experiências com outras instituições que seguem padrões semelhantes, promovendo um alinhamento contínuo com as melhores práticas globais. A troca de conhecimento fortalece o repositório e permite que o RDC-Arq inove sem comprometer os requisitos normativos.

A implementação de uma equipe interna dedicada ao monitoramento e ao cumprimento das normas também contribui para que o RDC-Arq mantenha suas certificações em conformidade. Gava e Flores (2021) sugerem que a criação de uma equipe de compliance interna garante uma supervisão constante dos processos e práticas do repositório, além de preparar a instituição para auditorias externas. Essa equipe especializada assegura que o RDC-Arq atenda aos requisitos de certificação e que suas práticas sejam ajustadas conforme as normas evoluem, promovendo uma operação sempre alinhada às regulamentações vigentes.

4.11 DOCUMENTAÇÃO E REGISTRO DE PROCESSOS

A documentação e o registro dos processos são elementos cruciais para o funcionamento eficaz e confiável de um RDC-Arq. Esses registros detalhados possibilitam que o repositório mantenha uma história precisa de todas as atividades realizadas em cada documento arquivístico digital, promovendo a transparência e a rastreabilidade dos processos. Santos e Flores (2022) observam que a documentação é essencial para assegurar que qualquer ação executada no RDC-Arq possa ser auditada e verificada, o que contribui para a confiabilidade e a autenticidade dos documentos arquivísticos digitais.

O registro de processos é especialmente importante em ambientes onde documentos arquivísticos podem ser auditados ou utilizados como prova legal, pois a documentação detalhada permite que o RDC-Arq demonstre a autenticidade e a integridade dos registros

preservados. Gava e Flores (2021) enfatizam que o repositório deve manter uma documentação contínua que inclua informações sobre todas as atividades realizadas, como ingestão, verificação de integridade, atualizações e descarte. Essas informações são fundamentais para garantir a preservação a longo prazo e para que o RDC-Arq possa sustentar a autenticidade de seus documentos mesmo em auditorias complexas.

A documentação dos processos no RDC-Arq também permite que o repositório implemente uma abordagem preventiva em relação à preservação digital, identificando problemas antes que eles comprometam a integridade dos documentos. Chaves (2023) destaca que a documentação de processos possibilita que padrões sejam observados e analisados, o que facilita a identificação precoce de possíveis falhas ou vulnerabilidades. Com essa abordagem preventiva, o RDC-Arq pode tomar medidas para proteger os documentos e ajustar suas práticas de preservação conforme necessário.

Além de favorecer a auditoria e a prevenção de problemas, a documentação de processos também contribui para a governança do RDC-Arq, permitindo uma gestão documental mais eficiente. Santos e Mazuco (2020) argumentam que o registro sistemático das atividades do repositório digital estabelece uma base sólida para a governança e facilita o acompanhamento de todas as operações realizadas no RDC-Arq. A documentação permite que a equipe de preservação compreenda melhor as necessidades dos documentos arquivísticos e os trate de acordo com suas características e requisitos específicos de preservação.

A documentação do RDC-Arq deve ser organizada de forma a proporcionar fácil acesso e clareza para os profissionais que a consultam. Andrade e Chagas (2021) sugerem que a organização da documentação deve seguir padrões bem definidos, utilizando sistemas de indexação e categorias que facilitem a recuperação das informações. Isso assegura que a equipe do RDC-Arq possa localizar rapidamente os registros necessários para auditorias ou processos de verificação, promovendo a eficiência e a transparência nas operações de preservação digital.

A manutenção de um histórico detalhado dos processos de preservação digital é fundamental para a continuidade e consistência das operações do RDC-Arq. Gava e Flores (2021) observam que o histórico dos processos ajuda a garantir que os procedimentos do repositório sejam seguidos de forma consistente, evitando problemas decorrentes de práticas inconsistentes. Essa continuidade operacional é especialmente importante em ambientes institucionais onde as políticas de preservação digital devem ser mantidas ao longo do tempo, independentemente de mudanças de equipe ou de administração.

A documentação de processos no RDC-Arq também permite que o repositório atenda a exigências de conformidade e certificação, uma vez que normas internacionais frequentemente requerem registros detalhados sobre as atividades de preservação. A ISO 16363, por exemplo, estipula que repositórios digitais confiáveis mantenham registros completos que demonstrem a conformidade com os padrões de preservação digital. Andrade e Chagas (2023) destacam que a documentação adequada facilita o processo de certificação, uma vez que permite que os auditores avaliem de maneira precisa as práticas e procedimentos do RDC-Arq.

A utilização de ferramentas de gestão de documentos e sistemas de registro eletrônico é recomendada para facilitar a documentação e o armazenamento de registros no RDC-Arq. Chaves (2023) argumenta que o uso de sistemas eletrônicos não apenas facilita a organização dos documentos, mas também permite que os registros sejam acessados rapidamente e de maneira segura, melhorando a eficiência operacional. Essas ferramentas possibilitam que o RDC-Arq mantenha uma documentação completa e acessível, promovendo a integridade e a confiabilidade dos processos de preservação.

A documentação detalhada dos processos de preservação digital também fortalece a segurança e a rastreabilidade dos documentos arquivísticos digitais. Segundo Santos e Mazuco (2020), o registro das atividades realizadas no RDC-Arq permite que cada interação com os documentos seja documentada, oferecendo uma visão completa sobre quem acessou ou alterou cada documento ao longo do tempo. Essa rastreabilidade é uma medida de segurança que assegura que apenas usuários autorizados tenham acesso aos documentos, reduzindo o risco de adulterações e mantendo a integridade dos registros.

A documentação e o registro de processos também facilitam a integração entre o RDC-Arq e outras plataformas e sistemas de gestão documental, permitindo que o repositório funcione de forma integrada com o ambiente institucional mais amplo. Andrade e Chagas (2023) sugerem que a interoperabilidade entre sistemas é fortalecida pela documentação de processos, pois permite que as informações armazenadas no RDC-Arq sejam compartilhadas e compreendidas por outros sistemas e repositórios. Isso aumenta a usabilidade dos documentos arquivísticos e facilita a troca de informações entre diferentes plataformas.

A transparência promovida pela documentação de processos no RDC-Arq é um fator que contribui para a confiança dos usuários e para a credibilidade institucional. Como discutem Gava e Flores (2021), a documentação permite que o repositório digital funcione de forma aberta e transparente, mostrando que todos os processos são monitorados e registrados. Essa prática aumenta a confiança das partes interessadas, que podem verificar a conformidade

do RDC-Arq com os padrões de preservação digital, promovendo a credibilidade e a responsabilidade institucional.

A documentação adequada também possibilita que o RDC-Arq implemente processos de melhoria contínua, ajustando suas práticas e procedimentos conforme necessário para otimizar a preservação digital. Andrade e Chagas (2021) afirmam que a análise dos registros documentados permite que o repositório identifique áreas que podem ser aprimoradas, promovendo uma abordagem de melhoria contínua que assegura que o RDC-Arq se mantenha atualizado com as melhores práticas de preservação. Essa análise constante dos registros fortalece a eficácia do repositório e assegura que ele opere de forma eficiente ao longo do tempo.

A documentação dos processos no RDC-Arq funciona como uma ferramenta de organização e controle, essencial para assegurar que todas as operações realizadas no repositório sejam conduzidas de forma padronizada e transparente. Andrade e Chagas (2023) observam que a documentação permite uma visão abrangente dos fluxos de trabalho, oferecendo uma referência que orienta a equipe em todas as etapas da preservação digital, desde a ingestão de documentos até sua preservação e descarte. Esse registro estruturado promove uma operação mais coesa e minimiza a margem de erro nas atividades do repositório.

O uso de registros detalhados facilita o processo de monitoramento e auditoria no RDC-Arq, pois oferece uma trilha de auditoria completa que documenta todas as interações com os documentos arquivísticos. Santos e Flores (2020) destacam que essa trilha de auditoria é essencial para garantir a transparência e a confiabilidade do repositório, uma vez que permite rastrear todas as modificações realizadas e avaliar a conformidade das práticas de preservação com os padrões estabelecidos. Esses registros são particularmente úteis em casos de auditoria externa, onde é necessário comprovar a integridade e autenticidade dos documentos preservados.

A documentação é também uma ferramenta importante para a avaliação de desempenho do RDC-Arq, permitindo que a instituição identifique áreas que necessitam de melhorias e ajuste suas práticas de acordo com os resultados observados. Andrade e Chagas (2021) sugerem que a análise dos registros permite uma visão detalhada de cada etapa do processo de preservação, o que possibilita ajustes operacionais para otimizar o funcionamento do repositório. Essa prática de revisão contínua assegura que o RDC-Arq evolua e adapte suas práticas para atender às novas demandas e desafios da preservação digital.

Além de servir como base para auditorias e avaliações, a documentação dos processos facilita a comunicação e o treinamento dentro do RDC-Arq. Gava e Flores (2021) apontam

que os registros de procedimentos padronizados permitem que novos colaboradores compreendam rapidamente os fluxos de trabalho, assegurando que a equipe opere de forma coesa e consistente. A documentação torna-se, assim, uma ferramenta educativa que promove a transmissão do conhecimento institucional e a continuidade das operações, independentemente de mudanças no quadro de funcionários.

A prática de manter registros de processos no RDC-Arq também promove a criação de um histórico institucional, preservando o conhecimento acumulado ao longo do tempo. Andrade e Chagas (2023) observam que essa documentação oferece uma perspectiva valiosa sobre a evolução das práticas de preservação digital, permitindo que futuras gerações de profissionais analisem e compreendam as decisões tomadas ao longo do tempo. Esse histórico institucional é fundamental para que o RDC-Arq construa uma base de conhecimento que apoie a inovação e a adaptação contínua do repositório.

A documentação dos processos auxilia o RDC-Arq na gestão de mudanças e adaptações tecnológicas, pois oferece um registro completo dos procedimentos e tecnologias utilizadas. Chaves (2023) destaca que, ao documentar todas as práticas de preservação e as tecnologias implementadas, o repositório possui um mapa detalhado que facilita a transição para novas soluções tecnológicas sem comprometer a integridade dos documentos arquivísticos. A documentação não apenas sustenta as operações diárias, mas também facilita a adaptação a novos contextos, promovendo a longevidade e a eficácia do RDC-Arq.

A documentação de processos no RDC-Arq pode ser fortalecida com o uso de ferramentas automatizadas que registram atividades em tempo real, permitindo um acompanhamento mais preciso e completo das operações. Andrade e Chagas (2021) afirmam que a automação dos registros reduz a possibilidade de erros humanos e facilita a geração de relatórios, promovendo maior eficiência e precisão no acompanhamento das atividades realizadas no repositório. Essa prática permite que o RDC-Arq mantenha um controle mais rigoroso sobre todos os seus processos e garante que cada operação esteja devidamente registrada.

Além da automação, o RDC-Arq pode adotar práticas de documentação que contemplem a recuperação de desastres, estabelecendo registros específicos para ações de contingência e recuperação de dados. Gava e Flores (2021) sugerem que a documentação dos processos de contingência permite que o repositório mantenha um plano de recuperação bem estruturado e que a equipe esteja preparada para lidar com situações de emergência. Essa documentação é fundamental para a continuidade das operações, assegurando que o RDC-Arq possa responder de forma rápida e eficaz a eventos imprevistos.

A documentação no RDC-Arq também pode incluir diretrizes para a gestão de alterações tecnológicas, detalhando como o repositório deve proceder em caso de atualização de sistemas ou substituição de tecnologias. Andrade e Chagas (2023) observam que a definição de políticas de adaptação tecnológica permite que o RDC-Arq mantenha sua funcionalidade mesmo diante de mudanças no ambiente digital. Essas diretrizes facilitam a transição para novas ferramentas e tecnologias, assegurando que o repositório funcione de maneira contínua e que os documentos arquivísticos sejam preservados com segurança.

A documentação também pode ser acompanhada de auditorias internas regulares, que revisem a precisão e a completude dos registros no RDC-Arq. Andrade e Chagas (2023) apontam que as auditorias internas ajudam a identificar lacunas na documentação e asseguram que cada processo seja registrado de maneira abrangente e clara. Essas auditorias permitem que o RDC-Arq refine suas práticas de documentação, melhorando a qualidade dos registros e promovendo uma operação mais transparente e organizada.

Para garantir a eficiência e a organização dos registros, o RDC-Arq pode implementar um sistema de indexação e classificação dos processos documentados, facilitando a recuperação de informações. Gava e Flores (2021) sugerem que a indexação dos registros permite uma consulta mais rápida e precisa, especialmente em auditorias ou revisões internas. Esse sistema contribui para a agilidade e a acessibilidade da documentação, assegurando que as informações estejam organizadas e prontamente disponíveis para a equipe e para eventuais auditorias externas.

5 METODOLOGIA

A metodologia adotada nesta pesquisa seguiu uma abordagem qualitativa, com o intuito de compreender a complexidade dos requisitos arquivísticos e operacionais necessários para a implementação do RDC-Arq. A análise qualitativa proporcionou uma exploração dos fatores que influenciam o objeto da pesquisa, conforme destacam autores como Creswell (2017). Nesse sentido, a pesquisa recorreu à análise documental utilizando esse método como base para avançar na compreensão dos elementos preparatórios para a implementação de um RDC-Arq.

A análise documental foi realizada com base em normas internacionais de preservação digital, como a ISO 16363 e o modelo OAIS, além de documentos institucionais e publicações acadêmicas relacionadas ao RDC-Arq. Ainda, foi analisado os documentos relativos ao modelo Hipátia, primeira experiência bem sucedida de implementação de um RDC-Arq no Brasil com garantia da cadeia de custódia. A pesquisa documental permitiu a identificação dos padrões e diretrizes que orientam a criação de repositórios digitais confiáveis.

A coleta de dados incluiu, ainda, a consulta institucional ao Instituto Brasileiro de Informação em Ciência e Tecnologia (IBICT), responsável direto pela implementação do modelo Hipátia. Essa consulta possibilitou uma compreensão mais aprofundada dos processos de preservação digital, permitindo a identificação das dificuldades e dos desafios enfrentados no dia a dia da operação e manutenção dos repositórios digitais. A troca de experiências por meio da consulta ofereceu um olhar mais humanizado e realista sobre a aplicação dos modelos teóricos no contexto prático.

A análise dos dados coletados por meio da análise documental permitiu a construção de um panorama completo sobre as necessidades, desafios e soluções envolvidas na implementação do RDC-Arq. Com isso, foram destacados os aspectos práticos que precisam ser considerados para garantir a eficácia e a sustentabilidade de um processo institucional de implementação de um projeto de repositório digital confiável.

Os resultados obtidos proporcionaram uma visão abrangente sobre os requisitos técnicos, organizacionais e institucionais necessários para a implementação bem-sucedida do RDC-Arq, destacando as dificuldades práticas encontradas pelas instituições. A partir dos passos anteriores, foi proposto um formulário eletrônico que visa ser um instrumento de

avaliação da maturidade dos aspectos institucionais necessários para se ter uma implementação bem-sucedida de um RDC-Arq.

6 RESULTADOS E DISCUSSÃO

A implementação de um Repositório Arquivístico Digital Confiável (RDC-Arq) é um desafio multidimensional que envolve aspectos técnicos, legais e administrativos. O arcabouço normativo que orienta essa implementação no Brasil combina legislação nacional e diretrizes internacionais, visando garantir a autenticidade, integridade, confiabilidade e acessibilidade dos documentos digitais ao longo do tempo.

A Resolução nº 51, de 2023, do (CONARQ), representa um avanço significativo, promovendo a segurança da informação e o acesso à memória institucional. A implementação dos requisitos operacionais e arquivísticos, bem como o cumprimento das obrigações estabelecidas, são fundamentais para a transparência, a eficiência administrativa e a preservação do patrimônio documental.

A Resolução nº 51, do CONARQ, abre uma discussão entre a gestão de documentos digitais e físicos no âmbito da administração pública e de entidades privadas que gerenciam acervos arquivísticos de interesse público. O objetivo é garantir a integridade, a autenticidade, a confiabilidade e o acesso a longo prazo aos documentos. Sendo assim, existem requisitos operacionais e arquivísticos definidos pela resolução, bem como as obrigações de sua implementação.

6.1 REQUISITOS OPERACIONAIS.

Os requisitos operacionais referem-se às condições técnicas e administrativas necessárias para a gestão eficiente dos documentos. Entre eles, destacam-se:

- **Interoperabilidade:** Os sistemas de gestão de documentos devem ser capazes de se comunicar e compartilhar informações entre si, garantindo a integração com outros sistemas institucionais;
- **Segurança da Informação:** Devem ser adotadas medidas de proteção contra acessos não autorizados, perda, corrupção ou destruição de documentos, incluindo criptografia e controle de acesso;
- **Auditabilidade:** Os sistemas precisam permitir o registro de todas as atividades realizadas, com logs de auditoria que garantam a rastreabilidade das ações;

- Escalabilidade e Sustentabilidade: Deve-se considerar a capacidade de expansão dos sistemas e a eficiência no uso de recursos tecnológicos e energéticos.

6.2 REQUISITOS ARQUIVÍSTICOS.

Os requisitos arquivísticos estão relacionados às boas práticas de gestão documental, visando a preservação e o acesso aos registros ao longo do tempo. Entre eles estão:

- Classificação e Avaliação: Os documentos devem ser classificados de acordo com planos de classificação e tabelas de temporalidade, definindo prazos de guarda e destinação final;
- Autenticidade e Integridade: Garantia de que os documentos não sofreram alterações indevidas, mantendo sua originalidade e valor probatório;
- Preservação Digital: Implementação de estratégias para a preservação de documentos digitais, incluindo migração de formatos e armazenamento seguro;
- Acessibilidade: Facilitar o acesso à informação por meio de mecanismos de busca eficientes e adaptados a diferentes públicos.

6.3 OBRIGATORIEDADES DE IMPLEMENTAÇÃO:

A Resolução nº 51 impõe a obrigatoriedade de que as instituições públicas e privadas com acervos de interesse público implementem:

- Políticas de Gestão Documental: Criação de normativas internas que regulamentem os processos de produção, organização, armazenamento e destinação de documentos;
- Capacitação Contínua: Treinamento regular de profissionais para assegurar o cumprimento das boas práticas arquivísticas;
- Adoção de Sistemas Informatizados: Utilização de sistemas eletrônicos de gestão documental que atendam aos requisitos operacionais e arquivísticos estabelecidos;
- Monitoramento e Avaliação: Estabelecimento de mecanismos de controle e auditoria para verificar a conformidade com as diretrizes da resolução.

A implementação de um RDC-Arq exige uma série de segurança técnica, organizacional e legal para garantir sua eficácia e conformidade com os requisitos de

preservação, acessibilidade e integridade dos documentos ao longo do tempo. Os principais aspectos preparatórios para o sucesso de sua implementação podem incluir:

Definição de Objetivos, onde é estabelecido claramente as finalidades do repositório, como preservação de documentos a longo prazo, acessibilidade e segurança da informação, posteriormente um Mapeamento de Requisitos identificando as necessidades específicas da organização ou da comunidade que usará o repositório, incluindo tipos de documentos, volume de dados e requisitos legais ou regulamentares.

Necessário avaliar a escolha da plataforma, selecionar um sistema de gestão de documentos e um Repositório Arquivístico Digital que seja confiável, escalável e compatível com os padrões arquivísticos, verificando a capacidade de armazenamento e a Garanta que haja infraestrutura de armazenamento adequada para suportar o crescimento do repositório ao longo do tempo, considerando o uso de tecnologias como armazenamento em nuvem e soluções de backup. E por fim, a questão da segurança, onde na implementação de medidas de segurança física e digital, como criptografia, autenticação de usuários e controle de acesso para proteger dados sensíveis.

Adoção de Padrões Arquivísticos, utilizando normas reconhecidas, como ISO 14721 (OAIS) para sistemas de preservação de arquivos digitais e ISO 16363 para auditórios de repositórios digitais, para garantir que o repositório esteja em conformidade com os requisitos de confiabilidade e preservação. Definir e adotar esquemas de metadados arquivísticos para garantir a documentação adequada de todos os objetos digitais e suas versões ao longo do tempo. Interoperabilidade e Garantia que o sistema de repositório esteja configurado para ser interoperável com outros repositórios ou sistemas de informação, promovendo o acesso e compartilhamento de dados de maneira eficiente.

Importante definir estratégias para garantir que os arquivos digitais sejam preservados ao longo do tempo, incluindo a migração de formatos obsoletos, controle de integridade e recuperação de desastres, com planos de Backup e Recuperação: estabelecendo um plano robusto de backup e recuperação de dados para evitar perdas em caso de falhas no sistema, implementar práticas de auditoria e monitoramento contínuo para garantir que os documentos armazenados atendam aos requisitos de proteção e integridade e treinamento para os usuários, oferecendo capacitação para os administradores do sistema, técnicos de TI e outros usuários envolvidos na gestão do repositório.

Com a intenção de preparar as instituições que desejam implementar um RDC-Arq, foi desenvolvido um formulário de avaliação para auxiliar no planejamento preliminar da implementação de um RDC-Arq.

As respostas fornecidas permitirão identificar o estágio de desenvolvimento de cada instituição em relação à implementação do RDC-Arq, bem como as condições organizacionais e técnicas que influenciam esse processo. A análise dos dados pode ser organizada em duas seções principais: Requisitos Organizacionais e Requisitos Técnicos.

A primeira parte da pesquisa teve como objetivo principal entender a disposição organizacional das instituições para a implementação do RDC-Arq, considerando uma série de fatores que influenciam diretamente a adoção e o sucesso desse modelo. Entre os aspectos analisados, destacaram-se a identificação da necessidade de implementação, o mapeamento dos setores envolvidos, a alocação de recursos financeiros e humanos necessários para o desenvolvimento do projeto, e a presença de demandas externas que poderiam exercer pressão para a adoção do modelo de repositório digital confiável. Através dessas questões, busca-se avaliar não apenas a vontade das instituições em adotar o RDC-Arq, mas também a preparação organizacional em termos de recursos, estrutura e planejamento estratégico.

A maioria das instituições já tem identificado a necessidade de implementar o RDC-Arq dentro de suas estruturas organizacionais. Esse reconhecimento, embora esperado em muitas organizações que lidam com grandes volumes de dados e documentos digitais, reflete uma crescente conscientização sobre a importância da preservação digital e a urgência de atender aos padrões internacionais de autenticidade e durabilidade dos repositórios digitais. Esse alinhamento estratégico indica que as instituições estão progressivamente cientes dos benefícios e das exigências envolvidas na adoção do RDC-Arq, o que representa um avanço importante para a área da gestão arquivística e digital.

Um alto índice de reconhecimento da necessidade de implementação reflete uma crescente conscientização sobre a importância de garantir a integridade e a acessibilidade dos dados a longo prazo, principalmente em um contexto em que documentos e informações se tornou uma prioridade para muitas organizações. A implementação do RDC-Arq, ao atender a esses requisitos, se apresenta como uma resposta estratégica e necessária para a gestão de repositórios digitais confiáveis. Contudo, algumas instituições ainda reconheceram essa necessidade, o que pode ser resultado de uma falta de compreensão plena sobre os benefícios que o modelo de repositório digital confiável oferece ou sobre a urgência de adotar práticas adequadas de preservação digital. Esse cenário sugere que algumas organizações podem estar subestimando a importância de se adaptar às novas exigências tecnológicas e normativas que regem a preservação de documentos digitais.

Em relação ao mapeamento dos setores envolvidos no formulário, a análise vai revelar uma diferença significativa entre as instituições. Algumas em que grande parte todos setores

participarão do processo, enquanto outras estarão em fase inicial de organização interna. A evidência a diversidade de abordagens adotadas pelas instituições em termos de alocação de responsabilidades e integração de diferentes áreas dentro do processo de preservação digital. A participação de setores como Gestão Documental e Tecnologia da Informação, por exemplo, pode ser mencionada como fundamental para garantir a interoperabilidade e a eficácia do sistema de preservação digital, enquanto outros setores, como Administração e Alta Direção, desempenharam papéis de suporte e decisão estratégica. O mapeamento desses setores é crucial para garantir que todas as áreas envolvidas compreendam suas funções e responsabilidades dentro do projeto, o que facilita a integração e o sucesso da implementação do RDC-Arq.

Observa-se que a maioria das instituições pode indicar a participação da Gestão Documental e da Tecnologia da Informação como setores principais envolvidos na implementação do RDC-Arq. A Gestão Documental certamente será destacada nas instituições como essencial para garantir a conformidade com os padrões arquivísticos exigidos, sendo um setor de grande importância, dado que o RDC-Arq tem como objetivo assegurar a preservação e acessibilidade dos documentos digitais, o que exige práticas de gestão rigorosas e alinhadas às normas internacionais. A participação da Tecnologia da Informação, também é fundamental, já que esse setor é responsável pela infraestrutura tecnológica necessária para a implementação e manutenção do sistema de repositório digital, além de garantir a integração entre os diferentes sistemas da instituição.

A Administração e a Alta Direção são envolvidas no processo de implementação do RDC-Arq, de participação, respectivamente. A presença desses setores na implementação reflete a necessidade de apoio institucional estratégico para o sucesso do projeto. Administração contribui para a alocação de recursos, enquanto a Alta Direção desempenha um papel crucial no processo decisório, garantindo que o projeto receba a atenção necessária em termos de prioridades e recursos, além de promover a adesão e comprometimento com os objetivos do RDC-Arq.

A questão do orçamento e dos recursos humanos destacados para o projeto de implementação do RDC-Arq é essencial para compreender a viabilidade financeira e operacional das instituições. Sem a alocação adequada de recursos financeiros e humanos, a implementação do RDC-Arq poderia enfrentar obstáculos significativos.

Os dados podem revelar que, embora a maioria das instituições tenha destinado recursos humanos para o projeto, um número significativo ainda não havia alocado orçamento específico para a implementação do RDC-Arq. Esse fator pode representar um obstáculo

considerável para o progresso do projeto, dado que a falta de orçamento pode comprometer a infraestrutura necessária para a implementação eficaz do sistema. A falta de recursos financeiros adequados pode resultar na incapacidade de adquirir os equipamentos e softwares necessários, além de afetar a capacitação e treinamento de pessoal, o que, por sua vez, pode retardar ou até inviabilizar a implementação do RDC-Arq em algumas instituições. Portanto, o planejamento orçamentário adequado e a alocação de recursos financeiros são fundamentais para garantir a continuidade e o sucesso do projeto a longo prazo.

A segunda parte do formulário de pesquisa foi dedicada a avaliar os requisitos técnicos essenciais para a implementação do RDC-Arq. Esta seção abordou questões relacionadas à integração de sistemas computacionais existentes, ao tratamento de arquivos físicos, à infraestrutura tecnológica disponível nas instituições e às normativas internas de preservação digital. A implementação de um repositório digital confiável exige não apenas a adequação dos processos e práticas organizacionais, mas também a infraestrutura tecnológica adequada, capaz de suportar a grande quantidade de dados e documentos digitais que serão armazenados, preservados e acessados ao longo do tempo.

A integração de sistemas computacionais existentes ao RDC-Arq é um ponto de destaque na análise feita para as instituições. A capacidade de integrar o RDC-Arq com os sistemas já utilizados pelas organizações é essencial para garantir a interoperabilidade e a eficiência do processo de preservação digital. A integração dos sistemas pode ajudar a otimizar o fluxo de informações, evitar redundâncias e garantir que os dados arquivísticos sejam corretamente armazenados e acessados. Essa integração pode apresentar desafios técnicos significativos, especialmente para instituições que utilizam sistemas legados ou que ainda não possuem infraestrutura suficiente para suportar um repositório digital confiável.

A análise revelará que a grande maioria das instituições já havia mapeado os sistemas que seriam integrados ao RDC-Arq, o que pode demonstrar uma preocupação com a interoperabilidade e a eficiência do processo. Esse mapeamento é essencial para garantir que os dados e documentos arquivísticos possam ser transferidos de forma segura e eficiente entre os sistemas existentes e o novo repositório digital confiável. A integração entre os sistemas é um passo crítico, pois assegura que as informações sejam corretamente armazenadas e acessadas, facilitando o processo de preservação digital a longo prazo. Uma parcela significativa das instituições ainda não tinha realizado esse mapeamento, o que pode indicar um desafio técnico considerável a ser enfrentado para garantir uma integração fluida entre os sistemas. Essa falta de preparação pode acarretar problemas de compatibilidade, que podem

impactar a eficácia do sistema e atrasar a implementação do RDC-Arq, uma vez que a integração de diferentes sistemas exige ajustes técnicos e recursos especializados.

Outro aspecto relevante abordado na pesquisa foi a questão do processamento e a inclusão de arquivos físicos no RDC-Arq, uma vez que muitas instituições ainda lidam com documentos não digitais. A inclusão de arquivos no repositório digital são etapas fundamentais para garantir que todos os documentos e dados relevantes sejam preservados de forma segura e acessível. O processamento de arquivos físicos envolve a transformação de documentos físicos em formatos digitais, processo que pode ser desafiador devido ao volume de documentos a ser digitalizado, à qualidade da digitalização necessária e à adequação dos recursos tecnológicos e humanos para realizar essa tarefa. Além disso, a digitalização deve ser feita de acordo com normas rigorosas de preservação para garantir a integridade e autenticidade dos documentos ao longo do tempo.

As instituições podem afirmar que os arquivos físicos seriam processados e incluídos no RDC-Arq, o que mostra que algumas organizações já estão cientes da necessidade de digitalizar e integrar seus documentos físicos ao novo sistema. No entanto, as instituições ainda precisam planejar ou implementar esse processamento, o que pode indicar desafios relacionados à falta de recursos, a escassez de pessoal qualificado ou a inexistência de um plano detalhado para gerenciar a conversão de documentos físicos em formatos digitais.

Embora os arquivos físicos podem ser processados e submetidos ao RDC-Arq, ainda pode existir uma divisão considerável quanto a esse ponto, as instituições não tendo planejado ou implementado a digitalização de documentos físicos. Esse cenário reflete a complexidade e os desafios envolvidos nesse processo. A digitalização e a preservação de documentos físicos representam obstáculos técnicos significativos, especialmente em termos de custos e tempo necessários para concluir a digitalização de grandes volumes de documentos. O processo de digitalização pode demandar equipamentos especializados, como scanners de alta resolução, e a adoção de tecnologias para garantir a qualidade das imagens e a integridade dos documentos.

A infraestrutura tecnológica é um pilar essencial para garantir que o sistema de repositório digital confiável funcione de maneira eficaz e segura. Para implementar um RDC-Arq, as instituições precisam de servidores adequados, sistemas de backup robustos e um ambiente de rede que suporte o armazenamento e o acesso rápido aos dados. A segurança da informação também se torna um fator importante, uma vez que os repositórios digitais devem estar protegidos contra ataques cibernéticos e falhas que possam comprometer a integridade dos documentos preservados.

Será possível avaliar quais instituições já haviam mapeado a infraestrutura tecnológica necessária para a implementação do RDC-Arq. Esse dado pode indicar que a maioria das organizações já reconhece a importância de dispor de uma infraestrutura robusta para suportar o novo sistema e garantir a preservação de dados digitais a longo prazo. No entanto, algumas instituições ainda podem não ter mapeado a infraestrutura necessária, o que sugere que, para essas organizações, a falta de recursos tecnológicos pode ser um dos principais desafios a ser superado antes da implementação do RDC-Arq. A ausência de um mapeamento claro e adequado pode prejudicar a capacidade das instituições de realizar a implementação de maneira eficiente e segura, podendo resultar em atrasos ou falhas no processo de preservação digital.

A análise dos dados sobre a infraestrutura tecnológica mapeada, pode juntamente com as respostas relacionadas aos normativos internos, permitir concluir que, embora a maioria das instituições esteja avançando na preparação de sua infraestrutura para a implementação do RDC-Arq, ainda existem desafios a serem enfrentados, especialmente em termos de adequação de recursos tecnológicos e na criação de uma base normativa sólida que oriente as práticas de preservação digital. As instituições que ainda não completaram essas etapas devem priorizar a realização desses mapeamentos e a implementação de políticas internas claras para garantir a efetividade e a longevidade de seus repositórios digitais confiáveis.

Ao analisar os dados obtidos nesta pesquisa, é possível estabelecer uma comparação com os estudos realizados por outros autores sobre a implementação e os desafios da preservação digital em repositórios arquivísticos. O diagnóstico situacional feito por Almeida e Araújo (2022), que investigaram a preservação dos arquivos nato-digitais no Centro de Empreendedorismo da UFS, trouxe à tona a importância do planejamento prévio e da estrutura organizacional para o sucesso da implementação de repositórios digitais. De maneira semelhante, as respostas obtidas nesta pesquisa podem destacar que, apesar do avanço em algumas instituições, ainda existem obstáculos consideráveis relacionados à alocação de recursos financeiros e humanos, assim como o mapeamento adequado da infraestrutura tecnológica necessária para a implementação do RDC-Arq. A falta de um orçamento específico, observada nas instituições, é uma preocupação que também foi apontada por Faria e Silva (2020) como um desafio significativo em seus estudos sobre os custos envolvidos na preservação digital no Arquivo Nacional do Brasil.

Outro estudo relevante é o de Andrade e Chagas (2021), que propuseram o aperfeiçoamento do modelo conceitual do RDC-Arq para auditoria e certificação, comparando-o com o modelo TRAC (Trustworthy Repositories Audit & Certification). Os

resultados da pesquisa podem indicar que a maioria das instituições já havia planejado a integração de sistemas computacionais, mas ainda existem desafios técnicos para garantir essa integração de forma fluida e sem interrupções. A preocupação com a interoperabilidade entre os sistemas e a adequação da infraestrutura tecnológica, identificada nas instituições nesta pesquisa, também foi discutida por Braga (2021), que ressaltou a importância da integração eficaz para a implementação de repositórios digitais confiáveis no Brasil. Em seu estudo, Braga apontou que as dificuldades enfrentadas pelas instituições no que se refere à infraestrutura e à integração de tecnologias legadas são comuns, o que reforça a necessidade de soluções adequadas para a integração de sistemas e de investimentos substanciais em recursos tecnológicos.

A questão do processamento de arquivos físicos foi abordada de forma similar por Chaves (2023), que analisou a preservação de documentos arquivísticos digitais a longo prazo. Embora uma parcela das instituições participantes desta pesquisa, pode afirmar que os arquivos físicos seriam processados e submetidos ao RDC-Arq, a divisão significativa sobre essa questão demonstra a complexidade do processo de digitalização e a resistência de algumas instituições em lidar com os custos e o tempo necessários para a conversão de documentos físicos em formatos digitais. Chaves também destaca a importância da digitalização para garantir a preservação a longo prazo, uma vez que muitos documentos físicos ainda são essenciais para as coleções arquivísticas.

O estudo de Pignataro *et al.* (2023), que trata da gestão dos formatos de preservação de arquivos no Archivematica, ilustra a relevância da implementação de padrões de metadados para garantir a preservação de documentos digitais. Na mesma linha, a pesquisa realizada nesta dissertação identificou que muitas instituições talvez ainda não haviam implementado uma estrutura adequada de metadados e descrição de seus acervos digitais, o que pode afetar a acessibilidade e a durabilidade desses documentos no longo prazo. Esse desafio de implementar normas e padrões para a preservação digital foi discutido por Gava e Flores (2021), que enfatizaram a necessidade de uma abordagem sistêmica para a preservação digital, onde as tecnologias e os processos de gestão de arquivos digitais devem ser integrados de maneira eficiente para garantir a confiabilidade e a segurança das informações.

A comparação com o trabalho de Santos e Flores (2020), que analisaram a infraestrutura organizacional necessária para repositórios arquivísticos digitais confiáveis à luz da ISO 16363, revela que as instituições brasileiras ainda enfrentam desafios em termos de adaptação às normas e diretrizes internacionais de preservação digital. Embora a maioria das instituições participantes desta pesquisa tenha reconhecido a importância de uma

infraestrutura adequada, grande parte ainda não ter mapeado essa infraestrutura, refletindo a necessidade urgente de investimentos e de planejamento estratégico para garantir a conformidade com as melhores práticas globais.

A proposta de auditoria e certificação de repositórios arquivísticos digitais confiáveis, discutida por Flores (2021), também se alinha com as dificuldades enfrentadas pelas instituições investigadas nesta pesquisa. A falta de recursos e a ausência de um planejamento adequado para a implementação dos modelos propostos, como o RDC-Arq, podem comprometer a capacidade de certificar esses repositórios e garantir sua conformidade com os padrões de preservação digital exigidos.

No contexto da preservação sistêmica, como abordado por Gava e Flores (2021), é possível observar que as respostas desta pesquisa corroboram a necessidade de uma abordagem holística para a preservação digital. A falta de uma visão sistêmica da preservação, que envolva todos os setores da instituição, como apontado por Santos e Mazuco (2020), pode prejudicar a implementação de repositórios arquivísticos digitais confiáveis. A integração entre a gestão documental, a tecnologia da informação e a alta direção é essencial para garantir que o processo de preservação digital seja eficaz e sustentável a longo prazo.

O estudo de Gava e Flores (2020) sobre os repositórios arquivísticos digitais confiáveis como plataforma de preservação digital em um ambiente de gestão arquivística é um reflexo das descobertas desta pesquisa, que identificaram que muitas instituições ainda estão em estágio inicial de implementação do RDC-Arq. A necessidade de uma plataforma robusta e integrada para garantir a preservação digital e a gestão dos acervos arquivísticos foi destacada em grande parte das respostas, e o estudo de Gava e Flores enfatiza a importância de uma gestão integrada que envolva tanto aspectos tecnológicos quanto organizacionais para garantir o sucesso a longo prazo de projetos de preservação digital.

Essas comparações demonstram que, embora haja um crescente movimento em direção à implementação de repositórios digitais confiáveis no Brasil, as instituições ainda enfrentam desafios significativos, tanto em termos de recursos financeiros e humanos quanto em relação à infraestrutura tecnológica e à integração de sistemas. O formulário de pesquisa vai assessorar e evidenciar a necessidade de uma abordagem mais coordenada e estratégica, que envolva todos os setores da instituição e esteja alinhada às melhores práticas e diretrizes internacionais, como as propostas por autores renomados na área da preservação digital.

6.4 CONSULTA AO IBICT:

Após consulta institucional ao IBICT, responsável direto pela implementação do modelo Hipátia, foi possível identificar a necessidade de criação do formulário eletrônico. Esse formulário tem o objetivo de servir como um instrumento de avaliação da maturidade dos aspectos institucionais essenciais para uma implementação bem-sucedida de uma RDC-Arq. Com base na documentação comprovada, foram destacados os aspectos centrais que influenciam a capacidade das instituições de se prepararem para a implantação de um repositório digital compatível com os padrões exigidos para a preservação a longo prazo.

Após consulta ao IBICT, foi estabelecido que seria desenvolvida uma ferramenta denominada Formulário para Mapeamento de Requisitos que Antecedem a Implementação de um RDC-Arq. O objetivo dessa ferramenta é atender instituições interessadas na implementação de um Repositório Digital Confiável Arquivístico (RDC-Arq), mas que ainda não possuem um direcionamento claro sobre como desenvolver o projeto.

Essas instituições geralmente têm um conhecimento mínimo sobre a legislação vigente e estão cientes das possibilidades de facilitação oferecidas pelo Hipatia. No entanto, enfrentam desafios para identificar os requisitos necessários e os passos iniciais antes de dar início à implementação do RDC-Arq.

7 CONCLUSÃO

Dessa forma, o formulário busca orientar essas organizações, fornecendo um diagnóstico prévio e estruturado, permitindo que compreendam melhor as exigências legais, técnicas e operacionais envolvidas no processo. Isso contribui para a construção de um plano mais sólido e eficaz para a implementação do RDC-Arq, reduzindo incertezas e aumentando as chances de sucesso do projeto.

Existe um conjunto extenso de normativos e legislações que regulamentam a implementação de um Repositório Digital Confiável Arquivístico (RDC-Arq), incluindo a Resolução nº 51 do CONARQ, que estabelece diretrizes para sua adoção. No entanto, muitas instituições enfrentam dificuldades para compreender e aplicar esses requisitos na prática, especialmente na fase inicial do processo.

Diante desse cenário, estou desenvolvendo uma ferramenta que tem como objetivo auxiliar as instituições na preparação para a implementação do RDC-Arq. Essa ferramenta servirá como um guia estruturado, permitindo que as organizações avaliem seu nível de maturidade em relação às exigências normativas, identifiquem lacunas e planejem as ações necessárias antes de dar início ao projeto.

Ao oferecer uma abordagem organizada e acessível, essa solução busca facilitar o entendimento das exigências legais e técnicas, promovendo uma transição mais eficiente e segura para o modelo de repositório digital confiável. Dessa forma, a ferramenta se tornará um recurso estratégico para as instituições que precisam iniciar os trabalhos de implementação do RDC-Arq, garantindo maior conformidade e sucesso no processo.

Os resultados obtidos podem indicar que, embora a maioria das instituições participantes já tenha identificado a necessidade e os setores envolvidos na implementação do RDC-Arq, existem desafios consideráveis no que diz respeito ao orçamento, recursos humanos, infraestrutura tecnológica e integração de sistemas. A falta de normativas internas sobre preservação digital e a ausência de um planejamento detalhado para o processamento de arquivos físicos também representam obstáculos importantes para a implementação efetiva do RDC-Arq.

Conclusão deste estudo reafirma a importância da criação e implementação de um RDC-Arq em um contexto onde a transformação digital intensifica a dependência de registros eletrônicos. A crescente produção de dados digitais em setores críticos, como o governamental, jurídico, educacional e de saúde, torna imperativa a adoção de mecanismos

capazes de garantir a integridade, autenticidade e acessibilidade desses documentos ao longo do tempo. Observa-se que a preservação de documentos digitais não se limita a uma questão de adequação tecnológica, mas envolve um compromisso institucional e social com a proteção da memória documental e a transparência nos processos de gestão.

A adoção de um RDC-Arq está diretamente associada à capacidade das instituições de lidar com os desafios impostos pela natureza volátil dos documentos digitais. Diferente dos documentos físicos, que possuem uma durabilidade intrínseca e são acessíveis independentemente de recursos tecnológicos, os documentos digitais dependem de uma infraestrutura complexa e de constante atualização para evitar a obsolescência e garantir a preservação. A análise revelou que a implementação de um RDC-Arq permite a criação de uma estrutura sólida e normativa para a preservação digital, proporcionando um ambiente seguro para que os documentos arquivísticos sejam mantidos com integridade e autenticidade reconhecíveis, como estabelecido em diretrizes internacionais, incluindo a norma ISO 16363.

Com a introdução de normativas como a Lei de Acesso à Informação (LAI) no Brasil e a General Data Protection Regulation (GDPR) na União Europeia, as demandas legais para a preservação de documentos arquivísticos digitais se tornam ainda mais prementes. Esses dispositivos legais não apenas asseguram o direito dos cidadãos ao acesso à informação, mas também exigem das instituições uma política de preservação documental que garanta a autenticidade e confiabilidade dos registros mantidos. O RDC-Arq possibilita o cumprimento dessas obrigações ao assegurar que os documentos digitais não sejam alterados ou corrompidos com o tempo, promovendo a confiança no acervo institucional e a transparência nas relações entre governo, cidadãos e instituições.

O processo de implementação de um RDC-Arq envolve tanto o investimento em tecnologia quanto a capacitação de profissionais qualificados. A integração de recursos humanos especializados, com conhecimentos que vão desde a arquivística digital até a segurança cibernética, se mostra indispensável para o sucesso de um RDC-Arq. Somente com uma equipe treinada e capaz de compreender as nuances dos documentos digitais é possível garantir que os processos de preservação e manutenção do repositório ocorram de forma eficaz e estejam em conformidade com as normas de preservação. Tal demanda evidencia que a preservação digital confiável não é uma ação isolada, mas um processo contínuo que exige planejamento, atualização tecnológica e comprometimento institucional.

A implementação de sistemas de backup, redundância de dados e controles rigorosos de acesso são componentes fundamentais de um RDC-Arq, uma vez que evitam a perda de dados e a adulteração dos documentos preservados. Esses elementos facilitam o intercâmbio e

a interoperabilidade dos documentos entre diferentes plataformas e instituições, promovendo a criação de um ecossistema de preservação digital mais coeso e eficiente. O desenvolvimento de RDC-Arqs contribui para uma cultura de preservação digital que prioriza a integridade e autenticidade dos documentos arquivísticos em longo prazo. Ao criar uma estrutura normativa e tecnológica para a preservação dos documentos digitais, as instituições estão melhor preparadas para enfrentar os riscos associados à perda e adulteração de informações críticas. Um RDC-Arq fortalece a governança documental, garantindo que os documentos digitais sejam gerenciados e mantidos conforme os padrões legais e éticos que norteiam o setor.

A implementação de um RDC-Arq não se limita a uma medida técnica ou regulatória, mas representa uma estratégia institucional que promove a segurança, autenticidade e acessibilidade da informação arquivística digital. Ao adotar um repositório digital confiável, as instituições protegem seu patrimônio documental, cumprem com suas obrigações legais e estabelecem uma relação de confiança com a sociedade, assegurando que a memória e o conhecimento registrados em documentos digitais estejam disponíveis para futuras gerações e que continuem a servir como fontes de prova e evidência, consolidando-se como ferramentas essenciais para a transparência e eficiência organizacional.

REFERÊNCIAS

ALMEIDA, Maurício Barcellos. Uma introdução ao XML, sua utilização na internet e alguns conceitos complementares. **Ciência da Informação**, Brasília, v. 31, n. 2, p. 5-13, maio/ago. 2002.

ALMEIDA, Valdemir; ARAÚJO, Alessandra. Preservação dos arquivos nato-digitais do Centro de Empreendedorismo da UFS: diagnóstico situacional. **Revista Brasileira de Educação em Ciência da Informação**, v. 9, n. especial, p. 1-17, 2022.

AMERICAN LIBRARY ASSOCIATION. **Definitions of digital preservation**. 2007. Disponível em: <http://www.lita.org/ala/mgrps/divs/alcts/resources/preserv/defdigpres0408.cfm>. Acesso em: 06 fev. 2025.

ANDRADE, Fábio Lopes; CHAGAS, Cintia Aparecida. Proposta de aperfeiçoamento do modelo conceitual para Repositórios Arquivísticos Digitais Confiáveis (RDC-Arq) para auditoria e certificação a partir da comparação com o modelo de critérios Trustworthy Repositories Audit & Certification: Criteria and Checklist (TRAC). **ÁGORA: Arquivologia em debate**, v. 31, n. 63, p. 1-19, 2021.

BELLOTTO, Heloísa Liberalli; CAMARGO, Ana Maria de Almeida (Coord.). **Dicionário de terminologia arquivística**. São Paulo: Associação dos Arquivistas Brasileiros – Núcleo Regional de São Paulo; Secretaria de Estado da Cultura, 1996.

BELLOTTO, Heloísa Liberalli. **Arquivística: objetos, princípios e rumos**. São Paulo: Associação de Arquivistas de São Paulo, 2002.

BRAGA, Tiago Emmanuel Nunes. Hipátia: a proposta do IBICT para o RDC-Arq. **Seminário Internacional de Preservação Digital**, n. 5, 2021.

BRAGA, Tiago Emmanuel Nunes. O Modelo Hipátia: a proposta do IBICT para implementação de RDC-ARQ no Brasil. **Tendências da Pesquisa Brasileira em Ciência da Informação**, v. 16, 2023.

BRAGA, Tiago Emmanuel Nunes; HOLANDA, Alex Pereira; PIGNATARO, Tatiana Canelhas. Resolução RDC-Arq Conarq: uma análise dos novos requisitos informacionais propostos. **Revista Brasileira de Preservação Digital**, v. 3, p. e022004-e022004, 2022.

BRASIL. Resolução nº 51, de 25 de agosto de 2023. Dispõe sobre as Diretrizes para a Implementação de Repositórios Arquivísticos Digitais Confiáveis, Versão 2. Disponível em: <https://www.gov.br/conarq/pt-br/legislacao-arquivistica/resolucoes-do-conarq/resolucao-conarq-no-51-de-25-de-agosto-de-2023>. Acesso em: 5 fev. 2025.

CABRAL, Jacqueline Ribeiro; PEREIRA, Igor Muniz. Notas sobre o direito à memória no ambiente digital e sua relação com os arquivos. **Revista Brasileira de Educação em Ciência da Informação**, v. 8, 2021.

CHAVES, Elisa Maria Lopes. Preservação de documentos arquivísticos digitais a longo prazo em repositórios digitais confiáveis. **Revista Ibero-Americana de Ciência da Informação**, v. 16, n. 1, p. 50-66, 2023.

CONSELHO NACIONAL DE ARQUIVOS. Câmara Técnica de Documentos Eletrônicos. **Modelo de requisitos para sistemas informatizados de gestão arquivística de documentos: e-ARQ** Brasil. Dez. 2009. Versão 1.1. Disponível em: <http://www.conarq.arquivonacional.gov.br/media/publicacoes/earqmet/earqbrasilv1.1.pdf>. Acesso em: 06 fevereiro 2025.

CONSELHO NACIONAL DE DESENVOLVIMENTO CIENTÍFICO E TECNOLÓGICO. **Política Nacional de Memória da Ciência e da Tecnologia**: relatório da Comissão Especial constituída pela Portaria 116/2003 do Presidente do CNPq em 04 de julho de 2003. Set. 2003. Disponível em: <http://ghc.ifi.unicamp.br/SBHC/Memoria-CT.pdf>. Acesso em: 06 fevereiro 2025.

DE ANDRADE, Fabio Lopes; CHAGAS, Cintia Aparecida. Repositórios digitais confiáveis: a verificação de compatibilidade entre modelos internacionais de critérios de preservação digital no longo prazo e o RDC-Arq. **ÁGORA: Arquivologia em debate**, v. 33, n. 66, p. 1-22, 2023.

FARIA, Maximiliano Martins; DA SILVA, Tiago Cesar. Estudos de custos para preservação digital e repositório digital confiável: o caso do Arquivo Nacional do Brasil. **Revista Brasileira de Preservação Digital**, v. 5, p. e024002-e024002.

FLORES, Daniel. Auditoria e Certificação de SGD, RDC-Arq e Plataformas de Transparência Ativa em Arquivos: CCDA Plena. **Seminário Internacional de Preservação Digital**, n. 5, p. 35-35, 2021.

GAVA, Tânia Barbosa Salles; FLORES, Daniel. Auditoria e certificação ao longo da cadeia de custódia digital arquivística. **Informação & Informação**, v. 26, n. 4, p. 424-449, 2021.

GAVA, Tânia Barbosa Salles; FLORES, Daniel. Preservação digital sistêmica. **ARQUIVO, DOCUMENTO E INFORMAÇÃO EM CENÁRIOS HÍBRIDOS: anais do Simpósio Internacional de Arquivos. Anais [...]** São Paulo: Eventus, 2021.

GAVA, Tânia Barbosa Salles; FLORES, Daniel. Repositórios arquivísticos digitais confiáveis (RDC-Arq) como plataforma de preservação digital em um ambiente de gestão arquivística. **Informação & Informação**, v. 25, n. 2, p. 74-99, 2020.

MORAES, Margarete Farias. Segurança, privacidade e confidencialidade dos registros em saúde. **Informação em Pauta**, v. 5, n. 1, p. 23-35, 2020.

MORI, Alexandre *et al.* Um paralelo entre a tecnologia blockchain e os requisitos do RDC-Arq. **Ibersid: revista de sistemas de información y documentación**, v. 14, n. 1, p. 29-40, 2020.

PIGNATARO, Tatiana Canelhas *et al.* A gestão dos formatos de preservação de arquivos no Archivematica: estudo de caso com o Processo Judicial Eletrônico. In: **Anais do Workshop de Informação, Dados e Tecnologia-WIDaT**. 2023.

PIRES, Cassio Felipe de Oliveira; LINDEN, Leolibia Luana. Análise de elementos descritivos e padrões de metadados em plataformas de descrição, acesso e difusão de acervos digitais. In: **Workshop de Informação, Dados e Tecnologia (6.: 2023: Brasília, DF). Anais**.

Brasília: MCTI; IBICT/RNP. 2023.

SANTOS, Henrique Machado; FANTINEL, Elisângela Gorete; FLORES, Daniel. Requisitos para plataformas arquivísticas de acesso e difusão. **ÁGORA: Arquivologia em debate**, v. 33, n. 66, p. 1-24, 2023.

SANTOS, Henrique Machado; FLORES, Daniel. Infraestrutura organizacional necessária ao repositório arquivístico digital confiável: um diálogo com a ISO 16363. **Revista Brasileira de Biblioteconomia e Documentação**, v. 16, p. 1-29, 2020.

SANTOS, Henrique Machado; FLORES, Daniel. Preservação sistêmica para repositórios arquivísticos. **Revista Eletrônica de Comunicação, Informação & Inovação em Saúde**, v. 14, n. 3, 2020.

SANTOS, Henrique Machado; FLORES, Daniel. Transformações dos Pacotes de Informação na Cadeia de Custódia Digital Arquivística. **Páginas a&b: arquivos e bibliotecas**, p. 18-35, 2022.

SANTOS, Henrique Machado; MAZUCO, Fabiana Ciocheta; FLORES, Daniel. Preservação sistêmica de documentos arquivísticos digitais: uma perspectiva holística. **PerCursos**, v. 21, n. 46, p. 244-271, 2020.

SANTOS, Vanderlei Batista. Preservação digital de documentos arquivísticos potenciais: reconhecendo e enfrentando o problema. **Revista Brasileira de Preservação Digital**, v. 3, p. e022005-e022005, 2022.

SHINTAKU, Milton *et al.* Uso do protocolo de interoperabilidade OAI-ORE para preservação digital. **Revista Brasileira de Preservação Digital**, v. 4, p. e023012-e023012, 2023.

SHINTAKU, Milton; BRAGA, Tiago Emmanuel Nunes; DE FARIA OLIVEIRA, Alexadre. Hipátia: uma ferramenta livre no apoio à preservação digital. **Revista Brasileira de Preservação Digital**, v. 2, p. e021006-e021006, 2021.

SILVA, Ney Lúcio da; PARRELA, Ivana Denise. Preservação, gerenciamento e governança arquivísticos na Justiça Eleitoral de Minas Gerais. **Em Questão**, v. 29, p. e-128008, 2023.

APÊNDICE A

FORMULÁRIO PARA MAPEAMENTO DE REQUISITOS QUE ANTECEDEM A IMPLEMENTAÇÃO DE UM RDC-ARQ

SEÇÃO 1: CARACTERIZAÇÃO DO RESPONDENTE

Nome da Instituição:

Pessoa responsável por responder o questionário:

Sector(es) responsável por responder o questionário:

Data de Preenchimento:

Telefone de contato:

E-mail de contato:

SEÇÃO 2: REQUISITOS ORGANIZACIONAIS

1. **A Instituição já identificou a necessidade de implementar um RDC-Arq no âmbito organizacional?**

- ☐ () Sim
- ☐ () Não

Se a resposta para a pergunta anterior for **não**, pode finalizar o preenchimento do formulário.

2. **Já foram mapeados os setores que estarão envolvidos no processo de implementação de um RDC-Arq?**

- ☐ () Sim
- ☐ () Não

3. **Se a resposta ao item 2 foi SIM, quais são esses setores?**

- ☐ [] Gestão documental
- ☐ [] Tecnologia da Informação
- ☐ [] Administração
- ☐ [] Áreas de negócio
- ☐ [] Alta direção
- ☐ [] Outros: _____

4. **Se a resposta ao item 2 foi NÃO, há algum setor específico fazendo este levantamento?**

- ☐ _____

5. **Há demanda externa que imponha a implementação do RDC-Arq?**

- ☐ () Sim
- ☐ () Não

6. **Há orçamento destacado para o projeto de implementação do RDC-Arq?**

- ☐ () Sim
- ☐ () Não

7. **Há recurso humano destacado para o projeto de implementação do RDC-Arq?**

- ☐ () Sim

- () Não

SEÇÃO 3: REQUISITOS TÉCNICOS

1. **Foram mapeados os sistemas computacionais que serão integrados ao RDC-ARq?**
 - () Sim
 - () Não
2. **Os arquivos físicos serão processados e submetidos ao RDC-ARq?**
 - () Sim
 - () Não
3. **Foi mapeada a infraestrutura tecnológica a ser destacada para implementação do RDC-ARq?**
 - () Sim
 - () Não
4. **Existem normativos internos que tratem do tema de preservação digital?**
 - () Sim
 - () Não
5. **A Instituição possui sistemas de gestão documental?**
 - () Sim
 - () Não