

ANEXO VII – REQUISITOS OBRIGATÓRIOS PARA SISTEMAS INFORMATIZADOS DE GESTÃO ARQUIVÍSTICA DE DOCUMENTOS (SIGAD) E REQUISITOS PARA UM REPOSITÓRIO DIGITAL CONFIÁVEL (RDC-Arq).

Os requisitos mínimos e obrigatórios de um SIGAD são aqueles critérios mínimos para garantir a produção, manutenção e preservação de documentos arquivísticos autênticos, confiáveis, precisos e acessíveis, fundamentais para o funcionamento das seis operações propostas pelo e-ARQ Brasil. Sendo assim, aplicando-se esses critérios, selecionaram-se os quarenta requisitos mínimos e obrigatórios a seguir:

Aspectos de funcionalidade	Requisitos mínimos e obrigatórios
1 Organização dos documentos arquivísticos: plano de classificação e manutenção dos documentos	1.1 Configuração e administração do plano de classificação no Sigad
	1.2 Classificação e metadados das unidades de arquivamento
	1.3 Gerenciamento dos dossiês/processos
	1.4 Requisitos adicionais para o gerenciamento de processos
	1.5 Volumes: abertura, encerramento e metadados
	1.6 Gerenciamento de documentos e processos/dossiês arquivísticos convencionais e híbridos
2 Tramitação e fluxo de trabalho	2.1 Controle do fluxo de trabalho
	2.2 Controle de versões e do status do documento
3 Captura	3.1 Procedimentos gerais
	3.2 Captura em lote
	3.3 Captura de mensagens de correio eletrônico

Aspectos de funcionalidade	Requisitos mínimos e obrigatórios
	3.4 Captura de documentos convencionais ou híbridos
	3.5 Formato de arquivo e estrutura dos documentos a serem capturados
	3.6 Estrutura dos procedimentos de gestão
4 Avaliação e destinação	4.1 Configuração da tabela de temporalidade e destinação de documentos
	4.2 Aplicação da tabela de temporalidade e destinação de documentos
	4.3 Exportação de documentos
	4.4 Eliminação
	4.5 Avaliação e destinação de documentos arquivísticos convencionais e híbridos
5 Pesquisa, localização e apresentação dos documentos	5.1 Aspectos gerais
	5.2 Pesquisa e localização
	5.3 Apresentação: visualização, impressão, emissão de som
6 Segurança	6.1 Cópias de segurança
	6.2 Controle de acesso
	6.3 Classificação da informação quanto ao grau de sigilo e restrição de acesso à informação sensível
	6.4 Trilhas de auditoria

Aspectos de funcionalidade	Requisitos mínimos e obrigatórios
	6.5 Assinaturas digitais
	6.6 Criptografia
	6.7 Marcas d'água digitais
	6.8 Acompanhamento de transferência
	6.9 Autoproteção
	6.10 Alterar, apagar e truncar documentos arquivísticos digitais
7 Armazenamento (itens de infra de TI)	7.1 Durabilidade
	7.2 Capacidade
	7.3 Efetividade de armazenamento
8 Preservação	8.1 Aspectos físicos
	8.2 Aspectos lógicos
	8.3 Aspectos gerais
9 Funções administrativas	
10 Usabilidade	

REQUISITOS PARA UM REPOSITÓRIO DIGITAL CONFIÁVEL: Os requisitos apresentados a seguir estão definidos em nível conceitual e devem ser cumpridos no desenvolvimento de um repositório digital confiável. Reitere-se que esses requisitos estão baseados na norma ISO 16363: 2012, e abrangem todos os tipos de materiais digitais, inclusive os documentos arquivísticos. Os requisitos estão organizados em três conjuntos: infraestrutura organizacional; gerenciamento do documento digital; e tecnologia, infraestrutura técnica e segurança.

Infraestrutura organizacional: O ambiente em que o repositório digital vai se estabelecer tem que cumprir determinados requisitos, conforme descrito a seguir.

a. Governança e viabilidade organizacional- O repositório tem como missão o compromisso com a preservação, o gerenciamento e o acesso de longo prazo dos documentos digitais. Essa missão é claramente identificada por todos os interessados no repositório e envolve: mandato legal, contexto organizacional e requisitos regulatórios. O repositório tem um plano de sucessão formal, planos de contingência e/ou acordos estabelecidos para garantir a continuidade do serviço, no caso de o repositório parar de operar ou de a instituição responsável e/ou financiadora mudar seu escopo.

b. Estrutura organizacional e de pessoal - O repositório tem uma equipe dotada de qualificação e formação necessárias, e em número suficiente, para garantir todos os serviços e funcionalidades pertinentes ao repositório. Além disso, deve manter um programa de desenvolvimento profissional contínuo.

c. Transparência de procedimentos e arcabouço político - O repositório deve demonstrar explicitamente seus requisitos, decisões, desenvolvimento e ações que garantem a preservação de longo prazo e o acesso a conteúdos digitais sob seus cuidados. Dessa forma, assegura aos usuários, gestores, produtores e certificadores que está cumprindo plenamente seu papel enquanto um repositório digital confiável. Para tanto, o repositório deve:

- definir a comunidade alvo e sua base de conhecimento;
- possuir políticas e definições, acessíveis publicamente, que demonstrem como os requisitos do serviço de preservação serão contemplados;
- possuir políticas, procedimentos e mecanismos de atualização, na medida em que o repositório cresce e a tecnologia e práticas da comunidade evoluem;
- documentar permissões legais – por meio de acordos de custódia, normas de procedimentos e outros – que o isentem de responsabilidade, no caso de alterações passíveis de ocorrer em estratégias de preservação digital;
- fazer o registro histórico das mudanças de procedimentos, de software e hardware;
- relacionar o registro histórico, acima referido, com as estratégias de preservação digital, e descrever os potenciais efeitos dessas mudanças sobre os documentos digitais;
- demonstrar que está sistematicamente avaliando a satisfação das expectativas dos 13 CONARQ - Implementação de Repositórios Arquivísticos Digitais Confiáveis – RDC-Arq / 2015 produtores e dos usuários, e buscando atendê-las;
- estar comprometido com a definição, coleta, auditoria e fornecimento (sob demanda) de mecanismos de controle da integridade dos documentos digitais sob sua custódia;

- estar comprometido em realizar regularmente uma autoavaliação de seu funcionamento e renovar sua certificação; e

- estar comprometido em notificar as entidades certificadoras sobre as mudanças operacionais que afetarão seu status de certificação (no caso de repositórios já certificados).

d. Sustentabilidade financeira: Um repositório digital confiável deve demonstrar sustentabilidade financeira. Para isso, deve ter um plano de gestão que observe os seguintes aspectos:

- demonstração da capacidade de obter recursos financeiros estáveis e contínuos para sustentá-lo, seja por meio de prestação de serviço, parcerias, doações, verba da própria instituição, dentre outros;

- revisão e ajustes anuais;

- transparência dos procedimentos para obtenção dos recursos e auditoria dos mesmos, de acordo com o sistema jurídico no qual o repositório se insere; e

- compromisso dos ciclos de planejamento com o equilíbrio dos riscos, benefícios, investimentos e gastos.

e. Contratos, licenças e passivos: Os contratos, licenças e passivos firmados pelo repositório devem ser claros e mensuráveis; delinear papéis, responsabilidades, prazos e condições; e ser facilmente acessíveis ou disponíveis aos interessados. Esses contratos, licenças e passivos podem envolver tanto a relação entre o repositório e os produtores de documentos digitais, como a relação entre o repositório e fornecedores de serviços. Esses mesmos instrumentos devem especificar todos os direitos e obrigações do repositório sobre os documentos digitais a ele confiados, em especial no que diz respeito à propriedade intelectual e a restrições de uso.

Gerenciamento do documento digital: O gerenciamento dos documentos de um repositório digital confiável deve estar de acordo com o modelo de referência OAIS, que estabelece a formação de pacotes de informação envolvendo os documentos digitais (informação de conteúdo) e seus metadados (informação de representação). São três os tipos de pacotes de informação:

- Pacote de informação para submissão (submission information package – SIP) – refere-se à admissão dos documentos digitais e seus metadados associados.

- Pacote de informação para arquivamento (archival information package – AIP) – refere-se ao acondicionamento e armazenamento dos documentos digitais e seus metadados associados.

- Pacote de informação para disseminação (dissemination information package – DIP) – refere-se ao acesso aos documentos digitais e seus metadados associados.

TRAC apresenta os requisitos para gerenciamento do documento no repositório digital, categorizados em seis grupos, com base nas funcionalidades, conforme detalhado a seguir:

a. Admissão: captura de documentos digitais A admissão consiste na entrada dos documentos e seus metadados no repositório digital. Os requisitos de admissão variam dependendo do tipo de material, do contexto legal e da relação entre o produtor de documento e o repositório. Independentemente dessas variações, pode-se afirmar que a admissão se inicia com o recebimento de um SIP, que é convertido em AIP, e termina quando um AIP está seguro no repositório, incluindo a criação de cópias de segurança. A seguir, apresentam-se requisitos gerais a serem cumpridos pelo repositório, cuja adequação deve ser avaliada de acordo com a missão e as necessidades de cada repositório:

- identificar as propriedades do documento que serão preservadas (ex.: o conteúdo, layout, tabela de cor, resolução da imagem, canais de som etc.);
- especificar claramente a informação que deve estar associada ao documento (metadados associados) no momento da sua submissão;
- ter mecanismos para autenticar a origem dos documentos que estão sendo admitidos no repositório, de forma a garantir sua proveniência;
- ter procedimentos para verificar a integridade do SIP, o que pode ser feito por meio de procedimentos automatizados e/ou checagem humana;
- ter o controle físico (controle completo dos bits) dos documentos transmitidos com cada SIP, a fim de preservá-los;
- fornecer ao produtor/depositante relatórios do andamento dos procedimentos durante todo o processo de admissão;
- demonstrar em que momento a responsabilidade pela preservação do documento submetido (SIP) é formalmente aceita pelo repositório; e
- ter registros de todas as ações e processos administrativos que ocorrem durante o processo de admissão e são relevantes para a preservação.

OBS: No caso de um repositório para documentos arquivísticos, a definição dos metadados deve observar o e-ARQ Brasil (nas fases corrente e intermediária) e a NOBRADE (na fase permanente). Para a admissão de documentos no repositório, no caso de transferência ou recolhimento, devem-se observar os procedimentos indicados na Resolução nº 24, de 3 de agosto de 2006, do CONARQ.

b. Admissão: criação do pacote de arquivamento - O repositório deve completar o processo de admissão, criando um pacote de informação apropriado para arquivamento (AIP), com toda a informação recebida do produtor. A fim de garantir que o pacote de

informação recebido do produtor, e verificado pelo repositório, seja convertido para o formato de arquivamento (AIP) e armazenado para preservação de longo prazo, um repositório deve atender os seguintes requisitos

- descrever cada classe de informação (texto estruturado, imagem matricial, banco de dados, imagem em movimento e outras) a ser preservada pelo repositório, e como ela está implementada – essa descrição deve apontar os componentes-chave do AIP: o documento arquivístico, sua informação de representação (informação estrutural e semântica) e as várias categorias de informação descritiva de preservação (fixidade, proveniência e contexto), e ainda como esses componentes se relacionam;

- descrever minuciosamente as diferentes classes de informação e como os AIPs são implementados, nos casos em que a especificidade daquelas classes exigir ações de preservação diferentes (por exemplo, a imagem TIFF que é processada por um sistema pode necessitar de ações de preservação diferentes das ações necessárias à imagem TIFF que é apresentada para o olho humano);

- descrever como os AIPs são construídos a partir dos SIPs, ou seja, apontar todas as transformações pelas quais passarão os documentos e os metadados submetidos, e os metadados a serem adicionados no momento da formação do AIP;

- ser capaz de demonstrar se os SIPs foram aceitos e transformados em um AIP integralmente ou em parte, ou ainda se foram recusados;

- atribuir aos AIPs, identificadores que sejam únicos, persistentes e visíveis aos gestores e auditores, de acordo com padrões reconhecidos (por exemplo: Handle System, DOI, URN, PURL);

- no caso de o documento já possuir um identificador único, a ele atribuído no SIP, o repositório deverá mantê-lo no AIP, ou criar um outro identificador, que deverá ser associado, de maneira persistente, ao do SIP;

- ter acesso a ferramentas amplamente reconhecidas para apoiar o monitoramento dos componentes digitais dos documentos, tais como diretórios de formatos de arquivos (ex.: PRONOM – base de dados com registro de formatos mantida pelo arquivo nacional do Reino Unido¹⁵) e registros de outras informações de representação;

- registrar, em um banco de dados local, a informação de representação dos documentos admitidos, quando essa informação não estiver disponível nas ferramentas mencionadas no ponto anterior;

- registrar metadados de preservação associados aos documentos admitidos, de maneira a apoiar sua integridade, localização, legibilidade e proveniência, dentre outros;

- ter procedimentos para testar se os documentos são compreensíveis pela comunidade alvo e, em caso negativo, adequá-los às necessidades dessa comunidade (ex.: documentos voltados para deficientes visuais);
- verificar a completude e a correção de cada AIP no momento em que é gerado, isto é, no momento em que o SIP é convertido em AIP;
- ter um mecanismo independente para verificar a integridade do conjunto do seu acervo, ou seja, verificar que todos os documentos previstos foram, de fato, admitidos no repositório, justificando possíveis lacunas; e
- documentar todas as ações relevantes à preservação dos documentos e que estão relacionadas à criação do AIP.

c. Planejamento da preservação Um repositório digital deve fazer o planejamento da preservação dos documentos sob sua custódia, a fim de enfrentar os problemas trazidos pela obsolescência tecnológica e fragilidade do suporte. Esse planejamento deve ser feito a partir de uma política de preservação digital, ser bem documentado e incluir:

- estratégias de preservação bem definidas e periodicamente atualizadas, apontando e detalhando cada procedimento a ser adotado, como, por exemplo, a normalização de formatos;
- mecanismos para monitoramento e notificação quando alguma informação de representação dos documentos no repositório estiver se tornando obsoleta ou inviável (ex.: um formato de arquivo que esteja entrando em desuso, um suporte que esteja no final de sua vida útil);
- mecanismos de mudanças do plano de preservação como resultado do monitoramento; e
- fornecimento de evidências sobre a eficácia do plano de preservação.
- utilização das estratégias previstas no planejamento da preservação, que podem ser várias e devem ser registradas nos metadados de preservação;
- atender minimamente a dois aspectos da preservação digital – os cuidados com armazenamento (controle dos suportes, dos formatos e da localização de cópias) e a eventual necessidade de migração (atualização de suportes e conversão de formatos);
- preservação do documento digital (informação de conteúdo do AIP) originalmente admitido no repositório e daquele resultante da última migração;
- monitoramento constante da integridade dos AIPs, por meio do registro de metadados de fixidade e de logs de checagem dessa integridade (por exemplo, checksum); e

- registro de todas as ações de preservação realizadas nos AIPs. As migrações podem provocar alterações na forma e no conteúdo do documento, entretanto, no caso de documentos arquivísticos, não se admite a alteração de conteúdo. As migrações e quaisquer alterações da forma documental daí decorrentes devem ser registradas como metadados, a fim de apoiar a presunção de autenticidade do documento.

e. Gerenciamento de informação - Uma funcionalidade essencial de um repositório digital confiável é o gerenciamento da informação, aqui entendido como a gestão das informações descritivas (metadados) dos documentos admitidos no repositório. O principal objetivo desses metadados é apoiar o acesso e a recuperação dos documentos, e vão além das informações descritivas mais usuais (autor, título, data), envolvendo outras informações descritivas úteis aos usuários, tais como tamanho do arquivo disponível para download ou informação sobre a aplicação necessária para ler o arquivo. O gerenciamento da informação descritiva envolve os seguintes aspectos:

- metadados mínimos que permitam a busca e localização dos documentos – esses metadados devem ser identificadores conhecidos pela comunidade-alvo de usuários (ex.: número de matrícula do servidor público, título de livro numa biblioteca, número de processo);

- captura ou criação dos metadados mínimos pelo repositório, durante o processo de admissão, e associação desses metadados ao AIP correspondente;

- integridade referencial entre os AIPs e sua informação descritiva (metadados), ou seja, todo AIP deve ter uma informação descritiva, e toda informação descritiva deve apontar para um AIP; e

- permanência da integridade referencial, mesmo no caso de quebra temporária da relação entre o AIP e seus metadados descritivos – nesse caso, o repositório deve ser capaz de restaurar a relação rompida.

f. Gerenciamento de acesso Todo repositório deve produzir pacotes de disseminação de informação (DIP), atendendo aos seguintes requisitos:

- divulgação, para a comunidade de usuários, das opções disponíveis de acesso aos documentos e de entrega dos mesmos;

- implementação de uma política de registro dos acessos ocorridos que esteja de acordo com as necessidades de controle desses acessos, tanto da parte do repositório como dos produtores dos documentos nele admitidos;

- concessão de acesso a cada AIP, para os usuários autorizados e da forma devida (ex.: autorização de “somente leitura”, ou acesso a um número limitado de itens por período), em conformidade com o acordo estabelecido entre o repositório e o produtor/depositante;

- documentação e implementação de políticas de acesso (identificação e autenticação de usuários), em conformidade com os acordos estabelecidos entre o repositório e o produtor/depositante – essas políticas de acesso podem variar, desde a isenção da necessidade de identificação de usuário até o controle rígido da identificação e autenticação do usuário;
- registro de falhas de controle de acesso (como, por exemplo, um acesso indevidamente negado) e uso desse registro para avaliar eventuais falhas no sistema de segurança;
- demonstração de que o processo que gera o DIP atende completamente à requisição do usuário (ex.: se o usuário pediu um conjunto de documentos, receberá o conjunto completo; se ele pediu um documento, receberá apenas esse único documento);
- demonstração de que o processo que gera o DIP está correto em relação ao pedido do usuário (ex.: se o repositório oferece imagens nos formatos JPG e PNG, o usuário deve receber, dentre esses, o formato que solicitou);
- demonstração de que todos os pedidos de acesso resultam em uma resposta de aceitação ou rejeição; e
- garantia da autenticidade dos DIPs, por meio da entrega de cópias autênticas dos originais ou da viabilidade de rastreamento auditável da relação entre o DIP e o objeto original – para isso, um repositório deve ser capaz de demonstrar o processo de construção do DIP a partir de um AIP.

Tecnologia, infraestrutura técnica e segurança: Esses requisitos não prescrevem hardware e software específicos para garantir a preservação de longo prazo dos AIPs, mas apenas descrevem as melhores práticas das áreas de gestão de dados e segurança, que devem ser atendidas por um repositório digital confiável.

a. **Infraestrutura de sistema** Um repositório deve possuir uma infraestrutura tecnológica robusta, de maneira a apoiar a confiabilidade dos AIPs nele mantidos. Para tanto, deve observar os seguintes aspectos:

- funcionamento do repositório com base num sistema operacional e outros softwares de infraestrutura que tenham um bom suporte do mercado e da comunidade de usuários;
- adequação dos processos, do hardware e do software do sistema de backup às necessidades do repositório;
- gerenciamento do número de cópias de todos os documentos mantidos no repositório, e a localização de cada uma delas;

- mecanismos para garantir o sincronismo entre as cópias de um mesmo documento, ou seja, garantir que as mudanças intencionais feitas em uma cópia sejam propagadas para todas as outras;

- mecanismos efetivos para a detecção de corrupção ou perda de bits;

- relato dos incidentes de corrupção ou perda de dados eventualmente ocorridos e adoção de medidas para reparação ou substituição desses mesmos dados;

- previsão de procedimentos de atualização de suporte (refreshing) e de migração decorrentes do cumprimento do prazo de vida do suporte ou da obsolescência dos componentes de hardware;

- documentação da gestão de mudanças capaz de identificar alterações em processos críticos que afetem a capacidade de o repositório cumprir com suas responsabilidades obrigatórias;

- previsão de procedimentos para testar o efeito de mudanças críticas no sistema; e

- ponderação entre os riscos e os benefícios nas decisões de atualização de software de segurança.

b. Tecnologias apropriadas - O repositório deve adotar uma tecnologia de hardware e software apropriada para os serviços que presta, procedimentos para o recebimento e monitoramento de notificações e para a avaliação da necessidade de mudanças na tecnologia utilizada.

c. Segurança - A segurança do repositório não se limita a aspectos de tecnologia, mas abrange também instalações físicas e ações de pessoas. Os aspectos de segurança incluem:

- análise sistemática de dados, sistemas, pessoas e instalação física;

- adoção de procedimentos de controle para tratar adequadamente as necessidades de segurança;

- delineamento de papéis, responsabilidades e autorizações relativas à implementação de mudanças no sistema; e

- plano de prevenção de desastres e de reparação, que inclua, ao menos, um backup, offsite, de tudo o que é mantido no repositório (documentos, metadados, trilhas de auditoria etc.), inclusive do próprio plano de reparação.