

Consulta Pública Eletrônica

Solução de Gerenciamento de Conteúdo Empresarial (Enterprise Content Management – ECM)

<https://www.serpro.gov.br/consultas-publicas/sede/nnnn-2025>

Brasília/DF, junho de 2025.



Sumário

1.Objeto	3
1.1 Consulta ao Mercado sobre Tecnologias Disruptivas Aplicadas à Transformação Digital de Processos	3
1.2. Jornada do documento	6
1.3 Transparência e Integridade	6
2. Especificação do Objeto	8
2.1 Requisitos Gerais	8
2.1.1 Integração e Absorção de Sistemas Legados	8
2.1.2 Funcionalidades Gerais	9
2.1.3 Administração	11
2.1.4 Suporte e Integração a Processos	12
2.1.5 Requisitos Relacionados a Métricas	13
2.1.6 Requisitos de Acessibilidade	13
2.1.7 Requisitos de Usabilidade	14
2.1.8 Correspondência entre o sistema e o mundo real	14
2.1.9 Controle e liberdade do usuário	14
2.1.10 Consistência e padrões	14
2.1.11 Prevenção de erros	14
2.1.12 Reconhecimento em vez de memorização	15
2.1.13 Flexibilidade e eficiência de uso	15
2.1.14 Design estético e minimalista	15
2.1.15 Ajuda e documentação	15
2.1.16 Integrações (interoperabilidade)	15
2.1.17. Captura	16
2.1.18 Classificação	20
2.1.19 Retenção e Gestão de Registros	25
2.1.20 Gestão de Conteúdo	30
2.1.21 Segurança da Informação	44
2.1.22 Segurança para dados em nuvem	52

2.1.23 Privacidade para dados em Nuvem

54

1.Objeto

A presente consulta pública eletrônica, no formato Request For Information – RFI, tem por objeto identificar soluções, empresas e colher contribuições do mercado para a contratação de solução de Gerenciamento de Conteúdo Empresarial (Enterprise Content Management – ECM), com o objetivo de estruturar a transformação digital dos processos internos do SERPRO, tendo como piloto inicial o processo de aquisições.

A solução deverá possibilitar, ainda, a **absorção e/ou integração de sistemas legados e a incorporação dos dados neles contidos**, permitindo a centralização, interoperabilidade e preservação do histórico institucional. A proposta visa reduzir a dependência de tecnologias obsoletas, simplificar a gestão do processo e viabilizar a descontinuação progressiva de aplicações redundantes, com segurança e rastreabilidade.

1.1 Consulta ao Mercado sobre Tecnologias Disruptivas Aplicadas à Transformação Digital de Processos

Considerando a estratégia de modernização dos processos internos do SERPRO — a ser iniciada pelo processo de aquisições — esta consulta pública visa colher contribuições sobre **o uso de tecnologias emergentes e ferramentas disruptivas**, tais como:

- Inteligência Artificial (IA);
- Aprendizado de Máquina (Machine Learning);
- Fluxo operacional auto-orquestrado de fluxos documentais e decisórios;
- Assistentes digitais ou agentes autônomos para apoio à elaboração de artefatos técnicos e administrativos.

Diante disso, solicita-se ao mercado:

a) Quais soluções e frameworks de IA podem ser aplicadas com segurança e auditabilidade na geração assistida de documentos técnicos como:

- DODs (Documentos de Oficialização de Demanda);
- Plano de Contratações Anual;
- Estudos Técnicos Preliminares (ETP);
- Termos de Referência/ Projeto Básico;
- Pareceres;
- Minutas Editais;
- Minutas contratuais;
- Notas técnicas, despachos e justificativas administrativas.

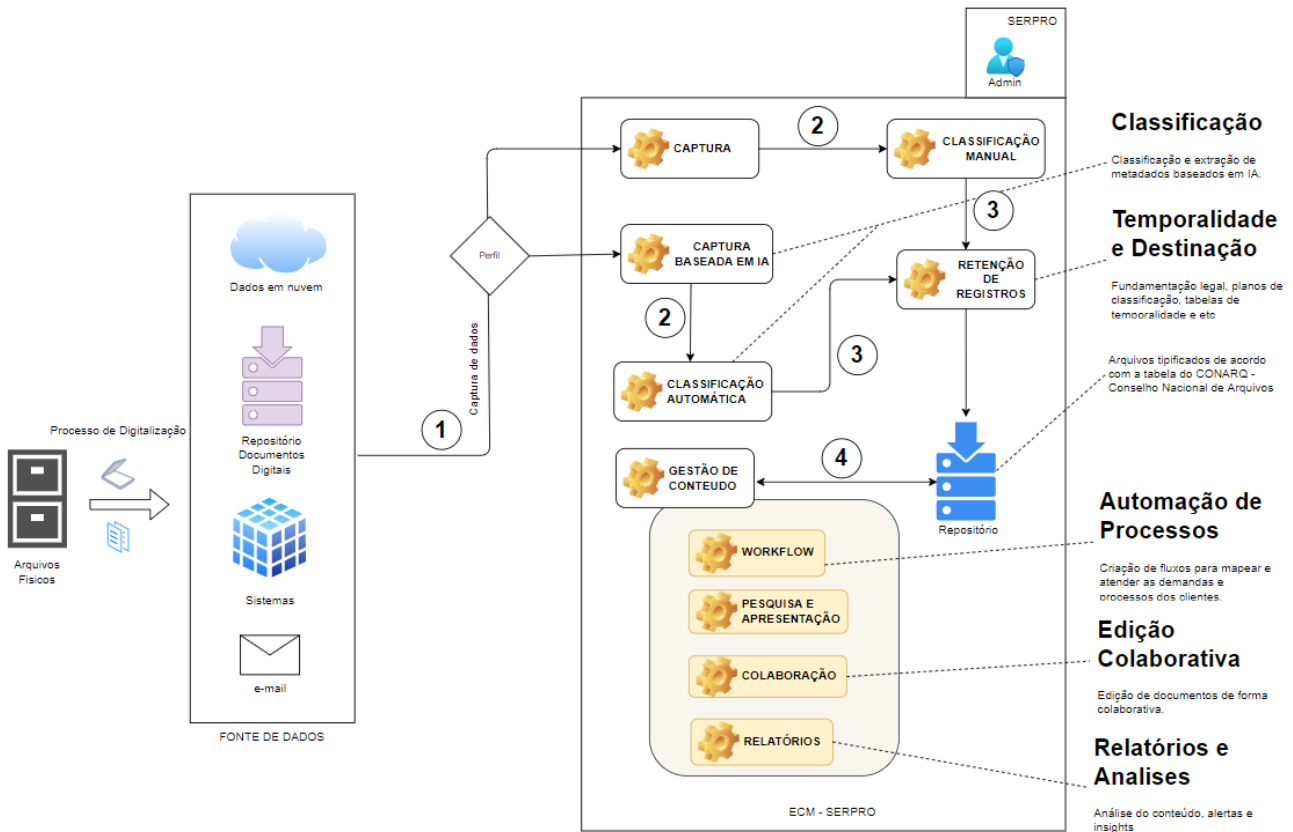
- b) Como essas soluções podem ser treinadas, auditadas e contextualizadas em ambientes corporativos sensíveis, como o SERPRO, respeitando requisitos de sigilo, LGPD, controle e versionamento?
- c) Quais práticas ou ferramentas o mercado recomenda para garantir que artefatos produzidos por IA estejam em conformidade com normativos vigentes, e que possam ser validados juridicamente e tecnicamente sem comprometer a governança?
- d) De que forma o fluxo operacional auto-orquestrado — aliando RPA, IA e ECM — pode otimizar fluxos como tramitação, análise, preenchimento, execução (fluxo de pagamentos e fluxo aplicação de penalidades) e consolidação de informações ao longo do ciclo de contratações públicas?
- e) Há soluções no mercado que integrem geração assistida por IA com motores de decisão, *templates* parametrizáveis e APIs para sistemas legados?
- f) O mercado possui experiências concretas com uso de IA e fluxo operacional auto-orquestrado em processos semelhantes em empresas públicas ou privadas? Há casos de sucesso que possam ser compartilhados?

As empresas interessadas devem responder à Consulta Pública, por meio do endereço eletrônico: consulta publica.supec@serpro.gov.br, com as seguintes informações:

- **Da Identificação da Empresa:**
 - Nome completo e fantasia.
 - CNPJ.
 - Endereço completo.
 - Site WEB (www).
- **Do Contato:**
 - Nome completo do responsável pela resposta desta Consulta Pública.
 - Cargo, telefones e endereço de e-mail.
- **Da Solução:**
 - Nome da solução oferecida, objeto desta consulta pública.
 - Nome do fabricante.
 - Site WEB do fabricante da solução (www).
- Descrição detalhada da solução e seus componentes (Documentos/datasheet, etc).
- Checklist se os requisitos da solução são atendidos (Sim/Não/Parcial), observações.

- Descrição detalhada do(s) modelo(s) de comercialização da solução (Licenças perpetua, subscrição, on-premise, SaaS).
- Descrição detalhada das métricas de licenciamento da solução.
- **Estudo de preços** (sku/part number, nome do software, métricas de licenciamento, serviços e outros, valores unitários) para as **modalidades de comercialização licenças perpetua, subscrição e SaaS**.
- **Base de Clientes:**
 - Quantidade de clientes no Brasil;
 - Nomes dos entes públicos que já adquiriram a solução.
- **Experiência e Suporte Técnico:**
 - O suporte é prestado pelo fabricante ou parceiro?
 - Quais os níveis de serviços ofertados para a solução (Tempo de atendimento, tempo da solução, etc).
- Informar a forma de repasse de conhecimento, resumos das grades e carga horária, para a administração e operação da solução.

1.2. Jornada do documento



- Carga de dados na solução do ECM, com obtenção de metadados;
- Classificação de dados de forma manual e automática;
- Temporalidade e Destinação para correta retenção dos registros;
- Gestão de conteúdo

1.3 Transparência e Integridade

Todos os documentos e informações relacionados ao processo de contratação do Serpro e desta consulta pública estão disponíveis no portal de transparência:

<https://www.transparencia.serpro.gov.br/acesso-a-informacao/licitacoes-e-contratos>

Regulamento de Licitações e Contratos do Serpro:

<https://www.transparencia.serpro.gov.br/acesso-a-informacao/licitacoes-e-contratos/documentos/regulamento>

Para este processo foi observado a política de integridade de acordo com art. 32, inc. V, da Lei nº 13.303/2016, Programa Corporativo de Integridade do Serpro – PCINT (TR - 138/2022) e a Cartilha de Integridade do Processo de Aquisições e Contratações.

Para conhecimento das regras de conduta no relacionamento entre fornecedores e empregados do Serpro, acesse a Cartilha de Integridade do Processo de Aquisições e Contratações, disponível no link: https://www.transparencia.serpro.gov.br/aceso-a-informacao/licitacoes-e-contratos/documentos/Cartilha_paq_verso_final_diagramada.pdf

Ressaltamos que o Serpro não concede ou autoriza nenhum tipo de registro de oportunidade em seus processos de contratação.

2. Especificação do Objeto

2.1 Requisitos Gerais

2.1.1 Integração e Absorção de Sistemas Legados

2.1.1.1 Importação de Conteúdo Histórico

2.1.1.1.1 A solução deverá permitir a ingestão de documentos e dados armazenados em sistemas legados, mantendo metadados, estrutura de diretórios, trilhas de auditoria e versionamento, sempre que disponíveis.

2.1.1.2 Migração Automatizada e Parametrizável

2.1.1.2.1 Deverá ser possível configurar rotinas automatizadas de migração de conteúdo e dados a partir de diferentes fontes (sistemas, repositórios, banco de dados, etc), com suporte a regras de transformação e classificação durante a carga.

2.1.1.3 Registro de Proveniência

2.1.1.3.1 Todo conteúdo migrado de sistemas legados deverá conter marcação de origem e data de importação, garantindo a rastreabilidade histórica e a integridade arquivística.

2.1.1.4 Repositório Unificado e Busca Global

2.1.1.4.1 A solução deverá possibilitar a centralização do acervo institucional em um repositório lógico único, permitindo a busca global por conteúdos migrados e nativos, com filtros por origem, contexto processual e período temporal.

2.1.1.5 Integração com API e Camadas de Interoperabilidade

2.1.1.5.1 Deverão ser disponibilizadas APIs ou conectores que permitam a integração direta com sistemas ainda em uso, de modo a garantir continuidade operacional durante o período de coexistência.

2.1.1.5.2 A solução deve ser compatível com formatos amplamente utilizados em sistemas legados (ex.: XML, CSV, JSON, PDF/A, DOCX, ODT, entre outros).

2.1.1.5.2.1 Devem ser observadas boas práticas de arquivística digital, interoperabilidade e conformidade com normas como MoReq, OAIS, ISO 15489 e e-ARQ Brasil.

2.1.1.5.2.2 Todo o processo de absorção deve ser auditável, com logs e relatórios de validação pós-migração.

2.1.1.5.2.3 Deve haver suporte à duplicação de documentos durante a migração, com preservação de versões e metadados associados.

2.1.2 Funcionalidades Gerais

2.1.2.1 A solução deverá ser instalada On-Premise ou SaaS.

2.1.2.2 A solução deve obrigatoriamente suportar arquitetura multi-tenant (multi-inquilino). Isso significa que uma única instância do sistema deve ser capaz de atender múltiplos clientes, usuários ou unidades organizacionais, mantendo o isolamento lógico entre os dados, configurações e recursos de cada um.

2.1.2.3 Não será permitido que o ambiente seja duplicado ou que múltiplas instâncias completas da aplicação sejam criadas para cada novo cliente ou unidade. O modelo de implantação deve permitir o compartilhamento eficiente de recursos computacionais, garantindo escalabilidade, segurança, isolamento lógico e facilidade de manutenção.

2.1.2.4 O fornecedor ou equipe responsável pela aplicação deverá assegurar:

2.1.2.4.1 Isolamento adequado de dados entre os tenants.

2.1.2.4.2 Controle de acesso segmentado por tenant.

2.1.2.4.3 Capacidade de gestão e monitoramento centralizado.

2.1.2.4.4 Customizações limitadas por tenant (quando aplicável), sem comprometer a integridade da instância compartilhada.

2.1.2.5 Caso a solução dependa de outras ferramentas, plataformas ou componentes de terceiros para operar corretamente (ex: bancos de dados, serviços de autenticação, motores de workflow, sistemas de mensagens etc.), o fornecedor deverá:

2.1.2.5.1 Informar claramente todas as dependências externas necessárias.

2.1.2.5.2 Incluir no fornecimento todos os licenciamentos, subscrições ou autorizações de uso necessárias para o funcionamento da aplicação na nuvem privada.

2.1.2.5.3 Garantir que tais dependências estejam devidamente suportadas e integradas à solução.

2.1.2.6 As funcionalidades de automação de processos de negócio, gerenciamento eletrônico de documentos e retenção de registros devem ser do mesmo fabricante, de forma a ser totalmente e nativamente integrados.

2.1.2.7 A solução deverá possuir integração entre todos os módulos componentes, isto é, não ser necessária importação e exportação manuais (ou seja, com intervenção do usuário) de dados, uma vez que a integração deve garantir que uma única transação desencadeie todas as ações a ela pertinentes, tornando os processos de negócio totalmente integrados entre si;

2.1.2.8 A solução deverá armazenar todos os conteúdos em um repositório único, gerenciado de maneira centralizada e acessível a todos os usuários;

2.1.2.9 A solução deverá prover funcionalidades relacionadas ao gerenciamento do ciclo de vida das aplicações da solução, contemplando a documentação, o controle de mudanças e testes, o versionamento e a instalação (deploy) que agregue automaticamente todos os componentes e dados necessários para transferência das aplicações, de forma controlada, entre os ambientes de Desenvolvimento, Homologação/Aceite e Produção;

2.1.2.10 Os arquivos gerenciados pela solução deverão ser armazenados em volumes externos aos containers ou servidor de forma que estes possam fazer parte de processos de backup e restauração, e metadados (índices e atributos) em SGDB (Sistema Gerenciador de Banco de Dados).

2.1.2.11 A solução deverá ser WEB, compatível com os navegadores (browser) atuais: Microsoft Edge, Google Chrome e Mozilla Firefox;

2.1.2.12 A solução deverá suportar no mínimo 1000 requisições por segundo.

2.1.2.13 O acesso a interface web deve ser protegido por criptografia SSL no mínimo de 256 bits; A solução deverá permitir a implantação dos serviços em uma arquitetura distribuída, permitindo assim a escalabilidade horizontal da solução;

2.1.2.14 A solução deverá permitir a escalabilidade de maneira vertical, onde ao se incluir mais recursos em um único servidor aumenta-se a capacidade da solução;

2.1.2.15 Os serviços, núcleo da solução (repositório e pesquisa), devem poder ser implantados em alta-disponibilidade com balanceamento de carga;

2.1.2.16 A solução deverá possibilitar ser executada sob uma plataforma de Containers (Docker, Podman e/ou Kubernetes, sem a dependência de licenças adicionais de outros produtos de gerenciamento de containers).

2.1.2.17 A solução deve ser nativamente compatível com armazenamento de arquivos em servidores CAS (Content-addressable storage), NAS (Network-attached storage) e SAN (Storage Area Network).

2.1.2.18 A solução deve prover cópias de segurança e restauração de dados que garantam o armazenamento seguro, bem como a disponibilidade desses dados em caso de necessidade.

2.1.2.19 A solução deve permitir a implementação de redundância na infraestrutura de hardware, software e rede.

2.1.2.20 Deverá ser mantido pelo fornecedor um ciclo de vida com atualizações constantes da solução, de forma a manter softwares atualizados com as últimas correções de segurança evitando vulnerabilidades conhecidas.

2.1.2.21 A solução deve ser adaptável para funcionar nas diferentes *Stacks* presentes na Nuvem de Governo, que podem ser de provedores diferentes do(s) qual(is) a aplicação executa fora da Nuvem de Governo.

2.1.3 Administração

2.1.3.1 A solução deverá ser escalável, a fim de permitir adaptação a organizações de diferentes tamanhos e complexidades.

2.1.3.2 A solução deverá fornecer evidências do grau de escalabilidade ao longo do tempo. Avaliações quantitativas devem incluir:

2.1.3.2.1 Tamanho máximo do repositório que pode ser suportado com desempenho adequado;

2.1.3.2.2 O número máximo de usuários simultâneos que podem ser atendidos com desempenho adequado;

2.1.3.2.3 Sobrecarga administrativa prevista para um período de cinco anos, permitindo o crescimento do número de usuários e da quantidade de registros;

2.1.3.2.4 Quantidade de reconfigurações e indisponibilidades previstas para um período de cinco anos, permitindo o crescimento do número de usuários e da quantidade de registros;

2.1.3.2.5 Quantidade de reconfigurações e indisponibilidades previstas para um período de cinco anos, permitindo mudanças substanciais na estrutura da organização, nos esquemas de classificação e na administração de usuários.

2.1.3.3 A solução deverá ser capaz de se adequar ao grau de disponibilidade estabelecido pela organização, possibilitando o uso de redundância para em caso de manutenções o serviço não seja indisponibilizado.

2.1.3.4 A solução deverá permitir integração com solução/módulo de anti-malware para realizar a verificação de vírus ou pragas antes da efetivação da captura.

2.1.3.5 Após falha ou descontinuidade do sistema, quando a recuperação automática não for possível, a solução deverá ser capaz de entrar em modo de manutenção, no qual é oferecida a possibilidade de restaurar o sistema para um estado seguro.

2.1.3.5.1 Na restauração ao estado seguro, a solução deverá ser capaz de garantir a recuperação de perdas ocorridas, inclusive dos documentos de transações mais recentes.

2.1.3.6 A solução deverá preservar um estado seguro de funcionamento, interrompendo completamente a interação com usuários comuns, quando ocorrer um dos erros a seguir:

2.1.3.6.1 Falha de comunicação entre cliente e servidor;

2.1.3.6.2 Perda de integridade das informações de controle de acesso;

2.1.3.6.3 Falta de espaço para registro nas trilhas de auditoria.

2.1.3.7 Quando não for possível escrever na trilha de auditoria, a solução deverá impedir toda operação de qualquer usuário e passar para o modo de manutenção.

2.1.3.8 A solução deverá suportar a criação de ambiente de homologação de modo que as modificações no sistema e em sua base tecnológica têm que ser verificadas num ambiente exclusivo para essa finalidade, de modo a garantir que, após a implantação das alterações, os dados continuem sendo acessados sem alteração de conteúdo.

2.1.3.9 A solução deverá permitir que os administradores, de maneira controlada e sem esforço excessivo, recuperem, visualizem e reconfigurem os parâmetros do sistema e os atributos dos usuários.

2.1.3.10 A solução deverá dispor de documentação referente a aspectos de administração do sistema. A documentação deve incluir todas as informações necessárias para o correto gerenciamento do sistema.

2.1.3.11 A solução deverá possibilitar a expansão da estrutura de armazenamento.

2.1.3.12 A solução deverá ao oferecer ao administrador facilidades para monitoração da capacidade de armazenamento.

2.1.3.13 A solução deverá informar, automaticamente, ao administrador quando os dispositivos de armazenamento on-line atingirem níveis críticos de ocupação.

2.1.3.14 A solução deverá utilizar técnicas de restauração de dados em caso de falhas.

2.1.3.15 A solução deverá utilizar mecanismos de proteção contra escrita, que previnam alterações indevidas e mantenham a integridade dos dados armazenados.

2.1.3.16 A solução deverá possibilitar a verificação da integridade dos dispositivos de armazenamento.

2.1.4 Suporte e Integração a Processos

2.1.4.1 A solução deverá permitir a importação, modelagem e execução dos processos de negócio já em operação (BPM) — em particular o processo de aquisições do Serpro — garantindo a integridade do processo (etapas, regras, documentos e pontos de decisão) viabilizando ajustes, melhorias e evoluções por meio de configurações parametrizáveis, sem necessidade de desenvolvimento de código adicional, com adoção de tecnologias disruptivas que proporcionem automação do processo.

2.1.5 Requisitos Relacionados a Métricas

2.1.5.1 A solução deverá prover suporte à integração com soluções de web analytics que possibilite avaliar a quantidade de usuários por períodos, as jornadas de uso dos usuários na solução e o tempo de interação dos usuários nas funcionalidades.

2.1.5.2 A solução deverá permitir integração com ferramentas para análise exploratória de dados, permitindo uma avaliação mais profunda de dados e geração de insights acionáveis;

2.1.5.3 Prover suporte à integração com solução de monitoramento de ambientes, geração de alarme em relação a métricas estipuladas para o negócio ou ambiente monitorado.

2.1.5.4 Prover API ou Serviços para exposição de Dados Estatísticos relativos ao negócio e uso da solução;

2.1.5.5 A solução deverá prover mecanismos para coleta de feedback dos usuários.

2.1.5.6 A solução deverá permitir integração com ferramentas de experimentação que implementam teste A/B ou Multivariado por meio de alterações dinâmicas na interface de usuário, sem necessidade de intervenção em código fonte;

2.1.5.7 A solução deverá realizar registro de log de atividade;

2.1.6 Requisitos de Acessibilidade

2.1.6.1 Todo conteúdo visual relevante ao contexto de uso — como imagens, ícones, gráficos e botões com elementos imagéticos — deve incluir uma descrição textual alternativa. Essa descrição precisa transmitir, de forma clara e objetiva, a informação essencial contida no elemento visual.

2.1.6.2 Os textos exibidos em interfaces digitais devem apresentar relação de contraste entre primeiro plano e segundo plano mínima de 4,5:1, garantindo legibilidade adequada.

2.1.6.3 A medição do contraste deve ser realizada conforme normas técnicas internacionalmente reconhecidas, preferencialmente as diretrizes WCAG.

2.1.6.4 Todas as funcionalidades interativas da solução digital — incluindo, mas não se limitando a menus, botões, formulários e links — devem ser plenamente operáveis por meio de teclado.

2.1.6.5 Todas as soluções digitais devem disponibilizar um mecanismo de salto de conteúdo — como um link "Pular para conteúdo" ou atalho equivalente — que permita aos usuários ignorar blocos repetitivos de navegação (cabeçalhos, menus principais) e acessar diretamente o conteúdo principal da página.

2.1.6.6 Todos os campos de formulário em soluções digitais devem possuir rótulos textuais permanentes e descritivos, visíveis e programaticamente associados aos respectivos campos, que indiquem claramente o conteúdo solicitado (ex.: "Nome completo", "E-mail", "Senha").

2.1.6.7 Todo elemento interativo que receba foco via teclado — incluindo, mas não se limitando a links, botões, campos de formulário e controles de interface — deve apresentar um indicador visual de foco claramente perceptível, que se destaque do conteúdo adjacente e preserve a identidade visual do sistema.

2.1.7 Requisitos de Usabilidade

2.1.7.1 A interface do sistema deve seguir os princípios e heurísticas de usabilidade seguindo os padrões internacionais como listados abaixo:

2.1.7.2 Visibilidade do status do sistema

2.1.7.3 O sistema deve possuir uma trilha de navegação (*breadcrumb*) para indicar ao usuário sua localização.

2.1.7.4 Cada item da solução deve possuir menu sensível ao contexto, exibindo apenas as funções disponíveis e permitidas para aquele tipo de item.

2.1.7.4 Toda ação do usuário deve gerar resposta visual/auditiva clara. Por exemplo: carregamentos, confirmações, erros.

2.1.8 Correspondência entre o sistema e o mundo real

2.1.8.1 A interface do sistema deve utilizar linguagem, ícones e fluxos que reflitam o modo como os usuários pensam e se comunicam no mundo real, evitando jargões técnicos e priorizando termos, formatos e sequências familiares ao público-alvo.

2.1.9 Controle e liberdade do usuário

2.1.9.1 A solução deve ser responsiva, se adaptando aos diversos meios de acessos web, seja via browser, smartphone (Android e iOS) e tablet (Android e iOS).

2.1.9.2 O sistema deve permitir a criação de atalhos para objetos mais utilizados ou favoritos.

2.1.9.3 A solução deve permitir a gravação de opções padrão para entrada de dados, como valores definidos pelo usuário, valores anteriores, listas configuráveis, dados contextuais e valores predefinidos por administradores.

2.1.10 Consistência e padrões

2.1.10.1 A interface deve estar disponível em português do Brasil ou permitir a sua tradução.

2.1.11 Prevenção de erros

2.1.11.1 Caso haja algum menu sensível ao contexto, este deverá exibir apenas as funções que o usuário tem permissão para executar, reduzindo a chance de erros operacionais.

2.1.12 Reconhecimento em vez de memorização

2.1.12.1 A solução deve incluir dicas de ajuda nos campos, reduzindo a necessidade de memorização de procedimentos.

2.1.12.2 A ajuda on-line deve ser contextual, remetendo diretamente ao tópico relacionado à tarefa em execução.

2.1.13 Flexibilidade e eficiência de uso

2.1.13.1 A interface deve ser intuitiva e exigir poucas ações para completar tarefas padrão.

2.1.14 Design estético e minimalista

2.1.14.1 A interface deve ser clara, organizada e inteligível, com documentação técnica e de uso bem estruturada.

2.1.14.2 Ajudar os usuários a reconhecerem, diagnosticar e recuperar erros

2.1.15 Ajuda e documentação

2.1.15.1 A solução deve possuir sistema de ajuda on-line contextual.

2.1.15.2 A ajuda deve estar vinculada à função ou tarefa em execução, refletindo o contexto real da atividade do usuário.

2.1.15.3 Deve fornecer documentação completa, clara e organizada para instalação, uso e todos os componentes técnico

2.1.16 Integrações (interoperabilidade)

2.1.16.1 A solução deverá ser capaz de interoperar com outros sistemas informatizados, permitindo, pelo menos, consulta, recuperação, importação e exportação de documentos e seus metadados.

2.1.16.2 A solução deverá seja capaz de interoperar com outros sistemas por meio de padrões abertos de interoperabilidade. Por exemplo, padrões abertos como os estabelecidos pela e-PING, XML, CMIS e Dublin Core.

2.1.16.3 A solução deverá permitir a aplicação dos requisitos de segurança descritos neste documento para executar operações de interoperabilidade.

2.1.16.4 A solução deverá disponibilizar APIs bem documentadas e robustas que facilitem a integração com sistemas externos, permitindo a transferência eficiente de dados.

2.1.16.5 A solução deve fornecer RestAPI's para integração com sistemas externos para a manipulação de objetos do repositório, possuindo pelo menos, as seguintes funções: inclusão, consulta e edição de atributos de documentos;

2.1.16.6 A solução deverá possuir APIs abertas e flexíveis para integração fácil com sistemas de terceiros, como sistemas ERP, CRM, SEI, BPM, outros aplicativos empresariais.

2.1.16.7 A solução deverá possibilitar a integração com ferramentas BPM para uma automação mais avançada e completa de processos de negócios.

2.1.16.8 A solução deverá adotar e suportar padrões de integração amplamente reconhecidos, como REST e SOAP para facilitar a interoperabilidade.

2.1.16.9 A solução deverá possuir conectores pré-construídos ou ser capaz de se conectar com sistemas de CRM, ERP, SEI, BPM e outras ferramentas de software empresarial, como por exemplo Microsoft Office 365, Google Workspace.

2.1.16.10 A solução deve permitir integração com serviço de e-mail corporativo por meio de protocolos padrão de mercado, como IMAP, garantindo compatibilidade com múltiplos fornecedores, além de oferecer integrações nativas com plataformas como Microsoft Outlook/Exchange, Google Workspace. Essa integração deve permitir que os anexos dos e-mails sejam gravados diretamente no repositório, bem como o e-mail em si e permitir inclusive a criação de workflows a partir do recebimento por e-mail.

2.1.16.11 A solução deve permitir integração com suíte de colaboração, como por exemplo Microsoft Office 365, Google Workspace. Essa integração deve permitir a edição de documentos diretamente na solução;

2.1.16.12 A solução deve suportar integração com serviços de e-mail corporativo possibilitando o envio e recebimento de e-mails.

2.1.17. Captura

2.1.17.1 A solução deverá garantir as seguintes funções na captura:

2.1.17.1.1 Registrar e gerenciar todos os documentos não digitais;

2.1.17.1.2 Registrar e gerenciar todos os documentos digitais ou híbridos, independentemente do contexto tecnológico;

2.1.17.1.3 Classificar todos os documentos de acordo com o plano ou código de classificação;

2.1.17.1.4 Controlar e validar a introdução de metadados.

2.1.17.2 A solução deverá ser capaz de capturar documentos digitais das formas a seguir:

2.1.17.2.1 Captura de documentos produzidos dentro da solução;

2.1.17.2.2 Captura de documento digital produzido fora da solução;

2.1.17.2.3 Captura de documento produzido em workflow ou em outros sistemas integrados a solução;

2.1.17.2.4 Captura de documentos em lote.

2.1.17.3 A solução deverá ser capaz de capturar e manter todos os componentes digitais do documento.

2.1.17.4 A solução deverá permitir o registro dos metadados e garantir que se mantenham associados ao documento, componente digital ou classe.

2.1.17.5 A solução deverá permitir prever a inserção dos metadados obrigatórios, no momento da captura de processos.

2.1.17.6 A solução deverá ser capaz de atribuir um número identificador a cada dossiê/processo e documento capturado, que serve para identificá-lo desde o momento da captura até sua destinação final na solução.

2.1.17.7 A solução deverá permitir a configuração do formato do número identificador atribuído. O identificador pode ser numérico ou alfanumérico, ou pode incluir os identificadores encadeados das entidades superiores no ramo apropriado da hierarquia.

2.1.17.8 A solução deverá gerar número identificador na seguinte forma:

2.1.17.8.1 Ser gerado automaticamente, sendo vedada sua introdução manual e alteração posterior; ou

2.1.17.8.2 Ser atribuído pelo usuário e validado pela solução antes de ser aceito.

2.1.17.9 A solução deverá permitir prever a adoção da numeração única de processos e/ou documentos oficiais a fim de garantir a integridade do número atribuído ao processo e/ou documento na unidade protocolizadora de origem.

2.1.17.10 A solução deverá garantir que os metadados associados a um documento sejam inseridos e alterados somente por usuários autorizados, sendo devidamente registrados em trilha de auditoria.

2.1.17.11 A solução deverá ser capaz de inserir, automaticamente, os metadados previstos

2.1.17.12 A solução deverá permitir a visualização do registro de entrada do documento na solução com todos os metadados inseridos automaticamente e os demais a serem atribuídos pelo usuário.

2.1.17.13 A solução deverá permitir a inserção de outros metadados após a captura. Por exemplo: Carimbo de tempo da assinatura digital.

2.1.17.14 No caso da captura de documentos constituídos por mais de um componente digital, a solução tem que:

2.1.17.14.1 Tratar o documento como uma unidade indivisível, assegurando a relação entre os componentes digitais;

2.1.17.14.2 Preservar a integridade do documento, mantendo a relação entre os componentes digitais;

2.1.17.14.3 Garantir a integridade do documento quando de sua recuperação, visualização e gestão posteriores;

2.1.17.14.4 Gerenciar a destinação de todos os componentes digitais que compõem o documento como uma unidade indivisível.

2.1.17.15 A solução deverá possuir a funcionalidade de OCR (Optical Character Recognition), sendo preciso e capaz de extrair caracteres impressos de textos de documentos digitalizados, garantindo a pesquisa eficaz e a indexação apropriada.

2.1.17.16 A solução deverá possuir a funcionalidade de ICR (Intelligent Character Recognition), sendo preciso e capaz de extrair caracteres manuscritos que se encontram em imagem de documentos digitalizados, garantindo a pesquisa eficaz e a indexação apropriada.

2.1.17.17 A solução deverá possuir a funcionalidade de OMR (Optical Mark Recognition), sendo preciso e capaz de interpretar e extrair eletronicamente informação de campos marcados que se encontram em imagem de documentos digitalizados, garantindo a pesquisa eficaz e a indexação apropriada.

2.1.17.18 A solução deverá permitir a captura em lote de documentos gerados por outros sistemas. Esse procedimento tem que:

2.1.17.18.1 permitir a importação de transações predefinidas de arquivos em lote;

2.1.17.18.2 registrar, automaticamente, cada um dos documentos importados contidos no lote;

2.1.17.18.3 permitir e controlar a edição do registro dos documentos importados;

2.1.17.18.4 validar a integridade dos metadados.

2.1.17.19 A solução deverá permitir capturar mensagens de correio eletrônico após selecionadas quais serão objeto de registro.

2.1.17.20 A solução deverá permitir que os usuários tratem e capturem as mensagens de chegada a partir do seu próprio sistema de correio eletrônico. O usuário deve poder tratar cada mensagem na caixa de entrada, como se segue:

2.1.17.20.1 Visualizar cada mensagem de correio e uma indicação dos respectivos anexos, caso existam;

2.1.17.20.2 Visualizar os conteúdos dos anexos utilizando um dispositivo para visualização de documentos em diferentes formatos;

2.1.17.20.3 Registrar no sistema a mensagem de correio e respectivos anexos como um novo documento de arquivo;

2.1.17.20.4 Relacionar a mensagem e respectivos anexos a um documento existente no sistema;

2.1.17.20.5 Capturar automaticamente metadados de data e hora da transmissão da mensagem e todos os destinatários.

2.1.17.21 A solução deverá assegurar a captura do nome, e não somente do endereço, do originador do correio eletrônico. Por exemplo, "José Silva", além de "j_silva@serpro.gov.br".

2.1.17.22 A solução deverá permitir ser capaz de capturar também os documentos não digitais e/ou híbridos.

2.1.17.23 A solução deverá permitir acrescentar aos metadados dos documentos não digitais informações sobre sua localização de guarda. Essa informação só será acessada por usuários autorizados.

2.1.17.24 A solução deverá permitir garantir que a parte digital de um documento ou dossiê/processo híbrido seja tratada de forma análoga aos documentos ou dossiê/processo inteiramente digitais.

2.1.17.25 A solução deverá permitir tratar um documento ou dossiê/processo híbrido como uma unidade indivisível, assegurando a relação entre a parte digital e a não digital.

2.1.17.26 A solução deverá possuir a capacidade de capturar documentos com diferentes formatos de arquivo e estruturas, e no mínimo as seguintes fontes:

2.1.17.26.1 Câmera;

2.1.17.26.2 Dispositivos Móveis;

2.1.17.26.3 Scanner;

2.1.17.26.4 Mainframe;

2.1.17.26.5 E-mail;

2.1.17.26.6 Formulário Web;

2.1.17.26.7 Armazenamento externo;

2.1.17.26.8 Dados em Nuvem (ex.: Google, Amazon, Microsoft, Oracle);

2.1.17.26.9 Bancos de Dados (Oracle, Microsoft SQL Server, PostgreSQL, MySQL);

2.1.17.26.10 Documentos em formatos PDF, ODS, ODT, ODP, DOC, DOCX, RTF, XSL, XLSX, PPT, PPTX, PPS, HTM, HTML, TXT, TIF, TIFF, PNG, JPG, JPEG, BMP, GIF, MP4, MOV, MKV, WMV, AVI e DWG

2.1.17.27 A solução deverá ser capaz de incluir novos formatos de arquivos à medida que forem sendo adotados pela empresa.

2.1.17.28 A solução deverá ser capaz de registrar em metadados as informações relativas à dependência de software, quando capturar documentos em formatos diferentes dos previstos pelo programa de gestão de documentos da empresa.

2.1.17.29 A solução deverá suportar os três principais padrões em protocolo de comunicação com scanners: TWAIN, ISIS e KOFAX.

2.1.18 Classificação

2.1.18.1 Configuração e administração do plano de classificação

2.1.18.1.1 A Solução deve ser capaz de importar e ser compatível com um plano de classificação, com as seguintes informações:

2.1.18.1.1.1 Identificador da classe;

2.1.18.1.1.2 Nome da classe;

2.1.18.1.1.3 Código da classe;

2.1.18.1.1.4 Subordinação da classe;

2.1.18.1.1.5 Indicação de permissão de uso;

2.1.18.1.1.6 Indicação de classe ativa/inativa.

2.1.18.1.2 A Solução deverá permitir a criação de classes, subclasses, grupos e subgrupos nos níveis do plano de classificação de acordo com o método de codificação adotado.

2.1.18.1.3 A Solução deverá permitir a usuários autorizados acrescentar novas classes sempre que necessário.

2.1.18.1.4 A Solução deverá permitir registrar a data de abertura de uma nova classe no respectivo metadado.

2.1.18.1.5 A Solução deverá permitir registrar a mudança de nome, identificador e código de uma classe já existente no respectivo metadado.

2.1.18.1.6 A Solução deverá permitir o deslocamento de uma classe inteira, incluídas as subclasses, grupo, subgrupos e documentos nela classificados, para outro ponto do plano de classificação,

bem como o desmembramento ou fusão de classes. Nesse caso, é necessário fazer o registro do deslocamento nos metadados do plano de classificação.

2.1.18.1.7 A Solução deverá permitir que apenas usuários autorizados tornem inativa uma classe em que não sejam mais classificados documentos.

2.1.18.1.8 A Solução deverá permitir que um usuário autorizado apague uma classe inativa.

2.1.18.1.9 A Solução deverá impedir a eliminação de uma classe que tenha documentos nela classificados. Essa eliminação pode ocorrer a partir do momento em que todos os documentos ali classificados tenham sido recolhidos ou eliminados ou que esses documentos tenham sido reclassificados.

2.1.18.1.10 A Solução deverá permitir a associação de metadados às classes, conforme estabelecido no padrão de metadados, e deve restringir a inclusão e alteração desses mesmos metadados somente a usuários autorizados.

2.1.18.1.11 A Solução deverá permitir disponibilizar pelo menos dois mecanismos de atribuição de identificadores a classes do plano de classificação, prevendo a possibilidade de se utilizarem ambos, separadamente ou em conjunto, na mesma aplicação:

2.1.18.1.11.1 Atribuição de um código numérico ou alfanumérico;

2.1.18.1.11.2 Atribuição de um termo que identifique cada classe.

2.1.18.1.12 A Solução deverá permitir utilizar o termo completo para identificar uma classe.

2.1.18.1.12.1 Entende-se por termo completo toda a hierarquia referente àquela classe. Por exemplo:

2.1.18.1.12.1.1 MATERIAL: AQUISIÇÃO: MATERIAL PERMANENTE: COMPRA

2.1.18.1.12.1.2 MATERIAL: AQUISIÇÃO: MATERIAL DE CONSUMO: COMPRA.

2.1.18.1.13 A Solução deverá permitir assegurar que os termos completos, que identificam cada classe, sejam únicos no plano de classificação.

2.1.18.1.14 A Solução deverá permitir a pesquisa e navegação na estrutura do plano de classificação por meio de uma interface gráfica.

2.1.18.1.15 A Solução deverá ser capaz de importar e exportar, total ou parcialmente, um plano de classificação.

2.1.18.1.16 A Solução deverá permitir prover funcionalidades para elaboração de relatórios de apoio à gestão do plano de classificação, incluindo a capacidade de:

2.1.18.1.16.1 Gerar relatório completo do plano de classificação;

2.1.18.1.16.2 Gerar relatório parcial do plano de classificação a partir de um ponto determinado na hierarquia;

2.1.18.1.16.3 Gerar relatório dos documentos ou dossiês/processos classificados em uma ou mais classes do plano de classificação;

2.1.18.1.16.4 Gerar relatório de documentos classificados por unidade administrativa.

2.1.18.2 Classificação e metadados das unidades de arquivamento

2.1.18.2.1 A Solução deverá permitir a classificação das unidades de arquivamento somente nas classes autorizadas.

2.1.18.2.2 A Solução deverá permitir a classificação de um número ilimitado de unidades de arquivamento dentro de uma classe.

2.1.18.2.3 A Solução deverá permitir utilizar o termo completo da classe para identificar uma unidade de arquivamento, tal como especificado no requisito 2.1.18.12.

2.1.18.2.4 A Solução deverá permitir a associação de metadados às unidades de arquivamento e deve restringir a inclusão e alteração desses metadados a usuários autorizados.

2.1.18.2.5 A Solução deverá permitir associar os metadados das unidades de arquivamento conforme estabelecido no padrão de metadados.

2.1.18.2.6 A Solução deverá permitir que uma nova unidade de arquivamento herde, da classe em que foi classificada, alguns metadados predefinidos.

2.1.18.2.6.1 Exemplos desta herança são prazos de guarda previstos na tabela de temporalidade e destinação e restrição de acesso.

2.1.18.2.7 A Solução deverá permitir relacionar os metadados herdados de forma que uma alteração no metadado de uma classe seja automaticamente incorporada à unidade de arquivamento que herdou esse metadado.

2.1.18.2.8 A Solução deverá permitir a alteração conjunta de um determinado metadado em um grupo de unidades de arquivamento previamente selecionado.

2.1.18.2.9 A Solução deverá permitir que uma unidade de arquivamento e seus respectivos volumes e/ou documentos sejam reclassificados por um usuário autorizado e que todos os documentos já inseridos permaneçam nas unidades de arquivamento e nos volumes que estão sendo transferidos, mantendo a relação entre documentos, volumes e unidades de arquivamento.

2.1.18.2.10 A Solução deverá permitir associar, automaticamente, ao dossiê/processo o prazo e a destinação previstos na classe em que o documento foi inserido.

2.1.18.3 Classificação automática de documentos

2.1.18.3.1 A solução deverá prover nativamente funcionalidades para a classificação automática de documentos do repositório permitindo a atribuição automatizada de uma classificação de records management aos documentos.

2.1.18.3.2 A classificação automática de documentos deve ser baseada em uma combinação de aprendizado de máquina (machine learning), regras e análise de conteúdo dos documentos.

2.1.18.3.3 A definição de regras de classificação automática deve ser baseada em palavras-chave e/ou metadados.

2.1.18.3.4 A funcionalidade de classificação automática de documentos deverá fornecer um painel de acompanhamento para a validação dos resultados do processo com passo-a-passo para o usuário realizar ajustes nas configurações.

2.1.18.3.5 A funcionalidade de classificação automática deverá oferecer sugestões ao usuário para melhoria do processo de classificação com base nos dados extraídos dos documentos.

2.1.18.3.6 Durante a configuração ou melhoria do processo de classificação automática deverá ser possível ao usuário incluir uma lista de documentos para teste, que deverá ser analisada pelo processo e fornecido os dados resultantes para a tomada de decisão do usuário.

2.1.18.4 Classificação de informação sigilosa e restrição de acesso

2.1.18.4.1 A solução deverá implementar a classificação de grau de sigilo e demais caracterizações de restrição de acesso de documentos, dossiês/processos e classes do plano de classificação, e de todas as operações de usuários nos documentos.

2.1.18.4.2 A solução deverá implementar a identificação de restrições legais de acesso baseando-se nos seguintes atributos de segurança:

2.1.18.4.2.1 Tipo de restrição legal de acesso;

2.1.18.4.2.2 Credencial de segurança do usuário.

2.1.18.4.3 A solução deverá tratar a classificação de grau de sigilo baseando-se pelo menos nos seguintes atributos de segurança:

2.1.18.4.3.1 Grau de sigilo do documento, com pelo menos: ultrassecreto, secreto e reservado;

2.1.18.4.3.2 Credencial de segurança do usuário;

2.1.18.4.4 A solução deverá recusar o acesso de usuários a documentos que possuam grau de sigilo superior à sua credencial de segurança.

2.1.18.4.5 A solução deverá garantir que documentos sem atribuição de grau de sigilo ou identificação de outras restrições de acesso, provenientes de fontes externas ao sistema, estejam sujeitos às políticas de controle de acesso e de sigilo.

2.1.18.4.6 A solução deverá ser capaz de manter a marcação de restrição de acesso original durante a importação de documentos a partir de fontes externas ao sistema.

2.1.18.4.7 A solução deverá permitir que um dos itens abaixo seja selecionado durante a configuração:

2.1.18.4.7.1 Graus de sigilo e restrições de acesso a serem atribuídos a classes e dossiês/processos;

2.1.18.4.7.2 Classes e dossiês/processos sem grau de sigilo ou outras restrições de acesso.

2.1.18.4.8 Em caso de erro ou reavaliação, o administrador autorizado tem que ser capaz de alterar o grau de sigilo ou outra restrição de acesso de todos os documentos arquivísticos de um dossiê/processo ou de uma classe, numa única operação.

2.1.18.4.8.1 A informação quanto à desclassificação, reclassificação, redução do prazo de sigilo ou alteração de restrição de acesso deverá ser registrada nos logs de auditoria.

2.1.18.4.9 A solução deverá garantir que o grau de sigilo ou outra restrição de acesso de um documento importado esteja associado a um usuário autorizado com a credencial de segurança pertinente para receber o documento.

2.1.18.4.10 A solução deverá permitir somente ao usuário autorizado, mediante confirmação, a desclassificação, redução do grau de sigilo ou alteração de restrição de acesso de um documento.

2.1.18.4.10.1 A informação quanto à desclassificação, reclassificação, redução do prazo de sigilo ou alteração de restrição de acesso deverá ser registrada nos logs de auditoria.

2.1.18.4.11 A solução deverá impedir que um documento com classificação de sigilo seja eliminado.

2.1.18.4.12 A solução deverá implementar metadados nos níveis de dossiê, documento ou cópia truncada de documento para controlar o acesso à informação com restrição de acesso.

2.1.18.4.13 A solução deverá permitir a um usuário autorizado fazer uma cópia truncada de um documento, com o objetivo de não alterar o original.

2.1.18.4.14 A solução deverá possibilitar a ocultação de informação sigilosa contida no documento original, permitindo:

2.1.18.4.14.1 Retirada de páginas de um documento;

2.1.18.4.14.2 Adição de retângulos opacos para ocultar nomes ou palavras sensíveis;

2.1.18.4.14.3 Quaisquer outros recursos necessários para formatos de vídeo ou áudio, caso existam.

2.1.18.4.15 Quando uma cópia truncada é produzida, a solução deverá registrar essa ação nos metadados do documento e da cópia truncada, incluindo, pelo menos, data, hora, motivo e quem a produziu.

2.1.18.4.16 A solução deverá registrar uma referência cruzada a uma cópia truncada nos mesmos dossiês/processos e documentos em que se encontra o documento original.

2.1.19 Retenção e Gestão de Registros

2.1.19.1 Configuração da tabela de temporalidade e destinação de documentos

2.1.19.1.1 A Solução deverá prover funcionalidades para definição e manutenção de tabela de temporalidade e destinação de documentos, associada ao plano de classificação.

2.1.19.1.2 A Solução deverá permitir manter tabela de temporalidade e destinação de documentos com as seguintes informações:

2.1.19.1.2.1 identificador da classe;

2.1.19.1.2.2 Prazo de guarda na idade corrente;

2.1.19.1.2.3 Evento que determina o início de contagem do prazo de retenção na idade corrente;

2.1.19.1.2.4 Prazo de guarda na idade intermediária;

2.1.19.1.2.5 Evento que determina o início de contagem do prazo de retenção na idade intermediária;

2.1.19.1.2.6 Destinação final;

2.1.19.1.2.7 Sigilo associado à classe;

2.1.19.1.2.8 Observações.

2.1.19.1.3 A Solução deverá permitir prever, pelo menos, as seguintes situações para destinação:

2.1.19.1.3.1 Apresentação dos documentos para reavaliação em data futura;

2.1.19.1.3.2 Eliminação;

2.1.19.1.3.3 Exportação para transferência;

2.1.19.1.3.4 Exportação para recolhimento (guarda permanente).

2.1.19.1.4 A Solução deverá possibilitar a iniciação automática da contagem dos prazos de guarda referenciados na tabela de temporalidade e destinação de documentos, pelo menos, a partir dos seguintes eventos:

2.1.19.1.4.1 Abertura de dossiê/processo;

2.1.19.1.4.2 Arquivamento de dossiê/processo;

2.1.19.1.4.3 Desarquivamento de dossiê/processo;

2.1.19.1.4.4 Inclusão de documento sigiloso em um dossiê/processo, se aplicável.

2.1.19.1.5 Acontecimentos específicos, descritos na tabela de temporalidade e destinação como, por exemplo, cinco anos a contar da data de aprovação das contas, quando não puderem ser detectados automaticamente pela solução, deverão poder ser informados ao sistema por um usuário autorizado.

2.1.19.1.6 A Solução deverá possibilitar que a definição dos prazos de guarda seja expressa por:

2.1.19.1.6.1 Um número inteiro de meses ou

2.1.19.1.6.2 Um número inteiro de anos.

2.1.19.1.7 A Solução deverá limitar a definição e a manutenção (alteração, inclusão e exclusão) da tabela de temporalidade e destinação de documentos a usuários autorizados.

2.1.19.1.8 A Solução deverá permitir que um usuário autorizado altere o prazo ou destinação prevista em um item da tabela de temporalidade e destinação de documentos e garantir que a alteração tenha efeito em todos os documentos ou dossiês/processos associados àquele item.

2.1.19.1.9 A Solução deverá ser capaz de manter o histórico das alterações realizadas na tabela de temporalidade e destinação de documentos.

2.1.19.1.10 A Solução deverá ser capaz de importar e exportar total ou parcialmente uma tabela de temporalidade e destinação de documento.

2.1.19.1.11 A Solução deverá prover funcionalidades para elaboração de relatórios que apoiem a gestão da tabela de temporalidade e destinação, incluindo a capacidade de:

2.1.19.1.11.1 Gerar relatório completo da tabela de temporalidade e destinação de documentos;

2.1.19.1.11.2 Gerar relatório parcial da tabela de temporalidade e destinação de documentos a partir de um ponto determinado na hierarquia do plano de classificação;

2.1.19.1.11.3 Gerar relatório dos documentos ou dossiês/processos aos quais foi atribuído um determinado prazo de guarda.

2.1.19.2 Aplicação da tabela de temporalidade e destinação de documentos

2.1.19.2.1 A solução deverá fornecer recursos integrados à tabela de temporalidade e destinação de documentos para implementar as ações de destinação.

2.1.19.2.2 Para cada dossiê/processo, a solução deverá permitir acompanhar automaticamente os prazos de guarda determinados para a classe à qual pertence.

2.1.19.2.3 A solução deverá fornecer funcionalidades para informar ao usuário autorizado sobre os documentos ou dossiês/processos que já cumpriram ou estão para cumprir o prazo de guarda previsto.

2.1.19.2.4 A solução deverá fornecer funcionalidades para gerenciar o processo de destinação, que tem que ser iniciado por usuário autorizado e cumprir os seguintes passos:

2.1.19.2.4.1 Identificar automaticamente os documentos ou dossiês/processos que atingiram os prazos de guarda previstos;

2.1.19.2.4.2 Informar o usuário autorizado sobre todos os documentos ou dossiês/processos que foram identificados no passo anterior;

2.1.19.2.4.3 Possibilitar a alteração do prazo ou destinação previstos para aqueles documentos ou dossiês/processos, caso necessário;

2.1.19.2.4.4 Proceder à ação de destinação quando confirmada pelo usuário autorizado.

2.1.19.2.5 A solução tem sempre que pedir confirmação antes de realizar as ações de destinação.

2.1.19.2.6 A solução deverá restringir as funções de destinação somente a usuários autorizados.

2.1.19.2.7 A solução deverá permitir adotar automaticamente a temporalidade e a destinação vigentes na nova classe, quando um administrador transferir documentos ou dossiês/processos de uma classe para outra, em virtude de uma reclassificação,

2.1.19.3 Exportação de documentos

2.1.19.3.1 A solução deverá ser capaz de exportar documentos e dossiês/processos digitais e seus metadados para outro sistema dentro ou fora do órgão ou entidade.

2.1.19.3.2 A solução ao exportar os documentos e dossiês/processos de uma classe para executar uma ação de transferência ou recolhimento, deverá ser capaz de exportar todos os documentos e dossiês/processos da classe incluídos na ação de destinação, com seus respectivos volumes, documentos e metadados associados.

2.1.19.3.3 A solução deverá ser capaz de exportar um documento e dossiê/processo ou grupo de documentos e dossiês/processos numa sequência de operações, de modo que:

2.1.19.3.3.1 O conteúdo, o contexto e a estrutura dos documentos não se degradem;

2.1.19.3.3.2 Todos os componentes de um documento digital sejam exportados como uma unidade. Por exemplo, uma mensagem de correio eletrônico e seus respectivos anexos;

2.1.19.3.3.3 Todos os metadados do documento sejam relacionados a ele de forma que as ligações possam ser mantidas no novo sistema;

2.1.19.3.3.4 Todas as ligações entre documentos, volumes e dossiês/processos sejam mantidas.

2.1.19.3.4 A solução deverá permitir a exportação de todos os tipos de documentos que está apta a capturar.

2.1.19.3.5 A solução deverá produzir um relatório detalhado sobre qualquer falha que ocorra durante uma exportação. O relatório deverá permitir identificar os documentos e dossiês/processos que originaram erros de processamento ou cuja exportação não tenha sido bem-sucedida.

2.1.19.3.6 A solução deverá conservar todos os documentos e dossiês/processos digitais que foram exportados, pelo menos até que tenham sido importados no sistema destinatário com êxito.

2.1.19.3.7 A solução deverá manter metadados relativos a documentos e dossiês/processos que foram exportados. O administrador deve indicar o subconjunto de metadados que deverá ser mantido.

2.1.19.3.8 A solução deverá permitir gerar listagem para descrever documentos e dossiês/processos digitais que estão sendo exportados.

2.1.19.4 Eliminação

2.1.19.4.1 A solução deverá permitir restringir a função de eliminação de documentos ou dossiês/processos somente a usuários autorizados.

2.1.19.4.2 A solução deverá pedir confirmação da eliminação a um usuário autorizado antes que qualquer ação seja tomada com relação ao documento e dossiê/processo e cancelar o processo de eliminação se a confirmação não for dada.

2.1.19.4.3 A solução deverá impedir sempre a eliminação de uma unidade de arquivamento digital ou de qualquer parte de seu conteúdo, a não ser quando estiver de acordo com a tabela de temporalidade e destinação de documentos. A eliminação será devidamente registrada em trilha de auditoria.

2.1.19.4.4 A solução deverá avisar ao usuário autorizado quando um documento ou dossiê/processo que estiver sendo eliminado se encontrar relacionado a outro; os sistemas também têm de suspender o processo até que seja tomada uma das medidas abaixo:

2.1.19.4.4.1 Confirmação pelo usuário autorizado para prosseguir ou cancelar o processo;

2.1.19.4.4.2 Produção de um relatório especificando os documentos ou dossiês/processos

2.1.19.4.5 A solução deverá garantir que as referências sejam verificadas antes de eliminar o arquivo digital, quando um documento tem várias referências armazenadas no sistema.

2.1.19.4.6 A solução deverá produzir um relatório detalhando de qualquer falha que ocorra durante uma eliminação. O relatório deverá permitir a identificação dos documentos cuja eliminação não tenha sido bem-sucedida.

2.1.19.4.7 A solução deverá exigir do usuário autorizado a confirmação, quando eliminar documentos ou dossiês/processos híbridos, de que a parte na forma não digital desses documentos ou dossiês/processos seja eliminada também antes de confirmar a eliminação da parte digital.

2.1.19.4.8 A solução deverá permitir gerar relatório com os documentos e dossiês/processos que serão eliminados.

2.1.19.4.9 A solução deverá permitir manter metadados relativos a documentos e dossiês/processos eliminados. O administrador deve indicar o subconjunto de metadados que deverá ser mantido.

2.1.19.4.10 A solução deverá avisar ao usuário autorizado quando um documento ou dossiê/processo atingir o seu tempo de retenção estabelecido, para que se proceda a eliminação dos mesmos.

2.1.19.5 Avaliação e destinação de documentos não digitais e híbridos

2.1.19.5.1 A solução deverá permitir aplicar a mesma tabela de temporalidade e destinação de documentos para os documentos não digitais, digitais ou híbridos.

2.1.19.5.2 A solução deverá permitir acompanhar os prazos de guarda dos documentos não digitais e deve dar início aos procedimentos de eliminação ou transferência desses documentos, tomando em consideração suas especificidades.

2.1.19.5.3 A solução deverá permitir alertar o administrador sobre a existência e a localização de uma parte não digital associada a um documento híbrido que esteja destinado a ser exportado, transferido ou eliminado.

2.1.19.5.4 A solução deverá ser capaz de manter, para cada documento ou dossiê/processo, o histórico das mudanças de mídia sofridas por esse documento ou dossiê/processo.

2.1.19.5.5 A solução deverá fornecer um recurso de acompanhamento para monitorar e registrar informações acerca do local atual e do deslocamento de dossiês/processos digitais e não digitais.

2.1.19.5.6 A função de acompanhamento de mudança de suporte ou de local tem que registrar metadados que incluam:

2.1.19.5.6.1 Identificador do documento atribuído pelo sistema;

2.1.19.5.6.2 Localização atual e localizações anteriores (definidas pelo usuário);

2.1.19.5.6.3 Data e hora do envio/deslocamento;

2.1.19.5.6.4 Data e hora da recepção no novo local;

2.1.19.5.6.5 Destinatário;

2.1.19.5.6.6 Usuário responsável pela mudança de suporte ou de local (sempre que for adequado);

2.1.19.5.6.7 Método da mudança de suporte ou de local.

2.1.20 Gestão de Conteúdo

2.1.20.1 Automação de Processos

2.1.20.1.1 A solução deve permitir a tramitação de documentos de forma que cada unidade tenha acesso ao documento em tempo real sob a execução do orçamento, contratos e prestação de contas, de forma simples e eficaz, porém garantindo a integridade e imutabilidade do documento;

2.1.20.1.2 O sistema deve garantir a confiabilidade de que as cláusulas contidas em determinado contrato sejam alteradas apenas se houver anuência das partes envolvidas;

2.1.20.1.3 O sistema deve garantir a rastreabilidade das transações e alterações ocorridas no contrato durante todo o seu ciclo de vida;

2.1.20.1.4 O sistema deve garantir a execução automática de todas as cláusulas pré-definidas, a cada etapa do contrato, aplicando a cláusula penal prevista no contrato.

2.1.20.1.5 O sistema deve permitir a automatização de tarefas recorrentes da gestão contratual, incluindo:

2.1.20.1.5.1 Geração de minutas contratuais a partir de modelos parametrizados;

2.1.20.1.5.2 Emissão de alertas sobre marcos contratuais, tais como vencimentos, reajustes, aditivos, garantias e entregas pactuadas;

2.1.20.1.5.3 Registro automatizado de eventos contratuais relevantes (assinaturas, publicações, alterações, encerramentos);

2.1.20.1.6 O sistema deve permitir a integração com sistemas orçamentários e financeiros para vincular contratos a empenhos, liquidações e pagamentos, com atualização automática da execução financeira, deve permitir ainda a integração conforme item 2.1.16.10, permitindo a criação de fluxos a partir dele.

2.1.20.1.7 A solução deverá possuir um recurso de fluxo de trabalho que permita fornecer os passos necessários para o cumprimento de trâmites. Nesse caso, cada passo significa o deslocamento de um documento ou dossiê/processo de um participante para outro, a fim de serem objeto de ações.

2.1.20.1.8 A solução deverá ter capacidade, sem limitações, de estabelecer o número necessário de trâmites nos fluxos de trabalho.

2.1.20.1.9 O fluxo de trabalho da solução deverá permitir disponibilizar uma função para avisar um participante do fluxo, de que um documento lhe foi enviado, especificando a ação necessária.

2.1.20.1.10 O fluxo de trabalho da solução deverá permitir o uso de envio de correio eletrônico no próprio sistema, para que um usuário possa informar a outros usuários sobre documentos que requeiram sua atenção.

2.1.20.1.11 O recurso de fluxo de trabalho da solução deverá permitir que fluxos de trabalho pré-programados sejam definidos, alterados e mantidos exclusivamente por usuário autorizado.

2.1.20.1.12 A solução deverá permitir que o administrador possa autorizar usuários individuais a redistribuir tarefas ou ações de um fluxo de trabalho a um usuário ou grupo diferente do previsto.

2.1.20.1.13 A solução deverá permitir registrar a tramitação de um documento, a fim de que os usuários possam conhecer a situação de cada documento no fluxo de trabalho.

2.1.20.1.14 A solução deverá gerenciar os documentos em filas de espera, que possam ser examinadas e controladas por usuário autorizado em um fluxo de trabalho.

2.1.20.1.15 A solução deverá ter a capacidade de deixar que os usuários visualizem a fila de espera de trabalhos a eles destinados e selecionem os itens a serem trabalhados no recurso de fluxo de trabalho.

2.1.20.1.16 A solução deverá fornecer fluxos condicionais de acordo com os dados de entrada do usuário ou a partir dos dados da solução. Os fluxos que remetem o documento a um dos participantes dependem de uma condição determinada por um deles.

2.1.20.1.17 A solução deverá fornecer um histórico de movimentação dos documentos do fluxo de trabalho.

2.1.20.1.18 A solução deverá permitir que usuários autorizados interrompam ou suspendam temporariamente um fluxo com o objetivo de executar outro trabalho.

2.1.20.1.19 A solução deverá permitir incluir processamento condicional, isto é, permitir que um fluxo de trabalho seja suspenso para aguardar a chegada de um documento e prossiga automaticamente quando este for recebido.

2.1.20.1.20 A solução deverá permitir reconhecer indivíduos e grupos de trabalho como participantes no fluxo de trabalho.

2.1.20.1.21 A solução deverá permitir que a captura de documentos desencadeie, automaticamente, fluxos de trabalho.

2.1.20.1.22 A solução deverá fornecer meios de elaboração de relatórios completos para permitir que gestores monitorem a tramitação dos documentos e o desempenho dos participantes.

2.1.20.1.23 A solução deverá registrar a tramitação de um documento em seus metadados. Os metadados referentes à tramitação devem registrar data e hora de envio e recebimento, e a identificação do usuário.

2.1.20.1.24 A solução deverá assegurar que qualquer modificação nos atributos dos fluxos leve em conta os documentos a ele vinculados.

2.1.20.1.25 A solução de gestão de conteúdos deve possuir funcionalidade nativa para o desenho e execução de fluxos de trabalho;

2.1.20.1.26 A ferramenta de desenho deve ser integrada ao gerenciador de conteúdo, ou seja, ela deve ser acessada diretamente por opção de menu, a segurança e usuários do fluxo devem ser gerenciados pela solução e deve ser possível aplicar todos os controles que a solução possui sobre o modelo de fluxo de trabalho criado, como por exemplo, controle de versão;

2.1.20.1.27 Os desenhos dos fluxos de trabalho devem ser realizados de maneira gráfica, sem a necessidade de instalação de qualquer componente ou software na estação cliente, e compatível com padrão BPMN (Business Process Management Notation);

2.1.20.1.28 O fluxo de trabalho deve ser capaz de exportar informações do repositório em XML, tais como metadados, templates, pastas, para integração com sistemas legados;

2.1.20.1.29 A solução deverá ser capaz de importar arquivos XML com informações de sistemas legados para tratamento no fluxo de trabalho;

2.1.20.1.30 A solução deverá permitir a definição de processo de forma gráfica e amigável ao usuário, possibilitando desenho através de interface gráfica com "Drag And Drop", sem codificação.

2.1.20.2 Pesquisa

2.1.20.2.1 A solução deverá fornecer facilidades para pesquisa, localização e apresentação dos documentos.

2.1.20.2.2 A solução deverá permitir executar pesquisa de forma integrada, isto é, apresentar todos os documentos e dossiês/processos, sejam eles digitais, híbridos ou não digitais, que satisfaçam aos parâmetros da pesquisa.

2.1.20.2.3 A solução deverá permitir que todos os metadados de gestão de um documento ou dossiê/processo possam ser pesquisados.

2.1.20.2.4 A solução deverá permitir que o conteúdo dos documentos em forma de texto possa ser pesquisado.

2.1.20.2.5 A solução deverá permitir que um documento ou dossiê/processo possa ser recuperado por meio de todas as formas de identificação implementadas, incluindo, no mínimo:

2.1.20.2.5.1 Identificador;

2.1.20.2.5.2 Título;

2.1.20.2.5.3 Assunto;

2.1.20.2.5.4 Datas;

2.1.20.2.5.5 Interessado;

2.1.20.2.5.6 Autor/redator/originador;

2.1.20.2.5.7 Classificação de acordo com plano ou código de classificação.

2.1.20.2.6 A solução deverá fornecer uma interface que possibilite a pesquisa combinada de metadados e de conteúdo do documento por meio dos operadores booleanos “e”, “ou” e “não”.

2.1.20.2.7 A solução deverá permitir que os termos utilizados na pesquisa possam ser qualificados, especificando-se um metadado ou o conteúdo do documento como fonte de busca.

2.1.20.2.8 A solução deverá permitir a utilização de caracteres curinga e de truncamento à direita para pesquisa de metadados. Por exemplo, o argumento de pesquisa “Bra*il” pode recuperar “Brasil” e “Brazil”, e o argumento de pesquisa “Arq*” pode recuperar “Arquivo”, “Arquivística”.

2.1.20.2.9 A solução deverá permitir a utilização de caracteres curinga e de truncamento à direita para pesquisa no conteúdo do documento.

2.1.20.2.10 A solução deverá permitir que os usuários armazenem pesquisas para reutilização posterior.

2.1.20.2.11 A solução deverá permitir que os usuários refinem pesquisas já realizadas.

2.1.20.2.12 A solução deverá permitir que usuários autorizados configurem e alterem os campos default de pesquisa de forma a definir metadados como campos de pesquisa.

2.1.20.2.13 A solução deverá permitir a pesquisa e recuperação de uma unidade de arquivamento completa e exibir a lista de todos os documentos que a compõem, como uma unidade e num único processo de recuperação.

2.1.20.2.14 A solução deverá permitir limitar o acesso a qualquer informação (metadado ou conteúdo de um documento arquivístico) se restrições de acesso e questões de segurança assim determinarem.

2.1.20.2.15 A solução deverá permitir apresentar o resultado da pesquisa como uma lista de documentos e dossiês/processos digitais, não digitais ou híbridos que cumpram os parâmetros da consulta e deve notificar o usuário se o resultado for nulo.

2.1.20.2.16 A solução deverá oferecer ao usuário as opções após apresentar o resultado da pesquisa:

2.1.20.2.16.1 Visualizar os documentos e dossiês/processos resultantes da pesquisa;

2.1.20.2.16.2 Redefinir os parâmetros de pesquisa e fazer nova consulta.

2.1.20.3 A solução deverá permitir a configuração do formato da lista de resultados de pesquisa pelo usuário ou administrador, incluindo recursos e funções como:

- 2.1.20.3.1 Seleção da ordem em que os resultados de pesquisa são apresentados;
- 2.1.20.3.2 Determinação do número de resultados de pesquisa exibidos em cada tela;
- 2.1.20.3.3 Estabelecimento do número máximo de resultados para uma pesquisa;
- 2.1.20.3.4 Armazenamento dos resultados de uma pesquisa;
- 2.1.20.3.5 Definição dos metadados a serem exibidos nas listas de resultados de pesquisa.

2.1.20.4 A solução deverá apresentar o conteúdo de todos os documentos arquivísticos digitais definidos pelo programa de gestão de documentos, de forma que:

- 2.1.20.4.1 Preserve as características de exibição visual e de formato apresentados pela aplicação geradora;
- 2.1.20.4.2 Exiba todos os componentes do documento digital em conjunto, como uma unidade.

2.1.20.5 No caso de necessidade de captura de documentos em formatos de arquivo não previstos no programa de gestão de documentos, a solução deverá permitir o download do documento para que possa ser visualizado em outro ambiente.

- 2.1.20.5.1 A solução deverá permitir a impressão dos documentos e deverá permitir manter a forma documental apresentada pelas aplicações geradoras.
- 2.1.20.5.2 No caso de necessidade de captura de documentos em formatos de arquivo não previstos no programa de gestão de documentos, a solução deverá permitir o download do documento para que ele possa ser visualizado em outro ambiente.
 - 2.1.20.5.2.1 A solução deverá permitir a exibição em tela de todos os metadados associados aos documentos e dossiês/processos resultantes de uma pesquisa.
 - 2.1.20.5.2.2 A solução deverá permitir a impressão de uma lista dos documentos e dossiês/processos resultantes de uma pesquisa.
 - 2.1.20.5.2.3 A solução deverá permitir que os metadados exibidos nas listas a que se referem os requisitos 2.1.20.3 possam ser definidos pelo usuário.
 - 2.1.20.5.2.4 A solução deverá ser capaz de realizar pesquisa e exibição de documentos e dossiês/processos, simultaneamente, para diversos usuários.

2.1.20.6 Gestão de Documentos

- 2.1.20.6.1 Elaboração de documentos

2.1.20.6.1.1 A solução deve permitir a visualização online sem custo adicional no licenciamento de, pelo menos, os seguintes formatos:

2.1.20.6.1.1.1 TIFF;

2.1.20.6.1.1.2 JPG;

2.1.20.6.1.1.3 PDF/PDF-A;

2.1.20.6.1.1.4 DOC;

2.1.20.6.1.1.5 DOCX;

2.1.20.6.1.1.6 XLS;

2.1.20.6.1.1.7 XLSX;

2.1.20.6.1.1.8 PPT;

2.1.20.6.1.1.9 PPTX;

2.1.20.6.1.1.10 VSD (MS-Visio);

2.1.20.6.1.1.11 HTML;

2.1.20.6.1.1.12 TXT;

2.1.20.6.1.1.13 RTF;

2.1.20.6.1.1.14 GIF;

2.1.20.6.1.1.15 BMP.

2.1.20.6.1.1.16 DWG.

2.1.20.6.1.2 A solução deverá gerar automaticamente miniaturas (thumbnails) da primeira página dos documentos para exibição na lista de navegação do repositório e lista de resultados de pesquisa, para pelo menos, os arquivos de DOC, DOCX, XLS, XLSX, PPT, PPTX, PDF, PDF/A, DWG e imagens raster.

2.1.20.6.1.3 A solução deve permitir a conversão de documentos para formato PDF e PDF/A independente do formato de origem, com opção de inclusão ou não de todas as marcações, anotações e restrições que componham o documento;

2.1.20.6.1.4 A solução deve permitir a criação de anotações nas imagens dos documentos, independente do formato, com pelo menos as seguintes funcionalidades: anotação com linhas, setas e balões, inclusão de texto livre e em caixa, inclusão de imagens (carimbos) e marcação de texto (em documentos de texto);

- 2.1.20.6.1.5 As anotações incluídas em um documento não podem alterar o documento original, devendo estas informações serem armazenadas apartadas do arquivo do documento;
- 2.1.20.6.1.6 A solução deve permitir selecionar a visualização das anotações de um documento ou não, e deve informar ao usuário caso o documento possua algum tipo de anotação atribuída;
- 2.1.20.6.1.7 A solução deverá gerir metadados relativos à preservação dos documentos e seus respectivos componentes.
- 2.1.20.6.1.8 A solução deverá ser capaz de exibir/reproduzir o conteúdo de documentos que incluam imagem fixa, imagem em movimento e som.
- 2.1.20.6.1.9 A solução deverá possibilitar a definição dos metadados a serem impressos.
- 2.1.20.6.1.10 A solução deverá permitir a impressão de uma lista dos documentos que compõem um dossiê/processo.
- 2.1.20.6.1.11 A solução deverá permitir que todos os documentos de um dossiê/processos sejam impressos em uma ou mais operações.
- 2.1.20.6.1.12 A solução deverá ter mecanismos destinados a exportar, para fins de reprodução, documentos que não possam ser impressos, tais como documentos sonoros, vídeos e multimídia.
- 2.1.20.6.1.13 A solução deve permitir que usuários naveguem na estrutura de objetos do repositório através de pastas hierárquicas com a opção de filtrar os tipos de objetos exibidos;
- 2.1.20.6.1.14 A solução deve permitir que usuários enviem vários documentos ao mesmo tempo por e-mail, sendo que os documentos serão compactados e anexados à mensagem;
- 2.1.20.6.1.15 A solução deve permitir a criação de, pelo menos, os seguintes tipos de objeto: atalho para outro objeto do repositório, coleção de objetos, documentos, pastas, formulários eletrônicos, objetos para referência a documentos físicos, links para URL's externas e relatórios;
- 2.1.20.6.1.16 A solução deverá permitir automatizar a produção de documentos por meio da exibição de formulários e modelos predefinidos pelo programa de gestão arquivística de documentos.
- 2.1.20.6.1.17 A solução deverá permitir vincular à automatização da produção de documentos:
- 2.1.20.6.1.17.1 Numeração automática por espécie documental;
 - 2.1.20.6.1.17.2 Classificação arquivística;
 - 2.1.20.6.1.17.3 Marcação de sigilo legal;
 - 2.1.20.6.1.17.4 Autuação de processo;
 - 2.1.20.6.1.17.5 Outras.

2.1.20.6.2 Elaboração de Formulários

2.1.20.6.2.1 A ferramenta deve ser capaz de suportar a criação de formulários eletrônicos para coletar informações estruturadas do usuário, como questionários, enquetes, metadados, entre outros;

2.1.20.6.2.2 O formulário deve poder ser utilizado pela ferramenta de fluxo de trabalho para customização da interface com o usuário nos passos que necessitem de uma interação do usuário com o fluxo. Também deve ser possível iniciar um fluxo de trabalho a partir de um formulário;

2.1.20.6.2.3 O formulário deve ser armazenado pelo repositório e deve receber tratamento igual a outros itens do repositório, como controle de versão e segurança;

2.1.20.6.2.4 O formulário deve ser feito em HTML, podendo ser utilizado CSS e Javascript para enriquecer a experiência do usuário;

2.1.20.6.2.5 A solução deverá permitir minimamente campos de preenchimento obrigatório, opcional, oculto e somente leitura por atividade e sem codificação;

2.1.20.6.2.6 A solução deverá permitir campos com indicação de valor padrão (default);

2.1.20.6.2.7 A solução deverá possuir recurso de validação de campos;

2.1.20.6.2.8 A solução deverá possuir máscaras de entrada de dados para campos;

2.1.20.6.3 Permissionamento

2.1.20.6.3.1 A definição de permissões deve ser hierárquica entre a estrutura de pastas e subpastas, podendo ser alterada em qualquer objeto, quebrando a herança, por usuários que tenham permissão;

2.1.20.6.3.2 As permissões devem ser configuradas por usuários específicos ou grupos de usuários;

2.1.20.6.3.3 Ao alterar uma permissão de uma pasta, o usuário deve ter a opção de replicar as alterações em todos os seus objetos filho, de maneira hierárquica;

2.1.20.6.3.4 Cada objeto do repositório deve ter um usuário como proprietário definido em suas permissões;

2.1.20.6.3.5 Os objetos no repositório devem conter URL's persistentes para que seja feito o acesso direto a eles. Estas URL's não podem ser alteradas quando um objeto é movido de pasta ou possuir uma nova versão. Esta URL deve apontar sempre para a versão mais atual do objeto;

2.1.20.6.3.6 A solução deve prover mecanismo de controle de permissionamento nos objetos com, pelo menos, as seguintes possibilidades: visualizar o objeto, visualizar o conteúdo do objeto,

modificar seus atributos, adicionar itens ou versões, realizar o check-in/check-out, excluir o objeto ou versões e alterar suas permissões;

2.1.20.6.4 Versionamento

2.1.20.6.4.1 A solução deve controlar a alteração em documentos mantendo um histórico de versões, sendo permitido a usuários autorizados excluir ou reverter versões anteriores;

2.1.20.6.4.2 A solução deverá registrar o status de transmissão do documento, ou seja, se é minuta, original ou cópia no fluxo de trabalho.

2.1.20.6.4.3 A solução deverá manter o identificador único do documento, e controlar as diversas versões deste documento.

2.1.20.6.4.4 Deve ser possível controlar as versões principais e secundárias (1.0, 1.1, 1.2, 2.0) dos objetos;

2.1.20.6.4.5 Deve ser possível controlar a permissão de usuários, impossibilitando que eles visualizem as versões secundárias de objetos, ou seja, esses usuários só poderão visualizar documentos em versões principais;

2.1.20.6.4.6 Qualquer alteração em objetos do repositório deve gerar uma nova versão;

2.1.20.6.4.7 O repositório deve exibir seus objetos sempre na versão mais atual, podendo o usuário, com permissões para tal, visualizar o histórico de versões;

2.1.20.6.4.8 A solução deve realizar o gerenciamento de check-in e check-out de documentos, de maneira que documentos que estejam em estado de check-out não possam ser alterados por outros usuários;

2.1.20.6.4.9 Um administrador deve ter a permissão para desfazer bloqueios de objetos em check-out;

2.1.20.6.4.10 Ao realizar o check-in de um documento, o usuário deve ter a possibilidade de incluir uma nova versão do objeto ou apenas desfazer o bloqueio do objeto;

2.1.20.6.4.11 A solução deverá manter o histórico de versões de todos os documentos com versionamento habilitado

2.1.20.6.4.12 A solução deverá permitir recuperar documento de versão anterior.

2.1.20.6.4.13 A solução deverá possuir um sistema automático de controle de versões para rastrear mudanças em documentos ao longo do tempo.

2.1.20.6.4.14 A solução deverá permitir recuperar e visualizar versões anteriores de um documento, incluindo a capacidade de restaurar uma versão anterior, se necessário.

2.1.20.6.4.15 A solução deverá ter rotina que permita a aprovação formal de novas versões antes de serem disponibilizadas para todos os usuários.

2.1.20.6.4.16 Deve ter controle de versões mesmo para documentos criptografados, garantindo a integridade dos dados ao longo do tempo.

2.1.20.6.4.17 A solução deverá permitir que os usuários selecionem pelo menos uma das seguintes ações:

2.1.20.6.4.17.1 registrar todas as versões do documento como um só documento arquivístico;

2.1.20.6.4.17.2 registrar uma única versão do documento como um documento arquivístico;

2.1.20.6.4.17.3 registrar cada uma das versões do documento, separadamente, como um documento arquivístico.

2.1.20.6.4.18 A solução não deve considerar minutas como versão. Cada versão deve ser dotada de completeza.

2.1.20.6.5 Colaboração

2.1.20.6.5.1 A solução deve permitir que para cada objeto do repositório seja possível iniciar uma discussão atrelada ao registro com funcionalidades de inclusão de comentário, respostas a comentários aninhadas, marcação de usuário e avaliação do comentário;

2.1.20.6.5.2 A ferramenta deve disponibilizar segurança específica para as discussões, tais como leitura, criação e capacidade total de incluir/apagar discussões;

2.1.20.6.5.3 A solução deverá possuir mecanismos intuitivos para compartilhar documentos com colegas de equipe, interna ou externamente, com opções de permissões configuráveis.

2.1.20.6.6 Assinatura digital

2.1.20.6.6.1 A solução deverá ser capaz de prover meios para se verificar a origem e a integridade dos documentos com assinatura digital.

2.1.20.6.6.2 Somente administradores autorizados têm que ser capazes de incluir, remover ou atualizar no sistema os certificados digitais de computadores ou de usuários.

2.1.20.6.6.3 A solução deverá ser capaz de verificar a validade da assinatura digital no momento da captura do documento.

2.1.20.6.6.4 A solução, no processo de verificação da assinatura digital, tem que ser capaz de registrar, como metadado, o seguinte:

2.1.20.6.6.4.1 Validade da assinatura verificada;

2.1.20.6.6.4.2 Registros da verificação da assinatura;

2.1.20.6.6.4.3 Data e hora em que ocorreu a verificação.

2.1.20.6.6.5 A solução deverá ser capaz de armazenar, juntamente com o componente digital, conforme os metadados do e-ARQ Brasil, as informações de certificação a seguir:

2.1.20.6.6.5.1 Assinatura digital;

2.1.20.6.6.5.2 Certificado digital (cadeia de certificação) usado na verificação da assinatura;

2.1.20.6.6.6 A solução deverá ser compatível com as normas e padrões de Assinatura Digital do ICP Brasil.

2.1.20.6.7 Carimbo digital do tempo.

2.1.20.6.7.1 A solução deverá ter acesso a relógios e carimbador de tempo confiáveis seguindo as normas e padrões determinados pela ICP-Brasil.

2.1.20.6.7.2 A solução deverá ser capaz de verificar a validade do carimbo digital do tempo no momento da captura do documento.

2.1.20.6.7.3 A solução, no processo de verificação do carimbo digital do tempo, tem que ser capaz de registrar, nos metadados do documento, o seguinte:

2.1.20.6.7.3.1 Validade do carimbo digital do tempo;

2.1.20.6.7.3.2 Registro da verificação do carimbo digital do tempo;

2.1.20.6.7.3.3 Data e hora em que ocorreu a verificação.

2.1.20.6.8 Marcas d'água digitais

2.1.20.6.8.1 A solução deverá ser capaz de recuperar informação contida em marcas d'água digitais.

2.1.20.6.8.2 A solução deverá ser capaz de armazenar documentos arquivísticos digitais que contenham marcas d'água digitais.

2.1.20.6.8.3 Durante a conversão de um documento para PDF, deve ser possível realizar a inclusão de uma marca d'água no documento final;

2.1.20.7 Gerenciamento dos dossiês/processos

2.1.20.7.1 A solução deverá permitir registrar nos metadados as datas de abertura e de encerramento do dossiê/processo.

2.1.20.7.2 A solução deverá permitir a emissão de um aviso caso o usuário anexe um documento que já tenha sido anexado no mesmo dossiê/processo.

2.1.20.7.3 A solução deverá permitir que um dossiê/processo seja encerrado por meio de procedimentos regulamentares e somente por usuários autorizados.

2.1.20.7.4 A solução deverá permitir a consulta aos dossiês/processos já encerrados por usuários autorizados.

2.1.20.7.5 A solução deverá permitir impedir o acréscimo de novos documentos a dossiês/processos já encerrados. Dossiês/processos encerrados devem ser reabertos para receber novos documentos.

2.1.20.7.6 A solução deverá garantir sempre a integridade da relação hierárquica entre classe, dossiê/processo, volume e documento, independentemente de atividades de manutenção, ações do usuário ou falha de componentes da solução. Em hipótese alguma pode a solução permitir que uma ação do usuário ou falha da solução dê origem a inconsistência em sua base de dados.

2.1.20.7.7 A solução deverá gerar numeração sequencial sem falhas para documentos integrantes do processo digital, não se admitindo que documentos diferentes recebam a mesma numeração.

2.1.20.7.8 A solução deverá impedir a renumeração dos documentos integrantes de um processo digital.

2.1.20.7.9 A solução deverá permitir procedimentos para juntada de processos segundo a legislação específica na devida esfera e âmbito de competência. A juntada pode ser por anexação ou apensação. Este procedimento deve ser registrado nos metadados do processo.

2.1.20.7.10 A solução deverá permitir procedimentos para desapensação de processos segundo a legislação específica na devida esfera e âmbito de competência. Esse procedimento deve ser registrado nos metadados do processo.

2.1.20.7.11 A solução deverá permitir procedimentos para desentranhamento de documentos integrantes de um processo, segundo norma específica na devida esfera e âmbito de competência. Esse procedimento deve ser registrado nos metadados do processo.

2.1.20.7.12 A solução deverá permitir procedimentos para desmembramento de documentos integrantes de um processo, segundo norma específica na devida esfera e âmbito de competência. Esse procedimento deve ser registrado nos metadados do processo.

2.1.20.7.13 A solução deverá permitir o encerramento dos processos incluídos seus volumes e metadados.

2.1.20.7.14 A solução deverá permitir o desarquivamento para reativação dos processos, por usuário autorizado e obedecendo a procedimentos legais e administrativos. Para manter a integridade do processo, somente o último volume receberá novos documentos ou peças.

2.1.20.7.15 A solução deverá permitir que um volume herde, automaticamente, do dossiê/processo ao qual pertence, alguns metadados predefinidos, como, por exemplo, classes e temporalidade.

2.1.20.7.16 A solução deverá permitir a abertura de volumes para qualquer dossiê/processo que não esteja encerrado.

2.1.20.7.17 A solução deverá assegurar que um volume conterá somente documentos. Não é permitido que um volume contenha outro volume ou outro dossiê/processo.

2.1.20.7.18 A solução deverá permitir que um volume seja encerrado por meio de procedimentos regulamentares e apenas por usuários autorizados.

2.1.20.7.19 A solução deverá assegurar que, ao ser aberto um novo volume, o precedente seja automaticamente encerrado. Apenas o volume produzido mais recentemente pode estar aberto; os demais volumes existentes no dossiê/processo têm que estar encerrados.

2.1.20.7.20 A solução deverá impedir a reabertura, para acréscimo de documentos, de um volume já encerrado.

2.1.20.7.21 A solução deverá capturar documentos ou dossiês/processos não digitais e gerenciá-los da mesma forma que os digitais.

2.1.20.7.22 A solução deverá gerenciar a parte não digital e a parte digital integrantes de dossiês/processos híbridos, associando-as com o mesmo número identificador atribuído pelo sistema e o mesmo título, além de indicar que se trata de um documento arquivístico híbrido.

2.1.20.7.23 A solução deverá permitir que um conjunto específico de metadados seja configurado para os documentos ou dossiês/processos não digitais e incluir informações sobre o local de arquivamento.

2.1.20.7.24 A solução deverá dispor de mecanismos para acompanhar a movimentação do documento arquivístico não digital, de forma que fique evidente para o usuário a localização atual do documento.

2.1.20.7.25 A solução deverá possuir mecanismos de impressão e reconhecimento de códigos de barras para automatizar a introdução de dados e acompanhar a movimentação de documentos ou dossiês/processos não digitais.

2.1.20.7.26 A solução deverá assegurar que a recuperação de um documento ou dossiê/ processo híbrido permita, igualmente, a recuperação dos metadados da parte digital e da não digital.

2.1.20.7.27 A solução deverá garantir que a parte não digital e a parte digital correspondente recebam a mesma classificação de sigilo, sempre que os documentos ou dossiês/processos híbridos estiverem classificados quanto ao grau de sigilo.

2.1.20.8 Administração e Manutenção do Conteúdo

2.1.20.8.1 A Solução deverá incluir rotina de manutenção de:

2.1.20.8.1.1 Dados de usuários e de grupos;

2.1.20.8.1.2 Perfis de acesso;

2.1.20.8.1.3 Plano de classificação;

2.1.20.8.1.4 Bases de dados;

2.1.20.8.1.5 Tabelas de temporalidade.

2.1.20.8.2 A solução deverá fornecer relatórios flexíveis para que o administrador possa gerenciar os Documentos E Seu Uso. Esses Relatórios Devem Apresentar, No Mínimo:

2.1.20.8.2.1 Quantidade De Dossiês/Processos, Volumes E Itens A Partir De Parâmetros Ou tributos definidos (Tempo, Classe, Unidade Administrativa Etc.);

2.1.20.8.2.2 Estatísticas De Transações Relativas A Dossiês/Processos, Volumes E Itens;

2.1.20.8.2.3 Atividades Por Usuário.

2.1.20.8.3 A Solução Deverá Permitir Que Somente Administradores Autorizados Sejam Capazes de Realizar As Seguintes Ações:

2.1.20.8.3.1 Remover Ou Revogar Os Atributos De Segurança Dos Documentos;

2.1.20.8.3.2 Criar, alterar, remover ou revogar as credenciais de segurança dos usuários.

2.1.20.8.4 A solução deverá permitir, a um administrador autorizado, anular a operação em caso de erro do usuário ou do sistema.

2.1.20.8.5 Em situações excepcionais, o administrador tem que ser autorizado a apagar ou corrigir dossiês/processos, volumes e documentos. Nesse caso, A solução deverá:

2.1.20.8.5.1 Registrar integralmente a ação de apagar ou corrigir na trilha de auditoria;

2.1.20.8.5.2 Produzir um relatório de anomalias para o administrador;

2.1.20.8.5.3 Eliminar todo o conteúdo de um dossiê/processo ou volume, quando forem eliminados;

2.1.20.8.5.4 Garantir que nenhum documento seja eliminado se tal ação resultar na alteração de outro documento arquivístico;

2.1.20.8.6 Informar o administrador sobre a existência de ligação entre um dossiê/processo ou documento prestes a ser apagado e qualquer outro dossiê/processo ou documento, solicitando confirmação antes de concluir a operação;

2.1.20.8.7 Manter a integridade total do metadado, a qualquer momento.

2.1.20.8.7.1 Em caso de erro na inserção de metadados, o administrador terá que corrigi-lo, e a solução deverá registrar essa ação na trilha de auditoria.

2.1.21 Segurança da Informação

2.1.21.1 Autenticação, Autorização e Acesso

2.1.21.1.1 Deverá possibilitar a Integração com Login Único do SERPRO com autenticação através de SSO (Single Sign On) compatível com OpenID Connect 1.0 ou SAML 2.0, implementando as recomendações do protocolo OAuth.

2.1.21.1.2 A solução deve permitir a integração com Login Único do SERPRO, com autenticação através de Federação SSO (Single Sign-On) compatível com ao menos um dos seguintes protocolos, em ordem de prioridade:

2.1.21.1.3 OpenID Connect 1.0 com implementação de Authorization Code Flow. Caso a Solução necessite utilizar Client público, deverá ser implementada a extensão "Proof Key for Code Exchange" (PKCE).

2.1.21.1.4 SAML 2.0 com implementação de assinatura e criptografia do payload SAML.

2.1.21.1.5 Caso a solução mantenha um cadastro de usuários, deve disponibilizar uma SDK/API para gestão (criação, edição e remoção) desse cadastro.

2.1.21.1.6 Para implementar o controle de acesso, a solução deverá manter pelo menos os seguintes atributos dos usuários, de acordo com a política de segurança:

2.1.21.1.6.1 Identificador do usuário;

2.1.21.1.6.2 Autorizações de acesso;

2.1.21.1.6.3 Credenciais de autenticação.

2.1.21.1.6.4 A solução deverá exigir que o usuário esteja devidamente identificado e autenticado antes de iniciar qualquer operação no sistema.

2.1.21.1.6.5 A solução deverá garantir que os valores dos atributos de segurança e controle de acesso, associados ao usuário, estejam dentro de conjuntos de valores válidos.

2.1.21.2 Autorização e Acesso

2.1.21.2.1 A solução deverá permitir acesso às funções do sistema somente a usuários autorizados e sob controle rigoroso da administração do sistema (Permissionamento, níveis de acesso e logs), a fim de proteger a autenticidade dos documentos arquivísticos digitais.

2.1.21.2.2 Se o usuário solicitar o acesso ou pesquisa de um documento arquivístico, volume ou dossiê/processo específico a que não tenha direito de acesso, a solução deverá fornecer uma das seguintes respostas (estabelecidas durante a configuração):

2.1.21.2.2.1 Mostrar o título e os metadados do documento;

2.1.21.2.2.2 Demonstrar a existência do dossiê/processo ou documento, mas não o respectivo título nem outro metadado;

2.1.21.2.2.3 Não mostrar qualquer informação do documento, nem indicar a sua existência.

2.1.21.2.3 Somente administradores autorizados têm que ser capazes de criar, alterar, remover ou revogar permissões associadas a papéis de usuários, grupos de usuários ou usuários individuais.

2.1.21.2.4 A solução deverá aplicar, imediatamente, alterações ou revogações dos atributos de segurança de usuários e de documentos digitais.

2.1.21.2.5 A solução deverá aplicar a política de controle de acesso a documentos por grupos de usuários considerando:

2.1.21.2.5.1 A identidade do usuário e sua participação em grupos;

2.1.21.2.5.2 Os atributos de segurança, associados ao documento arquivístico digital, às classes e/ou aos dossiês/processos.

2.1.21.2.6 O acesso a documentos, a dossiês/processos ou classes, tem que ser concedido se a permissão requerida para a operação estiver associada a pelo menos um dos grupos aos quais pertença o usuário.

2.1.21.2.7 A solução deverá permitir que um usuário pertença a mais de um grupo.

2.1.21.2.8 A solução deverá permitir que alguns usuários estipulem que outros usuários, papéis ou grupos de usuários podem ter acesso aos documentos sob sua responsabilidade. Essa permissão deve ser atribuída pelo administrador.

2.1.21.2.9 A solução deverá usar os seguintes atributos do usuário ao implementar a política de controle de acesso aos documentos digitais por papéis de usuários:

2.1.21.2.9.1 Identificação do usuário;

2.1.21.2.9.2 Papéis associados ao usuário.

2.1.21.3 A solução deverá usar os seguintes atributos dos documentos digitais ao implementar a política de controle de acesso por papéis:

2.1.21.3.1 Identificação do documento digital;

2.1.21.3.2 Operações permitidas aos vários papéis de usuários, sobre as classes ou unidades de arquivamento a que o documento pertence.

2.1.21.3.3 Acessos a documentos, dossiês/processos ou classes tem que ser concedido somente se a permissão requerida para a operação estiver presente em pelo menos um dos papéis associados ao usuário.

2.1.21.3.4 O acesso dos usuários ao serviço Web devem estar protegidos por meio de canal seguro (TLS 1.3 e superiores) e uso de certificado reconhecido como de confiança pelos navegadores compatíveis.

2.1.21.3.5 A utilização de múltiplo fator de autenticação deve ser obrigatória para todos os usuários e contas administrativas (contas privilegiadas) da solução.

2.1.21.3.6 O acesso às informações relativas ao serviço deve estar restrito somente aos usuários autorizados pelo SERPRO.

2.1.21.3.7 A solução deve prover criptografia de dados e objetos armazenados usando AES (Advanced Encryption Standard) de, no mínimo, 256 bits ou outro algoritmo com força de chave equivalente ou superior, neste último caso desde que aprovado pelo SERPRO.

2.1.21.3.8 A Solução deve registrar os acessos efetuados por todos os usuários em um arquivo de log para efeito de auditoria, com informações suficientes para análise forense computacional e elaboração de relatórios gerenciais, com prazo de retenção mínimo de 1 (um) ano e até 5 anos, a critério do SERPRO, em conformidade com a Lei Nº 12.965/14 (Marco civil Internet) e Instrução Normativa GSIPR Nº5 de 30/08/21. Em casos de necessidade de informações que tenham legislação específica, o prazo de retenção deve considerar a referida legislação a partir da data de registro da coleta dos logs.

2.1.21.4 Conformidade com a legislação e regulamentações

2.1.21.4.1 A solução deverá possibilitar o armazenamento e gestão de documentos, tendo em vista a admissibilidade legal e o valor probatório dos mesmos, de acordo com o que é estabelecido na Legislação Arquivística Brasileira, conforme:

2.1.21.4.2 Lei nº 13.709/2018 - Lei Geral de Proteção de Dados Pessoais (LGPD), que dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

2.1.21.4.3 Lei Nº 12.527, DE 18 DE NOVEMBRO DE 2011 (LAI), que dispõe sobre os procedimentos a serem observados pela União, Estados, Distrito Federal e Municípios, com o fim de garantir o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal.

2.1.21.4.4 Decreto Nº 7.845, DE 14 DE NOVEMBRO DE 2012, que regulamenta procedimentos para o credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo no âmbito do Poder Executivo federal, e dispõe sobre o Núcleo de Segurança e Credenciamento, conforme o disposto nos arts. 25, 27, 29, 35, § 5º, e 37 da Lei nº 12.527, de 18 de novembro de 2011.

2.1.21.4.5 DECRETO Nº 7.724, DE 16 DE MAIO DE 2012 que regulamenta, no âmbito do Poder Executivo federal, os procedimentos para a garantia do acesso à informação e para a classificação de informações sob restrição de acesso, observados grau e prazo de sigilo, conforme o disposto na Lei nº 12.527, de 18 de novembro de 2011, que dispõe sobre o acesso a informações previsto no inciso XXXIII do caput do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição.

2.1.21.4.6 Lei Nº 12.682, de 9 de julho de 2012 que dispõe sobre a elaboração e o arquivamento de documentos em meios eletromagnéticos.

2.1.21.4.7 Lei Nº 13.874, de 20 de setembro de 2019, que dispõe da admissibilidade legal de documentos digitalizados.

2.1.21.4.8 Decreto Nº 10.278 de 18 de março de 2020, que regulamenta o disposto no inciso X do caput do art. 3º da Lei nº 13.874, de 20 de setembro de 2019, e no art. 2º-A da Lei nº 12.682, de 9 de julho de 2012, para estabelecer a técnica e os requisitos para a digitalização de documentos públicos ou privados, a fim de que os documentos digitalizados produzam os mesmos efeitos legais dos documentos originais.

2.1.21.4.9 Portaria nº 47, de 14 de fevereiro de 2020 que dispõe sobre o Código de Classificação e Tabela de Temporalidade e Destinação de Documentos relativos às atividades-meio do Poder Executivo Federal.

2.1.21.4.10 A solução deve estar em conformidade e ser compatível com os requisitos de Segurança para Provedores de Serviços em Nuvem de acordo com a Norma ISO 27017.

2.1.21.4.11 A solução deve estar em conformidade com os requisitos de Segurança definidos na norma IN GSI Nº5 de 30/08/2021.

2.1.21.4.12 Garantia de políticas e procedimentos de descarte ou reuso de recursos de forma segura. (ISO 27017 11.2.7)

2.1.21.4.13 Garantia do direito ao esquecimento para dados pessoais, conforme LGPD. (IN05 art. 19, VII)

2.1.21.5 Trilhas de Auditoria

2.1.21.5.1 A solução deverá ser capaz de registrar, na trilha de auditoria, ou log de eventos, informações acerca das ações a seguir:

- 2.1.21.5.1.1 data e hora da captura de todos os documentos;
- 2.1.21.5.1.2 responsável pela captura;
- 2.1.21.5.1.3 reclassificação, desclassificação ou redução do grau de sigilo de um documento ou dossiê/processo, com a classificação inicial e final;
- 2.1.21.5.1.4 qualquer alteração na tabela de temporalidade e destinação de documentos;
- 2.1.21.5.1.5 qualquer ação de reavaliação de documentos;
- 2.1.21.5.1.6 qualquer alteração nos metadados associados a classes, dossiês/processos ou documentos;
- 2.1.21.5.1.7 data e hora de produção, aditamento e eliminação de metadados;
- 2.1.21.5.1.8 ações de exportação e importação envolvendo os documentos;
- 2.1.21.5.1.9 usuário, data e hora de acesso ou tentativa de acesso a documentos e ao sistema;
- 2.1.21.5.1.10 tentativas de acesso negado a qualquer documento;
- 2.1.21.5.1.11 ações de eliminação de qualquer documento e seus metadados;
- 2.1.21.5.1.12 tentativas de exportação (inclusive para backup) e importação (inclusive restore);
- 2.1.21.5.1.13 alterações efetuadas nas permissões de acesso que afetem um dossiê/processo, documento ou usuário;
- 2.1.21.5.1.14 infrações cometidas contra mecanismos de controle de acesso, como por exemplo: escalação de privilégios, acesso não autorizado a dados e acesso a funcionalidades restritas, dentre outros;
- 2.1.21.5.1.15 todas as ações administrativas sobre os atributos de segurança (papéis, grupos, permissões etc.);
- 2.1.21.5.1.16 todas as ações administrativas sobre dados de usuários (cadastro, ativação, bloqueio, atualização de dados e permissões, troca de senha etc.);
- 2.1.21.5.1.17 todos os eventos de administração e manutenção das trilhas de auditoria (alarmes, cópias, configuração de parâmetros etc.).
- 2.1.21.5.2 A solução deverá registrar, em cada evento auditado, informações sobre a identidade do usuário, desde que essa identificação esteja de acordo com a política de privacidade e proteção de dados pessoais da organização e a legislação vigente.
- 2.1.21.5.3 A solução deverá permitir a leitura das trilhas de auditoria apenas a usuários autorizados.

2.1.21.5.4 A solução deverá assegurar que as informações da trilha de auditoria estejam disponíveis para inspeção, a fim de que uma ocorrência específica possa ser identificada e todas as informações correspondentes sejam claras e compreensíveis.

2.1.21.5.5 A solução deverá possuir mecanismos para realização de buscas nos eventos das trilhas de auditoria.

2.1.21.5.6 A solução deverá ser capaz de impedir qualquer modificação na trilha de auditoria.

2.1.21.5.7 Somente administradores autorizados têm que ser capazes de exportar as trilhas de auditoria sem afetar a trilha armazenada, ou transferir as trilhas de auditoria de um suporte de armazenamento para outro.

2.1.21.5.8 Somente administradores autorizados devem que ser capazes de configurar o conjunto de eventos auditáveis e seus atributos.

2.1.21.5.9 A solução deverá ser capaz de gerar um alarme para os administradores apropriados se o tamanho da trilha de auditoria exceder um limite preestabelecido.

2.1.21.5.10 Quando o espaço de armazenamento da trilha de auditoria atingir o limite preestabelecido, a solução deverá permitir somente operações auditáveis originadas por administradores. Todas as outras operações estarão bloqueadas até a liberação pelo administrador.

2.1.21.5.11 A solução deverá ser capaz de aplicar um conjunto de regras na monitoração de eventos auditados e, com base nelas, indicar a possível violação da segurança.

2.1.21.5.12 A solução deverá garantir pelo menos as seguintes regras para monitoração dos eventos auditados:

2.1.21.5.12.1 Acumulação de um número predeterminado de tentativas consecutivas de login com erro (autenticação malsucedida), conforme especificado pela política de segurança;

2.1.21.5.12.2 Ocorrência de vários login simultâneos do mesmo usuário em locais (computadores) diferentes;

2.1.21.5.12.3 Login do usuário fora do horário autorizado, após logoff no período normal.

2.1.21.5.13 A solução deverá fornecer relatórios sobre as ações que afetam classes, unidades de arquivamento e documentos, em ordem cronológica e organizados por:

2.1.21.5.13.1 Documento arquivístico, unidade de arquivamento ou classe;

2.1.21.5.13.2 Usuário;

2.1.21.5.13.3 Tipo de ação ou operação.

2.1.21.5.14 A solução deverá ser capaz de arquivar periodicamente a trilha de auditoria como documento arquivístico.

2.1.21.5.15 A solução deverá registrar na trilha de auditoria todas as alterações efetuadas nos metadados dos documentos ou dossiês/processos não digitais e híbridos.

2.1.21.5.16 A solução deverá registrar na trilha de auditoria todas as alterações ocorridas no fluxo de trabalho.

2.1.21.5.17 Em caso de remoção da cifração de documento, os seguintes metadados adicionais têm que ser registrados na trilha de auditoria:

2.1.21.5.17.1 Data e hora da remoção da cifração;

2.1.21.5.17.2 Identificação do executor da operação;

2.1.21.5.17.3 Motivo da remoção da cifração.

2.1.21.5.18 A solução deverá disponibilizar o conteúdo de auditoria coletado/extraído em formato passível de leitura em ferramentas não restritas/exclusivas (cliente de e-mail, editor de texto, planilhas, leitor de pdf, compactadores, entre outros).

2.1.21.5.19 A solução deverá disponibilizar relatório com toda a pesquisa e extração realizadas, contendo, pelo menos, as seguintes informações:

2.1.21.5.19.1 Identificação detalhada do conteúdo extraído com nome (ou UID) ou "hash" de cada arquivo;

2.1.21.5.19.2 Data e hora do início e término da pesquisa e extração;

2.1.21.5.19.3 Contas apuradas;

2.1.21.5.19.4 Volume de dados extraído; e

2.1.21.5.19.5 Identificação de quem realizou as ações.

2.1.21.5.20 A solução deverá permitir a extração automática das logs, preferencialmente via API, para alimentar um centralizador de logs ou "data Lake" do Serpro.

2.1.21.5.21 As trilhas de auditoria armazenadas em log devem também as seguintes informações:

2.1.21.5.21.1 Identificação do Usuário/conta de serviço;

2.1.21.5.21.2 Endereço IP do usuário;

2.1.21.5.21.3 Data, hora, em formato universal, considerando inclusive horário de verão.

2.1.21.5.21.4 Eventos referentes à autenticação de usuários (login/logout) incluindo logins das equipes de suporte ou contas de serviço;

2.1.21.5.21.5 Eventos operacionais e administrativos;

2.1.21.5.21.6 Valor anterior do campo ou atributo modificado;

2.1.21.5.21.7 Funcionalidade acessada; e

2.1.21.5.21.8 Data e hora do login e do logout (para cálculo de tempo da sessão)

2.1.21.5.22 Possibilidade de coletar, armazenar e proteger evidências para análise forense computacional, a fim de apoiar o Serpro na coleta de provas digitais.

2.1.21.6 Criptografia

2.1.21.6.1 A solução deverá permitir o uso da criptografia no armazenamento, na transmissão e na apresentação de documentos arquivísticos digitais ao implementar a política de sigilo.

2.1.21.6.2 A solução deverá limitar o acesso aos documentos cifrados somente àqueles usuários portadores da chave de decifração.

2.1.21.6.3 A solução deverá registrar os seguintes metadados sobre um documento cifrado:

2.1.21.6.3.1 indicação sobre se está cifrado ou não;

2.1.21.6.3.2 algoritmos usados na cifração;

2.1.21.6.3.3 identificação do remetente;

2.1.21.6.3.4 identificação do destinatário.

2.1.21.6.4 Somente usuários autorizados têm que ser capazes de realizar as operações a seguir:

2.1.21.6.4.1 incluir, remover ou alterar parâmetros dos algoritmos criptográficos instalados no sistema;

2.1.21.6.4.2 incluir, remover ou substituir chaves criptográficas de programas ou usuários do sistema;

2.1.21.6.4.3 cifrar e alterar a criptografia de documentos;

2.1.21.6.4.4 remover a criptografia de um documento.

2.1.21.6.4.5 A remoção da cifração pode ocorrer quando sua manutenção resultar na indisponibilidade do documento. Por exemplo, se a chave de cifração/decifração estiver embarcada em hardware inviolável cuja vida útil esteja prestes a se esgotar ou se o documento for desclassificado.

2.1.22 Segurança para dados em nuvem

2.1.22.1 Os dados, metadados, informações e conhecimentos produzidos ou custodiados pelo Serpro, transferidos para o provedor de serviço de nuvem, devem estar hospedados em território brasileiro, em conformidade com as disposições descritas na IN05/GSI, art. 18.

Os dados e informações do SERPRO sob custódia da CONTRATADA deverão ser tratadas como informações sigilosas, não podendo ser usadas pela CONTRATADA ou fornecidas a terceiros, sob nenhuma hipótese, sem autorização formal do SERPRO.

2.1.22.2 Os log's poderão ser exportados de forma programada, pela contratada, para armazenamento e acesso pelo SERPRO.

2.1.22.3 A responsabilidade do armazenamento é da contratada, para o período de 1 ano.

2.1.22.4 A solução deve comprovar que seus centros de dados implementam medidas de segurança impedindo acessos não autorizados, sejam eles por meio físicos ou virtuais, assegure a confidencialidade, privacidade e integridade dos dados.

2.1.22.5 A redundância implementada deve garantir a continuidade do funcionamento da solução no caso de ocorrência de falhas em equipamentos de rede, circuitos de comunicação, servidores físicos e ou virtuais e unidades de armazenamento.

9 Quando houver suspeita ou for detectado evidência de descumprimento das cláusulas contratuais, com impactos direto ou indireto aos produtos, sistemas e serviços do SERPRO ou de seus clientes, os fornecedores contratados são corresponsáveis por registrar o fato adverso imediatamente à gerência de relacionamento do Serpro mais próxima, ou responsável pelo acompanhamento dos serviços contratados.

2.1.22.7 Para que não haja prejuízos quanto ao entendimento, o registro da comunicação deve conter: a descrição do fato em si (o que ocorreu); a indicação de data e hora (quando ocorreu); a indicação do local da ocorrência percebida (onde ocorreu), seja local físico (endereço, andar, setor etc.), ou local sistêmico (sistema, tela, funcionalidade, etc). Caso seja possível, também indicar os responsáveis (quem provocou).

2.1.22.8 Realizar notificação em casos de violações de segurança ou outros incidentes que possam prejudicar confidencialidade, disponibilidade e integridade dos dados.

2.1.22.9 A omissão desses registros por parte do terceirizado ou fornecedor, poderão ser objeto de apuração pela área competente do Serpro, com aplicação de penalidades administrativas e contratuais.

2.1.22.10 A solução deve permitir que seja aplicada segregação lógica apropriada dos dados das aplicações virtualizadas, dos sistemas operacionais, do armazenamento e da rede a fim de estabelecer a separação de recursos utilizados, assim como garantir a separação de todos os

recursos utilizados pelo Provedor de Serviço de Nuvem daqueles recursos utilizados pela administração interna do Serpro.

2.1.22.11 O contrato a ser firmado com um provedor para a prestação do serviço de computação em nuvem deve conter dispositivos que tratem dos requisitos de segurança estabelecidos nesta norma, bem como no mínimo, os seguintes itens:

2.1.22.12 Termo de confidencialidade que impeça o provedor de serviço de nuvem de usar, transferir e liberar dados, sistemas, processos e informações do Serpro para empresas nacionais, transacionais, estrangeiras, países e governos estrangeiros; (IN05 art. 19, I)

2.1.22.13 Garantia da exclusividade de direitos, por parte do Serpro, sobre todas as informações tratadas, incluídas eventuais cópias disponíveis, tais como backups de segurança; (IN05 art. 19, II)

2.1.22.14 Proibição do uso de informações pelo provedor de serviço de nuvem para propaganda, otimização de mecanismos de inteligência artificial ou qualquer uso secundário não-autorizado;

2.1.22.15 Conformidade da política de segurança da informação do provedor de serviço de nuvem com a legislação brasileira; (IN05 art. 19, IV)

2.1.22.16 Devolução integral dos dados, informações e sistemas sob custódia do provedor de serviço de nuvem ao Serpro no término do contrato; (IN05 art. 19, V)

2.1.22.17 Eliminação, por parte do provedor de serviço de nuvem, ao término do contrato, de qualquer dado, informação ou sistema do Serpro, sob sua custódia, observada a legislação que trata da obrigatoriedade de retenção de dados; e (IN05 art. 19, VI)

2.1.22.18 Nível de segregação dos dados e a separação lógica de recursos e serviços que garanta a proteção necessária em ambientes de computação em nuvem, assim como que os recursos utilizados pelo provedor de serviço em nuvem possuam o isolamento necessário de forma não comprometer os recursos internos do Serpro. (IN05 art.15 - I)

2.1.22.19 Registro de todos os acessos, incidentes e eventos cibernéticos, incluídas as informações sobre sessões e transações do ambiente de nuvem armazenados por um período mínimo de um ano, pelo provedor de serviço. (IN05 art. 13, IV, a-b)

2.1.22.20 Os registros poderão ser exportados de forma programada, pela contratada, para armazenamento e acesso pelo SERPRO.

2.1.22.21 A responsabilidade do armazenamento é da contratada.

2.1.22.22 Possuir processos de gestão de continuidade de negócios e plano de recuperação de desastres que estabeleça procedimentos de recuperação e de restauração de plataforma, infraestrutura e aplicações em conformidade com as melhores práticas e legislações correlatas.

2.1.22.23 Assegurar que o provedor de serviço documente e comunique seus recursos, papéis e responsabilidades de segurança da informação para o uso de seus serviços em nuvem; (IN05 art. 16, II)

2.1.22.24 Garantia sobre a implementação de controles de segurança da informação pelo provedor de serviço em nuvem;(27002:2022)

2.1.22.25 Possua regiões no Brasil e possibilidade de garantir que os dados não sejam transferidos para o exterior, em situações que a legislação determine.

2.1.22.26 Assegurar que os requisitos de segurança da informação sejam atendidos em caso de subcontratação pelo provedor de serviços de nuvem; (27002:2022)

2.1.22.27 Permitir a portabilidade de dados e aplicativos e que as informações do Serpro estejam disponíveis para transferência de localização, em prazo adequado e sem custo adicional, de modo a garantir a continuidade do negócio e possibilitar a transição contratual; e (Diretrizes contratação SGD)

2.1.22.28 Assegurar que as informações sob custódia do fornecedor serão tratadas como informações sigilosas, não podendo ser usadas ou fornecidas por este a terceiros, sob nenhuma hipótese, sem autorização formal do Serpro. (Diretrizes contratação SGD)

2.1.22.29 Possuir um programa de gestão de vulnerabilidade para detectar e mitigar qualquer nova ameaça ao serviço de computação em nuvem.

2.1.22.30 Possuir um processo de gestão de mudanças em conformidade com as melhores práticas de mercado.

2.1.22.31 Garantia do suporte e disponibilidade adequados de serviços, dentro de um prazo acordado, quando da estratégia de saída do Serpro do serviço em nuvem. (ISO 27002)

2.1.23 Privacidade para dados em Nuvem

2.1.23.1 Nas contratações de serviços em nuvem (IaaS, PaaS e SaaS) devem ser observados, no mínimo, os requisitos de privacidade e segurança da informação, além daqueles constantes nos “templates” de artefatos da contratação disponibilizados pela SGD em parceria com a AGU:

2.1.23.2 Cada provedor de nuvem deve possuir, no mínimo, dois data centers em território brasileiro, capaz de ofertar serviços padronizados e altamente automatizados, nos quais os recursos de infraestrutura (por exemplo, computação, rede e armazenamento) são complementados por serviços de plataforma integrados, e deve cumprir os requisitos de segurança da informação estabelecidos nos artigos 20 e 25 da Instrução Normativa GSI/PR nº 5, de 30 de agosto de 2021;

2.1.23.3 Devem ser definidos os países e as regiões em cada país onde os serviços poderão ser prestados e os dados poderão ser armazenados, processados e gerenciados, e o provedor deve assegurar que dados sujeitos a limites geográficos não sejam migrados para além de fronteiras definidas em contrato;

2.1.23.4 A utilização de termo de confidencialidade, que deverá conter cláusula que impeça o integrador ou provedor de serviço de nuvem de usar, transferir, e liberar dados, sistemas, processos e informações do órgão ou da entidade para terceiros, como empresas nacionais, transnacionais, estrangeiras, países e governos estrangeiros, além de incluir a proibição do uso de informações do órgão ou da entidade para propaganda, otimização de mecanismos de inteligência artificial ou qualquer uso secundário não autorizado;

2.1.23.5 O Serpro deve ter um contrato por escrito com qualquer operador de dado pessoal que ela utilize, e deve assegurar que os seus contratos com os operadores de dados pessoais contemplem a implementação de controles apropriados, conforme descrito no Anexo B (ABNT NBR ISO/IEC 27701:2019);