MINISTÉRIO DA EDUCAÇÃO
INSTITUTO FEDERAL FARROUPILHA
COMISSÃO DE IMPLANTAÇÃO DE GESTÃO DOCUMENTAL

RELATÓRIO DE ANÁLISE DO SISTEMA INTEGRADO DE PATRIMÔNIO, ADMINISTRAÇÃO E CONTRATOS (SIPAC) – MÓDULO PROTOCOLO

Equipe:

Eduardo Feitoza – Arquivista

Magnus Oliveira – Téc. Em Arquivo

Marciéle Lucher - Arquivista

São Vicente do Sul, RS

2014

1 INTRODUÇÃO

Este relatório tem o objetivo de analisar o Módulo de Protocolo do Sistema Integrado de Patrimônio, Administração e Contratos – SIPAC e o Sistema de Gestão Eletrônica de Documentos - SIGED dos Sistemas Institucionais Integrados de Gestão – SIG. Essa solução foi desenvolvida pela Diretoria de Sistemas da Universidade Federal do Rio Grande do Norte e será implantada no Instituto Federal Farroupilha pela empresa AVMB através da execução do Contrato n° 35/2013.

O Módulo de Protocolo pretende gerenciar documentos e processos, registrar informações gerais, gerar número de protocolo, associar arquivos digitalizados, realizar despachos eletrônicos, classificar documentos, registrar a localização física, registrar ocorrências e diligências, realizar juntadas e desapensações, realizar arquivamento, gerenciar fluxos padrão e enviar memorandos.

O SIGED, por sua vez, pretende permitir a centralização do controle de documentos, upload da versão digital de documentos físicos, possibilidade de realizar buscas nos conteúdos dos documentos, a organização dos documentos por tipos e pastas, cadastro de descritores de documentos e versionamento de documentos cadastrados.

Esta análise terá como parâmetros os seguintes dispositivos normativos:

Lei n° 8.159/1991, que dispõe sobre a política nacional de arquivos públicos e privados;

Lei n° 9.784/1999, que regula o processo administrativo no âmbito da Administração Pública Federal;

Decreto n° 4.073/2002, que regulamenta a Lei n° 8.159/1991;

Portaria Normativa n° 05/SLTI/MPOG/2002, que dispõe sobre os procedimentos gerais para utilização dos serviços de protocolo, no âmbito da Administração Pública Federal, para os órgãos e entidades do Sistema de Serviços Gerais;

Decreto n° 4.915/2003, que dispõe sobre o Sistema de Gestão de Documentos de Arquivo – SIGA, da Administração Pública Federal;

Portaria n° 03/SLTI/MPOG/2003, que orienta aos órgãos e entidades integrantes do Sistema de Serviços Gerais quanto aos procedimentos relativos as atividades de Comunicações Administrativas, para utilização do número único de processos e documentos;

Lei n° 12.527/2011, que regula o acesso a informação previsto no inciso XXXIII do art. 5°, no inciso II do § 3° do art. 37 e no § 2° do art. 216 da Constituição Federal;

Portaria n° 92/MJ/2011, que aprova o Código de Classificação e a Tabela de Temporalidade e Destinação de Documentos de Arquivo relativos as atividades-fim das Instituições Federais de Ensino Superior;

Lei n° 12.682/2012, que dispõe sobre a elaboração e o arquivamento de

documentos em meios eletromagnéticos;

Decreto n° 7.724/2012, que regulamenta a Lei n° 12.527/2011;

Decreto n° 7.845/2012, que regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo;

Resoluções do Conselho Nacional de Arquivos – CONARQ:

1. Resolução n° 07/1997 que dispõe sobre os procedimentos para a eliminação de documentos no âmbito dos órgãos e entidades integrantes do Poder Público;

2. Resolução n° 14/2001, que aprova a versão revisada e ampliada da Resolução nº 4, de 28 de março de 1996, que dispõe sobre o Código de Classificação de Documentos de Arquivo para a Administração Pública: Atividades-Meio, a ser adotado como modelo para os arquivos correntes dos órgãos e entidades integrantes do Sistema Nacional de Arquivos (SINAR), e os prazos de guarda e a destinação de documentos estabelecidos na Tabela Básica de Temporalidade e Destinação de Documentos de Arquivo Relativos as Atividades-Meio da Administração Pública;

3. Resolução n° 20/2004, que dispõe sobre a inserção dos documentos digitais em programas de gestão arquivística de documentos dos órgãos e entidades integrantes do Sistema Nacional de Arquivos;

4. Resolução n° 25/2007, que dispõe sobre a adoção do Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos - e-ARQ Brasil pelos órgãos e entidades integrantes do Sistema Nacional de Arquivos – SINAR;

5. Resolução n° 31/2010, que dispõe a adoção das Recomendações para Digitalização de Documentos Arquivísticos Permanentes;

6. Resolução n° 32/2010, que dispõe sobre a inserção dos Metadados na Parte II do Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos – e-ARQ Brasil;

7. Resolução n° 35/2012, que atualiza o Código de Classificação de Documentos de Arquivo para a Administração Pública: Atividades-Meio e a Tabela Básica de Temporalidade e Destinação de Documentos de Arquivo Relativos às Atividades-Meio da Administração Pública, aprovados pela Resolução nº 14, de 24 de outubro de 2001, do CONARQ, publicada no DOU, de 8 de fevereiro de 2002;

8. Resolução n° 36/2012, que dispõe sobre a adoção das Diretrizes para a Gestão arquivística do Correio Eletrônico Corporativo pelos órgãos e entidades integrantes do Sistema Nacional de Arquivos – SINAR;

9. Resolução n° 37/2012, que aprova as Diretrizes para a Presunção de Autenticidade de Documentos Arquivísticos Digitais;

10. Resolução n° 38/2013, que dispõe sobre a adoção das "Diretrizes do Produtor - A Elaboração e a Manutenção de Materiais Digitais: Diretrizes Para Indivíduos" e "Diretrizes do Preservador - A Preservação de Documentos Arquivísticos digitais: Diretrizes para Organizações";

11. Resolução n° 39/2014, que estabelece diretrizes para a implementação de repositórios digitais confiáveis para a transferência e recolhimento de documentos

arquivísticos digitais para instituições arquivísticas dos órgãos e entidades integrantes do Sistema Nacional de Arquivos – SINAR.

1.1 e-ARQ Brasil

Destacamos, em especial, o Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos – e-ARQ Brasil que irá nortear a maior parte das análises. O e-ARQ Brasil é uma especificação de requisitos a serem cumpridos pela organização produtora/recebedora de documentos, pelo sistema de gestão arquivística e pelos próprios documentos, a fim de garantir sua confiabilidade e autenticidade, assim como sua acessibilidade. Além disso, o e-ARQ Brasil pode ser usado para orientar a identificação de documentos arquivísticos digitais. Ele ainda estabelece requisitos mínimos para um Sistema Informatizado de Gestão Arquivística de Documentos independentemente da plataforma tecnológica em que for desenvolvido e/ou implantado e especifica todas as atividades e operações técnicas da gestão arquivística de documentos, desde a produção, tramitação, utilização e arquivamento até a sua destinação final.

O e-ARQ Brasil é dividido em duas partes: Requisitos e Metadados. Os requisitos foram classificados em obrigatórios, altamente desejáveis e facultativos, de acordo com o grau maior ou menor de exigência. Por sua vez, os metadados foram classificados como obrigatório, obrigatório se possível e facultativo, também de acordo com o grau de exigência. Neste documento trataremos apenas dos requisitos e metadados obrigatórios e altamente desejáveis. Estes constarão na parte 3 deste relatório.

Os aspectos de funcionalidade tratados pelo e-ARQ Brasil são descritos nas seções abaixo.

1.2 Organização dos Documentos Arquivísticos: Plano de Classificação

A organização dos documentos arquivísticos é feita com base num plano de classificação. Por meio dele se estabelece a hierarquia e a relação orgânica dos documentos devidamente demonstradas na forma pela qual tais documentos são organizados em unidades de arquivamento.

Os documentos produzidos ou recebidos no decorrer das atividades de um órgão são acumulados em unidades de arquivamento e organizados d forma hierárquica em classes de acordo com um plano de classificação.

As atividades de gestão de documentos, como controle da temporalidade e destinação dos documentos, são feitas com base nas unidades de arquivamento. Desta forma, no momento do arquivamento os documentos devem ser inseridos em uma unidade de arquivamento, que está subordinada hierarquicamente ao plano de classificação.

1.2.1 Configuração e administração do plano de classificação

Referem-se as funcionalidades do sistema para apoiar a configuração do plano de classificação, ou seja, como desenhar um plano de classificação em um sistema.

1.2.2 Classificação e metadados dos documentos

Referem-se a formação e classificação dos documentos e a associação de metadados.

1.2.3 Gerenciamento dos documentos

Referem-se ao gerenciamento dos documentos arquivísticos no que diz respeito a controles de abertura e encerramento de dossiês\processos e seus respectivos volumes e inclusão de novos documentos nesses dossiês\processos e respectivos volumes ou em pastas virtuais.

1.2.4 Requisitos adicionais para o gerenciamento de documentos

Inclui requisitos específicos para a gestão de processos.

1.2.5 Volumes: abertura, encerramento e metadados

Em alguns casos os dossiês/processos são compartimentados em volumes ou partes, de acordo com normas e instruções estabelecidas. Essa divisão não está baseada no conteúdo intelectual dos dossiês/processos, mas em outros critérios, como a dimensão, o número de documentos, períodos de tempo etc. Essa prática tem como objetivo facilitar o gerenciamento físico dos dossiês/processos.

1.2.6 Gerenciamento de documentos arquivísticos convencionais, digitais e híbridos

O arquivo de uma organização pode conter documentos ou dossiês/processos digitais e convencionais. Um sistema deve registrar os documentos ou dossiês/processos convencionais, que devem ser classificados com base no mesmo plano de classificação usado para os digitais e deve ainda possibilitar a gestão de documentos ou dossiês/processos híbridos. Os documentos ou dossiês/processos híbridos são formados por uma parte digital e uma parte convencional.

1.3 Tramitação e Fluxo de Trabalho

Os requisitos desta parte tratam apenas dos casos em que o sistema inclui recursos de automação de fluxo de trabalho (workflow). Abrangem funções para controle do fluxo de trabalho e atribuição de metadados para registro da tramitação dos documentos incluindo a forma do documento (minuta, original ou cópia).

Os recursos do sistema para controle do fluxo de trabalho podem compreender:

Tramitação de um documento antes do seu registro/captura;

Tramitação posterior ao seu registro/captura.

As tecnologias de fluxo de trabalho transferem objetos digitais entre participantes sob o controle automatizado de um programa. São geralmente usadas para:

Gestão de processos ou de tarefas, tais como registro e destinação de documentos e dossiês/processos;

Verificação e aprovação de documentos ou dossiês/processos antes do registro;

Encaminhamento de documentos ou dossiês/processos de forma controlada, de um usuário para outro, com a identificação das ações a serem realizadas tais como:

1. “verificar documento”, “aprovar nova versão”;

Comunicação aos usuários sobre a disponibilidade de um documento arquivístico;

Distribuição de documentos ou dossiês/processos;

Publicação de documentos ou dossiês/processos na web.

Um participante de um fluxo de trabalho pode ser um indivíduo específico ou um grupo de trabalho. Um participante é o responsável pela realização de uma tarefa estabelecida ao longo de um fluxo de trabalho predefinido. No caso do participante ser um indivíduo, a tarefa é direcionada para um usuário com uma identificação específica. No caso do participante ser um grupo de trabalho, a tarefa é direcionada para o grupo (formado por vários usuários, cada um com sua identificação no sistema). A tarefa tem que ser distribuída entre os usuários do grupo e após, ser cumprida por um membro do grupo, o documento segue o fluxo previsto.

1.3.1 Controle de Versões e Forma de Documento

O sistema tem que ser capaz de, por meio do seu recurso de fluxo de trabalho, estabelecer a forma do documento, isto é, se trata de minuta, original ou cópia. No caso dos documentos digitais, esse status é estabelecido de acordo com a rota do documento no sistema. Assim, por exemplo:

Um documento criado no espaço individual ou do grupo mas não transmitido, é uma minuta;

Um documento transmitido do espaço individual ou do grupo para o espaço gerencial, onde não poderá mais ser alterado, e daí para fora da instituição, será sempre recebido como um original e armazenado no espaço de origem (individual, do grupo ou gerencial) como uma última minuta. Isso porque a transmissão acrescenta metadados ao documento (como data e hora da transmissão) que o tornam mais completo;

Um documento que é enviado do espaço individual para o do grupo para fins de comentários é uma minuta, que deverá ter seu número de versões devidamente controlado.

Quando um usuário autorizado recupera um documento do espaço gerencial e o armazena em seu espaço, ele cria uma cópia. O mesmo acontece quando o usuário reencaminha um documento para um outro usuário.

1.4 Captura

A captura consiste em declarar um documento como sendo um documento arquivístico ao incorporá-lo no sistema por meio das seguintes ações: registro, classificação, indexação, atribuição de metadados e arquivamento.

Dentre essas ações, o arquivamento envolve procedimentos diferentes no que diz respeito aos documentos digitais e convencionais. Enquanto os primeiros são arquivados dentro do sistema, os convencionais seguem a forma tradicional, isto é, pastas ou equivalentes, sendo referenciados no sistema. No caso de um documento convencional ser acompanhado de anexos digitais armazenados em mídia móvel (disquete, discos ópticos ou óptico-magnéticos, fitas magnéticas etc), esses anexos poderão tanto ser mantidos no sistema como nas referidas mídias.

A captura de documentos digitais no sistema pode ser feita de diversas formas:

Captura individual de documento produzido em arquivo digital fora do sistema, em aplicativo e formato específicos (.doc, .pdf, .rtf): o registro inicial é feito pelo usuário ao capturar o documento para o sistema;

Captura individual de documento produzido em workflow ou em outro sistema de forma integrada ao sistema: o registro e a anexação ao sistema de gestão podem ser automáticos, complementados pelo usuário do sistema;

Captura em lote: inclusão no sistema de um grupo de documentos do mesmo tipo oriundos de outro sistema ou de um GED. Ex.: faturas diárias, dossiês, processos.

1.4.1 Captura de mensagens de correio eletrônico

O correio eletrônico é um sistema usado para criar, transmitir e receber mensagens eletrônicas e outros documentos digitais por meio de redes de computadores. As características do correio eletrônico podem dificultar o seu gerenciamento. Assim, o sistema tem que permitir controles de gestão para:

Capturar todas as mensagens e anexos emitidos e recebidos;

Dotar os usuários da capacidade de capturar apenas mensagens e anexos previamente selecionados.

Obs.: este último procedimento requer que os usuários avaliem a pertinência e a importância dos itens, bem como o risco de não os capturar.

1.4.2 Captura de documentos convencionais ou híbridos

O programa de gestão de documentos de um órgão é único para documentos convencionais, digitais e híbridos. Assim, o sistema terá que capturar todos esses diferentes tipos de documentos.

A captura do documento convencional será realizada pelo sistema por meio das atividades de registro, classificação e indexação. O arquivamento será feito da forma apropriada ao suporte, formato e tipo do documento.

1.4.3 Formato de arquivo e estrutura dos documentos a serem capturados

Os órgãos e entidades precisarão capturar uma gama diversificada de documentos com formatos de arquivo e estruturas diferentes. Os requisitos técnicos para a captura variarão de acordo com a complexidade dos documentos. Em alguns ambientes não é possível identificar antecipadamente todas os formatos de arquivo e estruturas possíveis dos documentos, já que alguns são recebidos de fontes externas.

1.4.4 Documentos automodificáveis

Alguns documentos aparentam ter seus conteúdos alterados sem intervenção do usuário.

Um exemplo é um modelo para elaboração de correspondência cuja data é colocada automaticamente pelo sistema e armazenada como um “campo” ou “código”. Nesse caso, cada vez que o documento é exibido, a data apresentada é atualizada. Entretanto o documento lógico não se modifica, é apenas a sua exibição (documento conceitual) que sofre alterações conforme o software utilizado para visualizá-lo.

Outros documentos podem conter um código que os modifique realmente. É o caso de uma folha de cálculo com um “macro” sofisticado que a altera (por meio de software de aplicações utilizado para visualização) e, em seguida, guarda-a automaticamente.

Os documentos automodificáveis devem ser evitados. Caso isso não seja possível, os documentos devem ser armazenados em formatos que desativem o código automodificador ou visualizados por meio de software que não desencadeie a alteração.

Por exemplo: uma planilha de cálculo que contenha “macros” deve ser convertida para um formato estável, como o PDF, antes de ser capturada para o sistema.

Quando não for possível converter os documentos automodificáveis para formato estável ou visualizá-los por meio de software que não desencadeie a alteração, a captura desses documentos no sistema deve ser acompanhada do registro das informações relativas às funções automodificadoras nos metadados.

1.4.5 Estrutura dos procedimentos de gestão

A gestão arquivística de documentos digitais prevê o estabelecimento de três domínios dentro do ambiente eletrônico, a saber: espaço individual, espaço do grupo e espaço geral. O espaço individual corresponde ao espaço designado a cada funcionário. O espaço do grupo corresponde ao espaço designado a cada grupo de trabalho, equipe, comitê etc.

O espaço geral corresponde ao serviço de protocolo e arquivos do órgão. Sua principal característica é que uma vez ali, o documento não poderá mais ser alterado.

As regras estabelecidas pelo sistema de gestão arquivística de documentos definem em que espaços os documentos podem ser:

Produzidos, recebidos, alterados, capturados (registrados, classificados, indexados e arquivados ou encaminhados), armazenados e eliminados;

O espaço no qual os metadados serão incluídos;

Os direitos de acesso em cada espaço e a maneira pela qual os documentos

tramitarão dentro e fora do órgão ou entidade.

Uma vez capturados no espaço geral, os documentos e seus metadados têm que ser mantidos em versão definitiva e protegidos contra alterações deliberadas ou acidentais. O conteúdo, o contexto e a forma dos documentos capturados devem ser mantidos ao longo de todo seu ciclo de vida, a fim de preservar a sua autenticidade.

1.5 Avaliação e Destinação

Os requisitos desta seção referem-se aos procedimentos de avaliação e destinação dos documentos gerenciados pelo sistema.

No contexto do sistema, a avaliação dos documentos refere-se à aplicação da tabela de temporalidade e destinação de documentos. Essa tabela define o prazo pelo qual os documentos têm que ser mantidos no sistema e a destinação dos mesmos após esse prazo, ou seja, recolhimento ou eliminação.

Para cumprir a destinação prevista na tabela de temporalidade e destinação, um documento deve ser exportado do sistema. Além disso, o sistema pode exportar documentos para outro sistema por outras razões.

Esta seção estabelece requisitos para a configuração da tabela de temporalidade e destinação de documentos no sistema, para a aplicação da tabela de temporalidade e destinação no sistema e para exportação e eliminação de documentos de um sistema.

1.5.1 Configuração da tabela de temporalidade e destinação de documentos

Estes requisitos referem-se à criação e manutenção de tabelas de temporalidade no sistema.

1.5.2 Aplicação da tabela de temporalidade e destinação de documentos

Estes requisitos referem-se à aplicação da tabela de temporalidade e destinação de documentos, ou seja, aos procedimentos de controle e verificação dos prazos e da destinação prevista, antes de se proceder às ações de destinação propriamente ditas.

1.5.3 Exportação de documentos

Um sistema deve ter capacidade de exportar documentos para apoiar as ações de transferência e recolhimento de documentos, ou ainda para realizar uma migração ou enviar uma cópia para outro local ou sistema.

Em alguns casos os documentos serão eliminados do sistema após a exportação; em outros, serão mantidos. Em todos os casos, é absolutamente necessário que as ações sejam executadas de maneira controlada, fazendo-se registro nos metadados e na trilha de auditoria e verificando-se os documentos relacionados.

1.5.4 Eliminação

A eliminação de documentos arquivísticos deve ser realizada de acordo com o previsto na tabela de temporalidade e destinação de documentos, após a avaliação dos documentos e de acordo com a legislação vigente.

Da mesma forma que a exportação, as ações para eliminação de documentos arquivísticos no sistema têm de ser executadas de forma controlada, fazendo-se registro nos metadados e trilha de auditoria e verificando-se os documentos relacionados.

1.5.5 Avaliação e destinação de documentos arquivísticos convencionais e híbridos

Os documentos arquivísticos convencionais e os híbridos gerenciados pelo sistema devem ter os procedimentos de avaliação e destinação controlados pelo sistema, da mesma forma que os documentos digitais.

1.6 Pesquisa, Localização e Apresentação dos Documentos

O sistema precisa prover funcionalidades para pesquisa, localização e apresentação dos documentos arquivísticos com o objetivo de permitir o acesso a eles.

Todas essas funcionalidades têm de ser submetidas aos controles de acesso descritos na seção de segurança.

1.6.1 Pesquisa e localização

A pesquisa é o processo de identificação de documentos arquivísticos por meio de parâmetros definidos pelo usuário com o objetivo de confirmar, localizar e recuperar esses documentos, bem como seus respectivos metadados.

1.6.2 Apresentação: visualização, impressão, emissão de som

O sistema pode conter documentos arquivísticos com formatos e estruturas os mais

diversos e deve ter capacidade para apresentá-los ao usuário sem adulterá-los, seja exibindo na tela de computador, imprimindo ou emitindo som.

O sistema deverá informar os programas (software) adicionais necessários e a configuração adequada, como por exemplo: plug-in, configuração de navegador.

1.7 Segurança

Esta seção contém um conjunto de requisitos para serviços de segurança: cópias de segurança, controle de acesso (tanto baseado em perfis de usuário quanto grupos de usuários), classes de sigilo, trilhas de auditoria de sistemas, criptografia para sigilo, assinatura digital e marcas d'água digitais.

Os requisitos de identificação, autenticação de usuário e trilhas de auditoria devem integrar qualquer sistema. Políticas de segurança específicas poderão definir o rigor, maior ou menor, do tratamento dos demais requisitos.

No que diz respeito ao controle de acesso, esta especificação contempla três tipos de requisitos:

de controle de acesso baseado em perfis de usuário.

de controle de acesso por grupos.

de classificação quanto ao grau de sigilo.

Os três tipos de controle de acesso podem ser combinados e os requisitos de administração de controle de acesso devem ser adaptados a cada um dos tipos acima ou a combinação deles, de acordo com a legislação vigente.

Quanto ao uso da tecnologia de criptografia, tanto para sigilo quanto para autenticação, o rigor dos requisitos está sujeito à legislação vigente e à política de segurança específica.

Muitas vezes, a criptografia é usada como mecanismo de apoio ao controle de acesso para reforçar o sigilo de informações. Os requisitos de assinatura digital e certificação digital são necessários para aquelas organizações em que documentos são assinados digitalmente ou verificações eletrônicas de autenticidade são necessárias.

Esses requisitos não esgotam o tema segurança da informação, pois a segurança integral é sistêmica e abrange não somente a tecnologia, mas também pessoas, processos e legislação.

1.7.1 Cópias de segurança

As cópias de segurança têm por objetivo prevenir a perda de informações, e garantir a disponibilidade do sistema. Os procedimentos de backup devem ser feitos regularmente e, pelo menos uma cópia deve ser armazenada preferencialmente off-site.

Podem-se distinguir vários tipos de informação necessários ao funcionamento de um sistema. Essas informações compreendem os documentos digitais, metadados e informações de controle associadas às camadas de software relacionadas ao sistema (Sistema Operacional, Gerenciador de bancos de dados, software aplicativo). Todas essas informações devem ser incluídas nos procedimentos de cópias de segurança.

1.7.2 Controle de acesso

Esta seção trata dos requisitos de identificação e autenticação de usuários, controle de acesso baseado em grupos de usuários e em perfis de usuários, bem como dos requisitos comuns a qualquer tipo de controle de acesso.

Identificação e Autenticação de Usuários

Os requisitos abaixo tratam o mapeamento da identidade do usuário legítimo e as permissões concedidas a ele, imediatamente após sua autenticação.

Usuários acessam dados, metadados e funções via a interface do programa. A associação entre Identidade do Usuário e as autorizações de acesso é feita durante a fase de identificação e autenticação do usuário via a interface do programa, com base nas credenciais de autenticação.

Aspectos Gerais de Controle de Acesso

Os requisitos desta seção são aplicáveis a qualquer organização para a condução das suas funções e atividades, independente do modelo de controle de acesso adotado, de acordo com a política de segurança.

Controle de Acesso por Grupos de Usuários

Grupos são conjuntos de usuários (possivelmente com perfis diferentes) reunidos para a realização de alguma atividade em comum, por tempo determinado.

Estes requisitos só são aplicáveis às organizações onde há controle de acesso por

grupos de usuários.

Controle de Acesso por Perfis de Usuários

Perfis são funções ou cargos com responsabilidades e autoridades bem definidas.

Operações são tarefas executadas sobre os documentos, os dossiês/processos e as classes. Atribuições de usuários são as associações entre usuários e papéis. Um usuário pode estar associado a um ou mais perfis e vice-versa. Permissões são garantias aprovadas para realização de operações sobre documentos arquivísticos.

Estes requisitos só são aplicáveis aos órgãos onde há controle de acesso por perfis de usuários.

1.7.3 Classificação da informação quanto ao grau de sigilo e restrição de acesso à informação sensível

Os requisitos descritos nesta seção referem-se ao acesso aos documentos arquivísticos com base na classificação do grau de sigilo bem como restrição de acesso à informação sensível. Informação sensível pode estar relacionada à honra e à privacidade de pessoas ou a questões estratégicas e de segredo corporativo. Órgãos da administração pública são subordinados aos graus de sigilo definidos na legislação vigente.

Estes requisitos são aplicáveis às organizações em que o teor dos documentos produzidos e recebidos exige sigilo.

1.7.4 Trilhas de Auditoria

A trilha de auditoria consiste num histórico de todas as intervenções, ou tentativas de intervenções, feitas no documento e no próprio sistema. Nesse sentido, é também um metadado sobre os documentos arquivísticos digitais e informa sobre a sua autenticidade.

1.7.5 Assinaturas Digitais

Assinatura digital é uma seqüência de bits que usa algoritmos específicos, chaves criptográficas e certificados digitais para autenticar a identidade do assinante e confirmar a integridade de um documento. Certificação digital é uma técnica, baseada em uma infra-estrutura de chaves públicas, de garantia da validade de assinaturas digitais.

O uso de assinaturas digitais e de certificação digital na administração pública foi padronizado e normalizado com a criação da Infra-estrutura de Chaves Públicas Brasileira - ICP-Brasil.

Os requisitos só são aplicáveis quando há necessidade de utilizar assinaturas digitais para assegurar autenticação, imputabilidade e irretratabilidade (ou irrefutabilidade).

1.7.6 Criptografia

Criptografia é um método de codificação de objetos digitais segundo um código secreto (chave), de modo que estes não possam ser apresentados por uma aplicação de forma legível ou inteligível e somente usuários autorizados podem restabelecer sua forma original.

Esta seção trata dos serviços de segurança apoiados em criptografia. Estes requisitos só são aplicáveis às organizações onde há elevada necessidade de garantia de sigilo.

É importante salientar que, no uso de criptografia em documentos que apresentam longa temporalidade, devem ser tomadas medidas administrativas para garantir a manutenção do sigilo e do acesso a esses documentos. Esses documentos não devem ser armazenados criptografados. Alguns fatores que comprometem a criptografia no longo prazo são: comprometimento ou obsolescência da chave, indisponibilidade do portador da chave e evoluções tecnológicas.

É importante lembrar que o Conselho Internacional de Arquivos define longo prazo para documentos digitais como um período a partir de 5 anos contado a partir da data de produção.

1.7.7 Marcas d'água Digitais

Marcas d’água servem para marcar uma imagem digital com informação sobre a sua proveniência e características e são utilizadas para proteger propriedade intelectual. As marcas d’água sobrepõem, no mapa de bits de uma imagem, um desenho complexo, visível ou invisível, o qual só pode ser suprimido mediante a utilização de um algoritmo ou de uma chave protegida. Tecnologias semelhantes podem ser aplicadas a sons e a imagens em movimento digitalizadas.

O sistema pode manter, recuperar e assimilar novas tecnologias de marcas d'água. Estes requisitos só são aplicáveis às organizações onde são usadas marcas d'água digitais.

1.7.8 Acompanhamento de Transferência

Durante o seu ciclo de vida, os documentos arquivísticos digitais e seus respectivos metadados podem ser transferidos de uma mídia de suporte, ou de um local, para outro, à medida que o seu uso decresce e/ou se modifica. Essa transferência pode ser interna,

implicando, por exemplo, num deslocamento de armazenamento on-line para armazenamento off-line, como também pode ser externa, implicando num deslocamento para outra instituição. É necessário um recurso de acompanhamento, a fim de se registrar a mudança de local, tanto para facilitar o acesso como para cumprir requisitos regulamentares.

1.7.9 Autoproteção

Num ambiente digital, a autoproteção consiste na capacidade do sistema de computação de verificar a integridade de programas e de dados de controle como uma medida de proteção inicial. As técnicas de autoproteção aumentam a confiança no funcionamento correto dos programas de computador.

Esta seção trata dos requisitos relativos à capacidade do sistema de se autoproteger contra quaisquer erros, falhas ou ataques ao próprio sistema.

Além dos requisitos de autoproteção, o sistema deverá interagir com outros sistemas de proteção, tais como: antivírus, firewall, anti-spyware etc.

1.7.10 Alterar, Apagar e Truncar Documentos Arquivísticos Digitais

Os documentos arquivísticos completos não podem, em regra, ser alterados e eliminados, exceto no término do seu ciclo de vida no sistema. No entanto, os Administradores podem precisar apagar documentos arquivísticos para corrigir erros de usuário (p. ex., declarar documentos de arquivo no dossiê/processo errado) ou para cumprir requisitos jurídicos no âmbito de legislação sobre proteção de dados. A ação de eliminar pode ter um dos significados seguintes:

Eliminação definitiva;

Retenção, acompanhada de uma anotação nos metadados do documento arquivístico, informando que o mesmo não está mais sob o controle da gestão de documentos arquivísticos.

A capacidade de apagar documentos tem que ser rigorosamente controlada para proteger a integridade dos documentos arquivísticos. Todas as informações referentes a essa ação têm que ser registradas na trilha de auditoria, e elementos indicativos da existência dos documentos arquivísticos apagados têm que permanecer nos dossiês afetados.

Às vezes, os administradores têm necessidade de publicar, ou de disponibilizar documentos arquivísticos que contêm informações sigilosas (seja em conseqüência de legislação sobre proteção de dados, seja por questões de segurança, ou de segredo comercial, etc). Por esse motivo, aos administradores têm que ser dado o poder de retirar a informação sensível, sem afetar o documento arquivístico correspondente. Esse processo é chamado de truncamento, ou de corte, e o sistema armazena o documento original e a cópia truncada,

chamada de “extrato”.

1.8 Armazenamento

A estrutura de armazenamento no sistema deve fazer parte de uma arquitetura tecnológica que permita a preservação e a recuperação de longo prazo dos documentos arquivísticos. Por isso, essa estrutura deve abrigar os documentos, seus metadados, os metadados do sistema (informações sobre segurança, direitos de acesso e usuários, entre outros), trilhas de auditoria e cópias de segurança. Do ponto de vista físico, tais informações residem em dispositivos de armazenamento eletrônicos, magnéticos e ópticos.

A arquitetura tecnológica para gerenciamento de arquivos digitais deve ser planejada e dimensionada de acordo com a missão e as competências da organização. Além disso, os equipamentos devem adequar-se às características on-line ou off-line das operações.

Operações on-line são aquelas que só podem ser realizadas através do sistema, ao passo que operações off-line podem ser realizadas em outros sistemas computacionais, desvinculadas do funcionamento do sistema.

O sistema deve utilizar dispositivos e técnicas de armazenamento que garantam a integridade dos documentos arquivísticos digitais.

Os itens seguintes enumeram requisitos de armazenamento organizados segundo os critérios de durabilidade, capacidade e viabilidade técnica.

1.8.1 Durabilidade

Os dispositivos de armazenamento do sistema e os documentos neles armazenados devem estar sujeitos a ações de preservação que garantam sua conservação de longo prazo.

1.8.2 Capacidade

O sistema deve garantir escalabilidade no armazenamento, permitindo expansão ilimitada dos dispositivos de armazenamento.

1.9 Preservação

Exatamente como no caso dos documentos convencionais, a preservação de documentos arquivísticos digitais não é um fim em si mesmo. Antes, possui um propósito que deve ser considerado na definição e na implementação das estratégias de preservação. A razão para preservação de um determinado documento pode ser seu valor probatório e/ou informativo.

Os documentos arquivísticos digitais gerenciados por um sistema devem ser preservados durante todo o período de tempo previsto para sua guarda, conforme determinado na tabela de temporalidade e destinação de documentos. Ressalte-se que as características desses documentos demandam atenção específica, principalmente naqueles que serão mantidos por mais de cinco anos, o que, nesse contexto, já é considerado de longo prazo.

A degradação do suporte e a obsolescência tecnológica são os principais fatores de comprometimento da preservação dos documentos digitais, uma vez que ameaçam sua autenticidade, integridade e acessibilidade.

A degradação do suporte é causada por fatores como falta de controle de temperatura, umidade, luminosidade, agentes químicos e biológicos agressores, bem como manipulação inadequada ou qualidade do suporte utilizado. Além de respeitar as condições ambientais especificadas pelo fabricante, é preciso realizar a substituição dos suportes antes do fim de sua vida útil, técnica conhecida como rejuvenescimento (refreshing).

No que diz respeito à obsolescência tecnológica, refere-se tanto a hardware quanto a software e formatos. É resultado das mudanças causadas pelo desenvolvimento de novas tecnologias e sua ascensão no mercado.

O hardware obsoleto pode ser, por exemplo, um determinado tipo de suporte (disco óptico, fita magnética, por exemplo), unidades de disco, unidades de fita magnética ou os próprios processadores e componentes utilizados na execução de programas (software).

Em alguns casos, os fabricantes procuram manter a compatibilidade com o antigo hardware, assegurando que software e formatos antigos continuem sendo utilizados. No entanto, essa situação não persiste indefinidamente, pois a compatibilidade geralmente é mantida somente em relação aos hardwares recém-substituídos.

As mudanças em software – incluindo sistemas operacionais, sistemas de gerenciamento de banco de dados e aplicativos como editores de texto, planilhas eletrônicas, editores de imagem, entre outros – costumam ser bastante freqüentes. O software podem ser simplesmente descontinuados, substituídos por outros equivalentes, supostamente melhores, ou ainda ter sua versão atualizada para correção de bugs ou acréscimo de novas funcionalidades. É importante notar que os fornecedores de software deixam de prestar suporte a versões mais antigas de seus produtos.

Os formatos também sofrem alterações, muitas vezes em função de mudanças

ocorridas nos programas (software) aos quais estão associados. Novos programas (software) podem ser compatíveis com os formatos antigos, mas também podem apresentar incorreções durante operações de leitura e escrita de dados nesses formatos. Algumas técnicas comumente utilizadas para evitar os riscos provenientes da obsolescência tecnológica são:

Preservação da tecnologia: evita a necessidade imediata de implementação de novos sistemas. Porém, as necessidades de manutenção e integração com outros sistemas podem apresentar problemas ao longo do tempo. A preservação do hardware, em especial, é uma alternativa cara, mesmo nas situações em que o hardware é compartilhado entre mais de um usuário. Além disso, essa alternativa não é exeqüível a longo prazo, uma vez que o hardware pode ser danificado de forma irreversível, ficando completamente indisponível.

Emulação: é a simulação de um determinado hardware ou software através de software. Permite que um computador moderno, possivelmente mais barato e de fácil manutenção, possa executar programas (software) antigos desenvolvidos originalmente para outra plataforma. Para evitar possíveis perdas de informação e funcionalidades, deve ser realizada com bastante rigor. A probabilidade de ocorrência de perdas de informações e funcionalidades aumenta à medida que são utilizadas diversas camadas de emulação, como resultado da aplicação dessa técnica repetidas vezes.

Conversão de dados: é empregada quando os formatos se tornam obsoletos. Os dados em formatos antigos são convertidos para novos formatos, apoiados em hardware e software mais atuais. Esse processo não está isento de problemas, podendo resultar em perdas de informações e funcionalidades. A conversão de dados também pode ser utilizada para reduzir a quantidade de formatos utilizados e, conseqüentemente, de sistemas a serem mantidos e gerenciados, de modo a facilitar as ações de preservação.

Migração: a migração para novos sistemas é realizada no caso de obsolescência de hardware, software ou formatos. Envolve, inclusive, a conversão de dados. Pode abranger uma grande quantidade de elementos – hardware, software e formatos – e, dessa forma, apresentar uma maior complexidade para ser planejada e executada. Apesar disso, mostra-se como uma alternativa interessante para acompanhamento das mudanças decorrentes da evolução tecnológica. A migração, assim como a emulação e a conversão de dados, apresenta riscos quanto à integridade e à funcionalidade dos documentos arquivísticos digitais, por isso, deve ser realizada de modo criterioso e sistemático.

Embora os problemas de degradação dos suportes e obsolescência tecnológica possam ser contornados com conhecimento técnico e uso de técnicas de preservação, sua resolução pode ser muito dispendiosa. Por isso, as preocupações com preservação devem existir desde a concepção do sistema e a escolha de sua base tecnológica. De uma forma geral, recomenda-se o uso de suportes de alta qualidade e que tenham uma vida útil prevista adequada para os propósitos de preservação, o monitoramento contínuo dos avanços tecnológicos e da degradação do suporte, a adoção de formatos abertos e a busca por soluções independentes de hardware, software e fornecedor.

As estratégias e os procedimentos de preservação devem ser bem definidos, documentados e periodicamente revisados. É importante destacar que as ações de preservação são contínuas e devem ser implementadas desde a produção dos documentos até sua destinação final.

Nesta seção, não se pretende apresentar procedimentos de preservação preestabelecidos ou argumentar em favor de uma técnica específica. Os requisitos foram organizados em aspectos físicos, lógicos e gerais.

1.10 Usabilidade

Projetar um sistema de software com boa usabilidade significa concentrar esforços para produção de um sistema que proporcione facilidade do uso, através de suporte para realização de tarefas simples, diretas e objetivas, que apóiem as metas de produtividade e qualidade de trabalho do usuário. Se os usuários do sistema encontrarem inúmeras dificuldades de operação, sua efetiva implantação pode fracassar, ocasionando desperdício de recursos.

Para se obter um maior grau de usabilidade deve-se pensar no usuário e em suas necessidades de utilização, o que significa criar um sistema fácil de entender, de operar e que siga padrões de boas práticas técnicas já conhecidas e bem estabelecidas.

Usabilidade depende diretamente das tarefas específicas que os usuários realizam por meio do sistema, bem como do nível de conhecimento do sistema pelos usuários envolvidos.

As recomendações para uma boa usabilidade estão associadas ao contexto operacional do sistema, aos diferentes tipos de usuários, tarefas, ambientes físicos e organizacionais.

Quando da elaboração da descrição das características do sistema, deve-se levar em consideração: facilidade de utilização da interface, tipos de usuários, facilidade na execução de tarefas, uso de equipamentos adequados, ergonomia, ambiente e contexto de uso.

1.11 Interoperabilidade

A adoção de regras e padrões de comunicação já consolidados permite a consulta entre sistemas heterogêneos sem que o usuário perceba as operações envolvidas, convergindo para uma relação sinérgica entre as partes.

Esta seção estabelece requisitos mínimos para que o sistema possa interoperar com

outros sistemas de informação, incluindo sistemas legados, respeitando normas de segurança de acordo com padrões abertos de interoperabilidade.

Por interoperabilidade, entende-se: “Intercâmbio coerente de informações e serviços entre sistemas. A interoperabilidade deve possibilitar a substituição de qualquer componente ou produto usado nos pontos de interligação por outro de especificação similar, sem comprometimento das funcionalidades do sistema”. Isto se faz através do uso de regras e padrões de comunicação.

O governo brasileiro definiu a arquitetura e-PING - Padrões de Interoperabiliade de Governo Eletrônico, visando à interoperabilidade nas diversas esferas do poder público.

Nos órgãos e entidades da Administração Pública Federal, o sistema tem que adotar a arquitetura e-PING a fim de aumentar a viabilidade técnica no intercâmbio de informações entre sistemas.

1.12 Disponibilidade

Requisitos de disponibilidade descrevem as exigências mínimas sobre prontidão de atendimento de um sistema.

Os requisitos de disponibilidade devem ser especificados pelo administrador do sistema de acordo o nível de serviço a ser fornecido. Por exemplo, os períodos previstos de atendimento (“8x5” indica 8 horas por dia útil. “24x7” indica atendimento contínuo), bem como tempo máximo tolerável em interrupções previstas. O grau de disponibilidade a ser estabelecido deve levar em conta fatores como, as regras de negócio da organização, a necessidade de realização de backup, manutenções planejadas, entre outros.

1.13 Desempenho e Escalabilidade

Os requisitos de desempenho enfocam a eficiência no atendimento aos usuários, de acordo com suas expectativas quanto aos tempos de resposta. Esses tempos de resposta são influenciados por fatores externos ao sistema, como, por exemplo, infra-estrutura de rede, volume de tráfego de dados e dimensionamento dos servidores e das estações de trabalho.

Para o sistema, entende-se escalabilidade como sendo a capacidade de um sistema responder a um aumento de usuários e volume de documentos arquivísticos, mantendo o desempenho das respostas do sistema. Para tanto, faz-se necessário, que a um aumento de hardware corresponda um aumento de desempenho.

Esses acréscimos de hardware podem se dar acrescentando-se mais hosts (escalabilidade horizontal) ou mais memória RAM e poder de processamento aos hosts existentes (escalabilidade vertical).

1.14 Conformidade Com A Legislação E Regulamentações

O sistema tem que cumprir a legislação e regulamentações vigentes.

1.14.1 RESOLUÇÃO N° 37/2012

A Resolução n° 37/2012 do CONARQ trata da presunção de autenticidade para documentos arquivísticos digitais. Partimos do princípio que autenticidade é a qualidade de um documento ser exatamente aquele que foiproduzido, não tendo sofrido alteração, corrompimento e auduteração. Já autenticação é a declaração de um documento arquivístico, num determinado momento, resultante do acréscimo de um elemento ou da afirmação por parte de uma pessoa investida de autoridade para tal.

Deste modo, podemos inferir que os documentos arquivísticos digitais podem ser autênticos sem serem autenticados. Essa situação é tratada como presunção de autenticidade que é a inferência da autenticidade de um documento arquivístico feita a partir de fatos conhecidos sobre a maneira como aquele documento foi produzido e mantido.

Assim, em um ambiente digital onde não possui mecanismos de autencidade, podemos presumir que os documentos são autênticos. Mas, conforme a resolução, o órgão deve cumprir os requisitos de:

Os procedimentos de controle compreendem quem produz, mantém/usa e preserva os documentos arquivísticos digitais e como essas ações são realizadas. Assim, é preciso que se definam direitos de acesso, espaços de trabalho (produção, recebimento, alteração, classificação, registro de metadados, arquivamento e destinação), conjunto de metadados e procedimentos de preservação.

O sistema informatizado tem que ser confiável. Para tanto deve incluir trilhas de auditoria, controle de acesso de usuários, métodos robustos para garantir a integridade dos documentos (como checksum ou hash), meios de armazenamento estáveis e medidas de segurança para controlar o acesso indevido à infraestrutura tecnológica (computadores, redes e dispositivos de armazenamento).

A entidade produtora e/ou custodiadora dos documentos arquivísticos digitais tem de possuir reputação idônea, demonstrar capacidade e conhecimento específico para gerenciar os documentos e, consequentemente, inspirar a confiança dos usuários.

1.14.2 RESOLUÇÃO N° 39/2014

A Resolução n° 39/2014 trata da adoção de repositórios digitais confiáveis para documentos arquivísticos. A adoção deste modelo é importante para a preservação de documentos arquivísticos digitais a longo prazo.

Considerando o material do SIGED encaminhado a estes arquivistas pudemos notar que este propõe-se a ser um repositório dos documentos digitais do SIG. Entretanto, percebemos que ele apenas armazena os documentos. Deste modo sugerimos que a AVMB estude a possibilidade de integrar o SIG com o Archivematica que consiste em um programa de código aberto que é voltado para manter padrões e acesso a longo prazo para objetos digitais.

1.15 OBSERVAÇÕES FINAIS

Não foi esclarecido em nenhum documento como se dará a captura dos documentos arquivísticos digitais em outros módulos do SIPAC e sistemas do SIG para o módulo protocolo. Tais documentos tem que ser gerenciados e avaliados de acordo com a legislação e técnicas vigentes;

Atualmente o IFFARROUPILHA não possui estrutura administrativa para colocar o módulo protocolo em produção. Há apenas uma unidade protocolizadora e nenhum arquivo central. Do mesmo modo, não possui a Comissão Permanente de Avaliação de Documentos de Arquivo e a Comissão Permanente de Avaliação de Documentos Sigilosos para balizar os trabalhos;

Em decorrência do que foi exposto no ponto anterior, há urgência de implementar os serviços de gestão documental nas unidades do Instituto;

Não fica claro a questão dos perfis de usuário pois não está claro os papéis de protocolizador, tramitador, distribuidor, arquivo corrente e arquivo intermediário. E as funções do Administrador estão dispersos em outros perfis.;

Deverão ser observadas as diretrizes constantes na Portaria Interministerial MJ/MP que aprova os procedimentos gerais para o desenvolvimento das atividades de protocolo, a Portaria Interministerial MJ/MP que aprova os procedimentos relativos à utilização do Número Único de Protocolo (NUP), e a Portaria Interministerial MP/MJ, que Institui o Sistema de Protocolo Integrado, que serão publicadas em janeiro de 2015.

2 ANÁLISE MÓDULO PROTOCOLO

2.1 Processos

A aba de Processos apresenta as seguintes funcionalidades: Cadastro, Movimentação, Juntada, Etiquetas para Capas, Etiquetas protocoladoras, Arquivo/Cancelamento/Diligência, Despachos e Gerenciamento.

2.1.1 Cadastro

Na opção Cadastro temos as atividades que envolve o cadastro e alterações de processos.

2.1.1.1 Cadastrar Processo

Dados Gerais do Processo

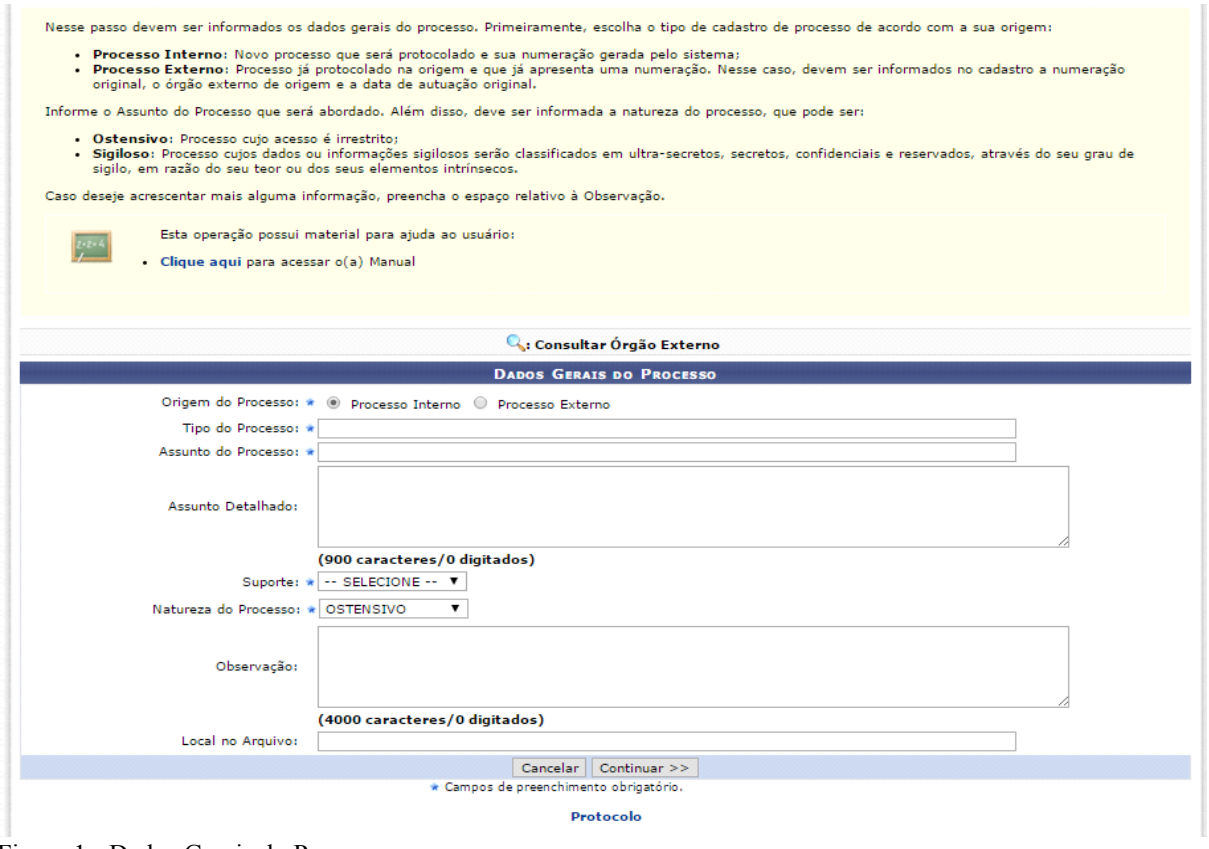

Figura 1 - Dados Gerais do Processo

Origem do Processo: verificar necessidade de cadastrar processo externo, visto que o processo externo já terá um registro de protocolo no seu órgão de origem, com seu histórico de movimentações e alterações. Ver projeto do governo federal de Protocolo Integrado.

Tipo do Processo: verificar a necessidade de inserção deste dado, baseado em um estudo da produção documental da instituição e uma análise dos termos presentes na listagem de tipos de processo, pois há uma clara confusão entre tipos documentais e assuntos.

Assunto do Processo: inserir os códigos de classificação adotados pela instituição.

Assunto detalhado: sem comentários.

Suporte:

O sistema oferece o cadastro de processos em suporte físico e suporte digital. Porém nota-se que não há diferenciação no tratamento do processo em virtude do suporte.

Natureza do processo:

Ostensivo: sem comentários.

Sigiloso: ao selecionar a opção sigiloso, aparece a seleção de grau de sigilo. Observar:

as autoridades que possuem competência para classificar, de acordo com o grau de sigilo, a fim de configurar os perfis de usuários;

os graus de sigilo passíveis de classificação no Instituto (reservado e pessoal);

a justificativa para a classificação como sigiloso.

Observações: sem comentários.

Local no arquivo: este campo pode ser retirado. Visto que este cadastro de processo é com o intuito de tramitação, não há necessidade de inserir esta informação.

Informações judiciais do Processo

Figura 2 - Informações Judiciais do Processo

Verificar a inserção das informações judiciais em processos digitais.

Documentos do processo

Situação 1 – Informar novo documento

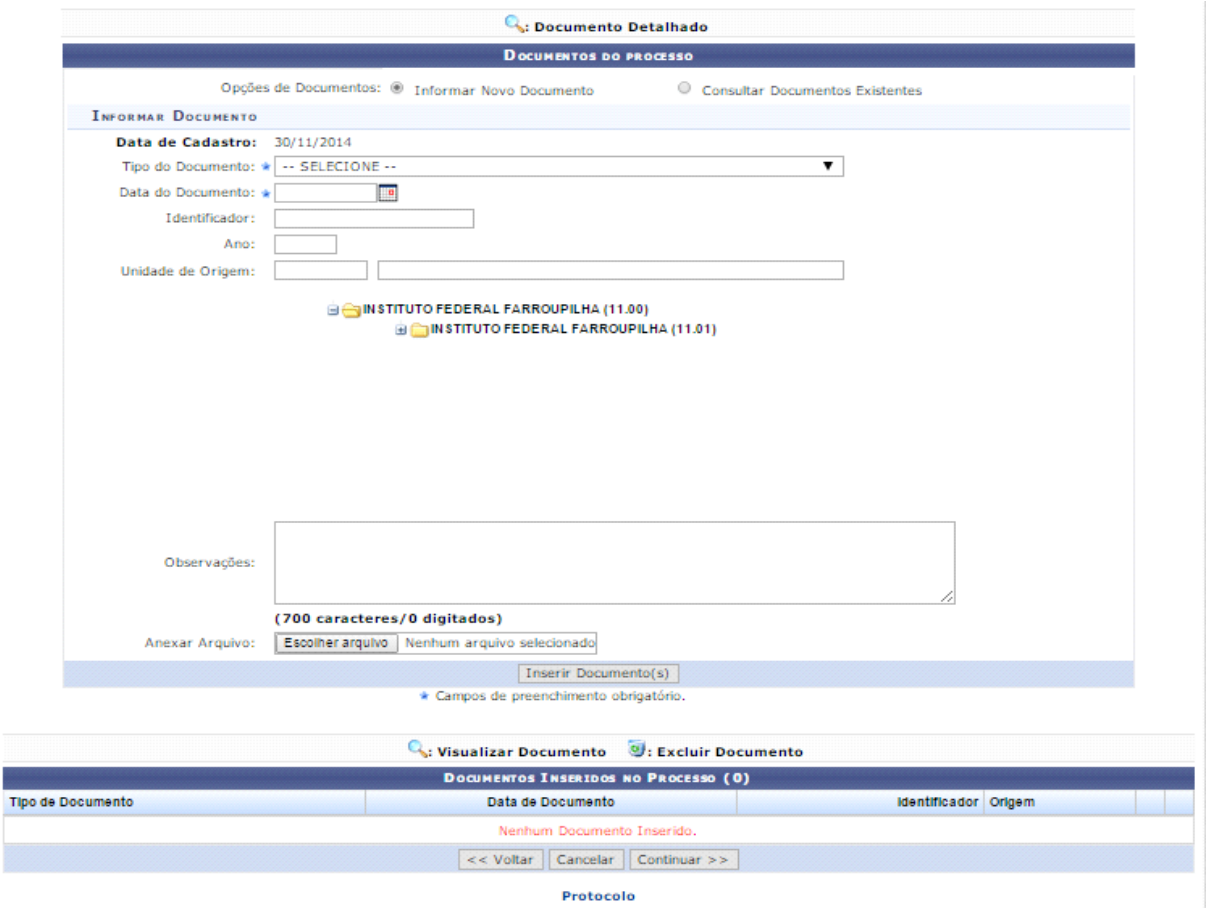

Figura 3 - Documentos do processo - incluir novo documento

Tipo documento: verificar listagem de tipos de documentos.

Data do documento: sem comentários.

Identificador e ano: sem comentários.

Unidade de origem:

Incluir opção de entrada quando o documento for emitido por pessoa física ou órgão externo.

Anexar arquivo: a opção de anexar arquivo não consta como obrigatória, porém ao tentar continuar sem anexo, retorna o aviso “Para prosseguir com o cadastro do processo, pelo menos um documento deve ser inserido no mesmo”. Observar:

1. a necessidade de obrigatoriedade de um objeto digital vinculado ao cadastro de processos físicos;

2. formatos de documentos aceitos; é possível anexar documentos em formato alterável;

3. questão de limitação ao documento motivador da abertura do processo ou inserir todos os documentos que formam o processo. Não há limite de documentos a serem anexados nesta etapa;

4. formalização do processo digital.

Situação 2 – Consultar Documentos existentes

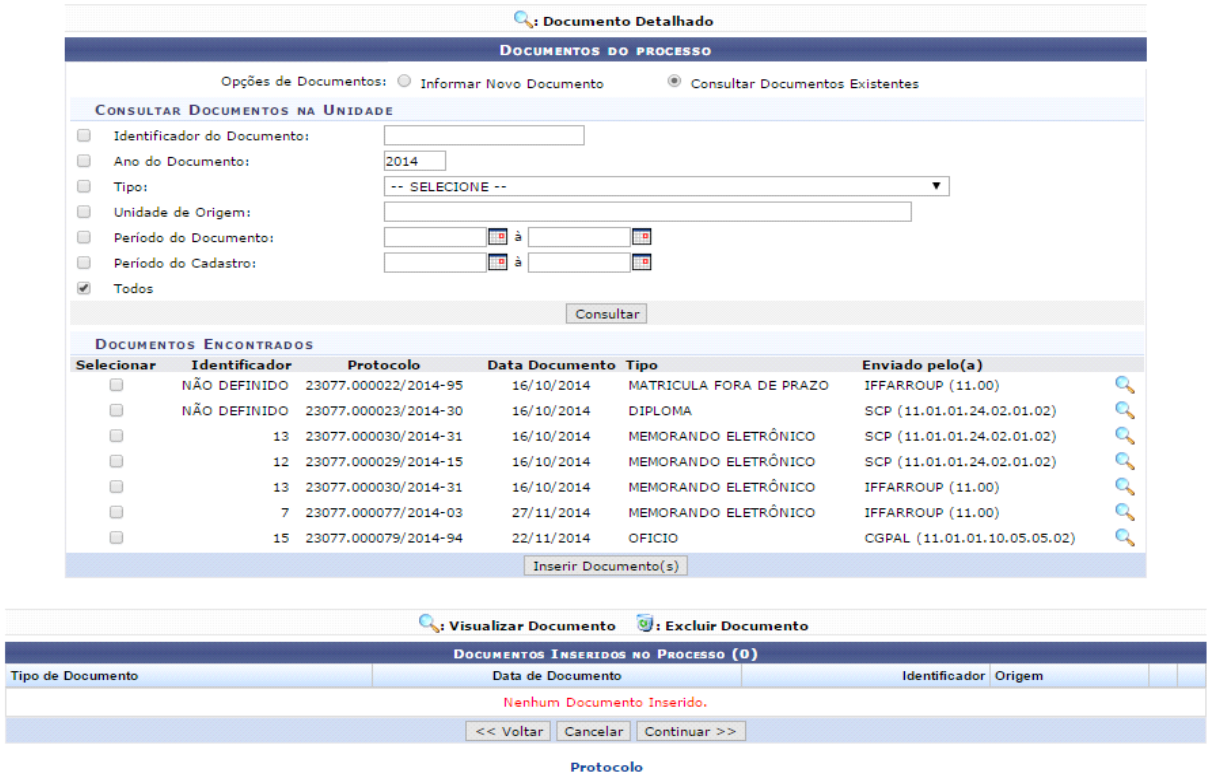

Figura 4 - Documentos do processo - consultar existentes

Ao selecionar inserir documentos já existentes, ou seja, já cadastrados no sistema, o módulo abre uma tela de consulta com os documentos que podem ser selecionados como documentos motivadores do processo.

Observar se histórico de movimentação e alterações do documentos vinculado ao processo é mantido e se estas informações continuam visíveis após a autuação do documento.

Dados do interessado a ser inserido

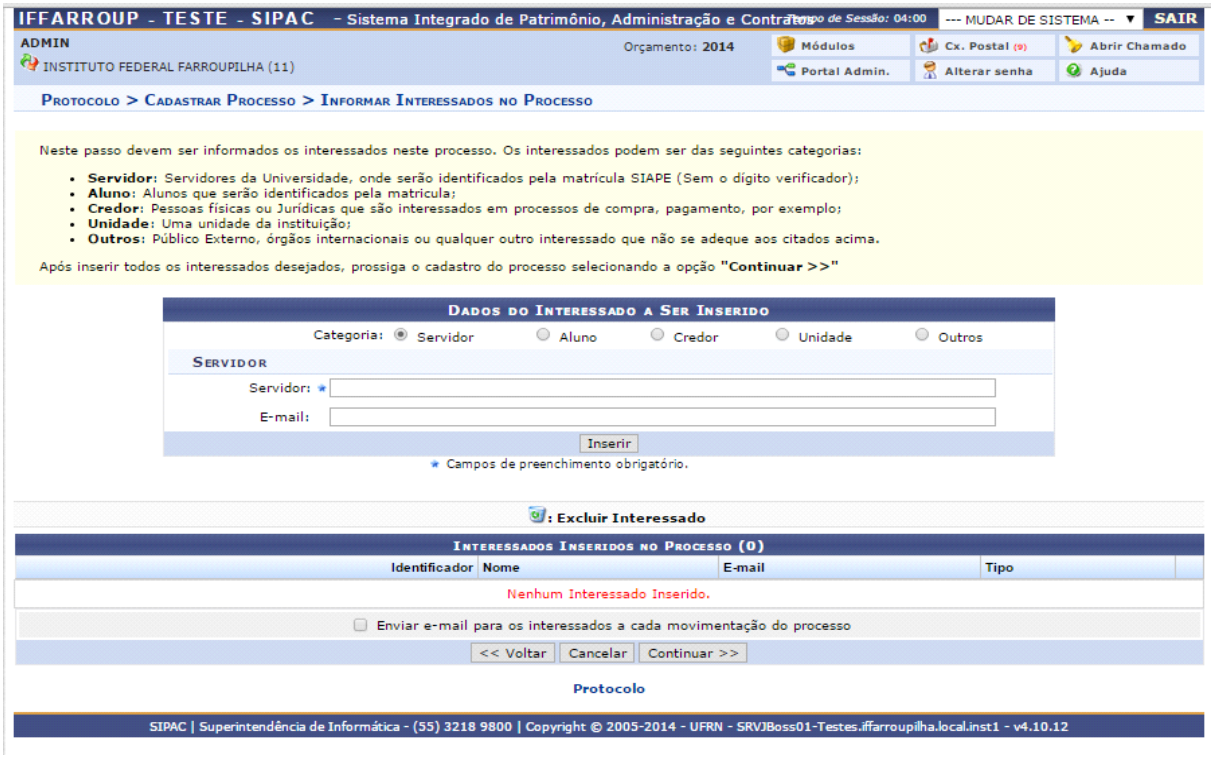

Figura 5 - Dados do interessado a ser inserido

A unidade protocoladora seria a responsável por definir se os interessados acompanhariam a movimentação do processo?

Dados do arquivo a ser anexado

Figura 6 - Dados do arquivo a ser anexado

Observar:

1. metadados de cadastro dos documentos a ser anexados;

2. os formatos de arquivos aceitos;

3. a configuração dos processos em que são anexados estes documentos.

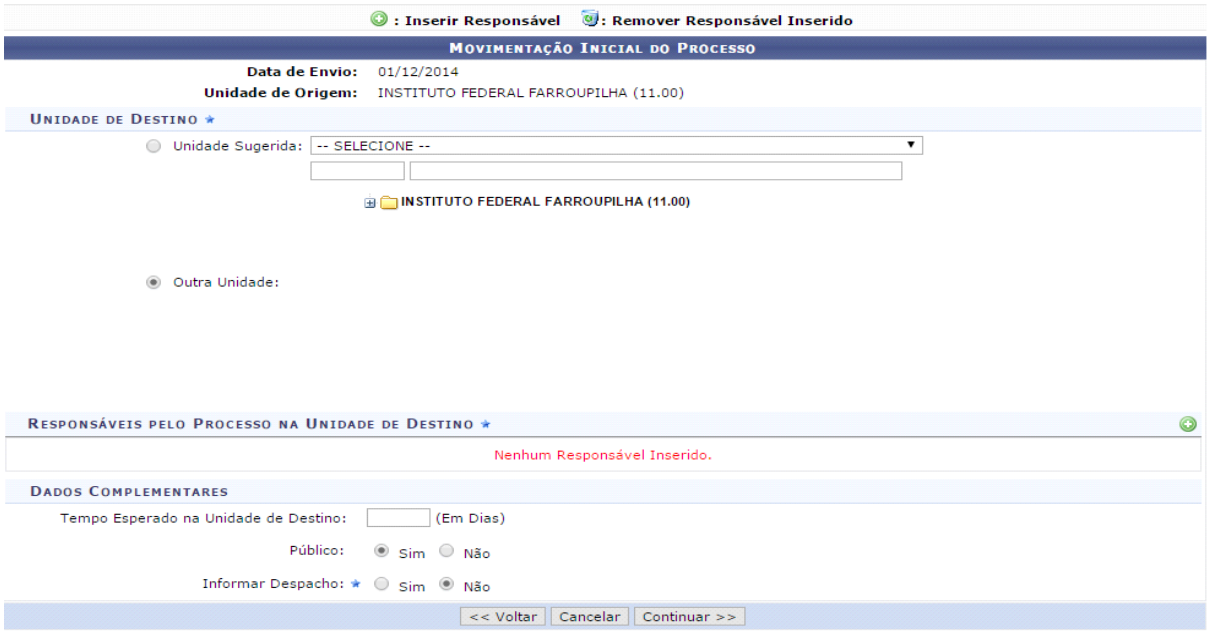

Figura 7 - Movimentção inicial do processo

Movimentação inicial do processo

Nesta etapa são inseridas as informações referentes ao órgão de destino do processo e informações sobre despacho.

Unidade de destino: inserir campo de entrada para destinação a órgãos externos.

Responsável pelo processo na unidade de destino: dado obrigatório quande de processos sigilosos.

Dados complementares:

Tempo esperado na unidade de destino: sem comentários

Público: retirar este dado ou verificar qual a função deste. Se o processo for sigiloso, qual o motivo a opção de público? Se o processo for ostensivo, por que a opção de tornar não público?

Informar despacho: verificar a necessidade deste campo, já que quando da criação do processo e sua movimentação inicial, o processo não teria ainda despachos.

Ao selecionar a opção Sim, novos campos são mostrados:

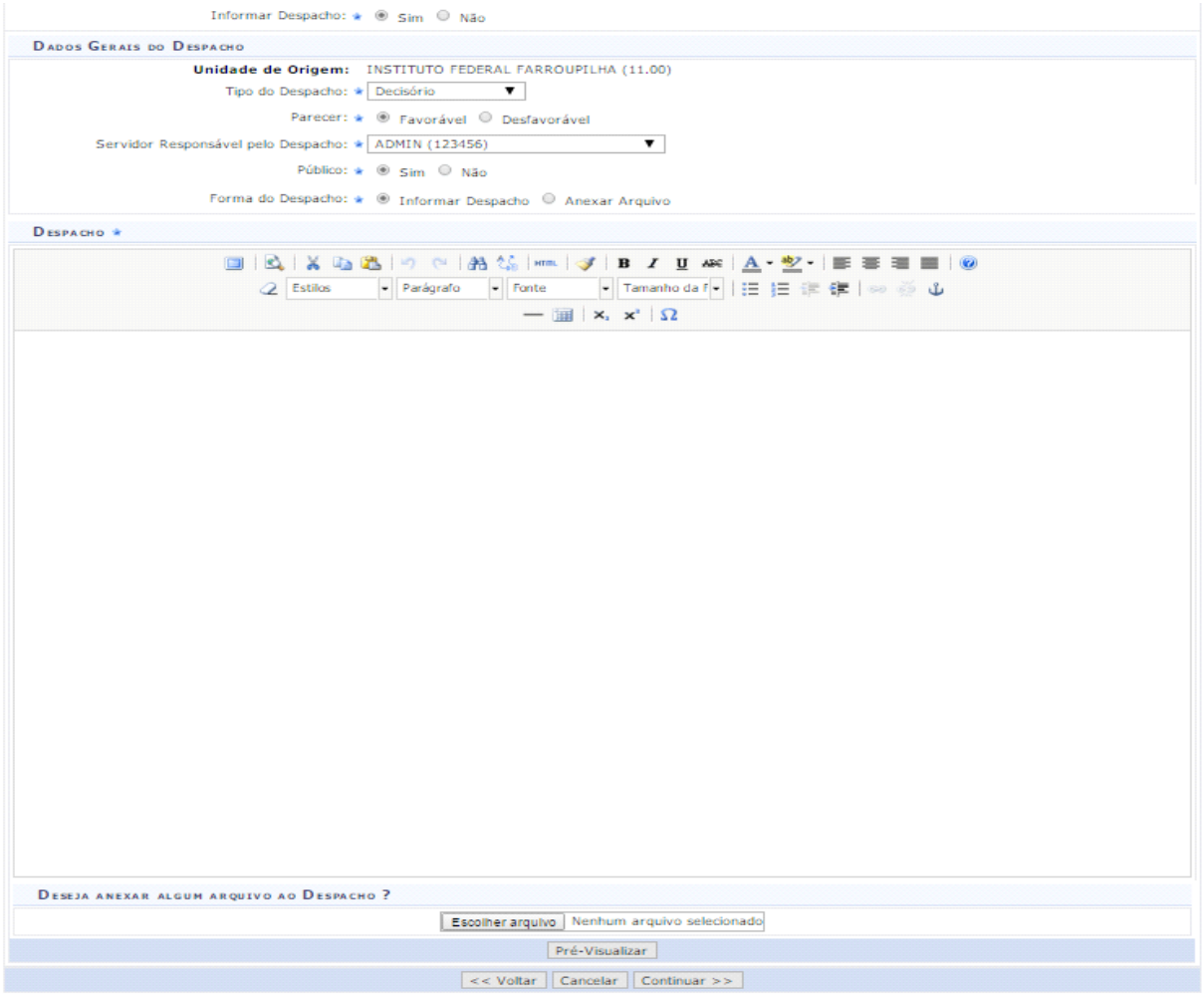

Figura 8 - Dados gerais do despacho

Tipo de despacho: sem comentários.

Parecer: sem comentários

Servidor responsável pelo despacho: verificar esta possibilidade de indicar outra pessoa como o responsável/autor do despacho.

Público: verificar qual a função deste dado. Retirar este dado.

Forma do despacho:

1. Informar despacho: É possível redigir o despacho na tela aberta. Verificar a formatação do despacho como texto.

2. Anexar arquivo: possibilidade de anexar documento. Verificar formatos de arquivo aceitos.

Ao visualizar o despacho redigido, aparece o termo “Autenticado digitalmente”. Retirar este termo, já que não condiz com a definição de autenticação digital.

Não foi possível prosseguir com o cadastro do processo, já que ao selecionar a unidade de destino retorna o erro “Unidade de destino não pode ser gestora”.

Segundo o manual do Sistema, as próximas etapas do cadastro seriam: confirmação do cadastro, geração da capa do processo e geração da guia de movimentação.

2.1.1.2 Alterar Processo

Não está claro quais os processos passíveis de alteração ou em que momento eles podem ser alterados. De acordo com os exemplos existentes, seria possível alterar apenas processos não recebidos pela unidade de destino. Porém, seria apenas na fase de movimentação inicial ou a qualquer momento da produção e trâmite do documento?

Ao escolher o processo a ser alterado, as etapas são iguais ao cadastro de processo. Salienta-se que, aparentemente, é possível alterar qualquer dado do processo, bem como excluir objetos digitais vinculados ao processo. Os únicos dados não modificáveis nesta aba são o NUP e o órgão de destino (que pode ser alterado em outra funcionalidade).

Restringir as modificações no documento.

As informações referentes as alterações realizadas no processo são visíveis quando da consulta de processo detalhado/histórico.

2.1.1.3 Alterar responsável

Não foi possível verificar a funcionalidade. Manual não localizado.

2.1.1.4 Anexar Documentos.

Não foi possível verificar. Segundo o manual, esta funcionalidade anexa novos documentos (não cadastrados no sistema) ao processo, porém o documento não é protocolado.

Verificar a configuração destes anexos no processo digital.

2.1.1.5 Autuar processo

Verificar a necessidade desta funcionalidade, uma vez que o Cadastro de processo possui a mesma funcionalidade.

2.1.1.6 Cadastrar Despacho

Etapas iguais ao Informar despacho no Cadastro de processo.

2.1.1.7 Cadastrar Ocorrência

Não foi possível verificar. Verificar qual a função.

2.1.1.8 Registrar dados do processo

Esta funcionalidade permite cadastrar processos com números de protocolos reservados através da funcionalidade Etiquetas protocoladoras. Verificar necessidade destas funcionalidades na instituição.

2.1.1.9 Fluxo do processo

Consultar o fluxo do processo: talvez esta funcionalidade poderia estar vinculada a Consultas/Relatórios e não ao Cadastro de Processo.

2.1.1.10 Processos sigilosos

Desclassificar processos:

Figura 9 - Confirmação de desclassificação de processo sigiloso

Consulta de Processos sigilosos: consulta e listagem dos processos sigilosos passíveis de alteração. Verificar autoridades competentes para desclassificação.

Confirmação de desclassificação de processo sigiloso: tornar o campo de observação obrigatório.

Reclassificar processos:

Consulta de Processos sigilosos: consulta e listagem dos processos sigilosos passíveis de alteração. Verificar autoridades competentes para reclassificação.

Confirmação de Reclassificação de Processo Sigiloso: tornar campo de Observação obrigatório.

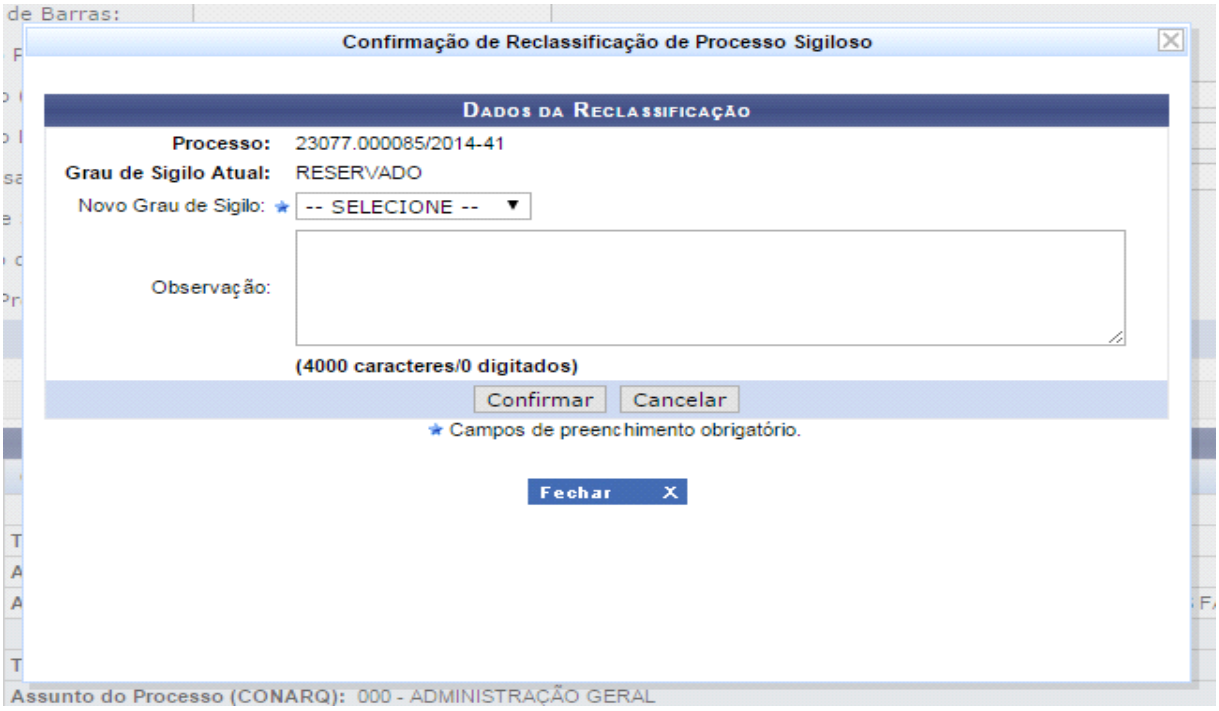

Figura 10 - Dados da reclassificação

2.1.2 Etiquetas para Capa

2.1.2.1 Gerar/Reimprimir Etiquetas

Situação 1 - Impressão

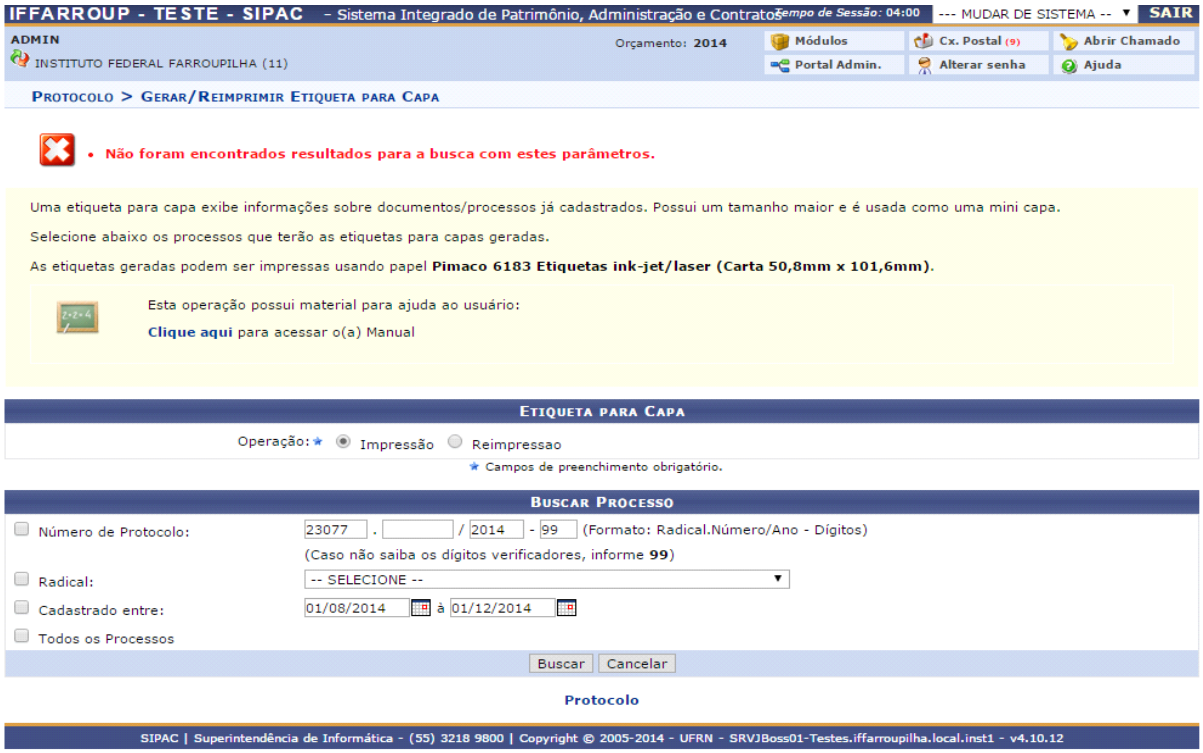

Figura 11 - Etiqueta para capa

Não foi possível verificar as outras etapas. A impressão de etiquetas poderia ser logo após o cadastro, tal como a impressão de capas, para agilizar o procedimento.

Situação 2 – Reimpressão

A opção Reimpressão permite que etiquetas de processos já impressas, sejam emitidas novamente. No entanto, mesmo com a obrigatoriedade de preenchimento do campo Justificativa, esta funcionalidade possibilitaria ações de má-fé.

Verificar compatibilidade com impressoras de etiquetas térmicas.

Figura 12 - Etiqueta para capa - consulta

Etiqueta reimpressa

Figura 13 - Etiqueta para capa - reimpressão

2.2.1.2 Histórico de Impressão / Reimpressão

O Sistema gera relatórios de quantidade de etiquetas impressa ou reimpressas por usuário.

Analisar inclusão de um relatório ou histórico de reimpressões (no detalhamento do processo) por processo informando a data, horário, justificativa e usuário.

Verificar erros de gravação em datas de impressão/reimpressão, do retorno do relatório quando por busca pelo NUP e as respectivas quantidades de impressões/reimpressões.

Figura 14 - Histórico de impressão/reimpressão de etiquetas para capa

2.1.3 Despachos eletrônicos

2.1.3.1 Autenticar

Não foi possível verificar.

Esta funcionalidade permite que o usuário autorize despachos cuja autoria foi indicada como dele.

Modificar termo Autenticar por Autorização.

2.1.4 Movimentação

2.1.4.1 Alterar encaminhamento

Processos encaminhados pela unidade do usuário e que ainda não tenham sido recebidos na unidade de destino podem ter o encaminhamento alterado.

Figura 15 - Processos enviados e ainda não recebidos

Processos enviados e ainda não recebidos: Tela de consulta e listagem de processos passíveis de alteração de encaminhamento.

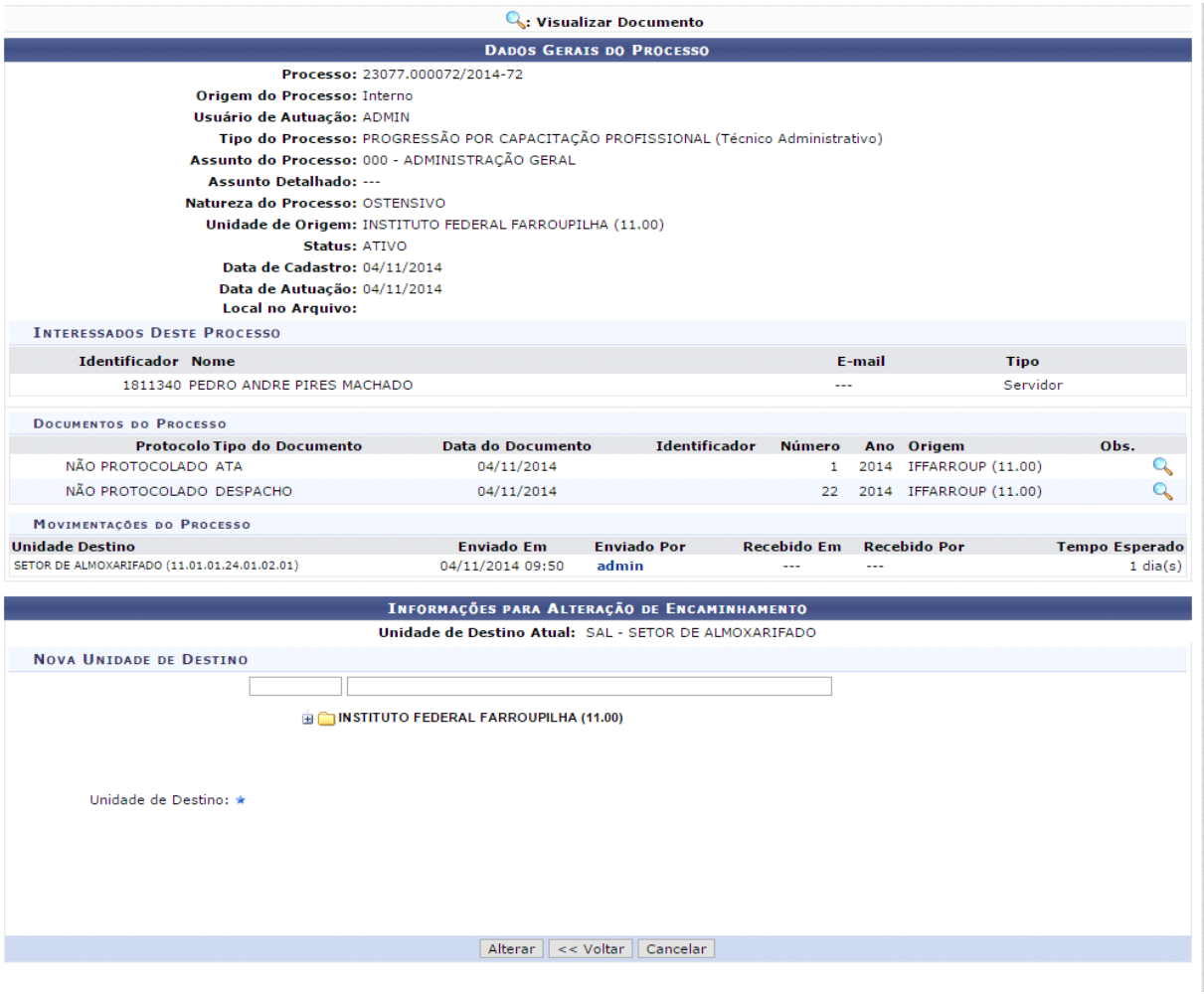

Figura 16 - Informações para alteração do encaminhamento

Nova Unidade de Destino: Inserir campo para encaminhamento a órgãos externos.

2.1.4.2 Cancelar encaminhamento

Esta funcionalidade permite cancelar o encaminhamento de processos que ainda não tenham sido recebidos pela unidade de destino.

Processos com movimentação inicial não podem ter o encaminhamento cancelado, apenas modificado.

As funcionalidades de alteração e cancelamento de encaminhamento poderiam ser unificadas em uma tela.

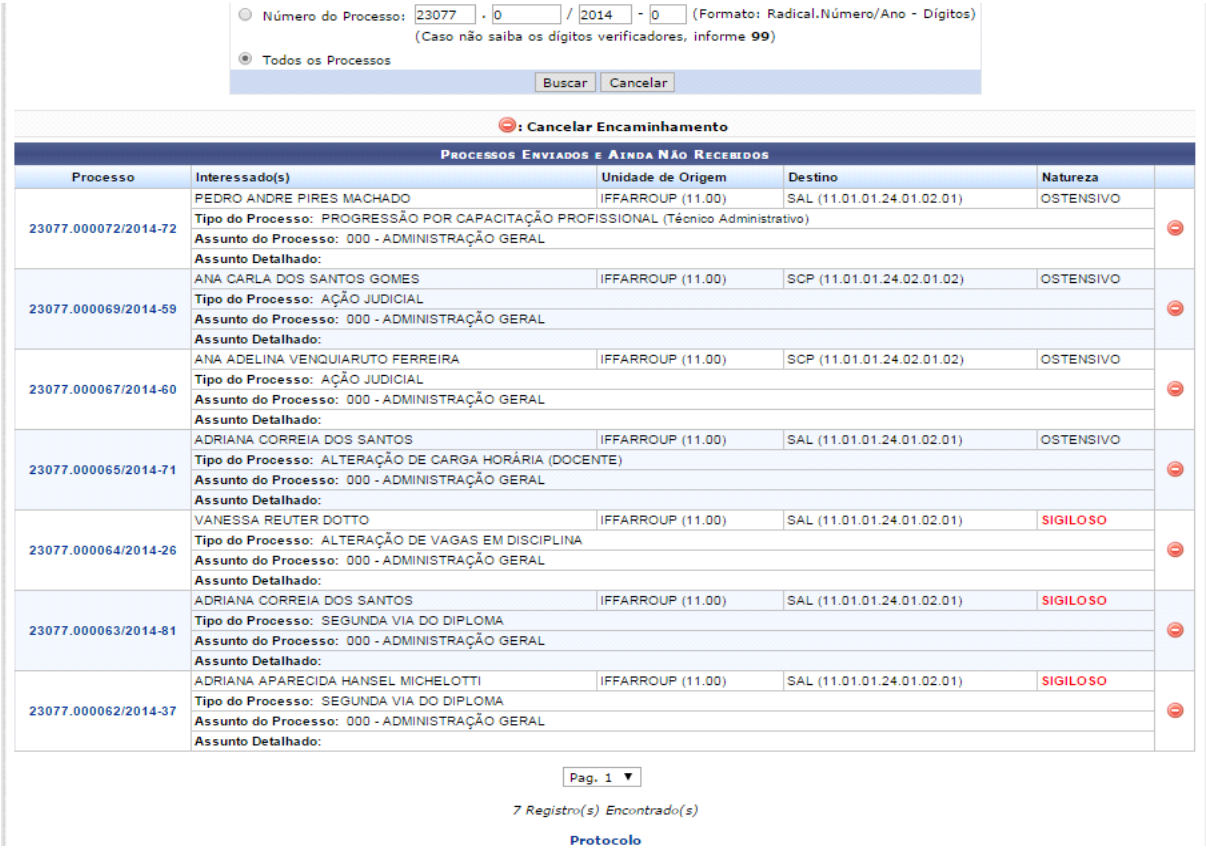

Figura 17 - Processos enviados e ainda não recebidos – cancelar encaminhamento

2.1.4.3 Registrar envio (saída)

Não foi possível verificar

2.1.4.4 Registrar recebimento

Não foi possível verificar.

Segundo o manual, há processos que bloqueiam a unidade. No que consiste este bloqueio? Quais os parâmetros para que os processos bloqueiem a unidade?

2.1.4.5 Ferramenta de para recebimento com Códigos de barras

Sem comentários.

2.1.5 Juntada

2.1.5.1 Juntada de processos

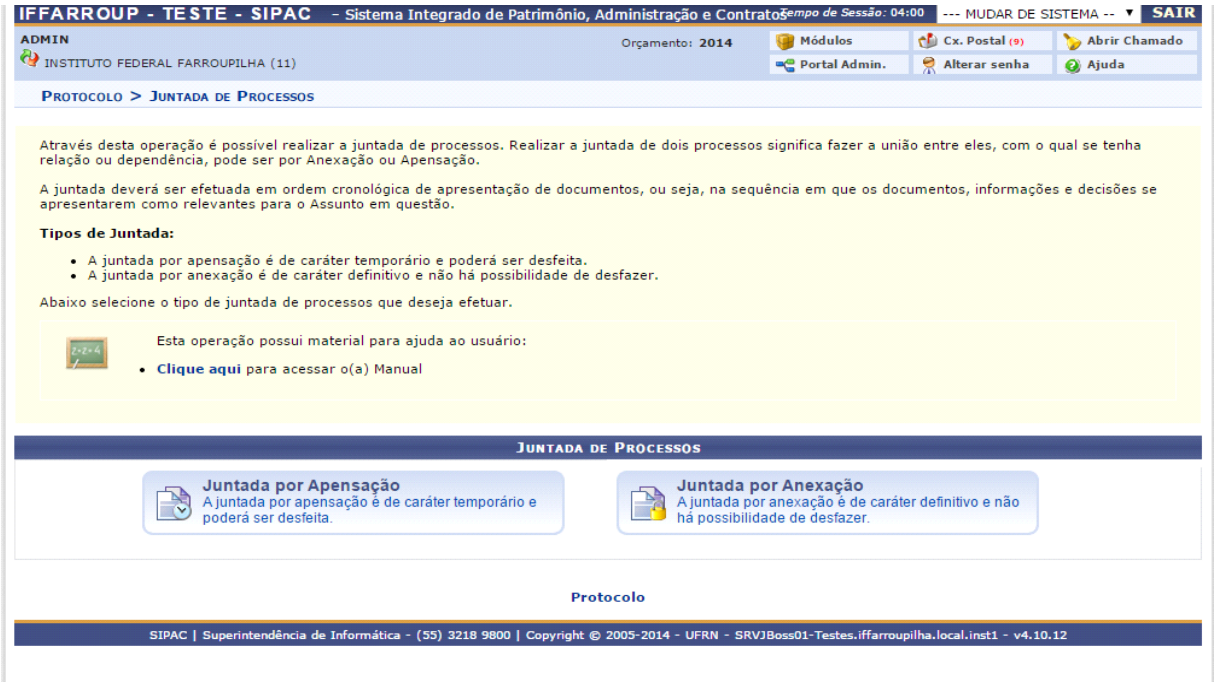

Figura 18 - Juntada de processos

A tela inicial apresenta os dois tipos de juntada: por apensação e por anexação.

Juntada por apensação: não foi possível verificar, pois não há retorno na busca por processos.

Juntada por anexação: não foi possível verificar pois não há retorno na busca por processos.

Poderia ser uma única tela, com a opção de escolha entre apensação e anexação, já que aparentemente o processo de juntada ocorre da mesma maneira.

2.1.5.2 Desapensação

Não foi possível verificar.

2.1.5.3 Cancelamento de juntadas

Excluir funcionalidade.

2.1.6 Etiquetas protocoladoras

Verificar necessidade desta funcionalidade para a instituição.

2.1.6.1 Gerar Etiquetas

Quando houver os radicais de todos os campus cadastrados, qualquer usuários poderá emitir lotes de etiquetas protocoladoras para campus que não o seu?

Não foi possível verificar.

2.1.6.2 Reimprimir Etiquetas

Não foi possível verificar.

2.1.6.3 Histórico de Impressão/Reimpressão

Não foi possível verificar.

2.1.7 Arquivo/Cancelamento/Diligência

2.1.7.1 Arquivar Processo

Não foi possível verificar.

Verificando o manual, percebeu-se que:

Tela de consulta atual do sistema não condizente com o manual;

Necessário outros campos para facilitar a busca de processos;

Não há registro de informação sobre data de arquivamento;

Não realiza arquivamento em dossiê;

Não consta a classificação;

Não consta a temporalidade;

Não há controle de prazos de guarda documental;

Não realiza transferência de documentos;

Funcionalidade precária. Apenas registra a localização física.

2.1.7.2 Desarquivar processo

Não foi possível verificar.

2.1.7.3 Diligência

Não foi possível verificar.

2.1.7.4 Solicitar cancelamento

Excluir funcionalidade.

2.1.7.5 Confirmar cancelamento

Excluir funcionalidade

2.1.8 Gerenciamento

2.1.8.1 Ocorrências com prazos atrasados

Sem comentários.

2.1.9 Despachos eletrônicos

2.1.9.1 Autenticar

Mudança do termo Autenticar por Autorizar.

Retirar expressão “Autenticado digitalmente” do corpo do texto dos despachos eletrônicos cadastradas. Expressão não corresponde ao tipo de operação realizada.

2.2 Documentos

2.2.1 Cadastro

2.2.1.1 Cadastrar documento

Situação 1 – Documento interno

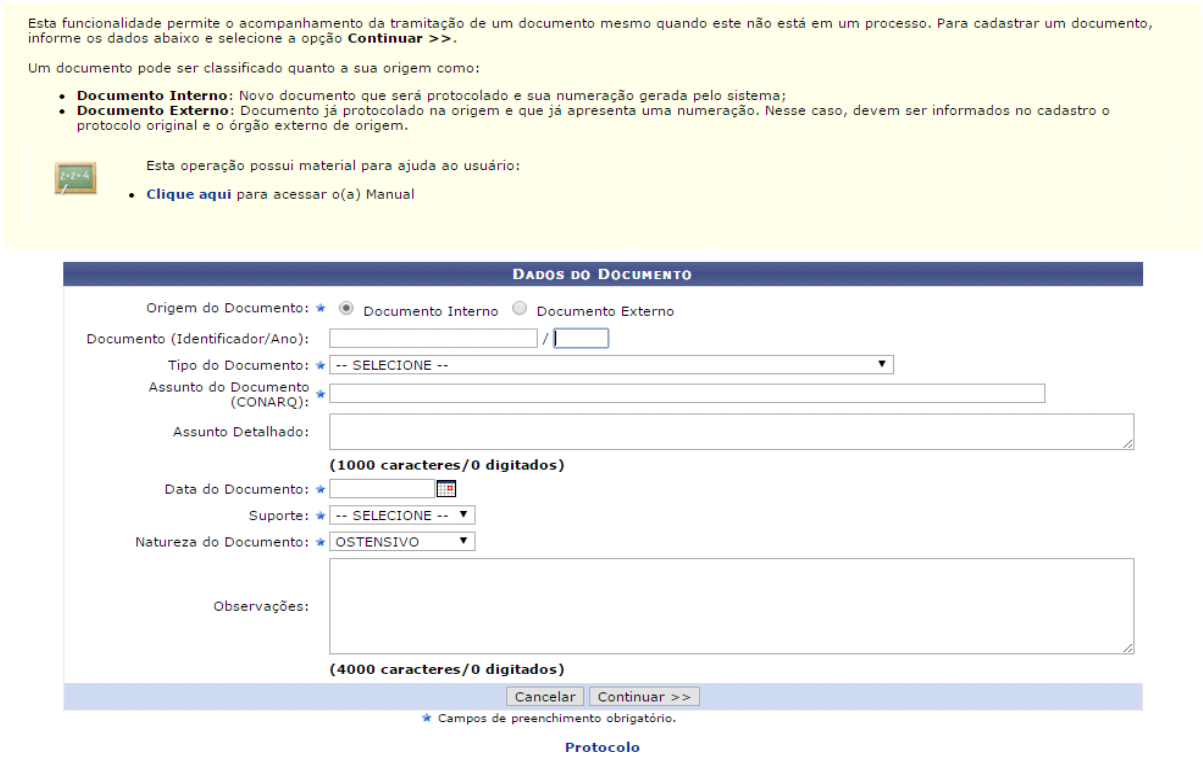

Figura 19 - Dados do documento

Dados do documento

Documento (Identificador/ano): sem comentários

Tipo do documento: verificar listagem de tipos de documentos.

Assunto do documento (CONARQ): sem comentários.

Assunto detalhado: sem comentários.

Data do documento: sem comentários.

Suporte: sem comentários.

Natureza do documento:

Ostensivo: sem comentários.

Sigiloso: ao selecionar a opção sigiloso, aparece a seleção de grau de sigilo. Observar:

1. as autoridades que possuem competência para classificar, de acordo com o grau de sigilo, a fim de configurar os perfis de usuários;

2. os graus de sigilo passíveis de classificação no Instituto (reservado e pessoal);

Observações: sem comentários.

Dados do arquivo a ser anexado

Figura 20 - Dados do arquivo a ser anexado

No cadastro de documento não é obrigatório a anexação de arquivo, mesmo quando o suporte do documento cadastrado é informado como digital. Ou seja, a captura de documento digital não é obrigatória.

Verificar a aceitação de anexos em formatos alteráveis.

Dados do interessado a ser inserido

Figura 21 - Dados do interessado a ser inserido

Movimentação inicial

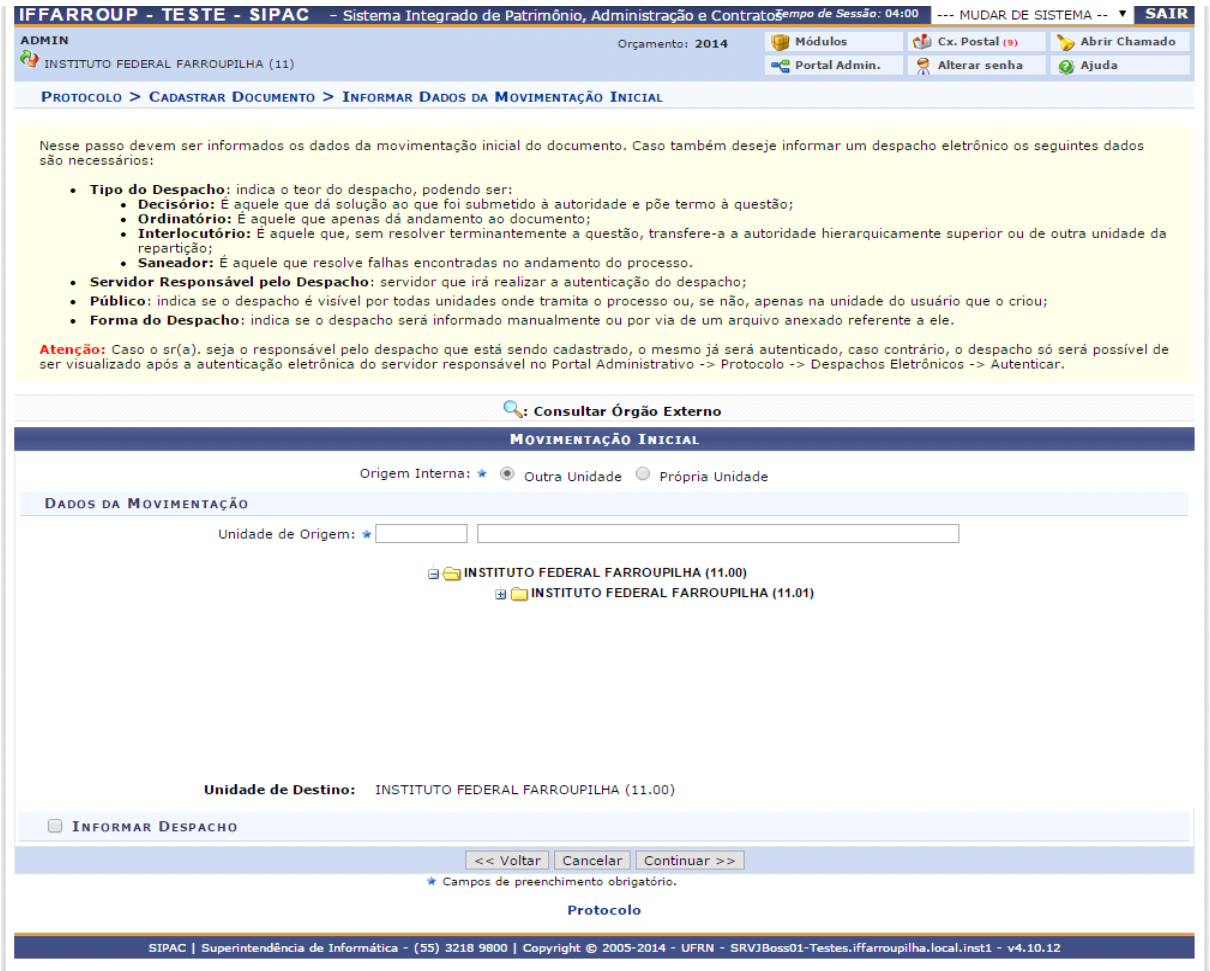

Figura 22 - Movimentação inicial

Unidade de destino: como proceder quando o documento é circular? Não é possível incluir mais de uma unidade de destino.

Informar despacho: procedimento idêntico ao cadastro de despacho em processos.

Não foi possível verificar as outras etapas.

Salientamos que não é possível inserir informações de expedição.

Situação 2 – Documento externo

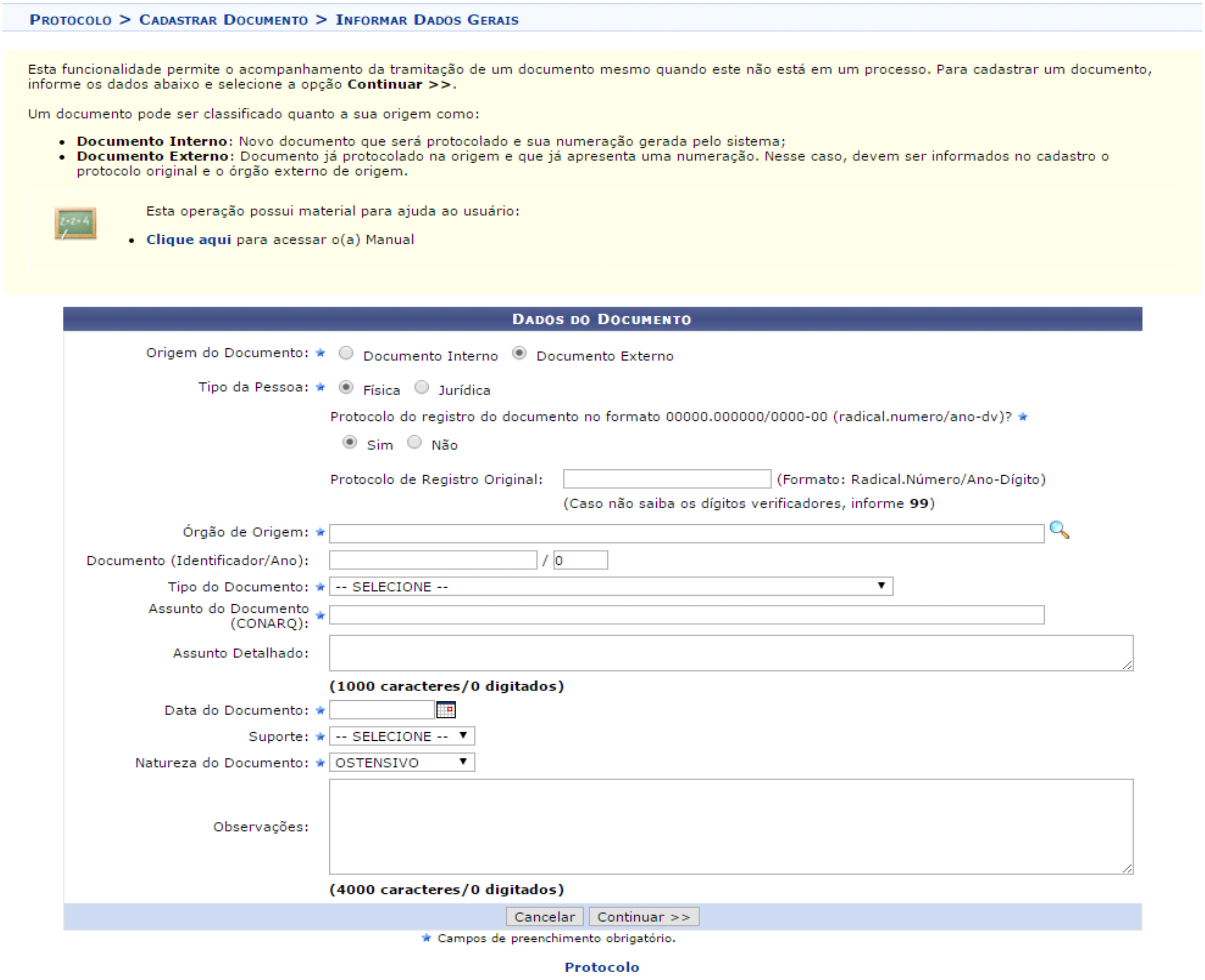

Figura 23 - Dados do documento - documento externo

Tipo de pessoa: não há diferenciação de metadados para cadastro de documentos emitidos por pessoa física ou jurídica.

Órgão de origem: necessário cadastro anterior dos órgãos externos. Gerará truncamento no fluxo do documento devido a espera do cadastro dos órgãos, que será feito apenas pela unidade central (reitoria).

Inserir campo para informar Pessoa física emissora do documento. Campos atuais abrangem apenas Pessoa jurídica.

Sistema torna obrigatório a informação de órgão de origem mesmo para pessoa física.

Documento (identificador/ano): sem comentários.

Tipo do documento: revisar listagem de tipos de documentos.

Assunto do documento (CONARQ): sem comentários.

Assunto detalhado: sem comentários.

Data do documento: inserir campo para informar data de recebimento de documentos

Suporte: sem comentários.

Natureza do documento:

Ostensivo: sem comentários.

Sigiloso: ao selecionar a opção sigiloso, aparece a seleção de grau de sigilo. Observar:

as autoridades que possuem competência para classificar, de acordo com o grau de sigilo, a fim de configurar os perfis de usuários;

os graus de sigilo passíveis de classificação no Instituto (reservado e pessoal);

a justificativa para a classificação como sigiloso.

Observação: sem comentários.

Dados do arquivo a ser anexado

Mesmo procedimento de inserção de informação do cadastro de documentos internos.

Dados do interessado a ser inserido

Mesmo procedimento de inserção de informação do cadastro de documentos internos.

Não é obrigatório a inserção de interessado.

Movimentação inicial

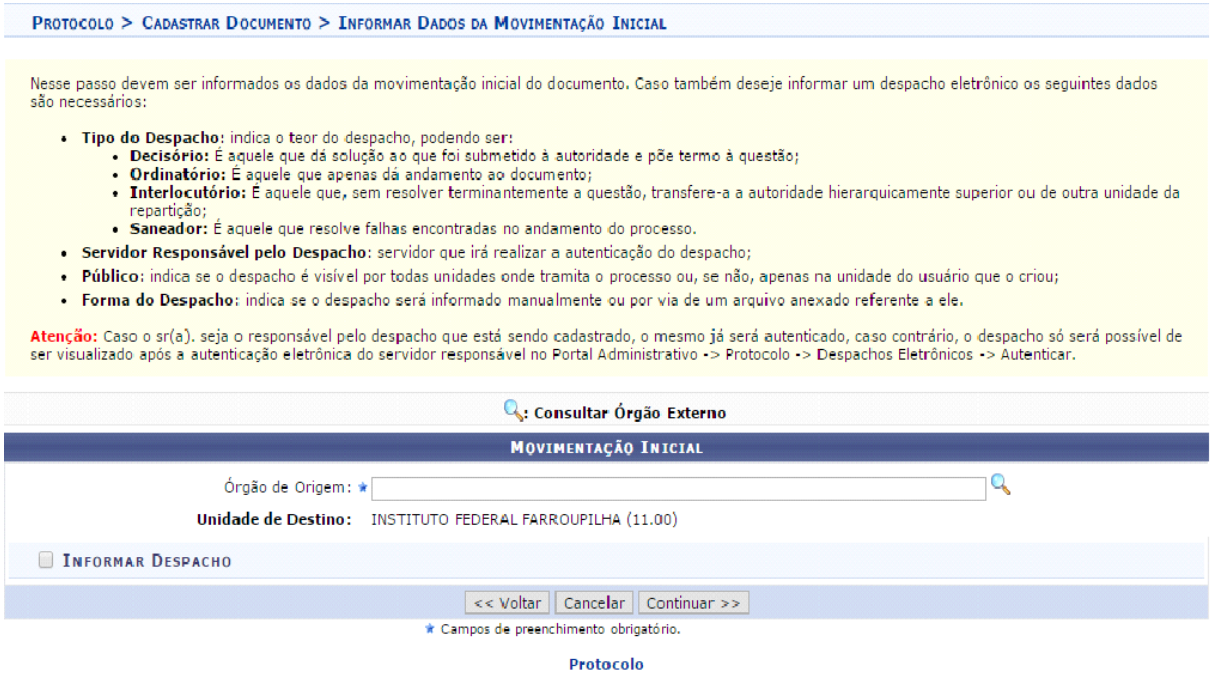

Figura 24 - Movimentação inicial - documento externo

Informar despacho: mesmo procedimento do cadastro de despachos em processos.

Após confirmação do cadastro, ao gerar comprovante de movimentação, a data informada como data de envio, na verdade seria a data de cadastro do documento na unidade de destino. Por isso, inserir campo de data de recebimento do documento externo na unidade.

2.2.1.2 Cadastrar ocorrência

Sem comentários.

2.2.1.3 Cadastrar despacho

Mesmo procedimento de cadastro de despacho em Cadastro de Processos.

2.2.1.4 Alterar documento

Verificar quais os documentos passíveis de alterações.

Dados do documento

Fgura 25 - Dados do documentos - alteração

Restringir dados que podem ser alterados. Atualmente, somente o número de protocolo e origem do documento não são alteráveis. Possibilidade de ações mal intencionadas.

Verificar bug sistema: não aparece campo para alterar natureza do documento, mas é necessário o preenchimento do campo para prosseguir.

Não foi possível verificar as próximas etapas.

2.2.1.5 Registrar dados do documento

Mesmo procedimento de Registrar dados de Processos.

2.2.1.6 Documentos sigilosos

Desclassificar documentos: mesmos procedimentos de Desclassificar processos.

Reclassificar documentos: mesmos procedimentos de Reclassificar processos.

2.2.2 **Movimentação**

2.2.2.1 Registrar recebimento

Não foi possível verificar.

2.2.2.2 Registrar envio (saída)

Não gera guia de movimentação.

2.2.2.3 Alterar encaminhamento

Não gera guia de movimentação.

2.2.2.4 Cancelar encaminhamento

Verificar como fica registrada a situação de documentos cujo encaminhamento foi cancelado.

2.2.3 Arquivo

2.2.3.1 Arquivar documento

Sobre a funcionalidade de arquivamento constatou-se que:

não realiza arquivamento em dossiê;

não consta a classificação;

não consta a temporalidade;

não há controle de prazos de guardar documental;

funcionalidade precária. Apenas registra a localização física, que não é informação obrigatória.

2.2.3.2 Desarquivar documento

Sem comentários.

2.2.4 Despachos eletrônicos

2.2.4.1 Autenticar

Mudança do termo Autenticar por Autorizar.

Retirar expressão "Autenticado digitalmente" do corpo do texto dos despachos eletrônicos cadastradas. Expressão não corresponde ao tipo de operação realizada.

2.3 Memorandos

Esta funcionalidade refere-se a emissão de memorandos eletrônicos e suas alterações e movimentações.

2.3.1 Cadastro

2.3.1.1 Cadastrar Memorando

Cadastro de memorando eletrônico

Figura 26 - Cadastro memorando eletrônico

Opção Com cópias: há alguma sinalização de que o memorando recebido é cópia e não original?

Memorando eletrônico

Redação do memorando

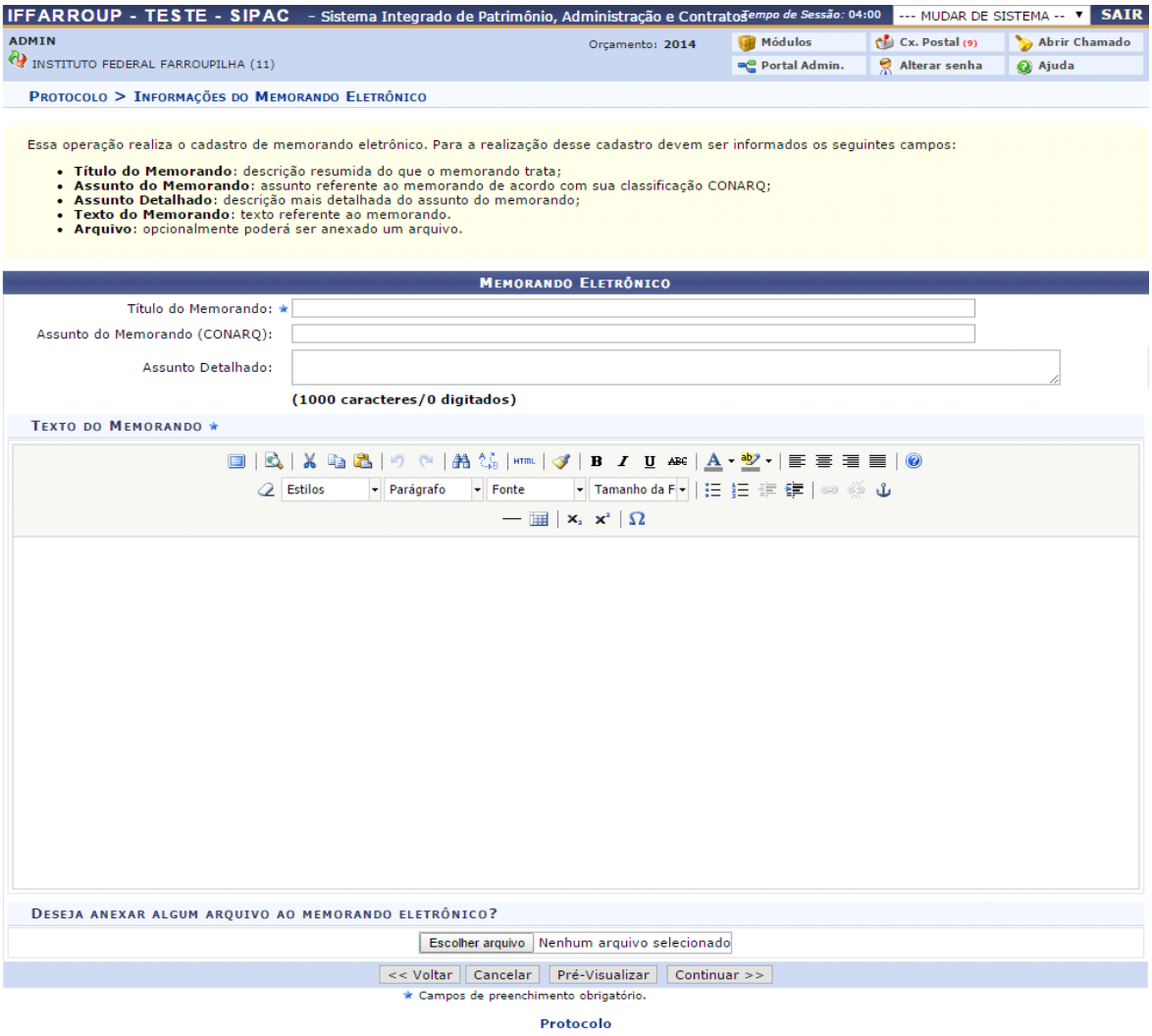

Figura 27 - Memorando eletrônico

Título do Memorando: sem comentários.

Assunto do memorando (CONARQ): campo não obrigatório. Em que momento do ciclo documental será inserida a classificação do memorando?

Assunto detalhado: sem comentários.

Texto do Memorando: Revisar a forma e estrutura da espécie documental Memorando, de acordo com as normas do Manual de Redação da Presidência da Republica, na apresentação final do documento:

Retirar logo da Instituição.

Inserir Destinatário: nome e Cargo. O memorando apresenta esta informação apenas quando na tela de cadastro da unidade destinatária, marcar a opção “Não encontrei a unidade, buscar por responsável”.

Trocar termo Título por Assunto.

O local será inserido de acordo com a cidade do Campus onde o servidor está lotado? Centros de Referências serão também cadastrados como unidades, para que seja possível puxar a cidade da unidade?

Inserir numeração de parágrafo e recuo de parágrafo.

Retirar o número de identificador (id) do corpo do texto. Deixar apenas a numeração do memorando.

Trocar termo “autenticado”.

Servidores responsáveis por autenticar o memorando

Figura 28 - Servidores responsáveis por autenticar o memorando

Assinatura do servidor: Qualquer usuário pode definir outrem como responsável pela autorização do memorando?

Trocar o termo “autenticar”.

Ver conceitos de autor e redator. Sistema deve manter registro dos dois perfis.

Unidade do servidor: servidor terá mais de uma unidade vinculada ao seu perfil? Por exemplo, terá registro dos conselhos, colegiados, comissões de modo que o servidor selecione de qual unidade aquele documento será emitido?

Opção Gravar: salva o documento, que é mantido em Rascunhos (painel de memorandos).

Enviar memorando: encaminha o memorando, desde que o autenticador seja o mesmo usuário que está conectado. Caso o autenticados seja outro usuário, o memorando será encaminhado para autenticação, para posterior envio a unidade de destino.

2.3.1.2 Cadastrar memorando circular

Verificar necessidade desta funcionalidade. Poderia ser inserida uma opção na tela de cadastro do memorando para configurar como Memorando circular, abrindo inserção de vários destinatários naquela funcionalidade.

Consulta de grupos / Grupos destinatários memorando circular

Figura 29 - Consulta de grupos

Grupos de destinatários: onde são cadastrados os grupos? Não seria uma opção mais viável a seleção de destinatário por destinatário?

Não tornará mais moroso o processo de envio de memorandos caso o grupo de destinatários não esteja cadastrado previamente?

Próximas etapas idênticas ao procedimento de cadastro de Memorando normal.

2.3.1.3 Enviar/alterar memorandos

Quais os memorandos são passíveis de alteração nesta funcionalidade?

Qual a diferença desta funcionalidade da apresentada na aba Rascunhos do Painel de Memorandos?

2.3.2 Leitura

2.3.2.1 Gerenciar Permissão de Leitura de Memorandos na Unidade

Verificar qual o objetivo desta funcionalidade e a necessidade dela na instituição.

Estas permissões seriam relativas a documentos sigilosos?

2.3.3 Movimentação

2.3.3.1 Encaminhar memorando

Consulta de memorandos recebidos

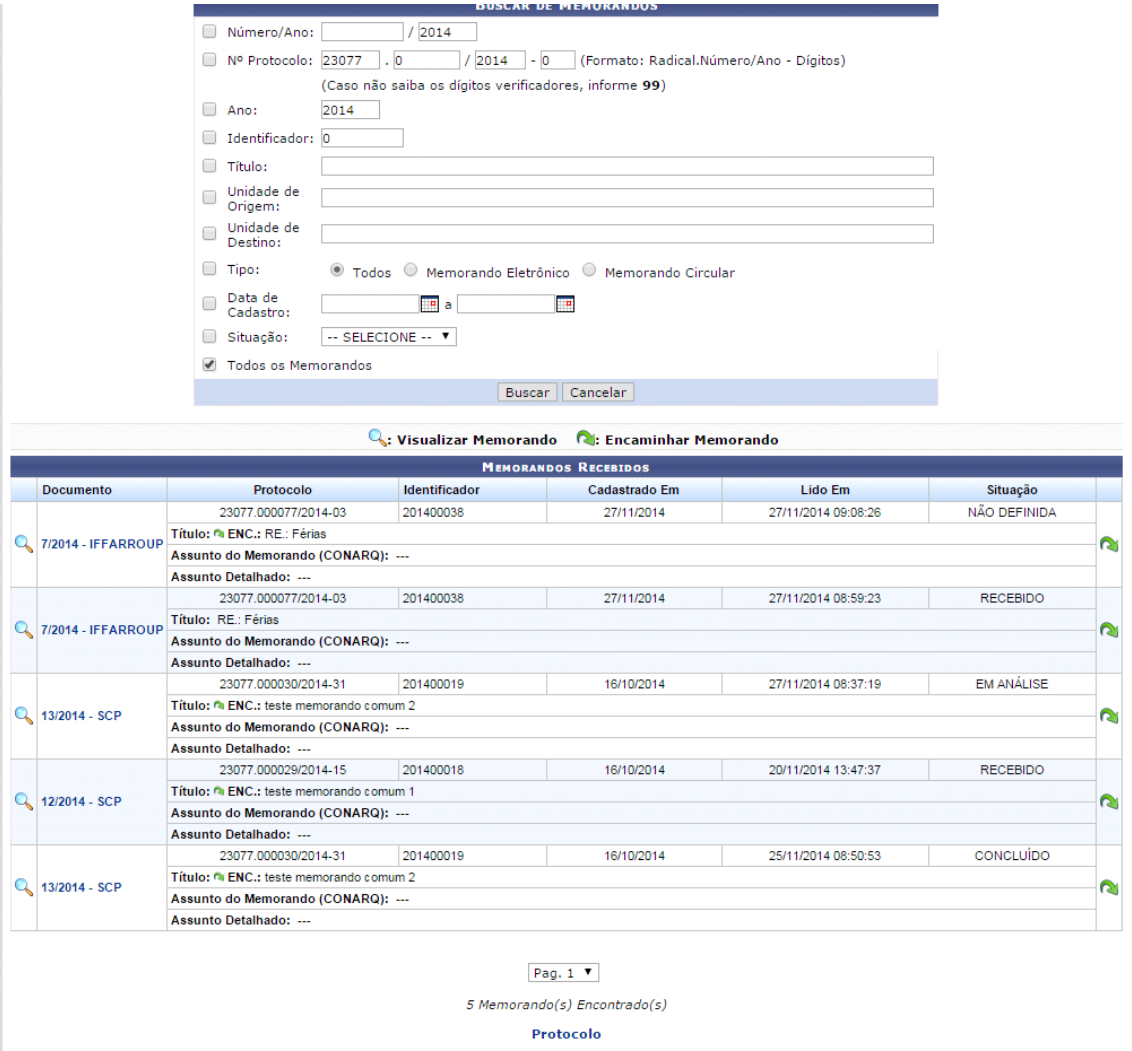

Figura 30 - Encaminhamento de memorandos

Serão mantidos registros de a quais unidades e servidores o memorando foi encaminhado, para que não ocorra reencaminhamentos desnecessários?

2.3.3.2 Cancelar encaminhamento

Verificar as situações em que um memorando pode ter encaminhamento cancelado.

Justificativa não obrigatória.

2.3.4 Autenticação

2.3.4.1 Autenticar memorandos

Alterar o termo “autenticar” por autorizar.

2.3.5 Consultas

Simplicar Consultas. Talvez manter apenas Painel de Memorandos, com todas as funcionalidades necessárias.

Verificar erro: permite encaminhar resposta a memorando circular.

Verificar erro: registro de movimentações não está registrando corretamente todas as movimentações.

Considerações gerais sobre Memorandos

A instituição deverá definir se continuará o uso de memorandos físicos ou se adotará completamente o uso de memorandos eletrônicos.

Verificar a anexação de documentos em formatos alteráveis.

Verificar a inserção de controle de versões.

Verificar a conformidade de dados. Há termos em que no cadastro do memorando tem uma definição e que no corpo do documento adquire outra configuração. Pode gerar confusão entre os usuários.

Alterar o termo “autenticar” por “autorizar” visto que a expressão utilizada não condiz com a operação realizada.

Retirar a opção de exportar memorando em versão final para formato .doc. Possíveis alterações.

Avaliar a inserção de autenticações digitais para a garantir a validade do documento e sua autenticidade.

Verificar a possibilidade de unificação de algumas telas para simplificar e facilitar o uso pelos servidores.

Modificar a formatação e estrutura do memorando para adequação às normas de redação oficial.

Verificar a adequação aos metadados obrigatórios de acordo com o e-ARQ Brasil.

2.4 Administração

2.4.1 Cadastro

2.4.1.1 Classificação CONARQ

Manter histórico de modificações do plano de classificação, como por exemplo, inserções de novas classes e subclasses, modificações de nomenclaturas de classes.

Qual o critério utilizado para definir a possibilidade de criação ou não de processos de acordo com a classificação.

Vincular a tabela de temporalidade com o plano de classificação.

2.4.1.2 Tipo de processo

Readequar a listagem.

Clara confusão entre espécies documentais, tipos documentais e assuntos.

Manual descreve como uma classificação por tema. Retirar esta descrição pois pode gerar confusão na utilização do usuário.

2.4.1.3 Graus de sigilo do processo

Inserir os prazos de acordo com a classificação do grau de sigilo.

2.4.1.4 Situação de ocorrência

Sem comentários.

2.4.1.5 Tipos de documento

Readequar a listagem.

2.4.1.6 Unidades para tramitação externa

Sem comentários.

2.4.1.7 Cadastrar órgão externo

Verificar quais os usuários terão permissão de cadastrar órgãos externos.

Estudar se não haverá morosidade na tramitação de processos e documentos caso apenas a Reitoria possa cadastrar as unidades externas.

Como será realizado o controle do trâmite externo de processos e documentos?

2.5 Consultas/Relatórios

Incluir consulta de processos de acordo com o prazo de guarda e fases do ciclo documental.

Incluir consulta de documentos e processos de acordo com o prazo de guarda de sigilo.

Retirar Consultas de Memorandos (mesma funcionalidade presente em Memorandos/Painel de Memorandos).

3 REQUISITOS OBRIGATÓRIOS

CÓDIGO	REQUISITO OBRIGATÓRIO	OBSERVAÇÃO	METADADO	DEFINIÇÃO
1	Organização dos documentos arquivísticos: Planos de Classificação e manutenção de documentos			
1.1	Configuração e Administração de Planos de Classificação de Documentos			
1.1.1	Incluir e ser compatível com o Plano de Classificação do IFF	O Plano de Classificação de Documentos deve ser aprovado pelo Arquivo Nacional, nos termos da legislação vigente.		
1.1.2	Garantir a criação de classes, subclasses, grupos e subgrupos nos níveis do acordo com o Plano de Classificação de acordo com o método de codificação adotado.	Ao se adotar o método decimal para codificação, cada classe poderá ter até no máximo dez subordinações e assim sucessivamente.		
1.1.3	Permitir a usuários autorizados acrescentar novas classes, subclasses, grupos e subgrupos que se fizer necessário			
1.1.4	Registrar a data da abertura de uma nova classe, subclasse, grupo e subgrupo no respectivo metadado		Registro de abertura	Registra informações: data\hora e responsável pela abertura
1.1.5	Registrar a mudança de nome de uma classe, subclasse, grupo e subgrupo já existente no respectivo metadado		Registro de mudança de nome de classe\subclasse\grupo\subgrupo	Registra informações: data\hora, responsável e nome anterior.

1.1.6	Permitir o deslocamento de uma classe inteira, incluindo as subclasses, grupos e subgrupos dos documentos ali classificados, para um outro ponto do Plano de Classificação	Nesse caso, é necessário fazer o registro do deslocamento nos metadados do Plano de Classificação	Registro de deslocamento de classe\subclasse\grupo\subgrupo (mudança de subordinação)	Registra informações: data\hora, responsável e subordinação anterior
1.1.7	Permitir que um usuário autorizado apague uma classe, subclasse, grupo e subgrupo inativa	Só pode ser apagada uma classe, subclasse, grupo e subgrupo que não tenha documentos ali classificados	Registro de extinção de classe, subclasse, grupo e subgrupo	Registra informações: Data\hora e responsável pela extinção

1.1.8	Permitir que um usuário autorizado inative uma classe, subclasse, grupo e subgrupo onde não serão mais classificados documentos, podendo reativá-las se necessário		Registro de desativação	Registra informações: data\hora e responsável pela desativação
			Registro de reativação	Registra informações: data\hora e responsável pela reativação
			Indicador de classe, subclasse, grupo e subgrupo ativa\inativa	Indica se a classe, subclasse, grupo ou subgrupo estão ativas ou inativas
1.1.9	Impedir a eliminação de uma classe, subclasse, grupo e subgrupo que tenham documentos classificados	Essa eliminação poderá ocorrer a partir do momento em que todos os documentos ali classificados tenham sido recolhidos ou eliminados, e seus metadados apagados ou que esses documentos tenham sido reclassificados		

1.1.10	Permitir a associação de metadados as classes, subclasses, grupos e subgrupos conforme estabelecido no padrão de metadados, e restringir a inclusão e alteração desses mesmos metadados somente a usuários autorizados			
1.1.11	Disponibilizar pelo menos dois mecanismos de atribuição de identificadores a classes, subclasses, grupos e subgrupos do Plano de Classificação, prevendo a possibilidade de se utilizar ambos, separadamente ou em conjunto, na mesma aplicação.			
1.1.11.1	Atribuição de um código numérico		Classificação – código	Registra a referência numérica que associa o documento a sua classe, subclasse, grupo ou subgrupo.
1.1.11.2	Atribuição de um termo que identifique cada classe, subclasse, grupo ou subgrupo		Classificação – nome	Refere-se a denominação da classe, subclasse, grupo ou subgrupo
1.1.12	Utilizar o termo completo para identificar uma classe ,subclasse,grupo ou subgrupo	Entende-se por termo completo toda a hierarquia referente aquela classe, subclasse, grupo ou subgrupo. Ex: MATERIAL: AQUISIÇÃO: MATERIAL PERMANENTE:		

		COMPRA		
1.1.13	Assegurar que os termos completos, que identificam cada classe, subclasse, grupo e subgrupo, sejam únicos no Plano de Classificação			
1.1.14	Prever um atributo associado às classes, subclasses, grupos e subgrupos para registrar a permissão de uso para classificar um documento	Em algumas classes, subclasses, grupos e subgrupos não são permitidos incluir documentos, nesses casos os documentos devem ser classificados apenas nos níveis subordinados		
1.1.14	Prover funcionalidades para elaboração de relatórios para apoiar a gestão dos Planos de Classificação, incluindo a capacidade de:			
1.1.14.1	Gerar relatório completo dos Planos de Classificação			
1.1.14.2	Gerar relatório parcial dos Planos de Classificação a partir de um ponto determinado na hierarquia			
1.1.14.3	Gerar relatório de documentos classificados em uma ou mais classes, subclasses, grupos e subgrupos dos Planos de Classificação			
1.1.14.4	Gerar relatório de documentos classificados por unidade administrativa			
1.2	Classificação e metadados dos			

	documentos			
1.2.1	Permitir a classificação de documentos somente nas classes, subclasses, grupos e subgrupos autorizados			
1.2.2	Permitir a classificação de um número ilimitado de documentos dentro de uma classe, subclasse, grupo e subgrupo			
1.2.3	Utilizar a classificação completa (classe, subclasse, grupo e subgrupo) para identificar um documento tal como especificado no item 1.1.12		Nome	Divisão de um plano ou código de classificação. Refere-se às classes, subclasses, grupos e subgrupos.
			Código	Divisão de um plano ou código de classificação, representado por números que mediante uma convenção representam a classe. Refere-se às classes, subclasses, grupos e subgrupos.
1.2.4	Permitir a associação de metadados aos documentos e restringir a inclusão e alteração desses mesmos metadados somente a usuários autorizados			
1.2.5	Associar os metadados dos documentos conforme estabelecido no padrão de metadados			

1.2.6	Permitir que sejam associados, automaticamente, a um novo documento determinados metadados pré-definidos	Exemplos dessa herança: temporalidade prevista e restrição de acesso		
1.2.7	Permitir a reclassificação por usuário autorizado de um documento e outros que o integram			
1.2.8	Permitir que na reclassificação de documentos sejam associados, automaticamente, aos outros documentos que o integram todos os seus metadados pré-definidos			
1.3	Gerenciamento de documentos			
1.3.1	Registrar nos metadados a data de produção ou recebimento e encerramento do documento	Esta data pode se constituir em parâmetro para aplicação dos prazos de guarda e destinação do documento	Registro de abertura	Registra informações: data:hora e responsável pela abertura
			Registro de encerramento	Registra informações: data\hora e responsável pelo encerramento
1.3.2	Permitir que um documento seja encerrado através de procedimentos regulamentares e somente por usuários autorizados			
1.3.3	Permitir a consulta aos documentos já encerrados por usuários autorizados			
1.3.4	Impedir o acréscimo de novos documentos a processos\dossiês já encerrados	Processos ou dossiês encerrados deverão ser reabertos para receber novos documentos		

1.3.5	Impedir a eliminação de uma unidade de arquivamento digital ou de qualquer parte de seu conteúdo em todas as ocasiões, a não ser nos prazos previstos na Tabela de Temporalidade de Documentos e nos casos de captura indevida de documento, efetuada por usuário autorizado	A eliminação será devidamente registrada em trilha de auditoria		
1.3.6	Garantir a integridade da relação hierárquica entre classe, subclasse, grupo, subgrupo, processo\dossiê, volume e documento em todos os momentos, independentemente de atividades de manutenção, ações do usuário ou falha de componente do sistema	Em hipótese alguma poderá ocorrer uma situação em que qualquer ação do usuário ou falha do sistema de origem a uma inconsistência na base de dados do Sistema		
1.4	Requisitos adicionais para o gerenciamento de documentos			
1.4.1	Prever a autuação de processos, por usuário autorizado, conforme estabelecido em legislação específica			
1.4.2	Prever que os documentos integrantes do processo digital recebam numeração seqüencial sem falhas, não se admitindo que documentos diferentes recebam a mesma numeração		Numeração de folhas de documentos	Numeração seqüencial das folhas de documentos inseridos em um processo.
1.4.3	Controlar a renumeração dos documentos integrantes de um processo digital	Este requisito tem por objetivo impedir a exclusão não autorizada de documentos de um processo. Casos especiais que autorizem a renumeração devem	Numeração de folhas de documentos	Numeração 64eqüencial das folhas de documentos inseridos em um processo.

		obedecer aos procedimentos oficiais		
1.4.4	Prever procedimentos para juntada\desentranhamento, anexação, apensamento\desapensamento e desmembramento de documentos aos dossiês ou processos, de acordo com os procedimentos oficiais	Este procedimento deverá ser registrado nos metadados do processo\dossiê. O apensamento é o ato de juntar um processo\dossiê a outro que com ele esteja relacionado, a pedido de uma das partes, em caráter temporário, permanecendo o processo\dossiê apensado fora do documento principal	Registro de apensamento	Registrar informações: data\hora do apensamento, responsável pelo apensamento, identificador do processo que foi apensado
		Este procedimento deverá ser registrado nos metadados do processo\dossiê. O desapensamento é o ato de separar fisicamente um ou mais processos\dossiês apensados	Registro de desapensamento	Registrar informações: data\hora do desapensamento, responsável pelo desapensamento, identificador do processo que foi desapensado

		Este procedimento deverá ser registrado nos metadados do processo\dossiê. O desentranhamento é o procedimento que consiste na retirada autorizada de um ou mais documentos juntados a um processo\dossiê.	Registro de desentranhamento	Registra informações: data\hora do desentranhamento, responsável pelo desentranhamento, identificador das peças que foram desentranhadas
		Este procedimento deverá ser registrado nos metadados do processo\dossiê. O desmembramento consiste na retirada autorizada de documentos de um processo\dossiê para a formação de um outro processo	Registro de desmembramento	Registrar informações: data\hora, responsável pelo desmembramento, registro dos documentos retirados, identificador do novo processo formado com os documentos retirados
		Este procedimento deverá ser registrado nos metadados do processo\dossiê. A anexação é o ato de juntar um processo\dossiê a outro que com ele esteja relacionado, a pedido de uma das partes, em caráter permanente, permanecendo o	Registro de anexação	Registra informações: data\hora da anexação, responsável pela anexação, identificador dos processos anexados

		processo\dossiê anexado dentro do documento principal		
		Este procedimento deverá ser registrado nos metadados do processo\dossiê. A juntada é o ato de inserir em um processo\dossiê, em caráter definitivo, outros documentos que dele farão parte integrante	Registro de juntada	Registra informações: data\hora da juntada, responsável pela juntada, identificador do documento que foi juntado
1.4.5	Prever o encerramento de documentos, incluindo seus volumes e metadados		Registro de encerramento	Registra informações: data\hora e responsável pelo encerramento
1.4.6	Prever o desarquivamento para reabertura de documentos por usuário autorizado, de acordo com os procedimentos oficiais	Para manter a integridade do documento, somente o último volume receberá novos documentos	Registro de reabertura	Registra informações: data\hora e responsável pela reabertura
1.5	Volumes: abertura, encerramento e metadados		Número do volume	Número 67eqüencial de registro atribuído aos volumes

1.5.1	Permitir que um volume herde automaticamente do processo\dossiê ao qual pertence, determinados metadados pré-definidos, como por exemplo, procedência, classificação e temporalidade			
1.5.2	Permitir a abertura de volumes a qualquer processo\dossiê que não esteja encerrado		Registro de abertura	Registra informações: data\hora e responsável pela abertura
1.5.3	Assegurar que um volume somente conterá documentos. Não é permitido que um volume contenha outro volume ou outro processo\dossiê			
1.5.4	Permitir que um volume seja encerrado através de procedimentos oficiais e somente por usuários autorizados		Registro de encerramento de volume	Registra informações: data\hora e responsável pelo encerramento de volume
1.5.5	Assegurar que, ao abrir um novo volume, o volume precedente seja automaticamente encerrado	Apenas o volume produzido mais recentemente poderá estar aberto, todos os outros volumes existentes no processo\dossiê têm que estar fechados		
1.5.6	Impedir a rearbetura de um volume já encerrado para acréscimo de documentos			
1.6	Gerenciamento de documentos arquivísticos convencionais, digitais e híbridos			

1.6.1	Capturar documentos arquivísticos convencionais, digitais e híbridos e gerenciá-los com base nos mesmos Planos de Classificação e Tabelas de Temporalidade de Documentos		Tipo de suporte	1. Indicar se o documento é digital, convencional ou híbrido. 2. Especificar o material sobre o qual as informações são registradas: papel, filme, fita magnética, disco magnético, disco ótico, meio digital
1.6.2	Gerenciar a parte convencional e a parte digital integrantes de documentos híbridos, associando as com o mesmo número identificador atribuído pelo sistema, além de indicar que se trata de um documento arquivístico híbrido		Identificador único	Registra o código gerado automaticamente que identifica o processo, dossiê ou o documento de maneira a distingui-los dos demais
			Tipo de suporte	1. Indicar se o documento é digital, convencional ou híbrido. 2. Especificar o material sobre o qual as informações são registradas: papel, filme, fita magnética, disco magnético, disco ótico, meio digital

1.6.3	Permitir a configuração de um conjunto específico de metadados para os documentos convencionais e a inclusão de informações sobre o local de arquivamento		Localização	Registra o local de armazenamento atual do documento. Pode ser um lugar (depósito, estante, repositório digital), uma notação física ou um link
1.6.4	Ter mecanismos para acompanhar a tramitação do documento arquivístico convencional, digital ou hibrído, de forma que se evidencie ao usuário a localização atual do documento		Registro de tramitação	Registra informações: identificação do documento, data\hora de transmissão, remetente, data\hora do recebimento, destinatário, situação do trâmite
1.6.5	Ser capaz de oferecer ao usuário funcionalidades para solicitar ou reservar a consulta a um documento arquivístico convencional, enviado uma mensagem para o detentor atual desse documento ou para o Administrador			
1.6.6	Assegurar que a recuperação de um documento híbrido permita igualmente a recuperação dos metadados tanto da parte digital como da parte convencional			
1.6.7	Sempre que os documentos híbridos estiverem classificados quanto ao seu grau de sigilo, garantir que a parte convencional e a parte digital correspondente recebam a mesma classificação de sigilo			

1.6.8	Registrar na trilha de auditoria todas as alterações efetuadas nos metadados dos documentos convencionais e híbridos			
2	Tramitação e fluxo de trabalho			
2.1	Controle do fluxo de trabalho			
2.1.1	Um recurso de fluxo de trabalho tem que fornecer os passos necessários para o cumprimento de trâmites preestabelecidos ou ad hoc. Nesse caso, cada passo significa o deslocamento de um documento, de um agente para outro, a fim de registrar uma manifestação ou decisão		Registro de tramitação	Registra informações: identificação do documento, data\hora de transmissão, remetente, data\hora do recebimento, destinatário, situação do trâmite
2.1.2	Ter capacidade, sem limitações, de estabelecer o número necessário de trâmites nos fluxos de trabalho			
2.1.3	Disponibilizar uma função para avisar a um agente que participe do fluxo que um documento lhe foi enviado, especificando a ação necessária			
2.1.4	Permitir que fluxos de trabalho pré-programados sejam definidos, alterados e mantidos exclusivamente por usuário autorizado			
2.1.5	Registrar na trilha de auditoria todas as alterações ocorridas nesse fluxo			
2.1.6	Registrar a tramitação dos documentos a fim de que os usuários possam conhecer a situação de cada documento no processo		Registro de tramitação	Registra informações: identificação do documento, data\hora de transmissão, remetente, data\hora do

				recebimento, destinatário, situação do trâmite
2.1.7	Fornecer um histórico da tramitação dos documentos	O histórico de tramitação corresponde a um conjunto de metadados de datas de entrada e saída; nomes de responsáveis; providências, etc	Registro de tramitação	Registra informações: identificação do documento, data\hora de transmissão, remetente, data\hora do recebimento, destinatário, situação do trâmite
2.1.8	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 é recebido			
2.1.9	Reconhecer indivíduos e grupos de trabalho como participantes			
2.1.10	Fornecer meios de elaboração de relatórios técnicos completos para permitir que gestores monitorem a tramitação dos documentos e o desempenho dos participantes			
2.1.11	Registrar a tramitação de um documento em seus metadados. Os metadados referentes a tramitação devem registrar data e hora de envio e de recebimento e identificação do usuário			
2.2	Controle de versões e forma do			

	documento			
2.2.1	Registrar a forma de transmissão do documento, ou seja, se é minuta, original ou cópia.		Forma	Registra o estágio de preparação e transmissão de documentos: original (primeiro documento completo e efetivo), cópia (resultado da reprodução de um documento), minuta ou rascunho (versão preliminar do documento)
2.2.2	Controlar as diversas versões de um documento que está sendo tramitado		Versão	Uma ou mais variantes de um mesmo documento. Registra informações: Identificador da versão, descrição de alterações, data\hora da produção da versão
2.2.3	Associar e relacionar as diversas versões de um documento			
2.2.4	Manter o identificador único do documento, e o controle de versões deve ser registrado em metadados específicos			
3	Captura		Domínio	Origem do registro do documento. Instituição legitimamente responsável pela captura, autuação ou

				registro do documento
3.1	Captura: procedimentos gerais			

3.1.1	A captura tem que garantir a execução das seguintes funções:		Número de protocolo	Número sequencial automático de registro no Sistema, atribuído ao documento no ato do protocolo
			Número do documento	Número atribuído ao documento no ato de sua criação. Corresponde à sigla do órgão produtor, número atribuído e data da produção
			Número do processo\dossiê	Número sequencial atribuído ao processo\dossiê (por ano)
			Registro de captura	Registra informações: identificação do documento, data\hora da captura, responsável pela captura
3.1.1.1	Registrar e gerenciar todos os documentos convencionais			
3.1.1.2	Registrar e gerenciar todos os documentos digitais e híbridos, independente do			

	contexto tecnológico			
3.1.1.3	Classificar todos os documentos de acordo com os Planos de Classificação		Classificação - código	Registra a referência numérica que associa o documento ao seu contexto de produção, composta das seguintes unidades de informação: classe, subclasse, grupo e subgrupo
3.1.1.4	Controlar e validar a introdução de metadados			
3.1.2	Capturar documentos digitais das seguintes formas:			
3.1.2.1	Captura de documentos produzidos dentro do Sistema			
3.1.2.2	Captura de documento individual produzido em arquivo digital fora do Sistema, inclusive mensagens de correio eletrônico			
3.1.2.3	Captura de documento individual produzido em workflow ou outros sistemas integrados ao Sistema			
3.1.2.4	Captura de documentos em lote			
3.1.3	Aceitar o conteúdo do documento, bem como as informações que definem sua aparência, mantendo as associações entre as várias informações digitais relacionadas ao documento, isto é, anexos e links de hipertexto			

3.1.4	Permitir a inserção de todos os metados, obrigatórios e altamente desejáveis, definidos na sua configuração e garantir que se mantenham associados ao documento:			
3.1.4.1	Nome do arquivo digital		Nome do arquivo digital	Corresponde à denominação padronizada das séries documentais.
3.1.4.2	Número identificador atribuído pelo Sistema		Identificador único	Registra o código gerado automaticamente que identifica o processo, dossiê ou o documento de maneira a distingui-los dos demais
3.1.4.3	Data de produção ou recebimento		Data de produção	Registro cronológico (data e hora) e tópico (local) da produção do documento
3.1.4.4	Data e hora de transmissão e recebimento			
3.1.4.5	Data e hora da captura			
3.1.4.6	Descrição abreviada		Descrição	Correponde ao assunto. Trata-se de um resumo abreviado do conteúdo do documento, elaborado com o uso de vocabulário controlado. Diferente do já estabelecido no código de classificação

3.1.4.7	Classificação de acordo com os Planos de Classificação		Classificação - código	Registra a referência numérica que associa o documento ao seu contexto de produção, composta das seguintes unidades de informação: classe, subclasse, grupo e subgrupo
3.1.4.8	Prazos de guarda			
3.1.4.9	Autor (pessoa física ou jurídica)		Autor	Indica a pessoa física ou jurídica que tem autoridade e competência para emitir o documento ou em cujo nome ou sob cujo comando o documento foi emitido
3.1.4.10	Redator (se diferente do autor)		Redator	Indica o responsável pela elaboração do documento
3.1.4.11	Originador		Originador	Indica a pessoa a quem pertence o endereço eletrônico ou a conta de login onde o documento é gerado ou enviado
3.1.4.12	Destinatário (com seu cargo)		Destinatário	Indica a pessoa física ou jurídica a quem o documento é dirigido

3.1.4.13	Nome do setor responsável pela execução contida no documento		Unidade produtora de documentos	Indica o órgão ou setor que produziu o documento no exercício de suas funções e atividades. O documento permanece na Unidade Produtora cumprindo seu prazo de vigência, ou seja, durante o tempo necessário para que produza efeitos administrativos e legais plenos, cumprindo a finalidade que determinou sua produção
3.1.4.14	Indicação de anotação		Indicação de anotação	Registra se foi feita anotação no documento
3.1.4.15	Indicação de anexos			

3.1.4.16	Restrição de acesso		Níveis de acesso	Indica os níveis de acesso segundo a classificação da informação quanto à categoria e ao grau de sigilo e restrição de acesso

			Registro de classificação de sigilo	Registra informações: data\hora e responsável pela classificação de categoria e grau de sigilo
			Registro de desclassificação de sigilo	Registra informações: data\hora e responsável pela desclassificação de categoria e grau de sigilo
3.1.4.17	Registro das migrações e data em que ocorrem			
3.1.4.18	Espécie\tipo\genêro documental		Espécie	Registra a configuração que assume um documento de acordo com a disposição e a natureza das informações nele contidas. Ex: processo, ata, relatório, projeto
			Gênero	Registra a configuração que assume um documento de acordo com o sistema de signos utilizado na comunicação de seu conteúdo. Ex.: audiovisual, textual, cartográfico, iconográfico

			Tipo documental	Refere-se a configuração que assume uma espécie documental de acordo com a atividade que a gerou. Ex.: processo de adiantamento, ata de reunião, relatório de atividades

3.1.4.19	Indicação de versão		Versão	Uma ou mais variantes de um mesmo documento. Registra informações: identificador da versão, descrição de alterações, data\hora da produção da versão
3.1.4.20	Associações a documentos diferentes que possam estar relacionados pelo fato de registrarem a mesma atividade ou se referirem a mesma pessoa ou situação		Relação com outros documentos	Registro de relações significantes do documento com outros pelo fato de registrarem a mesma atividade, pessoa ou situação ou diferentes níveis de agregação (processo\dossiê, volume e documento) ou diferentes manifestações do mesmo documento em

				diversos formatos
3.1.4.21	Formato e software (nome e versão) sob o qual o documento foi produzido ou no qual foi capturado		Contexto tecnológico	Registra o ambiente tecnológico (hardware, software e padrões) que envolve o documento
3.1.4.22	Máscaras de formatação (template) necessárias para interpretar a estrutura do documento			
3.1.4.23	Descritores (diferentes dos já estabelecidos nos Planos de Classificação):			
3.1.4.24	Localização física		Localização	Registra o local de armazenamento atual do documento. Pode ser um lugar (depósito, estante, repositório digital), uma notação física ou um link
3.1.4.25	Idioma		Idioma	Registra o idioma em que é expresso o conteúdo do documento
3.1.4.26	Quantidade de folhas\páginas		Quantidade de folhas\páginas	Registra a quantidade de folhas\páginas do

				documento
3.1.4.27	Outros que se julgarem necessários			
3.1.5	Prever a inservação dos metadados obrigatórios, previstos em procedimentos oficiais, no momento da captura de documentos			
3.1.6	Atribuir um número identificador para cada documento, que serve para identificá-lo desde o momento da captura até sua destinação final dentro do sistema			
3.1.7	O formato do número identificador atribuído pelo Sistema deve ser definido no momento da configuração do Sistema	O identificador deve ser único e seqüencial e pode ser numérico ou alfanumérico		
3.1.8	O número identificador atribuído pelo Sistema tem que:		Identificador único	Registra o código gerado automaticamente que identifica o processo, dossiê ou o documento de maneira a distingui-los dos demais
3.1.8.1	Ser gerado automaticamente, sendo vedado sua introdução manual e alteração posterior; ou			

3.1.8.2	Ser atribuído pelo usuário e validado pelo Sistema antes de ser aceito	Uma opção seria gerar o número identificador automaticamente, mas nesse caso, ocultá-lo do usuário, permitindo a este introduzir uma sequência não necessariamente única como um "identificador". O usuário empregaria essa sequência como um identificador, mas o Sistema a consideraria como metadado pesquisável, definido pelo usuário		

3.1.9	Prever a adoção da numeração única de documentos de acordo com a legislação específica a fim de garantir a integridade do número atribuído ao documento na unidade de protocolo de origem		Número de identificação de protocolo	Registra a referência numérica que associa o documento ao seu contexto de produção, composta da informação do órgão produtor
			Identificador único	Registra o código gerado automaticamente que identifica o processo, dossiê ou o documento

				de maneira a distingui-los dos demais
			Indicação de anexos	Indica se o documento tem anexos
			Interessado	Registra o nome e\ou identificação da pessoa física ou jurídica cujo conteúdo do documento lhe interessa diretamente
			Procedência	Registra a instituição que originou o documento
			Relação com outros documentos	Registro de relações significantes do documento com outros pelo fato de registrarem a mesma atividade, pessoa ou situação ou diferentes níveis de agregação (processo\dossiê, volume e documento) ou diferentes manifestações do mesmo documento em diversos formatos

3.1.10	Garantir que os metadados associados a um documento sejam inseridos somente por usuários autorizados			
3.1.11	Garantir que os metadados associados a um documento sejam alterados somente por administradores e usuários autorizados e devidamente registrados em trilhas de auditoria			
3.1.12	Garantir a visualização do registro de entrada do documento dentro do Sistema com todos os metadados inseridos automaticamente e os demais a serem atribuídos pelo usuário	Exemplo: o Sistema pode atribuir, automaticamente, o número identificador, a data de captura, o originador e requerer que o usuário preencha os demais metadados		
3.1.13	Garantir a inserção de outros metadados após a captura	Exemplo: data e hora de alteração e mudança de suporte		
3.1.14	Sempre que um documento digital tiver mais de uma versão, o Sistema tem que permitir que os usuários selecionem pelo menos uma das seguintes ações:			
3.1.14.1	Registrar todas as versões do documento como um só documento arquivístico			
3.1.14.2	Registrar uma única versão do documento como um documento arquivístico			
3.1.14.3	Registrar cada uma das versões do documento, separadamente, como um documento arquivístico			

3.1.15	Em relação aos documentos digitais que mantém associações com outras informações digitais, o Sistema tem que:			
3.1.15.1	Tratar o documento como uma unidade indivisível, assegurando a relação entre as informações digitais			
3.1.15.2	Preservar a integridade do documento, mantendo a relação entre as informações digitais			
3.1.15.3	Garantir a integridade do documento quando da recuperação, visualização e gestão posteriores			
3.1.15.4	Gerenciar a destinação de todas as informações digitais que compõem o documento como uma unidade indivisível			
3.1.16	Emitir um aviso caso o usuário tente registrar um documento que já tenha sido registrado no mesmo processo\dossiê			
3.2	Captura em lote		Data de produção	Registro cronológico (data e hora) e tópico (local) da produção do documento
3.2.1	Proporcionar a captura em lote de documentos gerados por outros Sistemas. Esse procedimento tem que:			

3.2.1.1	Permitir importação de transações pré-definidas de arquivos em lote	Exemplos de lote de documento podem ser: mensagens de correio eletrônico, correspondência digitalizada por meio de scanner, documentos provenientes de um departamento, de um grupo ou indivíduo, transações de aplicações de um computador ou ainda documentos oriundos de um sistema de gestão de documentos		
3.2.1.2	Registrar, automaticamente, cada um dos documentos importados contidos no lote			
3.2.1.3	Permitir e controlar a edição do registro de documentos importados			
3.2.1.4	Validar a integridade dos metadados			
3.3	Captura de mensagens de correio eletrônico			
3.3.1	Permitir que, na fase de configuração, se opte por uma das seguintes operações:		Data da produção	Registro cronológico (data e hora) e tópico (local) da produção do documento
3.3.1.1	Capturar mensagens de correio eletrônico após selecionar quais serão objeto de registro; ou			
3.3.1.2	Capturar automaticamente todas as mensagens de correio eletrônico			

3.4	Captura de documentos convencionais ou hibrídos		Relação com outros documentos	Registro de relações significantes do documento com outros pelo fato de registrarem a mesma atividade, pessoa ou situação ou diferentes níveis de agregação (processo\dossiê, volume e documento) ou diferentes manifestações do mesmo documento em diversos formatos
			Tipo de suporte	1. Indicar se o documento é digital, convencional ou híbrido. 2. Especificar o material sobre o qual as informações são registradas: papel, filme, fita magnética, disco óptico, meio digital
3.4.1	Capturar também os documentos convencionais e\ou híbridos			
3.4.2	Acrescentar aos metadados dos documentos convencionais informações sobre a sua localização	Essa informação só será acessada por usuários autorizados	Localização	Registra o local de armazenamento atual do documento. Pode ser um lugar (depósito, estante, repositório

				digital), uma notação física ou um link
3.5	Formato de arquivo e estrutura dos documentos a serem capturados			
3.5.1	Possuir a capacidade de capturar documentos de diferentes formatos de arquivo e estruturas			
3.5.2	Capturar documentos que se apresentam com as seguintes estruturas:			
3.5.2.1	Simples: texto, imagens, mensagens de correio eletrônico, slides digitais, som			
3.5.2.2	Composta: mensagens de correio eletrônico com anexos, páginas web, publicações eletrônicas, bases de dados			
3.5.3	Incluir novos formatos e arquivos à medida que forem sendo adotados pelo órgão ou entidade			
3.6	Estrutura dos procedimentos de gestão			
3.6.1	Reconhecer três domínios para o controle dos procedimentos de gestão: espaço individual, espaço de grupo e espaço geral			
3.6.2	Operacionalizar as regras estabelecidas pelo Sistema de gestão arquivística de documentos nos três espaços			
3.6.3	Impedir que o conteúdo de um documento seja alterado por usuários e Administradores, exceto nos casos em que a alteração fizer parte do processo			

	documental			
4	Avaliação e destinação			
4.1	Configuração da Tabela de Temporalidade de Documentos			
4.1.1	Prever funcionalidades para definição e manutenção de Tabela de Temporalidade de Documentos, associada ao Plano de Classificação do IFF			
4.1.2	Associar, automaticamente, ao documento o prazo e a destinação previstos na série na qual foi classificado			
4.1.3	Manter Tabelas de Temporalidade de Documentos com as seguintes informações:	As Tabelas de Temporalidade de Documentos do IFF deverão ser aprovadas pelo Arquivo Nacional, em conformidade com a legislação vigente		

4.1.3.1	Identificador da classe, subclasse, grupo e subgrupo		Classificação - código	Divisão de um plano ou código de classificação, representado por números que mediante uma convenção representam a classe. Refere-se às classes, subclasses, grupos e

				subgrupos.
			Classificação - nome	Divisão de um plano ou código de classificação. Refere-se às classes, subclasses, grupos e subgrupos.
4.1.3.2	Prazo de guarda na unidade produtora		Prazo de guarda na unidade produtora	Refere-se ao tempo em que o documento deverá permanecer no arquivo corrente do órgão, cumprindo a finalidade para a qual foi produzido. (Fase corrente)
4.1.3.3	Prazo de guarda na unidade com atribuições de arquivo		Prazo de guarda na unidade com atribuições de arquivo	Refere-se ao tempo em que o documento deve permanecer no arquivo intermediário para eventuais consultas, em decorrência do cumprimento de prazos prescricionais ou precaucionais. (Fase intermediária)

4.1.3.4	Destinação final		Destinação	Registra a decisão decorrente da avaliação documental, que determina o seu encaminhamento para eliminação ou guarda permanente, de acordo com a tabela de temporalidade
4.1.3.5	Observações		Observações	Registra informações: atos legais e razões de natureza administrativa que fundamentaram a indicação dos prazos propostos ou ainda informações relevantes sobre a produção, guarda ou conteúdo do documento
4.1.3.6	Evento que deflagra a contagem do prazo de retenção do documento na unidade produtora ou na unidade com atribuições de arquivo		Evento deflagrador de contagem de tempo	Evento que autoriza o início dos prazos prescricionais ou precaucionais, previstos nas Tabelas de Temporalidade de Documentos. Ex: aprovação das contas pelo TCE; término das fases recursal e executória

4.1.4	Prever ao menos as seguintes situações para destinação:			
4.1.4.1	Apresentação dos documentos para reavaliação em data futura			
4.1.4.2	Eliminação			
4.1.4.3	Exportação para transferência			
4.1.4.4	Exportação para recolhimento (guarda permanente)			
4.1.5	Prever a iniciação automática da contagem dos prazos de guarda referenciados nas Tabelas de Temporalidade de Documentos, a partir de pelo menos os seguintes eventos:	Acontecimentos específicos descritos na Tabela de Temporalidade como, por exemplo, "5 anos a contar da data da aprovação das contas" ou "vigência", quando não puderem ser detectados automaticamente, deverão ser informados ao Sistema por usuário autorizado		
4.1.5.1	Produção			
4.1.5.2	Arquivamento			
4.1.5.3	Desarquivamento			
4.1.5.4	Inclusão de novos documentos			
4.1.6	Prever que a definição dos prazos de guarda seja expressa por um número inteiro de anos			

4.1.7	Limitar a definição e a manutenção (alteração, inclusão e exclusão) das Tabelas de Temporalidade de Documentos a usuários autorizados		Registro de alteração	Registra informações: data\hora da alteração, responsável pela alteração, identificador da série que teve prazo ou destinação alterada, descrição da alteração (incluindo o prazo\destinação anterior)
4.1.8	Permitir que o usuário autorizado altere o prazo ou destinação prevista em um item da Tabela de Temporalidade de Documentos e garantir que a alteração tenha efeito em todos os documentos pertecentes a mesma série documental	As alterações na Tabela de Temporalidade de Documentos só poderão ser feitas como resultado de um processo de reavaliação realizado pela CPAD, em virtude de mudança do contexto administrativo, jurídico ou cultural. As propostas de alterações na Tabela de Temporalidade de Documentos deverão ser aprovados pelo Arquivo Nacional, em conformidade com a legislação vigente	Registro de alteração	Registra informações: data\hora da alteração, responsável pela alteração, identificador da série que teve prazo ou destinação alterada, descrição da alteração (incluindo o prazo\destinação anterior)
4.1.9	Prover funcionalidades para elaboração de relatórios que apóiem a gestão da Tabela de Temporalidade de Documentos, incluindo a capacidade de:			

4.1.9.1	Gerar relatório completo das Tabelas de Temporalidade de Documentos			
4.1.9.2	Gerar relatório parcial das Tabelas de Temporalidade de Documentos a partir de um ponto determinado na hierarquia dos Planos de Classificação			
4.1.9.3	Gerar relatório dos documentos aos quais está atribuído um determinado prazo de guarda			
4.1.9.4	Identificar eventuais inconsistências existentes entre as Tabelas de Temporalidade de Documentos e os Planos de Classificação			
4.2	Aplicação da Tabela de Temporalidade de Documentos			
4.2.1	Fornecer recursos integrados à Tabela de Temporalidade de Documentos para implementar as ações de destinação			
4.2.2	Para cada documento, o Sistema deverá acompanhar automaticamente os prazos de guarda determinados para a série a qual pertence			
4.2.3	Prover funcionalidades para informar ao usuário autorizado sobre os documentos que já cumpriram ou estão para cumprir o prazo de guarda previsto			

4.2.4	Prover funcionalidades para gerenciar o processo de destinação, que deve ser iniciado por usuário autorizado e cumprir os seguintes passos:		Destinação	Registra a decisão decorrente da avaliação documental, que determina o seu encaminhamento para eliminação ou guarda permanente, de acordo com a tabela de temporalidade
			Prazo de guarda	Registra o tempo de permanência dos documentos na unidade produtora e na unidade com atribuições de arquivo, de acordo com a tabela de temporalidade
4.2.4.1	Identificar, automaticamente, os documentos que cumpriram os prazos de guarda previstos na Tabela de Temporalidade			
4.2.4.2	Informar ao usuário autorizado sobre todos os documentos que foram identificados no passo anterior			
4.2.4.3	Possibilitar a alteração do prazo ou destinação previstos para aqueles documentos, caso necessário			
4.2.4.4	Proceder a ação de destinação quando confirmado por usuário autorizado			
4.2.5	Pedir confirmação antes de realizar as ações de destinação			

4.2.6	Restringir as funções de destinação a usuários autorizados			
4.2.7	Quando um Administrador transfere documentos de uma série para outra, em virtude de uma reclassificação, o Sistema deverá adotar, automaticamente, a temporalidade e a destinação da nova série			
4.2.8	Quando um documento digital (objeto digital) estiver associado a mais de um processo ou dossiê, e tiver prazos de guarda diferentes associados a ele, o Sistema tem que, automaticamente, verificar todos os prazos de guarda e destinação previstos para esse documento e garantir que o mesmo seja mantido em cada processo\dossiê pelo tempo definido na tabela de temporalidade de documentos, de forma que:	Quando um documento digital estiver associado a mais de um processo ou dossiê, o Sistema deverá criar um registro para cada referência desse documento. Cada registro estará vinculado ao mesmo documento digital. No momento da eliminação, o documento digital não poderá ser eliminado sem antes se verificar a temporalidade de todas as referências associadas a ele. O documento digital só poderá ser eliminado quando os prazos de guarda de todas as referências tiverem sido cumpridos. Antes disso, só se pode fazer a eliminação de cada registro		

		invidualmente		
4.2.8.1	A remoção de um documento de um processo\dossiê não prejudique a manutenção desse mesmo documento em outro processo\dossiê, até que todas as referências desse documento tenham atingido o prazo de guarda previsto			
4.2.8.2	A manutenção de um documento em um processo\dossiê de prazo de guarda mais longo não obrigue a permanência desse mesmo documento em outro processo\dossiê de prazo de guarda mais curto. Nesse caso, o registro do documento de prazo de guarda mais curto tem que ser removido, mas o documento é mantido no Sistema			

4.3	Exportação de documentos			
4.3.1	Permitir exportar documentos digitais e seus metadados para outro Sistema dentro ou fora do IFF			
4.3.2	Quando o Sistema exportar os documentos de uma série para executar uma ação de transferência ou recolhimento, tem que ser capaz de exportar todos os documentos da mesma série incluídos na ação de destinação, com seus respectivos volumes, documentos e metadados associados			
4.3.3	Exportar um documento ou grupo de documentos numa sequência de operações , de modo que:			
4.3.3.1	O conteúdo, o contexto e a estrutura dos seus documentos não se degradem			
4.3.3.2	Todos os componentes de um documento digital sejam exportados como uma unidade. Por exemplo, uma mensagem de correio eletrônico e seus respctivos anexos			
4.3.3.3	Todos os metadados do documento sejam relacionados a ele de forma que as ligações possam ser mantidas no novo Sistema			
4.3.3.4	Todas as ligações entre documentos e volumes sejam mantidas			
4.3.4	Exportar todos os tipos de documentos que está apto a capturar			

4.3.5	Produzir um relatório detalhado sobre qualquer falha que ocorra durante uma exportação. O relatório tem que identificar os documentos que tenham originado erros de processamento ou cuja exportação não tenha sido bem sucedida			
4.3.6	Conservar todos os documentos digitais que tiverem sido exportados, pelo menos até que tenham sido importados no Sistema destinatário com êxito			
4.3.7	Manter metadados relativos a documentos que foram exportados	O Administrador deve indicar o subconjunto de metadados que deverá ser mantido		
4.3.8	Gerar listagem em meio digital em papel para descrever documentos digitais que estão sendo exportados	Este requisito se aplica principalmente nos casos em que é feita exportação para transferência ou recolhimento para o Arquivo Nacional. Nesse caso, a listagem deverá ser produzida no formato estabelecido pelo Arquivo Nacional		
4.4	Eliminação		Registro de eliminação	Registra informações: data\hora da eliminação, responsável pela eliminação, número da relação de eliminação, do edital e do termo de eliminação

4.4.1	Restringir a função de eliminação de documentos somente a usuários autorizados			
4.4.2	Pedir confirmação da eliminação a um usuário autorizado antes que qualquer ação seja tomada com relação ao documento e cancelar o processo de eliminação se a confirmação não for dada			
4.4.3	Avisar ao usuário autorizado quando um documento em vias de ser eliminado se encontrar relacionado a outro; o Sistema também tem de suspender o processo até que seja tomada uma das medidas abaixo:			
4.4.3.1	Confirmação pelo usuário autorizado para prosseguir ou cancelar o processo			
4.4.3.2	Produção de um relatório especificando os documentos envolvidos e todas as ligações com outros documentos			
4.4.4	Quando um documento tem várias referências armazenadas, o Sistema tem que garantir que todas essas referências sejam verificadas antes de se proceder a eliminação do documento digital			
4.4.5	Produzir um relatório detalhando qualquer falha que ocorra durante uma eliminação. O relatório tem que identificar os documentos cuja eliminação não tenha sido bem sucedida			

4.4.6	Gerar relatórios com os documentos que serão eliminados	Um relatório deverá seguir o modelo da Listagem de Eliminação de Documentos, conforme establecido na legislação vigente, e o outro deverá seguir o modelo do Edital de Ciência de Eliminação de Documentos, conforme legislação vigente.		
4.4.7	Manter metadados relativos aos documentos que foram eliminados. O Administrador deve indicar o subconjunto de metadados que deverá ser mantido	O Sistema deverá gerar o Termo de Eliminação de Documentos, conforme legislação vigente	Registro da eliminação	Registra informações: data\hora da eliminação, responsável pela eliminação, número da relação de eliminação, do edital e do termo de eliminação
4.5	Avaliação de documentos arquivísticos convencionais, digitais e híbridos			
4.5.1	Aplicar as mesmas Tabelas de Temporalidade de Documentos para os documentos convencionais, digitais ou híbridos			
4.5.2	Acompanhar os prazos de guarda dos documentos convencionais e dar início aos procedimentos de eliminação ou transferência desses documentos, tomando em consideração suas especificidades			

4.5.3	Alertar o Administrador sobre a existência e localização de uma parte convencional associada a um documento híbrido que esteja destinado a ser exportado, transferido ou eliminado			
5	Pesquisa, localização e apresentação de documentos			
5.1	Fornecer facilidades para pesquisa, localização e apresentação de documentos			
5.2	Pesquisa e localização			
5.2.1	Fornecer uma série flexível de funções que atuem sobre os metadados relacionados com os diversos níveis de agregação (documento, classe, subclasse, grupo e subgrupo) e sobre os conteúdos dos documentos arquivísticos por meio de parâmetros definidos pelo usuário, com o objetivo de localizar e acessar os documentos e\ou metadados, quer individualmente, quer reunidos em grupo			
5.2.2	Executar pesquisa de forma integrada, isto é, apresentar todos os documentos, sejam eles digitais, híbridos ou convencionais, que satisfaçam aos parâmetros da pesquisa			
5.2.3	Permitir que todos os metadados de gestão de um documento possam ser pesquisados			
5.2.4	Permitir que um documento possa ser recuperado por meio de um número identificador			

5.2.5	Permitir que um documento possa ser recuperado por meio de todas as formas de identificação implementadas, incluindo no mínimo:			
5.2.5.1	Identificador		Identificador único	Registra o código gerado automaticamente que identifica o processo, o dossiê ou o documento de maneira a distingui-los dos demais
5.2.5.2	Descritor		Descritor	Palavra, expressão ou símbolo convencionado para expressar o conteúdo do documento. Diferente do já estabelecido no código de classificação
5.2.5.3	Datas			
5.2.5.4	Procedência\interessado		Interessado	Registra o nome e\ou identificação da pessoa física ou jurídica cujo conteúdo do documento lhe interessa diretamente
			Procedência	Registra a instituição que originou o documento

5.2.5.5	Autor\redator\originador		Autor	Indica a pessoa física ou jurídica que tem autoridade e competência para emitir o documento ou em cujo nome ou sob cujo comando o documento foi emitido
			Redator	Indica o responsável pela elaboração do documento
			Originador	Indica a pessoa a quem pertence o endereço eletrônico ou a conta de login onde o documento é gerado ou enviado

5.2.5.6	Classificação de acordo com os Planos de Classificação		Código	Divisão de um plano ou código de classificação, representado por números que mediante uma convenção representam a classe. Refere-se às classes, subclasses, grupos e subgrupos.
			Nome	Divisão de um plano ou código de classificação. Refere-se às classes, subclasses, grupos e

				subgrupos.
5.2.6	Permitir a pesquisa e recuperação de um processo\dossiê completo e exibir a lista de todos os documentos que os integram, como uma unidade, em um único processo de recuperação			
5.2.7	Restringir o acesso a qualquer informação (metadado ou conteúdo do documento arquivístico) nos casos em que restrições de acesso e questões de segurança assim o exigirem, nos termos da lei		Níveis de acesso	Indica os níveis de acesso segundo a classificação da informação qaunto a categoria e ao grau de sigilo e restrição de acesso
			Registro de classificação de sigilo	Registra informações: data\hora e responsável pela classificação de categoria e grau de sigilo
			Registro de desclassificação de sigilo	Registra informações: data\hora e responsável pela desclassificação de categoria e grau de sigilo
5.3	Apresentação: visualização, impressão e emissão de som		Contexto tecnológico	Registra o ambiente tecnológico (hardware, software e padrões) que envolve o documento

5.3.1	Apresentar o resultado da pesquisa como uma lista de documentos digitais, convencionais ou híbridos que cumpram os parâmetros da mesma e notificar quando o resultado for nulo			
5.3.2	Após apresentar o resultado da pesquisa, o Sistema tem que permitir ao usuário as seguintes opções:			
5.3.2.1	Visualizar os documentos resultantes da pesquisa			
5.3.2.2	Redifinir os parâmetros de pesquisa e fazer nova consulta			
5.3.3	Apresentar o conteúdo de todos os tipos de documentos arquivísticos digitais capturados de forma que:			
5.3.3.1	Preserve as características de apresentação visual e formato apresentados pela aplicação geradora			
5.3.3.2	Exiba todos os componentes do documento digital em conjunto, como uma unidade			
5.3.4	Exibir em tela todos os tipos de documentos capturados			
5.3.5	Imprimir os documentos capturados, preservando o formato produzido pelas aplicações geradoras			
5.3.6	Exibir ou reproduzir o conteúdo de documentos que incluam imagem fixa, imagem em movimento e som			

5.3.7	Proporcionar ao usuário formas flexíveis de impressão de documentos com seus metadados, incluindo a possibilidade de definição dos metadados a serem impressos			
5.3.8	Exibir em tela e imprimir todos os metadados associados aos documentos resultantes de uma pesquisa			
5.3.9	Permitir a impressão de uma lista de documentos resultante de uma pesquisa			
5.3.10	Permitir a impressão de uma lista de documentos que compõem um processo\dossiê			
5.3.11	Permitir que todos os documentos de um processo\dossiê sejam impressos em uma única operação, na sequência determinada pelo usuário			
5.3.12	Incluir recursos destinados a transferir para suportes adequados documentos que não possam ser impressos, tais como som, vídeo e páginas web			
5.3.13	Realizar pesquisa e exibição de documentos simultaneamente para diversos usuários			
6	Segurança			
6.1	Cópias de segurança			
6.1.1	Permitir que, sob controle do seu Administrador, mecanismos de backup criem cópias de todas as informações nele contidas (documentos arquivísticos, metadados e parâmetros do Sistema)			

6.1.2	Manter o controle das cópias de segurança, prevendo testes de restauração			
6.1.3	Incluir funções para restituir os documentos de arquivo e metadados a um estado conhecido, utilizado uma combinação de cópias restauradas e rotinas de auditoria			
6.2	Controle de acesso			
6.2.1	Para implementar o controle de acesso, o Sistema tem que manter, pelo menos, os seguintes atributos dos usuários, de acordo com a política de segurança:			
6.2.1.1	Identificador do usuário		Identificador do agente	Identifica o agente (usuário, perfil e grupo)
			Nome do agente	Indica o nome do agente que pode se apresentar como usuário, perfil (função\cargo) ou grupo (conjunto de usuários reunidos para a realização de uma atividade temporária)
			Situação do agente	Indica se o agente está ativo ou inativo no sistema
6.2.1.2	Autorizações de acesso		Autorização de acesso	Nível de restrição de acesso (uso e intervenção) aos documentos e operações do sistema,

				de acordo com o perfil do usuário
6.2.1.3	Credenciais de autenticação	Senha, crachá, chave criptográfica, token USB, smartcard, biometria (de impressão digital, de retina, etc) são exemplos de credenciais de autenticação	Credenciais de autenticação	Autentica o usuário no sistema. Pode ser senha, biometria, certificado digital e chave privada
6.2.2	Exigir que o usuário esteja devidamente identificado e autenticado antes que este inicie qualquer operação no Sistema			
6.2.3	Garantir que os valores dos atributos de segurança e controle de acesso, associados ao usuário, estejam dentro de conjuntos de valores válidos			
6.2.4	Permitir acesso a funções do Sistema somente a usuários autorizados e sob controle rigoroso da Administração do Sistema a fim de proteger a autenticidade dos documentos arquivísticos digitais			
6.2.5	Somente Administradores autorizados têm que ser capazes de criar, alterar, remover ou revogar as permissões associadas a papéis de usuários, grupos de usuários ou usuários individuais			
6.2.6	Implementar a política de controle de acesso por grupos de usuários sobre documentos baseado no seguinte:			

6.2.6.1	Identidade do usuário e sua participação em grupos		Perfil de usuário	Relaciona o usuário a papéis e\ou grupos a que pertence
6.2.6.2	Atributos de segurança, associados ao documento arquivístico digital, a classe, subclasse, grupo e subgrupo			
6.2.7	O acesso a documentos ou classes, subclasses, grupos e subgrupos, tem que ser concedido se a permissão requerida para a operação estiver associada a pelo menos um dos grupos aos quais o usuário pertença			
6.2.8	Permitir que um usuário pertença a mais de um grupo			
6.2.9	Usar os seguintes atributos do usuário ao implementar a política de controle de acesso por perfis de usuários sobre documentos digitais:			
6.2.9.1	Identificação do usuário			
6.2.9.2	Perfis associados ao usuário			
6.2.10	Usar os seguintes atributos dos documentos digitais ao implementar a política de controle de acesso por perfis:			
6.2.10.1	Identificação do documento digital			
6.2.10.2	Operações permitidas para os vários perfis de usuários, sobre as classes, subclasses, grupos e subgrupos ou processos\dossiês a qual o documento pertence			

6.2.11	O acesso a documentos ou classes, subclasses, grupos e subgrupos tem que ser concedido somente se a permissão requerida para a operação estiver presente em pelo menos um dos perfis associados ao usuário			
6.2.12	Impedir que um usuário assuma perfis com direitos conflitantes			

6.3	Implementar a classificação de grau de sigilo sobre os documentos, processos\dossiês e as classes, subclasses, grupos e subgrupos do plano de classificação e sobre todas as operações de usuários nos documentos		Classificação de segurança	Refere-se a atribuição de categorias e graus de sigilo aos documentos ou as informações neles contidas, conforme legislação específica
			Prazo de restrição de acesso	Registra o prazo de restrição previsto para a categoria e grau de sigilo correspondente
			Registro de classificação de sigilo	Registra informações: data\hora e responsável pela classificação de categoria e grau de sigilo
			Registro de desclassificação de sigilo	Registra informações: data\hora e responsável pela desclassificação de categoria e grau de sigilo

			Registro de reclassificação de sigilo	Registra informações: data\hora e responsável pela reclassificação da categoria e grau de sigilo
6.3.1	Classificar os documentos de acordo com a categoria e o grau de sigilo correspondente e implementar as operações necessárias, baseando-se nos seguintes atributos de segurança para documentos e para usuários:			
6.3.1.1	Grau de sigilo do documento	O grau de sigilo do documento tem que estar associado a credencial de segurança do usuário	Grau de sigilo	Especificações dos graus de sigilo conforme legislação específica
6.3.1.2	Categoria do documento sigiloso		Categoria do documento sigiloso	Especificação da categoria de documento sigiloso conforme legislação específica
6.3.1.3	Credencial de segurança do usuário		Níveis de acesso	Indica os níveis de acesso segundo a classificação da informação quanto à categoria e ao grau de sigilo e restrição de acesso
6.3.2	Recusar o acesso de usuários a documentos que possuam um grau de sigilo superior a sua credencial de segurança			

6.3.3	Garantir que os documentos sem atribuição de grau de sigilo, importados a partir de fontes externas ao Sistema, estejam sujeitos às políticas de controle de acesso e de sigilo			
6.3.4	Manter a marcação de sigilo original durante a importação de documentos marcados com graus de sigilo, a partir de fontes externas ao Sistema			
6.3.5	Permitir que um dos itens abaixo seja selecionado durante a configuração:			
6.3.5.1	Graus de sigilo a serem atribuídos a séries e documentos			
6.3.5.2	Séries e documentos sem grau de sigilo			
6.3.6	Em caso de erro ou reavaliação, o Administrador tem que ser capaz de alterar o grau de sigilo de todos os documentos arquivísticos de uma classe, subclasse, grupo e subgrupo, numa única operação			
6.3.7	Garantir que o grau de sigilo de um documento importado esteja associado a um usuário autorizado com a credencial de segurança pertinente para receber o documento			
6.3.8	Permitir somente aos Administradores autorizados a possibilidade de alterar a configuração dos valores predefinidos (default) para os atributos de segurança e marcação de graus de sigilo, quando necessário e apropriado			

6.3.9	Somente Administradores autorizados têm que ser capazes de realizar as seguintes ações:			
6.3.9.1	Remover ou revogar os atributos de segurança de documentos			
6.3.9.2	Criar, alterar, remover ou revogar as credenciais de segurança de usuários			
6.3.10	Permitir somente ao usuário autorizado, mediante confirmação, a reclassificação, desclassificação ou redução do grau de sigilo de um documento			
6.3.11	Impedir que um documento sigiloso seja eliminado	Os documentos sigilosos têm que se tornar ostensivos para serem submetidos ao processo de avaliação e serem destinados		
6.3.12	Implementar metadados em relação aos documentos ou extratos de documentos para contralar o acesso a informação sensível			
6.4	Trilhas de auditoria			
6.4.1	Registrar na trilha de auditoria informações acerca das seguintes ações:			
6.4.1.1	Data e hora da captura de todos os documentos			
6.4.1.2	Responsável pela captura			
6.4.1.3	Reclassificação, desclassificação ou prorrogação do prazo de sigilo de um documento, com a classificação inicial e a classificação final			

6.4.1.4	Qualquer alteração nas Tabelas de Temporalidade de Documentos			
6.4.1.5	Qualquer ação de reavaliação de documentos			
6.4.1.6	Qualquer alteração nos metadados associados aos documentos ou classes			
6.4.1.7	Data e hora de produção, aditamento e eliminação de metadados			
6.4.1.8	Alterações efetuadas nas permissões de acesso que afetem um documento ou um usuário			
6.4.1.9	Ações de exportação e importação envolvendo os documentos			
6.4.1.10	Tentativas de exportação (inclusive para backups) e de importação (inclusive restore)			
6.4.1.11	Usuário, data e hora de acesso ou tentativa de acesso aos documentos e ao Sistema			
6.4.1.12	Tentativas de acesso negado a qualquer documento			
6.4.1.13	Ações de eliminação de qualquer documento e seus metadados			
6.4.1.14	Infrações cometidas contra mecanismos de controle de acesso			
6.4.1.15	Mudanças no relógio gerador de carimbos de tempo			
6.4.1.16	Todas as ações administrativas sobre os atributos de segurança (perfis, grupos, permissões, etc)			

6.4.1.17	Todas as ações administrativas sobre dados de usuários (cadastro, ativação, bloqueio, atualização de dados e permissões, troca de senha, etc)			
6.4.1.18	Todos os eventos de administração e manutenção das trilhas de auditoria (alarmes, cópias, configuração de parâmetros, etc)			
6.4.2	Registrar, em cada evento auditado, informações sobre a identidade do usuário, desde que tal identificação esteja de acordo com a política de privacidade da organização e a legislação vigente			
6.4.3	Assegurar que as informações da trilha de auditoria estejam disponíveis para inspeção a fim de que uma ocorrência específica possa ser identificada e que todas as respectivas informações sejam claras e compreensíveis			
6.4.4	Impedir qualquer modificação da trilha de auditoria			
6.4.5	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	A trilha de auditoria não pode ser excluída antes da data indicada na Tabela de Temporalidade. Porém, a transferência implica cópia da trilha para outro espaço de armazenamento com a subsequente liberação do espaço original. A exportação é a		

		cópia sem a liberação do espaço		
6.4.6	Fornecer relatórios sobre as ações que afetam classes, processo\dossiê e documentos, em ordem cronológica e organizados por:			
6.4.6.1	Documento arquivístico, processo\dossiê ou classe			
6.4.6.2	Usuário			
6.4.6.3	Tipo de ação ou operação			
6.4.7	Somente Administradores autorizados, acompanhados do auditor, tem que ser capazes de configurar o conjunto de eventos auditáveis e seus atributos			
6.5	Assinaturas digitais			
6.5.1	Somente Administradores autorizados têm que ser capazes de incluir, remover, ou atualizar no Sistema os certificados digitais de computadores ou de usuários			
6.5.2	Verificar a validade da assinatura digital no momento da captura do documento			
6.5.3	O Sistema, no processo de verificação da assinatura digital, tem que ser capaz de registrar nos metadados do documento o			

	seguinte:			
6.5.3.1	Validade da assinatura verificada			
6.5.3.2	Autoridade certificadora do certificado digital			
6.5.3.3	Data e hora em que a verificação ocorreu			
6.6	Criptografia			
6.6.1	Usar a criptografia no armazenamento, na transmissão e na apresentação de documentos arquivísticos digitais ao classificar documentos de acordo com os graus de sigilo			
6.6.2	Limitar o acesso aos documentos cifrados somente aqueles usuários portadores de chave de decifração			
6.6.3	Registrar os seguintes metadados sobre um documento cifrado:			
6.6.3.1	Indicação se está cifrado ou não			
6.6.3.2	Algoritmos usados na cifração			
6.6.3.3	Identificação do remetente			
6.6.3.4	Identificação do destinatário			
6.6.3.5	Indicação da robustez ou grau de segurança da criptografia			
6.6.4	Somente os usuários autorizados têm que ser capazes de realizar as seguintes operações:			
6.6.4.1	Incluir, remover ou alterar parâmetros dos algoritmos criptográficos instalados no Sistema			

6.6.4.2	Incluir, remover ou substituir chaves criptográficas de programas ou de usuários do Sistema			
6.6.4.3	Cifrar e alterar criptografia de documentos			
6.6.4.4	Remover a criptografia de um documento	A remoção da cifração pode ocorrer quando a sua manutenção resultar em indisponibilidade do documento. Por exemplo, quando a chave de cifração\decifração estiver embarcada em hardware inviolável cuja vida útil está prestes a se esgotar ou quando o documento for desclassificado		
6.6.5	No caso de remoção da cifração do documento, os seguintes metadados adicionais tem que ser registrados na trilha de auditoria:			
6.6.5.1	Data e hora da remoção da cifração			
6.6.5.2	Identificação do executor da operação			
6.6.5.3	Motivo da remoção da cifração			
6.7	Marcas d'água digitais			
6.7.1	Recuperar informações contida em marcas d'água digitais			
6.7.2	Armazenar documentos arquivísticos digitais que contenham marcas d'água digitais, assim como informação de apoio relacionada à marca d'água			

6.8	Acompanhamento de transferência			
6.8.1	Fornecer um recurso de acompanhamento para monitorar e registrar informações acerca do local atual e da transferência de documentos digitais e convencionais			
6.8.2	A função de acompanhamento de transferência tem que registrar metadados que incluam:		Registro de transferência	Registra informações: data\hora de envio, data\hora de recebimento, destinatário, método utilizado, responsável pela transferência, responsável pelo recebimento, localização\suporte anterior, localização\suporte atual, identificação do lote, número do termo de transferência
6.8.2.1	Número dos documentos atribuído pelo Sistema		Identificador único	Registra o código gerado automaticamente que identifica o processo, o dossiê ou o documento de maneira a distingui-los dos demais
6.8.2.2	Localização atual e também as localizações anteriores, definidas pelo usuário			
6.8.2.3	Data e hora de envio\transferência			

6.8.2.4	Data e hora da recepção no novo local			
6.8.2.5	Destinatário			
6.8.2.6	Usuário responsável pela transferência (sempre que adequado)			
6.8.2.7	Método de transferência			
6.9	Autoproteção			
6.9.1	Após falha ou descontinuidade do Sistema, quando a recuperação automática não for possível, o Sistema tem que ser capaz de entrar em modo de manutenção, no qual a possibilidade de restaurar o Sistema para um estado seguro é oferecida	Na restauração ao estado seguro, o Sistema deve ser capaz de garantir a recuperação de perdas ocorridas, incluindo os documentos de transações mais recentes		
6.9.2	Garantir que as funções de controle de acesso sejam invocadas antes de qualquer operação de acesso e retornadas sem erros antes do prosseguimento normal da operação			
6.9.3	Preservar um estado seguro de funcionamento, interrompendo completamente a interação com usuários comuns, quando quaisquer dos seguintes erros ocorrerem:			
6.9.3.1	Falha de comunicação entre cliente e servidor			
6.9.3.2	Perda de integridade das informações de controle de acesso			
6.9.3.3	Falta de espaço para registro nas trilhas de auditoria			

6.9.3.4	Quando não for possível escrever na trilha de auditoria, o Sistema deve impedir toda operação de qualquer usuário e passar para o modo de manutenção			
6.10	Alterar, apagar e truncar documentos arquivísticos digitais			
6.10.1	Permitir, a um Administrador autorizado a anulação da operação em caso de erro do usuário ou do Sistema	Anular uma operação não significa apagar um documento arquivístico capturado pelo Sistema. Não é possível anular a eliminação definitiva de documentos, por tratar-se de operação irreversível		
6.10.2	Em casos excepcionais, o Administrador tem que ser autorizado a apagar ou corrigir documentos e volumes. Nesses casos, o Sistema tem que:			
6.10.2.1	Registrar integralmente a ação de apagar ou corrigir na trilha de auditoria			
6.10.2.2	Produzir um relatório de anomalias para o Administrador			
6.10.2.3	Eliminar todo o conteúdo de um documento ou volume, quando os mesmos forem eliminados			
6.10.2.4	Garantir que nenhum documento seja eliminado, se tal ação resultar na alteração de outro documento arquivístico			

6.10.2.5	Informar ao Administrador sobre a existência de ligação entre um documento prestes a ser apagado e qualquer outro documento, solicitando antes de concluir a operação			
6.10.2.6	Manter a integridade total dos metadados, a qualquer momento			
6.10.3	No caso de erro na inserção de metadados, o Administrador terá que corrigi-lo e o Sistema terá que registrar essa ação na trilha de auditoria			
6.10.4	Permitir a um usuário autorizado fazer um extrato (cópia truncada) de um documento, com o objetivo de truncá-lo sem alterar o original			
6.10.5	Quando uma cópia truncada é produzida, o Sistema tem que registrar essa ação nos metadados do documento, incluindo pelo menos a data, a hora, o motivo e quem a produziu			
6.10.6	Armazenar na trilha de auditoria qualquer alteração efetuada para satisfazer os requisitos desta seção			
7	Armazenamento		Prazo de guarda	Registra o tempo de permanência dos documentos na unidade produtora e na unidade com atribuições de arquivo, de acordo com a tabela de temporalidade

7.1	Durabilidade			
7.1.1	A escolha de dispositivos tem que ser periodicamente revista sempre que a evolução tecnológica indicar mudanças importantes			
7.1.2	Atividades de migração tem que ser efetivadas preventivamente sempre que se torne patente ou previsível a obsolescência do padrão corrente			
7.1.3	Para as memórias secundárias, um Sistema tem que manter registro de MTBF (Mean Time Between Failure), bem como as datas de sua aquisição			
7.1.4	Para as memórias secundárias e terciárias, um Sistema tem que fazer o gerenciamento das mídias por meio do registro de durabilidade prevista, data de aquisição e histórico de utilização	Informações técnicas sobre previsibilidade de duração de mídias referidas na alínea 2 deste item devem ser obtidas preferencialmente a partir de órgãos independentes. Quando isso não for possível, podem ser utilizadas informações de fornecedores. Em ambos os casos, deve ficar registrada a origem da informação		

7.1.5	Quando se proceder a eliminação de documentos, as memórias de suporte têm que ser devidamente limpas, isto é, ter suas informações efetivamente indisponibilizadas	Este requisito aplica-se principalmente às memórias secundária e terciária, pela sua característica não volátil. As informações devem ser eliminadas de forma irreversível, incuindo, no caso de memória terciária, a possibilidade de destruição física das mídias		
7.2	Capacidade			
7.2.1	Possuir capacidade de armazenamento suficiente para acomadação de todos os documentos e suas cópias de segurança. Nesse sentido, os testes de carga deverão anteceder a implementação do Sistema	Para grandes volumes de dados é conveniente o uso de dispositivos com maior capacidade unitária de armazenamento, a fim de reduzir a sobrecarga operacional		

7.2.2	Em um Sistema, tem que ser prevista a possibilidade de expansão da estrutura de armazenamento	A quantidade de memória primária deve ser superestimada no momento de aquisição, a fim de minimizar as indisponibilidades do Sistema nas situações de expansão desse tipo de memória. Quando da aquisição de "disk arrays" as possibilidades de expansão dos equipamentos de controle devem ser consideradas. Para backups em fita magnética em sistemas com grande volume de informação, devem ser utilizados sistemas automáticos de seleção, troca e controle de fitas (robots)		
7.3	Efetividade de armazenamento			
7.3.1	Utilizar técnicas de restauração de dados em caso de falhas			
7.3.2	Utilizar mecanismos de proteção contra escrita, que previnam alterações indevidas e mantenham a integridade dos dados armazenados			
7.3.3	A integridade dos dispositivos de armazenamento tem que ser			

	periodicamente verificada			

8	Preservação		Identificador do documento digital	Identificador dos componentes digitais que integram o documento
			Registro de procedimentos de preservação	Registra informações: data\hora do procedimento, descrição e responsável. Informações históricas e planejadas (em campos separados)
			Registro de recolhimento	Registra informações: data\hora de envio, data\hora de recebimento, destinatário, método utilizado, responsável pelo recolhimento, localização\suporte anterior, localização\suporte atual, identificação do lote, número do termo de recolhimento
8.1	Aspectos físicos			

8.1.1	Os suportes de armazenamento do Sistema têm que ser acondicionados, manipulados e utilizados em condições ambientais compatíveis com sua vida prevista e\ou pretendida, dentro das especificações técnicas de seu fabricante e de entidades isentas e com base em estatísticas de uso	A vida útil pretendida de um suporte pode ser menor que sua vida útil, prevista, o que permite condições ambientais flexíveis	Características do documento digital	Registra informações: suporte, vida útil do suporte, tamanho, formato, aplicação utilizada para a criação do documento, nome original, ambiente de criação, informações sobre assinatura digital, relação entre os objetos
8.1.2	Permitir o controle da vida útil dos suportes para auxiliar no processo de rejuvenescimento		Características do documento digital	Registra informações: suporte, vida útil do suporte, tamanho, formato, aplicação utilizada para a criação do documento, nome original, ambiente de criação, informações sobre assinatura digital, relação entre os objetos
8.2	Aspectos lógicos			
8.2.1	Manter cópias de segurança	As cópias de segurança devem ser guardadas em ambientes seguros, em local diferente de onde se encontra a informação original	Cópias de segurança	Registra informações sobre as cópias de segurança de documentos arquivísticos digitais e seus metadados, bem como de parâmetros do sistema operacional, do gerenciados de banco de dados, do sistema

				informatizado de gerenciamento e do software aplicativo, sua localização e características
8.2.2	Possuir funcionalidades para a verificação periódica dos dados armazenados, visando a detecção de possíveis erros	Nesse caso, recomenda-se o uso de um checksum robusto, ou seja, que permita a constatação da integridade dos dados e seja seguro quanto a fraudes		
8.2.3	Permitir a substituição dos dados armazenados que apresentarem erros			
8.2.4	Ações de preservação têm que ser efetivadas sempre que se torne patente ou previsível a obsolescência da tecnologia utilizada pelo Sistema			
8.2.5	Suportar a transferência em bloco de documentos (incluindo as demais informações associadas a cada documento) para outros suportes e\ou sistemas, de acordo com as normas aplicáveis aos formatos utilizados			
8.3	Aspectos gerais			
8.3.1	Registrar as operações de preservação realizadas, em trilhas de auditoria			

8.3.2	As modificações em um Sistema e em sua base tecnológica têm que ser verificadas em um ambiente exclusivo para essa finalidade, de modo a garantir que, após a implantação das alterações, os dados continuem sendo acessados sem alteração de conteúdo			
8.3.3	Gerir metadados relativos a preservação dos documentos e seus respectivos componentes			
9	Funções administrativas			
9.1	Permitir que o Administrador, de uma maneira controlada e sem esforço excessivo, visualize e reconfigure os parâmetros do Sistema e os atributos dos usuários			
9.2	Fornecer relatórios flexíveis para o Administrador gerenciar os documentos e seu uso, que apresentem no mínimo:			
9.2.1	Quantidade de documentos (avulsos, processos, dossiês), volumes e itens, a partir de parâmetros ou atributos definidos (tempo, classe, unidade administrativa etc)			
9.2.2	Estatísticas de transação relativas a documentos, volumes e itens			
9.2.3	Relatórios de atividades por usuário			
9.3	Prover documentação cobrindo aspectos de Administração do Sistema. A documentação deve incluir todas as informações necessárias para o correto			

	gerenciamento do Sistema			
10	Conformidade com a legislação e regulamentações			
10.1	O Sistema deve estar de acordo com a legislação e normas pertinentes, tendo em vista a admissibilidade legal e o valor probatório dos documentos arquivísticos			
10.2	Estar de acordo com a legislação, normas e procedimentos específicos para gestão e acesso de documentos arquivísticos, em observância a política de arquivos e gestão documental implementada pelo Conselho Nacional de Arquivos			
10.3	Estar em conformidade com requisitos regulamentares específicos e códigos de boa prática necessários para a execução de determinadas atividades			
11	Usabilidade			
11.1	O Sistema deve restringir o acesso as funcionalidades administrativas impossibilitando sua visualização ao usuário final	Exemplos: as operações não disponíveis aparecem com fonte atenuada nos menus e possuem efeito nulo quando acionadas. O acesso as operações indisponíveis é restrito pela configuração de menus que não as apresentam ao usuário sem		

		permissão de executá-las		
11.2	Deve possuir documentação completa, clara, inteligível e organizada para a instalação e uso do software			
11.3	Deve possuir Sistema de ajuda on line			
11.4	Deve disponibilizar pelo menos dois papéis de acesso diferenciados, um para usuário final e outro para administrador de Sistema		Perfil de usuário	Relaciona o usuário a papéis e\ou grupos a que pertence
12	Interoperabilidade			
12.1	O Sistema deve ser capaz interoperar com outros sistemas de informação, incluindo sistemas legados de controle de documentos, através de padrões abertos de interoperabilidade	Por interoperabilidade, entende-se o intercâmbio coerente de informações e serviços entre sistemas. A interoperabilidade deve possibilitar a substituição de qualquer componente ou produto usado nos pontos de interligação por outro de especificação similar, sem comprometimento das funcionalidades do Sistema. Isto se faz através		

		do uso de regras e padrões de comunicação		
12.2	O Sistema deve aplicar os requisitos de segurança descritos neste documento para executar operações de interoperabilidade	Isso é fundamental para que as operações, feitas em ambiente com interoperabilidade, não afetem a integridade dos documentos e impossibilitem acessos não autorizados		
13	Disponibilidade			
13.1	O Sistema deve se adequar ao grau de disponibilidade estabelecido pelo IFF	Os requisitos de disponibilidade descrevem as exigências mínimas sobre prontidão de atendimento de um Sistema. Os requisitos de disponibilidade devem ser especificados pelo Administrador Central do Sistema, de acordo com o nível de serviço a ser		

		fornecido, os períodos previstos de atendimento, bem como o tempo máximo tolerável em interrupções previstas		
14	Desempenho e escalabilidade			
14.1	Incluir rotina de manutenção de:	Essas tarefas devem atender a mudanças planejadas, sem causar grandes sobrecargas de administração		
14.1.1	Dados de usuários e de grupos			
14.1.2	Perfis de acesso			
14.1.3	Planos de Classificação de Documentos			
14.1.4	Bases de dados			
14.1.5	Tabelas de Temporalidade de Documentos			
14.2	Deve ser expansível até comportar um número máximo preestabelecido de usuários simultâneos, provendo continuidade efetiva de serviços			

REQUISITOS ALTAMENTE DESEJÁVEIS

CÓDIGO	REQUISITO ALTAMENTE DESEJÁVEL	OBSERVAÇÃO	METADADO	DEFINIÇÃO
1	Organização dos documentos arquivísticos: Planos de Classificação e manutenção de documentos			
1.1	Configuração e Administração de Planos de Classificação de Documentos			
1.1.1	Deve ser capaz de importar e exportar total ou parcialmente um Plano de Classificação de Documentos			
1.2	Classificação e metadados das séries documentais			
1.2.1	Deve relacionar os metadados herdados de forma que a alteração no metadado de uma série seja automaticamente incorporada à série que herdou esse metadado			
1.2.2	Quando um documento é reclassificado, o Sistema deve manter registro de suas posições anteriores a reclassificação, de forma a manter um histórico			
1.2.3	Quando um documento é reclassificado, O Sistema deve permitir que o Administrador introduza as razões para a reclassificação			
1.3	Gerenciamento de documentos			
1.3.1	Deve ser capaz de registrar múltiplas referências a um documento digital, sem a necessidade de duplicá-lo fisicamente	Quando um documento digital estiver associado a outros documentos, o Sistema deverá criar um registro para cada		

		referência aos documentos associados		
1.4	Requisitos adicionais para o gerenciamento de documentos			
1.4.1	Deve prever funcionalidades para apoiar a pesquisa de existência de documento relativo a mesma ação ou interessado			
1.5	Volumes: abertura, encerramento e metadados			
1.5.1	Deve ser capaz de gerenciar volumes para subdividir processos\dossiês, fazendo distinção entre processos\dossiês e volumes			
1.5.2	Deve permitir a associação de metadados aos voumes e deve restringir a inclusão e a alteração desses mesmos metadados somente a usuários autorizados			
1.5.3	Deve permitir o registro de metadados correpondentes as datas de abertura e de encerramento de volumes			
1.5.4	Deve ter a capacidade de encerrar um volume digital automaticamente, desde que o critério predefinidos no momento da configuração do plano de classificação sejam seguidos, tais como:			
1.5.4.1	Volumes circunscritos a um período de tempo como, por exemplo, o término do ano civil			

1.5.4.2	Tempo decorrido desde o término de um determinado evento como, por exemplo, o mais aditamento de um documento de arquivo digital a esse volume			
2	Tramitação e fluxo de trabalho			
2.1	Controle do fluxo de trabalho			
2.1.1	O fluxo de trabalho de um Sistema deve permitir o uso do correio eletrônico para que um usuário possa informar a outros usuários sobre documentos que requeiram sua atenção	Esse requisito requer a integração com um Sistema de correio eletrônico existente		
2.1.2	O Administrador deve poder autorizar usuários individuais a redistribuir tarefas ou ações para outro usuário ou grupo diferentes daquele previsto em um fluxo de trabalho	Um usuário pode precisar enviar um documento a outro usuário, devido ao seu conteúdo ou no caso do usuário responsável se encontrar em licença		
2.1.3	Um recurso de fluxo de trabalho de um Sistema deve gerir os documentos em filas de espera que possam ser examinadas e controladas pelo Administrador			
2.1.4	O recurso de fluxo de trabalho de um Sistema deve ter a capacidade de deixar que os usuários visualizem a fila de espera de trabalho a eles destinado e que selecionem os itens a trabalhar			

2.1.5	Um recurso de fluxo de trabalho de um Sistema deve fornecer fluxos condicionais de acordo com os dados de entrada do usuário ou os dados do Sistema	Os fluxos que remetem o documento a um dos participantes dependem de uma condição determinada por um deles. Por exemplo: um fluxo pode levar um documento a um participante ou a um outro, conforme os dados de entrada do participante anterior; ou a definição do fluxo pode depender de um valor calculado pelo sistema		
2.1.6	O recurso de fluxo de trabalho de um Sistema deve poder associar limites de tempo a trâmites e\ou procedimentos individuais em cada fluxo e comunicar os itens que expiraram de acordo com tais limites			
2.1.7	Sempre que o participante for um grupo de trabalho, um recurso de fluxo de trabalho de um Sistema deve prever a forma de distribuição dos documentos entre os membros do grupo. Essa distribuição pode ser:			
2.1.7.1	De acordo com uma sequência circular pré-definida, o documento envia o próximo documento independentemente da conclusão da tarefa anterior; ou			

2.1.7.2	A medida que cada membro conclui a tarefa, o Sistema lhe envia o próximo documento da fila do grupo			
2.1.8	O recurso de fluxo de trabalho de um Sistema deve permitir que a captura de documentos desencadeie automaticamente fluxos de trabalho			
2.1.9	Deve manter versões dos fluxos alterados e estabelecer vínculos entre os documentos já processados ou em processamento nos fluxos alterados			
2.1.10	Deve assegurar que qualquer modificação nos atributos dos fluxos, como extinção ou ampliação do número de pessoas ou extinção de autorização, leve em conta os documentos vinculados			
3	Captura			
3.1	Captura: procedimentos gerais			
3.1.1	Deve utilizar vocabulário controlado para apoiar a atribuição do metadado descritor			
3.1.2	Deve ser capaz de relacionar o mesmo documento digital a mais de um processo ou dossiê, sem duplicação física do mesmo	Quando um documento digital estiver associado a mais de um processo\dossiê, o Sistema deverá criar um registro para cada referência desse documento. Cada registro estará vinculado ao mesmo objeto digital		

3.1.3	Deve ser capaz de inserir automaticamente os metadados previstos no Sistema para o maior número possível de documentos, pois isso diminui as tarefas do usuário do Sistema e garante maior rigor na inserção dos metadados	Exemplo: no caso de documentos com forma padronizada (formulários, modelos de requerimentos, de memorandos etc) alguns metadados podem ser inseridos automaticamente, tais como: número identificador, título, classificação, prazo de guarda		
3.1.4	Deve prestar assistência aos usuários no que diz respeito à classificação de documentos, por meio de algumas ou de todas as ações que se seguem:			
3.1.4.1	Tornar acessível ao usuário somente o subconjunto do Plano de Classificação de Documentos que diz respeito a sua atividade			
3.1.4.2	Indicar as últimas classificações feitas pelo usuário			
3.1.4.3	Indicar processos\dossiês que contenham documentos de arquivo relacionados			
3.1.4.4	Indicar classificações possíveis a partir dos metadados já inseridos			
3.1.4.5	Indicar classificações possíveis a partir do conteúdo do documento			

3.1.5	Deve permitir que um usuário transmita documentos a outro usuário para completar o processo de captura, no caso dos procedimentos dessa captura serem distribuídos entre vários usuários			
3.2	Captura de mensagens de correio eletrônico			
3.2.1	Deve assegurar a captura do nome e não somente do endereço do originador do correio eletrônico. Por exemplo, "Luiz Santos" além de isa25@ab.br			
3.3	Formato de arquivo e estrutura dos documentos a serem capturados			
3.3.1	Deve capturar, entre outros, os seguintes documentos:	A lista de documentos, que um Sistema tem que suportar, poderá sofrer variações		
3.3.1.1	Calendários eletrônicos			
3.3.1.2	Informações de outros aplicativos: contabilidade, folha de pagamento, desenho assistido por computador (CAD)			
3.3.1.3	Documentos em papel digitalizados por meio de scanner			
3.3.1.4	Documentos sonoros			
3.3.1.5	Videoclipes			
3.3.1.6	Diagramas e mapas digitais			
3.3.1.7	Dados estruturados (EDI)			
3.3.1.8	Bases de dados			
3.3.1.9	Documentos multimídia			

3.3.2	Deve permitir que um documento composto seja capturado de qualquer uma das formas seguintes:			
3.3.2.1	Como um único documento de arquivo composto			
3.3.2.2	Como um conjunto de documentos de arquivos simples relacionados, um para cada componente do documento composto			
3.4	Estrutura dos procedimentos de gestão			
3.4.1	Deve poder emitir um aviso, no caso de se tentar capturar um documento incompleto ou inconsistente de uma forma que venha a comprometer sua futura autenticidade	Exemplo: uma correpondência sem assinatura digital válida ou uma fatura de fornecedor não identificado		
3.4.2	Deve poder emitir um aviso, no caso de se tentar capturar um documento em que a futura verificação de sua autenticidade não for viável			
4	Avaliação e destinação			
4.1	Configuração da Tabela de Temporalidade de Documentos			
4.1.1	Deve ser capaz de manter o histórico das alterações realizadas na Tabela de Temporalidade de Documentos		Registro de alteração	Registra informações: data\hora da alteração, ersponsável pela alteração, identificador da série que teve prazo ou destinação alterada, descrição da alteração (incluindo o prazo\destinação

				anterior)
4.1.2	Deve ser capaz de importar e exportar total ou parcialmente uma tabela de temporalidade de documentos (Ver item 10 - Interoperabilidade)			
4.2	Aplicação da Tabela de Temporalidade de Documentos			
4.2.1	Deve prever, em determinados casos, dispositivos de aviso antes do início da execução de uma ação de destinação. Por exemplo, aviso ao Administrador caso um documento arquivístico possua um determinado nível de segurança			
4.3	Exportação de documentos			
4.3.1	Deve ser capaz de exportar documentos:			
4.3.1.1	Em seu formato nativo (ou no formato para o qual foi migrado)			
4.3.1.2	De acordo com os formatos definidos em padrões de interoperabilidade do governo (e-ping)			
4.3.1.3	De acordo com o formato definido pela instituição arquivística que irá receber a documentação, no caso de transferência ou recolhimento			

4.3.2	Deve ser capaz de exportar metadados nos formatos previstos pelo padrão de interoperabilidade do governo			
4.3.3	Deve possibilitar a inclusão de metadados necessários a gestão do arquivo permanente nos documentos que serão exportados para recolhimento			
4.3.4	Quando se exportar documentos híbridos, um Sistema deve exigir do usuário autorizado a confirmação de que a parte sob forma convencional dos mesmos documentos tenha passado pelo procedimento de destinação adequado antes de confirmar a exportação da parte sob forma digital		Tipo de suporte	1. Indicar se o documento é digital, convencional ou híbrido. 2. Especificar o material sobre o qual as informações são registradas: papel, filme, fita magnética, disco magnético, disco óptico, meio digital
4.3.5	Deve permitir que documentos sejam exportados mais de uma vez			
4.4	Eliminação			
4.4.1	Deve permitir a eliminação de documentos de forma irreversível a fim de que não possam ser restaurados por meio da utilização normal do Sistema, nem po rmeio de rotinas auxiliares do Sistema operacional, nem por aplicações especiais de recuperação de dados			

4.4.2	Quando eliminar documentos híbridos, o Sistema deve exigir do usuário autorizado a confirmação de que a parte sob forma convencional dos mesmos seja eliminada também antes de confirmar a eliminação da parte sob forma digital			
4.5	Avaliação de documentos arquivísticos convencionais e híbridos			
4.5.1	Deve exportar metadados de documentos convencionais			
5	Pesquisa, localização e apresentação de documentos			
5.1.1	Deve fornecer interface de pesquisa, localização e apresentação opcionais via ambiente web			
5.1.2	Deve prever a navegação gráfica no plano de classificação, a navegação direta de uma classe para os documentos arquivísticos nessa mesma classe, e a seleção, recuperação e apresentação direta dos documentos arquivísticos e de seus conteúdos por meio desse mecanismo			
5.2	Pesquisa e localização			
5.2.1	Deve permitir que os conteúdos sob a forma de texto dos documentos possam ser pesquisados			
5.2.2	Deve fornecer uma interface que possibilite a pesquisa combinada de metadados e de conteúdo do documento por meio dos operadores boolianos E, OU e NÃO			

5.2.3	Deve permitir que os termos utilizados na pesquisa possam ser qualificados, especificando-se um metadado ou o conteúdo do documento como fonte de busca			
5.2.4	Deve permitir a utilização de caracteres coringa e de truncamento a direita para a pesquisa de metadados	Exemplos: o argumento de pesquisa "Bra*" pode recuperar "Brasil" e "Brazil", o argumento de pesquisa "Arq*" pode recuperar "Arquivo", "Arquivística" etc		
5.2.5	Deve permitir a utilização de caracteres coringa e de truncamento a direita para a pesquisa no conteúdo do documento			
5.2.6	Deve proporcionar a pesquisa por proximidade, isto é, que uma palavra apareça no conteúdo do documento a uma distância máxima de outra			
5.2.7	Deve permitir que os usuários possam armazenar pesquisas para reutilização posterior			
5.2.8	Deve permitir que os usuários possam refinar pesquisas já realizadas			
5.2.9	Quando o órgão ou entidade utilizar vocabulário controlado, um Sistema deve ser capaz de realizar pesquisa dos documentos por meios de navegação desse instrumento			

5.2.10	Deve permitir que usuários autorizados configurem e alterem os campos default de pesquisa de forma a definir metadados como campos de pesquisa			
5.3	Apresentação: visualização, impressão e emissão de som			
5.3.1	Deve permitir que os documentos apresentados em uma lista de resultados sejam selecionados e, em seguida, abertos por meio de um clique ou toque de tela ou acionamento de tecla			
5.3.2	Deve permitir a configuração de formato da lista de resultados de pesquisa pelos usuários ou Administrador, incluindo recursos e funções tais como:			
5.3.2.1	Seleção da ordem em que os resultados de pesquisa são apresentados			
5.3.2.2	Determinação do número de resultados de pesquisa exibidos na tela de cada vez			
5.2.2.3	Estabelecimento do número máximo de resultados para uma pesquisa			
5.2.2.4	Definição dos metadados que devem ser exibidos nas listas de resultados de pesquisa			
5.3.3	Deve fornecer recursos que permitam a um usuário "navegar" para o nível de agregação imediatamente superior ou inferior, como por exemplo:			
5.3.3.1	De um documento para o processo\dossiê em que está incluído			

5.3.3.2	De um processo\dossiê para os documentos nela incluídos			
5.3.3.3	De um processo\dossiê para a classe correspondente			
5.3.3.4	De uma classe para um processo\dossiê a ela relacionados			
5.3.4	Deve permitir que os metadados exibidos nas listas a que se referem os requisitos (5.3.9 e 5.3.10 da Tabela de Requisitos Obrigatórios) possam ser definidos pelo usuário			
5.3.5	Deve ser capaz de apresentar os documentos arquivísticos em outros formatos além do nativo, tais como:	No que se refere a interoperalidade com outros Sistemas, ver código 10 Interoperabilidade		
5.3.5.1	Formato XML adequado para publicação			
5.3.5.2	Formato HTML adequado para publicação			
5.3.5.3	Formato aprovado por organismos padronizadores na sua esfera de competência			
5.3.6	Deve permitir que o Administrador determine que todas as cópias em papel de documentos sejam impressas junto com metadados pré-selecionados			
6	Segurança			
6.1	Cópias de segurança			
6.1.1	As mídias removíveis devem ter cópias em suportes equivalentes e armazenadas			

	off-site			
6.1.2	Os discos rígidos devem ter cópias de segurança armazenadas em pelo menos dois locais diferentes e fisicamente distantes			
6.1.3	Deve ser capaz de agendar automaticamente as cópias de segurança com periodicidade estipulada pelo Administrador. Deve permitir cópias incrementais ou completas			
6.1.4	Deve dispor de mecanismos de assinatura digital das cópias de segurança e integridade dos dados e a identificação do responsável pelo procedimento	As assinaturas digitais possibilitam a verificação de integridade inclusive em mídias que estejam off-site. Tais verificações podem ser realizadas sem o auxílio do Sistema		
6.1.5	Dados críticos de configuração e controle do Sistema operacional e do gerenciados do banco de dados devem ser especialmente protegidos. Mecanismos especiais de cópias de segurança deverão ser previstos para dados críticos			
6.1.6	Trilhas de auditoria devem ser copiadas com frequência, prevendo-se cópias a serem armazenadas em pelo menos um local off-site			
6.2	Controle de acesso			

6.2.1	As credenciais de autenticação só poderão ser alteradas pelo usuário proprietário ou pelo Administrador, com a anuência do proprietário, em conformidade com a política de segurança		Credenciais de autenticação	Autentica o usuário no sistema. Pode ser senha, biometria, certificado digital e chave privada
6.2.2	Se o usuário solicitar o acesso ou pesquisa de um documento arquivístico ou volume específicos aos quais não tenha o direito de acesso, o Sistema deve fornecer uma das seguintes respostas (estabelecidas durante a configuração):	Essas opções são apresentadas em ordem crescente de segurança. O requisito da terceira opção (isto é, a mais rigorosa) implica que um Sistema terá de excluir esses documentos de qualquer listagem de resultados de uma pesquisa. Esse procedimento é normalmente adequado para documentos que requeiram elevados graus de segurança e sigilo. O Sistema deve ser capaz de registrar e informar tentativas indevidas de acesso. Este requisito se aplica tanto em pesquisa em metadados quanto a pesquisa no próprio documento (texto livre)		
6.2.2.1	Mostrar a classificação e os metadados do documento			

6.2.2.2	Demonstrar a existência do documento, mas não a respectiva classificação nem outro metadado			
6.2.2.3	Não mostrar qualquer informação do documento, nem indicar a existência do mesmo			
6.2.3	Deve implementar imediatamente alterações ou revogações dos atributos de segurança de usuários e de documentos digitais			
6.2.4	Deve oferecer ferramentas de aumento de produtividade ao Administrador, tais como, realização de operações sobre lotes ou grupos de usuários e lotes de documentos digitais, agenda de tarefas, análises de trilhas e geração de alarmes			
6.2.5	Quando um Sistema controlar o acesso por grupos de usuários, papéis de usuários e usuários individuais, deve obedecer a uma hierarquia de permissões preestabelecida na política de segurança			
6.3	Classificação da segurança da informação quanto a categoria e ao grau de sigilo			
6.3.1	Deve garantir que não haja ambiguidade na associação entre as marcações de grau de sigilo e os outros atributos de segurança (permissões) do documento importado			
6.3.2	Deve permitir o armazenamento dos documentos sigilosos em meios físicos ou lógicos distintos			

6.4	Trilhas de auditoria			
6.4.1	Deve permitir apenas ao Administrador e ao auditor a leitura das trilhas de auditoria			
6.4.2	Deve possuir mecanismos para a realização de buscas nos eventos das trilhas de auditoria	Para facilidade de relatório, os resultados podem ser apresentados ordenados, mas esta ordenação não pode alterar os dados contidos na trilha		
6.4.3	Deve ser capaz de gerar um alarme, para os admininstradores apropriados, se o tamanho da trilha de auditoria exceder um limite preestabelecido	Esse alarme deve ser usado para indicar a proximidade do esgotamento de espaço reservado a trilha de auditoria		
6.4.4	Quando o espaço de armazenamento da trilha de auditoria atingir o limite preestabelecido, o Sistema deve permitir somente operações auditáveis originadas por administradores	Todas as outras operações estariam bloqueadas até liberação pelo Administrador		
6.4.5	Deve ser capaz de aplicar um conjunto de regras na monitoração de eventos auditados e, com base nessas regras, indicar a possível violação da segurança			
6.4.6	Deve garantir pelo menos as seguintes regras para a monitoração dos eventos auditados:			
6.4.6.1	Acumulação de um número pré-determinado de tentativas consecutivas de login com erro (autenticação mal sucedida), conforme especificado pela política de segurança			

6.4.6.2	Ocorrência de vários login simultâneos do mesmo usuário em locais (computadores) diferentes			
6.4.6.3	Login do usuário fora do horário autorizado, após logoff no período normal			
6.5	Assinaturas digitais			
6.5.1	O Sistema deve ser capaz de garantir a origem e a integridade dos documentos com assinatura digital			
6.5.2	O Sistema deve ser capaz de armazenar juntamente com o documento as seguintes informações de certificação:			
6.5.2.1	Assinatura digital			
6.5.2.2	Certificado digital (cadeia de certificação) usado na verificação da assinatura			
6.5.2.3	Lista de certificados revogados - LCR			
6.5.3	Deve ser capaz de receber atualizações tecnológicas quanto a plataforma criptográfica de assinatura digital			
6.5.4	Deve destruir, ou tornar indisponível, as chaves de criptografia quando estas estiverem contidas em listas de certificados revogados (LCR)			
6.5.5	Deve ter acesso a relógios e carimbador de tempo confiáveis para o seu próprio uso	O relógio gerador de selo de tempo deve ser sincronizado com o Observatório Nacional (Divisão do Serviço da Hora, disponível em: http://pcdsh01.on.br/)		

6.6	Criptografia			
6.6.1	Deve poder assegurar a captura de documentos cifrados, diretamente de uma aplicação de software que disponha da funcionalidade da cifração			
6.6.2	Deve possuir uma arquitetura capaz de receber atualizações tecnológicas quanto a plataforma criptográfica			
6.7	Marcas d'água digitais			
6.7.1	Deve possuir uma arquitetura capaz de receber atualizações tecnológicas quanto a plataforma de geração e de detecção de marca d'água digital			
6.8	Acompanhamento de transferência			
6.8.1	Deve ser capaz de manter, para cada documento, o histórico das movimentações e transferências de mídia sofridas por aquele documento			
6.9	Autoproteção			
6.9.1	Deve fazer a verificação de vírus ou pragas antes da efetiva captura			
6.9.2	Deve ter dispositivos e procedimentos que reduzam as possibilidades de erros, falhas e descontinuidades no seu funcionamento que causem danos ou perdas aos documentos arquivísticos digitais			
6.9.3	Deve garantir que os dados de segurança, quando replicados, sejam consistentes	Permissões de controle de acesso, chaves criptográficas e parâmetros de algoritmos criptográficos são		

		exemplos de dados de segurança		
6.9.4	Deve detectar o reenvio de dados de autenticação e segurança de um usuário, sem conhecimento deste. O evento deve ser registrado nas trilhas, cancelando a comunicação com o Sistema remoto\usuário e considerando o usuário fora do Sistema			
6.10	Alterar, apagar e truncar documentos arquivísticos digitais			
6.10.1	Para evitar erros irrecuperáveis, deve inibir a eliminação (permanente ou lógica) de grupos ou lotes de documentos fora do processo regular de eliminação prevista na Tabela de Temporalidade de Documentos			

6.10.2	Deve dispor de funções de ocultação de informação sigilosa contida na cópia truncada do documento, permitindo o seguinte:	Se o Sistema não fornecer diretamente esses recursos, tem que permitir que outros pacotes de software os proporcionem. É essencial que quando os recursos para truncar documento forem empregados, nenhuma informação retirada ou ocultada seja passível de visualização da cópia truncada na tela, nem quando imprenssa ou reproduzida por meios audiovisuais, independentemente da utilização de quaisquer recursos, tais como rotação, variação local ou qualquer outra manifestação		
6.10.2.1	Retirada de páginas de um documento			
6.10.2.2	Adição de retângulos opacos para ocultar nomes ou palavras sensíveis			
6.10.2.3	Quaisquer outros recursos necessários para formatos de vídeo ou de áudio, caso existam			
6.10.3	Deve registrar no documento original uma transferência cruzada a uma cópia truncada dele efetuada			

7	Armazenamento			
7.1	Durabilidade			
7.1.1	Deve utilizar preferencialmente dispositivos e padrões de armazenamento maduros, estáveis no mercado e amplamente disponíveis	Um Sistema deve utilizar preferencialmente padrões abertos de armazenamento (como por exemplo: ISO 9660:1999 - definição do formato de Sistemas de arquivos para CR-Rom). A escolha dos dispositivos deve contemplar padrões estáveis de mercado e fornecedores consolidados		
7.1.2	Para as memórias secundárias e terciárias, o Sistema deve manter estatísticas da durabilidade efetivamente observada			
7.1.3	No caso de uso de fitas magnéticas, o mecanismo de cópias de segurança provido pelo Sistema deve proporcionar meios para que o item 8.2.2 possa ser implementado automaticamente, integrado a ação de cópias de segurança			
7.1.4	O acesso as informações armazenadas em memória terciária deve ser efetuado preferencialmente mediante uso de rede de dados	O objetivo é minimizar o acesso físico as mídias, visando diminuição do desgaste. A manipulação direta das mídias deverá ser restrita aos administradores do Sistema e não aos usuários comuns		

7.2	Capacidade			
7.2.1	Deve permitir ao administrador configurar os limites de capacidade de armazenamento dos diversos dispositivos			
7.2.2	Deve oferecer facilidade ao Administrador para a monitoração da capacidade de armazenamento	Esse controle indica, por exemplo, capacidade utilizada, capacidade disponível e taxa de ocupação. Tais informações são úteis para subsidiar ações de expansão em tempo hábil		
7.2.3	Deve informar automaticamente ao Administrador quando os dispositvos de armazenamento on line atingirem níveis críticos de ocupação			
7.2.4	Deve manter estatísticas de taxa de crescimento de utilização de memória secundária e terciária para informar ao administrador previsões de exaustão de recursos	Este tipo de estimativa possibilita ao administrador antecipar ações de expansão antes que a utilização atinja níveis críticos		
7.3	Efetividade de armazenamento			
7.3.1	Os dispositivos de armazenamento de um Sistema devem suportar métodos de detecção de erros para leitura e escrita de dados			
7.3.2	A infraestrutura de um Sistema deve prever o uso de técnicas para garantir maior confiabilidade e desempenho. As técnicas recomendadas incluem:			

7.3.2.1	Espelhamento (mirroring) nas memórias secundárias para maior confiabilidade			
7.3.2.2	Partição de dados (data stripping) nas memórias secundárias para maior desempenho			
8	Preservação			
8.1	Aspectos físicos			
8.1.2	Deve permitir ao Administrador especificar a vida útil prevista\pretendida dos suportes		Características do documento digital	Registra informações: suporte, vida útil do suporte, tamanho, formato, aplicação utilizada para a criação do documento, nome original, ambiente de criação, informação sobre assinatura digital, relação entre os objetivos
8.1.3	Deve informar, automaticamente, quais são os suportes que se encontram próximos do fim de sua vida útil		Características do documento digital	Registra informações: suporte, vida útil do suporte, tamanho, formato, aplicação utilizada para a criação do documento, nome original, ambiente de criação, informação sobre assinatura digital, relação entre os objetivos
8.2	Aspectos lógicos			

8.2.1	Deve informar os resultados da verificação periódica dos dados armazenados, incluindo os erros detectados, bem como as substituições e as correções de dados realizadas			
8.2.2	Deve manter um histórico dos resultados da verificação periódica dos dados armazenados			
8.3	Aspectos gerais			
8.3.1	Deve utilizar suportes de armazenamento e de recursos de hardware e software que sejam maduros, estáveis no mercado e amplamento disponíveis			
8.3.2	Deve utilizar normas amplamente aceitas, descritas em especificações abertas e disponíveis publicamente, no que se refere as estruturas para codificação, armazenamento e banco de dados			
8.3.3	Deve evitar o uso de estruturas proprietárias para codificação, armazenamento ou banco de dados. Caso venha a utilizá-las, estas devem estar plenamente documentadas e a documentação disponível para o administrador			
9	Usabilidade			
9.1.1	A ajuda on line fornecida pelo Sistema deve ser vinculada a função ou tarefa executada, em todo o Sistema	Exemplo: quando se está executando uma operação de edição, uma vez acionada a ajuda, ela deve remeter para o tópico da		

		ajuda edição		
9.1.2	O Sistema deve permitir a personalização de conteúdo de ajuda on line por adição de texto ou edição de texto existente	Exemplo: o responsável pela administração de conteúdo da ajuda pode adicionar esclarecimentos ou alterar o conteúdo das descrições, de modo a facilitar o entendimento das funções		
9.1.3	Toda mensagem de erro produzida pelo Sistema deve ser clara e significativa, de modo a permitir que o usuário possa recuperar-se do erro ou cancelar a operação			
9.1.4	A interface do Sistema deve seguir padrões pré-estabelecidos e consolidados como boas práticas de projeto gráfico	Normas ou regras de interface podem ser relativas a utilização de padrão de identidade visual (ligada a "marca" da instituição ou alguma legislação especifica, bem como a utilização de guias de estilo para implementação e padronização da interface		

9.1.5	Deve empregar um conjunto simples e consistente de regras de interface, privilegiando a facilidade de aprendizado de operações pelos seus usuários	O uso de um conjunto de regras consistentes com o ambiente operacional em que o Sistema será executado permite que ele apresente menus, comandos e outras facilidades consistentes em toda aplicação. Essas regras de interface, quando compatíveis com outras aplicações principais já instaladas, levam a padronização da terminologia utilizada para funções, rótulos e ações consistentes em toda a aplicação		
9.1.6	A interface de visualização dos documentos arquivísticos deve fornecer o recurso de arrastar e soltar, se apropriado no ambiente operacional do Sistema			
9.1.7	Deve permitir que a sua estrutura de classes e processos\dossiês possa ser visualizada em diferentes formas de apresentação			
9.1.8	Deve ser possível personalizar a interface gráfica com o usuário de um Sistema. A personalização deve incluir pelo menos as seguintes possibilidades:			
9.1.8.1	Conteúdo de menus			

9.1.8.2	Formatos de telas			
9.1.8.3	Utilização de teclas de função			
9.1.8.4	Alteração de cores, fontes e tamanhos de fontes em telas e janelas			
9.1.9	Sempre que o Sistema utilizar janelas pop-up e barras de ferramentas, deve-se permitir ao usuário a possibilidade de configuração e de habilitar\desabilitar esse tipo de recurso	Porém, de forma a não infrigir a recomendação de uso de um conjunto simples e consistente de regras de interface		
9.1.10	Sempre que o Sistema permitir o uso de janelas, ele deve permitir sua movimentação, redimensionamento e gravação das modificações da aparência, de forma a permitir a personalização por perfil de usuário			
9.1.11	Deve permitir a seleção de avisos sonoros e a personalização de tom e volume, bem como a gravação dessas escolhas no p do usuário			
9.1.12	Deve permitir a gravação de opções default para entrada de dados de configuração:			
9.1.12.1	Valores de variáveis definidas pelo usuário			
9.1.12.2	Valores iguais aos de um item anterior			
9.1.12.3	Valores que possam ser selecionados de uma lista configurável			
9.1.12.4	Valores derivados do contexto, como data, referência do documento, identificador do usuário			

9.1.12.5	Valores pré-definidos por Administrador (para campos de metadados como, por exemplo, o nome da organização que está utilizando o Sistema)			
9.1.13	A interface de um Sistema com usuário deve ser apropriada para adaptações e personalizações que permitam a sua utilização por usuários com necessidades especiais. Essas adaptações e personalizações devem ser compatíveis com software especializado que possa vir a ser acoplado (por exemplo, leitores de telas para cegos), bem como seguir orientações especificas de acessibilidade de interface	Para ambientes e sítios apoiados na web é importante seguir orientações especificas de acessibilidade. É desejável que o padrão seguido possa ser verificado através da aplicação de uma validação manual ou automática, de preferência visando a obtenção de certificação de acessibilidade		
9.1.14	Deve permitir a realização de transações ou tarefas mais frequentemente executadas com um pequeno número de repetições (por exemplo, cliques de mouse) e sem mudanças excessivas de contexto			
9.1.15	Deve estar fortemente integrado com o Sistema de correio eletrônico da organização, de forma a permitir a geração de mensagens com possibilidade de manipular documentos digitais, sem necessidade de sair do Sistema	Esse requisito deve estar de acordo com as normas de segurança		

9.1.16	No caso de integração do Sistema com o correio eletrônico, deve ser possível fazer referências a documentos arquivísticos sem necessidade de envio de cópias adicionais			
9.1.17	Deve possuir integração com o Sistema padrão de edição de documentos, de modo que possa fazer uso da facilidade de gravação			
9.1.18	Deve permitir a definição e utilização de referências cruzadas entre documentos arquivísticos digitais correlacionados, permitindo uma fácil navegação entre eles, inclusive com o uso de hiperlinks		Relação com outros documentos	Registro de relações significantes do documento com outros pelo fato de registrarem a mesma atividade, pessoa, ou situação ou diferentes níveis de agregação (processo, volume e documento) ou diferentes manifestações do mesmo documento em diversos formatos
9.1.19	Deve fornecer para os usuários finais e administradores funções intuitivas e fáceis de usar, que requeira poucas ações para completar uma tarefa padrão. Particulamente em operação normal, o Sistema deve ser capaz de:			
9.1.19.1	Capturar e declarar um documento arquivístico com, no máximo, três cliques de mouse ou acionamentos de telas			

9.1.19.2	Apresentar todos os elementos de metados obrigatórios para a captura do documento com mínima demanda para o usuário			
9.1.19.3	Apresentar o conteúdo de um documento arquivístico, a partir de uma lista de pesquisa, com no máximo três cliques de mouse ou acionamentos de telas			
9.1.19.4	Apresentar os metadados de um documento arquivístico com no máximo, três cliques de mouse ou acionamentos de tarefas			
9.1.20	Deve levar em consideração as condições de operação como ruído, luminosidade, necessidade de rapidez na conclusão da tarefa, necessidades específicas para dispositivos móveis, ambiente desktop\web e necessidades de instalação automática, para configurar as formas de interação com o usuário	Exemplo: não se deve utilizar menus audíveis em ambientes que apresentam alto volume de ruídos na proximidade dos terminais de usuários		
10	Interoperabilidade			
10.1	Deve ser capaz de interoperar com outros Sistemas, permitindo pelo menos consulta, recuperação, importação e exportação de documentos e seus metadados	As operações de interoperabilidade devem respeitar a legislação vigente e a política de segurança		
10.2	Deve ser capaz de interoperar com outros Sistemas através de padrões abertos de interoperabilidade	Exemplo: padrões abertos como os estabelecidos pela e-PING, XML e Dublin Core		
11	Desempenho e escalabilidade			

11.1	Deve manter estatísticas dos tempos de atendimento, discriminados por tipo de operação			
11.2	Deve ser escalável, a fim de permitir adaptação a organizações de diferentes tamanhos e complexidades			
11.3	Deve fornecer evidências de grau de escalabilidade ao longo do tempo. Avaliações quantitativas devem incluir:			
11.3.1	O número máximo de sites remotos suportados com desempenho adequado			
11.3.2	O tamanho máximo do repositório, expresso em Gigabytes ou Terabytes, que pode ser suportado com desempenho adequado			
11.3.3	O número máximo de usuários simultâneos que possam ser atendidos com desempenho adequado			
11.3.4	A sobrecarga administrativa prevista para um período de cinco anos, permitindo crescimento do número de usuários e da quantidade de registros			
11.3.5	A quantidade de reconfigurações e de indisponibilidades previstas para um período de cinco anos, permitindo o crescimento do número de usuários e da quantidade de registros			

11.3.6	A quantidade de reconfigurações e de indisponibilidades previstas para um período de cinco anos, permitindo mudanças substanciais na estrutura da organização, mudanças nos esquemas de classificação e mudanças na administração de usuários			