



InterPARES 3 Project

International Research on Permanent Authentic Records in Electronic Systems

TEAM Brazil

Título: Case Study BR09 – Departamento de Gestão do Sistema de Arquivos do Estado de São Paulo (DGSAESP) – Sistema Informatizado Unificado de Gestão Arquivística de Documentos e Informações (SPdoc): Relatório final.

Status: Final (público).

Versão: 4.

Data de submissão: Dezembro de 2011.

Data da última revisão: Fevereiro de 2012.

Autor: Projeto InterPARES 3, TEAM Brasil.

Redator(es): Ieda Pimenta Bernardes
Elisangela Mendes Queiroz
Josival Soares de Souza
Arquivo Público do Estado de São Paulo

Margareth da Silva
Universidade Federal Fluminense

Project Component: Pesquisa.

URL:

Controle do documento

Histórico de versões			
<u>Versão</u>	<u>Data</u>	<u>Responsável</u>	<u>Notas</u>
1	22/12/2011	E. Queiroz	Versão apresentada à coinvestigadora Margareth da Silva, orientadora do estudo de caso.
2	6/1/2012	M. Silva	Versão revista pela coinvestigadora Margareth da Silva, orientadora do estudo de caso.
3	11/1/2012	C. Cobério C. Prado D. Santos L. Estrella	Versão final apresentada ao TEAM Brasil.
4	15/2/2012	E. Queiroz	Versão revista segundo observações do TEAM Brasil.

Sumário

A. Linhas gerais.....	1
B. Metodologia aplicada.....	1
C. Descrição do contexto.....	2
Contexto de proveniência.....	2
Contexto jurídico-administrativo.....	4
Contexto de procedimentos.....	4
Contexto documental.....	5
Contexto tecnológico.....	10
D. Respostas narrativas a perguntas pertinentes para os pesquisadores.....	10
E. Respostas narrativas a questões de pesquisa pertinentes ao projeto.....	14
F. Referências.....	17
G. Descobertas, recomendações e produtos.....	20
Apêndice 1.....	21
Apêndice 2.....	103

Relatório do estudo de caso

A. Linhas gerais

O Estudo de Caso BR09 apresenta uma peculiaridade em relação aos demais estudos desenvolvidos no âmbito do TEAM Brasil. Ao invés de tratar de um documento digital específico, este estudo analisa o Sistema Informatizado Unificado de Gestão Arquivística e de Informações (SPdoc), que deverá ser o principal indutor da implantação da gestão documental da administração pública do Estado de São Paulo. Esta é outra particularidade do Estudo de Caso BR09, pois o SPdoc não vem sendo desenvolvido para atender somente a uma instituição, mas a toda a administração pública estadual de São Paulo, com cerca de 13 mil unidades produtoras de documentos¹ espalhadas entre 25 secretarias e 64 outras entidades, dentre as quais, sociedades de economia mista, empresas públicas, fundações e autarquias, além das organizações sociais autônomas.

O SPdoc é um sistema unificado e informatizado de gestão arquivística de documentos que vem sendo desenvolvido desde 2004, conforme requisitos, padrões, normas e procedimentos arquivísticos que constituem a política estadual de arquivos, formulada e implementada pelo Arquivo Público do Estado de São Paulo, por meio da Instrução Normativa APE/SAESP – 1, de 10 de março de 2009. Na sua fase atual de desenvolvimento, o SPdoc opera, basicamente, como um sistema referencial de documentos convencionais produzidos em quatro secretarias de estado, onde o sistema funciona em caráter experimental². Pretende-se, contudo, que o SPdoc funcione plenamente, isto é, seja capaz de promover, na administração pública paulista, a gestão arquivística de documentos convencionais e digitais, desde sua produção até sua destinação final, quando se decide por sua eliminação ou preservação.

Pensando a implantação progressiva e o aperfeiçoamento contínuo do SPdoc, foi criado, em 2010, o Comitê Gestor do SPdoc, que está sob a autoridade do Departamento de Gestão do Sistema de Arquivos do Estado de São Paulo (DGSAESP). O Comitê Gestor é um organismo colegiado formado por representantes da administração pública paulista e coordenado pelo Arquivo Público do Estado de São Paulo, unidade da Casa Civil e órgão central do Sistema de Arquivos do Estado de São Paulo (SAESP), cujo funcionamento é administrado pelo DGSAESP.

Tendo em vista a sua função no Comitê Gestor do SPdoc, o DGSAESP identificou, no Projeto InterPARES 3, a possibilidade singular de aprimorar o SPdoc segundo os avanços mais recentes das pesquisas sobre a gestão de documentos digitais. Para além disso, o DGSAESP busca contribuir com a experiência do Arquivo Público do Estado de São Paulo para o desenvolvimento de conhecimento teórico-metodológico e prático sobre documentos arquivísticos autênticos em sistemas informatizados, objetivo do Projeto InterPARES.

B. Metodologia aplicada

Para a compreensão do SPdoc e de seu Comitê Gestor, o modelo de análise contextual proposto pelo IP3 foi fundamental. A legislação pertinente encontra-se publicada, evidenciando somente a necessidade de formar um compêndio mais amplo dos dispositivos legais indiretos que impactam no SPdoc, como, por exemplo, os que se referem à restrição de acesso e ao sigilo

¹ Veja o item “Contexto documental”, na seção “C” deste relatório.

² Casa Civil, Secretaria da Cultura, Secretaria da Gestão Pública e Secretaria dos Direitos da Pessoa com Deficiência.

de informações. Dados sobre a administração pública paulista foram encontrados nas publicações da Fundação do Desenvolvimento Administrativo, do Governo do Estado de São Paulo. Os instrumentos convencionais de gestão documental do SAESP são todos de fácil acesso, pois são produtos formulados pelo próprio DGSAESP, tais como os planos de classificação, as tabelas de temporalidade, as instruções normativas, os manuais etc.

Porém, o maior obstáculo encontrado durante a pesquisa foi a obtenção de informações sobre a estrutura tecnológica do SPdoc, porque a Companhia de Processamento de Dados do Estado de São Paulo (PRODESP), vinculada à Secretaria de Gestão Pública e responsável pelo desenvolvimento técnico do SPdoc, é uma sociedade de economia mista³, com quadro de funcionários e estrutura administrativa independentes. O fator que facilitou a disponibilização dos dados da estrutura tecnológica do SPdoc, dentro do possível, foi a presença, na equipe do estudo de caso, de funcionários do DGSAESP que também participam do núcleo de apoio ao Comitê Gestor, bem como a colaboração de servidores públicos que estão envolvidos no desenvolvimento do SPdoc desde 2004.

A aplicação do “Modelo para análise contextual” e das “Questões a serem respondidas pelos pesquisadores com relação aos estudos de caso de sistemas de gestão de documentos” auxiliou na ampliação do conhecimento sobre o SPdoc, permitindo identificar algumas lacunas e possíveis aperfeiçoamentos necessários ao bom funcionamento do sistema. Tais perspectivas são apresentadas no plano de ação esboçado.

C. Descrição do contexto

Contexto de proveniência

A criação do SPdoc foi motivada por uma antiga necessidade da administração pública do Estado de São Paulo de estabelecer um sistema unificado que controlasse a tramitação de todos os documentos produzidos em seus órgãos. Contudo, o SPdoc não foi projetado para ser apenas um sistema de registro de protocolo.

No período anterior à existência de seu Comitê Gestor, o SPdoc começou a ser desenvolvido no âmbito de um dos grupos técnicos do Comitê de Qualidade da Gestão Pública da Casa Civil⁴. Nos anos seguintes a sua instituição, por meio da Resolução CC-33 (8/4/2004), e a sua reestruturação, por meio da Resolução CC-10 (25/2/2005), permitiu-se entrada do Arquivo Público do Estado nesse grupo técnico, desde quando vem sendo desenvolvido para fazer a gestão arquivística informatizada dos documentos públicos estaduais – convencionais e digitais – do momento de sua produção até a sua destinação final: eliminação ou preservação.

Em 2007, a Secretaria de Gestão Pública assumiu o SPdoc, implantando-o, experimentalmente, em seis secretarias de estado⁵.

Em 25 de fevereiro de 2010, o Decreto n.º 55.476⁶ instituiu, na Casa Civil, um comitê gestor para orientar o desenvolvimento, a implementação e o aperfeiçoamento contínuo do SPdoc, de

³ Empresas de economia mista são aquelas que reúnem capital público e privado.

⁴ Comitê de Qualidade da Gestão Pública (CQGP) é um órgão deliberativo, normativo, de assessoramento e de representação nos assuntos de qualidade da gestão pública, que reúne o Secretário-Chefe da Casa Civil, o Secretário de Planejamento e Desenvolvimento Regional, o Secretário da Fazenda, o Secretário da Gestão Pública, o Procurador Geral do Estado e o Secretário Executivo, designado pelo Secretário-Chefe da Casa Civil. Para mais informações, ver: <http://www.cqgp.sp.gov.br>.

⁵ O SPdoc foi implantado experimentalmente nas seguintes secretarias: Casa Civil, Comunicações, Cultura, Direitos da Pessoa com Deficiência, Gestão Pública e Relações Institucionais. É importante observar que, com a reestruturação do governo paulista, em 2011, as secretarias de Comunicações e de Relações Institucionais foram extintas.

acordo com a política estadual de arquivos. Enquanto responsável pelo SPdoc, cabe ao seu Comitê Gestor⁷:

- desenvolver ações integradas entre a Casa Civil e a Secretaria de Gestão Pública nos assuntos afetos ao uso da tecnologia da informação nas atividades de protocolo e arquivo;
- planejar, coordenar e acompanhar a implementação gradual e progressiva do sistema;
- elaborar e propor diretrizes e procedimentos a serem adotados para a contínua manutenção e aprimoramento do sistema;
- planejar os recursos necessários ao pleno funcionamento, manutenção e aprimoramento do sistema;
- manifestar-se conclusivamente a respeito das formulações apresentadas por órgãos públicos a respeito do funcionamento do sistema;
- elaborar um projeto de capacitação de pessoal referente aos procedimentos de arquivo e protocolo e à operação do sistema, orientando sua execução;
- planejar e manter um serviço de orientação aos usuários do sistema;
- atualizar, ajustar e revisar, de forma permanente, os procedimentos e as práticas estabelecidas, garantindo sua compatibilidade;
- promover a atualização constante do sistema e a sua conformidade com a política estadual de arquivos e de segurança da informação;
- elaborar seu regimento interno;
- propor a definição de comissões técnicas, de acordo com as necessidades dos trabalhos;
- definir requisitos, metadados, formatos, padrões, normas e procedimentos arquivísticos a serem cumpridos pelo sistema;
- orientar o desenvolvimento de módulos específicos do sistema, visando à inclusão de documentos digitais e à preservação de documentos de guarda permanente;
- administrar, no sistema, a inclusão, alteração ou exclusão de funcionalidades arquivísticas;
- orientar a definição de critérios para acesso e sigilo de documentos públicos estaduais;
- estimular a participação da gestão municipal na implementação de políticas de arquivo e sua adesão ao sistema;
- homologar o sistema e as melhorias incorporadas;
- planejar a infraestrutura e a atualização permanente do ambiente tecnológico;
- avaliar o desempenho do sistema e incorporar melhorias de forma contínua;
- definir estratégias, procedimentos e técnicas de preservação digital;
- instituir procedimentos de segurança;
- elaborar políticas para assegurar a interoperabilidade do sistema, bem como a migração de dados de sistemas legados; e
- elaborar e manter atualizada a documentação de requisitos do sistema, bem como seus manuais básicos.

Para além dessas atribuições, o Comitê Gestor do SPdoc define a utilização dos recursos financeiros destinados ao sistema pela lei orçamentária do Estado de São Paulo⁸.

⁶ O Decreto nº 55.479, de 25 de fevereiro de 2010, que institui, na Casa Civil, o Comitê Gestor do SPdoc, foi alterado pelo Decreto nº 56.260, de 6 de outubro de 2010.

⁷ De acordo com o artigo 4º do Decreto nº 55.479, de 25 de fevereiro de 2010, e o artigo 2º da Resolução Casa Civil n.º 43, de 6 de outubro de 2010, que aprova o Regimento Interno do Comitê Gestor do SPdoc.

⁸ A Lei Orçamentária (LDO) calcula, anualmente, a receita e fixa as despesas do Estado de São Paulo.

Contexto jurídico-administrativo

O Comitê Gestor do SPdoc é um órgão colegiado estabelecido no Gabinete do Secretário-Chefe da Casa Civil e regido pelos decretos n.º 55.479, de 25 de fevereiro de 2010, e n.º 56.260, de 6 de outubro de 2010, e por seu regimento interno aprovado pela Resolução da Casa Civil n.º 43, de 6 de outubro de 2010.

O Comitê Gestor do SPdoc é composto por :

- três representantes da Secretaria da Casa Civil (o coordenador do Arquivo Público do Estado, o diretor do DGSAESP e um servidor público, de livre-escolha do Secretário-Chefe da Casa Civil);
- dois representantes da Secretaria de Gestão Pública (um deles da Unidade de Tecnologia da Informação e Comunicações); e
- um representante de cada um dos seguintes órgãos e entidades: Secretaria de Planejamento e Desenvolvimento Regional, Procuradoria Geral do Estado e PRODESP.

O Comitê Gestor do SPdoc é assessorado por:

- um núcleo de apoio, de responsabilidade do DGSAESP, composto por 9 servidores públicos desse departamento e um da Casa Civil; e
- uma comissão técnica de documentos digitais e uma comissão técnica de implementação e treinamento – outras comissões técnicas podem ser constituídas de acordo com as necessidades de trabalho.

Cada componente do Comitê Gestor exerce uma função específica.

O Arquivo Público do Estado, órgão central do SAESP, é responsável pela formulação e implementação da política estadual de arquivos, e seu dirigente coordena os trabalhos do Comitê Gestor do SPdoc.

O DGSAESP define os requisitos, os padrões, as normas e os procedimentos arquivísticos que asseguram, ao SPdoc, consistência, segurança e confiabilidade. O DGSAESP é, portanto, a autoridade arquivística do SPdoc, enquanto o Comitê Gestor funciona como sua autoridade administrativa.

A PRODESP, sociedade de economia mista vinculada à Secretaria de Gestão Pública, é a empresa contratada para o desenvolvimento técnico, a manutenção e a infraestrutura do SPdoc. Suas relações com o Comitê Gestor do SPdoc são regidas por um contrato específico.

Os representantes da Casa Civil, da Secretaria de Gestão Pública, da Secretaria do Planejamento e Desenvolvimento Regional e da Procuradoria Geral do Estado atuam em suas áreas, no cumprimento de atribuições do Comitê Gestor do SPdoc.

O núcleo de apoio e as comissões técnicas dão, respectivamente, apoio administrativo e técnico ao Comitê Gestor.

Contexto de procedimentos

Na administração pública paulista, a gestão de documentos é definida pela política estadual de arquivos, que consiste em um conjunto de diretrizes, normas e procedimentos que orientam a execução das atividades dos arquivos e protocolos dos órgãos e entidades que integram o SAESP.

O SAESP existe desde 1984, quando foi instituído pelo Decreto n.º 22.789, de 19 de outubro de 1984, tendo como órgão central o Arquivo Público do Estado e como coordenador de seu funcionamento o DGSAESP. O SAESP foi criado com o objetivo de assegurar e agilizar o acesso às informações e aos documentos públicos, preservar os documentos que integram o patrimônio documental do Estado e eliminar, com critério, os documentos desprovidos de valor

que justifique a sua guarda. Para tanto, os órgãos e entidades integrantes do SAESP, orientados pelo DGSAESP, realizam uma série de operações técnicas, em parte, automatizadas pelo SPdoc em seu estágio atual de desenvolvimento, e que, futuramente, serão totalmente realizadas pelo sistema, salvo algumas exceções⁹.

Ao apresentarmos, aqui, o programa de gestão de documentos da administração pública do Estado de São Paulo, não podemos deixar de mencionar o Programa de Gestão Documental Itinerante (PGDI) como uma das ações realizadas pelo DGSAESP com o intuito de possibilitar a implantação do SPdoc. O PGDI consiste numa força-tarefa do departamento, iniciada em 2011, para promover, inicialmente, nos órgãos da administração direta integrantes do SAESP, a elaboração de planos de classificação e tabelas de temporalidade das atividades-fim, bem como a avaliação da massa documental acumulada.

Contexto de documental

O SPdoc é um sistema unificado e informatizado de gestão arquivística de documentos convencionais e digitais. Este sistema vem sendo desenvolvido conforme requisitos, padrões, normas e procedimentos arquivísticos estabelecidos pelo DGSAESP, com o objetivo de padronizar a gestão documental da administração pública paulista.

Estima-se que, em 2011, existam cerca de 13 mil unidades produtoras de documentos no Estado de São Paulo, espalhadas entre órgãos da administração pública direta (secretarias de Estado) e entidades da administração pública indireta (sociedades de economia mista, empresas públicas, fundações, autarquias e organizações sociais autônomas)¹⁰. A implantação do Spdoc, nesta enorme estrutura, será realizada gradualmente, sob a coordenação do Comitê Gestor do SPdoc, e contará com a colaboração dos dirigentes das áreas de Tecnologia da Informação e das comissões de avaliação de documentos de arquivo¹¹ dos mencionados órgãos e entidades.

Em sua fase atual, o SPdoc funciona, experimentalmente, em quatro secretarias de estado, fazendo a gestão arquivística de documentos convencionais, ou seja, em papel. Desde a transferência do SPdoc da Secretaria de Gestão Pública para a Secretaria da Casa Civil, em 2010, o seu Comitê Gestor procura tomar as providências necessárias para que, futuramente, o sistema também seja capaz de produzir, gerir e preservar documentos arquivísticos digitais.

Dentre os procedimentos de arquivo e protocolo convencionais, listados abaixo, o SPdoc realiza total ou parcialmente aqueles que estão sublinhados:

- recebimento de documentos,
- registro de documentos,
- atuação,
- tramitação,
- despacho,

⁹ A criação, a forma, o conteúdo, a identidade, a organização e a manutenção dos documentos, no âmbito da administração pública do Estado de São Paulo, estão sujeitos à legislação arquivística nacional e estadual, em especial o Decreto n.º 54.276, de 27 de abril de 2009, que atribui ao Arquivo Público do Estado, enquanto órgão central do SAESP, a competência para definir requisitos, padrões, normas e procedimentos arquivísticos que orientem o desenvolvimento, a implementação e o aperfeiçoamento contínuo do SPdoc.

¹⁰ O cálculo estimado de unidades produtoras de documentos na administração pública paulista foi realizado, no âmbito do Projeto InterPARES, a partir do documento “Perfil da Administração Pública Paulista 2011”, elaborado pela Fundação do Desenvolvimento Administrativo (FUNDAPE).

¹¹ As comissões de avaliação de documentos de arquivo são grupos permanentes e multidisciplinares, constituídos por servidores públicos estaduais das áreas de administração geral e financeira, jurídica, de arquivo e de protocolo, e de demais áreas técnicas de atuação do órgão ou entidade da administração pública. Cabe às comissões: elaborar e aplicar os planos de classificação e tabelas de temporalidade de documentos; atuar como agentes multiplicadores das normas e procedimentos de gestão documental; orientar os procedimentos para eliminação, transferência ou recolhimento de documentos; e manter a interlocução permanente com o Departamento de Gestão do SAESP.

- juntada,
- desentranhamento,
- incorporação,
- desincorporação,
- apensamento,
- desapensamento,
- ordenação,
- acondicionamento,
- conservação,
- arquivamento e
- desarquivamento.

O SPdoc também incorpora, do sistema de gestão documental convencional, os seguintes procedimentos arquivísticos sublinhados abaixo, total ou parcialmente:

1. Avaliação e destinação da massa documental:

- aplicação das tabelas de temporalidade de documentos;
- oficialização das tabelas de temporalidade de documentos das atividades-fim;
- identificação e separação de documentos produzidos até 1940, para a guarda definitiva;
- guarda de documentos produzidos após de 1940, para que se cumpram prazos prescricionais e precautionais; e
- recolhimento ao Arquivo Público do Estado.

2. Conservação preventiva:

- controle ambiental,
- combate aos agentes biológicos,
- orientação sobre o manuseio dos documentos e
- estabilização dos documentos.

3. Eliminação de documentos de guarda temporária:

- consulta à Procuradoria Geral do Estado,
- seleção de amostragens,
- elaboração e aprovação da “Relação de eliminação de documentos”,
- publicação do “Edital de ciência de eliminação de documentos”,
- elaboração do “Termo de eliminação de documentos”,
- fragmentação dos suportes de registro das informações,
- doação das aparas e
- instrução do “Processo relativo aos trabalhos da comissão de avaliação de documentos de arquivos”.

4. Transferência e recolhimento:

- organizar, avaliar, higienizar, acondicionar e disponibilizar os instrumentos descritivos;
- solicitar autorização oficial;
- elaborar “Relação e termo de transferência” ou “Relação e termo de recolhimento”; e
- assegurar integridade de documentos.

Todos estes procedimentos agrupam-se, na interface do SPdoc, em oito macro-funcionalidades que dão acesso às suas respectivas funcionalidades, como apresentado na tabela abaixo:

1. Pré-cadastro
2. Documento
2.1. Autuação
2.1.1. Solicitação
2.1.2. Autuação
2.1.3. Cancelamento da solicitação
2.2. Cadastrar
2.3. Consultar
2.4. Encerrar
2.5. Encerrar e abrir volume
2.6. Instrução
3. Protocolo
3.1. Apensar/Desapensar
3.2. Desentranhar
3.3. Incorporar/Desincorporar
4. Tramitação
4.1. Enviar
4.2. Receber
4.3. Órgão Externo
4.3.1. Enviar
4.3.2. Receber
4.3.3. Registrar recebimento
4.4. Cancelar envio
5. Arquivo
5.1. Arquivar documento
5.2. Cadastro de arquivo
5.3. Desarquivar documento do arquivo corrente
5.4. Endereço do arquivamento
5.5. Reabertura de documento
5.5.1 Solicitar
5.5.2. Cancelar solicitação
5.6. Transferência de documento encerrado
5.6.1. Enviar
5.6.2. Reverter relação de transferência
5.7. Consulta de documento encerrado
5.7.1. Solicitar
5.7.2. Receber
5.7.3. Devolver
5.7.4. Cancelar transferência
5.8. Transferência de arquivos locais
5.9. Eliminação

5.9.1. Consulta
6. Relatórios
6.1. Relatório
6.1.1. Documentos em posse
6.1.2. Documentos externos em posse
6.1.3. Documentos encerrados não arquivados
6.1.4. Documentos arquivados não encerrados
6.1.5. Documentos enviados e não recebidos
6.1.6. Documentos pendentes na unidade administrativa
6.1.7. Arquivos com documentos
6.1.8. Usuários
6.1.9. Usuários por perfil
6.2. Reemissão
6.2.1. Documento
6.2.1.1. Protocolo de recebimento
6.2.1.2. Folha líder
6.2.1.3. Recusa de autuação
6.2.1.4. Solicitação de autuação de expediente
6.2.1.5. Autuação
6.2.1.6. Encerramento
6.2.1.7. Encerramento de volume
6.2.2. Protocolo
6.2.2.1. Incorporação
6.2.2.2. Apensamento
6.2.2.3. Desapensamento
6.2.2.4. Desentranhamento
6.2.2.5. Desincorporação
6.2.3. Tramitação
6.2.3.1. Relação de remessa – interna
6.2.3.2. Relação de remessa – externa
6.2.3.3. Relação de recebimento
6.2.4. Arquivo
6.2.4.1. Transferência de documentos encerrados
6.2.4.2. Reabertura
6.2.4.3. Reabertura NA
7. Administração

7.1. Formatos
7.2. Mensagens
7.3. Órgão expedidor de RG
7.4. Órgão externo
7.5. Órgãos externos preferenciais
7.6. Órgão produtor
7.7. Origem
7.7.1. Cadastro
7.7.2. Associação
7.8. Sistemas legados
7.8.1. Cadastro
7.8.2. Associação
7.9. Demanda
7.9.1. Cadastro
7.9.2. Associação
7.10. Tabela de Temporalidade
7.10.1. Área de atuação
7.10.2. Função
7.10.3. Subfunção
7.10.4. Atividade
7.10.5. Série documental
7.10.6. Série documental preferencial
7.11. Espécie
7.11.1. Cadastro
7.12. Unidade federativa
7.13. Unidade administrativa
7.14. Unidade administrativa preferencial
7.15. Transferir posse de documento
7.16. Alteração de dados do usuário
7.17. Sistema
7.17.1. Segurança
8. Ajuda
8.1. Manual
8.1.1. Plano de classificação de documentos – área-meio
8.1.2. Plano de classificação de documentos - ordem alfabética
8.1.3. Plano de classificação de documentos – cultura
8.1.4. Tabela de temporalidade – área-meio

8.1.5. Tabela de temporalidade – cultura

As funcionalidades são ações que os usuários executam conforme seus perfis. Cada funcionalidade pode representar uma única ação ou um conjunto de ações que são registradas quando estas modificam alguma informação no sistema.

É importante observar que, uma vez que o SPdoc se encontra em fase de transição, dentro de um processo de desenvolvimento e aperfeiçoamento, estas funcionalidades poderão ser modificadas de acordo com avaliações que deverão ser realizadas para verificar qual o grau de adequação (análise de conformidade) do SPdoc aos requisitos, padrões, normas e procedimentos arquivísticos estabelecidos pelo DGSAESP, na Instrução Normativa APE/SAESP – 1, de 10 de março de 2009.

No estágio de desenvolvimento atual, o SPdoc gera documentos apenas durante a execução das ações de algumas de suas funcionalidades do sistema. Apresentamos, abaixo, a relação destes documentos:

- protocolo de recebimento,
- folha líder,
- relação de remessa interna,
- relação de remessa externa,
- relação de recebimento,
- termo de solicitação de autuação de expediente,
- termo de recusa de autuação,
- termo de autuação,
- termo de empréstimo a terceiros,
- recibo de devolução de empréstimo a terceiros,
- termo de incorporação,
- termo de apensamento para piloto,
- termo de apensamento,
- termo de desapensamento para piloto,
- termo de desapensamento,
- termo de desentranhamento,
- termo de encerramento de volume,
- termo de abertura de volume,
- termo de encerramento,
- relação de transferência de documentos encerrados,
- relação de recebimento de documentos encerrados,
- termo de reabertura,
- relação de eliminação de documentos,
- edital de ciência de eliminação de documentos,
- termo de eliminação de documentos,
- relatório de documentos em posse,
- relatório de documentos externos em posse,
- relatório de documentos encerrados e não arquivados,
- relatório de documentos encerrados e arquivados,
- relatório de documentos arquivados e não encerrados,
- relatório de documentos enviados e não recebidos,
- relatório de documentos pendentes na unidade administrativa,
- relatório de arquivos com documentos,
- relatório de usuários,

- relatório de usuários por perfil e
- relatório de histórico do documento.

A manutenção do SPdoc é realizada em quatro níveis, segundo os perfis administrativos apresentados abaixo:

- Administrador técnico: responsável pelo atendimento das demandas do Comitê Gestor do SPdoc referentes à estrutura de banco de dados e a demais requisitos tecnológicos do sistema. A execução das atividades deste perfil compete à equipe da PRODESP da Casa Civil.
- Administrador central: responsável por inserir as tabelas de temporalidade de documentos; criar e excluir os perfis de administradores do órgão; cadastrar a estrutura administrativa dos órgãos; transferir a posse do documento, quando necessário; transferir o domínio do documento, quando necessário. A execução das atividades deste perfil compete, atualmente, a um membro do Comitê Gestor do SPdoc e a seu núcleo de apoio.
- Administrador do órgão: responsável, na sede do órgão, por criar e excluir perfis de usuários e por transferir o domínio do documento, quando necessário. A execução das atividades deste perfil compete, atualmente, ao coordenador da comissão de avaliação de documentos de arquivo do órgão.
- Administrador regional: responsável, na unidade descentralizada do órgão, por criar e excluir perfis de usuários e por transferir o domínio do documento, quando necessário. Atualmente, este perfil não está ativo.

É importante ressaltar que, durante a atual fase de desenvolvimento, os perfis do SPdoc não estão totalmente definidos, sendo a reestruturação destes estudada no âmbito do Comitê Gestor do sistema. Está sendo elaborado ato normativo, visando a oficializar o mecanismo de funcionamento do SPdoc e os perfis de administração.

Quanto aos requisitos e restrições normativos, científicos, artísticos e éticos, destacamos:

1. Requisitos obrigatórios e metadados do SPdoc: Instrução Normativa APE/SAESP – 1, de 10 de março de 2009, que estabelece as diretrizes e define os procedimentos para a gestão, a preservação e o acesso contínuo aos documentos arquivísticos digitais da administração pública do Estado de São Paulo.
2. Documentos sigilosos: a legislação estadual sobre graus de acesso e sigilo de documentos públicos ainda se encontra em fase de elaboração, pois acaba de ser promulgada a Lei n.º 12.527, de 18 de novembro de 2011, que regula, em âmbito nacional, o acesso a informações públicas, e deve ser tratada pelo grupo técnico criado pela Resolução CC-3, de 9/1/2012, no CQGP.
3. Conduta ética dos servidores públicos que operam o SPdoc: Decreto n.º 44.074, de 1º de julho de 1999 (ouvidorias de servidores públicos), Decreto n.º 45.040, de 4 de julho de 2000 (comissões de ética). Tanto as ouvidorias quanto as comissões de ética são sujeitas às considerações que emergem das interações entre os preceitos dos servidores públicos e os de suas categorias profissionais específicas, entre as quais podemos relacionar:
 - Lei n.º 10.261, de 28 de outubro de 1968 (Estatuto dos Funcionários Públicos do Estado de São Paulo);
 - Códigos de ética específicos de cada órgão e entidade da administração pública (por exemplo: a Resolução da Secretaria da Fazenda n.º 51, de 20 de dezembro de 2007; e a Portaria do Instituto de Pesos e Medidas do Estado de São Paulo n.º 218, de 19 de junho de 2009); e
 - Código de Ética Médica: Resolução CFM n.º 1931, de 17 de setembro de 2009, que, por exemplo, prevê: “É vedado ao médico permitir o manuseio e o conhecimento dos

prontuários por pessoas não obrigadas ao sigilo profissional quando sob sua responsabilidade”.

4. Proteção ao usuário do serviço público no Estado de São Paulo: Lei n.º 10.294, de 20 de abril de 1999.
5. Proteção de direitos autorais e de propriedade industrial dos documentos: Lei n.º 9.610, de 19 de fevereiro de 1998 (Lei de Direitos Autorais) e Lei n.º 9.279, de 14 de maio de 1996 (Lei da Propriedade Industrial).

Contexto tecnológico

O SPdoc opera em dois ambientes: na Internet, aberto aos cidadãos que possuam expedientes em órgãos que já utilizam o sistema; e “intragov”, restrito aos servidores públicos que utilizam o SPdoc ou são responsáveis por sua manutenção.

A infraestrutura do SPdoc varia conforme o ambiente no qual é operado:

- Internet: um servidor, Windows 2003 Enterprise x64, dois processadores Dual Core, 8GB de RAM.
- “Intragov”: três servidores em locais diferentes, Windows 2003 x64, dois processadores Dual Core, 8GB de RAM.

Dois outros servidores, também em locais distintos, auxiliam a converter as informações do SPdoc para o *cluster* de banco de dados, em um terceiro local. Tais computadores possuem Windows 2003 Enterprise x64, SQL Server 2005 Enterprise x64, quatro processadores Dual Core e 32GB de RAM.

As informações produzidas e armazenadas (inclusive os *back-ups*) no SPdoc estão em formato SQL. Documentos, como relações de remessa de documentos e declarações de recebimento, são convertidos em formato PDF por um *plug-in*.

Os requisitos mínimos para o funcionamento do SPdoc são o Internet Explorer 7 ou o Mozilla Firefox para a navegação, e o Adobe Acrobat Reader para abrir o formato PDF.

D. Respostas narrativas a perguntas pertinentes para os pesquisadores sobre os estudos de caso de sistemas de manutenção de documentos arquivísticos

O Sistema de Arquivos do Estado de São Paulo (SAESP) existe desde 1984, quando foi instituído pelo Decreto n.º 22.789, de 19 de outubro, tendo, como órgão central, o Arquivo Público do Estado e, como coordenador de seu funcionamento, o Departamento de Gestão do SAESP (DGSAESP). Dentre seus objetivos principais, está a harmonização das diversas fases da administração de documentos arquivísticos gerados pelos órgãos públicos, o que o caracteriza como um sistema de gestão documental ou de manutenção de documentos. Como se trata do patrimônio arquivístico de toda a administração pública paulista — distribuídos em arquivos correntes, intermediários e permanentes —, são necessários vários instrumentos à política de gestão documental do Estado. As comissões de avaliação de documentos de arquivos instituídas nos órgãos do governo paulista podem ser consideradas como um instrumento institucional. Podem ser considerados instrumentos legais os decretos, as resoluções e as instruções normativas elaborados pelo DGSAESP. E podem ser consideradas ferramentas de gestão o plano de classificação e a tabela de temporalidade de documentos da administração pública do Estado de São Paulo, referentes às atividades-meio, e aprovados pelo Decreto n.º 48.898, de 27 de agosto de 2004; e os planos de classificação e as tabelas de temporalidade de documentos das atividades-fim dos órgãos e entidades da administração direta e indireta, alguns já aprovados – e outros, em diferentes estágios de elaboração – pelo PGDI promovido pelo DGSAESP.

Existe, na administração pública do Estado de São Paulo, o esforço de estabelecer um sistema integrado e centralizado para todos os documentos, nos mais diversos suportes e formatos. O próprio SPdoc, objeto deste estudo de caso, explicita, em seu nome, esta iniciativa, ao se designar como “Sistema Informatizado Unificado de Gestão Arquivística de Documentos e Informações”. Concebido como ferramenta de controle que induz o uso dos instrumentos arquivísticos tradicionais (planos de classificação e tabelas de temporalidade dos documentos), o SPdoc visa a integrar todos os órgãos e entidades do Estado num único sistema, potencializando os seguintes benefícios da gestão documental:

- controle do fluxo de documentos e organização de arquivos;
- acesso rápido aos documentos públicos, garantindo agilidade nos processos decisórios;
- revisão e padronização de procedimentos administrativos, imprimindo maior qualidade e produtividade ao serviço público;
- preservação dos documentos que integram o patrimônio documental estadual; e
- eliminação criteriosa de documentos desprovidos de valor permanente.

Como o SPdoc está em desenvolvimento, aperfeiçoamento e implementação, prioriza-se a adesão das secretarias de estado, até serem englobadas todas as empresas públicas, fundações, autarquias, sociedades de economia mista e, em uma última etapa, outras instituições públicas das esferas municipal e estadual da administração paulista que apresentarem interesse em aderir ao sistema (não necessariamente nesta ordem). Como o pleno desenvolvimento e o funcionamento do SPdoc envolvem tanto aspectos tecnológicos quanto requisitos arquivísticos que alimentem a base de dados, é indispensável, para o ingresso no sistema, o atendimento de critérios de adesão definidos pelo Comitê Gestor do SPdoc e oficializados pela Resolução da Casa Civil 19, de 19 de abril de 2011. São quatro critérios:

- oficializar o plano de classificação e a tabela de temporalidade de documentos das atividades-fim do órgão, por meio de sua comissão de avaliação de documentos de arquivo, em conformidade com o Decreto n.º 29.838, de 18 de abril de 1989, e os artigos 18 e 23 do Decreto n.º 48.897, de 27 de agosto de 2004;
- apresentar diagnósticos sobre os sistemas legados de controle de documentos e outros sistemas do órgão;
- promover estudos para efetuar a migração de dados ou a integração com sistemas legados de controle de documentos e outros sistemas de informação do órgão, evitando a perda ou a corrupção de documentos e informações, nos termos do artigo 5º da Instrução Normativa APE/SAESP – 1, de 10 de março de 2009; e
- designar, no órgão, um administrador local do SPdoc, responsável por acompanhar sua implementação e funcionamento.

Devido à complexidade e à significativa dimensão da administração pública paulista, não foi possível, no âmbito do Projeto InterPARES 3, identificar detalhadamente os *softwares* em que são produzidos os documentos que deverão ser gerenciados pelo SPdoc. Na sua atual fase de desenvolvimento, na qual o SPdoc opera basicamente como um sistema referencial, sabe-se que os documentos controlados por ele são produzidos em: aplicativos para escritório (Microsoft Office, OpenOffice, BOffice etc.); programas para desenvolvimento de trabalhos gráficos (CorelDRAW Graphic Suites, Adobe Creative Suites etc.); e demais sistemas e aplicativos necessários para a execução das atividades dos órgãos públicos, que são as mais variadas possíveis. É importante destacar que, no governo paulista, são utilizados tanto *softwares* livres quanto proprietários, alguns destes últimos desenvolvidos pela PRODESP. Já no que se refere aos *hardwares* usados pelos servidores públicos estaduais, estes são tão ou mais diversos que os *softwares*, tendo sido impossível identificá-los durante o estudo de caso.

O objetivo do SPdoc é reunir os protocolos e os arquivos da administração pública estadual em uma mesma base de dados. Até o momento, contudo, não foi realizado um estudo detalhado sobre quais sistemas deverão migrar suas informações para o SPdoc ou interoperar com ele. Em um levantamento preliminar realizado pelo núcleo de apoio ao Comitê Gestor do SPdoc, foram identificados alguns sistemas de gestão eletrônica de documentos (GED), desenvolvidos, em sua maioria, pela PRODESP, que serão analisados pela Comissão Técnica de Implementação e Treinamento para a definição do procedimento a ser adotado durante o processo de adesão dos órgãos ao SPdoc. Como, atualmente, o SPdoc não possui um módulo de gestão arquivística de documentos arquivísticos digitais, os *softwares* em que o sistema fará a captura destes ainda não foram definidos. No entanto, o SPdoc já está interoperando com outros dois sistemas.

Como mencionado acima, o SPdoc, hoje, não captura nenhum tipo de documento. No entanto se pretende que ele seja capaz de realizar tal operação, quando seu módulo de gestão arquivística de documentos digitais entrar em operação. Neste, os documentos serão capturados e organizados de forma a refletir os processos de sua produção, de acordo com os planos de classificação e as tabelas de temporalidade dos documentos da administração pública do Estado de São Paulo (atividades-meio e atividades-fim). A metodologia adotada para a elaboração das ferramentas de gestão supracitadas baseia-se no agrupamento dos "documentos de arquivo, relacionando-os ao órgão produtor, à função, subfunção e atividade responsável por sua produção e acumulação"¹².

Em geral, o acesso aos documentos arquivísticos e os respectivos metadados controlados pelo SPdoc serão definidos de acordo com os perfis administrativos e operacionais do sistema, apresentados no quadro abaixo:

P E R F I S A D M N I S T R A T I V O S	Administrador técnico	<u>Quem?</u> Equipe PRODESP da Secretaria da Casa Civil.	<u>Responsável por:</u> atender às demandas do Comitê Gestor do SPdoc referentes à estrutura de banco de dados e demais requisitos tecnológicos do sistema.	<u>Acesso:</u> integral à estrutura do sistema, bem como a seus bancos de dados e metadados.
	Administrador central	<u>Quem?</u> Atualmente, um membro do Comitê Gestor do SPdoc e o núcleo de apoio ao mesmo comitê.	<u>Responsável por:</u> inserir as tabelas de temporalidade de documentos; criar e excluir perfis de administrador do órgão; cadastrar a estrutura administrativa dos órgãos; transferir a posse do documento, quando necessário; e transferir o domínio do documento, quando necessário	<u>Acesso:</u> integral aos metadados dos usuários, da estrutura do órgão e dos documentos; às tabelas de temporalidades de documentos; e aos documentos referenciados no sistema.

¹² Artigo 10, parágrafo único, do Decreto Estadual n.º 48.897/2004.

	Administrador do órgão	<u>Quem?</u> Atualmente, coordenador da comissão de avaliação dos documentos de arquivo do órgão.	<u>Responsável por:</u> na sede do órgão, criar e excluir perfis de usuários, e transferir o domínio do documento, quando necessário	<u>Acesso:</u> parcial aos metadados dos usuários e dos documentos do órgão; e aos documentos do órgão referenciados no sistema.
	Administrador regional	<u>Quem?</u> Atualmente, este perfil não está ativo.	<u>Responsável por:</u> na unidade descentralizada do órgão, criar e excluir perfis de usuários, e transferir o domínio do documento, quando necessário.	<u>Acesso:</u> parcial aos metadados dos usuários e dos documentos da unidade descentralizada do órgão; e aos documentos da unidade referenciados no sistema.
P E R F I S O P E R A C I O N A I S	Usuários do SPdoc	<u>Quem?</u> Funcionários públicos dos órgãos onde o sistema foi implantado.	<u>Responsável por:</u> operar as funcionalidades do sistema, conforme perfil criado (consulta, cadastrador, protocolo, arquivo etc.).	<u>Acesso:</u> parcial aos metadados dos documentos do seu respectivo órgão (conforme o perfil); e aos documentos referenciados no sistema.

Não podemos deixar de mencionar que, entre os usuários do SPdoc, estão os cidadãos que têm acesso a alguns metadados dos documentos de seu interesse, a partir do número de registro de protocolo, da data e da hora. Por fim, é importante ressaltar que, durante a atual fase de desenvolvimento, os perfis do SPdoc não estão totalmente definidos, sendo a reestruturação destes estudada no âmbito do Comitê Gestor do SPdoc.

Já foram definidos os padrões/ esquemas de descrição de metadados utilizados na produção, na manutenção e no uso dos documentos arquivísticos digitais, que devem orientar a elaboração dos requisitos funcionais do módulo de documentos digitais. O Arquivo Público do Estado, por meio do DGSAESP, publicou a Instrução Normativa APE/SAESP – 1, de 10 de março de 2009, que estabelece as diretrizes e define os procedimentos que deverão ser adotados por todos os órgãos e entidades da administração pública paulista, com o objetivo de garantir a gestão, a preservação e o acesso contínuo aos documentos arquivísticos digitais. Elaborada de acordo com

recomendações internacionais e nacionais¹³, essa instrução normativa apresenta, em seus anexos, os requisitos obrigatórios e altamente desejáveis, acompanhados de seus respectivos metadados, para os sistemas informatizados de gestão arquivística dos documentos convencionais e digitais produzidos pelo governo do Estado de São Paulo¹⁴.

O Comitê Gestor do SPdoc define a utilização dos recursos financeiros destinados ao SPdoc pela lei orçamentária que, anualmente, calcula a receita e fixa as despesas do Estado de São Paulo.

O SPdoc dispõe dos seguintes recursos tecnológicos:

- atendendo ao ambiente de Internet: um servidor, Windows 2003 Enterprise x64, dois processadores Dual Core, 8GB de RAM;
- atendendo ao ambiente “intragov”: três servidores, Windows 2003 Enterprise x64, dois processadores Dual Core, 8GB de RAM;
- atendendo ao ambiente que auxilia a converter as informações para o *cluster* de banco de dados: dois servidores (localizados nos municípios de Paraguassu e Pilar do Sul), Windows 2003 Enterprise x64, dois processadores Dual Core, 8GB de RAM; e
- atendendo ao *cluster* de banco de dados: dois servidores (localizados no município de Passos), Windows 2003 Enterprise x64, SQL Server 2005 Enterprise x64, com quatro processadores Dual Core, 32GB de RAM.

No que se refere à estrutura de preservação da informação, o SPdoc conta com um robô, modelo Storagetek SL 8500, localizado em uma sala-cofre do centro do processamento de dados da PRODESP, que realiza rotina diária de *back-up*.

As questões relativas ao acesso, à segurança, à privacidade de dados e à legislação da liberdade de informação foram discutidas durante o desenvolvimento inicial do SPdoc e, posteriormente, retomadas na elaboração da Instrução Normativa APE/SAESP – 1, de 10 de março de 2009, porém elas ainda precisam ser aprofundadas, sobretudo agora, após a promulgação da Lei n.º 12.527, de 18 de novembro de 2011, que regula, em âmbito nacional, o acesso a informações públicas.

Como mencionado anteriormente, na fase atual de desenvolvimento, o SPdoc funciona apenas como um sistema referencial dos documentos arquivísticos convencionais, ou seja, em papel. No entanto, pretende-se que ele seja também um sistema capaz de produzir, gerir e preservar documentos arquivísticos digitais. Tendo isso em mente, supõe-se, a partir de uma análise geral da “Cadeia de Preservação do InterPARES 2”, que os quatro níveis de complexidade detalhados (*A1 – Managing the Framework for the Chain of Preservation; A2 – Managing Records in a Record-making System; A3 – Managing Record in a Recordkeeping System; e A4 – Managing Records in a Permanent Preservation System*) são necessários ao SPdoc.

E. Respostas narrativas a questões de pesquisa pertinentes ao projeto

Antes de iniciar as respostas, é preciso chamar a atenção para o fato que grande parte das questões apresentadas abaixo ainda são objeto de reflexão do Arquivo Público do Estado de São Paulo, particularmente do DGSAESP, e do Comitê Gestor do SPdoc.

¹³ Principalmente, as recomendações das Organizações das Nações Unidas para a Educação, a Ciência e a Cultura (UNESCO); do Conselho Internacional de Arquivos (CIA); e do Conselho Nacional de Arquivos (CONARQ).

¹⁴ Para conhecer os requisitos obrigatórios e os altamente desejáveis e seus respectivos metadados, veja os apêndices 1 e 2 deste relatório.

Quais são os organismos de regulação, auditoria e decisão política que devem ser sensibilizados para a importância da preservação digital, e qual é a melhor forma de influenciá-los?

O organismo de regulação, auditoria e decisão política que deve ser sensibilizado é o Comitê Gestor do SPdoc (CGSPdoc), por meio da orientação que o DGSAESP impõe ao sistema. Ao se constituir como um órgão colegiado, o Comitê Gestor reúne não somente representantes de secretarias estratégicas do governo estadual, mas também, ou melhor, principalmente, profissionais de Arquivologia e de Tecnologia de Informação, cujo trabalho colaborativo é essencial à preservação digital.

Como adaptar o conhecimento existente a respeito da preservação de documentos arquivísticos digitais às necessidades e circunstâncias de instituições de pequeno e médio porte?

O Sistema de Arquivos do Estado de São Paulo (SAESP) é composto por instituições dos mais variados portes. O conhecimento existente a respeito da preservação de documentos arquivísticos digitais será disseminado pelo DGSAESP, responsável por coordenar o funcionamento do SAESP, independentemente do porte do órgão ou entidade.

O que diferencia a preservação de documentos arquivísticos digitais da preservação de outras entidades digitais que podem estar sob a responsabilidade dos arquivos?

O que diferencia, basicamente, esses dois tipos de preservação é o cuidado que se deve ter com os documentos arquivísticos digitais, “para garantir sua acessibilidade e legibilidade ao longo do tempo, mantendo intactos sua forma, seu conteúdo e suas relações até quando for necessário para a continuidade de sua credibilidade como documento de arquivo”¹⁵.

Que tipo de política, estratégia e procedimentos estes arquivos ou programas devem colocar em prática para estarem aptos a controlar os documentos arquivísticos digitais pelos quais são ou serão responsáveis, e de que fatores dependem estes mecanismos administrativos (ex.: esquema de prestação de contas específico, estrutura de governança)?

Com a implantação do SPdoc, pretende-se que o controle dos documentos arquivísticos da administração pública paulista seja unificado. Quanto a política, estratégias, procedimentos e mecanismos administrativos que os arquivos estaduais deverão adotar e/ ou recorrer para gerir seus documentos arquivísticos digitais, estes serão definidos pelo Arquivo Público do Estado, pelo Comitê Gestor do SPdoc e pelos dirigentes dos diversos órgãos, de acordo com suas respectivas atribuições.

Que planos de ação para a preservação de longo prazo destes conjuntos de documentos podem ser propostos?

De acordo com os dados levantados no “Modelo para análise contextual” e nas “Questões a serem respondidas pelos pesquisadores com relação aos estudos de caso de sistemas de gestão de documentos”, foi possível identificar algumas lacunas e apontar aperfeiçoamentos necessários ao bom funcionamento do SPdoc, sobretudo se se pretende que ele seja um sistema capaz de elaborar, gerir e preservar documentos arquivísticos digitais.

No entanto é importante chamar a atenção para o fato de que, devido à complexidade do objeto do Estudo de Caso BR09 e ao curto período disponível para o desenvolvimento da pesquisa — uma vez que o DGSAESP ingressou no Projeto InterPARES 3 apenas um ano e meio antes do encerramento deste —, o diagnóstico do SPdoc apresentado abaixo serve de base

¹⁵ InterPARES 2. *Diretrizes do Preservador - A preservação de documentos arquivísticos digitais: Diretrizes para organizações*. Tradução: Arquivo Nacional e Câmara dos Deputados. [Livreto sem local e data de publicação]. Introdução.

para uma primeira proposta de plano de ação, que não pôde ser desenvolvido plenamente no âmbito do InterPARES devido ao tempo exíguo.

Atividades administrativas

1. Documentação do SPdoc:

- Diagnóstico: A dificuldade em reunir as informações técnicas sobre o SPdoc revelou que a documentação referente à construção do sistema não está totalmente em posse do Comitê Gestor.
- Ação proposta: Recompilar a documentação do SPdoc.
- Envolvidos: Comitê Gestor do SPdoc e PRODESP.
- Status: Atividade iniciada pelo núcleo de apoio ao SPdoc e pela equipe PRODESP da Casa Civil.

Atividades arquivísticas

1. Conformidade do SPdoc com os procedimentos, requisitos e padrões do DGSAESP:

- Diagnóstico: Com o nível da análise feita no âmbito do InterPARES, não foi possível constatar se o SPdoc está de acordo com os requisitos, os padrões, as normas e os procedimentos arquivísticos, emanados do DGSAESP, que lhe asseguram consistência, segurança e confiabilidade.
- Ação proposta: Analisar a conformidade do SPdoc.
- Envolvidos: Comitê Gestor do SPdoc, DGSAESP e PRODESP.
- Status: Não iniciada, embora a análise preliminar do sistema tenha sido feita recentemente pela equipe PRODESP da Casa Civil. Esta indicou que o SPdoc atende a 28% dos requisitos obrigatórios da Instrução Normativa APE/SAESP – 1/2009, considerando-se que, dos 72% dos requisitos obrigatórios restantes, 50% se referem aos documentos digitais não contemplados no módulo do SPdoc em operação. Faz-se necessário, ainda, verificar a conformidade do SPdoc em relação aos procedimentos de protocolo e arquivo que o DGSAESP está sistematizando.

2. Identificação dos documentos arquivísticos produzidos pelo SPdoc:

- Diagnóstico: No que se refere aos documentos digitais gerados pelo SPdoc durante a execução de algumas de suas funcionalidades, não foi possível verificar quais destes são arquivísticos.
- Ação proposta: Identificar os documentos arquivísticos digitais gerados pelo SPdoc, na sua atual fase de desenvolvimento, e verificar, entre outros, se estes possuem forma fixa e conteúdo estável.
- Envolvidos: Comitê Gestor do SPdoc e DGSAESP.

Atividades sistêmicas

1. Responsabilidade pela manutenção do SPdoc

- Diagnóstico: Foi possível constatar que os indivíduos responsáveis pela manutenção do SPdoc ainda não estão claramente definidos.
- Ação proposta: Identificar os indivíduos responsáveis pela manutenção do SPdoc e definir suas atribuições.
- Envolvidos: Comitê Gestor do SPdoc.
- Status: Não iniciada, embora o núcleo de apoio ao Comitê Gestor já tenha iniciado os estudos para definir melhor os diferentes perfis do sistema.

2. Estratégias de manutenção e segurança do SPdoc

- Diagnóstico: De acordo com a pesquisa realizada, atualmente, a PRODESP realiza um *back-up* diário do SPdoc, mantendo o banco de dados por 21 dias, demais arquivos por trinta dias e os registros de *log in* por um ano.
 - Ação proposta: Verificar a eficácia da rotina de *back-up*.
 - Envolvidos: Comitê Gestor do SPdoc e PRODESP.
3. Acesso e segurança do SPdoc:
- Diagnóstico: Ainda que o acesso ao SPdoc seja feito por meio de *log in*, não foi possível constatar, com o nível de análise feita no âmbito do InterPARES, como são registradas as alterações feitas no sistema.
 - Ação proposta:: Verificar a estratégia de proteção do SPdoc contra ações não autorizadas, contemplando, entre outros, a estrutura de permissões de acesso e trilha de auditoria.
 - Envolvidos: Comitê Gestor do SPdoc, DGSAESP e PRODESP.
 - Status: Não iniciada, embora o Comitê Gestor do SPdoc já tenha solicitado à PRODESP a inclusão e/ ou a alteração de funcionalidades relacionadas à proteção do sistema. No que se refere à restrição de acesso, o Arquivo Público do Estado, por meio do DGSAESP, já iniciou os trabalhos necessários para adequar ao contexto estadual, a recém-promulgada Lei n.º 12.527, de 18 de novembro de 2011, que regula, em âmbito nacional, o acesso a informações públicas.

Um plano de ação selecionado para um conjunto documental pode ser válido para outro conjunto documental do mesmo tipo, que seja produzido e preservado pelo mesmo tipo de organização ou pessoa no mesmo país?

A proposta inicial de plano de ação apresentada anteriormente não pode ser utilizada como um modelo para sistemas de manutenção de documentos arquivísticos, uma vez que apresenta atividades pontuais necessárias ao aprimoramento do SPdoc.

Que conhecimento e qualificação são necessários aos responsáveis pela definição de políticas, procedimentos e planos de ação de preservação de documentos arquivísticos digitais em arquivos de pequeno e médio porte?

Pensando o caso da administração pública paulista, os responsáveis pela definição de políticas, procedimentos e planos de ação de preservação de documentos arquivísticos digitais precisam deter não somente o conhecimento técnico (arquivístico e de Tecnologia da Informação), mas também precisam conhecer o contexto de produção, gestão e preservação dos documentos arquivísticos digitais (aspectos administrativos, físicos, legais, logísticos etc.).

Como os profissionais de arquivo podem manter atualizado seu conhecimento a respeito de preservação digital frente aos ciclos cada vez mais curtos de mudança tecnológica?

No Brasil, para manterem seu conhecimento a respeito da preservação digital, os profissionais de arquivo precisam se manter informados sobre as mudanças tecnológicas e, sobretudo, sobre as pesquisas que estão sendo desenvolvidas pela comunidade arquivística. Para tanto, os profissionais de arquivo precisam: ter acesso a publicações da área; participar de encontros nacionais, internacionais e fóruns de debate e reflexão de um modo geral; além de, sempre que possível, se envolver com projetos de pesquisa como o Projeto InterPARES.

F. Referências

ARQUIVO NACIONAL. *Dicionário brasileiro de terminologia arquivística*. Rio de Janeiro: Arquivo Nacional, 2005. Disponível em:

<http://www.arquivonacional.gov.br/Media/Dicion%20Term%20Arquiv.pdf>

ARQUIVO PÚBLICO DO ESTADO DE SÃO PAULO / DEPARTAMENTO DE GESTÃO DO SISTEMA DE ARQUIVOS DO ESTADO DE SÃO PAULO. *Consolidação da legislação arquivística que orienta o trabalho do Departamento de Gestão do Sistema de Arquivos do Estado de São Paulo*. Arquivo Público do Estado de São Paulo: São Paulo, 2010. Disponível em: http://www.arquivoestado.sp.gov.br/saesp/Consolidacao_da_legislacao_arquivistica.pdf

ARQUIVO PÚBLICO DO ESTADO DE SÃO PAULO / DEPARTAMENTO DE GESTÃO DO SISTEMA DE ARQUIVOS DO ESTADO DE SÃO PAULO. *Política pública de arquivos e gestão documental do Estado de São Paulo*. Arquivo Público do Estado de São Paulo: São Paulo, 2010. Disponível em: http://www.arquivoestado.sp.gov.br/saesp/livro_politica_publica_de_arquivos_e_gestao_documental.pdf

ARQUIVO PÚBLICO DO ESTADO DE SÃO PAULO / DEPARTAMENTO DE GESTÃO DO SISTEMA DE ARQUIVOS DO ESTADO DE SÃO PAULO. *Manual de aplicação do plano de classificação e tabela de temporalidade da administração pública do Estado de São Paulo: atividades-meio*. São Paulo: Arquivo Público do Estado de São Paulo, 2008. Disponível em: http://www.arquivoestado.sp.gov.br/saesp/Manual_Aplicacao_da_Tabela_Temporalidade_verso_paraPDF.pdf

ARQUIVO PÚBLICO DO ESTADO DE SÃO PAULO / DEPARTAMENTO DE GESTÃO DO SISTEMA DE ARQUIVOS DO ESTADO DE SÃO PAULO. *Manual de elaboração do plano de classificação e tabela de temporalidade da administração pública do Estado de São Paulo: Atividades-Fim*. São Paulo: Arquivo Público do Estado de São Paulo, 2008. Disponível em: http://www.arquivoestado.sp.gov.br/saesp/Manual_de_Elaboracao_da_Tabela_Temporalidade_versao_paraPDF.pdf

ARQUIVO PÚBLICO DO ESTADO. *Plano de classificação e tabela de temporalidade de documentos da administração do Estado de São Paulo: atividades-Meio*. São Paulo: Arquivo Público do Estado de São Paulo, 2005. Disponível em: http://www.arquivoestado.sp.gov.br/saesp/Plano_de_Classificacao.pdf

BERNARDES, Ieda Pimenta; DELATORRE, Hilda. *Gestão documental aplicada*. São Paulo: Arquivo Público do Estado de São Paulo, 2008. Disponível em: http://www.arquivoestado.sp.gov.br/saesp/GESTAO_DOCUMENTAL_APLICADA_Ieda.pdf

CONSELHO NACIONAL DE ARQUIVOS / CÂMARA TÉCNICA DE DOCUMENTOS ELETRÔNICOS. *e-ARQ Brasil: Modelo de requisitos para sistemas informatizados de gestão arquivística de documentos eletrônicos*. Rio de Janeiro: Arquivo Nacional, 2011. Disponível em: <http://www.conarq.arquivonacional.gov.br/cgi/cgilua.exe/sys/start.htm>

CONSELHO NACIONAL DE ARQUIVOS. *Legislação arquivística brasileira*. Rio de Janeiro: Arquivo Nacional, 2011. Disponível em: <http://www.conarq.arquivonacional.gov.br/cgi/cgilua.exe/sys/start.htm?sid=48>

CONSELHO NACIONAL DE ARQUIVOS. *Recomendações para digitalização de documentos arquivísticos permanentes*. Rio de Janeiro: Arquivo Nacional, 2010. Disponível em:

http://www.conarq.arquivonacional.gov.br/media/publicacoes/recomenda/recomendaes_para_digitalizacao.pdf

CONSELHO NACIONAL DE ARQUIVOS / CÂMARA TÉCNICA DE DOCUMENTOS e UNESCO. *Carta para a preservação do patrimônio arquivístico digital*. Rio de Janeiro: Arquivo Nacional / UNESCO, 2005. Disponível em:

<http://www.conarq.arquivonacional.gov.br/media/carta.pdf>

ESCRITÓRIO DE PRODUTOS DA PRODESP. *Manual de dados de produtos*. São Paulo: PRODESP, 2010.

DURANTI, L (editor). *International Research on Permanent Authentic Records in Electronic Systems (InterPARES) 2: Experiential, Interactive and Dynamic Records*. Padova: Associazione Nazionale Archivistica Italiana, 2008. Disponível em:

http://www.interpares.org/ip2/display_file.cfm?doc=ip2_book_complete.pdf

DURANTI, L.; THIBOUDEAU, “The Concept of Record in Interactive, Experiential and Dynamic Environments: The View of InterPARES”, *Archival Science*, 6, 2006, 13-68.

DURANTI, L.; EASTWOOD, T.; MacNEIL, H. *The Preservation of the Integrity of Electronic Records*. Vancouver: University of British Columbia, 1997. Disponível em:

<http://www.interpares.org/UBCProject/index.htm>

FUNDAÇÃO DE DESENVOLVIMENTO ADMINISTRATIVO (FUNDAP). *Perfil da administração pública paulista*. São Paulo: FUNDAP, 2011. Disponível em:

<http://perfil.sp.gov.br/>

[Site atualizado anualmente]

IMPRESA OFICIAL DO ESTADO DE SÃO PAULO. *Diário Oficial do Estado de São Paulo*. Disponível em:

www.imprensaoficial.com.br/PortalIO/DO/HomeDO_2_0.aspx#21/12/2011

[O site disponibiliza os DO publicados entre 2003 e 2011]

InterPARES 2. *Diretrizes do preservador - A preservação de documentos arquivísticos digitais: diretrizes para organizações*. Tradução: Arquivo Nacional e Câmara dos Deputados. [Livreto sem local e data de publicação] Disponível em:

http://www.interpares.org/display_file.cfm?doc=ip2_preserver_guidelines_booklet--portuguese.pdf

InterPARES 2. *Diretrizes do produtor - A elaboração e a manutenção de materiais digitais: diretrizes para indivíduos*. Tradução: Arquivo Nacional e Câmara dos Deputados. [Livreto sem local e data de publicação] Disponível em:

http://www.interpares.org/display_file.cfm?doc=ip2_creator_guidelines_booklet--portuguese.pdf

InterPARES 2. *The Long-term Preservation of Authentic Electronic Records: Findings of the InterPARES Project*. Vancouver: University of British Columbia, 2001. Disponível em:

<http://www.interpares.org/book/index.cfm>

SANTOS, V. B. dos. *Gestão de documentos eletrônicos: Uma visão arquivística*. 2ª ed. Brasília: ABARAQ, 2005.

SÍTIO DO COMITÊ DE QUALIDADE DA GESTÃO PÚBLICA - CQGP:

<http://www.cqgp.sp.gov.br/conteudo/grupostec.html>

SÍTIO DO COMITÊ GESTOR DO SPdoc:

<http://www.arquivoestado.sp.gov.br/spdoc/>

SÍTIO DO CONSELHO NACIONAL DE ARQUIVOS – CONARQ:

<http://www.conarq.arquivonacional.gov.br/cgi/cgilua.exe/sys/start.htm>

SÍTIO DO DEPARTAMENTO DE GESTÃO DO SAESP:

http://www.arquivoestado.sp.gov.br/saespg_dg.php

SÍTIO DO PROJETO INTERPARES:

<http://www.interpares.org/welcome.cfm>

G. Descobertas, recomendações e produtos

É preciso iniciar a conclusão do Estudo de Caso BR09 explicitando as razões que restringiram o pleno desenvolvimento à pesquisa, quais sejam: o ingresso tardio do Departamento de Gestão do SAESP no Projeto InterPARES 3, que só se concretizou apenas um ano e meio antes do encerramento deste; e a complexidade do objeto de estudo, um sistema de gestão arquivística de documentos e não um documento arquivístico digital específico, como no caso dos demais estudos de caso do TEAM Brasil.

Devido às mencionadas limitações, os resultados do Estudo de Caso BR09, apresentados ao longo desse relatório, são a contribuição possível do DGSAESP ao InterPARES 3, sobretudo porque é preciso considerar o fato que o SPdoc ainda está em desenvolvimento e, no momento, não produz, gerencia ou preserva documentos arquivísticos digitais.

Assim sendo, um balanço final revela que as contribuições do InterPARES ao aprimoramento do SPdoc se mostraram mais representativas do que as do DGSAESP ao Projeto, particularmente no que se refere à Cadeia de Preservação do InterPARES 2, que contribuirá significativamente na modelagem dos novos módulos do SPdoc dedicados aos documentos arquivísticos digitais. Ademais, de um modo geral, o projeto proporcionou um rico ambiente de fomento ao conhecimento, que, além de capacitar os profissionais de arquivo, colabora com a conscientização das instituições responsáveis pela guarda de documentos arquivísticos digitais sobre a importância de começar o quanto antes pensar a preservação destes.

APÊNDICE 1

Requisitos obrigatórios e seus respectivos metadados para os sistemas informatizados de gestão arquivística dos documentos convencionais e digitais produzidos pelo Governo do Estado de São Paulo. Anexo I a que se refere o artigo 5º da Instrução Normativa APE / SAESP – 1/2009.

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	Elaboração de Planos de Classificação de Documentos para o órgão ou entidade.	<i>Os Planos de Classificação de Documentos devem ser aprovados pelo Arquivo Público do Estado, nos termos da legislação vigente.</i>		
1.1.2	Garantir a criação de funções, subfunções, atividades e séries de acordo com os Planos de Classificação de Documentos.			
1.1.3	Permitir a usuários autorizados acrescentar novas funções, subfunções, atividades ou séries			

	documentais sempre que se fizer necessário;				
1.1.4	Registrar a data de abertura de uma nova função, subfunção, atividade ou série no respectivo metadado.			Registro de abertura	Registra informações: data/hora e responsável pela abertura.
1.1.5	Registrar a mudança de nome de uma função, subfunção, atividade ou série já existente no respectivo metadado.			Registro de mudança de nome de função/sufunção/atividade/série	Registra informações: data/hora, responsável e nome anterior.
1.1.6	Permitir o deslocamento de uma função inteira, incluindo as subfunções, atividades e séries dos documentos ali classificados, para um outro ponto do Plano de Classificação.	<i>Nesse caso, é necessário fazer o registro do deslocamento nos metadados do Plano de Classificação.</i>		Registro de deslocamento de função/sufunção/atividade/série (mudança de subordinação)	Registra informações: data/hora, responsável e subordinação anterior.
1.1.7	Permitir que um usuário autorizado apague uma função, subfunção, atividade ou série inativa.	<i>Só pode ser apagada uma função, subfunção, atividade ou série que não tenha documentos ali classificados.</i>		Registro de extinção de função, subfunção, atividade ou série	Registra informações: data/hora e responsável pela extinção.
1.1.8	Permitir que um usuário autorizado inative uma função, subfunção, atividade ou série onde não serão mais classificados			Registro de desativação	Registra informações: data/hora e responsável pela desativação.

	documentos, podendo reativá-las se necessário.		Registro de reativação	Registra informações: data/hora e responsável pela reativação. Indica se a função, subfunção, atividade ou série estão ativas ou inativas.
1.1.9	Impedir a eliminação de uma função, subfunção, atividade ou série que tenham documentos ali classificados.	<i>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.</i>	Indicador de função, subfunção, atividade ou série ativa/inativa	
1.1.10	Permitir a associação de metadados às funções, subfunções, atividades ou séries 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 funções, subfunções, atividades e séries 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 ao seu contexto de produção, composta das seguintes unidades de informação: órgão produtor, função, subfunção, atividade e série documental
1.1.11.2	Atribuição de um termo que identifique cada função, subfunção, atividade ou série.		Classificação - nome	Refere-se à denominação do órgão produtor, da função, subfunção, atividade e série documental.
1.1.12	Assegurar que os termos completos, que identificam cada função, subfunção, atividade ou série, sejam únicos no Plano de Classificação.			
1.1.13	Utilizar o termo completo para identificar uma função, subfunção, atividade ou série.	<i>Entende-se por termo completo toda a hierarquia referente àquela função. Exemplo: Gestão de Bens</i>		

		<i>Materiais e Patrimoniais</i> <i>Controle de compras, serviços e obras</i> <i>Licitação e administração de contratos</i> <i>Contratos</i>		
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 funções, subfunções, atividades ou séries dos Planos de Classificação;			
1.1.14.4	Gerar relatório de documentos classificados por unidade administrativa.			
1.2	Classificação e metadados das séries documentais			
1.2.1	Permitir a classificação das séries documentais somente nas			

	funções, subfunções e atividades autorizadas.			
1.2.2	Permitir a classificação de um número ilimitado de séries documentais dentro de uma função, subfunção ou atividade.			
1.2.3	Utilizar a classificação completa (função, subfunção e atividade) para identificar uma série documental, tal como especificado no item 1.1.12.	Atividade	Indica a ação, encargo ou serviço decorrente do exercício de uma função, que pode ser identificada como atividade-meio ou atividade-fim.	
		Função	Indica o conjunto de atividades que o Estado exerce para a consecução de seus objetivos, que pode ser identificada como direta ou essencial e indireta ou auxiliar.	
		Órgão Produtor	Indica a instituição ou entidade juridicamente constituída e organizada responsável pela execução de funções do Estado.	
		Série	Indica o conjunto de documentos do mesmo tipo documental produzido por um mesmo órgão, em decorrência do exercício da mesma função, subfunção e atividade e que resultam de idêntica forma de produção e tramitação e obedecem à mesma temporalidade e destinação.	
		Subfunção	Indica o agrupamento de atividades afins, correspondendo cada subfunção a uma modalidade da respectiva função.	
1.2.4	Permitir a associação de metadados às séries documentais e restringir a inclusão e alteração desses mesmos metadados somente a usuários autorizados.			

1.2.5	Associar os metadados das séries documentais conforme estabelecido no padrão de metadados.				
1.2.6	Permitir que sejam associados, automaticamente, a uma nova série documental determinados metadados pré-definidos relacionados à função, subfunção ou atividade que lhe deu origem.				
1.2.7	Permitir a reclassificação por usuário autorizado de uma série documental e dos documentos que a integram.				
1.2.8	Permitir que na reclassificação da série sejam associados, automaticamente, aos documentos que a integram todos os seus metadados pré-definidos.				
1.3	Gerenciamento de documentos				
1.3.1	Registrar nos metadados a data da produção ou recebimento e encerramento 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 ou expedientes já encerrados.	<i>Processos ou expedientes encerrados deverão ser reabertos para receber novos documentos.</i>		
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.	<i>A eliminação será devidamente registrada em trilha de auditoria.</i>		
1.3.6	Garantir a integridade da relação hierárquica entre função, subfunção, atividade, série, documento, volume e item documental em todos os momentos, independentemente de atividades de manutenção, ações do usuário ou falha de componentes do sistema.	<i>Em hipótese alguma poderá ocorrer uma situação em que qualquer ação do usuário ou falha do sistema dê origem a uma inconsistência na base de dados do</i>		

		<i>Sistema.</i>		
1.4	Requisitos adicionais para o gerenciamento de documentos			
1.4.1	Prever a formação/autuação de processos, por usuário autorizado conforme estabelecido em legislação específica.			
1.4.2	Prever que os documentos integrantes do processo digital recebam numeração sequencial sem falhas, não se admitindo que documentos diferentes recebam a mesma numeração.		Numeração de folhas de documentos	Numeração sequencial das folhas de documentos inseridos em um processo, expediente ou dossiê.
1.4.3	Controlar a renumeração dos documentos integrantes de um processo digital.	<i>Este requisito tem por objetivo impedir a exclusão não autorizada de documentos de um processo. Casos especiais que autorizem a renumeração devem obedecer aos procedimentos oficiais.</i>	Numeração de folhas de documentos	Numeração sequencial das folhas de documentos inseridos em um processo, expediente ou dossiê.

<p>1.4.4</p>	<p>Prever procedimentos para junta/ desentranhamento, incorporação/ desincorporação, apensamento/ desapensamento e desmembramento de documentos aos expedientes ou processos, de acordo com os procedimentos oficiais.</p>	<p><i>Este procedimento deverá ser registrado nos metadados do expediente ou processo. O apensamento é o ato de anexar um processo/expediente a outro que com ele esteja relacionado, por determinação legal ou a pedido de uma das partes, em caráter temporário, permanecendo o processo/expediente apensado, fora do documento principal.</i></p>	<p>Registro de apensamento</p> <p>Registrar informações: data/hora do apensamento, responsável pelo apensamento, identificador do processo que foi apensado.</p>
---------------------	--	--	--

	<p><i>Este procedimento deverá ser registrado nos metadados do expediente ou processo. O desaparecimento é o ato de separar fisicamente um ou mais documentos (processo/expediente) apensados.</i></p>	<p>Registro de desaparecimento</p>	<p>Registrar informações: data/hora do desaparecimento, responsável pelo desaparecimento, identificador do processo que foi desapensado.</p>
	<p><i>Este procedimento deverá ser registrado nos metadados do expediente ou processo. O desentranhamento é o procedimento que consiste na retirada autorizada de um ou mais documentos juntados a um</i></p>	<p>Registro de desentranhamento</p>	<p>Registra informações: data/hora do desentranhamento, responsável pelo desentranhamento, identificador das peças que foram desentranhadas.</p>

		<i>processo ou expediente.</i>		
		<i>Este procedimento deverá ser registrado nos metadados do expediente ou processo. A desincorporação consiste em procedimento corretivo de uma incorporação impropriamente realizada.</i>	Registro de desincorporação	Registra informações: data/hora, responsável pela desincorporação, identificador do processo/expediente que foi desincorporado.
		<i>Este procedimento deverá ser registrado nos metadados do expediente ou processo. O desmembramento consiste na retirada autorizada de documentos de um</i>	Registro de desmembramento	Registrar informações: data/hora do desmembramento, responsável pelo desmembramento, registro dos documentos retirados, identificador do novo processo formado com os documentos retirados.

		<i>processo/expediente para a formação de um outro processo/expediente.</i>		
		<i>Este procedimento deverá ser registrado nos metadados do expediente ou processo. A incorporação consiste em incorporar um processo interno a outro quando estes tratarem do mesmo assunto e tiverem as mesmas partes interessadas.</i>	Registro de incorporação	Registra informações: data/hora da incorporação, responsável pela incorporação, identificador dos processos que foram incorporados.
		<i>Este procedimento deverá ser registrado nos metadados do expediente ou processo. A juntada é o</i>	Registro de juntada	Registra informações: data/hora da juntada, responsável pela juntada, identificador do documento que foi juntado.

		<i>ato de inserir em um processo/expediente, em caráter definitivo, outros documentos que dele farão parte integrante.</i>		
1.4.5	Prever o encerramento de expediente e processo, incluindo seus volumes e seus metadados.		Registro de encerramento	Registra informações: data/hora e responsável pelo encerramento.
1.4.6	Prever o desarquivamento para reabertura de expediente ou processo por usuário autorizado, de acordo com os procedimentos oficiais.	<i>Para manter a integridade do expediente ou processo somente o último volume receberá novos documentos.</i>	Registro de reabertura	Registra informações: data/hora e responsável pela reabertura.
1.5	Volumes: abertura, encerramento e metadados		Número do volume	Número sequencial de registro atribuído aos volumes de um processo/expediente.
1.5.1	Permitir que um volume herde automaticamente do expediente ou processo ao qual pertence, determinados metadados pré-definidos, como por exemplo, procedência, classificação e temporalidade.			
1.5.2	Permitir a abertura de volumes a		Registro de abertura	Registra informações: data/hora e responsável pela

	qualquer expediente ou processo que não esteja encerrado.			abertura.
1.5.3	Assegurar que um volume somente conterá documentos. Não é permitido que um volume contenha outro volume ou um outro expediente ou processo.			
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.	<i>Apenas o volume produzido mais recentemente poderá estar aberto, todos os outros volumes existentes nesse expediente ou processo têm que estar fechados.</i>		
1.5.6	Impedir a reabertura 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 óptico, 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 expediente, o processo ou o item documental 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 óptico, 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 híbrido, 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, enviando 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 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 <i>ad hoc</i> . Nesse caso, cada passo significa o deslocamento de um documento, de um agente para		Registro de tramitação	Registra informações: identificação do documento, data/hora de transmissão, remetente, data/hora do recebimento, destinatário, situação do trâmite.

	outro, a fim de registrar uma manifestação ou decisão.				
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.	<i>O histórico de tramitação corresponde a um conjunto de metadados de datas de</i>		Registro de tramitação	Registra informações: identificação do documento, data/hora de transmissão, remetente, data/hora do recebimento, destinatário, situação do trâmite.

		<i>entrada e saída; nomes de responsáveis; providências etc.</i>		
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 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 à 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, atuação 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/expediente	Número sequencial atribuído ao processo ou expediente (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: órgão produtor, função, subfunção, atividade e série documental
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 <i>workflow</i> 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 várias associações entre as várias informações digitais relacionadas ao documento, isto é, anexos e <i>links</i> de hipertexto.			

3.1.4	Permitir a inserção de todos os metadados, 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, prevista nos Planos de Classificação de Documentos.
3.1.4.2	Número identificador atribuído pelo Sistema;		Identificador único	Registra o código gerado automaticamente que identifica o expediente, o processo ou o item documental de maneira a distinguí-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	Corresponde 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: órgão produtor, função, subfunção, atividade e série documental
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 <i>login</i> 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 da ação 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 ocorreram.			

3.1.4.18	Espécie/tipo/gênero 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, projeto de edificação.
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 à mesma pessoa ou situação;	Relação com outros documentos	Registro de relações significativas do documento com outros pelo fato de registrarem a mesma atividade, pessoa ou situação ou diferentes níveis de agregação (processo/expediente, 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 (<i>template</i>) necessárias para interpretar a estrutura do documento;		
3.1.4.23	Descritores (diferentes dos já estabelecidos nos Planos de		

	Classificação);			Localização	
3.1.4.24	Localização física;				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.
3.1.5	Prever a inserção 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.				
3.1.8	O número identificador atribuído pelo Sistema tem que:		<i>O identificador deve ser único e sequencial e pode ser numérico ou alfanumérico.</i>	Identificador único	Registra o código gerado automaticamente que identifica o expediente, o processo ou o item documental de maneira a distingui-los dos demais.
3.1.8.1	Ser gerado automaticamente, sendo vedada sua introdução manual e alteração posterior; ou				

<p>3.1.8. 2</p>	<p>Ser atribuído pelo usuário e validado pelo Sistema antes de ser aceito;</p>	<p><i>Uma opção seria gerar o número identificador automaticamente, mas nesse caso, ocultá-lo do usuário, permitindo a este introduzir uma seqüência não necessariamente única como um "identificador". O usuário empregaria essa seqüência como um identificador, mas o Sistema a consideraria como metadado pesquisável, definido pelo usuário.</i></p>		
<p>3.1.9</p>	<p>Prever a adoção da numeração única de documentos de acordo com a legislação específica a fim de garantir a integridade do</p>		<p>Classificação - código</p>	<p>Registra a referência numérica que associa o documento ao seu contexto de produção, composta das seguintes unidades de informação: órgão produtor, função, subfunção, atividade e série</p>

	número atribuído ao documento na unidade protocolizadora de origem.			documental
			Identificador único	Registra o código gerado automaticamente que identifica o expediente, o processo ou o item documental 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/expediente, 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	<i>Exemplo: o Sistema pode atribuir,</i>		

	metadados inseridos automaticamente e os demais a serem atribuídos pelo usuário.	<i>automaticamente, o número identificador, a data de captura, o originador e requerer que o usuário preencha os demais metadados.</i>		
3.1.13	Garantir a inserção de outros metadados após a captura.	<i>Exemplo: data e hora de alteração e mudança de suporte.</i>		
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 mantêm 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 todos 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 expediente/processo.			
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 1	Permitir importação de transações pré-definidas de arquivos em lote;	<i>Exemplos de lote de documento podem ser: mensagens de correio eletrônico, correspondência digitalizada por meio de escâner, 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.</i>	
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 de 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 híbridos			Relação com outros documentos	Registro de relações significativas do documento com outros pelo fato de registrarem a mesma atividade, pessoa ou situação ou diferentes níveis de agregação (processo/expediente, 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 magnético, 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.		<i>Essa informação só será acessada por usuários autorizados.</i>	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 <i>web</i> , 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 Tabelas de Temporalidade de Documentos, associadas aos Planos de Classificação dos órgãos ou entidades.			
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:		<i>As Tabelas de Temporalidade de Documentos dos órgãos e entidades deverão ser aprovadas pelo Arquivo Público do Estado de São Paulo, em conformidade com a legislação vigente.</i>	

4.1.3.1	Identificador do órgão ou entidade;		Órgão Produtor	Indica a instituição ou entidade juridicamente constituída e organizada responsável pela execução de funções do Estado.
4.1.3.2	Identificador da função, subfunção, atividade e série documental;		Classificação - código	Registra a referência numérica que associa o documento ao seu contexto de produção, composta das seguintes unidades de informação: órgão produtor, função, subfunção, atividade e série documental
			Classificação - nome	Refere-se à denominação do órgão produtor, da função, subfunção, atividade e série documental.
4.1.3.3	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)
4.1.3.4	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)
4.1.3.5	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.
4.1.3.6	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.
4.1.3.7	Evento que deflagra a contagem do prazo de retenção do documento na unidade produtora ou na unidade com atribuições de		Evento deflagrador de contagem de tempo	Evento que autoriza o início dos prazos prescricionais ou precaucionais, previstos nas Tabelas de Temporalidade de Documentos. Exemplo: aprovação das contas pelo TCE; término

	arquivo.			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:	<i>Acontecimentos específicos descritos na Tabela de Temporalidade como, por exemplo, “12 anos a contar da data de aprovação das contas” ou “vigência”, quando não puderem ser detectados automaticamente, deverão ser informados ao</i>		

		<i>Sistema por usuário autorizado.</i>		
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 pertencentes à mesma série documental.	<i>As alterações na Tabela de Temporalidade de Documentos só poderão ser feitas como resultado de um processo de reavaliação realizado pela Comissão de</i>	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).

		<p><i>Avaliação de Documentos de Arquivo do órgão ou entidade, em virtude de mudança do contexto administrativo, jurídico ou cultural. As propostas de alterações na Tabela de Temporalidade de Documentos deverão ser aprovadas pelo Arquivo Público do Estado, em conformidade com a legislação vigente.</i></p>		
4.1.9	<p>Prover funcionalidades para elaboração de relatórios que apoiem a gestão da Tabela de Temporalidade de Documentos, incluindo a capacidade de:</p>			
4.1.9.1	<p>Gerar relatório completo das Tabelas de Temporalidade de</p>			

	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 à 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.
4.2.4.1	Identificar, automaticamente, os documentos que cumpriram os prazos de guarda previstos na 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.
4.2.4.2	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 à 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			

	<p>deverá adotar, automaticamente, a temporalidade e a destinação da nova série.</p> <p>4.2.8 Quando um documento digital (objeto digital) estiver associado a mais de um expediente ou processo, e tiver prazos de guarda diferentes associados a ele, o Sistema tem que, automaticamente, verificar todos os prazos de guarda e destinações previstos para esse documento e garantir que o mesmo seja mantido em cada expediente/processo pelo tempo definido na tabela de temporalidade de documentos, de forma que:</p>	<p><i>Quando um documento digital estiver associado a mais de um expediente ou processo, 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</i></p>		
--	--	---	--	--

		<p><i>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 individualment e.</i></p>		
<p>4.2.8.1</p>	<p>A remoção de um documento de um expediente/processo não prejudique a manutenção desse mesmo documento em outro expediente/processo, até que todas as referências desse documento tenham atingido o prazo de guarda previsto;</p>			

4.2.8. 2	A manutenção de um documento em um expediente/processo de prazo de guarda mais longo não obrigue a permanência desse mesmo documento em outro expediente/processo 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 órgão ou entidade.			
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 seqüência 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	<p>todos os componentes de um documento digital sejam exportados como uma unidade. Por exemplo, uma mensagem de correio eletrônico e seus respectivos anexos;</p>			
4.3.3.3	<p>todos os metadados do documento sejam relacionados a ele de forma que as ligações possam ser mantidas no novo Sistema;</p>			
4.3.3.4	<p>todas as ligações entre documentos e volumes sejam mantidas.</p>			
4.3.4	<p>Exportar todos os tipos de documentos que está apto a capturar.</p>			
4.3.5	<p>Produzir um relatório detalhando 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.</p>			
4.3.6	<p>Conservar todos os documentos digitais que tiverem sido exportados, pelo menos até que tenham sido importados no Sistema destinatário com êxito.</p>			
4.3.7	<p>Manter metadados relativos a documentos que foram</p>	<i>O</i>	<i>Administrador</i>	

	exportados.	<i>deve indicar o subconjunto de metadados que deverá ser mantido.</i>		
4.3.8	Gerar listagem em meio digital e em papel para descrever documentos digitais que estão sendo exportados.	<i>Este requisito se aplica principalmente nos casos em que é feita exportação para transferência ou recolhimento para o Arquivo Público do Estado. Nesse caso, a listagem deverá ser produzida no formato estabelecido pelo Arquivo Público do Estado.</i>		
4.4	Eliminação		Registro da eliminação	Registra informações: data/hora da eliminação, responsável pela eliminação, número da relação de eliminação, do edital e do termo de eliminação.
4.4.1	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 à 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.	<p><i>Um relatório deverá seguir o modelo da Relação de Eliminação de Documentos, conforme anexo I a que se refere o artigo 26 do Decreto nº 48.897/2004, e o outro deverá seguir o modelo do Edital de Ciência de Eliminação de Documentos, conforme anexo II a que se refere o artigo 27 do Decreto nº 48.897/2004.</i></p>	<p><i>O Sistema deverá gerar o Termo de Eliminação de Documentos,</i></p>	<p>Registra informações: data/hora da eliminação, responsável pela eliminação, número da relação de eliminação, do edital e do termo de eliminação.</p>
4.4.7	Manter metadados relativos aos documentos que foram eliminados. O Administrador deve indicar o subconjunto de metadados que deverá ser		Registro da eliminação	

	mantido.			
4.5	Avaliação de documentos arquivísticos convencionais, digitais e híbridos		<i>conforme anexo III a que se refere o artigo 28 do Decreto nº 48.897/2004.</i>	
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, série, atividade, subfunção, função) 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 expediente, o processo ou o item documental 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 <i>login</i> onde o documento é gerado ou enviado.
5.2.5.6	Classificação de acordo com os Planos de Classificação.		Atividade	Indica a ação, encargo ou serviço decorrente do exercício de uma função, que pode ser identificada como atividade-meio ou atividade-fim.
			Função	Indica o conjunto de atividades que o Estado exerce para a consecução de seus objetivos, que pode ser identificada como direta ou essencial e indireta ou auxiliar.
			Órgão Produtor	Indica a instituição ou entidade juridicamente constituída e organizada responsável pela execução de funções do Estado.

			Série	Indica o conjunto de documentos do mesmo tipo documental produzido por um mesmo órgão, em decorrência do exercício da mesma função, subfunção e atividade e que resultam de idêntica forma de produção e tramitação e obedecem à mesma temporalidade e destinação.
			Subfunção	Indica o agrupamento de atividades afins, correspondendo cada subfunção a uma modalidade da respectiva função.
5.2.6	Permitir a pesquisa e recuperação de uma série documental completa e exibir a lista de todos os documentos que a 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 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.
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	redefinir 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 expediente ou processo.				
5.3.11	Permitir que todos os documentos de um expediente ou processo sejam impressos em uma única operação, na seqüência 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 <i>web</i> .				
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 <i>backup</i> 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, utilizando 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, papel e grupo)
1				Nome do agente	Indica o nome do agente que pode se apresentar como usuário, papel (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.	<i>Senha, crachá, chave criptográfica, token USB, smartcard, biometria (de impressão digital, de retina, etc.) são exemplos de credenciais de autenticação.</i>	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, à função, subfunção, atividade e série.				
6.2.7	O acesso a documentos ou séries, 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 a função ou série à qual o documento pertence.				
6.2.11	O acesso a documentos ou séries 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	Classificação da segurança da informação quanto à categoria e ao grau de sigilo				
			Classificação de segurança		Refere-se à atribuição de categorias e graus de sigilo aos documentos ou às 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		Registra informações: data/hora e responsável pela desclassificação de categoria e grau de sigilo.

			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;	<i>O grau de sigilo do documento tem que estar associado à credencial de segurança do usuário.</i>	Grau de sigilo	Especificação 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 à 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 série, 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 (<i>default</i>) para os			

	atributos de segurança e marcações 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.	<i>Os documentos sigilosos têm que se tornar ostensivos para serem submetidos ao processo de avaliação e serem destinados.</i>		
6.3.12	Implementar metadados em relação aos documentos ou extratos de documentos para controlar o acesso à 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 séries;				
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 <i>backups</i>) e de importação (inclusive <i>restore</i>);				
6.4.1.	Usuário, data e hora de acesso ou				

11	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.	<i>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 o com a subsequente liberação do espaço original. A exportação é a cópia sem a liberação do</i>		

		<i>espaço.</i>		
6.4.6	Fornecer relatórios sobre as ações que afetam séries, unidades de arquivamento e documentos, em ordem cronológica e organizados por:			
6.4.6.1	Documento arquivístico, unidade de arquivamento ou série;			
6.4.6.2	Usuário;			
6.4.6.3	Tipo de ação ou operação.			
6.4.7	Somente Administradores autorizados, acompanhados do auditor, têm 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 àqueles usuários portadores da 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.	<i>A remoção da cifração pode ocorrer quando a sua manutenção resultar em indisponibilidade de do documento. Por exemplo, quando a chave de cifração/decifração estiver embarcada em hardware inviolável cuja vida útil está prestes a se</i>		

		<i>esgotar ou quando o documento for desclassificado</i>		
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 informação contida em marcas d'água digitais.			
6.7.2	Armazenar documentos arquivísticos digitais que contêm 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 incluem:	Registro de transferência	Registra informações: data/hora de envio, data/hora de recebimento, destinatário, método utilizado, responsável pela transferência, método utilizado, recebimento, localização/suporte anterior, localização/suporte atual, identificação do lote, número do termo de transferência.
6.8.2.1	Número identificador dos documentos atribuído pelo Sistema;	Identificador único	Registra o código gerado automaticamente que identifica o expediente, o processo ou o item documental 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.		
			<i>Na restauração ao estado seguro, o Sistema deve ser capaz de garantir a recuperação de perdas</i>

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.			
6.10	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.		<i>Anular uma operação não significa apagar um</i>	

		<i>documento arquivístico capturado pelo Sistema. Não é possível anular a eliminação definitiva de documentos, por tratar-se de operação irreversível.</i>		
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 Arquivo Público do Estado/Departamento de Gestão do Sistema de Arquivos do Estado de São Paulo-SAESP;			
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 confirmação 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 têm 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 (<i>Mean Time Between Failure</i>), 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.	<i>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</i>		

		<i>utilizadas informações de fornecedores. Em ambos os casos, deve ficar registrada a origem da informação.</i>	
7.1.5	Quando se proceder à eliminação de documentos, as memórias de suporte têm que ser devidamente limpas, isto é, ter suas informações efetivamente indisponibilizadas.	<i>Este requisito aplica-se principalmente às memórias secundária e terciária, pela sua característica não volátil. As informações devem ser eliminadas de forma irreversível, incluindo, no caso de memória terciária, a possibilidade de destruição física das mídias.</i>	
7.2	Capacidade		

<p>7.2.1</p>	<p>Possuir capacidade de armazenamento suficiente para acomodação de todos os documentos e suas cópias de segurança. Nesse sentido, os testes de carga deverão anteceder a implementação do Sistema.</p>	<p><i>Para grandes volumes de dados é conveniente o uso de dispositivos com maior capacidade unitária de armazenamento o, a fim de reduzir a sobrecarga operacional.</i></p>	
<p>7.2.2</p>	<p>Em um Sistema, tem que ser prevista a possibilidade de expansão da estrutura de armazenamento.</p>	<p><i>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”</i></p>	

		<p><i>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").</i></p>		
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 procedimento 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 útil prevista e/ou pretendida, dentro das especificações técnicas de seu fabricante e de entidades isentas e com base em estatísticas de uso.	<i>A vida útil pretendida de um suporte pode ser menor que sua vida útil prevista, o que permite condições ambientais mais flexíveis.</i>		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 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, informação sobre assinatura digital, relação entre os objetos.
8.2	Aspectos lógicos				

8.2.1	Manter cópias de segurança.	<i>As cópias de segurança devem ser guardadas em ambientes seguros, em local diferente de onde se encontra a informação original.</i>	Cópias de segurança	Registra informação sobre as cópias de segurança de documentos arquivísticos digitais e seus metadados, bem como de parâmetros do sistema operacional, do gerenciador 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 à detecção de possíveis erros.	<i>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.</i>		
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 à preservação dos documentos e seus respectivos componentes.				
9	Funções Administrativas				
9.1	Permitir que o Administrador, de uma maneira controlada e sem esforço excessivo, recupere, 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, expedientes), volumes e itens, a partir de parâmetros ou atributos definidos (tempo, função, série, unidade administrativa etc);				
9.2.2	Estatísticas de transações 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 à política de arquivos e gestão documental				

	implementada pelo Arquivo Público do Estado, órgão central do Sistema de Arquivos do Estado de São Paulo.			
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 às funcionalidades administrativas impossibilitando sua visualização ao usuário final.	<i>Exemplos: as operações não disponíveis aparecem com fonte atenuada nos menus e possuem efeito nulo quando acionadas. O acesso às operações indisponíveis é restrito pela configuração de menus que não as apresentam ao usuário sem permissão para executá-las.</i>		
12	Interoperabilidade			

12.1	O Sistema deve interoperar com outros sistemas de informação, incluindo sistemas legados de controle de documentos, através de padrões abertos de interoperabilidade.	<p><i>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 comprometer o funcionamento do Sistema. Isto se faz através do uso de regras e padrões de comunicação.</i></p>	
12.2	O Sistema deve aplicar os requisitos de segurança descritos neste documento para executar	<p><i>Isso é fundamental para que as</i></p>	

	operações de interoperabilidade.	<i>operações, feitas em ambiente com interoperabilidade, não afetem a integridade dos documentos e impossibilitem acessos não autorizados.</i>		
13	Disponibilidade			
13.1	O Sistema deve se adequar ao grau de disponibilidade estabelecido pelo órgão ou entidade.	<i>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</i>		

14	Desempenho e Escalabilidade		<i>fornecido, os períodos previstos de atendimento, bem como o tempo máximo tolerável em interrupções previstas.</i>	
14.1	Incluir rotina de manutenção de:		<i>Essas tarefas devem atender a mudanças planejadas, sem causar grandes sobrecargas de administração.</i>	
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.			

APÊNDICE 2

Requisitos altamente desejáveis e seus respectivos metadados para os sistemas informatizados de gestão arquivística dos documentos convencionais e digitais produzidos pelo Governo do Estado de São Paulo. Anexo II a que se refere o artigo 5º da Instrução Normativa APE / SAESP – 1/2009.

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.			
1.1.2	Deve possibilitar a consulta ao Plano de Classificação de Documentos a partir de qualquer atributo ou combinação de atributos e gerar relatórios com os resultados obtidos.			
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 à 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.	<i>Quando um documento digital estiver associado a outros documentos, o Sistema deverá criar um registro para cada referência aos documentos associados.</i>		
1.4	Requisitos adicionais para o gerenciamento de documentos			
1.4.1	Deve prever funcionalidades para apoiar a pesquisa de existência de documento relativo à mesma ação ou interessado.			
1.5	Volumes: abertura, encerramento e metadados			
1.5.1	Deve ser capaz de gerenciar volumes para subdividir processos, fazendo distinção entre processos e volumes.			

1.5.2	Deve permitir a associação de metadados aos volumes e deve restringir a inclusão e a alteração desses mesmos metadados somente a usuários autorizados.			
1.5.3	Deve permitir o registro de metadados correspondentes às datas de abertura e de encerramento de volumes.			
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 requirem sua atenção.	<i>Esse requisito requer a integração com um Sistema de correio eletrônico existente.</i>		
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.	<i>Um usuário pode precisar enviar um documento a outro usuário, devido ao seu conteúdo ou no caso do usuário responsável se encontrar em licença.</i>		
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.	<i>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.</i>		
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 Sistema 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 expediente, sem duplicação física do mesmo.	<i>Quando um documento digital estiver associado a mais de um expediente/processo, o Sistema deverá criar um registro para cada referência desse documento. Cada registro estará vinculado ao mesmo objeto digital.</i>		
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.	<i>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.</i>		
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 à sua atividade;			
3.1.4.2	Indicar as últimas classificações feitas pelo usuário;			

3.1.4.3	Indicar expedientes ou processos 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 lsa25@ab.br.			
3.3	Formato de arquivo e estrutura dos documentos a serem capturados			
3.3.1	Deve poder capturar, entre outros, os seguintes documentos:	<i>A lista de documentos, que um Sistema tem que suportar, irá variar de órgão para órgão.</i>		
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 escâner;			
3.3.1.4	Documentos sonoros;			
3.3.1.5	Vídeos; Vídeos;			
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 arquivo 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	<i>Exemplo: uma correspondência sem assinatura digital válida ou</i>		

	inconsistente de uma forma que venha a comprometer sua futura autenticidade.	<i>uma fatura de fornecedor não identificado.</i>		
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, responsável 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, dispositivo 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;				
4.3.1.3	De acordo com o formato definido pelo Arquivo Público do Estado 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 à 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			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

	adequado antes de confirmar a exportação da parte sob forma digital.			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 por meio 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 um ambiente <i>web</i> .			
5.1.2	Deve prever a navegação gráfica no plano de classificação, a navegação direta de uma função, subfunção, atividade ou série para os documentos arquivísticos nessa mesma função, subfunção, atividade ou série, 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 <i>booleanos</i> : “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 à direita para a pesquisa de metadados.	<i>Exemplos: o argumento de pesquisa “Bra*il” pode recuperar “Brasil” e “Brazil”; o argumento de pesquisa “Arq*” pode recuperar “Arquivo”, “Arquivística” etc.</i>		
5.2.5	Deve permitir a utilização de caracteres coringa e de truncamento à direita para 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 <i>default</i> 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;			
5.3.2.3	Estabelecimento do número máximo de resultados para uma pesquisa;			
5.3.2.4	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 a série em que está incluído;			
5.3.3.2	De uma série para os documentos nela incluídos;			
5.3.3.3	De uma série para a atividade, subfunção e função correspondentes;			
5.3.3.4	De uma atividade, subfunção e função para as séries a elas relacionadas.			
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:			
5.3.5.1	Formato XML adequado pra 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-			
			<i>No que se refere a interoperabilidade com outros Sistemas, ver código 10 Interoperabilidade</i>	

	selecionados.				
6	Segurança				
6.1	Cópias de segurança				
6.1.1	As mídias removíveis devem ter cópias em suportes equivalentes e armazenamento <i>off-site</i> .				
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.			<i>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.</i>	
6.1.5	Dados críticos de configuração e controle do Sistema operacional e do gerenciador 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 <i>off-site</i> .			
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):	<i>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 requeram 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</i>		

		<i>documento (texto livre).</i>		
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 à 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.		<i>Para facilidade de relatório, os resultados podem ser apresentados ordenados, mas esta ordenação não pode alterar os dados contidos na trilha.</i>	
6.4.3	Deve ser capaz de gerar um alarme, para os administradores apropriados, se o tamanho da		<i>Esse alarme deve ser usado para indicar a proximidade do esgotamento de espaço</i>	

	trilha de auditoria exceder um limite preestabelecido.	reservado à 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.	<i>Todas as outras operações estariam bloqueadas até a liberação pelo Administrador.</i>		
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 <i>login</i> com erro (autenticação mal sucedida), conforme especificado pela política de segurança;			
6.4.6.2	Ocorrência de vários <i>login</i> simultâneos do mesmo usuário em locais (computadores) diferentes;			
6.4.6.3	<i>Login</i> do usuário fora do horário autorizado, após <i>logout</i> 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 à 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.		<i>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/).</i>	
6.6	Criptografia			

6.6.1	Deve poder assegurar a captura de documentos cifrados, diretamente de uma aplicação de <i>software</i> que disponha da funcionalidade da cifração.			
6.6.2	Deve possuir uma arquitetura capaz de receber atualizações tecnológicas quanto à plataforma criptográfica.			
6.7	Marcas d'água digitais			
6.7.1	Deve possuir uma arquitetura capaz de receber atualizações tecnológicas quanto à 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 efetivação da 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.	<i>Permissões de controle de acesso, chaves criptográficas e parâmetros de algoritmos criptográficos são exemplos de dados de segurança.</i>		
6.9.4	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.			
6.9.5	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 irreparáveis, deve inibir a eliminação (permanente ou lógica) de grupos ou lotes de documentos fora do processo regular de eliminação previsto 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:	<i>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 impressa ou reproduzida por meios audiovisuais, independentemente da utilização de quaisquer recursos, tais como rotação, variação focal ou qualquer outra manifestação.</i>	
6.10.2.1	Retiradas 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 vídeos ou de áudio, caso existam.		
6.10.3	Deve registrar no documento original uma referência 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.	<i>Um Sistema deve utilizar preferencialmente padrões abertos de armazenamento (como exemplo: ISO 9660:1999 – definição do formato de Sistemas de arquivos para CR-Rom). A escolha dos dispositivos de armazenamento deve contemplar padrões estáveis de mercado e fornecedores consolidados.</i>		
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 à ação de cópias de segurança.			
7.1.4	O acesso às informações armazenadas em memória terciária deve ser efetuado preferencialmente mediante uso de rede de dados.	<i>O objetivo é minimizar o acesso físico às mídias, visando diminuição do desgaste. A manipulação direta das mídias deverá ser restrita aos administradores</i>		

		<i>do Sistema e não aos usuários comuns.</i>		
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.	<i>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.</i>		
7.2.3	Deve informar automaticamente ao Administrador quando os dispositivos de armazenamento <i>on line</i> 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.	<i>Este tipo de estimativa possibilita ao administrador antecipar ações de expansão antes que a utilização atinja níveis críticos.</i>		
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 (<i>mirroring</i>) nas memórias secundárias para maior confiabilidade;				
7.3.2.2	Partição de dados (<i>data stripping</i>) 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 objetos.	
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 objetos.	
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 <i>hardware</i> e <i>software</i> que sejam maduros, estáveis no mercado e amplamente disponíveis.			
8.3.2	Deve utilizar normas amplamente aceitas, descritas em especificações abertas e disponíveis publicamente, no que se refere às 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	Deve possuir documentação completa, clara, inteligível e			

	organizada para a instalação e uso do <i>software</i> .			
9.1.2	Deve possuir Sistema de ajuda <i>on line</i> .			
9.1.3	A ajuda <i>on line</i> fornecida pelo Sistema deve ser vinculada à função ou tarefa executada, em todo o Sistema.	<i>Exemplo: quando se está executando uma operação de edição, uma vez acionada a ajuda, ela deve remeter para o tópico da ajuda edição.</i>		
9.1.4	O Sistema deve permitir a personalização de conteúdo de ajuda <i>on line</i> por adição de texto ou edição de texto existente.	<i>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.</i>		
9.1.5	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.			
9.1.6	A interface do Sistema deve seguir padrões pré-estabelecidos e consolidados como boas práticas de projeto gráfico.	<i>Normas ou regras de interface podem ser relativas à utilização de padrão de identidade visual (ligado à “marca” da instituição ou alguma legislação específica do Estado, bem como a utilização de guias de estilo para implementação e padronização da interface.</i>		

9.1.7	Deve empregar um conjunto simples e consistente de regras de interface, privilegiando a facilidade de aprendizado de operação pelos seus usuários.	<i>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 à padronização da terminologia utilizada para funções, rótulos e ações consistentes em toda a aplicação.</i>		
9.1.8	A interface de visualização dos documentos arquivísticos deve fornecer o recurso de arrastar e soltar, se apropriado no ambiente operacional do Sistema.			
9.1.9	Deve permitir que a sua estrutura de funções, subfunções, atividades e séries possa ser visualizada em diferentes formas de apresentação.			
9.1.10	Deve ser possível personalizar a interface gráfica com o usuário de um Sistema. A personalização deve incluir pelo menos as seguintes possibilidades:			

9.1.10	Conteúdos de menus;				
9.1.10.1	Formatos de telas;				
9.1.10.2	Utilização de teclas de função;				
9.1.10.3	Alteração de cores, fontes e tamanhos de fontes em telas e janelas;				
9.1.10.4	Avisos sonoros.				
9.1.10.5	Sempre que o Sistema utilizar janelas <i>pop-up</i> e barras de ferramentas, deve-se permitir ao usuário a possibilidade de configuração e de habilitar/desabilitar esse tipo de recurso.				
9.1.11	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.				
9.1.12	Deve permitir a seleção de avisos sonoros e a personalização de tom e volume, bem como a gravação dessas escolhas no perfil do usuário.				
9.1.13	Deve permitir a gravação de opções <i>default</i> para entrada de				
9.1.14					

	dados de configuração:				
9.1.14 .1	Valores de variáveis definidas pelo usuário;				
9.1.14 .2	Valores iguais aos de um item anterior;				
9.1.14 .3	Valores que possam ser selecionados de uma lista configurável;				
9.1.14 .4	Valores derivados do contexto, como data, referência do documento, identificador do usuário;				
9.1.14 .5	Valores pré-definidos por um Administrador (para campos de metadados como, por exemplo, o nome da organização que está utilizando o Sistema).				
9.1.15	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 <i>software</i> especializado que possa vir a ser acoplado (por exemplo, leitores de telas para cegos), bem como seguir orientações específicas de acessibilidade de interface.			<i>Para ambientes e sítios apoiados na web é importante seguir orientações específicas de acessibilidade. É desejável que o padrão seguido possa ser verificado através da aplicação de uma validação manual ou automática, de preferência visando à obtenção de certificação de acessibilidade.</i>	

9.1.16	Deve permitir a realização de transações ou tarefas mais frequentemente executadas com um pequeno número de repetições (por exemplo, cliques de <i>mouse</i>) e sem mudanças excessivas de contexto.			
9.1.17	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.	<i>Esse requisito deve estar de acordo com as normas de segurança.</i>		
9.1.18	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.			
9.1.19	Deve possuir integração com o Sistema padrão de edição de documentos, de modo que possa fazer uso da facilidade de gravação.			
9.1.20	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		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

	<i>hyperlinks</i> .			agregação (processo/expediente, volume e documento) ou diferentes manifestações do mesmo documento em diversos formatos.
9.1.21	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.
9.1.22	Deve fornecer para os usuários finais e administradores funções intuitivas e fáceis de usar, que requeira poucas ações para completar uma tarefa padrão. Particularmente em operação normal, o Sistema deve ser capaz de:			
9.1.22 .1	Capturar e declarar um documento arquivístico com, no máximo, três cliques de <i>mouse</i> ou acionamentos de telas;			
9.1.22 .2	Apresentar todos os elementos de metadados obrigatórios para a captura do documento com mínima demanda para o usuário;			
9.1.22 .3	Apresentar o conteúdo de um documento arquivístico, a partir de uma lista de pesquisa, com no máximo três cliques de <i>mouse</i> ou acionamentos de telas;			

9.1.22.4	Apresentar os metadados de um documento arquivístico com no máximo, três cliques de <i>mouse</i> ou acionamentos de tarefas.			
9.1.23	Deve levar em consideração as condições de operação como ruído, luminosidade, necessidade de rapidez na conclusão da tarefa, necessidades específicas para dispositivos móveis, ambiente <i>desktop/web</i> e necessidades de instalação automática, para configurar as formas de interação com o usuário.	<i>Exemplo: não se deve utilizar menus audíveis em ambientes que apresentam alto volume de ruídos na proximidade dos terminais de usuários.</i>		
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.	<i>As operações de interoperabilidade devem respeitar a legislação vigente e a política de segurança.</i>		
10.2	Deve ser capaz de interoperar com outros Sistemas através de padrões abertos de interoperabilidade.	<i>Exemplo: padrões abertos como os estabelecidos pela e-PING, XML e Dublin Core.</i>		
11	Desempenho e Escalabilidade			
11.1	Deve manter estatísticas dos tempos de atendimento, discriminados por tipo de operação.			
11.2	Deve ser expansível até comportar um número máximo preestabelecido de usuários			

	simultâneos, provendo continuidade efetiva de serviços.			
11.3	Deve ser escalável, a fim de permitir adaptação a organizações de diferentes tamanhos e complexidades.			
11.4	Deve fornecer evidências de grau de escalabilidade ao longo do tempo. Avaliações quantitativas devem incluir:			
11.4.1	O número máximo de <i>sites</i> remotos suportados com desempenho adequado;			
11.4.2	O tamanho máximo do repositório, expresso em <i>Gigabytes</i> ou <i>Terabytes</i> , que pode ser suportado com desempenho adequado;			
11.4.3	O número máximo de usuários simultâneos que possam ser atendidos com desempenho adequado;			
11.4.4	A sobrecarga administrativa prevista para um período de cinco anos, permitindo crescimento do número de usuários e da quantidade de registros;			
11.4.5	A quantidade de reconfigurações e de indisponibilidades previstas para um período de cinco anos, permitindo o crescimento do número de usuários e da			

<p>11.4.6</p>	<p>quantidade de registros; 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.</p>			
----------------------	--	--	--	--

