INSTITUTO FEDERAL
BRASÍLIA

2016

LEVANTAMENTO DE REQUISITOS PARA IMPLANTAÇÃO DO PROCESSO ELETRÔNICO NACIONAL NO IFB

Grupo de Trabalho - PEN
Instituto Federal de Brasília - IFB

Grupo de Trabalho

Anderson da Silva Costa
Daniel Souza Coelho
Diego Brum Lima Rocha
Edimária Cerqueira Rodrigues Lamounier
Felipe Henrique de Melo
João Bezerra da Silva Júnior
Lucas Marinho Pimenta
Paulo Henrique Borges Silva
Pompylio Jeronimo de Lima

17/02/2016

Sumário

I - Introdução 5
II - Objetivo 6
III - Metodologia 6
IV - Legislação 7
V - Desenvolvimento 8
1. Estrutura Prévia à Implementação do Sistema 8
1.1 Gestão Documental 8
1.1.1 Unidade Organizacional 8
1.1.2 Espaço Físico, Recursos e Pessoal Qualificado 8
1.1.3 Comissão Permanente de Avaliação de Documentos (CPAD) 10
1.1.4 Política Arquivística 11
1.1.5 Considerações 12
1.2 Infraestrutura de Tecnologia da Informação e Comunicação 13
1.2.1 Detalhamento dos Serviços 13
1.2.2 Considerações 17
2.1 Ações de Gestão Documental 17
2.1.1 Captura 18
2.1.2 Gerenciamento de Documentos Físicos, Híbridos e Digitais 23
2.1.3 Avaliação, Temporalidade e Destinação 24
2.1.4 Eliminação 24
2.1.5 Transferência 24
2.1.6 Recolhimento 24
2.1.7 Pesquisa, Localização e Apresentação dos Documentos 25
2.1.8 Armazenamento 25
2.1.9 Preservação 27
2.1.10 Considerações 27
2.2 Ações de Protocolo 28
2.2.1 Recebimento, Classificação e Registro 29
2.2.2 Distribuição 31
2.2.3 Controle de Tramitação 31
2.2.4 Expedição 32
2.2.5 Exigência 32

2.2.6 Atuação 33
2.2.7 Numeração de Folhas 33
2.2.8 Encerramento e Abertura de Volumes 33
2.2.9 Despacho 34
2.2.10 Juntada 34
2.2.11Desapensação 35
2.2.12 Desentranhamento 35
2.2.13 Desmembramento 36
2.2.14 Reconstituição de Processo 36
2.2.15 Capa do processo 37
2.2.16 Arquivamento 37
2.2.17 Desarquivamento 38
2.2.18 Empréstimo/Vistas 38
2.2.19 Considerações 38
2.3 Segurança 39
2.3.1 Controle de Acesso 39
2.3.2 Classificação de Sigilo e Restrição de Acesso 40
2.3.3 Uso e Rastreamento 40
2.3.4 Trilha de Auditoria 41
2.3.5 Cópias de Segurança 41
2.3.6 Assinatura Digital 41
2.3.7 Criptografia 42
2.3.8 Marcas D'água 43
2.3.9 Acompanhamento de Transferência 43
2.3.10 Autoproteção 43
2.3.11 Segurança da Infraestrutura 44
2.3.12 Considerações 44
2.4 Metadados 46
2.4.1 Documento 46
2.4.2 Evento de Gestão 47
2.4.3 Classe 48
2.4.4 Agente 48
2.4.5 Componente Digital 48
2.4.6 Evento de Preservação 49
2.4.7 Considerações 49
2.5 Preservação Digital 50

2.5.1 Política de Preservação 50
2.5.2 Independência de Hardware Específico 51
2.5.3 Independência de Software Específico 51
2.5.4 Independência do Sistema Gerenciador 52
2.5.5 Migração Periódica de Suporte e Formato 53
2.5.6 Replicação do Sistema em Local Distante 55
2.5.7 Suporte de Armazenamento 55
2.5.8 Backup/Cópias de Segurança 56
2.5.9 Eliminação Periódica do Lixo Digital 57
2.5.10 Garantia da Autenticidade 58
2.5.11 Considerações 59
2.6 Plano de Gestão de Riscos de TI – Implantação do Processo Eletrônico Nacional no IFB 60
2.6.1 Contexto e Identificação dos Riscos 61
2.6.2 Estimativa, Avaliação e Tratamento 62
VI - Conclusão 70
VI - Referência Bibliográfica 71
ANEXOS 75

I - Introdução

O Decreto n° 8.539, de 8 de outubro de 2015, trouxe a necessidade da mudança de paradigma no que diz respeito aos processos administrativos nos órgãos da administração pública federal, os quais se encontram intimamente ligados à "cultura do papel" e aos procedimentos analógicos pertinentes a esta.

A sociedade contemporânea, por sua vez, vive em transformação constante advinda da evolução tecnológica, transformando a forma como as pessoas se relacionam, consomem e vivem, gerando a necessidade de adequação da administração pública para atender de forma mais eficiente as demandas cada vez crescentes desta população digital imersa na sociedade da informação.

Conforme o paradigma em questão, o Processo Eletrônico Nacional (PEN) vem como uma ação generalizada, abarcando órgãos e entidades da administração pública federal direta, autárquica e fundacional, exigindo a adoção de um Sistema Informatizado de Gestão Arquivística de Documentos (SIGAD) para os procedimentos administrativos, promovendo a ruptura da cultura analógica do papel, aproximando as entidades das demandas da sociedade por celeridade, transparência e eficiência.

Devido a obrigatoriedade de adoção ao PEN, foi instituído um Grupo de Trabalho Multidisciplinar - pela Portaria n° 2.797, de 8 de dezembro de 2015 - para realizar o levantamento dos requisitos mínimos para implantação do PEN no IFB.

Ao longo dos trabalhos verificou-se que o tema em questão encontra-se imerso em riscos e problemáticas técnicas e financeiras, pois a adoção de um sistema informatizado implica em ter todos os dados e documentos da Instituição disponíveis em rede, gerando riscos quanto a segurança desta informação, sua inviolabilidade, gestão e acesso, exigindo planejamento e estudos por parte da Instituição para que a adoção do sistema não comprometa a história institucional bem como seus documentos e recursos.

O relatório elenca quais requisitos devem estar presentes no SIGAD de forma a minimizar riscos e promover a gestão documental. Entretanto, fica claro que este trabalho não resume as ações necessárias à adoção ao PEN, sendo um relatório técnico norteador para futuro aprofundamento no tema com um planejamento exaustivo das ações e estudos que este tema ainda demanda.

II - Objetivo

Realizar levantamento dos requisitos mínimos para a implantação do Processo Eletrônico Nacional (PEN), construindo um documento técnico norteador para as futuras ações e tomadas de decisão por parte da alta gestão.

III - Metodologia

Para a consecução deste documento foram realizadas reuniões técnicas com representantes das áreas de gestão, TI, governança, mercado, arquivologia e administração.

Nestes encontros foram analisadas legislações pertinentes ao PEN e à segurança da informação, apoiando-se em documentos técnicos relacionados à infraestrutura de Tecnologia da Informação e à implementação de Sistemas Informatizados de Gestão Arquivística de Documentos (SIGAD), bem como respeitando a bibliografia especializada.

O relatório em questão é o resultado dos estudos e debates técnicos multidisciplinares, o qual apresenta os requisitos mínimos para a implantação do SIGAD.

Vale salientar que em todo estudo foi levada em consideração a criticidade da implantação deste sistema para o Instituto Federal de Brasília, tendo em vista que se trata de manipulação e guarda de informações, as quais constituem um dos bens mais importantes da instituição.

IV - Legislação

- Decreto n° 8.539, de 8 de outubro de 2015, da Presidência da República
- Portaria MEC n° 1.042 de 04 de novembro de 2015
- Lei n° 6.546/1978, Presidência da República
- Decreto 4.073 de 03/01/2002, Presidência da República
- Resolução n° 14 de 24/10/2001 do CONARQ
- Portaria AN/MJ n° 92 de 23/09/2011
- Lei n° 12.527/2011, Presidência da República
- Lei n° 9.279/96, Presidência da República
- Lei n° 9.610/98, Presidência da República
- Lei n° 9.456/97, Presidência da República
- Lei n° 9.609/98, Presidência da República
- Lei n° 10.973/04, Presidência da República
- Lei n° 12.527/2011, Presidência da República
- Lei n° 10.180/2001, Presidência da República
- Lei n° 8112/90, Presidência da República
- Portaria CGU n° 1.613/2012
- NC 09 DSIC/GSI/PR

V - Desenvolvimento

1. Estrutura Prévia à Implementação do Sistema

1.1 Gestão Documental

A gestão documental compreende um conjunto de procedimentos e operações técnicas referentes à produção, tramitação, uso, avaliação e arquivamento de documentos em fase corrente e intermediária, visando a sua eliminação ou recolhimento para guarda permanente. Tais ações implicam, necessariamente, em uma estrutura prévia para efetivação da gestão de documentos.

1.1.1 Unidade Organizacional

- É preciso uma unidade organizacional/pessoa que responda diretamente pela gestão, guarda e normalização da área arquivística no Instituto.
- É necessário um referencial institucional quando se trata da gestão de documentos tanto para responsabilização perante aos órgãos de controle quanto para dar suporte às áreas no que diz respeito às demandas documentais.

1.1.2 Espaço Físico, Recursos e Pessoal Qualificado

- É fundamental ter um espaço físico projetado e destinado a ser o arquivo da Instituição para a concretude da gestão documental, pois é o local reservado ao tratamento técnico e guarda da documentação proveniente das unidades organizacionais pelo período estipulado nas tabelas de temporalidade das áreas meio e fim, instituídas pela Resolução n° 14 do CONARQ e pela Portaria AN/MJ n° 92, respectivamente.
- É imprescindível a presença de corpo técnico qualificado e especializado na área arquivística, de forma a garantir o suporte adequado à documentação conforme metodologia e legislação da área, promovendo as intervenções necessárias à organização e manutenção do acervo.

- Considerando o disposto na Lei n° 6.546/1978, é necessária a presença do arquivista para promover:
    - Planejamento, organização e direção de serviços de arquivo;
    - Planejamento, orientação e acompanhamento do processo documental e informativo;
    - Planejamento, orientação e direção das atividades de identificação das espécies documentais e participação no planejamento de novos documentos e controle de multicópias;
    - Planejamento, organização e direção de serviços ou centro de documentação e informação constituídos de acervos arquivísticos e mistos;
    - Planejamento, organização e direção de serviços de microfilmagem aplicada aos arquivos;
    - Orientação do planejamento da automação aplicada aos arquivos;
    - Orientação quanto à classificação, arranjo e descrição de documentos;
    - Orientação da avaliação e seleção de documentos, para fins de preservação;
    - Promoção de medidas necessárias à conservação de documentos;
    - Elaboração de pareceres e trabalhos de complexidade sobre assuntos arquivísticos;
    - Assessoramento aos trabalhos de pesquisa científica ou técnico-administrativa;
    - Desenvolvimento de estudos sobre documentos culturalmente importantes.

Ressalta-se a necessidade da presença de pelo menos 2 (dois) técnicos em arquivo para promover apoio aos analistas promovendo:

- Recebimento, registro e distribuição dos documentos, bem como controle de sua movimentação;
- Classificação, arranjo, descrição e execução de demais tarefas necessárias à guarda e conservação dos documentos, assim como prestação de informações relativas a estes;

- Preparação de documentos de arquivos para microfilmagem e conservação e utilização do microfilme;
- Preparação de documentos de arquivo para processamento eletrônico de dados.
    - Considerando o tamanho do Instituto, que conta com a presença de 10 *Campi* e reitoria, recomenda-se a presença de no mínimo 3 arquivistas para promover o tratamento técnico à documentação e às demais atividades previstas na legislação necessárias à gestão documental, contando com a presença de pelo menos 2 (dois) técnicos em arquivo para apoio às atividades.
- Recursos garantem a continuidade das ações documentais pois asseguram mobiliário adequado e materiais de consumo em quantidade e qualidade razoáveis para os trabalhos técnicos e guarda dos documentos em conformidade com as exigências legais.

1.1.3 Comissão Permanente de Avaliação de Documentos (CPAD)

A CPAD deve ser instituída tendo em sua composição os seguintes perfis profissionais, conforme anexo da Resolução n° 14 de 24/10/2001:

- Arquivista ou responsável pela guarda da documentação;
- Servidores das unidades organizacionais às quais se referem os documentos a serem destinados, com profundo conhecimento das atividades desempenhadas;
- Historiador ligado à área de pesquisa de que trata o acervo;
- Profissional da área jurídica, responsável pela análise do valor legal dos documentos;
- Profissionais ligados ao campo de conhecimento de que trata o acervo objeto da avaliação;
- Outros profissionais que possam colaborar com as atividades da comissão (Considerando o panorama atual de documentos digitais, é recomendável a participação de profissionais da área de tecnologia da informação);

- A presença da CPAD justifica-se pelo Decreto 4.073 de 03/01/2002, que determina sua constituição em todos os órgãos e entidades da Administração Pública Federal, sendo responsável por:
  - Orientar e realizar o processo de análise, avaliação e seleção da documentação produzida e acumulada no âmbito do órgão tendo em vista a identificação dos documentos para a guarda permanente e ou eliminação.
  - Analisar, avaliar e selecionar a documentação da área meio observando-se a tabela de temporalidade e destinação presente em anexo à Resolução n° 14 de 24/10/2001 do CONARQ.
  - Analisar, avaliar e selecionar a documentação da área fim observando-se a tabela de temporalidade e destinação presente em anexo à Portaria AN/MJ n° 92 de 23/09/2011.
  - Estabelecer os prazos de guarda e a destinação final dos documentos não constantes nas tabelas de temporalidade e destinação das áreas meio e fim, observando-se a aprovação prévia pelo Arquivo Nacional.

1.1.4 Política Arquivística

- A política arquivística efetivará procedimentos, normas, treinamentos e rotinas de trabalho conforme a legislação e metodologia arquivísticas, possibilitando a efetivação da gestão documental desde a criação do documento até a sua destinação final.
- É recomendável a inclusão da política no Plano Diretor Institucional (PDI) por trazer legitimidade às ações relacionadas à gestão documental por se configurar como objetivo organizacional, sendo fundamental para o sucesso da política. Ressalta-se que é imprescindível o apoio da alta gestão para a consecução das metas relacionadas à gestão de documentos.
- Possibilita a alocação de recursos e servidores na gestão documental.
- Possibilita discussões em nível institucional acerca das ações documentais.
- Passos para implementação da política:

- Formação de equipe multidisciplinar contendo os seguintes profissionais: profissionais da área de tecnologia da informação; arquivista ou responsável pela guarda da documentação; profissionais da área jurídica; profissionais da administração; historiador; profissionais ligados à área finalística do instituto.
- Elaboração da política arquivística por meio de Portaria Normativa contendo padronização de procedimentos, rotinas de trabalho, diagnóstico da situação documental atual e cronograma para implementação/conclusão das ações de gestão de documentos.
- Preparação da infraestrutura e ambiente necessários para assegurar o sucesso da política.
- Implantação da política.
- Revisão e adaptações periódicas.

1.1.5 Considerações

No que tange à estrutura de gestão documental, as recomendações presentes neste subitem se fazem necessárias tendo em vista que a implementação de um sistema informatizado de gestão arquivística de documentos implica em tê-la em suporte convencional já estabelecido, não sendo possível o sucesso da implementação do sistema sem a adequação prévia aos requisitos elencados.

O não atendimento às demandas acarretarão em dificuldade de implementação e gestão do sistema, transferindo os mesmos problemas de gestão documental do suporte convencional para o meio eletrônico, isto é: ineficiência de busca e recuperação da informação, ausência de metodologia científica para as ações documentais, ineficiência e subaproveitamento do sistema, além de não atender às exigências legais no que diz respeito à documentação de arquivo do IFB, podendo a ausência desses itens ser objeto de auditorias que impliquem em prejuízos à instituição.

Não sendo possível a adoção, na íntegra, das recomendações elencadas, deve-se atentar quanto à prioridade da adoção dos requisitos. Para tanto, foi estabelecido o padrão de 1 a 3, sendo que 1 é extremamente necessário, 2 é necessário e 3 é altamente desejável:

- Unidade organizacional (1)

- Espaço físico (2)
- Recursos (no que diz respeito a estantes, caixas arquivo, luvas, máscaras e demais itens necessários ao armazenamento e tratamento dos documentos) (2)
- Pessoal qualificado (1)
- Comissão Permanente de Avaliação de Documentos (1)
- Política arquivística (1)

1.2 Infraestrutura de Tecnologia da Informação e Comunicação

Entendendo um Sistema Informatizado de Gestão Arquivística de Documentos (SIGAD) como um conjunto de tecnologias que permite a instituição gerenciar seus documentos arquivísticos em forma digital, é importante o provimento de segurança dessas informações, pela criticidade a elas inerentes.

Para tanto, uma infraestrutura mínima deve ser definida para o atendimento desse requisito.

1.2.1 Detalhamento dos Serviços

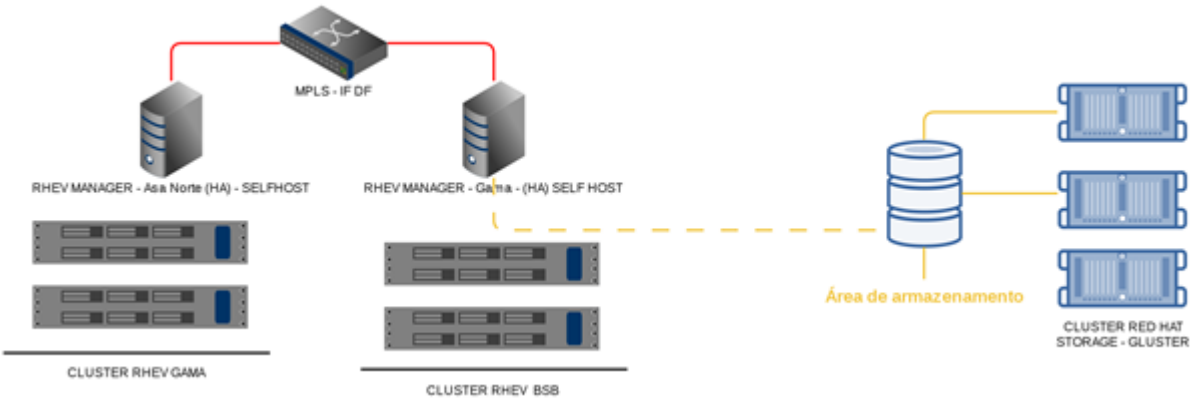
O escopo aqui definido, embora não seja único e definitivo, atende aos requisitos mínimos de segurança esperados para a implantação de um SIGAD no IFB.

Algumas soluções foram analisadas e optou-se por aquela que, em um estudo inicial, representará menor custo para a instituição.

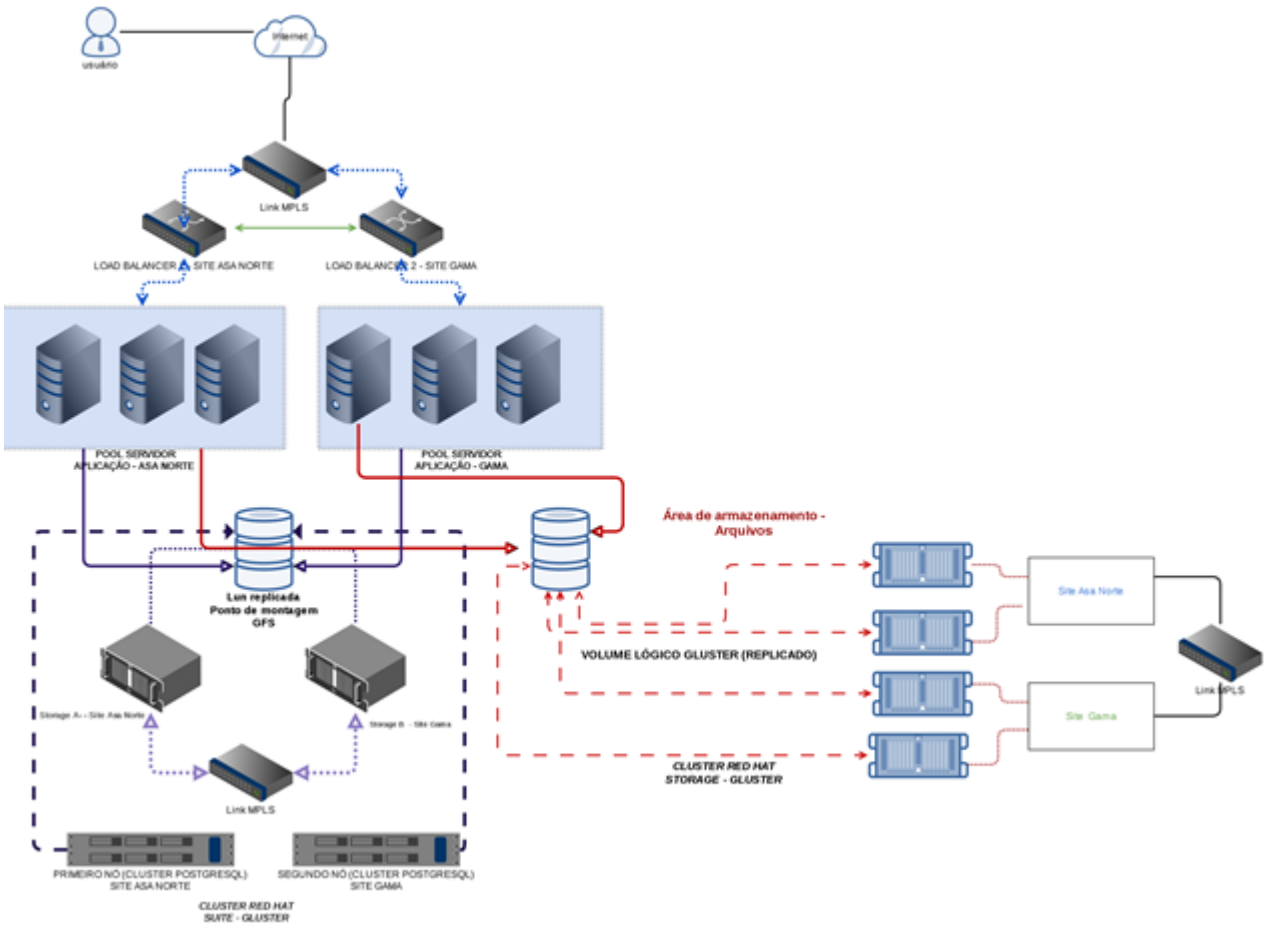
A solução consiste em manter uma infraestrutura com Balanceamento de Carga (BC) e com nuvem para clusterização de processamento. A esta nuvem estarão conectados servidores de aplicação, conversão, indexação e busca. Os dados serão armazenados num Repositório de Arquivos e tratados por um Servidor primário de Banco de Dados apoiado por dois servidores secundários, um tratando balanceamento e outro espelhamento.

Visando a segurança e disponibilidade dos dados, pensou-se na solução de um *site backup* com infraestrutura redundante num *data center* secundário em outra localidade.

1.2.1.1 Topologia de Rede (Macro)



1.2.1.2 Topologia de Rede (Micro)



1.2.1.3 Custo

Realizou-se um levantamento preliminar dos custos dos equipamentos e serviços de Tecnologia da Informação necessários para a implantação do Processo Eletrônico Nacional no Instituto Federal de Brasília. As estimativas foram realizadas tomando como base Atas de Registros de Preços de outros órgãos. Procurou-se seguir a padronização de marcas e equipamentos semelhante à já utilizada hoje no IFB e tomando como base a infraestrutura proposta para a solução.

É importante ressaltar que, além dos equipamentos e serviços apresentados, serão necessários ainda outros investimentos, como a implantação de um sistema de controle de incêndio no *data center*, controle de acesso aos equipamentos, prevenção de inundações, custo com licenciamento de *softwares*, entre outros. Parte dos valores de tais investimentos serão mencionados neste documento no intuito de apresentar um levantamento de custo inicial para este projeto.

Pretende-se que a aquisição do sistema a ser utilizado, assim como seu treinamento, não onere financeiramente o IFB. As opções de sistema avaliadas serão cedidas sem ônus, e a estratégia de implantação, incluindo a metodologia de treinamento, deverá envolver apenas recursos humanos da própria instituição.

O aprendizado da utilização do sistema será uma atividade constante, que dependerá muito da rotina de trabalho de cada servidor.

O treinamento inicial das funcionalidades básicas poderá ocorrer no próprio ambiente de trabalho por intermédio de disseminadores; também podem ser utilizados manuais e vídeos educativos para que o próprio servidor escolha a melhor forma e horário para aprender sobre a nova forma de se trabalhar utilizando o sistema.

Id	Equipamento	Descrição	Quant	Preço (R$)	Total
1	Firewall/Roteador/ Load balance	Equipamento de segurança com roteamento e balanceamento de carga	2	850.000,00	1.700.000,00

Id	Equipamento	Descrição	Quant	Preço (R$)	Total
2	Kit de licenças Red Hat	Licenças para gerenciamento de cluster	2	50.000,00	100.000,00
3	Storage	Equipamento tipo Storage com 2 controladoras + 2 baias com capacidade para 48 discos	2	330.000,00	660.000,00
4	Discos para Storage	Discos de 4 TB para Storage	32	8.500,00	272.000,00
5	Blade	Enclosure para 16 lâminas	2	90.000,00	180.000,00
6	Lâminas para Blade	Servidor do tipo lâmina	16	3.000,00	48.000,00
7	Tape library para backup	Equipamento para backup em fita	2	185.000,00	370.000,00
8	Cartuchos para Tape Library	Cartuchos para equipamento de backup	160	272,00	43.520,00
9	Kit de Licenças VMWARE	Licenças VMWARE	2	50.000,00	100.000,00
10	Treinamentos	-	1	60.000,00	60.000,00
11	Acessórios para solução – cabos, interfaces, tranceivers, etc.	-	1	60.000,00	60.000,00

Id	Equipamento	Descrição	Quant	Preço (R$)	Total
12	Link MPLS – 100 Mbps	Link redundante	1	10.000,00	10.000,00
Valor Total estimado da Solução					**3.603.520,00**

Tabela: Estimativa de Valores para equipamentos e serviços de Tecnologia da Informação

1.2.2 Considerações

Como afirmado anteriormente, a definição aqui apresentada é oriunda de um estudo preliminar e não definitivo. Desta sorte, é possível que no decorrer do processo, possa aparecer novo entendimento e mudar o norte da solução escolhida.

Sabe-se que no caso de inviabilidade de um *site backup*, outras opções são factíveis. O que não se pode deixar de levar em consideração é a necessidade de uma solução de contingência, mantendo um *backup* externo, num ambiente seguro, com sala cofre, ou simplesmente cofres de *backup*, por exemplo.

A melhor solução será aquela que apresentar melhor custo/benefício para a instituição, sem perder de vista a segurança da informação e a criticidade dos dados ou, simplesmente, a hipótese de perda destes.

2. Requisitos do Sistema

2.1 Ações de Gestão Documental

- Como um sistema informatizado de gestão arquivística de documentos, o sistema escolhido deverá atender aos requisitos posteriores como forma de se adequar à legislação e metodologia arquivísticas, sendo capaz de gerenciar os documentos físicos, híbridos e digitais ao longo do ciclo de vida destes.
- A gestão documental no sistema depende da inclusão dos planos de classificação e tabelas de temporalidade das áreas meio e fim.

2.1.1 Captura

- O sistema, para declarar um documento como arquivístico, deverá promover a captura deste, que consiste em incorporá-lo ao sistema a partir da sua produção, registro, classificação, indexação, atribuição de restrição de acesso e arquivamento.

2.1.1.1 Produção

- O sistema deverá prever o modelo de todos os documentos produzidos ao longo das atividades do IFB de forma a padronizá-los. Deve-se, para isso, ser feito um levantamento de todas as espécies documentais produzidas ao longo de cada tarefa, atividade e função do Instituto.
- É recomendável que esta padronização seja feita de acordo com as unidades organizacionais a fim de que os modelos reflitam as atividades desempenhadas.
- O sistema deverá trazer campo próprio para escolher e editar a espécie documental necessária ao usuário.
- A edição do documento no sistema deverá prever os registros das versões do documento a fim de se garantir sua autenticidade e possibilitar a recuperação de versões anteriores editadas pelo usuário.
- Uma vez enviado à outra unidade/assinado eletronicamente não será possível modificar o documento, pois este deixará de ser uma minuta para tornar-se um documento original.

2.1.1.2 Registro

- O sistema, após a criação do documento, deverá proceder com o registro deste.
- O sistema deverá gerar Número Único de Protocolo (NUP) em todos os processos e documentos avulsos que demandam análise, informação, despacho, parecer, decisão administrativa ou que tenham sido recebidos de órgãos externos e estejam sem NUP.
- O sistema deve ser capaz de registrar o documento a partir de metadados, possibilitando a recuperação e a gestão deste no sistema.

- Os metadados do registro do documento são:
  - Espécie/tipo do documento;
  - Número do documento (por setor ou geral);
  - Data e hora de produção do documento, de recebimento/transmissão, de captura;
  - Local de criação (área/computador);
  - Produtor do documento (autor);
  - Escritor;
  - Criador;
  - Originador;
  - Identificador de que o documento é avulso ou processo;
  - Número Único de Protocolo (NUP);
  - Número de anexos e os respectivos anexos com metadados de identificação;
  - Número de volumes e os respectivos volumes com metadados de identificação;
  - Número de páginas/documentos;
  - Código de classificação e o respectivo descritor, ou o assunto a que se refere o documento (do código); prazos de guarda;
  - Destinação final;
  - Assunto do documento;
  - Remetente/interessado/representante legal;
  - Destinatário; palavras-chave (taxonomia);
  - Responsável pelo registro do documento;
  - Classificação de sigilo e restrições de acesso;
  - Apontamento de que se trata de documento físico/digitalização/híbrido/digital e sua localização (quando for documento físico/híbrido/digitalizado).

2.1.1.3 Classificação Funcional e de Sigilo

- A classificação é a função matricial da gestão documental, o sistema deverá permitir a classificação conforme os planos de classificação instituídos pela portaria AN n°92 e resolução n° 14.

- O sistema deve integrar os instrumentos previstos nas normas (plano de classificação e tabela de temporalidade).
- O sistema só deve permitir a criação de um documento se este estiver classificado.
- Com a inserção dos instrumentos de classificação, é recomendável que a atividade (campo) ocorra de forma automática. O sistema identificará a área funcional a qual se está acessando e gerará uma lista de tipos documentais previamente classificados referente às atividades desta.
- Deve-se prever a possibilidade de se criar outros documentos que não sejam os listados pelo sistema num primeiro momento (mas já padronizados) que dizem respeito a atividades atípicas do setor. Nestas a classificação será manual.
- Ressalta-se a importância de orientação aos usuários acerca da necessidade do bom uso do campo, pois tende-se a preenchê-lo sem critérios, dificultando a gestão e a recuperação do documento.
- Vale destacar a necessidade de um mapeamento exaustivo e completo em cada área organizacional para a correta identificação dos tipos documentais criados ao longo das tarefas, atividades e funções, representando a realidade documental do setor de forma fidedigna. Este mapeamento não exclui a necessidade de atualização contínua das tipologias, pois as funções organizacionais mudam constantemente.
- O sistema deve prever as hipóteses de sigilo da informação previstas na Lei de Acesso à Informação (LAI) e em outros dispositivos legais, além de ser capaz de limitar a vista de determinados documentos/processos a setores/cargos específicos.
- Deve-se efetuar estudos a fim de se classificar aquelas informações que necessitem de sigilo, dada a possibilidade de prejuízos ao IFB que estas podem trazer caso não sejam restritas.
- O sistema deverá prever a classificação de sigilo dos documentos/processos, classificando-os em sigilosos (ultrassecretos, secretos e reservados), ostensivos ou em qualquer possibilidade de restrição das normas.
- Normas que restringem o acesso à informação:
    - Lei 12.527/11: Regula o acesso a informações;

- Lei nº 9.279/96: Regula direitos e obrigações relativos à propriedade industrial;
- Lei nº 9.610/98: Disciplina os direitos autorais;
- Lei nº 9.456/97: Estabelece a proteção dos direitos relativos à proteção dos cultivares;
- Lei nº 9.609/98: Estabelece o regime de proteção à propriedade intelectual de programa de computador;
- Lei nº 10.973/04: Dispõe sobre incentivos à inovação e à pesquisa científica e tecnológica no ambiente produtivo;
- Informações pessoais relativas à intimidade, vida privada, honra e imagem, em conformidade com o art. 31, § 1°, I da Lei n° 12.527/2011;
- Informações produzidas em decorrência de ações correicionais e de auditoria, observado o disposto no § 3º do art. 26 da Lei nº 10.180, de 6 de fevereiro de 2001; no art. 150 da Lei nº 8.112, de 11 de dezembro de 1990; e nos artigos 4º e 5º da Portaria nº 1.613/2012 da Controladoria-Geral da União.

- O sistema deve, a partir da classificação de sigilo atribuída ao documento em campo próprio, disponibilizar o acesso somente a quem for autorizado pela legislação.

2.1.1.4 Indexação

- A fim de se possibilitar a geração de metadados essenciais à busca e recuperação da informação, o sistema deverá ter o campo palavras-chave como de preenchimento obrigatório, só gerando os documentos após o preenchimento deste.
- Destaca-se a necessidade de orientação aos usuários da necessidade do bom uso do campo, pois tende-se a preenchê-lo sem critérios, dificultando a gestão e a recuperação do documento.
- A classificação automática/manual também permite a utilização de uma nova metodologia de indexação de documentos chamada taxonomia. Nesta, a partir da classificação atribuída pelo sistema/usuário ao documento criado, são geradas palavras chave em consonância com o

código de classificação atribuído ao documento, sendo necessário o complemento de apenas um ou dois termos pelo criador do documento.

- Por exemplo, ao se classificar um processo que trata da aquisição de um veículo, incluindo o código correspondente (042.11), o sistema preencherá automaticamente o campo de palavras-chave com:
  - Patrimônio (040);
  - Veículos (042);
  - Aquisição (042.1);
  - Compra (042.11).
  - Os termos referentes à classificação da metodologia taxonômica por si só já possibilitariam a recuperação de um item específico ou de um conjunto de documentos relacionados por sua função, mas cabe ainda ao responsável pelo registro discriminar o referido processo com termos como:
    - Carro/ônibus; 2/4 portas; motor flex; 1.0/1.6, especificando ainda mais o objeto, facilitando na recuperação da informação e potencializando a gestão documental.
    - O sistema deve incorporar essa metodologia, pois trará efetividade e assertividade na recuperação da informação.

2.1.1.5 Atribuição de Restrição de Acesso

- O sistema deverá atribuir restrições de acesso aos documentos identificados como sigilosos conforme a LAI e outras normas, onde somente determinados cargos terão acesso.
- O sistema também deve prever a restrição de acesso a determinadas unidades nos casos em que se haja necessidade por conta do conteúdo dos documentos, celeridade do processo etc.
- Ressalta-se que este é um campo obrigatório a ser preenchido no registro do documento.

2.1.1.6 Arquivamento

- O sistema, a partir dos prazos de guarda estipulados, deverá “arquivar” a documentação em uma espécie de arquivo corrente, intermediário e permanente.
- O sistema deverá arquivar os documentos organizados conforme os planos de classificação, alocando em pastas que representem a classificação atribuída a estes, mantendo-se desta forma a organicidade e possibilitando a gestão ao longo do ciclo de vida documental.
- É recomendável um espaço em disco “separado” da documentação em trâmite (corrente) para o arquivamento, de maneira a se formar um “arquivo intermediário” e “permanente“, facilitando a gestão da documentação que cumpriu sua função primária e desafogando o sistema no que diz respeito à documentação ainda em curso.
- O sistema deverá ser capaz de gerenciar processos híbridos e físicos, tanto o ciclo de vida quanto referências à localização física destes.

2.1.2 Gerenciamento de Documentos Físicos, Híbridos e Digitais

- O sistema deve ser capaz de gerenciar documentos físicos, digitais e híbridos.
- A documentação em suporte físico não pode ser ignorada pelo sistema, bem como os processos híbridos.
- Para que o sistema possa gerir esta documentação física juntamente com a digital, é necessária a organização do legado físico conforme a metodologia e legislação arquivísticas, isto é, classificar e ordenar os documentos, acondicioná-los e armazená-los em espaço apropriado.
- Posteriormente à organização do legado, devem-se incluir os metadados dos documentos físicos com a sua localização ou promover a sua digitalização para que se possa gerenciar todo o capital informacional da instituição pelo sistema.
- Deve-se prever espaço em disco suficiente que comporte as digitalizações previstas na norma (híbridos/externos/AFD).
- O sistema deverá trazer campo específico indicando que se trata de documentação física, apontando a sua localização física (estante, prateleira, caixa etc).

2.1.3 Avaliação, Temporalidade e Destinação

- Como atividade basilar da gestão documental, o sistema deve ser capaz de promover a avaliação documental de forma a racionalizar a acumulação dos documentos a partir do estabelecimento de prazos de guarda e destinação.
- Caso não ocorra de forma periódica, gerará custos extremos para a gestão e armazenamento de tudo que é produzido.
- A avaliação precede de documentos classificados, com sua temporalidade e destinação determinadas, de forma que o sistema possa gerar listas de documentos que tenham cumprido seu prazo de guarda para a avaliação.
- O sistema deve ser capaz de classificar, gerenciar e mostrar os prazos de guarda, a destinação final dos documentos e, além disso, promover com a transferência ao “arquivo intermediário” ou o recolhimento ao “arquivo permanente”, também com a geração de listas para aprovação do responsável.

2.1.4 Eliminação

- O sistema deverá, a partir da gestão dos prazos de guarda e da destinação final, gerar lista de eliminação a ser apreciada pela CPAD para posterior publicação de edital de ciência de eliminação e termo de eliminação.
- O sistema deve ser capaz de eliminar a documentação de forma a impossibilitar a recuperação do conteúdo dos documentos.

2.1.5 Transferência

- O sistema deve ser capaz de transferir a documentação para uma área de armazenamento separada (arquivo intermediário) ou para uma instituição para a guarda da documentação pelo prazo estipulado na tabela de temporalidade.

2.1.6 Recolhimento

- O sistema deve ser capaz de recolher a documentação ao arquivo permanente ou à instituição arquivística da sua esfera de competência respeitando-se:
    - Compatibilidade de suporte e formato, de acordo com as normas previstas pela instituição arquivística recebedora;
    - Documentação técnica necessária para interpretar o documento digital (processamento e estrutura dos dados);
    - Instrumento descritivo que inclua os metadados atribuídos aos documentos digitais e informações que possibilitem a presunção de autenticidade dos documentos recolhidos à instituição arquivística;
    - Informações sobre as migrações realizadas no órgão produtor, além de documentação organizada e classificada conforme legislação pertinente.

2.1.7 Pesquisa, Localização e Apresentação dos Documentos

- O sistema deve ser capaz de localizar e dar acesso aos documentos nele armazenados a partir dos metadados atribuídos aos documentos em sua captura e por meio de indexadores que representem seu conteúdo (taxonomia), reforçando a necessidade do correto preenchimento desses campos.
- A classificação permitirá manter uma documentação organizada e estruturada conforme critérios lógico-funcionais e hierarquizantes, trazendo efetividade na busca e recuperação da informação, além de permitir o gerenciamento deste capital informacional.
- A taxonomia permitirá a efetiva recuperação de conjuntos documentais ou de documentos específicos através da busca por termos hierarquizados e estruturados que representam o conteúdo dos documentos.

2.1.8 Armazenamento

- O sistema deve prever a gestão física, híbrida e digital da documentação do IFB, para tanto, é necessário atender a condições de armazenamento compatível com o volume documental de forma a resguardar a segurança

da informação, o acesso e a posteridade desta. Para tanto, deve-se observar:

- Volume e estimativa de crescimento dos documentos: este fator deve ser levado em conta para se avaliar a capacidade de armazenamento. Isto é, as áreas de depósito, os tipos e a quantidade de estantes e, para os documentos digitais, a capacidade dos dispositivos de armazenamento;
- Segurança dos documentos: as instalações de armazenamento (depósitos, arquivos, computadores) deverão prever a limitação de acesso aos documentos, como, por exemplo, o controle das áreas de armazenamento e sistemas de detecção de entrada não autorizada. O depósito deve estar localizado em área que não seja de risco. No caso de documentos digitais, devem ser previstos procedimentos que previnam a perda de documentos por falha do sistema;
- Características físicas do suporte e do ambiente: fatores como tipo de suporte, peso, grau de contaminação do documento e do ambiente, temperatura e umidade influenciam a adequação das condições de armazenamento. Nesse sentido, devem ser adotados procedimentos – como controle e verificação do tempo de vida útil e da estabilidade dos suportes – para prevenir danos aos documentos. É importante que os meios de acondicionamento sejam robustos e adequados ao formato e à quantidade de documentos. As áreas de depósito devem ter amplitude adequada, estabilidade de temperatura e de níveis de umidade, proteção contra sinistro, contaminação (isótopos radioativos, toxinas, mofo) e infestação de insetos ou micro-organismos. Os documentos digitais devem passar, periodicamente, pela troca de suporte, isto é, as informações contidas num suporte devem ser transferidas para outro. Essa técnica é denominada atualização (*refreshing*).
- Frequência de uso: o uso mais ou menos frequente dos documentos deve ser levado em conta na seleção das opções de armazenamento. No caso dos documentos convencionais, as opções envolvem acondicionamento (pastas suspensas, caixas) e localização dos depósitos (próximos ou distantes da área de trabalho). Já em relação

aos documentos digitais, as opções podem envolver armazenamento *on-line* (acesso imediato) ou *off-line*, nas chamadas "mídias removíveis" de armazenamento (disco óptico, fita magnética), em diferentes graus de disponibilidade e velocidade.

- Custo relativo das opções de armazenamento dos documentos: além do custo dos dispositivos de armazenamento, devem ser considerados, para sua manipulação, os valores dos equipamentos e do *software* de controle. Pelo previsível alto custo, pode-se considerar a possibilidade de terceirização do armazenamento. Nesse caso, porém, surgem outros problemas, como garantias legais sobre a custódia, restrições de acesso e capacidade tecnológica. Recursos como o uso de criptografia podem impedir o acesso não autorizado, assim como a utilização de *checksum* permite rastrear eventuais comprometimentos de conteúdo.

2.1.9 Preservação

- Deve haver uma política de preservação documental de forma a garantir o acesso, a preservação, a autenticidade e a posteridade da documentação física e digital.
- Deve-se promover atualização periódica de mídias e tecnologias que armazenam e gerenciam os documentos, além de se ter *backup* integral do sistema.

2.1.10 Considerações

Considerando que o sistema adotado deverá ser um Sistema Informatizado de Gestão Arquivística de Documentos (SIGAD) para atendimento aos requisitos do PEN, este precisará integrar todo o ciclo de vida documental desde a criação e uso dos documentos até a definição quanto a destinação final destes, eliminando-os ou preservando-os permanentemente. Para que estas ações sejam efetivamente realizadas pelo sistema, torna-se necessária a adoção dos requisitos apresentados anteriormente, pois se configuram como ações necessárias e inerentes à gestão de documentos.

O não atendimento aos requisitos elencados implicará em um sistema falho e que não atende completamente às demandas do PEN ou da gestão arquivística dos documentos, sendo inevitável para o sucesso da gestão informatizada a incorporação dessas ações, sob o risco de se criar massas documentais acumuladas em formato digital impossível de se gerir ou recuperar documentos, além de não atendimento à legislação arquivística vigente, que demanda tais ações independente do suporte do documento arquivístico.

Não sendo possível a adoção, na íntegra, das recomendações elencadas, deve-se atentar quanto à prioridade da adoção dos requisitos. Para tanto, foi estabelecido o padrão de 1 a 3, sendo que 1 é extremamente necessário, 2 é necessário e 3 é altamente desejável:

- Captura (1)
- Produção (1)
- Registro (1)
- Classificação (funcional e sigilo) (1)
- Indexação (1)
- Atribuição de restrição de acesso (1)
- Arquivamento (2)
- Gerenciamento de documentos físicos, híbridos e digitais (1)
- Avaliação, temporalidade e destinação (2)
- Eliminação (2)
- Transferência (2)
- Recolhimento (2)
- Pesquisa, localização e apresentação dos documentos (1)
- Armazenamento (1)
- Preservação (1)

2.2 Ações de Protocolo

- O sistema, por ser responsável pelo gerenciamento do ciclo de vida documental, atua diretamente nas atividades de protocolo, devendo atender aos requisitos relacionados adiante.

- O sistema deve promover as atividades de protocolo, que são: recebimento, classificação, registro, distribuição, controle da tramitação, expedição e autuação de documentos avulsos para formação de processos.
- A adoção do sistema deverá abarcar grande parte dos requisitos exigidos no e-Arq Brasil, de forma a priorizar os de caráter obrigatório. Ressalta-se que este é um processo gradual, devendo o sistema estar em constante monitoramento e aperfeiçoamento pelas áreas de gestão documental e TI.

2.2.1 Recebimento, Classificação e Registro

- É recomendável que o sistema seja capaz de receber documentação via e-mail ou mídia removível para integralização ao sistema de forma a garantir a sua confiabilidade, autenticidade, acessibilidade e gestão (observado o e-PING).
- O sistema deve ser capaz de gerenciar e registrar todos os documentos criados/recebidos independente do suporte. A gestão se resume a captura, registro, classificação, gerenciamento dos prazos de guarda e todos as demais atividades que são aplicáveis aos documentos convencionais, ou seja, o mesmo tratamento dado ao documento convencional/nato digital deve ser dado ao documento especial.
- O sistema deve ser capaz de integrar e gerir documentos digitalizados na formação de processos digitais, bem como ser capaz de promover a gestão de processos híbridos, isto é, promover a gestão documental tanto da parte física quanto da digital do processo. A conversão de documento físico para digital será realizada e registrada no sistema com os mesmos metadados dos natos digitais para fins de recuperação e gestão. Ressalta-se que a digitalização não dá valor legal de documento original à esta, sendo a guarda do documento físico inevitável.
- O sistema tem que emitir comprovante de recebimento de documentos.
- O sistema deve proceder com a classificação no ato do recebimento do documento/processo externo no protocolo e na criação do documento/processo no próprio setor pelo servidor que criou o documento. O sistema deve trazer um “campo classificação” que integrará os planos de

classificação da área meio e fim. É recomendável que o campo “palavras-chave” seja integrado com o campo classificação, proporcionando a adoção da metodologia denominada taxonomia para geração de termos indexadores a partir da classificação, devendo o responsável pelo documento completar a ação com 1 (um) ou 2 (dois) termos.

- O registro no sistema deverá abarcar os seguintes dados:
  - Espécie/tipo do documento;
  - Número do documento (por setor ou geral);
  - Data e hora de produção do documento, de recebimento/transmissão, de captura;
  - Local de criação (área/computador);
  - Produtor do documento (autor);
  - Escritor; criador; originador;
  - Identificador de que o documento é avulso ou processo;
  - Número Único de Protocolo (NUP);
  - Número de anexos e os respectivos anexos com metadados de identificação;
  - Número de volumes e os respectivos volumes com metadados de identificação;
  - Número de páginas/documentos;
  - Código de classificação e o respectivo descritor, ou o assunto a que se refere o documento (do código);
  - Prazos de guarda; destinação final;
  - Assunto do documento;
  - Remetente/interessado/representante legal;
  - Destinatário;
  - Palavras-chave (taxonomia);
  - Responsável pelo registro do documento;
  - Classificação de sigilo e restrições de acesso;
  - Apontamento de que se trata de documento físico/digitalização/híbrido/digital e sua localização (quando for documento físico/híbrido/digitalizado);
- O sistema deve prever as hipóteses de sigilo da informação previstas na LAI e em outros dispositivos legais, além de ser capaz de limitar a vista de

determinados documentos/processos a setores/cargos específicos. Deve-se efetuar estudos a fim de se classificar informações que necessitem de sigilo, dada a possibilidade de prejuízos ao IFB que estas possam trazer, caso não sejam restritas. O sistema deverá prever a classificação de sigilo dos documentos/processos, classificando-os em sigilosos (ultrassecretos, secretos e reservados), ostensivos ou em qualquer possibilidade de restrição das normas.

- O sistema deve, a partir da classificação de sigilo atribuída ao documento em campo próprio, disponibilizar o acesso somente a quem for autorizado pela legislação.
- Deve-se incluir a marcação de documento/processo “urgente”, o qual terá prioridade para as atividades de registro, classificação, distribuição, autuação etc (campo próprio).

2.2.2 Distribuição

- O sistema deve proceder com a distribuição e registrá-la contemplando as seguintes informações: identificação do documento por meio do NUP; remetente/interessado/representante legal; destinatário; especificações do documento, avulso ou processo, encaminhado: espécie/tipo, número e data de produção; identificador de que o documento é avulso ou processo; número de anexos e número de volumes; código de classificação e o respectivo descritor ou o assunto a que se refere o documento; data do encaminhamento; identificação do responsável pelo encaminhamento; data do recebimento; identificação do responsável pelo recebimento; providências a serem implementadas, quando couber.

2.2.3 Controle de Tramitação

- O sistema deve registrar o trâmite contemplando as seguintes informações: identificação do documento por meio do NUP; remetente/interessado/representante legal; destinatário; especificações do documento, avulso ou processo, encaminhado: espécie/tipo, número e data de produção; identificador de que o documento é avulso ou processo; número de

anexos e número de volumes; código de classificação e o respectivo descritor ou o assunto a que se refere o documento; data do encaminhamento; identificação do responsável pelo encaminhamento; data do recebimento; identificação do responsável pelo recebimento; providências a serem implementadas, quando couber.

- O sistema deve emitir alerta ao usuário responsável pelo documento quando este extrapolar o prazo determinado para sua apreciação e prosseguimento (só é possível após o mapeamento dos processos).

2.2.4 Expedição

- O sistema deve proceder com a expedição e registrá-la contemplando com as seguintes informações: a espécie/tipo do documento; o número e a data de produção do documento; a data de recebimento do documento; o identificador de que o documento é avulso ou processo; o Número Único de Protocolo (NUP); o número de anexo(s); o número de volume(s); o código de classificação e seu respectivo descritor ou o assunto a que se refere o documento; o remetente/interessado/representante legal; o destinatário.
- O sistema necessita ter um barramento compatível com o órgão ao qual se enviará o documento (barramento do PEN).

2.2.5 Exigência

- O sistema deve prever a possibilidade de devolução do documento ao setor/órgão de origem quando este estiver incompleto/equivocado/inconsistente. É recomendável o registro da ação de exigência para futura auditoria ou questionamentos (um despacho exigindo a correção do documento de forma justificada é suficiente).
- Pessoa física ou jurídica, não pertencentes à Administração Pública Federal, deverá ser convocada pela unidade administrativa interessada por meio de correspondência registrada, com Aviso de Recebimento (AR), ou por meio eletrônico que garanta o efetivo recebimento pela parte interessada para que

seja cumprida a exigência. A cópia da convocação expedida será anexada ao processo, juntamente com o respectivo aviso/confirmação de recebimento.

2.2.6 Atuação

- O sistema deve possibilitar a autuação de documento para formação de processo (o NUP do documento se mantém e vira o NUP do processo).
- Registrar no sistema constando as seguintes informações: nome do ministério ou órgão equivalente; nome do órgão ou entidade, quando couber; nome da unidade administrativa; número do processo (NUP); data de autuação; nome do interessado; e código de classificação e o respectivo descritor ou o assunto a que se refere o documento.
- As informações de trâmite do processo devem estar presentes junto às informações de identificação.

2.2.7 Numeração de Folhas

- Os documentos que compõem o processo devem ser apresentados sempre na ordem da sua inserção, que será feita sempre após o último documento, não sendo preciso numerá-los. Entretanto, dada a possibilidade de impressão deste para envio aos órgãos, entidades e empresas que não possuam barramento com o sistema adotado pelo IFB, é recomendável que haja a numeração das folhas no momento da impressão do documento digital.

2.2.8 Encerramento e Abertura de Volumes

- O sistema deve prever a possibilidade de encerramento e abertura de volumes. Apesar de não ser necessário nos processos nato digitais, é preciso a previsão do campo tendo em vista a gestão de documentos físicos e híbridos pelo sistema.
- O sistema deve registrar o encerramento do volume em sistema informatizado com as seguintes informações: data e hora de encerramento; responsável pelo encerramento; e número de documentos do volume;

- Abrir e registrar o novo volume em sistema informatizado com as seguintes informações: data e hora de abertura; responsável pela abertura; e identificador do número sequencial do primeiro documento a ser inserido.
    - As seguintes informações de identificação devem ser exibidas quando o volume for apresentado: Nome do ministério ou órgão equivalente; Nome do órgão ou entidade, quando couber; Nome da unidade administrativa; Número do processo (NUP); Data de autuação; Número do volume (utilizar numeração ordinal); Data de abertura do volume;
    - Nome do interessado; Código de classificação e o respectivo descritor ou o assunto a que se refere o documento.
- A numeração sequencial dos documentos seguirá a do volume anterior.
- Os volumes do processo tramitarão juntos.

2.2.9 Despacho

- O sistema deve prever a inserção de despacho através de documento próprio ou em campo próprio destinado a isso (avulso é melhor para a visualização).
- O sistema deve permitir o cancelamento de despacho, mas este ainda deve ser apresentado com a indicação de cancelamento (histórico das versões, trilha de auditoria com todas as versões e alterações do documento).

2.2.10 Juntada

- O sistema deve ser capaz de prever a juntada por anexação e apensação de documentos avulsos e processos. Deve-se registrar a ação de juntada pelo sistema em campo próprio a partir de despacho e prever o registro das informações do documento/processo de forma a relacioná-los com o documento/processo principal (informar por meio de despacho).
- Quando a anexação tratar de processo a processo, deve-se registrar no sistema as seguintes informações: registro do evento de anexação de processo(s) a processo; atualização do controle da numeração sequencial dos documentos no processo.

- Registro, nos dados do processo principal, das seguintes informações referentes a cada processo anexado: data e hora da anexação; responsável pela anexação; identificador do(s) processo(s) acessório(s); identificador do último documento do processo principal antes da anexação; e número de documentos que integram o(s) processo(s) acessório(s) no momento da anexação; registro, nos dados do(s) processo(s) acessório(s), das seguintes informações: data e hora da anexação; responsável pela anexação; e NUP do processo principal.
- Quando a apensação tratar-se de processo a processo, deve-se registrar no sistema as seguintes informações: registro do evento de apensação de processo(s) a processo; manutenção do controle da numeração sequencial dos documentos em cada um dos processos;
- Registro, nos dados do processo principal, das seguintes informações para cada processo apensado: data e hora da apensação; responsável pela apensação; identificador do(s) processo(s) apensado(s); e número de documentos que integram o(s) processo(s) apensado(s) no momento da apensação; registro, nos dados do(s) processo(s) acessórios(s), das seguintes informações: data e hora da apensação; responsável pela apensação; e NUP do processo principal.

2.2.11Desapensação

- O sistema deverá prever a desapensação com as informações registradas: Data e hora da desapensação; Responsável pela desapensação; Identificador do(s) processo(s) desapensado(s); Registro, nos dados do(s) processo(s) acessórios(s), das seguintes informações:
  - Data e hora da desapensação;
  - Responsável pela desapensação; e
  - NUP do processo principal.
  - A ação será justificada por meio de despacho próprio.

2.2.12 Desentranhamento

- O sistema deverá prever o desentranhamento que registrará a ação com as seguintes informações: data e hora do desentranhamento; responsável pelo desentranhamento; identificador do(s) documento(s) retirado(s); e motivo do desentranhamento.
- A ação será justificada por meio de despacho próprio.

2.2.13 Desmembramento

- O sistema deverá prever o desmembramento que registrará a ação com as seguintes informações: data e hora do desmembramento; responsável pelo desmembramento; identificador do(s) documento(s) retirado(s); identificador do novo processo formado com o(s) documento(s) retirado(s); e motivo do desmembramento;
- A ação será justificada por meio de despacho próprio.

2.2.14 Reconstituição de Processo

- Ao ocorrer a perda ou extravio de processo, a autoridade competente do órgão ou entidade deverá ser comunicada, cabendo a ela promover a apuração dos fatos, por meio de sindicância ou processo administrativo, e designar, formalmente, um servidor ou uma comissão para proceder à reconstituição do processo, sendo necessário que o sistema execute as seguintes ações:
  - Resgatar as informações e os documentos que integravam o processo perdido ou extraviado, solicitando, quando necessário, às unidades administrativas por onde o processo tramitou, a disponibilização de informações e/ou de cópias dos documentos;
  - Reunir os documentos obtidos durante a operação de reconstituição, encaminhando à unidade protocolizadora para autuação, sendo atribuído ao processo formado um novo número (NUP), mantendo-se o número (NUP) anterior como referência;
  - Lavrar o "Termo de Reconstituição de Processo", o qual será a primeira folha do processo reconstituído, devendo ser numerada e contendo:

nome do órgão ou entidade; nome da unidade protocolizadora; data; referência ao processo reconstituído; número que o novo processo receberá; órgão ou entidade produtor(a) do processo; interessado; código de classificação / descritor / resumo do assunto; número de folhas; motivo da reconstituição; assinatura do servidor; matrícula.

- Registrar a operação de reconstituição de processo em sistema informatizado;
- Encaminhar o processo à autoridade competente que determinou a reconstituição, para que siga seu trâmite.

- No caso de perda ou extravio de volume de um processo, deverão ser seguidos os mesmos procedimentos anteriormente descritos, mantendo-se a numeração original do processo, bem como lavrado o "Termo de Reconstituição de Volume" o qual será a primeira folha do volume reconstituído, devendo ser numerada e contendo: nome do órgão ou entidade; nome da unidade protocolizadora; data; órgão ou entidade produtor(a) do processo; interessado; código de classificação / descritor / resumo do assunto; número de folhas; motivo da reconstituição; assinatura do servidor; matrícula.

2.2.15 Capa do processo

- Não há capa nos processos nato digitais, mas deve-se apresentar as seguintes informações ao se exibir o processo: nome do ministério ou órgão equivalente; nome do órgão ou entidade, quando couber; nome da unidade administrativa; número do processo (NUP); data de autuação; nome do interessado; e código de classificação e o respectivo descritor ou o assunto a que se refere o documento.

2.2.16 Arquivamento

- O sistema pode prever uma área de guarda separada para os documentos que não se encontram em trâmite ou que já tenham cumprido o seu valor administrativo imediato, de forma a se criar um “arquivo intermediário” e um “arquivo permanente” digital para preservá-los e “desafogar” o sistema

com os documentos efetivamente ativos. Deve ainda separar e gerar uma lista de eliminação com a documentação que já cumpriu o prazo estipulado no instrumento para ser eliminado.

- O sistema deverá ser capaz de gerenciar processos híbridos e físicos, tanto o ciclo de vida quanto referências à localização física destes.

2.2.17 Desarquivamento

- O sistema deve prever a possibilidade de desarquivamento e proceder com esse registro. O documento desarquivado retornará à ativa, podendo ser anexado, autuado, objeto de análise etc.

2.2.18 Empréstimo/Vistas

- O sistema deve prever o registro das ações de empréstimo (para documentos físicos).
- O sistema deve proceder vistas (acesso via sistema ou cópia digital) aos documentos digitais quando solicitado e não forem de acesso restrito.

2.2.19 Considerações

O ciclo documental ao qual o sistema deve abranger aborda impreterivelmente as ações de protocolo, sendo um aspecto de fundamental importância para o andamento dos processos administrativos, pois estas atividades estão presentes em textos legais e se fazem obrigatórias independentemente da adoção ou não de sistemas informatizados.

Com a implementação de um sistema informatizado far-se-á necessário a execução das ações acima elencadas, sob risco de paralisação das atividades administrativas ou desatendimento às normas legais caso alguma das ações não seja realizável pelo sistema.

Não sendo possível a adoção, na íntegra, das recomendações elencadas, deve-se atentar quanto à prioridade da adoção dos requisitos. Para tanto, foi estabelecido o padrão de 1 a 3, sendo que 1 é extremamente necessário, 2 é necessário mas pode-se implementar no primeiro momento sem o requisito e 3 é altamente desejável:

- Recebimento, classificação e registro (1)
- Distribuição (1)
- Controle de tramitação (1)
- Expedição (1)
- Exigência (1)
- Atuação (1)
- Numeração de folhas (1)
- Encerramento e abertura de volumes (2)
- Despacho (1)
- Juntada (1)
- Desapensação (1)
- Desentranhamento (1)
- Desmembramento (1)
- Reconstituição de processo (2)
- Capa do processo (1)
- Arquivamento (3)
- Desarquivamento (3)
- Empréstimo (vista) (1)

2.3 Segurança

- O sistema deve ser capaz de ser seguro e garantir a confiabilidade dos documentos, isto é, garantir a fidedignidade e a autenticidade documentais.
- O documento precisa representar exatamente aquilo que atesta, sem possibilidade de adulteração, além disso, é preciso que o documento assuma a forma adequada para enunciar aquilo que está escrito.
- Consegue-se isso a partir de: controle de acesso; trilhas de auditoria; cópias de segurança; assinatura digital; classes de sigilo; criptografia para sigilo; marcas d'água etc.

2.3.1 Controle de Acesso

- O sistema deve prever o controle de acesso ao sistema e aos documentos por meio de:
  - Acesso ao sistema por meio de *login* e senha;
  - Restrição de acesso aos documentos;
  - Exibição dos documentos, criptografados ou não, e dos metadados somente aos usuários autorizados;
  - Uso e intervenção nos documentos somente pelos usuários autorizados.

2.3.2 Classificação de Sigilo e Restrição de Acesso

- O sistema deve prever as hipóteses de sigilo da informação previstas na LAI e em outros dispositivos legais, além de ser capaz de limitar a vista de determinados documentos/processos a setores/cargos específicos. Deve-se efetuar estudos a fim de se classificar aquelas informações que necessitem de sigilo dada a possibilidade de prejuízos ao IFB que estas podem trazer caso não sejam restritas. O sistema deverá prever a classificação de sigilo dos documentos/processos, classificando-os em sigilosos (ultrassecretos, secretos e reservados), ostensivos ou em qualquer possibilidade de restrição das normas (campo específico).
- O sistema deve, a partir da classificação de sigilo atribuída ao documento em campo próprio, disponibilizar o acesso somente a quem for autorizado pela legislação.

2.3.3 Uso e Rastreamento

- O sistema deve ser capaz de dar acesso por meio dos metadados mas também controlar seu uso a partir de:
  - Identificação da permissão de acesso dos usuários, isto é, do que cada um pode acessar;
  - Identificação da precaução de segurança e da categoria de sigilo dos documentos;
  - Garantia de que somente os indivíduos autorizados tenham acesso aos documentos classificados e aos originalmente sigilosos;

- Registro de todos os acessos, tentativas de acesso e uso dos documentos (visualização, impressão, transmissão e cópia para a área de transferência), com identificação de usuário, data, hora e, se possível, estação de trabalho;
- Revisão periódica das classificações de acesso a fim de garantir sua atualização.

2.3.4 Trilha de Auditoria

- O sistema deve ser capaz de rastrear as intervenções e as tentativas de intervenção nos documentos permitindo: identificar os autores de cada operação realizada nos documentos; prevenir a perda de documentos; monitorar todas as operações realizadas; garantir a segurança e a integridade.
- No caso de procedimentos que exijam prazo a ser cumprido pelo órgão ou entidade, devem ser implementadas ações de rastreamento, de forma a: determinar os passos a serem dados em resposta às atividades ou ações registradas no documento; atribuir a uma pessoa a responsabilidade por cada ação; registrar a data em que uma ação deve ser executada e a data em que ocorreu.

2.3.5 Cópias de Segurança

- Deve-se ter a previsibilidade de um *site backup* longe do *data center* com a cópia integral de todo o sistema, garantindo a recuperação dos dados do sistema em caso de sinistro.

2.3.6 Assinatura Digital

- O sistema deve prever a assinatura digital de todos os documentos criados. Nos documentos internos poderá ser feita por meio de *login* e senha, biometria ou ICPEdu. Nos documentos externos adota-se o ICP-Brasil, que por ter um custo considerável, seria exclusivo de cargos de no mínimo CD-2/3.

2.3.7 Criptografia

- O sistema deve criptografar os documentos e as informações que detenham algum grau de sigilo ou que tenham seu acesso limitado a determinados cargos/setores, possibilitando a integridade e resguardando informações particulares/sigilosas.
- Deve-se prever a posteridade da informação criptografada tendo em vista a necessidade de atualização por conta da obsolescência da chave.
- O sistema deve utilizar a criptografia baseada em algoritmo de Estado compatível com o grau de sigilo da informação conforme preconiza a NC 09 DSIC/GSI/PR.
    - Padrões mínimos para recurso criptográfico baseado em algoritmo de Estado (NC 09 DSIC/GSI/PR):

Nível de segurança da informação	**RSA/LD**	**Curvas Elípticas**
Reservado	2048	224
Secreto	3248	256
Ultrassecreto	Não recomendado	Não recomendado

Tabela I - Tamanho da chave

Classificação	**Algoritmo**	
	Chave	**Bloco**
Reservado	192	128
Secreto	256	128
Ultrassecreto	Não recomendado	

Tabela II - Algoritmos de bloco

Classificação	**Algoritmo**
Reservado	192

Secreto	256
Ultrassecreto	Não recomendado

Tabela III - Algoritmos sequenciais:

Classificação	**Algoritmo**
Ultrassecreto	Sequência aleatória

Tabela IV - Sistema de chave única:

2.3.8 Marcas D'água

- O sistema deve trazer em seus documentos marcas d'água que garantam a sua proveniência e integridade, dificultando a alteração ou falsificação da documentação nato digital/digitalizada.
- Deve-se promover a atualização constante do algoritmo/chave que protege a marca d'água dos documentos.

2.3.9 Acompanhamento de Transferência

- O sistema deve registrar cada transferência do documento, seja para uma área de armazenamento diferente dos documentos em trâmite ("arquivo intermediário"), seja para o "arquivo permanente". Deve-se registrar inclusive a transferência da documentação física e sua real localização, possibilitando a recuperação da informação de forma eficiente.
- O registro deve ocorrer inclusive na mudança de caixas, pastas e dossiês (inclusive digitais).

2.3.10 Autoproteção

- O sistema deve ser capaz de proteger seus dados e documentos de forma a garantir a sua integridade e confiabilidade, evitando erros, falhas e invasões. Para garantir a autoproteção deve-se prever uma estrutura sólida e eficiente de antivírus, *firewall*, *anti-spyware* etc.

2.3.11 Segurança da Infraestrutura

- Além das recomendações do NTIC devem-se observar os seguintes aspectos: as salas reservadas a computadores servidores, equipamentos de rede e ao armazenamento dos documentos digitais devem ter temperatura ambiente e umidade relativa do ar controladas e fornecimento estável de energia elétrica, contando com equipamento de *nobreak* e geradores de energia, devendo haver controle contínuo para verificar se estas condições estão sendo atendidas.
- Necessita-se equipamentos contra incêndio em toda a área de instalação e de acordo com as normas de segurança estabelecidas, os equipamentos contra incêndio devem ser verificados periodicamente e substituídos antes do término da vida útil prevista. Deve-se prever instalações adequadas de para-raios, com procedimentos de manutenção periódica, seguindo a legislação e as normas técnicas estabelecidas.
- A área reservada à instalação do sistema deve ser compartimentada, com o objetivo de controlar o acesso às informações, as salas de computadores servidores são de uso exclusivo de pessoal autorizado e devem ter controle eletrônico de acesso.
- Para acesso a áreas de segurança, identificações e credenciais de segurança têm de estar de acordo com as atribuições individuais e as regras de segurança do Instituto.

2.3.12 Considerações

A adoção de um sistema informatizado de gestão arquivística de documentos implica em uma mudança de paradigma para qualquer instituição, onde os processos e documentos até então físicos passam a ser nato digitais, isto é, passam a ser criados, armazenados e geridos digitalmente, acarretando a necessidade de mudança não só do modo de trabalhar e encarar a documentação de arquivo, mas também de como garantir a sua segurança.

É fato que atualmente existem diversas tecnologias para a proteção de dados que estão no ambiente digital, mas também é fato que a cada dia novos métodos são desenvolvidos para quebrar as barreiras de segurança dos sistemas informatizados para acesso aos dados e documentos ali armazenados.

Ao se implementar determinado sistema em uma instituição deve-se ter clara a necessidade de proteção desses dados, uma vez que ali encontram-se documentos de natureza sigilosa, documentos eminentemente administrativos e documentos pessoais, sendo que o vazamento ou acesso não autorizado de qualquer um destes documentos acarretará em prejuízos incalculáveis à Instituição, seja à sua imagem perante a sociedade seja o prejuízo financeiro que poderia ser causado, caso os dados fossem apagados após uma invasão.

Tendo em vista os riscos envolvidos ao se adotar um sistema informatizado, é inevitável a observância dos itens anteriores como forma de garantir, ou ao menos inibir possíveis ataques ou acessos não autorizados aos dados e documentos do sistema, sob risco de se perder ou ter extraviada a documentação armazenada no sistema, e com ela a história administrativa da Instituição, os documentos de natureza administrativa e os de natureza pessoal.

Não sendo possível a adoção, na íntegra, das recomendações elencadas, deve-se atentar quanto à prioridade da adoção dos requisitos. Para tanto, foi estabelecido o padrão de 1 a 3, sendo que 1 é extremamente necessário, sendo que 1 é extremamente necessário, 2 é necessário e 3 é altamente desejável:

- Controle de acesso (1)
- Classificação de sigilo e restrição de acesso (1)
- Uso e rastreamento (1)
- Trilha de auditoria (1)
- Cópias de segurança (1)
- Assinatura digital (1)
- Criptografia (1)
- Marcas d’água (3)
- Acompanhamento de transferência (2)
- Autoproteção (1)
- Segurança da infraestrutura (1)

2.4 Metadados

- O sistema deve conter dados que descrevam o documento de forma a possibilitar a sua correta recuperação, gestão, preservação, segurança e arquivamento ao longo do tempo de forma efetiva. A inserção de metadados no sistema é fundamental tendo em vista a quantidade informacional presente e futura que o sistema gerenciará, sendo inevitável o uso de dados que discriminem os documentos uns dos outros, tornando-os únicos e possibilitando a sua efetiva recuperação por diversos meios.

2.4.1 Documento

- O sistema deve prever os seguintes metadados que descrevam o documento e sua relação com o processo/dossiê:
  - Identificador do documento;
  - Número do documento;
  - Número do protocolo;
  - Identificador do processo/dossiê;
  - Número do processo/dossiê;
  - Identificador do volume;
  - Número do volume;
  - Tipo de meio;
  - Status;
  - Identificador de versão;
  - Título;
  - Descrição;
  - Assunto;
  - Autor;
  - Destinatário;
  - Originador;
  - Redator;
  - Interessado;
  - Procedência;

- Identificador do componente digital;
- Gênero;
- Espécie;
- Tipo;
- Idioma;
- Quantidade de folhas/página;
- Numeração sequencial dos documentos;
- Indicação de anexos;
- Relação com outros documentos;
- Níveis de acesso;
- Data de produção;
- Classe;
- Destinação prevista;
- Prazo de guarda;
- Localização.

2.4.2 Evento de Gestão

- O sistema deve registrar os seguintes metadados dos eventos de gestão os quais o documento passou ao longo do seu ciclo de vida:
  - Captura;
  - Tramitação;
  - Transferência;
  - Recolhimento;
  - Eliminação;
  - Abertura processo/dossiê;
  - Encerramento processo/dossiê;
  - Reabertura processo/dossiê;
  - Abertura volume;
  - Encerramento volume;
  - Juntada anexação;
  - Juntada apensação;
  - Desapensação;
  - Desentranhamento;

- Desmembramento;
- Classificação sigilo;
- Desclassificação sigilo;
- Reclassificação sigilo.

2.4.3 Classe

- O sistema deve registrar os seguintes metadados referentes aos níveis de agregação dos planos de classificação, da temporalidade e da destinação dos documentos:
  - Descrição de classe: Classe nome; Classe código; Classe subordinação; Registro de abertura; Registro de desativação; Reativação de classe; Registro de mudança de nome de classe; Registro de deslocamento de classe; Registro de extinção; Indicador de classe ativa/inativa.
  - Temporalidade associada à classe: Classe código; Prazo de guarda na fase corrente; Evento que determina a contagem do prazo de guarda na fase corrente; Prazo de guarda na fase intermediária; Evento que determina a contagem do prazo de guarda na fase intermediária; Destinação final; Registro de alteração; Observações.

2.4.4 Agente

- O sistema deve registrar os seguintes metadados referentes aos agentes que o acessam: Nome; Identificador; Autorização de acesso; Credenciais de autenticação; Relação; Status do agente.

2.4.5 Componente Digital

- O sistema deve registrar os seguintes metadados dos componentes digitais que compõem os documentos arquivísticos digitais:
  - Identificador do componente digital; Nome original; Características técnicas; Formato de arquivo; Armazenamento; Ambiente de *software*; Ambiente de *hardware*; Dependências; Relação com outros componentes digitais; Fixidade.

2.4.6 Evento de Preservação

- O sistema deve registrar os seguintes metadados referentes aos eventos de preservação: Compressão; Decifração; Validação de assinatura digital; Verificação de fixidade; Cálculo *hash*; Migração; Replicação; Verificação de vírus; Validação.

2.4.7 Considerações

Os metadados referentes aos documentos e às ações ligadas a estes são necessários tendo em vista que o sistema irá recuperar e gerir esta documentação através destes metadados, que são as informações pertinentes a cada documento armazenado no sistema, garantindo desta forma a sua efetiva recuperação, gestão, segurança e preservação.

Ressalta-se que a confiabilidade e a autenticidade dos documentos digitas estão intrinsecamente relacionados aos metadados, pois estes registram tudo o que aconteceu com o documento desde a sua criação até o seu arquivamento ou eliminação, sendo passível de investigação e auditoria que ateste a sua veracidade como um documento de arquivo inviolado.

A não observância de uma estrutura de metadados bem estruturada, conforme os requisitos elencados, implicará em documentos passíveis de adulteração, comprometendo a confiabilidade e autenticidade documentais, além de impedir a boa gestão do conjunto documental, bem como na sua busca e recuperação quando for necessária.

Não sendo possível a adoção, na íntegra, das recomendações elencadas, deve-se atentar quanto à prioridade da adoção dos requisitos. Para tanto, sendo que 1 é extremamente necessário, 2 é necessário e 3 é altamente desejável:

- Documento (1)
- Evento de gestão (1)
- Classe (1)
- Agente (1)
- Componente digital (1)
- Evento de preservação (1)

2.5 Preservação Digital

- Considerando a necessidade de se guardar a documentação arquivística digital pelo prazo estipulado nas tabelas de temporalidade da Portaria AN/MJ n°92 e Resolução n°14, o sistema deverá, tendo em vista a fragilidade do suporte e da obsolescência tecnológica, proceder com a preservação da informação digital assegurando o acesso e posteridade desta.

2.5.1 Política de Preservação

- A política de preservação garante a integridade dos documentos digitais ao longo do tempo por estabelecer padronização de procedimentos, rotinas de trabalho, de migração de suporte e de atualização tecnológica, além de estabelecer um plano de contingência em caso de sinistro, medidas essenciais para a garantia de acesso e salvaguarda da documentação institucional e dos servidores. A inexistência de tal política implica em insegurança da documentação, comprometendo não só a história institucional, mas toda a documentação de valor administrativo, fiscal e legal, além da documentação pertinente aos servidores e seus direitos, podendo causar danos irreversíveis passíveis de penalidades na esfera administrativa, cível e penal.
- Passos para implementação da política:
    - Formação de equipe multidisciplinar contendo os seguintes profissionais: profissionais da área de tecnologia da informação; arquivista ou responsável pela guarda da documentação; profissionais da área jurídica; profissionais da administração; historiador; profissionais ligados à área finalística do instituto.
    - Elaboração da política de preservação digital por meio de Portaria Normativa contendo padronização de procedimentos, rotinas de trabalho, de migração de suporte, de atualização tecnológica e plano de contingência em caso de sinistro.

- Preparação da infraestrutura e ambiente necessários para assegurar o sucesso da política.
- Implantação da política.
- Revisão e adaptações periódicas.

2.5.2 Independência de Hardware Específico

- É necessária a utilização de *hardware* comum e que não dependa exclusivamente de um fabricante/distribuidor, possibilitando liberdade para a migração, cópia e atualização sem a interferência ou dependência de uma empresa específica, comprometendo não só o acesso e a posteridade da informação, mas também os recursos financeiros dado a exclusividade de *hardware*, podendo o fornecedor descontinuar a tecnologia, o produto ou exigir preços altos para a manutenção/atualização.
- Deve-se observar a obsolescência do *hardware* bem como a sua estabilidade no mercado para evitar tecnologia ultrapassada ou que não tenha se estabilizado com risco de descontinuidade.
- Passos para a escolha do *hardware*:
  - Verificar possibilidade de *hardware* com diversas tecnologias e independência de fabricante/distribuidor;
  - Verificar estabilidade da tecnologia utilizada no *hardware*;
  - Verificar obsolescência do *hardware*;
  - Providenciar migração do *hardware*.

2.5.3 Independência de Software Específico

- É necessária a utilização de *software* comum e que não dependa exclusivamente de um fabricante/distribuidor, possibilitando liberdade para a migração, cópia e atualização sem a interferência ou dependência de uma empresa específica, comprometendo não só o acesso e a posteridade da informação, mas também os recursos financeiros dado a exclusividade de *software*, podendo o fornecedor descontinuar a

tecnologia, o produto ou exigir preços altos para a manutenção/atualização.

- Deve-se observar a obsolescência do *software* bem como a sua estabilidade no mercado para evitar tecnologia ultrapassada ou que não tenha se estabilizado com risco de descontinuidade.
- Passos para a escolha do *software*:
  - Verificar a possibilidade de uso de padrões abertos;
  - Permitir o acesso por diversos *softwares* disponíveis no mercado;
  - Verificar a estabilidade da tecnologia utilizada no *software*;
  - Verificar a obsolescência do *software*;
  - Providenciar a migração do *software*.

2.5.4 Independência do Sistema Gerenciador

- Depender exclusivamente do sistema para a preservação e acesso aos documentos é perigoso, pois acarreta uma dependência na qual a instituição se põe como refém do desenvolvedor. A restrição ao código fonte impede a atualização do sistema às necessidades organizacionais além de impossibilitar o melhoramento contínuo deste.
- Passos para um sistema gerenciador confiável:
  - Conversão de banco de dados para estrutura aberta;
  - Banco de dados em estrutura com estrutra de codificação aberta;
  - Servidor do depósito digital;
  - Estrutura de diretórios conhecida e organizada da documentação digital.
- Os metadados, assim como os documentos, também devem funcionar de forma independente do sistema em formatos abertos, pois são fundamentais para a indexação e contextualização dos documentos arquivísticos. Uma tecnologia muito utilizada para este fim é o XML (*eXtensible Markup Language*), que permite o armazenamento e a interoperabilidade através dos padrões abertos.
- Os documentos e seus metadados devem ser acessíveis a qualquer momento independente de sistema gerenciador por meio de depósitos

digitais estruturados, não havendo, desta forma, dependência com o sistema, podendo ser acessível em caso de falha do sistema gerenciador.

- A organização dos diretórios do depósito digital deve conter nomenclatura conhecida e inteligível, tanto para os diretórios quanto para os arquivos (estruturação com base no plano de classificação da atividade meio e fim).

2.5.5 Migração Periódica de Suporte e Formato

- A fragilidade dos suportes, a obsolescência das tecnologias, mídias, programas e formatos trazem a necessidade de migração constante dos documentos digitais a fim de se garantir seu acesso e preservação com fidedignidade e autenticidade sem perda do conteúdo ou alteração na forma de apresentação deste. É necessária a migração constante dos suportes e dos formatos dos documentos digitais, pois a ausência de uma rotina de migração implica na perda da documentação de forma irreversível, devendo ocorrer antes mesmo do problema ser detectado.
- Deve-se estabelecer rotinas de migração de formato e suporte levando em consideração a obsolescência destes, a fragilidade do suporte e a necessidade confiabilidade e autenticidade documentais.
- Ao se proceder com a migração, deve-se atentar à exposição dos dados do documento. Este deve ser migrado com a maior segurança e garantia de integridade possível, para que se tenha um documento íntegro e autêntico, sem alterações indesejadas de dados, estrutura etc.
- Passos para a migração de formato:
  - Selecionar formato de preservação;
  - Verificar obsolescência e independência do formato;
  - Providenciar migração do formato;
  - Verificar confiabilidade e adequação do formato.
- Fatores para a escolha do formato:
  - Padrões de formato aberto/gratuitos: independência de *hardware* e *software*;
  - Acessibilidade: garantir o acesso sem a necessidade de *software* proprietário;

- Estabilidade: formatos estáveis que garantam a atualização e compatibilidade;
- Suporte e metadados: campos de metadados que garantam o acesso e a preservação;
- Especificidade do formato: deve-se ter os formatos bem especificados e definidos, quanto mais complexo o formato mais complexo é a necessidade de preservação.
- Interoperabilidade: é preciso que haja a interação entre diferentes sistemas.
- Autenticidade: o formato deve ser capaz de garantir a integridade e integralidade do documento, seus dados, metadados e a sua estrutura.
- Processabilidade: é a capacidade de processamento do documento, a capacidade de edição deste. Minutas, por exemplo, precisam ser editáveis; já digitalizações, como no caso do AFD, necessitam de formatos estáticos para se evitar modificações que comprometam a autenticidade do documento.
- Apresentação: o formato deve ser capaz de apresentar o documento como este realmente é, apresentando seus dados na ordenação correta, tamanho, cores e padrões corretos conforme foi criado.

- Passos para a migração de suporte:
  - Selecionar suporte de preservação;
  - Verificar obsolescência e independência do suporte;
  - Providenciar migração do suporte;
  - Verificar confiabilidade e adequação do suporte.
- Fatores para a escolha do suporte:
  - Compatibilidade: deve ser compatível com as demais tecnologias do mercado e as atuais tecnologias empregadas na instituição;
  - Estabilidade: o suporte deve ser estável, garantindo a preservação e a migração de suporte sem dificuldades ou riscos de instabilidade;
  - Acessibilidade: suporte que possa ser comprado em diversos fabricantes e modelos, evitando-se a dependência a uma empresa;
  - Confiabilidade: deve garantir o acesso sem demais riscos por um longo período;

- Qualidade: ter matéria-prima de boa qualidade, ter sido feito por processos confiáveis e de marca reconhecida;
- Capacidade: ser compatível com a quantidade de dados armazenados e com os futuros dados a serem armazenados. Esse dado é de fundamental importância para assegurar que não haverá falta de espaço de armazenamento para os documentos digitais.

2.5.6 Replicação do Sistema em Local Distante

- A criação de um *site backup* longe do *data center* é de fundamental importância tendo em vista que em caso de sinistro, se os documentos originais e os replicados estiverem fisicamente juntos, perder-se-á os documentos e a história administrativa em sua integralidade. Apesar da implementação de uma política preservação contendo um plano de contingência e de riscos, catástrofes podem ocorrer, sendo inevitável a necessidade de replicação dos dados em locais distintos.
- O *site backup* deve ter no mínimo o mesmo nível de segurança do *data center* principal, sendo recomendável inclusive o armazenamento em cofres de segurança antichamas e climatizados dos documentos considerados secretos.

2.5.7 Suporte de Armazenamento

- O suporte do documento digital é o mais sensível e frágil suporte para de armazenar informação da atualidade, estas características intrínsecas do suporte criam a necessidade constante de monitoramento e migração, devendo a instituição estar preparada para fazê-los. O suporte do documento digital não pode ser danificado. Qualquer dano, por menor que seja, pode comprometer o acesso aos documentos ali armazenados. A migração deve ser feita antes de constatado o erro ou dano, sendo este o fator mais difícil de ser controlado e monitorado, pois é invisível a olho nu, diferentemente dos documentos analógicos.
- Medidas aplicáveis para se garantir a integridade do suporte e da informação:

- Definir uma previsão de vida útil por suporte considerando: variáveis que causam a degradação; utilização; fatores biológicos; fatores ambientais; análise das mídias etc;
- Estabelecer uma tabela de confiabilidade para o tempo de uso e armazenamento. A tabela é fundamental para que se tenha a garantia de tempo hábil para a migração de suporte sem comprometer a confiabilidade dos documentos e do sistema;
- Armazenar o suporte em ambiente adequado. Estudos indicam grande grau de influência das condições ambientais para a durabilidade dos suportes e da preservação digital, sendo que a temperatura ideal varia de 10° a 20° com umidade relativa de 20% a 40%;
- Implementar rotinas de verificação do tempo de uso e armazenamento;
- Proceder com a migração ou rejuvenescimento do suporte.

2.5.8 Backup/Cópias de Segurança

- Ter uma política de *backup* é um pilar fundamental para a preservação e garantia da autenticidade documental tendo em vista a fragilidade do suporte e da possibilidade de catástrofes. É inevitável o *backup* integral dos dados do sistema, garantindo desta forma a possibilidade de acesso e a posteridade dos documentos, independente de falhas ou desastres.
- Implementar uma política de *backup* depende de:
  - Equipe responsável: definição da equipe responsável pela elaboração, implementação revisão e manutenção das rotinas de *backup*;
  - Acervo digital: definição de todo conteúdo que fará parte da política de *backup*, documentos, bases de dados, arquivos etc;
  - Normas e procedimentos: portaria normativa estabelecendo procedimentos padronizados para a realização, manutenção e confiabilidade do *backup*;
  - Conscientização do usuário: no que diz respeito a seguir os procedimentos e as regras estabelecidas;

- Implementação: colocação de todos os procedimentos e normas em funcionamento;
- Revisão periódica: considerando a evolução tecnológica, à realidade institucional etc.

2.5.9 Eliminação Periódica do Lixo Digital

- Apesar de não ser visível como na documentação analógica, a massa documental acumulada também está presente no ambiente digital de forma discreta, lotando os discos e o sistema com uma documentação desprovida de valor arquivístico ou que já tenha seu prazo de guarda atingido e que poderia ser eliminada. A falta metodologia arquivística dentro do sistema acarreta em uma documentação desorganizada e impossível de ser gerenciada a partir da determinação de valores e de possibilidades de eliminação. Para que se evite tal cenário, é inevitável a aplicação de metodologia arquivística para a organização do acervo digital desde sua criação até a destinação final dos documentos.
- O estabelecimento da gestão documental no sistema em todas as três fases (produção, utilização e destinação) garante uma informação estruturada e passível de uso e gestão. Ressalta-se a necessidade de se ter a classificação como a função matricial do sistema, já que todas as demais atividades arquivísticas dependem desta. A classificação proporciona um conjunto documental estruturado e organizado com base em princípios funcionais e hierarquizantes da documentação, possibilita também o controle dos prazos de guarda e o controle da destinação final dos documentos por se integrar às tabelas de temporalidade, ou seja, com a documentação digital classificada é possível gerar listas de eliminação a serem analisadas pela Comissão Permanente de Avaliação de Documentos (CPAD).
- O acúmulo do lixo digital além de comprometer o bom uso do sistema por sobrecarregá-lo, também gera custos altos à gestão, pois será tratado como um documento de valor, sendo incluído em migrações, em *backups*, e atualizações de *hardware* e *software*, aumentando exponencialmente o custo de cada uma dessas operações.

- Para que se evite o lixo digital é inevitável a integração do sistema com a gestão documental, principalmente no que diz respeito à classificação e ao estabelecimento de prazos de guarda e destinação final. Adotando-se um sistema integrado com a gestão, eliminações periódicas podem ocorrer sem comprometer o uso e a manutenção do sistema.
- Passos para proceder com a eliminação do lixo digital:
    - Tabela de temporalidade: a aplicação da tabela, dos prazos e destinações é precedida de documentação classificada, a partir da classificação dos documentos digitais pode-se gerenciar os prazos de guarda e a destinação final dos documentos. Estes instrumentos devem ser revistos sempre que necessário pela CPAD;
    - Avaliação: a avaliação é precedida de documentos classificados e de uma CPAD legalmente instituída com profissionais de diferentes áreas para avaliar o valor dos documentos. A avaliação determina os prazos de guarda e a destinação final dos documentos, atualizando a tabela de temporalidade bem como determinando a eliminação ou preservação dos documentos;
    - Proceder com a listagem de eliminação dos documentos que tenham cumprido os prazos de guarda e cuja destinação final é a eliminação;
    - Elaborar edital de ciência de eliminação a ser publicado no Diário Oficial da União;
    - Elaborar e assinar termo de eliminação;
    - Eliminar os documentos.

2.5.10 Garantia da Autenticidade

- A garantia da autenticidade do documento digital é essencial para que este seja fonte de prova e seja confiável. A autenticidade é garantida por meio de rígidos processos de segurança, controle de acesso, controle de metadados etc. Por ser exposta a cada migração, a preservação da autenticidade do documento digital merece atenção em cada nova migração ou mudança de formato, devendo-se adotar controles essenciais à garantia da confiabilidade e a fidedignidade do documento.

A garantia da autenticidade deve ser preservada desde a criação até a destinação final do documento.

- Garante-se a autenticidade do documento digital por meio de:
  - Trilhas de auditoria: rastreamento de todas as intervenções e suas tentativas feitas no documento a partir de informações registradas, verifica-se: acesso, alteração, visualização, exclusão, trâmite, migrações, outros;
  - Controle de acesso: deve-se restringir o acesso aos documentos a pessoal autorizado por meio de níveis de acesso;
  - Metadados de preservação: preserva e garante a integridade da informação ao longo do tempo, registra todo o histórico de acesso, migrações, rejuvenescimento, mídias, sistemas etc;
  - Exposição mínima do documento digital: deve-se acessá-lo somente quando necessário;
  - Ferramentas de migração: estabelecimento de rotinas de *refreshing* e migração de forma a não comprometer o documento pela obsolescência/fragilidade do suporte ou da tecnologia.

2.5.11 Considerações

Tendo em vista a fragilidade do suporte e da obsolescência tecnológica inerentes à documentação digital e ao sistema informatizado, é necessário que se observe os requisitos elencados como forma de se garantir a posteridade dos documentos e dados digitais pelo período estipulado na legislação.

A não observância dos requisitos expostos podem implicar em perda dos dados e documentos armazenados no sistema por conta de algum sinistro, dano na mídia de armazenamento ou obsolescência de *hardware* e *software* que não permita o acesso aos documentos.

Ressalta-se que a preservação da documentação digital deve ser um ponto de atenção e dedicação constantes, já que o paradigma digital traz a fragilidade e a obsolescência como fenômenos naturais nos sistemas e mídias.

Não sendo possível a adoção, na íntegra, das recomendações elencadas, deve-se atentar quanto à prioridade da adoção dos requisitos. Para tanto,

foi estabelecido o padrão sendo que 1 é extremamente necessário, 2 é necessário e 3 é altamente desejável:

- Política de preservação (1)
- Independência de *hardware* específico (3)
- Independência de *software* específico (3)
- Independência do sistema gerenciador (3)
- Migração periódica de suporte e formato (1)
- Replicação do sistema em local distante (1)
- Suporte de armazenamento (1)
- *Backup*/cópias de segurança (1)
- Eliminação periódica do lixo digital (1)
- Garantia da autenticidade (1)

2.6 Plano de Gestão de Riscos de TI – Implantação do Processo Eletrônico Nacional no IFB

De acordo com o Decreto nº 8539 de 8 de outubro de 2015 que dispõe sobre o uso do meio eletrônico para a realização do processo administrativo no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional e a portaria MEC nº 1042 de 04 de novembro de 2015, que dispõe sobre a implantação e o funcionamento do processo eletrônico no âmbito do Ministério da Educação, faz-se necessária a implantação de um sistema de gerenciamento eletrônico de documentos nos Institutos Federais em até dois anos a partir da publicação do decreto acima mencionado.

A adoção de um sistema eletrônico de gerenciamento de documentos, sem dúvidas, será um grande avanço na gestão de documentos do IFB, podendo trazer mais eficiência e agilidade aos processos da instituição. Porém, tal ação traz riscos, os quais devem ser conhecidos, analisados e tratados. Este documento é um planejamento preliminar de gerenciamento dos riscos que ameaçam o sucesso do projeto, seu impacto potencial e das ações que podem ser tomadas para tratá-los.

Neste trabalho foi utilizada a Metodologia de Gestão de Riscos do SISP, guia publicado em 2015 que busca orientar o trabalho de gestão de riscos de

segurança da informação no âmbito do SISP (Sistema de Administração dos Recursos de Tecnologia da Informação).

A metodologia é composta pelas seguintes etapas:

1 Estabelecer Contexto (EC);
2 Identificar Riscos (IR);
3 Estimar Riscos (ER);
4 Avaliar Riscos (AR);
5 Tratar Riscos (TR);
6 Comunicar Riscos (CR);
7 Monitorar Riscos (MR).

As etapas 1 a 5 serão contempladas neste documento. As atividades de comunicação e monitoramento dos riscos serão executadas durante o projeto.

2.6.1 Contexto e Identificação dos Riscos

2.6.1.1 Contexto

A primeira atividade da gestão de riscos é designar o contexto no qual será feita a análise de riscos.

Esse trabalho engloba o projeto de implantação do PEN no âmbito do IFB, portanto, as atividades deste projeto serão incluídas na análise de riscos. No entanto, dada a magnitude do projeto, é necessário dividi-lo em pelo menos 3 (três) contextos, objetivando uma análise de riscos mais objetiva e eficiente. Dessa forma, foram identificados os contextos principais neste projeto: pessoal, infraestrutura e sistema.

Não foi considerada, neste trabalho, a parte interna do sistema. Os riscos relacionado a este contexto são tratados no processo de desenvolvimento do produto.

2.6.1.2 Identificação

O trabalho de identificação dos riscos foi executado utilizando, como principais técnicas, a análise documental e o *pondering/brainstorm*. A lista de riscos identificados é apresentada na Tabela 1, divididos por contexto:

Item	*Contexto*	*Risco*
1	Pessoal	Ausência de profissionais de TI capacitados no sistema;
2		Saída de profissionais envolvidos no projeto;
3	Infraestrutura	Indisponibilidade devido à pane elétrica;
4		Indisponibilidade devido à falha no link de comunicação;
5		Indisponibilidade devido à danos aos equipamentos (incêndio, inundação, vandalismo);
6		Falta de espaço lógico para armazenamento de informações;
7		Instabilidade no serviço devido à quantidade de acessos;
8		Perda de dados dos servidores;
9		Roubo de dados dos servidores;
10		Indisponibilidade por ataque;
11	Sistema	Sistema não atender às necessidades da Instituição/Legislação
12		Implantação demorada devido as dificuldades técnicas
13		Demora para atualizar ou corrigir o sistema

Tabela 1: Riscos identificados

2.6.2 Estimativa, Avaliação e Tratamento

Esta etapa trata da estimação (consequências, probabilidade, nível) dos riscos identificados anteriormente. O nível do risco é o produto da consequência pela probabilidade. Estimados os riscos, estes devem ser classificados de acordo com o nível (avaliação) e deve ser definido o tipo de tratamento que será aplicado a cada um.

2.6.2.1 Estimativa

Risco 1: Ausência de profissionais de TI capacitados no sistema;

Probabilidade: 3 - Depende do sistema que será escolhido. Neste caso, adotou-se o valor médio.

Consequência: 3 - Média
Nível do risco: 9
Tipo de tratamento: Mitigar
Ação de tratamento 1.1: Solicitar documentação (documentação de código, tutoriais, guias, etc) ao órgão responsável pelo sistema.
Ação de tratamento 1.2: Providenciar treinamentos para os servidores envolvidos na implantação e manutenção do sistema.

Risco 2: Saída de profissionais envolvidos no projeto;

Probabilidade: 3 - Média
Consequência: 3 - Média
Nível do risco: 9
Tipo de tratamento 1: Aceitar (Probabilidade)
Tipo de tratamento 2: Mitigar (Consequência)
Ação de tratamento 2.1: Incentivar o compartilhamento de informação entre os participantes do projeto, de forma que um membro da equipe consiga dar continuidade às atividades de outro que porventura saia.

Risco 3: Indisponibilidade devido à pane elétrica nos equipamentos;

Probabilidade: 1- Baixa. O datacenter do IFB e os *campi* definitivos já possuem um sistema de proteção elétrica que reduz drasticamente os riscos de problemas na rede elétrica de TI (ausência de fornecimento, sobrecarga, etc).
Consequência: 5 - Alta
Nível do risco: 5
Tipo de tratamento 1: Mitigar (Probabilidade)
Ação de tratamento 3.1: Acionar o fabricante da solução assim que for detectada alteração em algum equipamento.

Risco 4: Indisponibilidade devido à falha no link de comunicação;

Probabilidade: 3 - Média. O link de dados que o IFB utiliza apresenta baixa indisponibilidade. Porém, como todo serviço semelhante, está sujeito à falhas.
Consequência: 5 - Alta
Nível do risco: 15
Tipo de tratamento: Mitigar (Probabilidade)
Ação de tratamento 4.1: Contratar um segundo link de dados para o datacenter do IFB.

Risco 5: Indisponibilidade devido à danos aos equipamentos (incêndio, inundação, vandalismo);

Probabilidade: 3 - Média
Consequência: 5 - Alta
Nível do risco: 15
Tipo de tratamento: Mitigar (Probabilidade)
Ação de tratamento 5.1: Implantar um sistema de proteção contra incêndio no datacenter do IFB e no *site backup* do sistema.
Ação de tratamento 5.2: Adaptar a estrutura da sala do datacenter do IFB de forma a evitar inundações ou infiltrações que possam danificar os equipamentos.
Ação de tratamento 5.3: Implantar sistema de controle de acesso e de câmeras de vigilância (já parcialmente implantado) nas dependências do datacenter do IFB e no *site backup* do sistema, reduzindo as chances de acesso indevido ao local.

Risco 6: Falta de espaço lógico para armazenamento de informações;

Probabilidade: 3 - Média. A solução de armazenamento de dados do IFB possui grande espaço para armazenamento de dados e, por ser uma solução modular, pode ser expandida de acordo com as necessidades da instituição. Porém, dado que toda documentação do Instituto passará a circular em formato digital, a demanda de espaço de armazenamento pode crescer rapidamente.
Consequência: 5 - Alta
Nível do risco: 15
Tipo de tratamento: Mitigar (Probabilidade)
Ação de tratamento 6.1: Planejar o volume de armazenamento necessário para o funcionamento do sistema em seus primeiros 2 anos, baseando-se em dados de outros órgãos que já utilizam a solução.
Ação de tratamento 6.2: Caso necessário, adquirir mais discos para os equipamentos de armazenamento e até mesmo novos equipamentos, com base no resultado do planejamento da Ação 5.1.
Ação de tratamento 6.3: Monitorar a utilização do volume de armazenamento disponível, efetuando a expansão do volume de armazenamento sempre que a quantidade de espaço utilizada se aproxime dos 80%.

Risco 7: Instabilidade no serviço devido à quantidade de acessos;

Probabilidade: 3 - Média
Consequência: 3 - Média
Nível do risco: 9
Tipo de tratamento: Mitigar (Ocorrência)

Ação de tratamento 7.1: Planejar a quantidade esperada de acessos ao sistema, baseando-se na experiência de outros órgãos e na quantidade de servidores com acesso ao sistema.
Ação de tratamento 7.2: Realizar testes exaustivos antes da implantação efetiva (produção) do sistema, de forma a garantir que a infraestrutura suportará a demanda da instituição.
Ação de tratamento 7.3: Fazer os ajustes necessários na infraestrutura de acordo com o resultado dos testes efetuados.

Risco 8: Perda de dados dos servidores;

Probabilidade: 3 - Média
Consequência: 5 - Alta
Nível do risco: 15
Tipo de tratamento: Mitigar (Ocorrência)
Ação de tratamento 8.1: Implantar e manter estrutura redundante de datacenter (*site backup*) e de armazenamento (storage).
Ação de tratamento 8.2: Verificar se a solução de cópia de segurança (backup) utilizada hoje no IFB atende às necessidades do sistema.
Ação de tratamento 8.3: Caso necessário, implantar e manter nova solução de backup para os dados do sistema.

Risco 9: Roubo de dados dos servidores;

Probabilidade: 3 - Médio
Consequência: 5- Alta
Nível do risco: 15
Tipo de tratamento: Mitigar (Ocorrência)
Ação de tratamento 9.1: Implantar e manter solução de segurança (firewall, IDS, IPS, proxy, etc) na rede do IFB para evitar ataques à segurança dos dados armazenados.
Ação de tratamento 9.2: Verificar os protocolos e interfaces de comunicação com o barramento PEN em relação à criptografia, acesso e confidencialidade dos dados.
Ação de tratamento 9.3: Realizar testes exaustivos antes da implantação efetiva (produção) do sistema, de forma a garantir os requisitos de segurança necessários. Se necessário, contratar uma equipe externa para realizar esta atividade.

Risco 10: Indisponibilidade por ataque;

Probabilidade: 3 - Médio.
Consequência: 3 - Médio
Nível do risco: 9
Tipo de tratamento: Mitigar (Ocorrência)

Ações de tratamento 10: Ver ações 9.1, 9.2 e 9.3.

Risco 11: Sistema não atender às necessidades da Instituição ou da Legislação

Probabilidade: 1 – Baixa.
Consequência: 5 - Alta
Nível do risco: 5
Tipo de tratamento: Mitigar (Ocorrência)
Ação de tratamento 11.1: Estudar cuidadosamente as opções de sistemas disponíveis para atender esta necessidade;
Ação de tratamento 11.2: Documentar e mapear o funcionamento dos processos impactados pelo PEN e comparar com os fluxos suportados pelo sistema;

Risco 12: Implantação demorada devido as dificuldades técnicas

Probabilidade: 3 – Médio
Consequência: 3 - Médio
Nível do risco: 9
Tipo de tratamento: Mitigar (Ocorrência)
Ação de tratamento 10.1: Ver ações 1.1 e 1.2.

Risco 13: Demora para atualizar ou corrigir o sistema

Probabilidade: 1 – Baixo
Consequência: 3 - Médio
Nível do risco: 3
Tipo de tratamento: Mitigar (Ocorrência)
Ação de tratamento 13.1: Ver ação 11.1.
Ação de tratamento 13.2: Manter contato com a equipe/instituição que desenvolve a aplicação, de forma que as necessidades de melhorias ou correções possam ser repassadas no menor tempo possível.

A Tabela 2 apresenta um resumo dos riscos levantados, avaliados e das ações de tratamento estabelecidas. Os riscos estão ordenados decrescente de nível de risco.

ID	Contexto	Risco	Nível			Tratamento	
			P	C	N	Tipo	Ações
8	Infraestrutura de TI	Perda de dados nos servidores;	3	5	15	Mitigar	Implantar e manter estrutura redundante de datacenter (*site backup*) e de armazenamento (*storage*).
							Verificar se a solução de cópia de segurança (backup) utilizada hoje no IFB atende às necessidades do sistema.
							Caso necessário, implantar e manter nova solução de backup para os dados do sistema.
9	Infraestrutura de TI	Roubo de dados dos servidores;	3	5	15	Mitigar	Implantar e manter solução de segurança (f*irewall, IDS, IPS, proxy, etc*) na rede do IFB para evitar ataques à segurança dos dados armazenados.
							Verificar os protocolos e interfaces de comunicação com o barramento PEN em relação à criptografia, acesso e confidencialidade dos dados.
							Realizar testes exaustivos antes da implantação efetiva (produção) do sistema, de forma a garantir os requisitos de segurança necessários. Se necessário, contratar uma equipe externa para realizar esta atividade.
5	Infraestrutura de TI	Indisponibilidade devido à danos aos equipamentos (incêndio, inundação, vandalismo);	3	5	15	Mitigar (Probabilidade)	Implantar um sistema de proteção contra incêndio no datacenter do IFB e no *site backup* do sistema.
							Implantar sistema de controle de acesso e de câmeras de vigilância (já parcialmente implantado) nas dependências do datacenter do IFB e no *site backup* do sistema, reduzindo as chances de acesso indevido ao local.
							Adaptar a estrutura da sala do datacenter do IFB de forma a evitar inundações ou infiltrações que possam danificar os equipamentos.
6	Infraestrutura de TI	Falta de espaço lógico para armazenamento de informações;	3	5	15	Mitigar (Probabilidade)	Planejar o volume de armazenamento necessário para o funcionamento do sistema em seus primeiros 2 anos, baseando-se em dados de outros órgãos que já utilizam a solução.

ID	Contexto	Risco	Nível			Tratamento	
			P	C	N	Tipo	Ações
							Caso necessário, adquirir mais discos para os equipamentos de armazenamento e até mesmo novos equipamentos, com base no resultado do planejamento da Ação 6.1.
							Monitorar a utilização do volume de armazenamento disponível, efetuando a expansão do volume de armazenamento sempre que a quantidade de espaço utilizada se aproxime dos 80%.
10	Infraestrutura de TI	Indisponibilidade por ataque;	3	3	9	Mitigar	Implantar e manter solução de segurança (firewall, IDS, IPS, proxy, etc) na rede do IFB para evitar ataques à segurança dos dados armazenados.
							Verificar os protocolos e interfaces de comunicação com o barramento PEN em relação à criptografia, acesso e confidencialidade dos dados.
							Realizar testes exaustivos antes da implantação efetiva (produção) do sistema, de forma a garantir os requisitos de segurança necessários. Se necessário, contratar uma equipe externa para realizar esta atividade.
4	Infraestrutura de TI	Instabilidade no serviço devido à falha no link de comunicação;	3	3	9	Mitigar (Probabilidade)	Contratar um segundo link de dados para o datacenter do IFB.
7	Infraestrutura de TI	Instabilidade no serviço devido à quantidade de acessos;	3	3	9	Mitigar (Probabilidade)	Planejar a quantidade esperada de acessos ao sistema, baseando-se na experiência de outros órgãos e na quantidade de servidores com acesso ao sistema.
							Realizar testes exaustivos antes da implantação efetiva (produção) do sistema, de forma a garantir que a infraestrutura suportará a demanda da instituição.
							Fazer os ajustes necessários na infraestrutura de acordo com o resultado dos testes efetuados.

ID	Contexto	Risco	Nível			Tratamento	
			P	C	N	Tipo	Ações
12	Sistema	Implantação demorada devido a dificuldades técnicas	3	3	9	Mitigar	Solicitar documentação (documentação de código, tutoriais, guias, etc) ao órgão responsável pelo sistema.
							Providenciar treinamentos para os servidores envolvidos na implantação e manutenção do sistema.
1	Pessoal	Ausência de profissionais de TI capacitados no sistema;	3	3	9	Mitigar	Solicitar documentação (documentação de código, tutoriais, guias, etc) ao órgão responsável pelo sistema.
							Providenciar treinamentos para os servidores envolvidos na implantação e manutenção do sistema.
2	Pessoal	Saída de profissionais envolvidos no projeto;	3	3	9	Aceitar (Probabilidade)	-
						Mitigar (Consequência)	Incentivar o compartilhamento de informação entre os participantes do projeto, de forma que um membro da equipe consiga dar continuidade às atividades de outro que porventura saia.
3	Infraestrutura de TI	Indisponibilidade devido à pane elétrica;	1	5	5	Mitigar (Probabilidade)	Acionar o fabricante da solução assim que for detectada alteração em algum equipamento.
11	Sistema	Sistema não atender às necessidades da Instituição/Legislação	1	5	5	Mitigar	Estudar cuidadosamente as opções de sistemas disponíveis para atender esta necessidade;
							Documentar e mapear o funcionamento dos processos impactados pelo PEN e comparar com os fluxos suportados pelo sistema;
13	Sistema	Demora para atualizar ou corrigir o sistema	1	3	3	Mitigar	Estudar cuidadosamente as opções de sistemas disponíveis para atender esta necessidade;
							Manter contato com a equipe/instituição que desenvolve a aplicação, de forma que as necessidades de melhorias ou correções possam ser repassadas no menor tempo possível.

Tabela 2: Resumo da Análise de Riscos do Projeto

VI - Conclusão

Tomando como base o Decreto nº 8.539 de 8 de outubro de 2015, que dispõe sobre o uso do meio eletrônico para a realização do processo administrativo no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional; e a portaria MEC nº 1.042 de 04 de novembro de 2015, que dispõe sobre a implantação e o funcionamento do processo eletrônico no âmbito do Ministério da Educação, faz-se necessária a implantação de um Sistema Informatizado de Gestão Arquivística de Documentos nos Institutos Federais em até dois anos a partir da publicação do decreto acima mencionado.

Para dar maior embasamento à tomada de decisão, foram realizados estudos e análises dos requisitos mínimos necessários à implantação do barramento PEN no Instituto Federal de Brasília, com toda observância aos critérios de segurança da informação. Todavia, é imprescindível enfatizar que o presente documento não exclui a importância de novos estudos e trabalhos técnicos, tais como:

- Levantamento de custos de cada uma das ações relacionadas;
- Comparativo entre as opções de sistemas presentes no mercado;
- Mensuração documental e projeto de um arquivo central; dentre outros.

Por todo exposto, fica claro que este projeto exigirá esforço, comprometimento e recursos da instituição. Porém, é evidente também que o sucesso do projeto poderá gerar inúmeros benefícios para toda a comunidade do IFB, especialmente seu cliente final, o cidadão.

É possível desde já concluir que a implantação de um Sistema Informatizado de Gestão Arquivística de Documentos no Instituto Federal de Brasília representará um passo importante rumo à processos de negócio mais transparentes, ágeis e eficientes, desde que atendidos os requisitos e tratados os riscos aqui apresentados. Mais do que simplesmente atender à uma determinação legal, o gerenciamento eletrônico de documentos é uma grande oportunidade para que o IFB entre numa nova era de gestão da informação, adequada aos desafios que o serviço público enfrenta nesta segunda década do século XXI.

VI - Referência Bibliográfica

BRASIL. Decreto n° 8.539, de 08 de outubro de 2015. **Dispõe sobre o uso do meio eletrônico para a realização do processo administrativo no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2015/Decreto/D8539.htm>.

BRASIL. Portaria MEC n° 1.042, de 04 de novembro de 2015. **Dispõe sobre a implantação e o funcionamento do processo eletrônico no âmbito do Ministério da Educação.** Disponível em: <http://www.abmes.org.br/legislacoes/visualizar/id/1799>

BRASIL. Portaria Interministerial n° 1.677, de 07 de outubro de 2015. **Define os procedimentos gerais para o desenvolvimento das atividades de protocolo no âmbito dos órgãos e entidades da Administração Pública Federal.** Disponível em: <http://www.comprasgovernamentais.gov.br/arquivos/outros_normas/portaria-1677.pdf>.

BRASIL. Portaria Interministerial n° 2.320, de 30 de dezembro de 2015. **Institui o Sistema Protocolo Integrado no âmbito dos órgãos e entidades da Administração Pública Federal.** Disponível em: <http://www.comprasgovernamentais.gov.br/paginas/portarias/portaria-interministerial-no-2-320-de-30-de-dezembro-de-2014>.

BRASIL. Portaria Interministerial n° 2.321, de 30 dezembro de 2015. **Define os procedimentos relativos à utilização do Número Único de Protocolo - NUP no âmbito dos órgãos e entidades da Administração Pública Federal e dá outras providências.** Disponível em: <http://www.comprasgovernamentais.gov.br/paginas/portarias/portaria-interministerial-no-2-321-de-30-de-dezembro-de-2014>.

BRASIL. Medida Provisória n° 2.200-2, de 44 de agosto de 2001. **Institui a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, transforma o Instituto Nacional de Tecnologia da Informação em autarquia, e dá outras providências.** Disponível em: <http://www.planalto.gov.br/ccivil_03/mpv/Antigas_2001/2200-2.htm>.

BRASIL. Norma Complementar n° 20, de 15 de julho de 2014. **Diretrizes de segurança da informação e comunicações para instituição do processo de tratamento da informação nos órgãos e entidades da administração pública federal.** Disponível em: <http://dsic.planalto.gov.br/documentos/nc_20_TRATAMENTO_DA_INFORMACAO.pdf>.

BRASIL. Resolução n° 20, de 16 de julho de 2004. **Dispõe sobre a inserção dos documentos digitais em programas de gestão arquivística de documentos dos órgãos e entidades integrantes do Sistema Nacional de Arquivos.** Disponível em: <http://www.conarq.arquivonacional.gov.br/legisla%C3%A7%C3%A3o/resolu%C3%A7%C3%B5es-do-conarq/262-resolu%C3%A7%C3%A3o-n%C2%BA-20,-de-16-de-julho-de-2004.html>.

BRASIL. Resolução n° 25, de 27 de abril de 2007.**Dispõe sobre a adoção do Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos - e-ARQ Brasil pelos órgãos e entidades integrantes do Sistema Nacional de Arquivos - SINAR.** Disponível em: <http://www.conarq.arquivonacional.gov.br/legisla%C3%A7%C3%A3o/resolu%C3%A7%C3%B5es-do-conarq/267-resolu%C3%A7%C3%A3o-n%C2%BA-25,-de-27-de-abril-de-2007.html>.

BRASIL. Resolução n° 32, de 17 de maio de 2010. **Dispõe sobre a inserção dos Metadados na Parte II do Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos - e-ARQ Brasil.** Disponível em: <http://www.conarq.arquivonacional.gov.br/legisla%C3%A7%C3%A3o/resolu%C3%A7%C3%B5es-do-conarq/274-resolu%C3%A7%C3%A3o-n%C2%BA-32,-de-17-de-maio-de-2010.html>.

BRASIL. Lei n° 12.682, de 09 de julho de 2012. **Dispõe sobre a elaboração e o arquivamento de documentos em meios eletromagnéticos.** Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/Lei/L12682.htm>.

BRASIL. Lei n° 8.159, de 08 de janeiro de 2001.**Dispõe sobre a política nacional de arquivos públicos e privados e dá outras providências.** Disponível em: <http://www.planalto.gov.br/ccivil_03/LEIS/L8159.htm>.

BRASIL. Decreto n° 4.073, de 03 de janeiro de 2002. **Regulamenta a Lei no 8.159, de 8 de janeiro de 1991, que dispõe sobre a política nacional de arquivos públicos e privados.** Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto/2002/d4073.htm>.

BRASIL. Lei n° 12.527, de 18 de novembro de 2011. **Regula o acesso a informações previsto no inciso XXXIII do art. 5o, no inciso II do § 3o do art. 37 e no § 2o do art. 216 da Constituição Federal; altera a Lei no 8.112, de 11 de dezembro de 1990; revoga a Lei no 11.111, de 5 de maio de 2005, e dispositivos da Lei no 8.159, de 8 de janeiro de 1991; e dá outras providências.** Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm>.

BRASIL. Portaria AN/MJ n° 92, de 23 de setembro de 2011. **Aprova o Código de Classificação e a Tabela de Temporalidade e Destinação de Documentos de Arquivo relativos às Atividades-Fim das Instituições Federais de Ensino Superior (IFES).** Disponível em: <http://www.siga.arquivonacional.gov.br/index.php/24-legislacao-e-normas/205-portaria-an-mj-n-92-de-23-de-setembro-de-2011>.

BRASIL. Portaria MEC nº 1.224, de 18 de dezembro de 2013. **Institui normas sobre a manutenção e guarda do Acervo Acadêmico das Instituições de Educação Superior (IES) pertencentes ao sistema federal de ensino.** Disponível em: <http://www.siga.arquivonacional.gov.br/index.php/24-legislacao-e-normas/201-portaria-mec-n-1-224-de-18-de-dezembro-de-2013>.

BRASIL. Portaria MEC nº 1.261, de 23 de dezembro de 2013. **Determina a obrigatoriedade do uso do Código de Classificação e a Tabela de Temporalidade e Destinação de Documentos de Arquivo relativos às Atividades-Fim das Instituições Federais de Ensino Superior, aprovado pela Portaria nº 92 do Arquivo Nacional, de 23 de setembro de 2011, pelas IFES e dá outras providências.** Disponível em: <http://www.siga.arquivonacional.gov.br/index.php/24-legislacao-e-normas/200-portaria-mec-n-1-261-de-23-de-dezembro-de-2013>.

BRASIL. Resolução nº 14, de 24 de outubro de 2001. **Aprova a versão revisada e ampliada da Resolução nº 4, de 28 de março de 1996, que dispõe sobre o Código de Classificação de Documentos de Arquivo para a Administração Pública: Atividades-Meio, a ser adotado como modelo para os arquivos correntes dos órgãos e entidades integrantes do Sistema Nacional de Arquivos (SINAR), e os prazos de guarda e a destinação de documentos estabelecidos na Tabela Básica de Temporalidade e Destinação de Documentos de Arquivo Relativos as Atividades-Meio da Administração Pública.** Disponível em: <http://www.conarq.arquivonacional.gov.br/legisla%C3%A7%C3%A3o/resolu%C3%A7%C3%B5es-do-conarq/256-resolu%C3%A7%C3%A3o-n%C2%BA-14,-de-24-de-outubro-de-2001.html>.

RONDINELLI, ROSELY CURI. **Gerenciamento arquivístico de documentos eletrônicos**. 4ª Edição. Rio de Janeiro: FGV, 2005.

SANTOS, V. B. dos; INNARELLI, H. C; SOUSA. R. T. B. de. **Arquivística: Temas contemporâneos: Classificação, preservação digital, gestão do conhecimento**. 3ª Edição. Distrito Federal: Senac, 2013.

ANEXOS

1. **Decreto n° 8.539, de 8 de outubro de 2015.**
2. **Portaria MEC 1.042 de 04 de novembro de 2015.**