Projeto Básico SUPEC 00057/2020

Título

Consulta Pública para aquisição de um Sistema Informatizado de Gestão Arquivística de Documentos (SIGAD)

1ª Versão

Vinculação com Documento de Oficialização de Demanda

Número DOD	Titulo da Demanda	Número do Item	Nome do Objeto	Descrição
2018-00019	INSTRUMENTO CONTRATUAL SEM ÔNUS E CONSULTA PÚBLICA	2	CONSULTA PÚBLICA	

1.0 Objeto

1. Consulta Pública para aquisição de um Sistema Informatizado de Gestão Arquivística de Documentos (SIGAD)

2.0 Especificação do objeto a ser contratado

2.1. Aquisição de um Sistema Informatizado de Gestão Arquivística de Documentos (SIGAD).

2.2. Características de um SIGAD:

2.2.1. Organização dos documentos arquivísticos: plano de classificação e manutenção de documentos

2.2.1.1. Configuração e administração do plano de classificação no SIGAD

2.2.1.1.1. Incluir e ser compatível com o plano de classificação do órgão ou entidade.

2.2.1.1.2. Garantir a criação de classes, subclasses, grupos e subgrupos nos níveis do plano de classificação de acordo com o método de codificação adotado

2.2.1.1.3. Permitir a usuários autorizados acrescentar novas classes sempre que necessário

2.2.1.1.4. Registrar a data de abertura de uma nova classe no respectivo metadado

2.2.1.1.5. Registrar a mudança de nome de uma classe já existente no respectivo metadado

2.2.1.1.6. Permitir o deslocamento de uma classe inteira, incluídas as subclasses, grupo, subgrupos e documentos nela classificados, para outro ponto do plano de classificação. Nesse caso, é necessário fazer o registro do deslocamento nos metadados do plano de classificação.

2.2.1.1.7. Permitir que um usuário autorizado apague uma classe inativa.

2.2.1.1.8. Impedir a eliminação de uma classe que tenha documentos nela classificados. Essa eliminação pode ocorrer a partir do momento em que todos os documentos ali classificados tenham sido recolhidos ou eliminados, e seus metadados apagados, ou que esses documentos tenham sido reclassificados.

2.2.1.1.9. Permitir a associação de metadados às classes, conforme estabelecido no padrão de metadados, e deve restringir a inclusão e alteração desses mesmos metadados somente a usuários autorizados.

2.2.1.1.10. Disponibilizar pelo menos dois mecanismos de atribuição de identificadores a classes do plano de classificação, prevendo a possibilidade de se utilizar ambos, separadamente ou em conjunto, na mesma aplicação: atribuição de um código numérico ou alfanumérico; atribuição de um termo que identifique cada classe.

2.2.1.1.11. Prever um atributo associado às classes para registrar a permissão de uso daquela classe para classificar um documento.

2.2.1.1.12. Utilizar o termo completo para identificar uma classe.

2.2.1.1.13. Assegurar que os termos completos, que identificam cada classe, sejam únicos no plano de classificação.

2.2.1.1.14. Importar e exportar, total ou parcialmente, um plano de classificação.

2.2.1.1.15. Prover funcionalidades para elaboração de relatórios de apoio à gestão do plano de classificação, incluindo a capacidade de:

2.2.1.1.15.1. Gerar relatório completo do plano de classificação;

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

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

2.2.1.1.15.4. Gerar relatório de documentos classificados por unidade administrativa.

2.2.1.2. Classificação e metadados das unidades de arquivamento

2.2.1.2.1. Permitir a classificação das unidades de arquivamento somente nas classes autorizadas.

2.2.1.2.2. Permitir a classificação de um número ilimitado de unidades de arquivamento dentro de uma classe.

2.2.1.2.3. Utilizar o termo completo da classe para identificar uma unidade de arquivamento, tal como especificado no item 2.2.1.1.13.

2.2.1.2.4. Permitir a associação de metadados às unidades de arquivamento e deve

restringir a inclusão e alteração desses metadados a usuários autorizados.

2.2.1.2.5. Associar os metadados das unidades de arquivamento conforme estabelecido no padrão de metadados.

2.2.1.2.6. Permitir que uma nova unidade de arquivamento herde, da classe em que foi classificada, alguns metadados predefinidos.

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

2.2.1.3. Gerenciamento dos dossiês/processos

2.2.1.3.1. Registrar nos metadados as datas de abertura e de encerramento do dossiê/processo.

2.2.1.3.2. Permitir que um dossiê/processo seja encerrado por meio de procedimentos regulamentares e somente por usuários autorizados.

2.2.1.3.3. Permitir a consulta aos dossiês/processos já encerrados por usuários autorizados.

2.2.1.3.4. Impedir o acréscimo de novos documentos a dossiês/processos já encerrados.

2.2.1.3.5. Impedir sempre a eliminação de uma unidade de arquivamento digital ou de qualquer parte de seu conteúdo, a não ser quando estiver de acordo com a tabela de temporalidade e destinação de documentos.

2.2.1.3.6. Garantir sempre a integridade da relação hierárquica entre classe, dossiê/processo, volume e documento, e entre classe, pasta e documento, independentemente de atividades de manutenção, ações do usuário ou falha de componentes do sistema

2.2.1.4. Requisitos adicionais para o gerenciamento de processos

2.2.1.4.1. Prever a formação/autuação de processos, por usuário autorizado conforme estabelecido em legislação específica.

2.2.1.4.2. Prever funcionalidades para apoiar a pesquisa sobre a existência de processo relativo à mesma ação ou interessado.

2.2.1.4.3. Prever que os documentos integrantes do processo digital recebam numeração sequencial sem falhas, não se admitindo que documentos diferentes recebam a mesma numeração.

2.2.1.4.4. Controlar a renumeração dos documentos integrantes de um processo digital.

2.2.1.4.5. Prever procedimentos para juntada de processos segundo a legislação específica na devida esfera e âmbito de competência. A juntada pode ser por anexação ou apensação

2.2.1.4.6. Prever procedimentos para desapensação de processos segundo a legislação específica na devida esfera e âmbito de competência

2.2.1.4.7. Prever procedimentos para desentranhamento de documentos integrantes de um processo, segundo norma específica na devida esfera e âmbito de competência

2.2.1.4.8. Prever procedimentos para desmembramento de documentos integrantes de um processo, segundo norma específica na devida esfera e âmbito de competência.

2.2.1.4.9. Prever o encerramento dos processos incluídos seus volumes e metadados.

2.2.1.5. Volumes: abertura, encerramento e metadados

2.2.1.5.1. Gerenciar volumes para subdividir dossiês/processos, fazendo a distinção entre dossiês/processos e volumes.

2.2.1.5.2. Permitir que um volume herde, automaticamente, do dossiê/processo ao qual pertence, alguns metadados predefinidos, como, por exemplo, procedência, classes e temporalidade.

2.2.1.5 3. Permitir a abertura de volumes para qualquer dossiê/processo que não esteja encerrado.

2.2.1.5.4. Assegurar que um volume conterá somente documentos. Não é permitido que um volume contenha outro volume ou outro dossiê/processo.

2.2.1.5.5. Permitir que um volume seja encerrado por meio de procedimentos regulamentares e apenas por usuários autorizados.

2.2.1.5.6. Assegurar que, ao ser aberto um novo volume, o precedente seja automaticamente encerrado.

2.2.1.5.7. Impedir a reabertura, para acréscimo de documentos, de um volume já encerrado.

2.2.1.6. Gerenciamento de documentos e processos/dossiês arquivísticos convencionais e híbridos

2.2.1.6.1. Capturar documentos ou dossiês/processos convencionais e gerenciá-los da mesma forma que os digitais.

2.2.1.6.2. Gerenciar a parte convencional e a parte digital integrantes de dossiês/processos híbridos, associando-as com o mesmo número identificador atribuído

pelo sistema e o mesmo título, além de indicar que se trata de um documento arquivístico híbrido.

2.2.1.6.3. Permitir que um conjunto específico de metadados seja configurado para os documentos ou dossiês/processos convencionais e incluir informações sobre o local de arquivamento.

2.2.1.6.4. Dispor de mecanismos para acompanhar a movimentação do documento arquivístico convencional, de forma que fique evidente para o usuário a localização atual do documento.

2.2.1.6.5. Capaz de oferecer ao usuário funcionalidades para solicitar ou reservar a consulta a um documento arquivístico convencional, enviando uma mensagem para o detentor atual do documento ou para o administrador.

2.2.1.6.6. Assegurar que a recuperação de um documento ou dossiê/processo híbrido permita, igualmente, a recuperação dos metadados da parte digital e da convencional.

2.2.1.6.7. Garantir que a parte convencional e a parte digital correspondente recebam a mesma classificação de sigilo sempre que os documentos ou dossiês/processos híbridos estiverem classificados quanto ao grau de sigilo.

2.2.1.6.8. Registrar na trilha de auditoria todas as alterações efetuadas nos metadados dos documentos ou dossiês/processos convencionais e híbridos.

2.2.2. Tramitação e fluxo de trabalho (workflow)

2.2.2.1. Controle do fluxo de trabalho

2.2.2.1.1. Fornecer os passos necessários para o cumprimento de trâmites pré-estabelecidos ou aleatórios. Nesse caso, cada passo significa o deslocamento de um documento ou dossiê/processo de um participante para outro, a fim de serem objeto de ações.

2.2.2.1.2. Ter capacidade, sem limitações, de estabelecer o número necessário de trâmites nos fluxos de trabalho.

2.2.2.1.3. Disponibilizar uma função para avisar um participante do fluxo de que um documento lhe foi enviado, especificando a ação necessária.

2.2.2.1.4. Permitir o uso do correio eletrônico, para que um usuário possa informar a outros usuários sobre documentos que requeiram sua atenção.

2.2.2.1.5. Permitir que fluxos de trabalho pré-programados sejam definidos, alterados e mantidos exclusivamente por usuário autorizado.

2.2.2.1.6. Registrar na trilha de auditoria todas as alterações ocorridas neste fluxo.

2.2.2.1.7. Registrar a tramitação de um documento a fim de que os usuários possam conhecer a situação de cada um no processo.

2.2.2.1.8. Gerir os documentos em filas de espera que possam ser examinadas e controladas pelo administrador.

2.2.2.1.9. Ter a capacidade de deixar que os usuários visualizem a fila de espera de trabalhos a eles destinados e selecionem os itens a serem trabalhados.

2.2.2.1.10. Fornecer um histórico de movimentação dos documentos.

2.2.2.1.11. Incluir processamento condicional, isto é, permitir que um fluxo de trabalho seja suspenso para aguardar a chegada de um documento e prossiga automaticamente quando este é recebido.

2.2.2.1.12. Poder associar limites de tempo a trâmites e/ou procedimentos individuais em cada fluxo e comunicar os itens que expiraram de acordo com esses limites.

2.2.2.1.13. Reconhecer indivíduos e grupos de trabalho como participantes.

2.2.2.1.14. Fornecer meios de elaboração de relatórios completos para permitir que gestores monitorem a tramitação dos documentos e o desempenho dos participantes.

2.2.2.1.15. Registrar a tramitação de um documento em seus metadados. Os metadados referentes à tramitação devem registrar data e hora de envio e recebimento, e a identificação do usuário.

2.2.2.1.16. Manter versões dos fluxos alterados e estabelecer vínculos entre os documentos já processados ou em processamento nos fluxos alterados.

2.2.2.2. Controle de versões e do status do documento

2.2.2.2.1. Um recurso de fluxo de trabalho do SIGAD tem que ser capaz de registrar o status de transmissão do documento, ou seja, se é minuta, original ou cópia.

2.2.2.2.2. Ser capaz de controlar as diversas versões de um documento que está tramitando

2.2.2.2.3. Ser capaz de associar e relacionar as diversas versões de um documento.

2.2.2.2.4. Manter o identificador único do documento, e o controle de versões tem que ser registrado em metadados específicos.

2.2.3. Captura

2.2.3.1. Procedimentos gerais

2.2.3.1.1. A captura tem que garantir a execução das seguintes funções:

2.2.3.1.1.1. registrar e gerenciar todos os documentos convencionais;

2.2.3.1.1.2. registrar e gerenciar todos os documentos digitais, independentemente do contexto tecnológico;

2.2.3.1.1.3. classificar todos os documentos de acordo com o plano ou código de classificação;

2.2.3.1.1.4. controlar e validar a introdução de metadados.

2.2.3.1.2. Ser capaz de capturar documentos digitais das formas a seguir:

2.2.3.1.2.1. Captura de documentos produzidos dentro do SIGAD;

2.2.3.1.2.2. Captura de documento individual produzido em arquivo digital fora do SIGAD;

2.2.3.1.2.3. Captura de documento individual produzido em workflow ou em outros sistemas integrados ao SIGAD;

2.2.3.1.2.4. Captura de documentos em lote.

2.2.3.1.3. Aceitar o conteúdo do documento, bem como as informações que definem sua aparência, mantendo as associações entre os vários objetos digitais que compõem o documento, isto é, anexos e links de hipertexto.

2.2.3.1.4. Permitir a inserção de todos os metadados obrigatórios e opcionais definidos na sua configuração e garantir que se mantenham associados ao documento. Os metadados obrigatórios são:

- nome do arquivo digital;

- número identificador atribuído pelo sistema;

- data de produção;

- data e hora de transmissão e recebimento;

- data e hora da captura;

- título ou descrição abreviada;

- classificação de acordo com o plano ou código de classificação;

- prazos de guarda;

- autor (pessoa física ou jurídica);

- redator (se diferente do autor);

- originador;

- destinatário (e respectivo cargo);

- nome do setor responsável pela execução da ação contida no documento;

- indicação de anotação;

- indicação de anexos;

- indicação de versão;

- restrição de acesso;

- registro das migrações e data em que ocorreram

2.2.3.1.4.1. Os metadados opcionais se referem a informações mais detalhadas sobre o documento, tais como:

- espécie / tipo / gênero documental;

- associações a documentos diferentes que podem estar relacionados pelo fato de registrarem a mesma atividade ou se referirem à mesma pessoa ou situação;

- formato e software (nome e versão) em que o documento foi produzido ou capturado;

- máscaras de formatação (templates) necessárias para interpretar a estrutura do documento;

- assunto / descritor (diferentes do já estabelecido no código de classificação);

- localização física; e

- outros que se julgarem necessários.

2.2.3.1.5. Prever a inserção dos metadados obrigatórios, previstos em legislação específica na devida esfera e âmbito de competência, no momento da captura de processos.

2.2.3.1.6. Ser capaz de atribuir um número identificador a cada dossiê/processo e documento capturado, que serve para identificá-lo desde o momento da captura até sua destinação final no SIGAD.

2.2.3.1.7. O formato do número identificador atribuído pelo sistema deve ser definido no momento da configuração do SIGAD.

2.2.3.1.8. O número identificador atribuído pelo sistema tem que ser:

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

- atribuído pelo usuário e validado pelo sistema antes de ser aceito.

2.2.3.1.9. Prever a adoção da numeração única de processos e/ou documentos oficiais de acordo com a legislação específica a fim de garantir a integridade do número atribuído ao processo e/ou documento na unidade protocolizadora de origem.

2.2.3.1.10. Utilizar tesauro ou vocabulário controlado para apoiar a atribuição do metadado assunto/descritor.

2.2.3.1.11. Garantir que os metadados associados a um documento sejam inseridos somente por usuários autorizados.

2.2.3.1.12. Garantir que os metadados associados a um documento sejam alterados somente por administradores e usuários autorizados e devidamente registrados em trilhas de auditoria.

2.2.3.1.13. Ser capaz de inserir, automaticamente, os metadados previstos no sistema para o maior número possível de documentos, pois isso diminui as tarefas do usuário do sistema e garante maior rigor na inserção dos metadados

2.2.3.1.14. Garantir a visualização do registro de entrada do documento no sistema com todos os metadados inseridos automaticamente e os demais a serem atribuídos pelo usuário.

2.2.3.1.15. Garantir a inserção de outros metadados após a captura.

2.2.3.1.16. Sempre que um documento tiver mais de uma versão, o SIGAD tem que permitir que os usuários selecionem pelo menos uma das seguintes ações: - registrar todas as versões do documento como um só documento arquivístico; - registrar uma única versão do documento como um documento arquivístico; - registrar cada uma das versões do documento, separadamente, como um documento arquivístico.

2.2.3.1.17. Prestar assistência aos usuários no que diz respeito à classificação dos documentos, por meio de algumas ou de todas as ações a seguir: - tornar acessível ao usuário somente o subconjunto do plano de classificação que diz respeito à sua atividade; - indicar as últimas classificações feitas pelo usuário; indicar dossiês que contenham documentos de arquivo relacionados; - indicar classificações possíveis a partir dos metadados já inseridos, como, por exemplo, o título; - indicar classificações possíveis a partir do conteúdo do documento.

2.2.3.1.18. No caso de documentos ou dossiês/processos constituídos por mais de um objeto digital, o SIGAD tem que: - tratar o documento como uma unidade indivisível, assegurando a relação entre os objetos digitais; - preservar a integridade do documento, mantendo a relação entre os objetos digitais; - garantir a integridade do documento quando de sua recuperação, visualização e gestão posteriores; - gerenciar a destinação de todos os objetos digitais que compõem o documento como uma unidade indivisível.

2.2.3.1.19. Emitir um aviso caso o usuário tente registrar um documento que já tenha sido registrado no mesmo dossiê/processo.

2.2.3.2. Captura em lote

2.2.3.2.1. Um SIGAD tem que proporcionar a captura em lote de documentos gerados por outros sistemas. Esse procedimento tem que:

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

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

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

- validar a integridade dos metadados.

2.2.3.3. Captura de mensagens de correio eletrônico

2.2.3.3.1. Permitir que, na fase de configuração, seja escolhida uma das seguintes operações:

- capturar mensagens de correio eletrônico após selecionar quais serão objeto de registro; ou

- capturar, automaticamente, todas as mensagens de correio eletrônico.

2.2.3.3.2. Assegurar a captura do nome, e não somente do endereço, do originador do correio eletrônico. Por exemplo, “Luís Santos”, além de “lsa25@ab.br”.

2.2.3.4. Captura de documentos convencionais ou híbridos

2.2.3.4.1. Poder capturar também os documentos convencionais e/ou híbridos.

2.2.3.4.2. Acrescentar aos metadados dos documentos convencionais informações sobre sua localização.

2.2.3.5. Formato de arquivo e estrutura dos documentos a serem capturados

2.2.3.5.1. Possuir a capacidade de capturar documentos com diferentes formatos de arquivo e estruturas

2.2.3.5.2. Poder capturar, entre outros, os documentos a seguir:

- calendários eletrônicos;

- informações de outros aplicativos – contabilidade, folha de pagamento, desenho assistido por computador (CAD);

- documentos em papel digitalizados por meio de escâner;

- documentos sonoros;

- videoclipes;

- diagramas e mapas digitais;

- dados estruturados (EDI);

- bases de dados;

- documentos multimídia.

2.2.3.5.3. Capturar documentos que se apresentam com as seguintes estruturas:

- simples: texto, imagens, mensagens de correio eletrônico, slides digitais, som.

- composta: mensagens de correio eletrônico com anexos, páginas web, publicações eletrônicas, bases de dados.

2.2.3.5.4. Ser capaz de incluir novos formatos de arquivos à medida que forem sendo adotados pelo órgão ou entidade.

2.2.3.6. Estrutura dos procedimentos de gestão

2.2.3.6.1. Ser capaz de reconhecer três domínios para o controle dos procedimentos de gestão: espaço individual, espaço do grupo e espaço geral.

2.2.3.6.2. Ser capaz de operacionalizar as regras estabelecidas pelo sistema de gestão arquivística de documentos nos três espaços.

2.2.3.6.3. Impedir que o conteúdo de um documento seja alterado por usuários e administradores, exceto se a alteração fizer parte do processo documental.

2.2.3.6.4. Emitir um aviso caso se tente capturar um documento incompleto ou inconsistente a ponto de comprometer sua futura autenticidade.

2.2.4. Avaliação e destinação

2.2.4.1. Configuração da tabela de temporalidade e destinação de documentos

2.2.4.1.1. Prover funcionalidades para definição e manutenção de tabela de temporalidade e destinação de documentos, associada ao plano de classificação do órgão ou entidade

2.2.4.1.2. Associar, automaticamente, ao dossiê/processo o prazo e a destinação previstos na classe em que o documento foi inserido.

2.2.4.1.3. Manter tabela de temporalidade e destinação de documentos com as seguintes informações: - identificador do órgão ou entidade; - identificador da classe; - prazo de guarda na fase corrente; - prazo de guarda na fase intermediária; - destinação final; - observações; - evento que determina o início da contagem do prazo de retenção na fase corrente e na fase intermediária

2.2.4.1.4. Prever, pelo menos, as seguintes situações para destinação: - apresentação

dos documentos para reavaliação em data futura; - eliminação; - exportação para transferência; - exportação para recolhimento (guarda permanente)

2.2.4.1.5. Prever a iniciação automática da contagem dos prazos de guarda referenciados na tabela de temporalidade e destinação de documentos, pelo menos, a partir dos seguintes eventos: - abertura de dossiê; - arquivamento de dossiê/processo; - desarquivamento de dossiê/processo; - inclusão de documento em um dossiê/processo

2.2.4.1.6. Prever que a definição dos prazos de guarda seja expressa por: um número inteiro de dias ou um número inteiro de meses ou um número inteiro de anos ou uma combinação de um número inteiro de anos, meses e dias

2.2.4.1.7. Limitar a definição e a manutenção (alteração, inclusão e exclusão) da tabela de temporalidade e destinação de documentos a usuários autorizados

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

2.2.4.1.9. Ser capaz de manter o histórico das alterações realizadas na tabela de temporalidade e destinação de documentos

2.2.4.1.10. Prover funcionalidades para elaboração de relatórios que apóiem a gestão da tabela de temporalidade e destinação, incluindo a capacidade de:

- gerar relatório completo da tabela de temporalidade e destinação de documentos;

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

- gerar relatório dos documentos ou dossiês/processos aos quais foi atribuído um determinado prazo de guarda;

- identificar as inconsistências existentes entre a tabela de temporalidade e destinação de documentos e o plano de classificação.

2.2.4.2. Aplicação da tabela de temporalidade e destinação de documentos

2.2.4.2.1. Fornecer recursos integrados à tabela de temporalidade e destinação de documentos para implementar as ações de destinação.

2.2.4.2.2. Para cada dossiê/processo, um SIGAD tem que acompanhar automaticamente os prazos de guarda determinados para a classe à qual pertence

2.2.4.2.3. Prover funcionalidades para informar ao usuário autorizado sobre os documentos ou dossiês/processos que já cumpriram ou estão para cumprir o prazo de guarda previsto

2.2.4.2.4. Prover funcionalidades para gerenciar o processo de destinação, que tem de ser iniciado por usuário autorizado e cumprir os seguintes passos:

- identificar automaticamente os documentos ou dossiês/processos que atingiram os prazos de guarda previstos;

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

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

- proceder à ação de destinação quando confirmada pelo usuário autorizado.

2.2.4.2.5. Pedir confirmação antes de realizar as ações de destinação

2.2.4.2.6. Prever, em determinados casos, dispositivo de aviso antes do início de uma ação de destinação. Por exemplo, emitir aviso ao administrador, caso um documento arquivístico possua um determinado nível de segurança

2.2.4.2.7 Restringir as funções de destinação a usuários autorizado

2.2.4.2.8 Quando um administrador transfere documentos ou dossiês/processos de uma classe para outra, em virtude de uma reclassificação, o SIGAD tem que adotar automaticamente a temporalidade e a destinação vigentes na nova classe

2.2.4.2.9 Quando um documento digital (objeto digital) estiver associado a mais de um dossiê ou processo, e tiver prazos de guarda diferentes associados a ele, o SIGAD tem que automaticamente verificar todos os prazos de guarda e as destinações previstas para esse documento e garantir que ele seja mantido em cada dossiê/processo pelo tempo definido na tabela de temporalidade e destinação de documentos, de forma que:

- a remoção de um documento de um dossiê/processo não prejudique a manutenção desse mesmo documento em outro dossiê/processo, até que todas as referências desse documento tenham atingido o prazo de guarda previsto;

- a manutenção de um documento em um dossiê/processo por prazo mais longo não obrigue a permanência desse mesmo documento em outro dossiê/processo de prazo mais curto. Nesse caso o registro do documento com prazo mais curto tem que ser removido, mas o documento é mantido no SIGAD

2.2.4.3. Exportação de documentos

2.2.4.3.1. Ser capaz de exportar documentos e dossiês/processos digitais e seus metadados para outro sistema dentro ou fora do órgão ou entidade

2.2.4.3.2. Quando um SIGAD exportar os documentos e dossiês/processos de uma classe para executar uma ação de transferência ou recolhimento, tem que ser capaz de exportar todos os documentos e dossiês/processos da classe incluídos na ação de

destinação, com seus respectivos volumes, documentos e metadados associados

2.2.4.3.3. Ser capaz de exportar um documento e dossiê/processo ou grupo de documentos e dossiês/processos numa seqüência de operações, de modo que:

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

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

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

- todas as ligações entre documentos, volumes e dossiês/processos sejam mantidas.

2.2.4.3.4. Ser capaz de exportar dossiês/processos:

- em seu formato nativo (ou no formato para o qual foi migrado);

- de acordo com o formatos definidos em padrões de interoperabilidade;

- de acordo com o formato definido pela instituição arquivística que irá receber a documentação, no caso de transferência ou recolhimento.

2.2.4.3.5. Ser capaz de exportar metadados nos formatos previstos pelo padrão de interoperabilidade do governo

2.2.4.3.6. Ser capaz de exportar todos os tipos de documentos que está apto a capturar.

2.2.4.3.7. Produzir um relatório detalhado sobre qualquer falha que ocorra durante uma exportação. O relatório tem que identificar os documentos e dossiês/processos que originaram erros de processamento ou cuja exportação não tenha sido bem sucedida

2.2.4.3.8. Conservar todos os documentos e dossiês/processos digitais que foram exportados, pelo menos até que tenham sido importados no sistema destinatário com êxito

2.2.4.3.9. Manter metadados relativos a documentos e dossiês/processos que foram exportados

2.2.4.3.10. Gerar listagem em meio digital e em papel para descrever documentos e dossiês/processos digitais que estão sendo exportados

2.2.4.3.11. Possibilitar a inclusão de metadados necessários à gestão do arquivo permanente nos documentos e dossiês/processos que serão exportados para recolhimento

2.2.4.3.12. Quando se exportar documentos e dossiês/processos híbridos, um SIGAD deve exigir do usuário autorizado a confirmação de que a parte na forma convencional

dos mesmos documentos e dossiês/processos tenha passado pelo procedimento de destinação adequado antes de confirmar a exportação da parte na forma digital

2.2.4.3.13. Permitir que documentos sejam exportados mais de uma vez

2.2.4.4. Eliminação

2.2.4.4.1. Restringir a função de eliminação de documentos ou dossiês/processos somente a usuários autorizados

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

2.2.4.4.3. Avisar o usuário autorizado quando um documento ou dossiê/processo que estiver sendo eliminado se encontrar relacionado a outro; os sistemas também têm de suspender o processo até que seja tomada uma das medidas abaixo:

- confirmação pelo usuário autorizado para prosseguir ou cancelar o processo;

- produção de um relatório especificando os documentos ou dossiês/processos envolvidos e todas as ligações com outros documentos ou dossiês/processos

2.2.4.4.4. Permitir a eliminação de documentos ou dossiês/processos de forma irreversível a fim de que não possam ser restaurados por meio da utilização normal do SIGAD nem por meio de rotinas auxiliares do sistema operacional nem por aplicações especiais de recuperação de dados

2.2.4.4.5. Quando um documento tem várias referências armazenadas no sistema, um SIGAD tem que garantir que todas essas referências sejam verificadas antes de eliminar o objeto digital.

2.2.4.4.6. Produzir um relatório detalhando qualquer falha que ocorra durante uma eliminação. O relatório tem que identificar os documentos cuja eliminação não tenha sido bem sucedida.

2.2.4.4.7. Quando eliminar documentos ou dossiês/processos híbridos, um SIGAD deve exigir do usuário autorizado a confirmação de que a parte na forma convencional dos mesmos seja eliminada também antes de confirmar a eliminação da parte na forma digital.

2.2.4.4.8. Gerar relatório com os documentos e dossiês/processos que serão eliminados.

2.2.4.4.9. Manter metadados relativos a documentos e dossiês/processos eliminados.

2.2.4.5. Avaliação e destinação de documentos arquivísticos convencionais e híbridos

2.2.4.5.1. Aplicar a mesma tabela de temporalidade e destinação de documentos para os documentos convencionais, digitais ou híbridos.

2.2.4.5.2. Acompanhar os prazos de guarda dos documentos convencionais e deve dar início aos procedimentos de eliminação ou transferência desses documentos, tomando em consideração suas especificidades.

2.2.4.5.3. Alertar o administrador sobre a existência e a localização de uma parte convencional associada a um documento híbrido que esteja destinado a ser exportado, transferido ou eliminado.

2.2.4.5.4. Exportar metadados de documentos e dossiês/processos convencionais.

2.2.5. Pesquisa, localização e apresentação dos documentos

2.2.5.1. Aspectos gerais

2.2.5.1.1. Fornecer facilidades para pesquisa, localização e apresentação dos documentos

2.2.5.1.2. Prever a navegação gráfica no plano de classificação, a navegação direta de uma classe para os documentos arquivísticos produzidos nesta classe e a seleção, recuperação e apresentação direta dos documentos arquivísticos e de seus conteúdos por meio desse mecanismo

2.2.5.2. Pesquisa e localização

2.2.5.2.1. Fornecer uma série flexível de funções que atuem sobre os metadados relacionados com os diversos níveis de agregação (documento, unidade de arquivamento e classe) e sobre os conteúdos dos documentos arquivísticos por meio de parâmetros definidos pelo usuário, com o objetivo de localizar e acessar os documentos e/ou metadados, seja individualmente ou reunidos em grupo

2.2.5.2.2. Executar pesquisa de forma integrada, isto é, apresentar todos os documentos e dossiês/processos, sejam eles digitais, híbridos ou convencionais, que satisfaçam aos parâmetros da pesquisa

2.2.5.2.3. Permitir que todos os metadados de gestão de um documento ou dossiê/processo possam ser pesquisados

2.2.5.2.4. Permitir que um documento ou dossiê/processo possa ser recuperado por meio de um número identificador

2.2.5.2.5. Permitir que um documento ou dossiê/processo possa ser recuperado por meio de todas as formas de identificação implementadas, incluindo, no mínimo:

- identificador;

- título;

- assunto;

- datas;

- procedência/interessado;

- autor/redator /originador;

- classificação de acordo com plano ou código de classificação

2.2.5.2.6. Permitir que os termos utilizados na pesquisa possam ser qualificados, especificando-se um metadado ou o conteúdo do documento como fonte de busca

2.2.5.2.7. Permitir que os usuários refinem pesquisas já realizadas.

2.2.5.2.8. Quando o órgão ou entidade utilizar tesauros ou vocabulário controlado, um SIGAD deve ser capaz de realizar pesquisa dos documentos e dossiês/processos por meio da navegação nesses instrumentos

2.2.5.2.9. Permitir a pesquisa e recuperação de uma unidade de arquivamento completa e exibir a lista de todos os documentos que a compõem, como uma unidade e num único processo de recuperação.

2.2.5.2.10. Limitar o acesso a qualquer informação (metadado ou conteúdo de um documento arquivístico) se restrições de acesso e questões de segurança assim determinarem.

2.2.5.3. Apresentação: visualização, impressão, emissão de som

2.2.5.3.1. Apresentar o resultado da pesquisa como uma lista de documentos e dossiês/processos digitais, convencionais ou híbridos que cumpram os parâmetros da consulta e deve notificar o usuário se o resultado for nulo.

2.2.5.3.2. Após apresentar o resultado da pesquisa, um SIGAD tem que oferecer ao usuário as opções:

- visualizar os documentos e dossiês/processos resultantes da pesquisa;

- redefinir os parâmetros de pesquisa e fazer nova consulta.

2.2.5.3.3. Ser capaz de apresentar o conteúdo de todos os tipos de documentos arquivísticos digitais capturados, de forma que:

- preserve as características de exibição visual e de formato apresentados pela aplicação geradora;

- exiba todos os componentes do documento digital em conjunto, como uma unidade.

2.2.5.3.4. Ser capaz de exibir em tela todos os tipos de documentos capturados.

2.2.5.3.5. Ser capaz de imprimir os documentos capturados, preservando o formato produzido pelas aplicações geradoras.

2.2.5.3.6. Ser capaz de exibir/reproduzir o conteúdo de documentos que incluam imagem fixa, imagem em movimento e som.

2.2.5.3.7. Proporcionar ao usuário formas flexíveis de impressão de documentos com seus metadados e possibilitar a definição dos metadados a serem impressos.

2.2.5.3.8. Ser capaz de exibir em tela e imprimir todos os metadados associados aos documentos e dossiês/processos resultantes de uma pesquisa.

2.2.5.3.9. Permitir a impressão de uma lista dos documentos e dossiês/processos resultantes de uma pesquisa.

2.2.5.3.10. Permitir a impressão de uma lista dos documentos que compõem um dossiê/processo.

2.2.5.3.11. Permitir que todos os documentos de um dossiê/processo sejam impressos em uma única operação, na sequência determinada pelo usuário.

2.2.5.3.12. Incluir recursos destinados a transferir para suportes adequados documentos que não possam ser impressos, tais comodocumentos sonoros, vídeos e páginas web.

2.2.5.3.13. Ser capaz de realizar pesquisa e exibição de documentos e dossiês/processos, simultaneamente, para diversos usuários.

2.2.6. Segurança

2.2.6.1. Cópias de segurança

2.2.6.1.1. Permitir que, sob controle do seu administrador, mecanismos de backup criem cópias de todas as informações nele contidas (documentos arquivísticos, metadados e parâmetros do sistema)

2.2.6.1.2. O administrador do SIGAD tem que manter o controle das cópias de segurança, prevendo testes de restauração

2.2.6.1.3. Incluir funções para restituir os documentos de arquivo e metadados a um estado conhecido, utilizando uma combinação de cópias restauradas e rotinas de auditoria

2.2.6.2 Controle de acesso

2.2.6.2.1. Identificação e autenticação de usuários

2.2.6.2.1.1. Para implementar o controle de acesso, um SIGAD tem que manter pelo menos os seguintes atributos dos usuários, de acordo com a política de segurança:

- identificador do usuário;

- autorizações de acesso;

- credenciais de autenticação.

2.2.6.2.1.2. Exigir que o usuário esteja devidamente identificado e autenticado antes de iniciar qualquer operação no sistema.

2.2.6.2.1.3. Garantir que os valores dos atributos de segurança e controle de acesso, associados ao usuário, estejam dentro de conjuntos de valores válidos.

2.2.6.2.2. Aspectos gerais de controle de acesso

2.2.6.2.2.1. Permitir acesso a funções do sistema somente a usuários autorizados e sob controle rigoroso da administração do sistema, a fim de proteger a autenticidade dos documentos arquivísticos digitais.

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

2.2.6.2.3. Controle de acesso por grupos de usuários

2.2.6.2.3.1. Implementar a política de controle de acesso a documentos por grupos de usuários considerando:

- a identidade do usuário e sua participação em grupos;

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

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

2.2.6.2.3.3. Permitir que um usuário pertença a mais de um grupo

2.2.6.2.4. Controle de acesso por papéis de usuários

2.2.6.2.4.1. Usar os seguintes atributos do usuário ao implementar a política de controle de acesso aos documentos digitais por papéis de usuários:

- identificação do usuário;

- papéis associados ao usuário

2.2.6.2.4.2. Usar os seguintes atributos dos documentos digitais ao implementar a política de controle de acesso por papéis:

- identificação do documento digital;

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

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

2.2.6.2.4.4. Impedir que um usuário assuma papéis com direitos conflitantes.

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

2.2.6.3.1. Implementar a classificação de grau de sigilo de documentos, dossiês/processos e classes do plano de classificação, e de todas as operações de usuários nos documentos.

2.2.6.3.2. Implementar a classificação de grau de sigilo baseando-se nos seguintes atributos de segurança:

- grau de sigilo do documento;

- credencial de segurança do usuário.

2.2.6.3.3. Recusar o acesso de usuários a documentos que possuam grau de sigilo superior à sua credencial de segurança.

2.2.6.3.4. Garantir que documentos sem atribuição de grau de sigilo, importados a partir de fontes externas ao SIGAD, estejam sujeitos às políticas de controle de acesso e de sigilo.

2.2.6.3.5. Ser capaz de manter a marcação de sigilo original durante a importação de documentos a partir de fontes externas ao SIGAD.

2.2.6.3.6. Permitir que um dos itens abaixo seja selecionado durante a configuração:

- graus de sigilo a serem atribuídos a classes e dossiês/processos;

- classes e dossiês/processos sem grau de sigilo.

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

2.2.6.3.8. Garantir que o grau de sigilo de um documento importado esteja associado a um usuário autorizado com a credencial de segurança pertinente para receber o documento.

2.2.6.3.9. Permitir somente aos administradores autorizados a possibilidade de alterar a configuração dos valores predefinidos (default) para os atributos de segurança e marcação de graus de sigilo, quando necessário e apropriado.

2.2.6.3.10. Somente administradores autorizados têm que ser capazes de realizar as seguintes ações: remover ou revogar os atributos de segurança dos documentos; criar, alterar, remover ou revogar as credenciais de segurança dos usuários.

2.2.6.3.11. Permitir somente ao usuário autorizado, mediante confirmação, a desclassificação ou redução do grau de sigilo de um documento

2.2.6.3.12. Impedir que um documento sigiloso seja eliminado

2.2.6.3.13. Implementar metadados nos níveis de dossiê, documento ou extrato de documento para controlar o acesso à informação sensível.

2.2.6.4. Trilhas de auditoria

2.2.6.4.1. Ser capaz de registrar, na trilha de auditoria, informações acerca das ações a seguir:

- data e hora da captura de todos os documentos;

- responsável pela captura;

- reclassificação, desclassificação ou redução do grau de sigilo de um documento ou dossiê/processo, com a classificação inicial e final.

- qualquer alteração na tabela de temporalidade e destinação de documentos;

- qualquer ação de reavaliação de documentos;

- qualquer alteração nos metadados associados a classes, dossiês/processos ou documentos;

- data e hora de produção, aditamento e eliminação de metadados;

- alterações efetuadas nas permissões de acesso que afetem um dossiê/processo, documento ou usuário;

- ações de exportação e importação envolvendo os documentos;

- tentativas de exportação (inclusive para backup) e importação (inclusive restore);

- usuário, data e hora de acesso ou tentativa de acesso a documentos e ao SIGAD;

- tentativas de acesso negado a qualquer documento;

- ações de eliminação de qualquer documento e seus metadados;

- infrações cometidas contra mecanismos de controle de acesso;

- mudanças no relógio gerador de carimbos de tempo;

- todas as ações administrativas sobre os atributos de segurança (papéis, grupos, permissões etc.);

- todas as ações administrativas sobre dados de usuários (cadastro, ativação, bloqueio, atualização de dados e permissões, troca de senha etc.);

- todos os eventos de administração e manutenção das trilhas de auditoria (alarmes, cópias, configuração de parâmetros etc.).

2.2.6.4.2. Registrar, em cada evento auditado, informações sobre a identidade do usuário, desde que essa identificação esteja de acordo com a política de privacidade da organização e a legislação vigente.

2.2.6.4.3. Permitir apenas ao administrador e ao auditor a leitura das trilhas de auditoria.

2.2.6.4.4. Assegurar que as informações da trilha de auditoria estejam disponíveis para inspeção, a fim de que uma ocorrência específica possa ser identificada e todas as informações correspondentes sejam claras e compreensíveis.

2.2.6.4.5. Possuir mecanismos para realização de buscas nos eventos das trilhas de auditoria.

2.2.6.4.6. Ser capaz de impedir qualquer modificação na trilha de auditoria.

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

2.2.6.4.8. Fornecer relatórios sobre as ações que afetam classes, unidades de arquivamento e documentos, em ordem cronológica e organizados por:

- documento arquivístico, unidade de arquivamento ou classe;

- usuário;

- tipo de ação ou operação.

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

2.2.6.4.10. Somente administradores autorizados, acompanhados do auditor, têm que ser capazes de configurar o conjunto de eventos auditáveis e seus atributos.

2.2.6.5. Assinaturas digitais

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

2.2.6.5.2. Ser capaz de verificar a validade da assinatura digital no momento da captura do documento.

2.2.6.5.3. No processo de verificação da assinatura digital, tem que ser capaz de registrar, nos metadados do documento, o seguinte:

- validade da assinatura verificada;

- registro da verificação da assinatura;

- data e hora em que ocorreu a verificação.

2.2.6.6. Criptografia

2.2.6.6.1. Usar criptografia no armazenamento, na transmissão e na apresentação de documentos arquivísticos digitais ao implementar a política de sigilo

2.2.6.6.2. Limitar o acesso aos documentos cifrados somente àqueles usuários portadores da chave de decifração

2.2.6.6.3. Registrar os seguintes metadados sobre um documento cifrado:

- indicação sobre se está cifrado ou não;

- algoritmos usados na cifração;

- identificação do remetente;

- identificação do destinatário.

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

- incluir, remover ou alterar parâmetros dos algoritmos criptográficos instalados no SIGAD;

- incluir, remover ou substituir chaves criptográficas de programas ou usuários do SIGAD;

- cifrar e alterar a criptografia de documentos;

- remover a criptografia de um documento.

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

- data e hora da remoção da cifração;

- identificação do executor da operação;

- motivo da remoção da cifração.

2.2.6.7. Marcas d'água digitais

2.2.6.7.1. Ser capaz de recuperar informação contida em marcas d'água digitais.

2.2.6.7.2. Ser capaz de armazenar documentos arquivísticos digitais que contenham marcas d'água digitais, assim como informação de apoio relacionada à marca d'água.

2.2.6.8 Acompanhamento de transferência

2.2.6.8.1 Fornecer um recurso de acompanhamento para monitorar e registrar informações acerca do local atual e da transferência de dossiês/processos digitais e convencionais.

2.2.6.8.2 A função de acompanhamento de transferência tem que registrar metadados que incluam:

- número identificador dos documentos atribuído pelo sistema;

- localização atual e localizações anteriores, definidas pelo usuário;

- data e hora de envio/transferência; - data e hora da recepção no novo local;

- destinatário;

- usuário responsável pela transferência (sempre que for adequado);

- método de transferência.

2.2.6.9. Autoproteção

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

2.2.6.9.2. Garantir que as funções de controle de acesso sejam invocadas antes de qualquer operação de acesso e retornem sem erros antes do prosseguimento da operação.

2.2.6.9.3. Preservar um estado seguro de funcionamento, interrompendo completamente a interação com usuários comuns, quando ocorrer um dos erros a seguir: falha de comunicação entre cliente e servidor; perda de integridade das informações de controle de acesso; falta de espaço para registro nas trilhas de auditoria.

2.2.6.10. Alterar, apagar e truncar documentos arquivísticos digitais

2.2.6.10.1. Permitir, a um administrador autorizado, anular a operação em caso de erro do usuário ou do sistema

2.2.6.10.2. Em situações excepcionais, o administrador tem que ser autorizado a apagar ou corrigir dossiês/processos, volumes e documentos. Nesse caso, um SIGAD tem que:

- registrar integralmente a ação de apagar ou corrigir na trilha de auditoria;

- produzir um relatório de anomalias para o administrador;

- eliminar todo o conteúdo de um dossiê/processo ou volume, quando forem eliminados;

- garantir que nenhum documento seja eliminado se tal ação resultar na alteração de outro documento arquivístico;

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

- manter a integridade total do metadado, a qualquer momento.

2.2.6.10.3. Em caso de erro na inserção de metadados, o administrador terá que corrigi-lo, e o SIGAD tem que registrar essa ação na trilha de auditoria

2.2.6.10.4. Permitir a um usuário autorizado fazer um extrato (cópia truncada) de um documento, com o objetivo de não alterar o original.

2.2.6.10.5. Possibilitar a ocultação de informação sigilosa contida na cópia truncada do documento, permitindo:

- retirada de páginas de um documento;

- adição de retângulos opacos para ocultar nomes ou palavras sensíveis;

- quaisquer outros recursos necessários para formatos de vídeo ou áudio, caso existam. Se o SIGAD não fornecer, diretamente, esses recursos, tem que permitir que outros pacotes de software os proporcionem

2.2.6.10.6. Quando uma cópia truncada é produzida, um SIGAD tem que registrar essa ação nos metadados do documento, incluindo, pelo menos, data, hora, motivo e quem a

produziu.

2.2.6.10.7. Registrar uma referência cruzada a uma cópia truncada nos mesmos dossiês/processos, pastas e documentos em que se encontra o documento original.

2.2.6.10.8. Armazenar, na trilha de auditoria, qualquer alteração efetuada para satisfazer os requisitos desta seção.

2.2.7. Armazenamento

2.2.7.1. Durabilidade

2.2.7.1.1.Utilizar, preferencialmente, dispositivos e padrões de armazenamento maduros, estáveis no mercado e amplamente disponíveis.

2.2.7.1.2. A escolha de dispositivos tem que ser revista sempre que a evolução tecnológica indicar mudanças importantes.

2.2.7.1.3. Atividades de migração têm que ser efetivadas, preventivamente, sempre que se torne patente ou previsível a obsolescência do padrão corrente

2.2.7.1.4. Para as memórias secundárias, um SIGAD tem que manter registro de MTBF (mean time between failure), bem como suas datas de aquisição

2.2.7.1.5. Para as memórias secundárias e terciárias, o SIGAD tem que fazer o gerenciamento das mídias por meio do registro de durabilidade prevista, data de aquisição e histórico de utilização.

2.2.7.1.6. Quando se proceder à eliminação de documentos, as memórias de suporte têm que ser, devidamente, “sanitizadas”, isto é, ter suas informações, efetivamente, indisponibilizadas.

2.2.7.2. Capacidade

2.2.7.2.1. Possuir capacidade de armazenamento suficiente para acomodação de todos os documentos e suas cópias de segurança.

2.2.7.2.2. Ser prevista a possibilidade de expansão da estrutura de armazenamento.

2.2.7.3 Efetividade de armazenamento.

2.2.7.3.1. Utilizar técnicas de restauração de dados em caso de falhas.

2.2.7.3.2. Utilizar mecanismos de proteção contra escrita, que previnam alterações indevidas e mantenham a integridade dos dados armazenados.

2.2.7.3.3. A integridade dos dispositivos de armazenamento tem que ser, periodicamente, verificada.

2.2.8 Preservação

2.2.8.1. Aspectos físicos

2.2.8.1.1. Os suportes de armazenamento do SIGAD têm que ser acondicionados, manipulados e utilizados em condições ambientais compatíveis com sua vida útil prevista
e/ou pretendida, de acordo com as especificações técnicas do fabricante e de entidades isentas, e com base em estatísticas de uso.

2.2.8.1.2. Permitir o controle da vida útil dos suportes para auxiliar no processo de atualização.

2.2.8.2 Aspectos lógicos

2.2.8.2.1. Manter cópias de segurança.

2.2.8.2.2. Possuir funcionalidades para verificação periódica dos dados armazenados, visando à detecção de possíveis erros.

2.2.8.2.3. Permitir a substituição dos dados armazenados que apresentarem erros.

2.2.8.2.4. Ações de preservação têm que ser efetivadas sempre que se torne patente ou previsível a obsolescência da tecnologia utilizada pelo SIGAD.

2.2.8.2.5. Suportar a transferência em bloco de documentos (incluindo as demais informações associadas a cada documento) para outros suportes e/ou sistemas, de acordo com as normas aplicáveis aos formatos utilizados.

2.2.8.3. Aspectos gerais

2.2.8.3.1. Registrar, em trilhas de auditoria, as operações de preservação realizadas.

2.2.8.3.2. As modificações no SIGAD e em sua base tecnológica têm que ser verificadas num ambiente exclusivo para essa finalidade, de modo a garantir que, após a implantação das alterações, os dados continuem sendo acessados sem alteração de conteúdo

2.2.8.3.3. Gerir metadados relativos à preservação dos documentos e seus respectivos componentes

2.2.9. Funções administrativas

2.2.9.1. Permitir que os administradores, de maneira controlada e sem esforço excessivo, recuperem, visualizem e reconfigurem os parâmetros do sistema e os atributos dos usuários.

2.2.9.2. Fornecer relatórios flexíveis para que o administrador possa gerenciar os documentos e seu uso. Esses relatórios devem apresentar, no mínimo:

- quantidade de dossiês/processos, volumes e itens a partir de parâmetros ou atributos definidos (tempo, classe, unidade administrativa etc.);

- estatísticas de transações relativas a dossiês/processos, volumes e itens;

- atividades por usuário.

2.2.9.3. Dispor de documentação referente a aspectos de administração do sistema. A documentação deve incluir todas as informações necessárias para o correto gerenciamento do sistema.

2.2.10. Conformidade com a legislação e regulamentações

2.2.10.1. Estar de acordo com a legislação e as normas pertinentes, tendo em vista a admissibilidade legal e o valor probatório dos documentos arquivísticos.

2.2.10.2. Estar de acordo com a legislação e as normas específicas para gestão e acesso de documentos arquivísticos.

2.2.10.3. Estar em conformidade com requisitos regulamentares específicos e códigos de boa prática necessários para a execução de determinadas atividades.

2.2.11. Usabilidade

2.2.11.1. Possuir documentação completa, clara, inteligível e organizada para instalação e uso do software.

2.2.11.2. Possuir sistema de ajuda on-line.

2.2.11.3. Toda mensagem de erro produzida pelo SIGAD deve ser clara e significativa, de modo a permitir que o usuário se recupere do erro ou cancele a operação.

2.2.11.4. Empregar um conjunto simples e consistente de regras de interface, privilegiando a facilidade de aprendizado das operações pelos seus usuários.

2.2.11.5. O usuário deve poder personalizar a interface gráfica do SIGAD. A personalização deve incluir, pelo menos, as seguintes possibilidades:

- conteúdo de menus;

- formatos de tela;

- utilização de teclas de função;

- alteração de cor, fonte e tamanho de letra em telas e janelas;

- avisos sonoros

2.2.11 6. Sempre que o SIGAD utilizar janelas pop-up e barras de ferramentas, deve-se oferecer ao usuário a possibilidade de configurar e habilitar/desabilitar esse tipo de recurso.

2.2.11.7. Permitir a gravação de opções default para entrada de dados de configuração, como:

- valores de variáveis definidas pelo usuário;

- valores iguais aos de um item anterior;

- valores que possam ser selecionados em uma lista configurável;

- valores derivados do contexto, como data, referência do dossiê/processo, identificador do usuário;

- valores predefinidos por um administrador (para campos de metadados como, por exemplo, o nome da organização que está utilizando o sistema).

2.2.11.8. A interface do SIGAD com o usuário deve ser adequada a adaptações e personalizações que permitam sua utilização por usuários com necessidades especiais. Essas opções devem ser compatíveis com software especializado que possa vir a ser acoplado (por exemplo, leitores de tela para cegos), bem como seguir orientações específicas de acessibilidade de interface

2.2.11.9. Permitir a realização de transações ou tarefas mais frequentemente executadas com um pequeno número de interações (por exemplo, cliques de mouse) e sem mudanças excessivas de contexto

2.2.11.10. Estar fortemente integrado ao sistema de correio eletrônico da organização, de forma a permitir a geração de mensagens com possibilidade de manipular documentos digitais, sem necessidade de sair do SIGAD

2.2.11.11. Em caso de integração do SIGAD com o sistema de correio eletrônico, deve ser possível fazer referências a documentos arquivísticos sem necessidade de envio de cópias adicionais.

2.2.11.12. Estar integrado com o sistema padrão de edição de documentos, de modo que possa fazer uso da facilidade de gravação.

2.2.11.13. Permitir a definição e utilização de referências cruzadas entre documentos arquivísticos digitais correlacionados, bem como a fácil navegação entre eles, inclusive com o uso de hyperlinks.

2.2.11.14. Disponibilizar pelo menos dois papéis de acesso diferenciados, um para usuário final e outro para administrador de sistema.

2.2.11.15. Fornecer a usuários finais e administradores funções intuitivas e fáceis de usar, que requeiram poucas ações para completar uma tarefa padrão. Sobretudo

durante sua operação normal, o SIGAD deve ser capaz de:

- capturar e declarar um documento arquivístico com no máximo três cliques de mouse ou acionamentos de tecla;

- apresentar todos os elementos de metadados obrigatórios para a captura do documento com mínima demanda para o usuário;

- apresentar o conteúdo de um documento arquivístico, a partir de uma lista de pesquisa, com no máximo três cliques de mouse ou acionamentos de tecla;

- apresentar os metadados de um documento arquivístico com no máximo três cliques de mouse ou acionamentos de tecla.

2.2.11.16. Restringir o acesso às funcionalidades administrativas e impossibilitar sua visualização pelo usuário final.

2.2.12. Interoperabilidade

2.2.12.1. Ser capaz de interoperar com outros SIGAD, permitindo, pelo menos, consulta, recuperação, importação e exportação de documentos e seus metadados.

2.2.12.2. Ser capaz de interoperar com outros sistemas por meio de padrões abertos de interoperabilidade

2.2.12.3. Aplicar os requisitos de segurança descritos neste documento para executar operações de interoperabilidade

2.2.13. Disponibilidade

2.2.13.1. Adequar ao grau de disponibilidade estabelecido pela organização

2.2.14. Desempenho e escalabilidade

2.2.14.1. Ser expansível até comportar um número máximo, preestabelecido, de usuários simultâneos, provendo a continuidade efetiva dos serviços.

2.2.14.2. Incluir rotina de manutenção de:

- dados de usuários e de grupos;

- perfis de acesso;

- plano de classificação;

- bases de dados;

- tabelas de temporalidade.

2.2.14.3. Ser escalável, a fim de permitir adaptação a organizações de diferentes tamanhos e complexidades.

2.2.14.4. Fornecer evidências do grau de escalabilidade ao longo do tempo. Avaliações quantitativas devem incluir:

- número máximo de sítios remotos suportados com desempenho adequado;

- tamanho máximo do repositório, expresso em gigabytes ou terabytes, que pode ser suportado com desempenho adequado;

- o número máximo de usuários simultâneos que podem ser atendidos com desempenho adequado;

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

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

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

2.2.15. Arquitetura

2.2.15.1. Ter todas as tabelas armazenadas no Banco de dados Postgre SQL.

2.2.15.2. Poder ser utilizado em todas as suas funcionalidades por meio de navegadores (browsers).

2.2.15.3. Ser capaz de se integrar aos sistemas legado por meio de serviços REST - Representational State Transfer.

2.2.15.4. Ser capaz de executar em ambiente de nuvem nas plataformas, Dotnet-core, nginx (frontend web), Golang (com fontes), Java, Node, PHP, Python, Ruby, Tomcat ou Wildfly.

2.2.15.5. Ser capaz de executar em ambiente de nuvem com até 2GB de RAM.

2.2.15.6. Ser capaz de armazenar arquivos em storage ceph (https://www.redhat.com /pt-br/technologies/storage/ceph).

2.2.15.7. Ser capaz de implementar o protocolo Objeto/S3 (Preferencialmente) - https://aws.amazon.com/pt/s3/.

2.2.15.8. Ter aquitetura Stateless, com escalabilidade horizontal.

2.2.15.9. Ser capaz de gravar log em saída padrão.

2.2.15.10. Possuir requisições de entrada sobre http/s (ex: API REST).

2.2.15.11. Possuir Requisição de saída por egress (intranet) ou proxy autenticado (internet).

2.2.15.12. Possuir Endpoint de healthcheck.

2.2.15.13. Possuir Endpoint de métricas.

2.2.15.14. Estar aderente a norma SERPRO SG030 (Ver anexo).

3.0 Níveis de serviço e sancionamentos

N/A.

4.0 Especificação de valores e forma de pagamento

N/A.

5.0 Justificativa da contratação

5.1. Esta Consulta Pública está autorizada pelo Diretor da DIJUG por meio do SISCOR SUPOG 031406/2019-08 (cópia em anexo).

5.2. A Consulta Pública tem como objetivo validar junto ao mercado os requisitos necessários para contratação de empresa especializada.

5.3. A digitalização de documentos faz parte da transformação digital do SERPRO. ela está alinhada à transformação digital do Governo Federal. a aquisição de um sistema informatizado de gestão arquivística de documentos (SIGAD) irá acelerar a digitalização da primeira esteira, que trata da substituição de formulários em papel ou eletrônicos sem fluxo e sem cumprimento de exigências legais.

5.3.1. O SIGAD será de uso corporativo e promoverá segurança jurídica para a gestão documental - integração em única base de dados, eficácia na captura, recuperação, preservação e destinação (eliminação ou guarda permanente) dos documentos da empresa.

5.4. Necessidade da contratação

5.4.1. O SERPRO necessita proteger o seu patrimônio documental a fim de manter o seu caráter de prova, informação, memória e garantir o rastreamento dos documentos arquivísticos produzidos e recebidos ao longo do tempo.

5.4.2. O SERPRO deve estar em conformidade com a legislação arquivística e, em especial, ao e-ARQ Brasil.

5.4.3. A preservação e a admissibilidade jurídica dos documentos arquivísticos

produzidos e recebidos devem ser garantidos pelo SERPRO ao longo do tempo.

5.4.4. O controle, a confiabilidade, a preservação e o acesso a documentos arquivísticos digitais devem estar presentes no SIGAD.

6.0 Seleção do fornecedor

6.1. Consulta pública com fulcro no Art. 31, da Lei n° 9.784/1999, objetivando esclarecimentos sobre produtos, processos, soluções e tecnologias junto ao mercado.

7.0 Justificativa para aceitação de preços

N/A.

8.0 Gerenciamento contratual

8.1. A Consulta Pública Eletrônica será acompanhada pelos empregados:

8.1.1. Rogério Yoshikazu Matsuda, matrícula 21098956, lotado na DIOPE/SUPEC /ECTAN/ECTPB, Telefone: (61) 2021-8533, e-mail: rogerio.matsuda@serpro.gov.br.

8.1.2. Denys Alves Carneiro, matrícula 21103909, DIOPE/SUPEC/ECTAN/ECTPB, Telefone: (61) 2021-8649, e-mail: denys.carneiro@serpro.gov.br.

8.2. As empresas deverão encaminhar as sugestões de alterações da especificação desta consulta pública.

9.0 Considerações gerais

N/A.

Elaboração

Data : 24/01/2020
ROGERIO YOSHIKAZU MATSUDA - 21098956
SUPEC/ECTAN/ECTPB

Anexos

Arquivo: Pedido Autorização SISCOR
Arquivo: Resposta Autorização SISCOR