MINISTÉRIO DA DEFESA
COMANDO DA AERONÁUTICA

RTLI 03/SDTE

REQUISITOS TÉCNICOS, LOGÍSTICOS E INDUSTRIAIS PARA SISTEMA DE GERENCIAMENTO DE PROCESSOS DE NEGÓCIO INTEGRADO À BASE DE DADOS GEOESPACIAIS PARA AS ÁREAS DE AERÓDROMOS (AGA) E DE CARTOGRAFIA AERONÁUTICA (CAR)

2015

MINISTÉRIO DA DEFESA
COMANDO DA AERONÁUTICA
DEPARTAMENTO DE CONTROLE DO ESPAÇO AÉREO

RTLI 03/SDTE

REQUISITOS TÉCNICOS, LOGÍSTICOS E INDUSTRIAIS PARA SISTEMA DE GERENCIAMENTO DE PROCESSOS DE NEGÓCIO INTEGRADO À BASE DE DADOS GEOESPACIAIS PARA AS ÁREAS DE AERÓDROMOS (AGA) E DE CARTOGRAFIA AERONÁUTICA (CAR)

2015

MINISTÉRIO DA DEFESA
COMANDO DA AERONÁUTICA
DEPARTAMENTO DE CONTROLE DO ESPAÇO AÉREO

PORTARIA DECEA Nº 02/SDTE, DE 11 DE DEZEMBRO DE 2015.

Aprova a edição dos Requisitos Técnicos, Logísticos e Industriais para Sistema de Gerenciamento de Processos de Negócio Integrado à Base de Dados Geoespaciais para as áreas de Aeródromos (AGA) e de Cartografia Aeronáutica (CAR).

O CHEFE DO SUBDEPARTAMENTO TÉCNICO DO DEPARTAMENTO DE CONTROLE DO ESPAÇO AÉREO, no uso das atribuições que lhe confere o art. 1º, inciso II, alínea "g", da Portaria DECEA nº 1-T/DGCEA, de 2 de janeiro de 2015, resolve:

Art. 1º Aprovar a edição dos RTLI 03/SDTE/2015 "Requisitos Técnicos, Logísticos e Industriais para Sistema de Gerenciamento de Processos de Negócio Integrado à Base de Dados Geoespaciais para as áreas de Aeródromos (AGA) e de Cartografia Aeronáutica (CAR)".

Art. 2º Revogar a Portaria DECEA nº 11/SDTE, de 03 de dezembro de 2013, publicada em Boletim Interno nº 252, de 30 de dezembro de 2013.

Art. 3º Esta Portaria entra em vigor na data de sua publicação.

(a)Brig Eng FERNANDO CESAR PEREIRA SANTOS
Chefe do Subdepartamento Técnico do DECEA

(Publicado no Boletim Interno do DECEA nº 245 , de 23 de dezembro 2015).

SUMÁRIO

1 DISPOSIÇÕES PRELIMINARES

1.1 FINALIDADE

Definir os Requisitos Técnicos, Logísticos e Industriais (RTLI) para o Sistema de Gerenciamento de Processos de Negócio Integrado à Base de Dados Geoespaciais para as áreas de Aeródromos (AGA) e de Cartografia Aeronáutica (CAR), tendo em vista a Necessidade Operacional (NOP) nº 01/SDOP/2015, de 28/04/2015, encaminhada pela Parte nº 6/D-PLN4, de 26 de maio de 2015, em substituição à 07/SDOP/2013, de 5 de setembro de 2013, encaminhada pela Parte nº 11/D-PLN5, de 16 de setembro de 2013.

Esta RTLI substitui a RTLI nº 07/SDTE/2013, de 3 de dezembro de 2013. Assim, esta norma visa complementar as informações apresentadas na NOP 01/SDOP/2015, de 28/04/2015. Ou seja, os requisitos do sistema para aquisição e implantação são compostos pela NOP e por esta RTLI.

1.2 ÂMBITO

O sistema de que trata este RTLI deverá ser utilizado pelo DECEA, Órgãos do COMAER e usuários externos. O usuário externo é a pessoa jurídica ou física que utiliza o sistema para submeter processos da área de aeródromos à análise do COMAER e órgãos públicos externos ao COMAER (ex.: ANAC).

1.3 ABREVIATURAS

AAL	· Administração Aeroportuária Local
ABNT NBR ISO/IEC 27002:2005	· Norma que estabelece diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão de segurança da informação em uma organização
ABNT NBR ISO/IEC 9241-11:2002	· Norma que estabelece requisitos ergonômicos entre os quais se encontra orientações sobre usablilidade.
BPMN	· *Business Process Modeling Notation* (Notação de Modelagem de Processos de Negócio)
CAPTCHA	· *Completely Automated Public Turing Test to Tell Computers and Humans Apart* (Teste de Turing público completamente automatizado para diferenciação entre computadores e humanos)
COMAER	· Comando da Aeronáutica
DCA 66-1	· Diretriz do Comando da Aeronáutica sobre Atividade de Manutenção no Sistema de Controle do Espaço Aéreo
DECEA	· Departamento de Controle do Espaço Aéreo
ICA 400-31/2010	· Instrução do Comando da Aeronáutica sobre Gerenciamento do Ciclo de Vida de Sistemas e Materiais do SISCEAB
INTERNET	· Rede mundial interligada de computadores
INTRANET	· Rede da aeronáutica interligada de computadores
OPSTI	· Organização Provedora de Serviços de Tecnologia da Informação
OWASP	· *Open Web Application Security Project*

PDF	- *Portable Document Format* (Formato de Documento Portátil)
RTLI	- Requisitos Técnicos, Logísticos e Industriais
SAT	- *Site Acceptance Test* (Teste de Aceitação em Sítio)
SDTE	- Subdepartamento Técnico do DECEA
SGBD	- Sistema de Gerenciamento de Banco de Dados
SILOMS	- Sistema Integrado de Logística de Material e de Serviços da Aeronáutica
SISCEAB	- Sistema de Controle do Espaço Aéreo Brasileiro
SMTP	- *Simple Mail Transfer Protocol* (Protocolo de Transferência de Correio Simples)
TCP/IP	- *Transmission Control Protocol/Internet Protocol* (conjunto de protocolos de comunicação entre computadores em rede)

2 GENERALIDADES

2.1 CONCEITUAÇÃO

2.1.1 ARQUITETURA CLIENTE-SERVIDOR DE TRÊS CAMADAS

A arquitetura de três camadas possui uma camada intermediária entre o cliente e o servidor de banco de dados. Essa camada intermediária é conhecida por servidor de aplicações ou servidor *Web*, dependendo da aplicação. Esse servidor desempenha um papel intermediário armazenando as regras de negócio (procedimentos ou restrições) que são usadas para acessar os dados do servidor de banco de dados. Também pode incrementar a segurança do banco de dados verificando as credenciais do cliente antes de enviar uma solicitação ao servidor de banco de dados. Os clientes possuem interfaces gráfica e algumas regras de negócio adicionais específicas para a aplicação. O servidor intermediário recebe as solicitações do cliente, processa-as e envia comandos ao servidor de banco de dados, e então atua conduzindo (parcialmente) os dados processados do servidor de banco de dados para os clientes – dados que podem ser processados novamente e filtrados para a apresentação aos usuários em um formato gráfico. Desse modo, a interface com o usuário, as regras de aplicação e o acesso aos dados atuam como três camadas. (Elmasri e Navathe, 2005)

2.1.2 *BACKUP*

Cópias de Segurança de Arquivos. (ABNT NBR ISO/IEC 27002).

2.1.3 CONFIABILIDADE

Uma medida de tempo em que um serviço de TI ou outro item de configuração pode executar a sua função acordada sem interrupção. Geralmente medida como MTBF e MTBSI. O termo também pode ser usado para afirmar a possibilidade de que um processo, função etc. irá entregar os resultados requeridos. (ITIL®, 2011)

2.1.4 CONFIGURAÇÃO

Um termo genérico, usado para descrever um grupo de itens de configuração que trabalham em conjunto para fornecer um serviço de TI, ou uma parte identificável de um serviço de TI. Configuração também é usada para descrever as definições de parâmetros para um ou mais itens de configuração. (ITIL®, 2011)

2.1.5 CONJUNTO

É uma reunião de dois ou mais itens com a finalidade de executar uma função específica.

2.1.6 DESEJÁVEL

Para efeito deste documento, o termo “DESEJÁVEL” refere-se a requisitos desejáveis para o melhor atendimento à necessidade identificada.

2.1.7 DESEMPENHO

Uma medida do que foi alcançado ou executado por um sistema, uma pessoa, equipe ou processo ou serviço de TI. (ITIL®, 2011)

2.1.8 DEVE

Para efeito deste documento, o termo "DEVE" e suas conjugações referem-se aos requisitos mandatórios.

2.1.9 DISPONIBILIDADE

Habilidade de um serviço de TI ou outro item de configuração de desempenhar a sua habilidade acordada quando requerido. A disponibilidade é determinada pela confiabilidade, sustentabilidade, funcionalidade do serviço, desempenho e segurança. A disponibilidade é normalmente calculada em percentagens. Tal cálculo frequentemente se baseia no tempo de serviço acordado e na indisponibilidade. A melhor prática para calcular a disponibilidade de um serviço de TI é medir pela perspectiva do negócio. (ITIL®, 2011)

2.1.10 *FIREWALL*

Sistema ou combinação de sistemas que protege a fronteira entre duas ou mais redes. (ABNT NBR ISO/IEC 27002:2005)

2.1.11 EQUIPAMENTO

Material constituído de componentes, formando uma unidade e seus conjuntos, subconjuntos e peças, conectadas ou usadas em associação para executar uma função operacional.

2.1.12 EVENTO

Uma mudança de estado a qual possui significado para o gerenciamento de um item de configuração ou serviço. (ITIL®, 2011)

2.1.13 ICP-BRASIL

A Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil) é uma cadeia hierárquica e de confiança que viabiliza a emissão de certificados digitais para identificação virtual do cidadão. Observa-se que o modelo adotado pelo Brasil foi o de certificação com raiz única, sendo que o ITI (Instituto Nacional de Tecnologia da Informação), além de desempenhar o papel de Autoridade Certificadora Raiz (AC-Raiz), também tem o papel de credenciar e descredenciar os demais participantes da cadeia, supervisionar e fazer auditoria dos processos. (Instituto Nacional de Tecnologia da Informação, *site* visto em 16 outubro 2013 http://www.iti.gov.br/index.php/icp-brasil/o-que-e).

2.1.14 INTEGRIDADE

Um princípio de segurança que garante que dados e itens de configuração somente sejam modificados por pessoas e atividades autorizadas. A integridade considera todas as possíveis causas de modificação, incluindo falhas de *hardware* e *software*, eventos ambientais e intervenção humana. (ITIL®, 2011)

2.1.15 ITEM DE CONFIGURAÇÃO

Qualquer componente ou outro ativo de serviço que precise ser gerenciado de forma a entregar um serviço de TI. As informações sobre cada item de configuração são registradas em um registro de configuração no sistema de gerenciamento de configuração e é mantido por todo o seu ciclo de vida pelo gerenciamento de configuração e ativo de serviço. Os itens de configuração estão sob o controle do gerenciamento de mudança. Eles incluem tipicamente *hardware*, *software*, prédios, pessoas e documentos formais tais como documentação de processos e acordos de nível de serviço. (ITIL®, 2011)

2.1.16 *LOGGING*

Processo de estocagem de informações sobre eventos que ocorreram num *firewall* ou numa rede. (ABNT NBR ISO/IEC 27002:2005)

2.1.17 MANDATÓRIO (M)

À exceção dos itens informativos e dos classificados como desejável e opcional, todos os demais itens dos RTLI são de caráter mandatório, incluindo as provisões completas e provisões parciais, e deverão ser incluídos, obrigatoriamente, na proposta da OFERTANTE.

2.1.18 MANUTENÇÃO

Conjunto de ações ou medidas necessárias à preservação do Sistema ou do Material, para mantê-lo em serviço, restituir suas condições de utilização, prover a máxima segurança em sua operação e estender sua vida útil tanto quanto for desejável e viável técnica e economicamente. (ICA 400-31/2010)

2.1.19 MIME

Extensões Multi função para Mensagens de Internet é uma norma da Internet para o formato das mensagens de correio eletrônico. A grande maioria das mensagens de correio eletrônico é trocada usando o protocolo SMTP e usam o formato MIME. Os padrões SMTP e MIME utilizados nas mensagens na Internet possuem uma grande inter-relação, que por vezes são chamadas de mensagens SMTP/MIME.

2.1.20 MÓDULO

É a unidade funcional de um sistema, destinada a uma missão específica.

2.1.21 NECESSIDADE OPERACIONAL

Carência ou deficiência constatada, formalizada em documento específico, de mesmo nome, cuja superação, para o cabal desempenho da missão do Comando da Aeronáutica, dependa do fornecimento de um novo Sistema ou Material, ou de modificações em um já existente. A Necessidade Operacional (NOP) pode também decorrer de uma inovação tecnológica, que permita a realização de uma nova missão ou contribua para maior eficiência de uma missão já existente, ou ainda de uma oportunidade de mercado que favoreça a substituição de um Sistema ou de um Material obsoleto, ou o atendimento de uma carência de forma econômica. (ICA 400-31/2010)

2.1.22 NTP

É um protocolo para sincronização dos relógios dos computadores baseado no UDP para sincronização do relógio de um conjunto de computadores em redes de dados com latência variável. O NTP permite manter o relógio de um computador com a hora sempre certa e com grande exatidão.

2.1.23 OAUTH

É um padrão aberto para autorização em sistemas.

2.1.24 SISTEMA

É o conjunto de equipamentos integrados, formando uma unidade e seus conjuntos, subconjuntos e peças, conectados ou usados em associação para executar uma função.

2.1.25 SÍTIO

É o local físico onde está instalado determinado equipamento.

2.1.26 SMTP

Simple Mail Transfer Protocol é o protocolo padrão para envio de e-mails através da Internet. É um protocolo relativamente simples, baseado em texto simples, onde um ou vários destinatários de uma mensagem são especificados (e, na maioria dos casos, validados), sendo, depois, a mensagem transferida.

2.1.27 SUPORTE LOGÍSTICO

O Suporte Logístico é a composição de todas as medidas necessárias para assegurar o apoio a um Sistema ou Material ao longo do seu Ciclo de Vida. Os elementos de Suporte devem ser desenvolvidos de forma integrada entre si. Os principais elementos do Suporte Logístico são: planejamento da manutenção e serviços; equipamentos de teste e de apoio; embalagem, manuseio, armazenagem e transporte; pessoal e treinamento; instalações; dados técnicos e de catalogação; e recursos de informática. (ICA 400-31/2010)

2.1.28 TECNOLOGIA *WEB*

Ferramentas utilizadas para entregar informação e serviço (serviço de nomeação, serviço de previsão de tempo) por uma rede de computadores interligados para usuários e outros sistemas da informação.

2.1.29 USABILIDADE

É a medida pela qual um produto pode ser usado por usuários específicos para alcançar objetivos específicos com efetividade, eficiência e satisfação em um contexto de uso específico. (ABNT NBR ISO/IEC 9241-11:2002)

2.1.30 USUÁRIO

É uma entidade que interage com o sistema durante sua execução. Essa interação ocorre através de comunicações (troca de mensagens). Pode ser um ser humano, um dispositivo de *hardware* ou até outro sistema.

2.2 INTRODUÇÃO

2.2.1 A publicação do Despacho Decisório pelo Ministério da Defesa, nº 007/MD, de 22 de abril de 2009, definiu as competências da Autoridade de Aviação Civil (ANAC) e da Autoridade Aeronáutica (COMAER), bem como das legislações publicadas pelo COMAER (Portaria nº 256/GC5, de 13 de maio de 2011, ICA 63-19, de 12 de setembro de 2011, e da ICA 11-3, de 31 de agosto de 2012), para a área de aeródromos. Para o COMAER, estabeleceu-se:

a) a esfera de atuação do COMAER;

b) os órgãos do COMAER que devem atuar nos processos de análise de Planos Diretores Aeroportuários, de projetos de construção ou modificação de aeródromos e de objeto projetado no espaço aéreo;

c) a delimitação de competência e as áreas de atuação dos órgãos do COMAER; e

d) a interface e a forma de interação entre os diversos órgãos do COMAER.

2.2.2 Adicionalmente, as legislações estabeleceram sete fluxogramas processuais que representam os processos relativos à área de aeródromos. Para cada fluxo definido foram estabelecidos: os órgãos envolvidos no trâmite, a documentação exigida do interessado, prazos para execução das atividades pelos diversos órgãos do COMAER, formulários de verificação e formulários de validação técnica. Essas especificidades e a complexidade dos processos, aliadas à falta de ferramentas de controle de processos, sinalizaram grande dificuldade de coordenação entre os órgãos do COMAER.

2.2.3 As ineficiências geram sobrecarga e retrabalho dos órgãos envolvidos em decorrência conforme apontado na seção 2 da NOP 1/SDOP/2015, de 28/04/2015.

2.3 CONCEPÇÃO

2.3.1 O sistema DEVE ser utilizado pelo DECEA, Órgãos do COMAER e usuários externos.

2.3.2 O sistema DEVE realizar a gestão dos processos integrada com informações de localidade geográfica (mapa).

2.3.3 O sistema DEVE permitir a tramitação dos processos entre todos os entes (usuário externo e órgãos do COMAER).

2.3.4 O sistema DEVE fornecer um ambiente controlado para introdução e armazenamento de dados. DEVE, também, disciplinar a tramitação de documentos, aumentando a eficiência e eficácia de tempo, recursos e tramitação dos processos.

3 REQUISITOS TÉCNICOS

3.1 USABILIDADE

3.1.1 O sistema DEVE apresentar interface em português do Brasil.

3.1.2 O sistema DEVE prover uma interface visual única, coerente, intuitiva e personalizável para todas as funções do sistema.

3.1.3 O sistema DEVE ser customizável quanto à sua tela inicial, permitindo a identificação da instituição/unidade gerencial que está sediando o referido sistema.

3.1.4 O sistema DEVE permitir a customização dos cabeçalhos dos relatórios incluindo o logotipo e descrição da Organização.

3.1.5 O sistema DEVE possuir interfaces fáceis de usar e que não requeiram treinamento extensivo para o uso diário por parte dos usuários.

3.1.6 O sistema DEVE ter as telas de entrada de dados e funcionalidades descritas nativas. Isto é, as telas customizáveis não deverão necessitar de programação ou customização que implique consultoria posterior para serem colocadas disponíveis ao uso.

3.1.7 O sistema DEVE exibir ajuda, em português do Brasil, ao usuário (*help*) no contexto da tela aberta.

3.1.8 O sistema DEVE exibir sugestões de preenchimento ao se posicionar o cursor do mouse sobre um determinado campo.

3.1.9 O sistema DEVE disponibilizar interface gráfica *web* (WUI) para as operações de administração do sistema.

3.1.10 O sistema DEVE disponibilizar interface gráfica *web* (WUI) para todas as operações de usuário.

3.1.11 O sistema DEVE reportar ao usuário a ocorrência de falhas/erros durante sua execução. As mensagens de erro/falhas apresentadas pelo sistema DEVEM ser autoexplicativas para o usuário.

3.1.12 O sistema DEVE utilizar a configuração de data e hora através de um serviço de configuração de NTP (*Network Time Protocol*).

3.1.13 O sistema DEVE indicar aos usuários os campos da tela que são obrigatórios.

3.1.14 O sistema DEVE avisar ao usuário a existência de alterações pendentes, caso o mesmo solicite sair da janela ou do sistema.

3.1.15 O sistema DEVE informar ao usuário qual é a sua versão atual.

3.1.16 O sistema DEVE exibir informações de ajuda e de como contatar o administrador do sistema na janela de *login*. Essas informações podem ser configuradas pelo administrador do sistema.

3.1.17 As telas do sistema DEVEM ter *links* para outras telas relacionadas, sempre que possível. Deve-se evitar a quantidade grande de *links* (cliques de *mouse*) para obter a informação necessária.

3.1.18 O sistema DEVE informar a versão de documentos anexados.

3.1.19 O sistema DEVE possibilitar a elaboração de consultas gerenciais customizadas de acordo com as necessidades e periodicidade definida pelos usuários. As consultas gerenciais customizadas DEVEM possuir filtros que permitam sua emissão com seleção de atributos.

3.2 INTEROPERABILIDADE

3.2.1 O sistema DEVE ser baseado em Tecnologia *WEB.*

3.2.2 O sistema DEVE possuir repositório centralizado e único.

3.2.3 O sistema DEVE gerar os relatórios a partir de modelos (*templates*). Os formatos estão definidos na NOP 1/SDOP/2015 na seção 3.2.1.5 alínea e.

3.2.4 O sistema DEVE exportar o dado em massa, conforme definido na NOP 1/SDOP/2015 na seção 3.2.1.6 alínea f e g.

3.2.5 O sistema DEVE enviar relatórios por e-mail utilizando SMTP (*Simple Mail Transfer Protocol*) e MIME (*Multi-part multimídia*).

3.3 ESPECIFICAÇÃO DO PROCESSO

3.3.1 O sistema NÃO DEVE permitir a duplicação de dados.

3.3.2 O sistema DEVE permitir a modelagem gráfica (*drag-and-drop*) dos processos em ambiente *Web*.

3.3.3 O sistema DEVE permitir modelagem e automação de processos conforme padrão BPMN, UML ou fluxograma em ambiente *Web*.

3.3.4 O sistema DEVE permitir o acompanhamento dos fluxos em andamento através de interface gráfica Web (WUI).

3.3.5 O sistema DEVE gravar histórico completo das revisões realizadas sobre os processos.

3.3.6 O sistema DEVE permitir o controle de revisão sobre os processos, mantendo vários versionamentos.

3.3.7 O sistema DEVE controlar o versionamento de documentos.

3.3.8 O sistema DEVE permitir o monitoramento de pendências de usuários.

3.3.9 O sistema DEVE permitir a inicialização, suspensão, cancelamento e eliminação de processos.

3.3.10 O sistema DEVE utilizar contadores de tempo (*timers*) facilmente configuráveis para apoiar na gestão das regras de negócio do processo, sendo aplicado tanto na modelagem quanto na execução de um processo de negócio.

3.3.11 O tempo de arquivamento dos processos e dados DEVE ser de 5 anos.

3.4 CONSULTAS E VISUALIZAÇÕES

3.4.1 O sistema DEVE permitir a consulta de processos, principalmente os 'em execução', com visualização gráfica do fluxograma.

3.4.2 O sistema DEVE permitir a consulta de pendências.

3.4.3 O sistema DEVE permitir a visualização dos indicadores de desempenho dos processos.

3.4.4 O sistema DEVE permitir a realização de auditoria dos eventos ocorridos na execução de processo e atividades.

3.4.5 O sistema DEVE permitir a definição de indicadores de desempenho associados aos processos e acompanhamento do cumprimento das metas estabelecidas.

3.4.6 O sistema DEVE possuir semáforos que sinalizam visualmente o nível de cumprimento dos resultados.

3.5 PERFORMANCE

3.5.1 O sistema DEVE permitir o acesso simultâneo para diferentes perfis previamente configurados.

3.5.2 O sistema NÃO DEVE possuir limites com relação ao número de projetos controlados nem quanto à capacidade de armazenamento.

3.5.3 Os seguintes parâmetros de performance DEVEM ser medidos em rede local:

a) tempo máximo para navegação entre páginas: 1 segundo;

b) tempo máximo para transação: 2 segundos; e

c) tempo máximo para consultas: 6 segundos para consultas textuais e geográficas e 2 segundos para outras consultas.

3.6 CONFIABILIDADE

3.6.1 O sistema DEVE manter o conjunto de atributos que evidenciam a capacidade do sistema na manutenção do nível de desempenho e integridade das informações armazenadas, em um determinado intervalo de tempo, sob as condições acordadas.

3.6.2 O sistema DEVE manter a integridade dos dados durante as transações (atualizações simultâneas).

3.6.3 O sistema DEVE ser confiável, não ter qualquer defeito ou falha e produzir resultados consistentes e uniformes.

3.6.4 O sistema NÃO DEVE apresentar qualquer tipo de inconsistência de dados.

3.6.5 O sistema DEVE prever que a aplicação possa ser encerrada abruptamente, e as alterações realizadas na sessão e não salvas NÃO DEVEM ser confirmadas (*rollback*).

3.7 ESCALABILIDADE

3.7.1 O sistema DEVE ser expansível de forma a permitir o atendimento das necessidades de negócio pelo crescimento do número de usuários, ou também pelo aumento das informações a serem processadas, preservando os investimentos realizados anteriormente.

3.8 DISPONIBILIDADE

3.8.1 O sistema DEVE estar disponível 24x7 (vinte quatro por sete).

3.8.2 O sistema DEVE possuir 97% de disponibilidade.

3.8.3 O sistema NÃO DEVE ter indisponibilidade em dias consecutivos.

3.8.4 O sistema NÃO DEVE ter indisponibilidade por mais de uma hora nos casos de atualizações de *software*.

3.9 PORTABILIDADE

3.9.1 O sistema DEVE possuir interface *WEB* (WUI).

3.9.2 É DESEJÁVEL que o sistema seja compatível com servidor de aplicação Apache.

3.9.3 É DESEJÁVEL que o sistema utilize o sistema operacional Linux para prover o serviço. Do mesmo modo, é DESEJÁVEL que o restante do *software* básico (servidor *WEB/Application Server*, banco de dados) seja preferencialmente livre, de forma a permitir o alinhamento com os preceitos da NSCA 7-11.

3.9.4 O sistema DEVE estar em conformidade com os padrões *WEB* (*WEB Standards*) recomendados pelo *World Wide Web Consortium* (W3C).

3.10 RECURSOS COMPUTACIONAIS

3.10.1 O SGBD DEVE possuir recursos de replicação.

3.10.2 O SGBD DEVE ter capacidade de realizar operações de *backup* (*hot backup*), mantendo a operacionalidade do sistema.

3.11 ARQUITETURA

3.11.1 O sistema DEVE apresentar alta coesão e baixo acoplamento.

3.11.2 O sistema DEVE apresentar identificação de exceções e seu tratamento.

3.11.3 O sistema DEVE apresentar prevenção e tolerância a falhas.

3.11.4 A arquitetura do sistema DEVE ser centralizada, cliente-servidor de três camadas, com acesso realizado através de rede. O sistema DEVE estar disponível através da INTRAER e INTERNET.

3.12 SEGURANÇA

3.12.1 MODULARIZAÇÃO DA ARQUITETURA

3.12.1.1 O sistema DEVE ser subdividido em módulos de menor complexidade e com funcionalidade e interfaces bem definidas. Cada módulo deve fazer o tratamento das informações que envia e recebe de forma independente. Os módulos do sistema devem disponibilizar apenas as funcionalidades necessárias aos outros módulos.

3.12.2 AUTENTICAÇÃO

3.12.2.1 O sistema DEVE autenticar o acesso a todas as funcionalidades/módulos que o usuário possa executar no sistema, autenticação centralizada. Cada módulo do sistema DEVE ter acesso à credencial do usuário já autenticada, não exigindo nova autenticação.

3.12.2.2 O sistema DEVE utilizar o princípio do menor privilégio, concedendo apenas os privilégios necessários para os usuários executarem suas atividades no sistema.

3.12.2.3 O sistema DEVE alertar o administrador do sistema sobre a tentativa de acessos não autorizados.

3.12.2.4 O acesso DEVE ser controlado por um procedimento que estabeleça a identidade do usuário com grau de confiança (autenticação), e só então conceder determinados privilégios (autorização) de acordo com o que for estabelecido para o perfil de acesso deste usuário.

3.12.2.5 O sistema DEVE permitir ao administrador do sistema o bloqueio de acesso de usuário.

3.12.2.6 O sistema DEVE enviar uma notificação ao administrador do sistema após a terceira tentativa consecutiva com autenticação incorreta e bloquear a conta de usuário.

3.12.2.7 O sistema DEVE permitir ao administrador o bloqueio/desbloqueio do acesso de usuário ao sistema.

3.12.2.8 O sistema NÃO DEVE permitir que sejam reutilizadas as últimas 3 senhas.

3.12.2.9 O sistema DEVE permitir ao administrador alterar as senhas dos outros usuários, mas não poderá visualizá-las. A alteração na senha deverá ser automaticamente informada ao usuário cadastrado.

3.12.2.10 O sistema DEVE obrigar a troca de senha no primeiro *login* após o cadastro ou após alteração da senha pelo administrador.

3.12.2.11 O sistema DEVE permitir ao usuário modificar sua própria senha.

3.12.2.12 O sistema DEVE permitir ao usuário reiniciar (RESET) a senha a qualquer momento.

3.12.2.13 O sistema DEVE distribuir ao usuário sua senha pessoal e intransferível para acesso.

3.12.2.14 O sistema DEVE adotar política de senhas que garanta, no mínimo, 8 (oito) caracteres, sendo eles ao menos um número, um caractere minúsculo, um caractere maiúsculo e um caractere especial (#;.%$&@![]{}()).

3.12.2.15 O sistema DEVE permitir ao administrador de sistemas configurar o período de validade das senhas, considerando como período padrão 6 meses.

3.12.2.16 O sistema DEVE possuir mecanismos que forcem o uso de senhas não triviais.

3.12.2.17 O sistema NÃO DEVE armazenar senhas embutidas no código (*hard-coding*).

3.12.2.18 O sistema DEVE utilizar a ferramenta de CAPTCHA para *login* de usuário externo.

3.12.2.19 O sistema DEVE utilizar protocolo padrão aberto para autenticação.

3.12.2.20 É DESEJÁVEL que o sistema utilize o protocolo para autenticação OAuth.

3.12.2.21 O sistema DEVE permitir a um determinado usuário o acesso único ao sistema, não permitindo acessos simultâneos.

3.12.2.22 O sistema DEVE permitir o uso e gerenciamento de perfis de acesso. Esse gerenciamento DEVE ser integrado ao protocolo de autenticação.

3.12.2.23 O sistema DEVE permitir ao administrador do sistema associar perfis de acesso às funcionalidades correspondentes.

3.12.2.24 O sistema DEVE prover mecanismos de segregação de usuários através de nível de atuação (usuários, analista de processo, administração,...).

3.12.2.25 O sistema DEVE possuir mecanismos para restringir as operações no sistema conforme o perfil dos usuários.

3.12.2.26 O sistema DEVE possibilitar o controle de restrições de acesso por usuário e por grupo de usuários.

3.12.2.27 O sistema DEVE permitir ao administrador do sistema definir o tempo de inatividade do usuário para encerramento da conexão.

3.12.2.28 O sistema DEVE habilitar o controle de acesso e a rastreabilidade por usuário do sistema.

3.12.2.29 O sistema DEVE permitir a definição do tempo de inatividade do usuário para encerramento da conexão (sessão), devendo encerrá-la quando o tempo for alcançado.

3.12.3 PROTEÇÃO DOS DADOS

3.12.3.1 A proteção de dados do sistema DEVE incluir: a política de controle de acesso, a importação e exportação de dados, a proteção de dados em transferência interna, a informação residual e a manutenção da integridade de dados internos mesmo em operações simultâneas.

3.12.3.2 Todas as saídas de dados do sistema DEVEM ser devidamente codificadas/formatadas para garantir que estes sejam recebidos conforme esperado pelo cliente.

3.12.3.3 O sistema DEVE validar as entradas e saídas em todos os módulos, no cliente e no servidor.

3.12.3.4 O sistema DEVE tratar todas as mensagens de erro de forma a exibir apenas informações referentes à operação do usuário, expondo o mínimo possível sobre as características ou arquitetura do sistema. DEVE, também, transmitir informações tratadas do erro, retornando ao usuário o *status* do sistema.

3.12.3.5 O sistema DEVE armazenar a senha e transmiti-la de forma criptografada (SHA-1 ou superior).

3.12.4 ASSINATURA DIGITAL

3.12.4.1 O sistema DEVE possibilitar que documentos sejam assinados digitalmente (ICP-Brasil) durante a execução do fluxo.

3.12.5 TRILHAS DE AUDITORIA

3.12.5.1 O sistema DEVE implementar Trilhas de Auditoria (*logs*), de forma a garantir a rastreabilidade, registrando os acessos ao sistema, as modificações, a criação de registros e os erros.

3.12.5.2 O sistema DEVE manter total trilha de auditoria referente às transações realizadas.

3.12.5.3 O sistema DEVE registrar em *log* todos os eventos do sistema. Os atributos dos *logs* são:

a) tipo do evento;

b) componente do sistema;

c) dia e hora do evento;

d) informação específica do evento, tal como: dado afetado, mensagem de erro etc; e

e) informação específica do usuário, tal como: acesso simultâneo, tempo de *logon*, origem do acesso.

3.12.5.4 O sistema DEVE incluir no registro de *log* do sistema:

a) ações do usuário;

b) mudanças na configuração;

c) mudanças no estado do sistema;

d) erros e falhas; e

e) mensagens de transações.

3.12.5.5 O sistema DEVE permitir o filtro de todos os registros de *log* por período (data e hora de início e de fim) e por intervalos (ano, mês, dia, hora e minuto).

3.12.5.6 O sistema DEVE permitir que os registros de *log* filtrados possam ser exportados em formato PDF e impressos.

3.12.6 INFRAESTRUTURA

3.12.6.1 DEVE ser feito o *hardening* do(s) servidor(es), removendo *softwares* desnecessários, otimizando as configurações de sistema e desabilitando serviços desnecessários para melhor aproveitamento dos recursos e mitigando eventuais vulnerabilidades do sistema.

3.12.7 CONTINUIDADE DO SISTEMA

3.12.7.1 Para permitir a execução da política de *backup*, o sistema DEVE:

a) realizar *backup* de todas as informações necessárias – dados e configurações armazenadas – para recuperação em caso de incidente ou desastre;

b) permitir a configuração de agendamento de *backup* automático;

c) permitir a criação de pacote de *backup* pelo usuário autorizado a qualquer momento;

d) realizar a importação de pacote de *backup* a partir de procedimento manual; e

e) permitir armazenar os pacotes de *backup* em local pré-configurado em mídia local ou através da rede.

3.12.7.2 O armazenamento de *backup*, dados e configurações do sistema NÃO DEVE ser restrito, possibilitando uso de acordo com o espaço disponível no recurso de armazenamento. Ou seja, NÃO DEVE haver imposição de limite pelo *software*.

3.12.8 MONITORAMENTO

3.12.8.1 DEVEM ser implementados mecanismos de controle, monitoramento e detecção de intrusão atendendo às melhores práticas de defesa de perímetro. O sistema poderá utilizar a infraestrutura do ambiente a ser implantado, caso este já possua estas características.

3.12.8.2 A infraestrutura DEVE ser dotada de *firewall*.

3.12.8.3 O ambiente em que se encontra o sistema DEVE permitir o monitoramento do desempenho do sistema e possibilidade de ações corretivas sistêmicas.

3.12.8.4 O sistema DEVE notificar o administrador quando o espaço dos recursos de armazenamento estiver perto do seu uso total. Esse parâmetro, medido em percentual de ocupação do recurso, DEVE ser configurado pelo administrador do sistema.

3.12.8.5 O sistema DEVE permitir a limpeza parcial dos recursos armazenados quando houver o esgotamento dos recursos de armazenamento.

3.12.9 OUTROS

3.12.9.1 É DESEJÁVEL que o sistema apresente as seguintes características com relação à Segurança para o *Software* (Código-Fonte):

a) observar os requisitos de segurança previstos na Norma ABNT NBR ISO/IEC 15408; e

b) observar os requisitos de segurança previstos na Norma ABNT NBR ISO/IEC 27002.

3.12.9.2 É DESEJÁVEL que o sistema seja submetido a Testes de Segurança para avaliar toda a infraestrutura do projeto, para se identificar os *gaps* de segurança da informação e determinar ações corretivas e preventivas. Além disso, deve-se realizar testes funcionais no sistema, incluindo a análise de código-fonte, análise de risco e teste de invasão, para avaliar a eficiência e eficácia dos controles de segurança da informação implementados.

3.12.9.3 Na realização dos testes de aceitação (SAT), DEVE-SE considerar a verificação dos Dez Riscos de Segurança mais críticos em aplicações *web* (*The Top 10 Most Critical Web Application Security Risks***)** recomendado pela OWASP, que reúne os riscos de ataque mais críticos exploráveis a partir de vulnerabilidades nas aplicações web.

4 REQUISITOS LOGÍSTICOS

4.1 REQUISITOS LOGÍSTICOS GERAIS

4.1.1 O sistema DEVE possuir um programa de suporte logístico contemplando, no mínimo:

a) plano de manutenção;

b) requisitos de pessoal técnico para manutenção; e

c) treinamento e suporte de treinamento.

4.1.2 É DESEJÁVEL que o sistema seja composto, na sua maior parte, se não no todo, por itens nacionalizados e/ou de tecnologia dominada por empresas brasileiras.

4.1.3 DEVE ser preenchido o formulário para classificação do sistema conforme a ICA 7-22 "Classificação dos Sistemas de Tecnologia da Informação do SISCEAB" ou outra norma que venha a substituí-la.

4.1.4 O sistema DEVE possuir licença de *software* vitalícia para uso durante seu ciclo de vida.

4.1.5 O sistema, assim como os seus componentes, DEVE ser implantado no SILOMS.

4.1.6 O *hardware* utilizado no sistema DEVE ser adquirido considerando-se que ele formará uma solução única e completa.

4.1.7 O *hardware* utilizado no sistema DEVE ser adquirido com garantia mínima *on-site* de 05 (cinco) anos.

4.1.8 Após o término da garantia supracitada, todo o hardware utilizado DEVE ser totalmente substituído por novo hardware, o qual DEVERÁ atender a todos os requisitos técnicos descritos neste documento.

4.1.9 Toda a solução do sistema DEVE possuir garantia mínima (suporte e atualizações) de 05 (cinco) anos.

4.2 DOCUMENTAÇÃO TÉCNICA

4.2.1 Toda documentação técnica e operacional DEVE ser fornecida de forma digital, sendo no mínimo em pdf em formato adequado para impressão e encadernação. A documentação operacional DEVE estar em Português do Brasil, sendo DESEJÁVEL para a documentação técnica.

4.2.2 A documentação referida no item anterior DEVE ser entregue aos órgãos que irão operar o sistema, além do DECEA e PAME-RJ (órgão gestor de manutenção).

4.2.3 Estes manuais DEVEM possuir, no mínimo:

a) Plano de manutenção;

b) Requisitos de pessoal técnico para manutenção;

c) Treinamento e suporte de treinamento;

d) Descrição geral do sistema;

e) Descrição detalhada do sistema;

f) Diagrama de instalação;

g) Instruções para a instalação;

h) Instruções para a operação;

i) Manual do usuário;

j) Instruções de manutenção preventiva e corretiva, incluindo a utilização de *softwares* (instalação, desinstalação, configuração, realinhamento de parâmetros operacionais), diagnóstico de panes e da utilização das ferramentas e equipamentos com esse objetivo; e

k) Procedimentos para manutenção periódica do sistema sugerido.

4.3 TREINAMENTO

4.3.1 Os treinamentos DEVEM contemplar uma seção teórica e uma seção prática e DEVEM ser fornecidos em Português.

4.3.2 O fornecedor DEVE se responsabilizar pelos instrutores, pelas instalações e por todo o material necessário ao desenvolvimento do curso.

4.3.3 DEVE ser fornecida ao DECEA toda a documentação didática necessária aos treinamentos, inclusive as que permanecerão de posse de cada aluno.

4.3.4 As turmas e tipos de treinamento necessários são listados abaixo:

a) turmas de treinamento para Supervisor e Elaborador de Processos; e

b) turmas de treinamento de Técnico de Operação e Manutenção, instalação e configuração do sistema. Deverá permitir aos técnicos identificar falhas (independentemente de sinalização de pane), bem como capacitá-los a solucioná-las.

4.3.5 Os treinamentos DEVEM envolver todos os órgãos pertinentes e o PAME-RJ.

4.3.6 O planejamento do treinamento deverá considerar: as metas a serem atingidas em cada treinamento, os requisitos de treinamento (necessidades), as restrições (foco), o público-alvo, o procedimento de concepção do treinamento e a forma de transposição do conteúdo.

4.3.7 A verificação dos resultados do treinamento deverá ser feita através da avaliação dos treinandos nos aspectos: organização do ambiente de treinamento, recursos didáticos e autoavaliação do treinando.

4.3.8 Caso a análise dos resultados do treinamento apresente faltas, devem ser criadas alternativas (soluções) para atender às necessidades remanescentes. Deve estar previsto um segundo treinamento, caso o primeiro não tenha atingido os resultados previstos.

4.4 OPERAÇÃO ASSISTIDA

4.4.1 Deverá ser realizada operação assistida com duração mínima de 2 (dois) meses a partir da data de entrada em produção do sistema. Deverão ser previstos treinamentos práticos de correção de falhas (panes) passíveis de ocorrência no sistema.

4.5 MANUTENÇÃO DO *SOFTWARE*

4.5.1 O sistema DEVE proporcionar procedimentos rápidos e seguros de manutenção corretiva e preventiva.

4.5.2 O Plano de Manutenção do sistema DEVE garantir o seu suporte continuado, conforme política de manutenção do SISCEAB documentada na DCA 66-1 "Atividade de Manutenção no Sistema de Controle do Espaço Aéreo".

4.5.3 A elaboração do plano de manutenção para o sistema DEVE considerar como gestor o PAME-RJ ou OPSTI DECEA a ser designado pelo SDTE.

4.5.4 O sistema DEVE ter ambientes de homologação e de produção segregados.

4.5.5 O Proponente DEVE garantir a manutenção corretiva (correção de erros) do sistema pelo prazo de 12 (doze) meses após a aceitação técnica.

4.5.6 Todas as correções ou atualizações realizadas no sistema DEVEM ser testadas, aprovadas e documentadas.

4.5.7 Todos os *softwares* necessários ao funcionamento e reinstalação futura, atualizações existentes, suas licenças e demais ferramentas ou dispositivos necessários à manutenção do sistema DEVEM ser entregues até a entrada em operação do sistema ao PAME-RJ.

4.6 RECEBIMENTOS TÉCNICOS E OPERACIONAIS

4.6.1 Os testes de recebimento técnico serão divididos em duas etapas distintas (fábrica e campo), para as quais o fornecedor DEVE apresentar, para aprovação do DECEA, com no mínimo 45 dias de antecedência, documento contendo o Plano dos Procedimentos de Testes pretendidos, contendo todos os testes que comprovem as características técnicas mencionadas na proposta de fornecimento e nos documentos técnicos.

4.6.2 O DECEA poderá prever e realizar testes e medidas adicionais àqueles contidos nos cadernos de testes do fornecedor, desde que os julguem necessários à comprovação do desempenho dos equipamentos.

4.6.3 A aprovação do DECEA, com a aceitação dos relatórios/certificados, não eximirá o fornecedor de sua responsabilidade de executar o fornecimento de acordo com os requisitos contidos nos documentos técnicos.

4.6.4 Os testes em campo somente serão iniciados se o sistema, bem como o instrumental de testes, estiver no local definido pelo DECEA, devidamente instalado pelo fornecedor e pronto para o início dos trabalhos.

4.6.5 Os testes de recebimento em campo (SAT) DEVEM ter a participação de representante(s) indicado(s) pelo DECEA e pelo mantenedor (conforme item 4.5.3 deste documento), somente após os quais os equipamentos serão considerados como recebidos.

5 REQUISITOS INDUSTRIAIS

5.1 CERTIFICAÇÃO E HOMOLOGAÇÃO

5.1.1 O sistema DEVE ter seu cumprimento de missão, desempenho e segurança certificados pelo ICEA ou por órgão técnico de reconhecimento internacional para que esse Instituto, após avaliação, possa emitir um certificado de convalidação.

5.1.2 O sistema, após o recebimento técnico, DEVE ser homologado pelo DECEA, satisfeitas todas as condições operacionais para sua utilização, para ser considerado recebido em campo.

5.2 GARANTIA DA QUALIDADE

5.2.1 É DESEJÁVEL que a proponente apresente certificação ABNT NBR ISO/IEC 9001-2008.

5.2.2 A proponente DEVE apresentar o resultado de testes de segurança dos sistemas realizados por empresas especializadas em teste de *software*, segundo o *framework* OWASP ou equivalente, devidamente aprovado pelo DECEA.

5.2.3 É DESEJÁVEL que a proponente tenha um nível de certificação CMMI ou certificação equivalente.

6 DISPOSIÇÕES FINAIS

6.1 Caso algum dos requisitos referenciados na NOP e nesta RTLI indicar alguma restrição aos produtos oferecidos no mercado, deve ser realizada uma reunião com os envolvidos no processo para alinhamento da necessidade.

6.2 Os casos não previstos nesta publicação DEVEM ser submetidos à avaliação do Exmo. Sr. Chefe do Subdepartamento Técnico do DECEA.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS – ABNT NBR ISO/IEC 27002. *Código de prática para a gestão da segurança da informação*. Rio de Janeiro. RJ, 2005

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS – ABNT NBR ISO/IEC 9241-11. *Requisitos Ergonômicos para Trabalho de Escritórios com Computadores Parte 11 – Orientações sobre Usabilidade*. Rio de Janeiro, RJ, 2002.

BÉLGICA. EUROCONTROL Headquarters. *Especificação para Intercâmbio de Informação Aeronáutica*: **EUROCONTROL-SPEC-151**. Bruxelas, 2012.

BRASIL. Comando da Aeronáutica. Departamento de Controle do Espaço Aéreo. *Gerenciamento do Ciclo de Vida de Materiais da Aeronáutica*: **ICA 400-31**. Rio de Janeiro, RJ, 2010.

BRASIL. Comando da Aeronáutica. Departamento de Controle do Espaço Aéreo. NOP nº 01/SDOP/2013, de 19 de fevereiro de 2013.

INGLATERRA. Office for Government Commerce (OGC). *Glossário e Abreviações ITIL® de Português do Brasil v1.0*. 2011.

Elmasri, Ramez; Navathe, Shamkant B. *Fundamentos de Banco de Dados*. Editora: Pearson Education/Addison Wesley, 4ª Edição, 2005.

OWASP - *Open Web Application Security Project*. *Site* https://www.owasp.org/index.php. Acessado em 19 de novembro de 2013.