

V Reunião: Processo de Certificação

<https://docs.google.com/presentation/d/15G8D6HWj6SSnDoK1B89x93YhNRMfoCzC/edit?usp=drivesdk&oid=115891639852919271691&rtpof=true&sd=true>

Cenários de testes sugeridos e discutidos:

- Interoperabilidade:

- Garantir interoperabilidade entre sistemas
 - Teste: DSS ao USS, USS ao USS, USS ao DSS
- Testar Funcionalidade de acesso remoto via API
 - Teste: Provedor - Usuario
 - Declaratório
- Ciber: Certificados HTTPS, bloqueando http
- Incident Report
 - Armazenamento de Logs
 - Tipo de log e tempo pra cada tipo
 - Provedor dá o OK que está ciente do que é necessário
 - Como será verificado?
 - Inspeções
 - Definir quais são as informações críticas que necessitam teste
- Categorizar os provedores A, B, C, D
 - De acordo com as capacidades comprovadas por teste e declaratórios
- Disponibilizar EndPoint para consulta de Logs (inspeção)
- Testar Formato da comunicação (padrão ASTM)
- Atentar aos casos criminais que possam vir a ocorrer, em questão de responsabilização
 - Matriz de responsabilidade clara
- Definir quais os requisitos são necessários
 - Definir quais devem ser testados
 - Definir quais são declaratórios
- Planejamento de risco e plano de contingencia
- Requisitos para áreas diferentes (remota)
 - Haverão requisitos diferentes para diferentes categorias
 - Fase 1: Categoria A

- Testes em tempo Real: Capacidade do provedor de comunicar informações de espaço aéreo para o usuário e para o DSS
- Provedor deve fornecer acesso de "usuário de testes" para que o DECEA possa fazer testes
- Validar consistência de dados:
 - Verificar formatação, casas decimais, formatos de polígonos
 - Determinar margem de erro aceitável
- Teste de carga requisição ao DSS e ao provedor
 - Performance dos sistemas do Provedor sob alta carga de informação (Ex: Evento com muitos usuários próximos ao mesmo tempo)
 - Impacto na telemetria, requisições, comunicação
- Maneira de classificar provedor: Autonomia do provedor sem DSS
- Verificar clareza da visualização de dados, dashboard
- Verificar se a interface está amigável o suficiente para o usuário
 - Exigir o "OK" do operador
- Resposta a alterações normativas: Garantir um tempo de atualização do sistema
 - definir um tempo para os provedores implementarem as mudanças
 - definir um tempo para alterações críticas
 - Caso a caso mediante análise do time técnico
 - Estabelecer limitantes condicionais até o provedor cumprir
 - Não há um tempo para correção> Mas é exigido que o plano de ação seja imediato
- Provedor que passou por acidentes precisa sofrer novo processo de certificação
- Garantir autenticidade e autenticação segura de usuários
 - exigir autenticação em 3 fatores do usuário
- Armazenamento histórico:
 - Em casos especiais, definir requisitos especiais de armazenameto:
 - Acidente: Guardar todos os logs existentes dentro do intervalo de 24h antes e após o evento.
- Disponibilidade de Documentação e Treinamento:
 - Verificar existência de documentação disponível para o usuário
 - Verificar existência de treinamento do sistema para o usuário
- Mecanismo de comunicação de incidentes:
 - Garantir que o provedor tenha o mecanismo de incident report
 - Obrigatoriedade de Reportar incidentes envolvendo pessoas
 - Qual a prerrogativa do provedor?
 - incidentes de sistema em termos de eficiência de prestação de serviços
- Hierarquia da solicitação:
 - Testar interação com outras operações de prioridades diferentes

Lista sugerida pela SpeedBird:

1. Interoperability with Other Systems: Assess the interoperability of the CIS platform with existing air traffic management systems and UAS platforms.
2. API Functionality for External Access: Test the availability and functionality of APIs for external access to CIS data.
3. Data Integration with Multiple Platforms: Verify that the CIS can successfully aggregate data

from multiple sources involved in UAS operations.

4. Security Protocol Compliance: Ensure that the CIS adheres to cybersecurity protocols to protect sensitive information.
5. Data Format Compliance: Test the CIS's ability to handle and transmit data in formats compliant with relevant industry standards (i.e ASTM's and EAROCAE's provision)
6. Real-Time Data Availability: Verify that users can access real-time data about UAS operations, including flight status and airspace restrictions.
7. Data Consistency and Accuracy: Validate that the information provided by the CIS is consistent and accurate across all integrated systems.
8. Scalability of the Platform: Assess the scalability of the CIS to handle increasing numbers of users and UTM airspaces.
9. System Performance under Load: Evaluate the performance of the CIS under high data load conditions to ensure stability and responsiveness.
10. Data Visualization Features: Test the effectiveness of data visualization tools within the platform to present complex operational data clearly.
11. User-Friendly Interface: Evaluate the user interface of the CIS for intuitiveness and ease of navigation for different user roles.
12. Response to Regulatory Changes: Ensure that the CIS can adapt its information services quickly in response to changes in UAS regulations.
13. User Access Management: Ensure robust user authentication and authorization mechanisms are in place to manage user access levels.
14. Historical Data Management: Assess the platform's ability to archive and retrieve historical data.
15. Training and Documentation Availability: Ensure that comprehensive training and user documentation are available for users to understand CIS functionalities.
16. Incident Reporting Mechanism: Ensure there is a mechanism for logging and reporting incidents of UTM's.

Sugestões extras:

- Agendar FRZ: Próximo fórum

GOVERNANÇA/OPERACIONAL

- Qual a diretriz para o provedor em caso de queda de sistema BR-UTM
 - Operações em curso podem finalizar
 - Novas operações não podem iniciar

Revision #4

Created 13 November 2024 16:25:13 by Cenato

Updated 20 December 2024 13:00:02 by Cenato