Parque de Material de Eletrônica
da Aeronáutica do Rio de Janeiro

Interconexões Aeronáuticas e Cyber-segurança
Workshop SWIM BR - 2023

Objetivo

Conhecer as Redes e a Cyber-segurança do SISCEAB (Cn)

Roteiro

1. O que é o CGTEC?
2. NOC: Centro de Operações das Redes
3. INTRAER e ATN-Br
4. SOC: Centro de Operações da Segurança da Informação
5. Interconexões Seguras

O CGTEC

Conectar

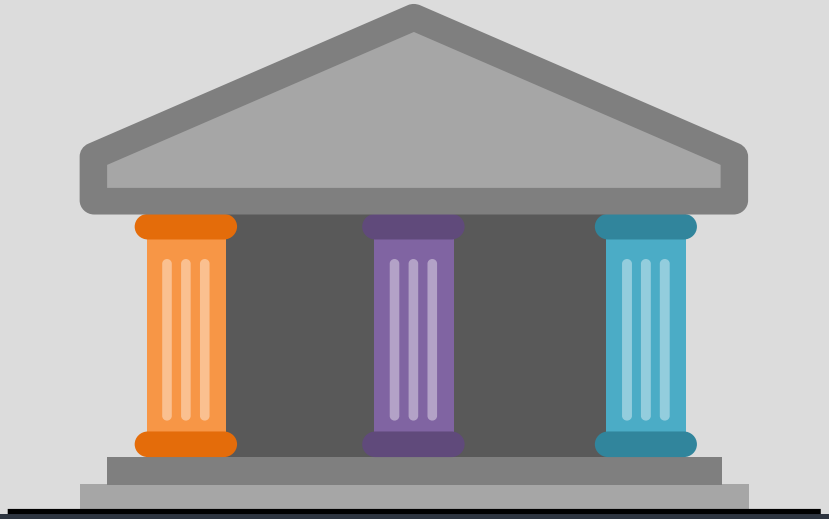
O NuCGTEC abriga o Centro de Operações de Redes (NOC), com a missão de **monitorar** e operar as redes operacional (ATN-Br) e administrativa (INTRAER) com foco na **disponibilidade** e **segurança**.

Proteger

O NuCGTEC abriga o Centro de Operações de Segurança (SOC) do DECEA, cuja missão é **monitorar**, operar e evoluir a segurança do SISCEAB com vistas à **gestão de riscos, à prevenção e ao tratamento de incidentes.**

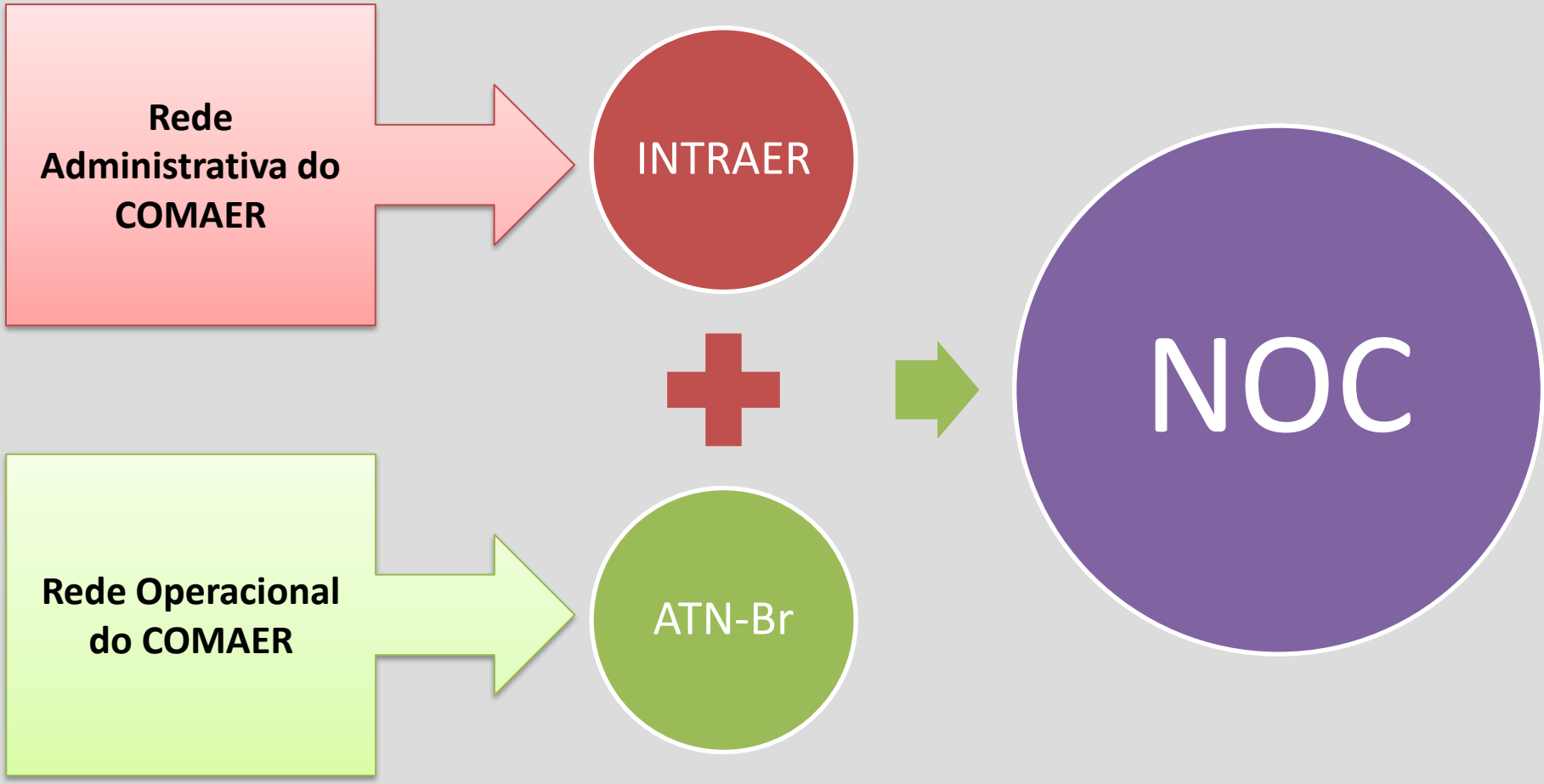
Monitorar

O NuCGTEC possui a missão de **monitorar** o estado técnico dos ativos do SISCEAB e do SISDABRA, com foco na **disponibilidade** dos serviços, visão holística **do impacto de inoperâncias, melhoria dos processos de manutenção e da predição de falhas**.



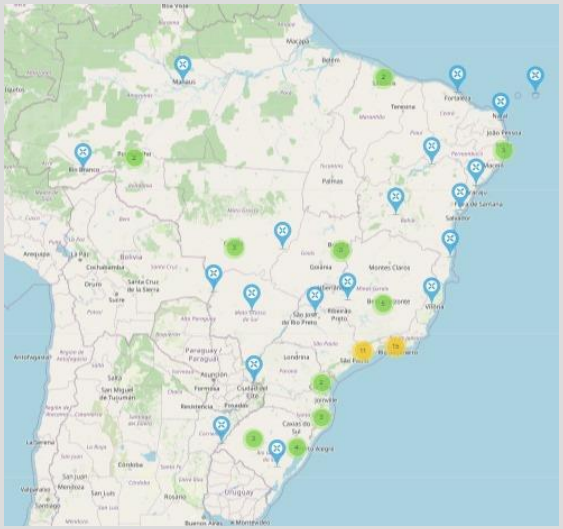
NOC: Centro de Operações das Redes

- **Responsável pela Operação e Evolução das Redes:**



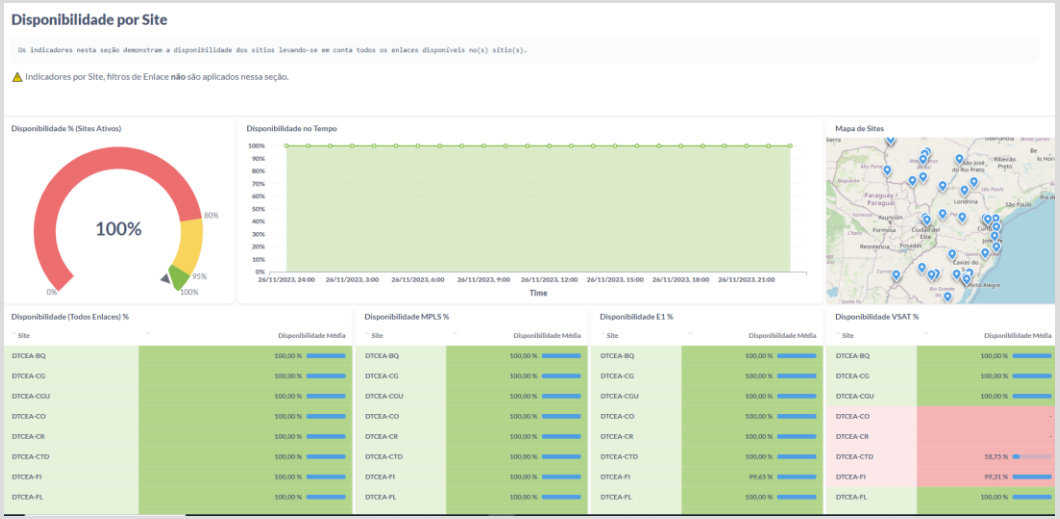
NOC: Centro de Operações das Redes

- Rede INTRAER
  - Migrada para SDWAN (IPv4).
  - Foco nos serviços administrativos.
  - 86 PoP: 128 em 2024.
  - Diversos Serviços Operacionais suportados.
    - Migração para a ATN-Br.



NOC: Centro de Operações das Redes

- Rede ATN-Br
  - Solução SDN Frequentis (All over IP).
  - Apenas serviços operacionais.
  - 77 PoP.
  - Operação no CINDACTA II, CINDACTA III.
    - CRCEA em implantação.



NOC: Serviços Operacionais nas Redes

- V/UHF
- Telefonia Operacional
- DLRS
- RADAR
- AMHS
- FMC
- GEA
- PLN
- RACAM
- SIGMA
- SAGITARIO
- AMAN
- TATIC
- CRONOS
- WEBRADAR
- DATALINK (DCL)
- TATIC
- CPDLC
- R-AFIS
- D-ATIS.

O CGTEC

Conectar

O NuCGTEC abriga o Centro de Operações de Redes (NOC), com a missão de **monitorar** e operar as redes operacional (ATN-Br) e administrativa (INTRAER) com foco na **disponibilidade** e **segurança**.

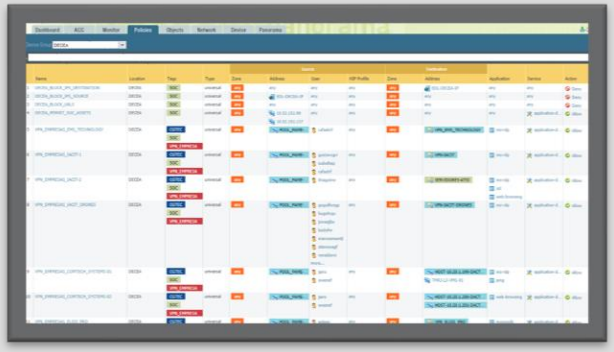
Proteger

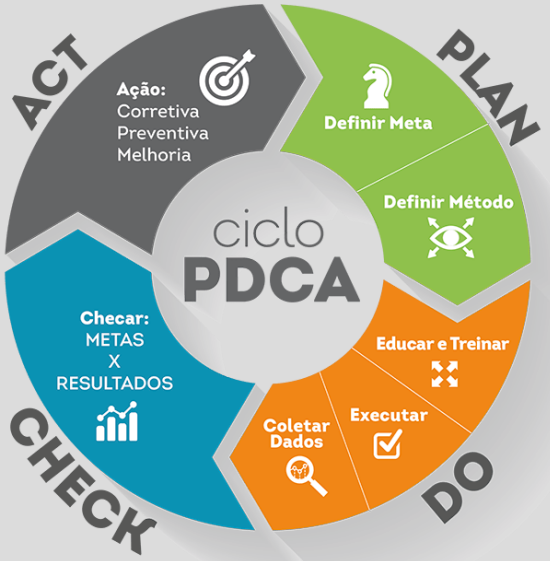
O NuCGTEC abriga o Centro de Operações de Segurança (SOC) do DECEA, cuja missão é **monitorar**, operar e evoluir a segurança do SISCEAB com vistas à **gestão de riscos, à prevenção e ao tratamento de incidentes.**

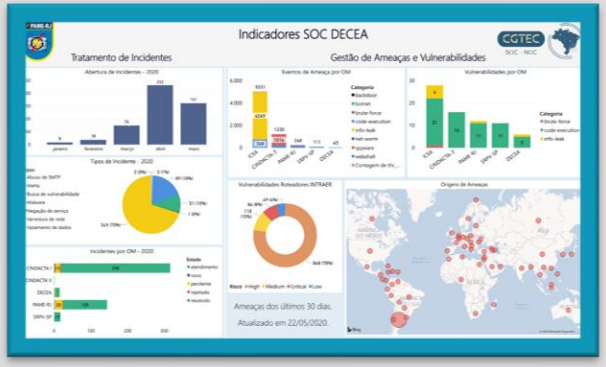
Monitorar

O NuCGTEC possui a missão de **monitorar** o estado técnico dos ativos do SISCEAB e do SISDABRA, com foco na **disponibilidade** dos serviços, visão holística **do impacto de inoperâncias, melhoria dos processos de manutenção e da predição de falhas**.

Planejamento Estratégico do SOC







SOC: Serviços Oferecidos

- Proteção de Perímetro
- Segurança das WAN
- Auditoria em Firewall
- Orquestração
- Threat Sharing
- Gestão de Endereçamento
- Gestão do DLRS Terrestre

Cliente COMAER

- VPN para Empresas
- Vulnerabilidades
- ETIR
- Indicadores e BI
- Gestão da Identidade
- Segurança de Endpoint
- Gestão da Criptografia

Cliente DECEA

SOC: NGFW

Proteção de Perímetro

Auditoria de Firewall

Segurança das WAN

- 02 *Panorama Servers*.
- *NG Firewalls Palo Alto*
  - FW em Operação (38):
    - CINDACTA I, CINDACTA II, CINDACTA III, CINDACTA IV, CRCEA-SE, GCC, PAME, ICEA, DECEA, CGNA, CCA-BR, CCA-RJ, DCTA, GAP(AF/AN/NT), BASC, CLA e CABW.
  - FW Planejados (4):
    - COMAE, COPE, COPE-S e CABE.

SOC: Threat Sharing

SOC DECEA: Mitigando Riscos Globais de Ameaças Cibernéticas

Threat Sharing

O que fazemos?

Integrar Eventos
- CERT.br
- Fontes Globais
- Tempo Real

Avaliar Risco
- Filtrar Eventos
- Correlacionar
- Classificar

Proteger
- Bloquear
- Fronteiras
- Imediatamente

Como fazemos?

+10.000 Ativos	Múltiplas Fontes	Inteligência Ativa	Reduzindo Riscos	Acima de tudo :
				
Monitorando	Entendendo	Correlacionando	Mitigando	Contribuindo

20 anos cert.br

SOC: Threat Sharing

SOC DECEA: Mitigando Riscos Globais de Ameaças Cibernéticas

Defesa Ativa do DECEA

Conforme previsto em seu Planejamento Estratégico, o SOC DECEA ativou a orquestração automática na proteção contra ameaças cibernéticas. Esta ação, que é possibilitada pela integração com fontes confiáveis (Ex.: CERT.BR), permite que ameaças conhecidas possam ser bloqueadas automaticamente pelos Firewalls Palo Alto. Baseando-se em eventos que estão acontecendo no mundo todo, o SOC protege o DECEA de ofensores já conhecidos, adquiridos através da troca de informações com os órgãos creditados. Como consequência, é proporcionada uma camada adicional de proteção às redes do DECEA.

Indicadores de Resultado

ICAO Cyber Security Panel

Cyber Information Sharing Guide (Draft) – Item 6.2.3

*"It is recommended to aviation stakeholders to use **MISP** to share cyber-information as:*

- *It helps automating the use of the information received to update various security systems such as SIEM/SOC, Firewalls, Anti-Virus SW, IDPS/IPS.*
- *It allows to share rapidly information (time can be an important element of the effectiveness to protect infrastructures).*
- *It allows to simply update progressively an event with additional related information.*
- *No need to differentiate the recipient list based on the TLP marking: all types of TLP marking can be sent via MISP."*

SOC: DLRS

Gestão de Redes Seguras

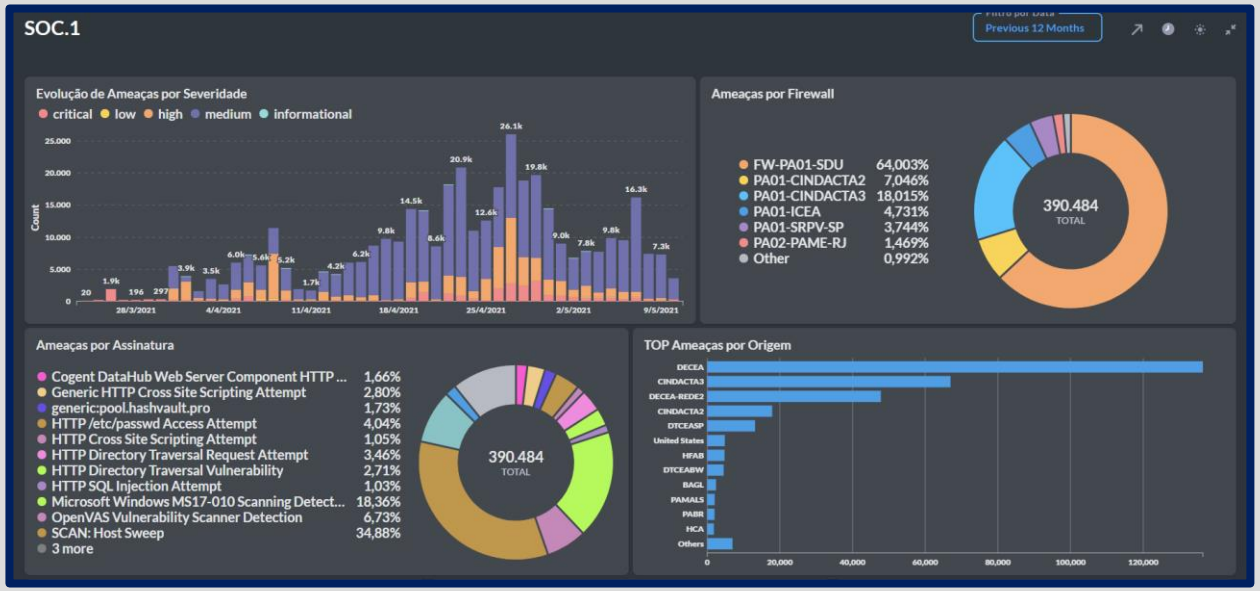
Gestão da Criptografia

- Certificate Authority CGTEC
- DLRS: Gestão do Segmento Terrestre
  - Instalação do R&S Trusted Objects Manager (TOM) no PAME-RJ.
  - Coordenação da Instalação dos DLRS nos Sítios.

SOC - BI

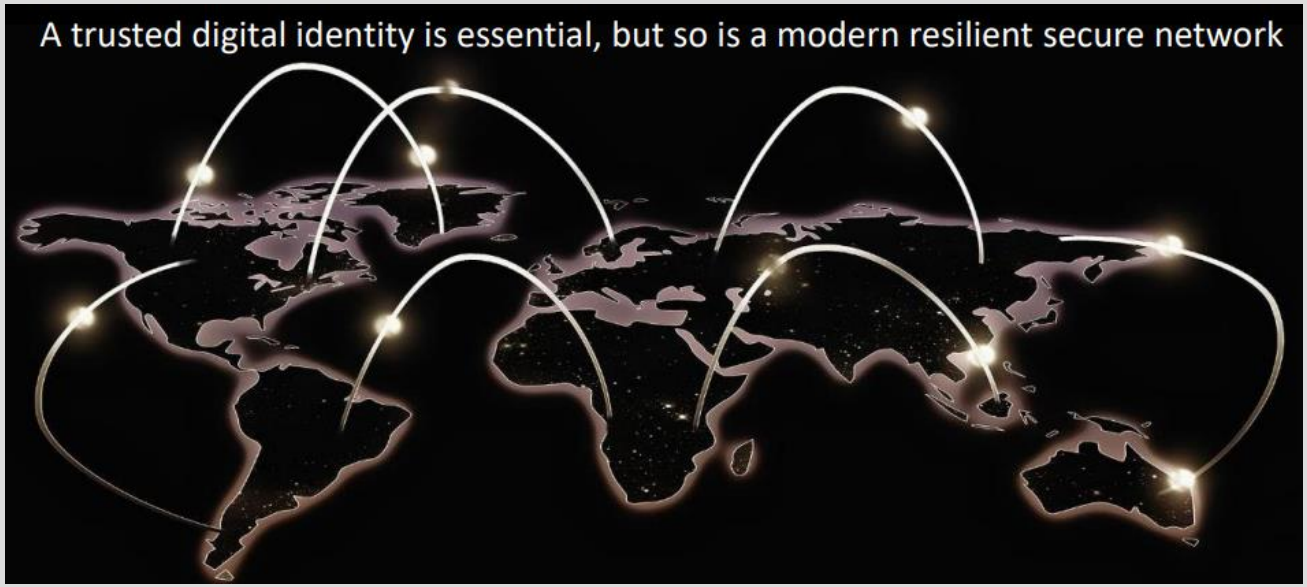
Indicadores

- BI CGTEC
  - Suporte à DECISÃO
    - SOC
    - Autoridades



Interconexões Seguras

SWIM:
Necessário prover segurança para as Interconexões



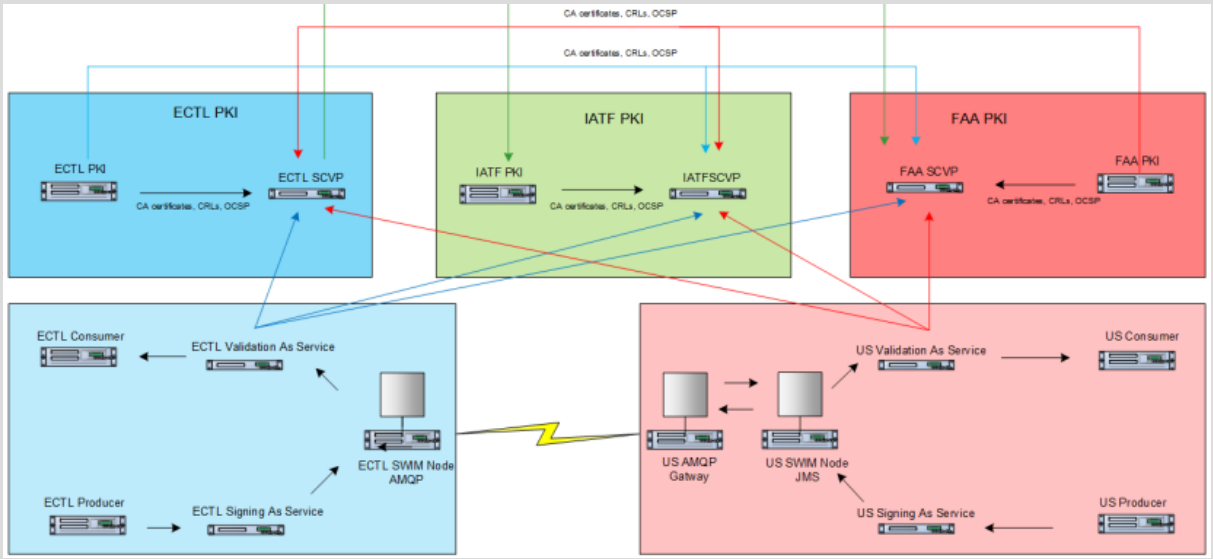
IATF

“Cyber threats are a growing global concern. To protect the safety of flight operations from these threats and ensure business continuity, the more integrated and automated air navigation system should continue to provide for trusted information exchanges on a global basis. This means that in a digital environment, communication parties should be able to identify themselves mutually and the information exchanged should not be able to be modified by unauthorized parties.” (What is the International Aviation Trust Framework? - Uniting Aviation)

Mais em: Informal Briefing on International Aviation Trust Framework - Council Briefings 2021 - ICAO TV

Interconexões Seguras: IATF

- Características
  - Identidade Digital: Baseado em Solução PKI.
  - Tráfego sobre IP (IPv6).
  - Isolada da INTERNET.
  - Resiliente (Alta Disponibilidade).
  - Endereçamento e Nomenclatura Padronizados.
  - Segura.



Interconexões Seguras

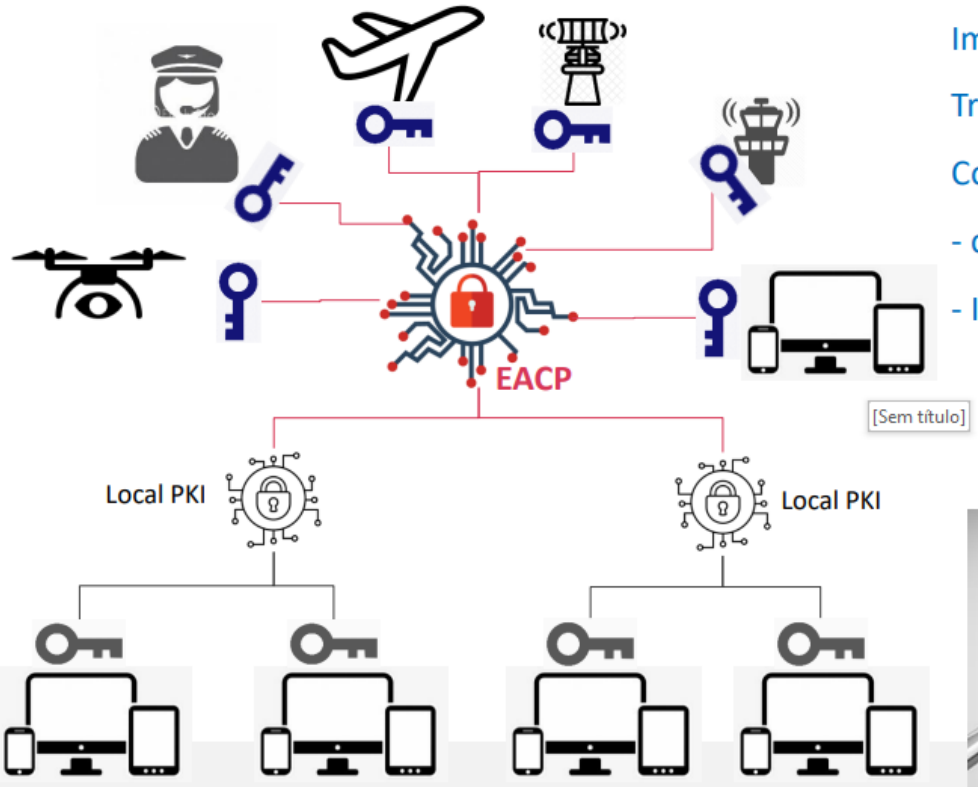
Co-financed by the Connecting Europe Facility of the European Union

SESAR DEPLOYMENT MANAGER

EUROCONTROL

European Aviation Common PKI (EACP)

A Building Block for the European Aviation Digital Infrastructure



[Sem título]

Improve security throughout aviation value chain

Trust Framework (governance, policies, procedures)

Common service reducing costs & providing:

- certificates
- Interoperability between existing PKI

Targeting hundreds of users

Roteiro

1. O que é o CGTEC?
2. NOC: Centro de Operações das Redes
3. INTRAER e ATN-Br
4. SOC: Centro de Operações da Segurança da Informação
5. Interconexões Seguras

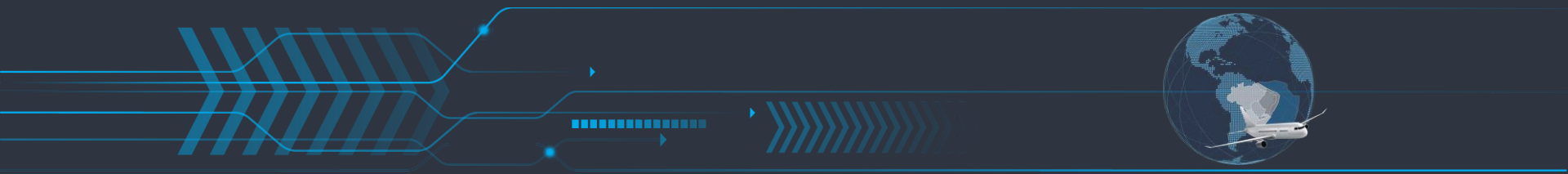
Objetivo

Conhecer as Redes e a Cyber-segurança do SISCEAB (Cn)

Parque de Material de Eletrônica
da Aeronáutica do Rio de Janeiro

Departamento
de Controle do Espaço Aéreo

FORÇA AÉREA BRASILEIRA
Asas que protegem o País



WWW.DECEA.GOV.BR