GOBIERNO DE ESPAÑA

MINISTERIO DE TRANSPORTES, MOVILIDAD Y AGENDA URBANA

AESA AGENCIA ESTATAL DE SEGURIDAD AÉREA

EASA HIGH LEVEL CYBERSECURITY CONFERENCE

Setting up a consistent and efficient regulation and oversight for cybersecurity risks in aviation in Spain

David Nieto
Director of Airports and Aviation Security
Madrid, 04-03-2020

F-SGA-FOR-01 2.0

Contents

1 National Cybersecurity Actors

2 Regulatory Framework

3 National Cybersecurity Framework

4 AESA Oversight System

5 Actions in 2020

Contents

1 National Cybersecurity Actors

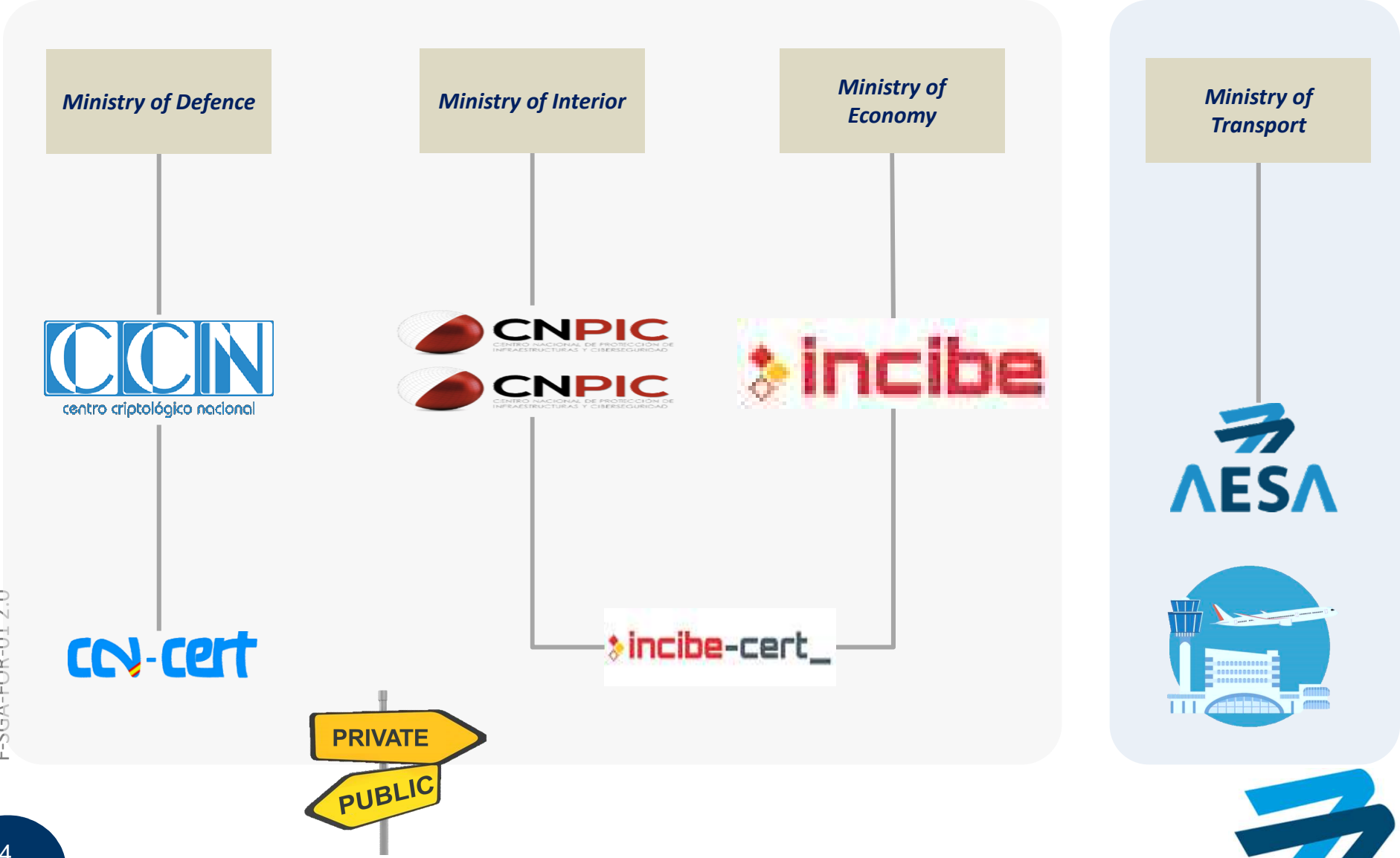
2 Regulatory Framework

3 National Cybersecurity Framework

4 AESA Oversight System

5 Tasks 2020

Entities involved



NATIONAL CRYPTOLOGIC CENTRE (CCN)

The National Cryptologic Centre is the body responsible for cybersecurity of public entities

- FUNCTIONS

REGULATION → ens Esquema Nacional de Seguridad 10 años Real Decreto 3/2010, de 8 de enero

TRAINING → AESA

INCIDENTS → ccn-cert

NATIONAL CRITICAL INFRASTRUCTURE PROTECTION AND CYBERSECURITY CENTRE

CNPIC
CENTRO NACIONAL DE PROTECCIÓN DE INFRAESTRUCTURAS Y CIBERSEGURIDAD

Appropriate Authority

Critical Infrastructures of Essential Services (NIS DIRECTIVE)

- Certification Framework

incibe-cert_

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

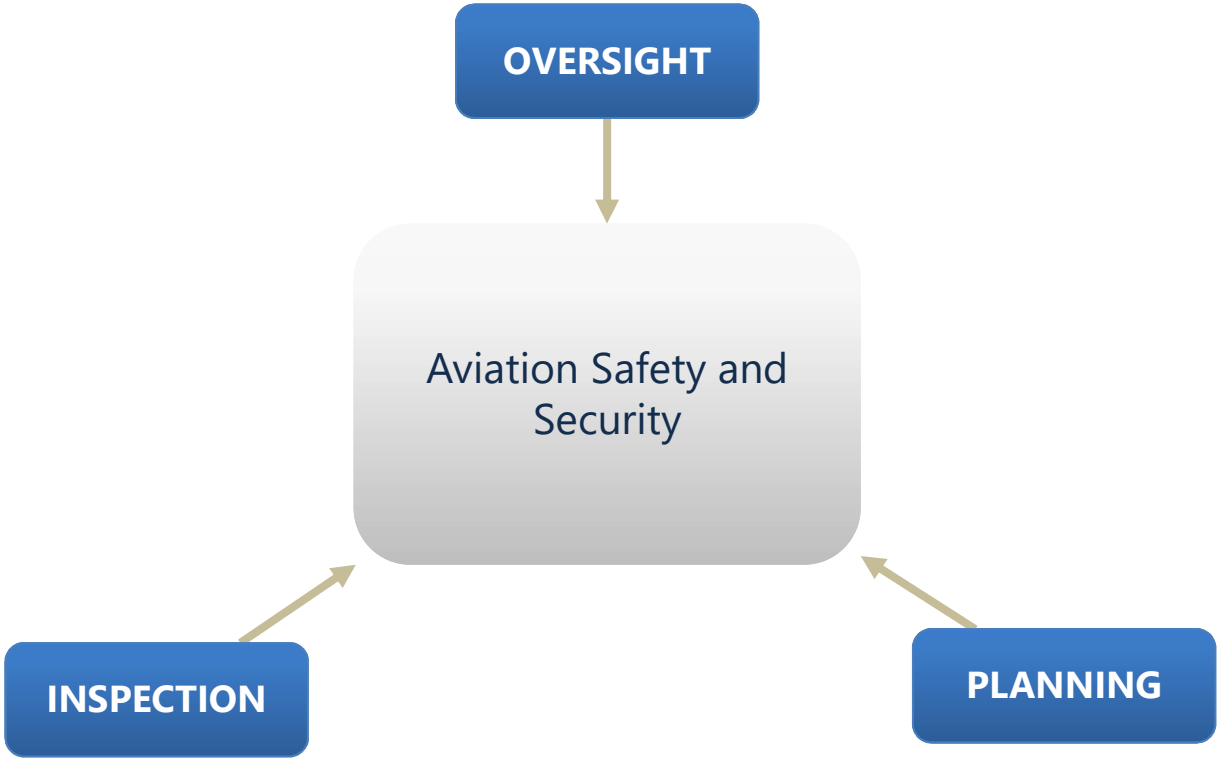
CNPIC
CENTRO NACIONAL DE PROTECCIÓN DE INFRAESTRUCTURAS Y CIBERSEGURIDAD

Formal agreement

SPANISH AVIATION SAFETY AND SECURITY AGENCY

State Body, created in 2008, that ensures that civil aviation standards are observed in all aeronautical activity in Spain.

With competencies with:



AESA - Organisational Structure

AESA - International cybersecurity groups

ECAC

- ✓ ECAC Cyber Threats to Civil Aviation Study Group

EASA

- ✓ ESCP
- ✓ STORM
- ✓ Cybersecurity (EM y WGs)

OACI

- ✓ Cyber threats Risk Assessment Working Group.

EUROCONTROL

- ✓ NEASCOG
- ✓ Cybersecurity training

NATIONAL CIBERSECURITY FOR CIVIL AVIATION WORKING GROUP

- Main aim coordination at national level
- Members representatives and observers
  - ✓ Aviation appropriate authorities (civil and military)
  - ✓ Ministry of interior and law enforcement bodies
  - ✓ Cybersecurity appropriate authorities
  - ✓ Industry
- Objectives:
  1. Monitoring and regulatory development
  2. Identification of ICT services in civil aviation
  3. Interlocution and representation before other institutions
  4. Information sharing (national and international level)

Contents

1 National Cybersecurity Actors

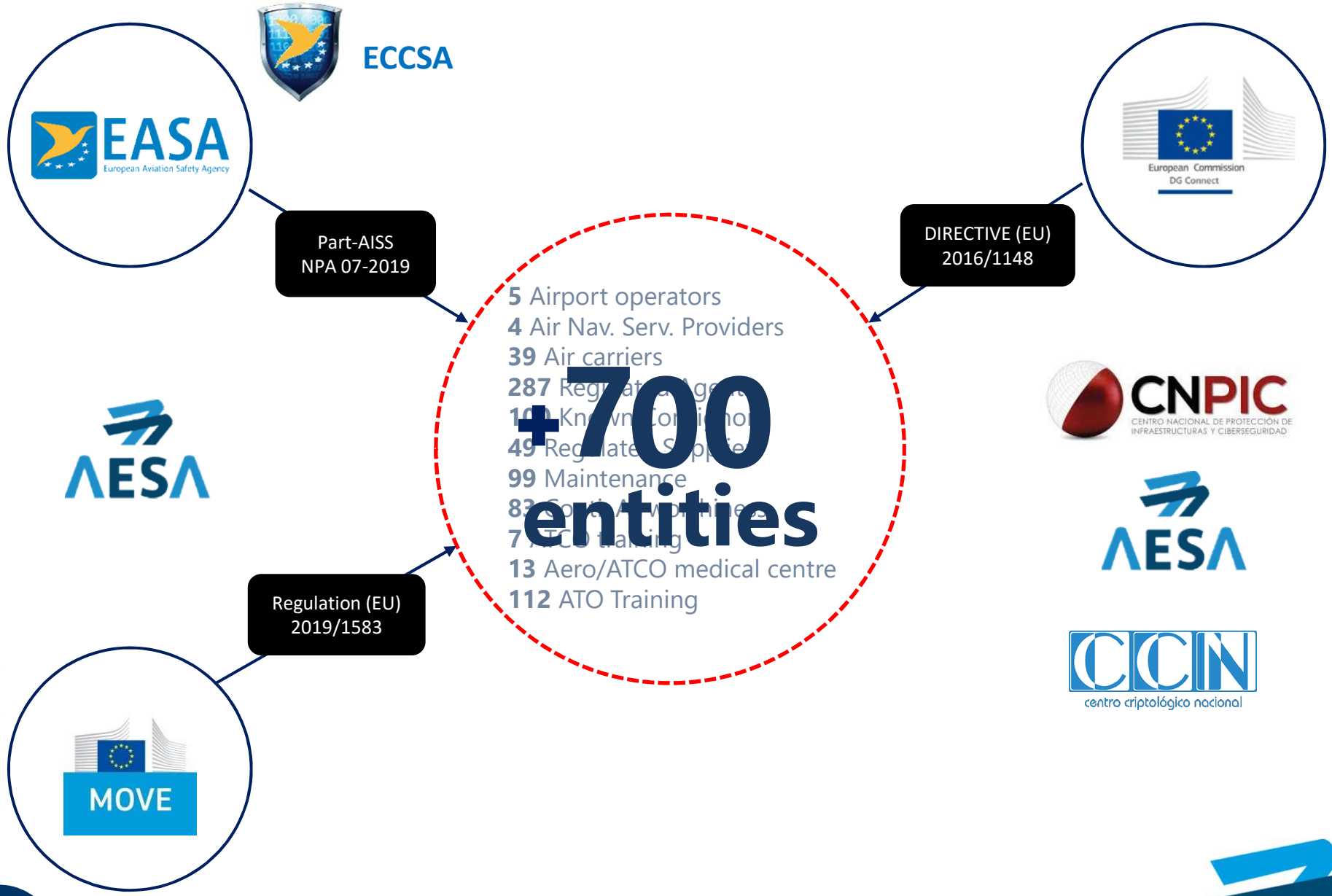
2 Regulatory Framework

3 National Cybersecurity Framework

4 AESA Oversight System

5 Tasks 2020

2.Regulatory framework



F-SGA-FOR-01 2.0

Regulation, scope and authorities with responsibilities

REGULATION		SCOPE					ES AUTHORITY	
UE	NATIONAL	AIRPORTS	AIR CARRIERS	ANSP	CAMO AND PART 145 ORGNAISATIONS	ATO AND ATCO ORGANISATIONS	CNPIC	AESA
Directive 2016/1148 (NIS Directive)	Royal Decree-Law 12/2018	●	●	●			●	●
Regulation (UE) 2015/1998	NCASP	●	●				●	●
Reglamento (UE) 2017/373	Transposition not needed			●				●
Part AISS (EASA) Regulation (UE) (NPA)	Transposition not needed	●	●	●	●	●		●

Transversal concept

Contents

1 National Cybersecurity Actors

2 Regulatory Framework

3 National Cybersecurity Framework

4 AESA Oversight System

5 Tasks 2020

National Cybersecurity Scheme for Public Sector

CCN centro criptológico nacional

ens Esquema Nacional de Seguridad

10 años

Real Decreto 3/2010, de 8 de enero

75 SECURITY MEASURES

based on the ISO/IEC 27001:2013

Organisational Framework
Set of measures related to the overall organization of security

4

Security Policy
Security Standards
Security Procedures
Authorisation Process

Operational Framework
Measures to protect the operation of t a system as an integral set of components with one purpose

31

Planning
Access Control
Operation
External Services
...

Protection Measures
Measures to protect specific assets, according to their nature, with the level required in each security dimension

40

Facilities and Infrastructures
Resource Management
Equipment protection
...

National Critical Infrastructure Protection and Cybersecurity Centre

Sources

CERTIFICATION SCHEME

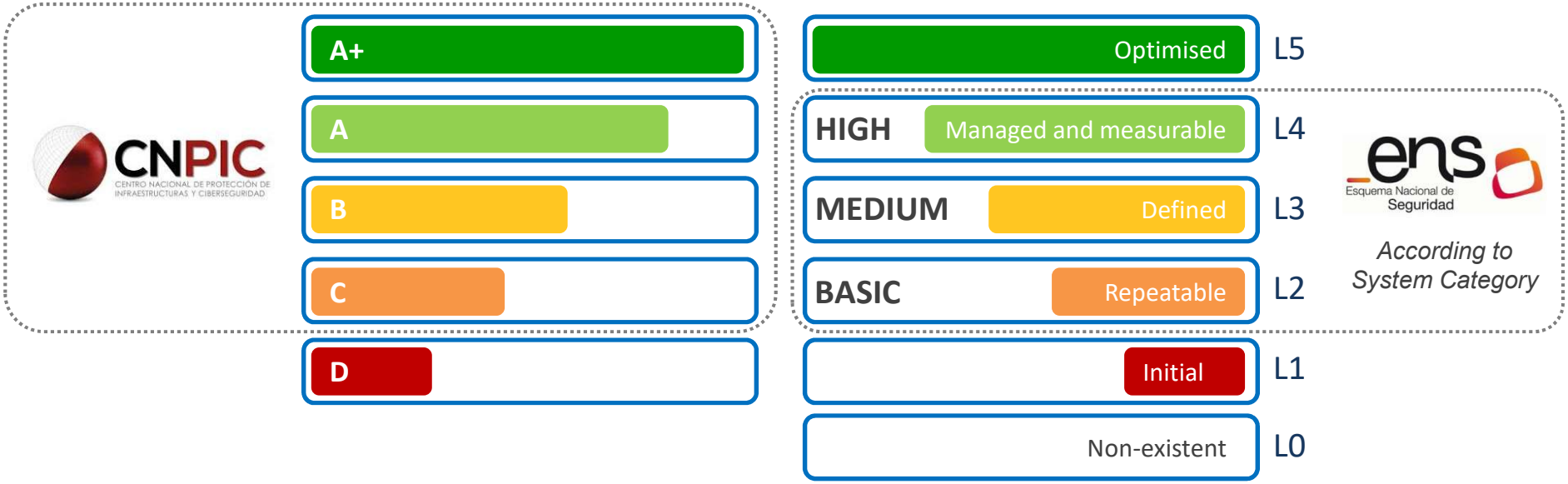
CNPIC
CENTRO NACIONAL DE PROTECCIÓN DE INFRAESTRUCTURAS Y CIBERSEGURIDAD

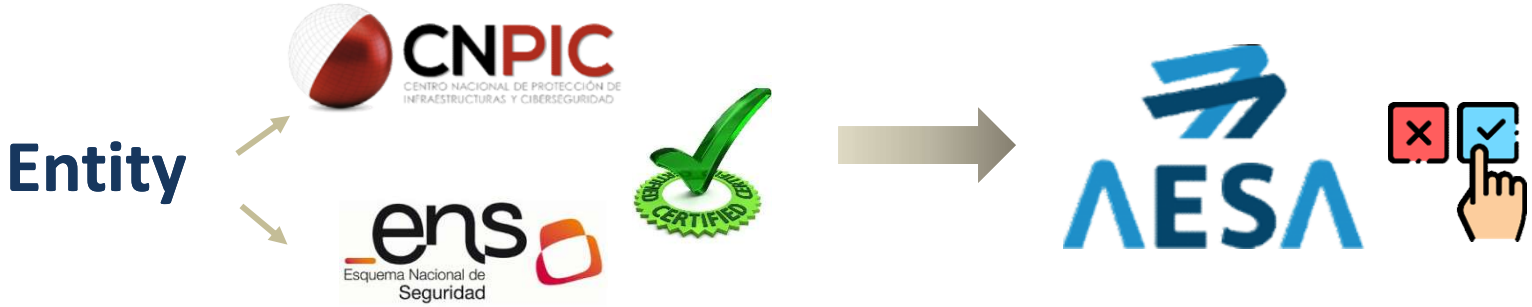
ens
Esquema Nacional de Seguridad

ENSI_C4V
certsi
Esquema Nacional de Seguridad Industrial

LEET SECURITY
ICT Rating
PASSED

Maturity Levels Security Measures





Contents

1 National Cybersecurity Actors

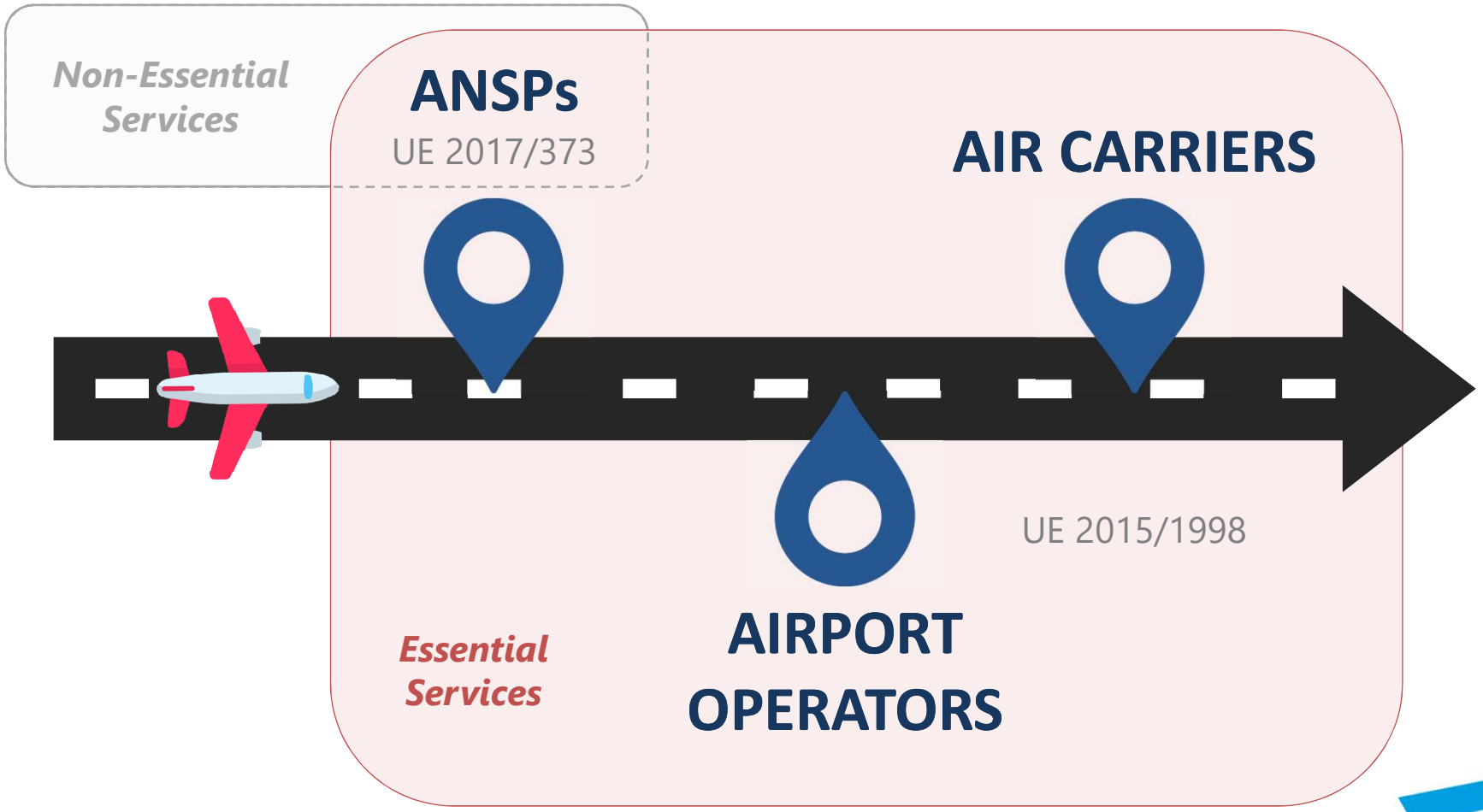
2 Regulatory Framework

3 National Cybersecurity Framework

4 AESA Oversight System

5 Tasks 2020

Inspections scheduled during 2020



OVERSIGHT: ESSENTIAL SERVICE PROVIDERS

Multidisciplinary Team

CNPIC
CENTRO NACIONAL DE PROTECCIÓN DE INFRAESTRUCTURAS Y CIBERSEGURIDAD

Leading Role
Controls

AESA
SECURITY

Coordination Role
Sectorial regulation

AESA
SAFETY

System Experts

COOPERATION AGREEMENT

F-SGA-FOR-01 2.0

4.AESA Oversight System

METHODOLOGY

PREPARATION

1. Choice of the audit subject and definition of objectives
2. Request for information from the entity
3. Submission of information
4. Analysis of information
5. Definition of the audit scope
6. Audit Planning

AUDIT

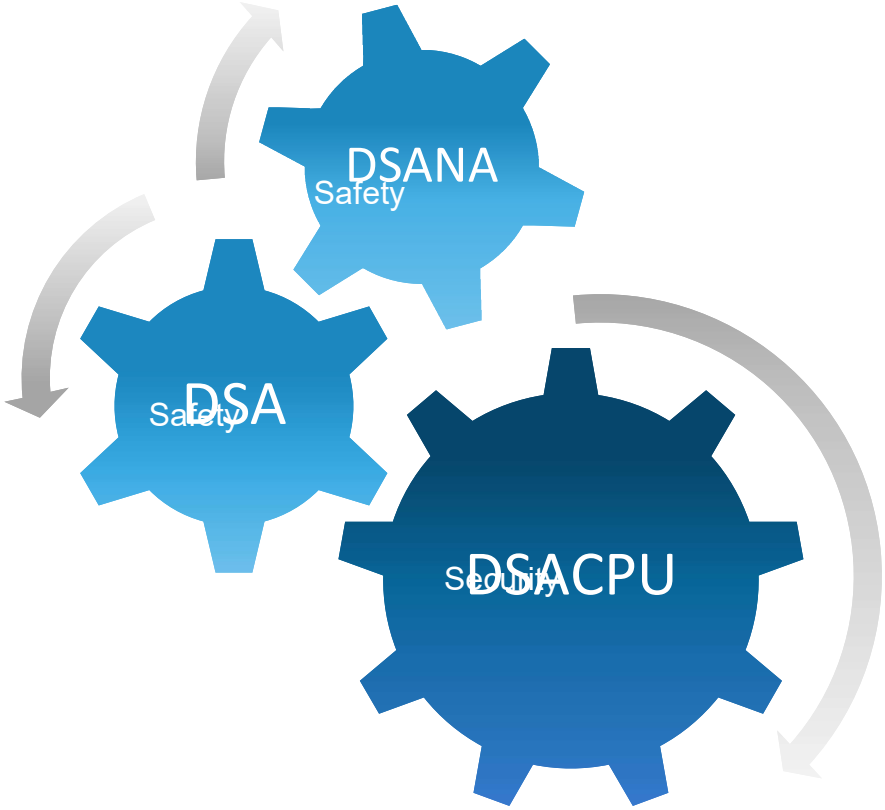
1. Kick-off meeting
2. Audit process
3. De-briefing meeting

AFTER THE AUDIT

1. Audit report
   Lessons learned and areas that need improvement
2. Post-audit information session
3. Submission of audit report

F-SGA-FOR-01 2.0

OVERSIGHT: NON-ESSENTIAL SERVICE PROVIDERS



Auditor Training

centro criptológico nacional

Contents

1 National Cybersecurity Actors

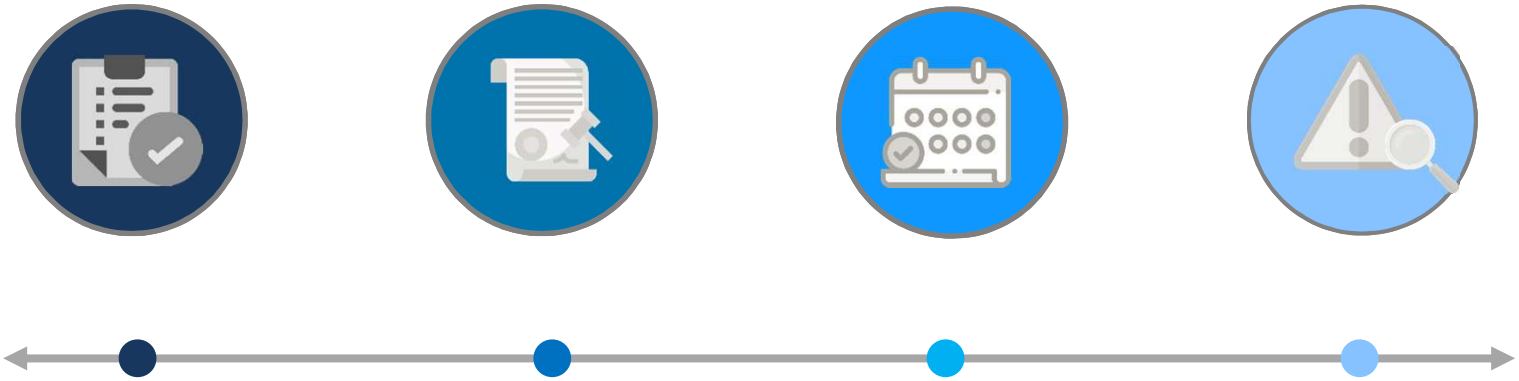
2 Regulatory Framework

3 National Cybersecurity Framework

4 AESA Oversight System

5 Tasks 2020

2020 Actions



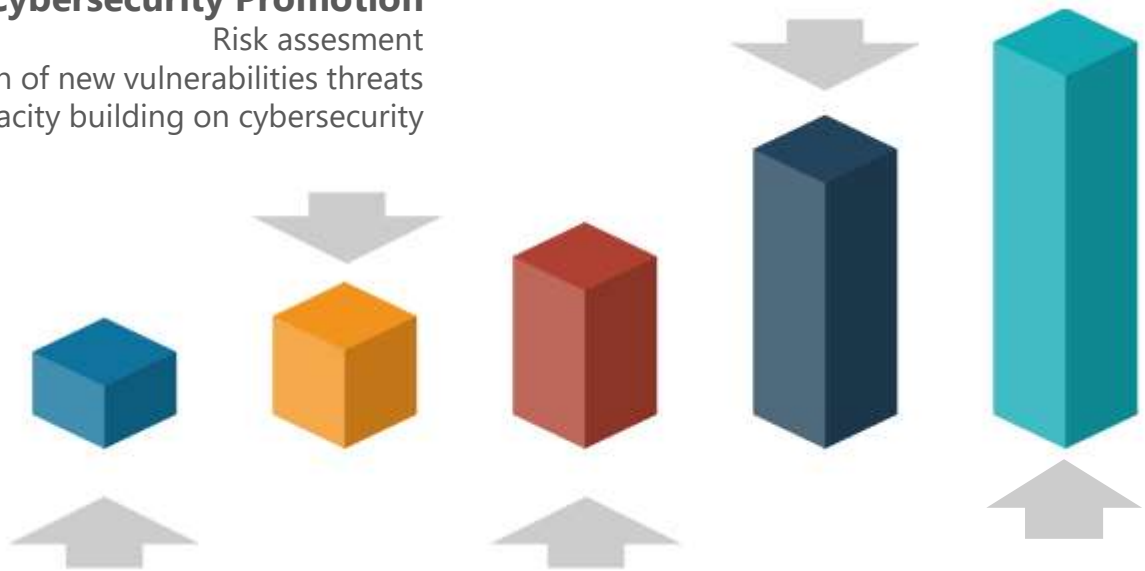
Audits	Inclusion of regulations NCASP	Multi-year plan Inspection	Risk Analysis at a national leveL

Capacity Building

Continous improvement…

International involvement
ICAO, ECAC, EASA, Eurocontrol, others

Cybersecurity Promotion
Risk assesment
Identification of new vulnerabilities threats
Capacity building on cybersecurity



Regulation
Development of national regulation
Promotion and follow up of cybersecurity standards
Development of specific recommendations

National Coordination
Coordination with national cybersecurity actors
Public private cooperation
Cybersecurity exercises
Information sharing
Incident response: CERTS

Oversight
Supervision of IT security systems.
Risk analysis, measures and protection mechanisms of operational systems.
Cybersecurity requirements: ICAO Annex 17, EU Regulation 1998/2015 and future NPA 2019-07

F-SGA-FOR-01 2.0

THANK YOU VERY MUCH!