CYBSEC-EXPO
THE CYBER SECURITY EVENT
2nd Edition

# CYBERSECURITY NELL'ERA DELLA NIS2: RISCHI E OPPORTUNITÀ NEL SETTORE AEROPORTUALE

CYBSEC-EXPO
THE CYBER SECURITY EVENT
2nd Edition

## NIS2: nuovi obblighi e implicazioni

**Alessandro Mancarella, Head of OT/IoT Security Consultancy, Cyber & Security Solutions Division, LEONARDO SPA**

**Modera: Marco Labricciosa Gallese**
**Membro Consiglio Direttivo per il Segmento IT**
**Direttore Operativo, A-ICE**

ORGANIZZATO DA

Air Tech Italy
Italian Airport Industry Association

LEONARDO
TECHNOLOGY FOR A SAFER FUTURE

Leonardo Cyber and Security Solutions

# NIS2

## Nuovi Obblighi e implicazioni

21/05/2025

Please avoid printing this colourful slide. Let’s save the planet together.

# LEONARDO

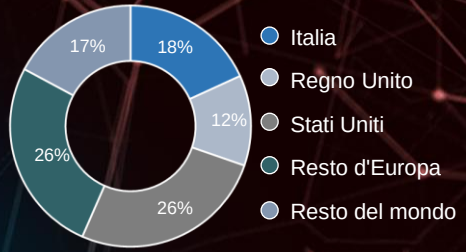
Leonardo è un gruppo industriale internazionale che realizza capacità tecnologiche in ambito Aerospazio, Difesa & Sicurezza. Protagonista dei principali programmi strategici a livello globale, è partner tecnologico di Governi, Amministrazioni della Difesa, Istituzioni e imprese.

**Settori**
Elicotteri, Aeronautica, Electronica, Cyber Security e Spazio

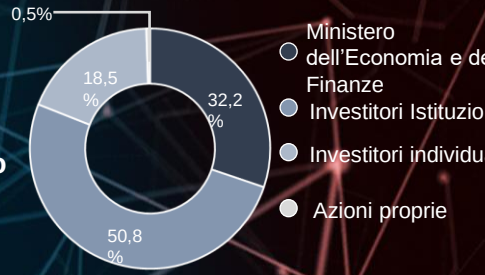
## Dipendenti


| € 17.8 bil. | € 20.9 bil. | € 1.5 bil. | € 44.2 bil. | € 2.5 bil. | 60,468 |
|---|---|---|---|---|---|
| revenues 2024 | Nuovi ordini 2024 | EBITA 2024 | Portafoglio 2024 | R&D | Dipendenti |

## Ricavi per Area geografica



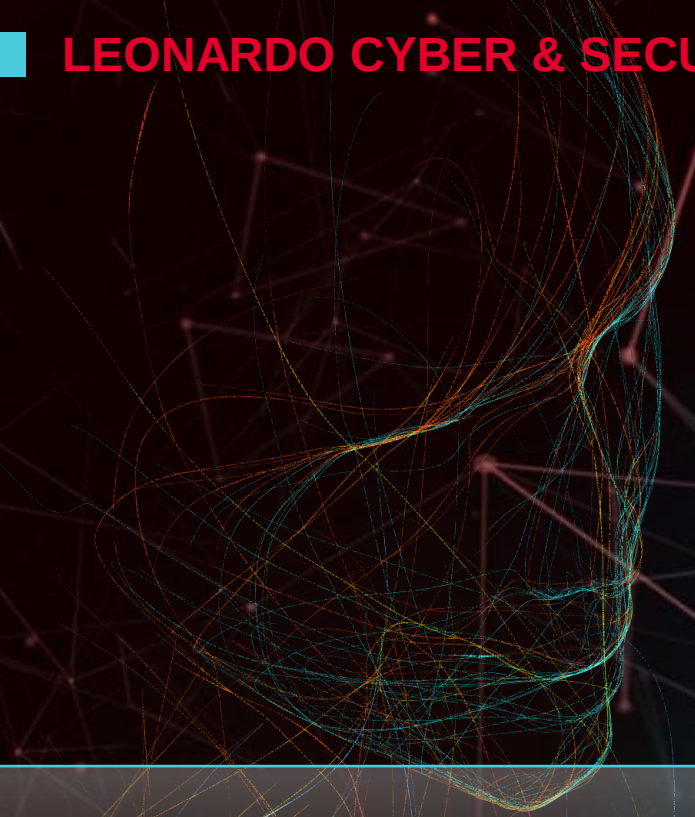

## Azionariato




## MAIN SHAREHOLDINGS AND JOINT VENTURES

| | | | | | | |
|---|---|---|---|---|---|---|
| LEONARDO UK 100% | KOPTER 100% | PZL-ŚWIDNIK 100% | AGUSTAWESTLAND PHILADELPHIA 100% | LEONARDO DRS 71.59% | TELESPAZIO 67% | GEM ELETTRONICA 65% |
| ATR 50% | ORIZZONTE SISTEMI NAVALI 49% | THALES ALENIA SPACE 33% | ELETTRONICA 31.33% | AVIO 29.63% | MBDA 25% | HENSOLDT 22.8% |

# LEONARDO CYBER & SECURITY SOLUTIONS



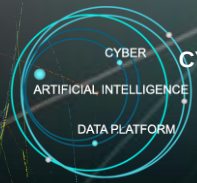
## VISIONE

***Paving a cyber secure, trustworthy and sustainable digital future***

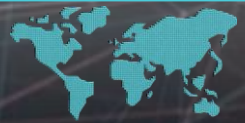
***We value your data, we protect what matters***

**2.750 PERSONE**

(50% CON FORMAZIONE STEM, 57% GIOVANI UNDER 30 SU TOTALE NUOVI INGRESSI NEL 2024)




**CYBER & RESILIENCE**
**SECURE DIGITAL & CLOUD**
**MISSION CRITICAL COMMS**



ITALY, UK,
USA, EU, KSA,
MALESIA

GLOBAL CYBERSEC CENTER

# CENTRO CYBER GLOBALE E FEDERATO

Trusted, Mission critical e AI-driven provider di **CYBERSECURITY**, con un modello logicamente e geograficamente federato, in grado di garantire la **CYBER MISSION ASSURANCE** dei Clienti


## I NUMERI CHIAVE

**177K**
Eventi di Sicurezza (EPS) gestiti/secondo

**500K+**
Vulnerabilità gestite/anno

**700+**
Certificazioni

**7,7M+**
Indicatori di Minaccia monitorati/anno

**9,1K**
Report intelligence personalizzati generati/anno

**29,1K**
Security Offence gestiti/anno

## TRUSTED

- Valenza tecnologica internazionale nella piena salvaguardia delle sovranità locali
- Garanzia dei principi di residenza nazionale ed europea dei dati

## MISSION CRITICAL

- Infrastrutture di erogazione dei servizi in ambienti protetti da minacce cyber e cinetiche
- Abilitato a gestire informazioni altamente sensibili

## AI-DRIVEN

- Threat Intelligence predittiva e Cyber Situational Awareness, modellazione & simulazione, rilevamento e risposta, rilevamento di deep fake
- Cyber observability e approccio known unknown

# Obblighi di Base | Ambiti di applicazione

Please avoid printing this colourful slide. Let’s save the planet together.

CYBSEC-EXPO
THE CYBER SECURITY EVENT
2nd Edition

# CYBERSECURITY NELL'ERA DELLA NIS2: RISCHI E OPPORTUNITÀ NEL SETTORE AEROPORTUALE

CYBSEC-EXPO
THE CYBER SECURITY EVENT
2nd Edition

## NIS2: nuovi obblighi e implicazioni

**Alessandro Mancarella, Head of OT/IoT Security Consultancy, Cyber & Security Solutions Division, LEONARDO SPA**

**Modera: Marco Labricciosa Gallese**
**Membro Consiglio Direttivo per il Segmento IT**
**Direttore Operativo, A-ICE**

ORGANIZZATO DA

Air Tech Italy
Italian Airport Industry Association

# Obblighi di Base | Determinazione ACN N°164179 (All. 1 e 2)

## GOVERN

- Cyber Role Model
- Valutazione personale autorizzato
- Cyber Security Risk Strategy
- Policy di Cyber Security
- Cyber Supply Chain Risk Management
- Monitoring & Improvement Processi cyber

## RECOVER

- Piano di ripristino dagli incidenti
- Comunicazione del piano di ripristino ai soggetti interessati

## RESPOND

- Incident Response Plan (CSIRP)
- Notifica degli incidenti

## DETECT

- Real Time Security Monitoring
- Strumenti di rilevazionbe (EDR, NDR, SIEM)


LEGENDA

*Misure di sicurezza aggiuntive per i soggetti essenziali*

*Requisiti applicabili almeno ai sistemi informativi e di rete rilevanti*

## IDENTIFY

- Asset Management -
- Gestione dei flussi -
- Cyber Risk Management -
- Vulnerability Management -
- Vulnerability Assessment e/o Penetration Test -
- Piani di Continuità Operativa, D&R e Gestione Crisi -

## PROTECT

- Gestione delle identità, autenticazione e controllo degli accessi -
- Verifiche periodiche di utenze e relative autorizzazioni -
- Accessi fisici -
- Consapevolezza e formazione del personale -
- Formazione al personale specializzato (compresi AdS) -
- Sicurezza dei dati (data-at-rest e data-in-transit) -
- Cifratura, MFA, Backup offline e test di ripristino -
- Hardening e configurazioni sicure -
- Dismissione sicura -
- Registrazione degli accessi da remoto degli AdS -
- Conservazione e centralizzazione dei log per il monitoraggio degli eventi di sicurezza -
- Sviluppo sicuro, Sicurezza delle reti e dei sistemi -
- Utilizzo di sistemi di comunicazione di emergenza -

# Responsabilità di OdA e Direttivi

## *Organi di Amministrazione e Direttivi ai sensi del D. Lgs. 138/2024*

### *Chi sono:*

***Persone fisiche responsabili*** dei soggetti NIS

***Rappresentanti legali*** dei soggetti NIS (con autorità di: rappresentazione, assunzione di decisioni, esercizio di controllo)

### *Responsabilità chiave:*

***Implementazione*** degli obblighi di base:

- Supervisione (***NON DELEGABILE***)
- Attuazione pratica (***DELEGABILE***)

***Violazione*** disposizioni NIS

## *Obblighi di base NIS (Determinazione ACN n. 164179) del 14 aprile 2025 Approvazione OdA e Direttivi*

*Organizzazione e politiche di sicurezza informatica*

*Valutazione dei rischi e piano di trattamento*

*Piano di adeguamento*

*Piano di gestione delle vulnerabilità*

*Piani operativi di cybersecurity che impattano le operazioni (Continuità Operativa, Ripristino, Gestione delle crisi)*

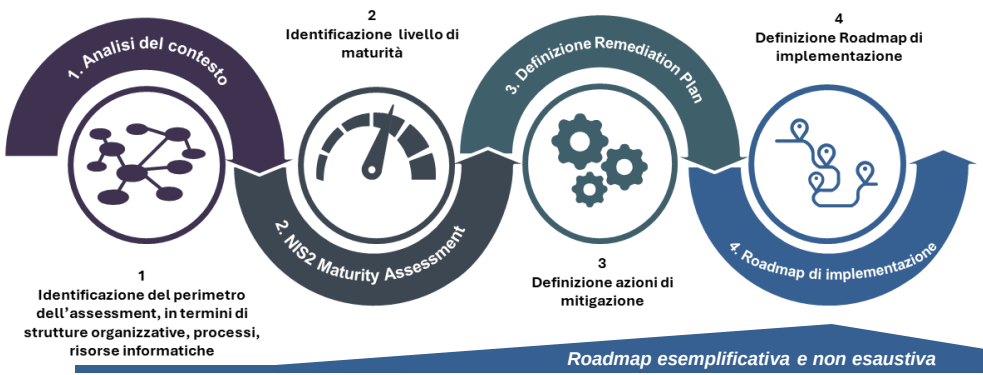
*Piano di formazione in materia di sicurezza informatica*

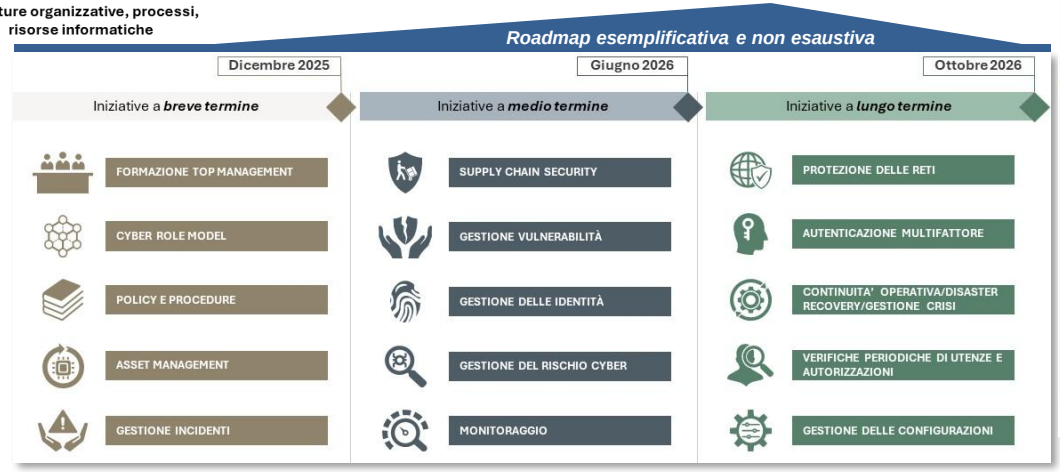
*Piano di risposta agli incidenti*

**Adempimenti in scadenza il 31 maggio**

- *I soggetti NIS devono caricare sul Portale ACN l'elenco dei membri di OdA e Direttivi (Codice Fiscale e PEC)*
- *I membri di OdA e Direttivi devono accedere al Portale ACN e accettare formalmente l'invito ad essere inseriti nell'elenco*

# Roadmap di Adeguamento | Prossimi Passi




1

**ANALISI DEL CONTESTO**

Vengono analizzati i seguenti ambiti:

- **Organizzativo** – analisi del modello di Governance della cyber security, andando a identificare e analizzare tutti i processi e le procedure di cyber.
- **Tecnologico** – analisi delle Infrastrutture tecnologiche a supporto dell'attuale erogazione del servizio in ambito NIS2.

2

**IDENTIFICAZIONE DEL LIVELLO DI MATURITA'**

Analisi della maturità dei controlli di sicurezza mediante interviste e analisi documentale dei processi cyber definiti nel contesto di analisi

3

**DEFINIZIONE PIANO DI REMEDIATION**

Analisi dei risultati e individuazione delle azioni da implementare per colmare i gap individuati durante la fase di Assessment. Il piano di Remediation contiene:

- Azioni di rientro di tipo Organizzative/Procedurali.
- Azioni di rientro di tipo tecnologiche.

4

**DEFINIZIONE ROADMAP DI IMPLEMENTAZIONE**

La pianificazione delle iniziative all'interno della roadmap di implementazione viene svolta coerentemente con i seguenti ***driver***:

- Propedeuticità delle iniziative, per garantire il corretto ordine di implementazione.
- **Priorità** in funzione delle strategie ed agli obiettivi di business aziendali.
- **Sinergia** con le altre iniziative già in corso o pianificate.
- ***Complessità operativa*** dell'implementazione, per una gestione ottimale delle risorse.
- **Scadenze normative** (ad esempio, l'obbligo di notifica incidenti verso l'Autorità a partire dal 1 Gennaio 2026).

# Thank you
# for your attention

Please avoid printing this colourful slide. Let’s save the planet together.

leonardo.com