ASSOLOMBARDA

ASSOLOMBARDA SERVIZI
SOCIETÀ BENEFIT

CYBERSECURITY NELLA FILIERA

Difesa & Aerospace

Percorso di ingresso per una PMI italiana: obblighi normativi, certificazioni e focus cyber

ASSOLOMBARDA

ASSOLOMBARDA SERVIZI
SOCIETÀ BENEFIT

Il percorso in cinque tappe

Per una PMI esistente che vuole entrare nella filiera difesa/aerospace

01

Definire l'offerta

Servizi, prodotti o sviluppo OT/embedded: capire dove c'è un ponte naturale con il core business

02

Obblighi e certificazioni

NIS2, CRA e Perimetro di Sicurezza; poi ISO 27001, ISO 9001, AQAP NATO

03

Abilitazioni di sicurezza

NOS personale e AP/NOSI/NOSIS aziendali, rilasciati dall'UCSe per trattare informazioni classificate

04

Qualifica fornitori

Registrazione sui portali vendor di Leonardo, Fincantieri, MBDA, Thales Alenia Space

05

Visibilità e rete

Adesione AIAD, partecipazione a Cybertech Europe e fiere di settore

ASSOLOMBARDA

ASSOLOMBARDA SERVIZI
SOCIETÀ BENEFIT

Obblighi normativi obbligatori: NIS2, PSNC e CRA

Il punto di partenza per ogni PMI: tre normative da rispettare per legge, prima ancora delle certificazioni di settore

NIS2

Direttiva UE 2022/2555 (D.Lgs. 138/2024): gestione del rischio e notifica incidenti per soggetti essenziali e importanti in 18 settori critici

Perimetro di Sicurezza Nazionale

D.L. 105/2019: tutela le reti e i sistemi ICT critici per lo Stato nei settori difesa e spazio/aerospazio, tra gli altri

CRA — Cyber Resilience Act

Regolamento (UE) 2024/2847: sicurezza by design obbligatoria per hardware e software con elementi digitali venduti nell'UE

Le prossime tre slide approfondiscono gli obblighi concreti per le aziende di ciascuna normativa.

ASSOLOMBARDA

ASSOLOMBARDA SERVIZI
SOCIETÀ BENEFIT

Approfondimento: NIS2

Obblighi di gestione del rischio cyber e notifica incidenti per soggetti essenziali e importanti

Cos'è

Direttiva UE 2022/2555 recepita con D.Lgs. 138/2024: introduce misure di gestione del rischio cyber e obblighi di notifica per i soggetti critici, sotto la vigilanza dell'ACN.

Chi è coinvolto

Soggetti essenziali e importanti in 18 settori critici (energia, trasporti, sanità, digitale, spazio, tra gli altri) e i loro fornitori ICT rilevanti lungo la supply chain.

Obblighi principali per l'azienda

- Governance: responsabilità non delegabile del board, formazione obbligatoria degli organi apicali
- Gestione del rischio: misure tecniche e organizzative proporzionate (accessi, crittografia, backup, continuità)
- Notifica incidenti: pre-allerta entro 24h e notifica entro 72h al CSIRT Italia
- Sicurezza della supply chain: mappatura e valutazione dei fornitori ICT rilevanti
- Registrazione e categorizzazione: iscrizione al portale ACN e classificazione di attività e servizi
- Sanzioni fino a 10 mln € o 2% del fatturato (essenziali), 7 mln € o 1,4% (importanti)

Percorso pratico: registrazione sul portale ACN → gap analysis → misure di sicurezza di base entro ottobre 2026

ASSOLOMBARDA

ASSOLOMBARDA SERVIZI
SOCIETÀ BENEFIT

Approfondimento: Cyber Resilience Act (CRA)

Requisiti di cybersecurity obbligatori per hardware e software venduti nel mercato UE

Cos'è

Regolamento (UE) 2024/2847: impone requisiti di sicurezza by design e by default per tutti i prodotti con elementi digitali immessi sul mercato europeo, lungo l'intero ciclo di vita.

Chi è coinvolto

Fabbricanti, importatori e distributori di hardware, software, firmware e dispositivi connessi (inclusi componenti embedded per difesa/aerospace), incluse le PMI.

Le scadenze chiave del CRA

11 settembre 2026 — Obblighi di segnalazione

Notifica di vulnerabilità sfruttate e incidenti gravi: allarme in 24h, notifica completa in 72h

11 dicembre 2027 — Piena applicazione

Requisiti essenziali di sicurezza, documentazione tecnica e marcatura CE obbligatori per la vendita nell'UE

Sanzioni

Fino a 15 milioni di euro o al 2,5% del fatturato globale annuo per le violazioni principali

Il CRA integra la NIS2: sicurezza dei prodotti (CRA) e sicurezza dei processi e dell'organizzazione (NIS2).

ASSOLOMBARDA

ASSOLOMBARDA SERVIZI
SOCIETÀ BENEFIT

Approfondimento: PSNC

Le reti e i sistemi ICT critici per la sicurezza dello Stato, tra cui difesa e aerospazio

Cos'è

Istituito dal D.L. 105/2019 (L. 133/2019): individua reti, sistemi e servizi ICT da cui dipendono funzioni e servizi essenziali dello Stato, sotto il coordinamento dell'ACN.

Chi è coinvolto

Soggetti pubblici e privati nei settori difesa, spazio/aerospazio, energia e telecomunicazioni. Coinvolge anche i fornitori ICT tramite la valutazione CVCN.

Obblighi principali

Censimento degli asset

Elenco annuale dei beni ICT strategici, secondo i criteri del DPCM 131/2020

Misure di sicurezza e notifica

Misure del DPCM 81/2021 e notifica obbligatoria degli incidenti al CSIRT ACN

Valutazione CVCN

Comunicazione preventiva al Centro di Valutazione e Certificazione Nazionale per l'acquisto di beni e servizi ICT critici

Sanzioni fino a 1,8 milioni di euro (fino al triplo in caso di reiterazione). Rilevante anche per i fornitori ICT di soggetti Perimetro.

ASSOLOMBARDA

ASSOLOMBARDA SERVIZI
SOCIETÀ BENEFIT

Focus cybersecurity: cosa serve davvero

Difesa e aerospace richiedono competenze più vicine all'OT/ICS che all'IT tradizionale

NIST 800-171

Protezione di informazioni controllate non classificate (CUI); rilevante per supply chain USA/NATO

DO-326A / ED-202A

Cybersecurity applicata a sistemi avionici, in coppia con DO-178C per il software di bordo

Sicurezza OT/ICS

Protocolli industriali (Modbus, CAN bus), sistemi embedded e real-time, non solo reti IT d'ufficio

CMMC (se USA)

Richiesto solo se l'azienda entra nella supply chain di player con contratti DoD americani

Le slide successive approfondiscono ciascuno di questi quattro temi nel dettaglio.

ASSOLOMBARDA

ASSOLOMBARDA SERVIZI
SOCIETÀ BENEFIT

Certificazioni aziendali abilitanti

Standard internazionali richiesti per essere un fornitore credibile nella filiera

ISO 9001

BASE

Sistema di gestione qualità: prerequisito di base richiesto a monte di qualsiasi fornitura

ISO/IEC 27001

CYBER

Gestione della sicurezza delle informazioni: quasi obbligatoria per fornitori IT/cyber del settore

AQAP 2110 / 2210

NATO

NATO Quality Assurance: necessaria per fornire prodotti/software su programmi NATO

NOSI

UCSe

Nulla Osta Sicurezza Industriale (UCSe): abilita l'azienda a trattare informazioni classificate

ASSOLOMBARDA

ASSOLOMBARDA SERVIZI
SOCIETÀ BENEFIT

Approfondimento: ISO/IEC 27001

Lo standard internazionale per la gestione della sicurezza delle informazioni in azienda

Cos'è

Standard internazionale (ISO/IEC 27001:2022) che definisce i requisiti per un Sistema di Gestione della Sicurezza delle Informazioni (ISMS), con approccio basato sul rischio.

Chi la richiede

Fornitori IT/cyber della filiera difesa e aerospace: quasi sempre un prerequisito nei bandi e nella qualifica fornitori di Leonardo, Fincantieri e Thales Alenia Space.

Requisiti principali

Risk assessment e trattamento del rischio

Identificazione sistematica delle minacce alla sicurezza delle informazioni e definizione delle misure di mitigazione

Controlli dell'Allegato A

93 controlli in 4 categorie: organizzativi, relativi alle persone, fisici e tecnologici

Sistema di gestione e miglioramento continuo

Politiche, ruoli e responsabilità definiti, ciclo Plan-Do-Check-Act (PDCA) e riesame periodico della direzione

Percorso di certificazione: gap analysis → implementazione ISMS e controlli → audit di certificazione (Stage 1 e Stage 2)

ASSOLOMBARDA

ASSOLOMBARDA SERVIZI
SOCIETÀ BENEFIT

Approfondimento: NIST 800-171

Protezione delle informazioni controllate non classificate (CUI) nella supply chain

Cos'è

Standard del NIST con 14 famiglie di controlli per proteggere informazioni sensibili non classificate quando risiedono su sistemi di aziende private, non federali. Nasce in America con uno scopo specific.

Quando serve

Quando l'azienda è subfornitrice, diretta o indiretta, di realtà con contratti del Dipartimento della Difesa USA (clausole DFARS) o programmi che trattano CUI. Può essere utilizzata come linea guida di sicurezza.

Famiglie di controllo principali

- Controllo degli accessi e autenticazione
- Audit e tracciabilità delle attività
- Gestione della configurazione dei sistemi
- Risposta agli incidenti di sicurezza
- Protezione dei sistemi e delle comunicazioni
- Valutazione e gestione del rischio

Percorso pratico: self-assessment → System Security Plan (SSP) → Plan of Action & Milestones (POA&M)

ASSOLOMBARDA

ASSOLOMBARDA SERVIZI
SOCIETÀ BENEFIT

Approfondimento: DO-326A / ED-202A

Lo standard di cybersecurity per la certificazione di aeronavigabilità

Cos'è

Standard (DO-326A negli USA, ED-202A in Europa) che integra la sicurezza informatica nel processo di certificazione di aeronavigabilità dei sistemi avionici.

Chi lo richiede

EASA e FAA, le autorità di certificazione aeronautica europea e americana, per qualunque sistema avionico immesso su un velivolo certificato.

Si integra con altri standard avionici

DO-178C

Sviluppo e certificazione del software di bordo

DO-254

Sviluppo e certificazione dell'hardware avionico

DO-326A / ED-202A

Security risk assessment lungo tutto il ciclo di vita

Processo tipico: security risk assessment → security development → security verification & test

ASSOLOMBARDA

ASSOLOMBARDA SERVIZI
SOCIETÀ BENEFIT

Approfondimento: sicurezza OT/ICS

Perché difesa e aerospace richiedono un approccio diverso dall'IT tradizionale

IT vs OT: priorità diverse

L'IT classico privilegia la riservatezza dei dati; l'OT (Operational Technology) privilegia la continuità operativa e la sicurezza fisica (safety), perché un guasto può avere conseguenze reali, non solo digitali.

Protocolli e bus tipici

Modbus e CAN bus per sistemi industriali ed embedded; MIL-STD-1553 e ARINC 429 per i bus dati avionici e militari.

IEC 62443

Il framework internazionale di riferimento per la sicurezza dei sistemi di controllo industriale (ICS/SCADA), sempre più richiamato anche nei capitolati difesa e aerospace.

Competenze chiave da costruire

- Sistemi embedded e RTOS (real-time operating systems)
- Segmentazione e monitoraggio delle reti industriali
- Analisi del rischio su asset fisici e safety-critical

ASSOLOMBARDA

ASSOLOMBARDA SERVIZI
SOCIETÀ BENEFIT

Abilitazioni di sicurezza: il quadro ufficiale

Persone fisiche e imprese: due percorsi distinti, con un'unica autorità che li rilascia

DIS
Dipartimento Informazioni per la Sicurezza

→

UCSe
Ufficio Centrale per la Segretezza (rilascia le abilitazioni)

L'UCSe è l'ufficio del DIS che materialmente concede NOS, AT, AP, NOSI e NOSIS dopo le verifiche di affidabilità.

Persone fisiche

NOS — Nulla Osta di Sicurezza

Abilitazione personale richiesta dall'ente o impresa di appartenenza per chi deve conoscere informazioni classificate RISERVATISSIMO o superiore.

AT — Abilitazione Temporanea

Richiedibile insieme al NOS in caso di urgenti e comprovate esigenze, in attesa del rilascio definitivo.

Imprese (abilitazione industriale)

AP — Abilitazione Preventiva

Per partecipare a gare classificate RISERVATISSIMO/SEGRETO; non abilita all'esecuzione del contratto

NOSI — Nulla Osta Sicurezza Industriale

Per gare SEGRETISSIMO ed eseguire lavori/forniture classificate RISERVATISSIMO, SEGRETO o SEGRETISSIMO

NOSIS — NOSI Strategico

Livello SEGRETO o superiore, riservato a imprese in settori strategici

Fonte: UCSe — Legge 124/2007 artt. 9 e 42; DPCM 5/2015 artt. 23-52. Per informazioni RISERVATO non serve abilitazione, ma vanno comunque seguite le prescrizioni di tutela.

ASSOLOMBARDA

ASSOLOMBARDA SERVIZI
SOCIETÀ BENEFIT

Glossario essenziale

Le sigle di questa presentazione spiegate in una riga, per chi parte da zero

DIS	Dipartimento delle Informazioni per la Sicurezza: il dipartimento di intelligence della Presidenza del Consiglio.
UCSe	Ufficio Centrale per la Segretezza: l'ufficio del DIS che rilascia le abilitazioni di sicurezza.
NOS	Nulla Osta di Sicurezza: abilita una persona a conoscere informazioni classificate.
NOSI	Nulla Osta Sicurezza Industriale: abilita un'azienda a trattare informazioni classificate.
AP	Abilitazione Preventiva: serve solo per partecipare a una gara classificata, non per eseguirla.
NOSIS	NOSI Strategico: versione rafforzata del NOSI per imprese in settori strategici.
ISO 27001	Certificazione internazionale sulla gestione della sicurezza delle informazioni in azienda.
AQAP	Standard NATO di garanzia qualità per i fornitori di programmi militari.
NIST 800-171	Standard USA per proteggere dati sensibili non classificati presso fornitori privati.
CMMC	Certificazione richiesta dal Dipartimento della Difesa USA ai propri fornitori cyber.
DO-326A / ED-202A	Standard di cybersecurity per certificare l'aeronavigabilità dei sistemi avionici.
IEC 62443	Standard internazionale per la sicurezza dei sistemi di controllo industriale (OT/ICS).
AIAD	Associazione italiana delle aziende di aerospazio, difesa e sicurezza.
OT / ICS	Operational Technology / Industrial Control Systems: i sistemi che controllano macchine e impianti, non solo dati.

ASSOLOMBARDA

ASSOLOMBARDA SERVIZI
SOCIETÀ BENEFIT

Player e canali di ingresso

Dove qualificarsi e farsi conoscere nella filiera italiana ed europea

Portali fornitori

Ad esempio Leonardo, Fincantieri: registrazione e vendor qualification

Cybertech Europe

Fiera di riferimento per incontrare buyer e integratori di sistema del settore

Assocazioni di riferimento

Associazione italiana aerospazio, difesa e sicurezza: accesso a bandi, eventi, partnership
Distretto Aeronautico Lombardo

ASD Europe

Federazione europea collegata ad AIAD: visibilità anche sul mercato continentale

ASSOLOMBARDA

ASSOLOMBARDA SERVIZI
SOCIETÀ BENEFIT

Prossimi passi concreti

1. Definire l'offerta cyber specifica (servizi, prodotto, OT/embedded) a partire dal core business attuale
2. Avviare ISO 27001 e ISO 9001 se non già presenti: sono il prerequisito per qualsiasi fornitura
3. Registrarsi sui portali fornitori dei grandi player e aderire ad AIAD per visibilità nella filiera
4. Valutare se servono NOS/NOSI in base al tipo di informazioni trattate nei progetti target

Contatti

Miriam Ieraci
Senior Professional Cybersecurity
Area Industria Energia e Innovazione
@ miriam.ieraci@assolombarda.it
Tel.: 0258370634 - Mob.: +39 3894724835

ASSOLOMBARDA