

Cybersecurity per le PMI

Milano, 20/04/2026



ASSOLOMBARDA



Shape the future
with confidence

Agenda

- | | | | | | |
|---|---------------|--------------------------------------|---|---------------|--|
| 1 | 09:30 - 10:00 | Accredito partecipanti | 5 | 10:50 - 11:10 | Aree di sicurezza nelle PMI
EY |
| 2 | 10:00 - 10:10 | Apertura dei lavori
Assolombarda | 6 | 11:10 - 11:30 | Azioni concrete per aumentare la postura cyber
EY |
| 3 | 10:10 - 10:30 | Panorama degli incidenti cyber
EY | 7 | 11:30 - 11:50 | ForgIA
Assolombarda + EY |
| 4 | 10:30 - 10:50 | Normativa cyber
Assolombarda | 8 | 11:50 - 12:00 | Chiusura dei lavori |

Referenti EY



Francesco Suffredini
Tech Risk Italian Leader
Francesco.Suffredini@it.ey.com



Davide Benevolo
Tech Risk Europe West Quality Leader
Davide.Benevolo@it.ey.com



Roberto Piuca
Data & AI Private Market
Roberto.Piuca@it.ey.com



Panorama degli incidenti cyber



Panorama globale e italiano

+48.7%

Incidenti cyber globali

% di incremento di incidenti cyber noti dal 2024 al 2025, **il valore incrementale più alto mai registrato**

- Cresce non solo il numero degli incidenti, ma anche la gravità: oltre 8 incidenti su 10 sono classificati come **High**, **Critical** o **Extreme**
- Compare la categoria **Extreme**, collocata al di sopra di Critical, per incidenti devastanti e sistemici
- Il **cybercrime** è dominante: rappresenta circa 9 incidenti su 10, segno di una vera e propria industrializzazione dell'attacco

+42.0%

Incidenti cyber in Italia

% di incremento di incidenti cyber noti dal 2024 al 2025

- L'Italia è un **bersaglio rilevante**: rappresenta circa 1 incidente su 10 dei totali mondiali noti
- I settori più colpiti includono la **pubblica amministrazione**, il **manifatturiero**, i **trasporti** e i **servizi**
- Non ci troviamo in uno scenario emergenziale, ma in una **nuova normalità di rischio elevato**

~25.0%

Attacchi alle PMI

% di PMI italiane che nel 2025 dichiarano di aver subito almeno un attacco negli ultimi 3 anni, **un valore triplicato rispetto al 2024**

- Le PMI rappresentano il **target ideale del cybercrime**, che è ormai industrializzato, scalabile e orientato al massimo ritorno economico, non alla complessità tecnica
- Le PMI sono **nodi critici di filiera**: oltre 8 su 10 operano con grandi imprese, pubbliche amministrazioni e infrastrutture critiche, diventando così un vettore di accesso indiretto

Gli scenari di incidente e gli impatti sulle PMI



Il phishing e il social engineering sono aumentati tra il 2024 e il 2025 del 75% a livello globale e del 66% a livello italiano. **Le PMI sono particolarmente vulnerabili** a questa tipologia di attacchi a causa di processi decisionali informali e fiducia personale come meccanismo di sicurezza

Impatti: Perdita finanziaria immediata - Difficoltà nel recupero dei fondi - Responsabilità interna e tensione organizzativa

200k€ - 500k€

Impatto economico medio per una PMI italiana che ha subito un attacco di phishing o di social engineering



Gli incidenti cyber nel settore manifatturiero sono aumentati tra il 2024 e il 2025 sia a livello globale (+79%) che a livello italiano (+14%). Il 16% degli incidenti globali avviene in Italia, dove **le PMI rappresentano la maggioranza di settore**

Impatti: Blocco della produzione - Penali sugli ordini - Danno di cassa immediato

40k€ - 360k€

Costo giornaliero medio di downtime per una PMI nel settore manifatturiero italiano colpita da un incidente cyber



La distribuzione delle minacce cyber relative alle terze parti ha raggiunto un peso del 10.6% sul totale europeo. Una **PMI compromessa** diventa la **porta d'ingresso nella filiera** per la propagazione degli incidenti

Impatti: Sospensione dei rapporti commerciali - Richieste di verifica e audit - Esclusione dalla filiera - Danno reputazionale

1.5M€ - 4M€

Impatto economico medio di una grande azienda italiana che ha subito un incidente cyber in seguito alla compromissione di una PMI della filiera

Minacce AI e nuove modalità di attacco

L'AI non è solo una tecnologia, è un **moltiplicatore di scala e velocità** degli attacchi

L'AI sta abbassando le **barriere d'ingresso** per gli attaccanti più velocemente di quanto le imprese stiano adattando le **difese**

Il numero di attacchi di phishing e social engineering è cresciuto fortemente grazie a **contenuti AI più credibili**

Gli **attacchi ibridi e multi-vettore** diventano estremamente difficili da rilevare con le difese tradizionali

L'AI introduce **nuove superfici di rischio**: uso non autorizzato di strumenti AI da parte dei dipendenti ed esfiltrazione involontaria di dati tramite prompt e modelli esterni

Nell'era dei **sistemi AI multi-agent** esistono strumenti in grado di gestire intere campagne di attacco in autonomia, dalla ricognizione alla compromissione



ASSOLOMBARDA

Normativa cyber



ASSOLOMBARDA



Cybersecurity e Normativa

Cosa cambia per le PMI e cosa non è più rinviabile

Miriam Ieraci · Professional Cybersecurity – Assolombarda

Non solo attacchi, ma anche responsabilità

Gli incidenti cyber crescono e con essi gli impatti economici e legali. La sicurezza informatica non è più una scelta tecnologica: è un **obbligo organizzativo**.

Rischio sistemico

Le PMI entrano direttamente o indirettamente nel perimetro normativo

Continuità operativa

La compliance è sempre più legata alla resilienza del business

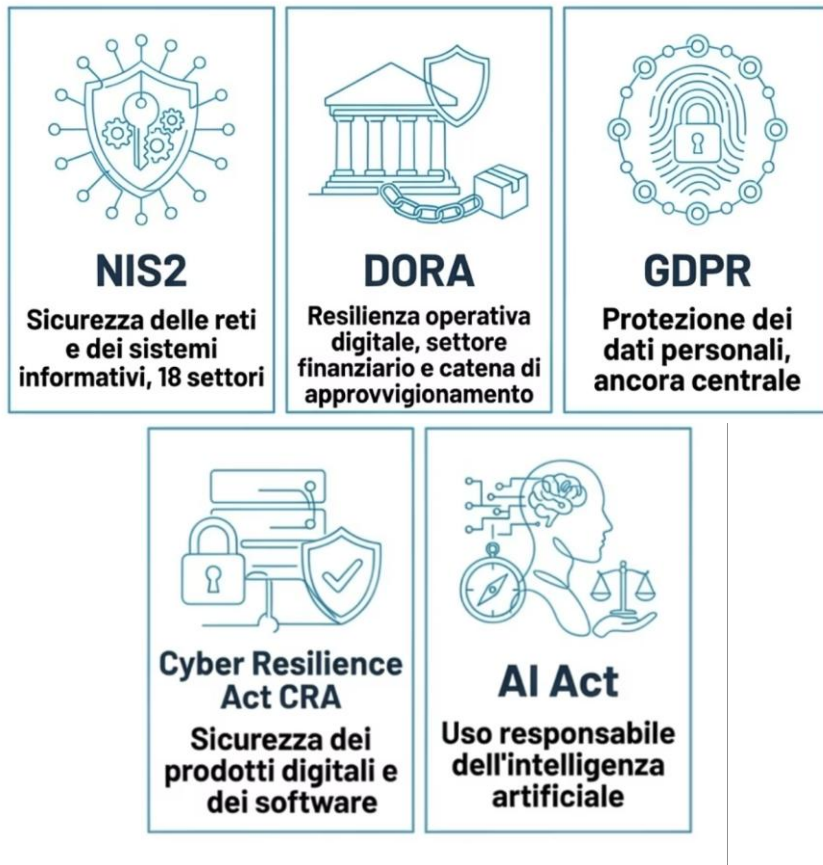
Fiducia e reputazione

Rapporti di filiera e immagine aziendale dipendono dalla sicurezza

- ❑ **Messaggio chiave:** La normativa non arriva perché le imprese sono troppo lente, ma perché il rischio è diventato sistemico.



Le principali normative da conoscere



Non tutte le normative si applicano a ogni PMI, ma **nessuna PMI può ignorarle del tutto**. Il perimetro si allarga progressivamente e la catena di fornitura è sempre più coinvolta.

NIS2

18 settori critici, obblighi di sicurezza e notifica incidenti

DORA & GDPR

Resilienza finanziaria e protezione dei dati personali

AI Act

Uso responsabile dell'IA

CRA

Prodotti digitali sicuri

DIRETTIVA NIS2

NIS2: L'Obbligo di Resilienza Digitale

La Direttiva NIS2 estende il perimetro della sicurezza cyber a **18 settori cruciali** (energia, sanità, trasporti, digitale, etc.), introducendo obblighi più stringenti per rafforzare la resilienza digitale dell'Unione Europea.

Cosa Cambia per le Imprese



Gestione Rischi

Mappare e proteggere asset informatici e sistemi critici.



Incident Response

Pianificare e notificare tempestivamente gli incidenti di sicurezza.



Sicurezza Catena di Fornitura

Estendere i requisiti di sicurezza a fornitori e partner.

Il recepimento nazionale è avvenuto a **ottobre 2024**, con le aziende che dovranno conformarsi con scadenze lungo tutto il 2026. Per le PMI italiane, ciò significa adeguare processi e tecnologie per evitare sanzioni e garantire la continuità operativa.



NIS2: Obblighi e Scadenze in Italia

Con il recepimento nazionale avvenuto nell'**ottobre 2024**, la Direttiva NIS2 introduce un quadro normativo più stringente per rafforzare la resilienza cibernetica delle imprese italiane. Gli obblighi si estendono a un'ampia gamma di settori critici, richiedendo un approccio proattivo alla sicurezza.

Misure Tecniche e Organizzative

Implementare soluzioni robuste per prevenire, rilevare e rispondere agli attacchi cyber.

Gestione degli Incidenti

Notifica obbligatoria degli incidenti significativi entro 24 ore e rapporto dettagliato entro 72 ore.

Continuità Operativa

Adottare piani di backup, recupero dati e gestione delle crisi per garantire la resilienza.

Sicurezza della Supply Chain

Valutare e gestire i rischi cyber lungo tutta la catena di fornitura, includendo i fornitori.

Formazione e Consapevolezza

Programmi di sensibilizzazione e formazione per il personale su temi di cybersecurity.



NIS2: LA ROADMAP

Le Tappe Fondamentali per la Compliance in Italia

Il recepimento nazionale della Direttiva NIS2 ha dato il via a un percorso di adeguamento che le imprese italiane devono affrontare con tempestività e metodo. Comprendere le scadenze è cruciale per una pianificazione efficace.

NIS2: Una Roadmap Dettagliata per la Compliance

Il percorso di adeguamento alla Direttiva NIS2 in Italia si articola in diverse fasi, con scadenze annuali e tappe fondamentali che richiedono un'attenta pianificazione.

Ciclo Annuale Ricorrente

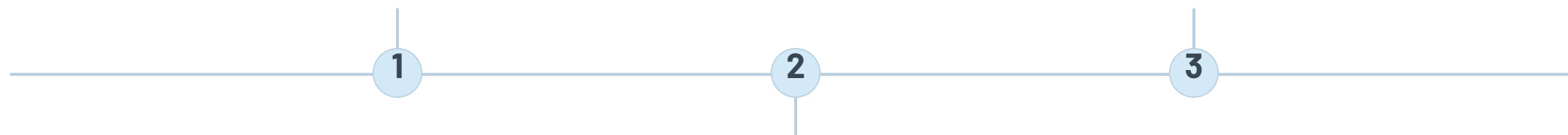
1 Gennaio – 28 Febbraio: Dichiarazione Dati Soggetti NIS (conferma/aggiornamento registrazione sul Portale NIS).

15 Aprile – 31 Maggio: Aggiornamento Annuale Informazioni (comunicazione di dati tecnici granulari come reti, asset critici, IP e nomi a dominio).

Evoluzione 2026-2027

Maggio – Luglio 2026: La Categorizzazione (ACN definirà criteri per classificare le attività NIS, distinguendo i sistemi che richiedono protezioni "avanzate" da quelli "base").

2027: Implementazione Obblighi di Lungo Termine (Misure di Sicurezza Avanzate, Piena Integrità della Supply Chain con audit e avvio Vigilanza e Ispezioni ACN).



"Giro di Boa" 2026

Dal 15 Gennaio 2026: Notifica Obbligatoria Incidenti Significativi al CSIRT Italia (entro 24h/72h/1 mese, classificando con Tassonomia Cyber ACN 2.0).

Entro Ottobre 2026: Implementazione Misure di Sicurezza Minime (i 13 pilastri per **Soggetti Importanti** e **Soggetti Essenziali**).

Comprendere queste fasi è cruciale per le PMI per passare dalla teoria alla pratica ispezionabile, garantendo la compliance e rafforzando la propria postura di sicurezza.

Cyber Resilience Act (CRA)

Il **Cyber Resilience Act (CRA)** è una nuova normativa UE che mira a migliorare la sicurezza dei prodotti con elementi digitali (hardware e software) immessi sul mercato. Estende la responsabilità della sicurezza ai produttori per l'intero ciclo di vita del prodotto.

Requisiti Chiave



Security by Design

Integrare la sicurezza fin dalle prime fasi di progettazione e sviluppo del prodotto.



Reporting degli Incidenti

Obbligo di notificare le vulnerabilità sfruttate e gli incidenti gravi alle autorità competenti.



Gestione delle Vulnerabilità

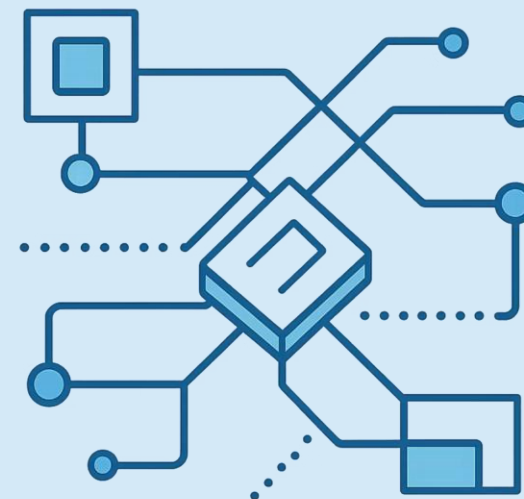
Identificare e risolvere proattivamente le vulnerabilità, garantendo aggiornamenti tempestivi.



Chi dovrà conformarsi

Tutti i fabbricanti (tutte le dimensioni, anche aziende extra-UE) che vendono nel mercato europeo. Gli importatori e i distributori devono assicurarsi che i dispositivi che immettono sul mercato siano conformi in materia di cybersicurezza.

Il CRA è stato pubblicato nel 2024 e i produttori avranno **36 mesi** per adeguarsi. Ciò impone a sviluppatori e aziende di prodotti digitali di rivedere i processi di sviluppo, le politiche di aggiornamento e le pratiche di gestione del rischio per garantire la conformità.



Gli obblighi dei soggetti CRA

Fabbricanti art. 13

Progettazione Sicura: Riduzione superficie di attacco, autenticazione robusta, integrità e riservatezza dei dati (Allegato I)

Valutazione dei Rischi: Obbligatoria per l'intero ciclo di vita: progettazione, sviluppo, produzione, consegna, manutenzione

Supply chain & open source: Componenti di terzi verificati; vulnerabilità notificate al manutentore e corrette nel prodotto

Gestione vulnerabilità: CVD, correzioni tempestive, aggiornamenti disponibili. Periodo di assistenza minimo: **5 anni**; ogni patch disponibile per **10 anni**

Doc e CE: Documentazione tecnica (All. VII), Dichiarazione UE di Conformità, marcatura CE prima della messa sul mercato

Importatori art. 19

Verifica prima dell'immissione sul mercato:

- il fabbricante abbia effettuato la valutazione di conformità e sia stata redatta la documentazione tecnica;
- il prodotto abbia la marcatura CE e la dichiarazione UE di conformità e istruzioni per l'uso comprensibili

Divieto di commercializzazione se non conforme: Se l'importatore ritiene che il prodotto non sia conforme al regolamento, non può immetterlo sul mercato finché non venga reso conforme.

Obbligo di segnalazione dei rischi: Se il prodotto presenta un rischio significativo di cybersicurezza, l'importatore deve:

- informare il fabbricante;
- informare le autorità di vigilanza del mercato degli Stati membri interessati.

Obblighi dopo l'immissione sul mercato: Se l'importatore scopre che il prodotto non è conforme deve: adottare misure correttive, oppure ritirarlo o richiamarlo dal mercato. Inoltre: deve conservare la dichiarazione UE di conformità per almeno 10 anni; Deve collaborare con le autorità di vigilanza fornendo documentazione e informazioni

Comunicazione delle vulnerabilità: Se l'importatore viene a conoscenza di una vulnerabilità del prodotto, deve informare il fabbricante senza indebito ritardo

Distributori art. 20

Verifica prima della distribuzione:

- il prodotto rechi la marcatura CE;
- abbia la documentazione richiesta e dalle istruzioni per l'uso;
- siano indicati fabbricante e, se applicabile, importatore con i relativi contatti;
- il prodotto sia conforme ai requisiti del CRA.

Obbligo di diligenza: I distributori devono agire con la dovuta diligenza rispetto ai requisiti del regolamento, tenendo conto del loro ruolo nella catena di fornitura.

Divieto di distribuire prodotti non conformi: Se ritiene o ha motivo di ritenere che un prodotto non sia conforme al CRA:

- non deve renderlo disponibile sul mercato finché non venga reso conforme;
- deve informare il fabbricante o l'importatore

Azioni in caso di rischio o non conformità:

un prodotto già distribuito non è conforme o presenta un rischio significativo di cybersicurezza, deve:

- informare fabbricante o importatore; adottare misure correttive (ritiro o richiamo se necessario);
- informare le autorità di vigilanza del mercato.

Cooperazione con le autorità Su richiesta delle autorità nazionali competenti, il distributore deve:

- fornire informazioni e documentazione necessarie;
- collaborare alle azioni per eliminare i rischi legati ai prodotti

"Non sono NIS2, quindi non mi riguarda"?

Molte PMI scoprono di essere coinvolte **indirettamente**. Essere fornitori di soggetti regolamentati o parte di catene critiche comporta obblighi contrattuali sempre più stringenti.

→ **Fornitori di soggetti NIS2**

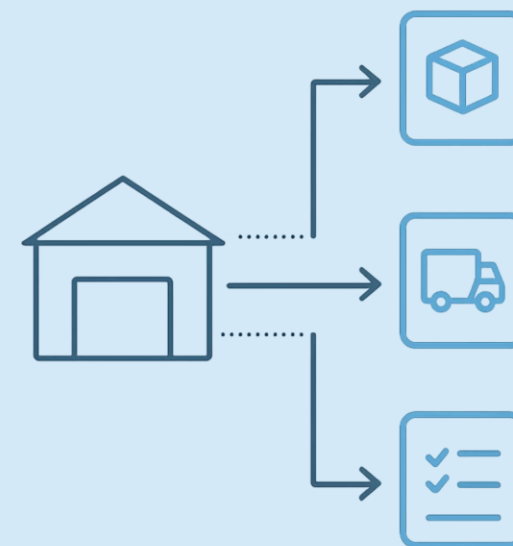
Le aziende regolamentate trasferiscono requisiti ai propri fornitori

→ **Catene di fornitura critiche**

La resilienza della filiera è sotto esame normativo

→ **Questionari, audit, certificazioni**

La sicurezza diventa un **requisito di mercato**, non solo di leggi



Non "più tecnologia", ma più organizzazione

Le normative convergono su pilastri comuni. Non esistono checklist universali: ogni impresa deve adattare le misure al proprio contesto.



Governance

Ruoli e responsabilità chiari a livello direzionale



Gestione del rischio

Valutazione strutturata delle minacce cyber



Misure di sicurezza

Proporzionate al rischio e al contesto aziendale



Gestione incidenti

Procedure definite di risposta e notifica



Formazione

Consapevolezza diffusa in tutta l'organizzazione



Supply chain

Controllo e qualifica dei fornitori critici



ERRORI FREQUENTI

Gli errori più comuni delle PMI

La conseguenza più frequente è una **compliance apparente** che non riduce il rischio reale.

Sicurezza delegata solo all'IT

Manca il coinvolgimento della direzione

Fornitori non gestiti

Nessuna valutazione del rischio nella supply chain

Politiche scritte ma non applicate

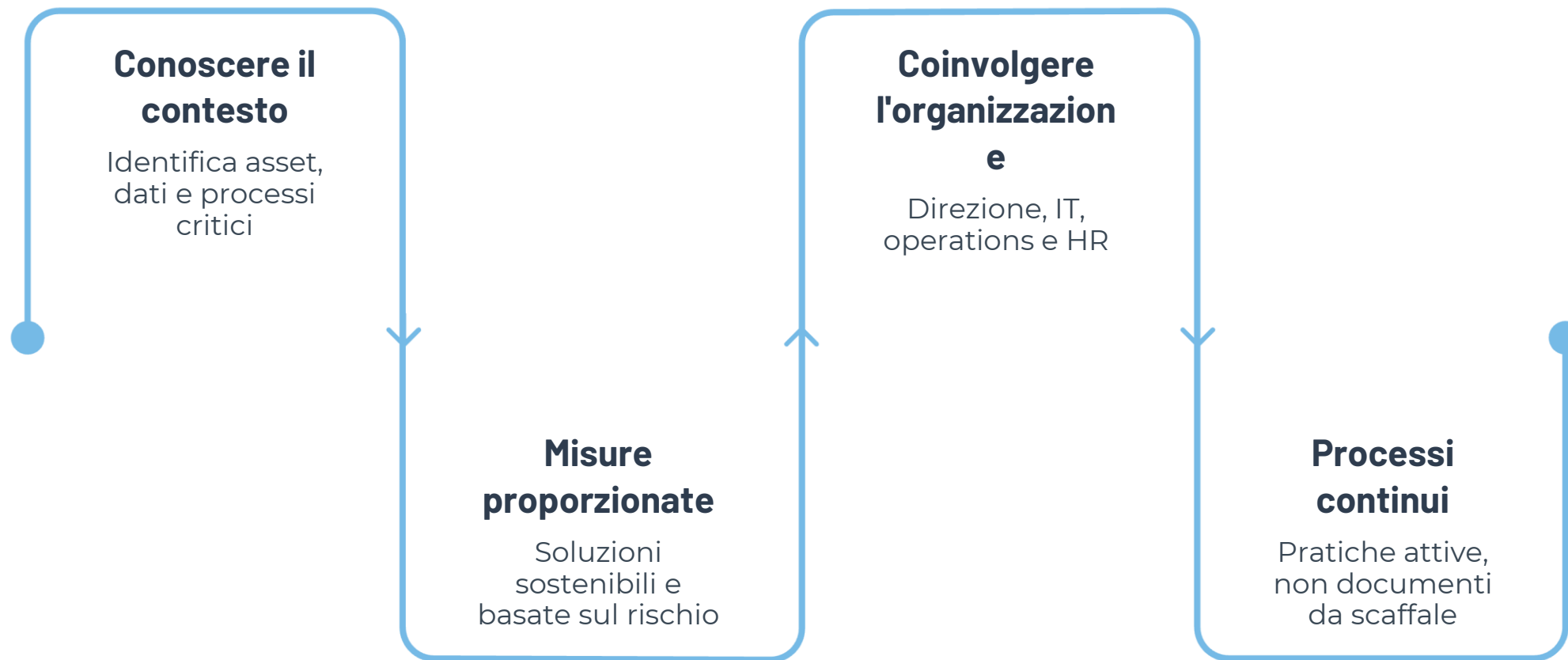
Documenti formali senza impatto operativo

Reazione improvvisata agli incidenti

Assenza di piani di risposta testati

Da compliance a sicurezza reale

La normativa chiede **processi**, non documenti da scaffale. Un approccio efficace parte dal contesto aziendale e coinvolge tutta l'organizzazione.



La direzione, l'IT, le operations e le risorse umane devono essere coinvolte attivamente: la sicurezza è responsabilità condivisa, non esclusiva del reparto tecnico.

Tre priorità non rinviabili

1

Sapere cosa proteggere

Analizzare i rischi, mappare dati, sistemi e processi critici. Senza questa consapevolezza, ogni misura è casuale.

2

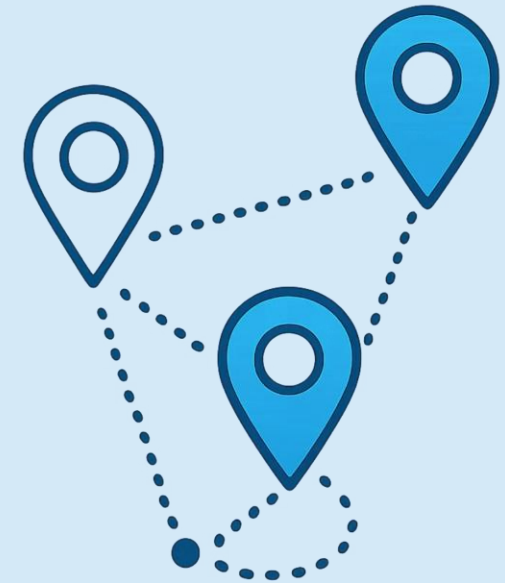
Sapere cosa fare in caso di incidente

Definire chi decide, chi comunica e chi interviene. La risposta deve essere pronta prima dell'evento.

3

Rendere le persone parte della sicurezza

Formazione continua, responsabilizzazione e cultura diffusa. Le persone sono la prima linea di difesa.



Il ruolo di Assolombarda

Accompagnare le imprese, non spaventarle.

*"La sicurezza
informatica è un
percorso, non un
adempimento una
tantum."*



Supporto interpretativo

Guida pratica sull'applicazione della normativa per le PMI



Formazione e sensibilizzazione

Iniziative dedicate per dirigenti, IT e collaboratori



Confronto istituzionale

Dialogo con stakeholder e istituzioni a tutela delle imprese



Approccio pragmatico

Soluzioni orientate alla realtà delle PMI italiane



PROSSIMO PASSO

Dalla norma alla pratica

"Abbiamo visto cosa chiede la normativa. Ora il punto è capire dove, nella realtà delle PMI, si concentrano le principali criticità operative."

Cosa sappiamo

Il quadro normativo e i requisiti fondamentali

Cosa esploriamo

Le criticità operative reali nelle PMI italiane

Cosa costruiamo

Un percorso concreto e sostenibile per la sicurezza



Aree di sicurezza nelle PMI



Aree in fase di sviluppo avanzato



Esposizione al rischio

Lo stanziamento di fondi non adeguati per la sicurezza informatica si traduce in controlli minimi carenti, governance debole e scarsa capacità di risposta agli incidenti, con un conseguente aumento della probabilità di attacchi e di relativi impatti economici e operativi significativi



Esposizione al rischio

La mancanza di commitment del management si traduce in assenza di priorità chiare e decisioni di investimento. I controlli di sicurezza risultano di conseguenza frammentati, reattivi o affidati all'improvvisazione, e questo aumenta fortemente la probabilità di incidenti gravi e ne amplifica l'impatto operativo ed economico

Budget

68%

Fondi cyber

% di PMI in cui esiste un budget dedicato o in cui parte del budget IT è destinabile alla sicurezza informatica

Commitment

64%

Vertici aziendali

% di PMI in cui i vertici aziendali indirizzano o considerano la tematica cyber

Identità digitali e controllo degli accessi

43%

MFA

% di PMI che utilizza
l'autenticazione a più fattori
per l'accesso ai servizi aziendali

Protezione dei dati

33%

Cifratura dei dati

% di PMI che adotta la cifratura
dei dati sulle workstation

Aree in fase di sviluppo



Esposizione al rischio

In presenza di una gestione poco strutturata degli accessi si riduce la capacità di prevenire abusi ed escalation dei diritti, rendendo i sistemi più vulnerabili anche a compromissioni di bassa complessità



Esposizione al rischio

In presenza di controlli di protezione del dato poco strutturati, anche attacchi di breve durata o accessi non autorizzati possono tradursi rapidamente in perdite di informazioni e impatti operativi, evidenziando come la vulnerabilità derivi dalla debolezza dei presidi di protezione più che dalla sofisticazione dell'attacco

Aree in fase di startup



Esposizione al rischio

La maggior parte delle PMI presenta una governance cyber ancora poco sviluppata, con ruoli, responsabilità e processi solo parzialmente definiti. La mancanza di strategie strutturate per la business continuity e il disaster recovery espone le aziende a rischi operativi prolungati in caso di attacco



Esposizione al rischio

L'assenza di un piano di formazione strutturato compromette la consapevolezza del rischio digitale e incrementa l'esposizione a rischi operativi legati a errori umani e al mancato riconoscimento delle minacce. La vulnerabilità delle organizzazioni deriva più dalla carenza di competenze diffuse che dalla complessità degli attacchi

Cyber governance

13%

Incident management

% di PMI che dispone di un piano di risposta agli incidenti aggiornato periodicamente

Formazione e competenze

5%

Formazione

% di PMI che dispone di piani di formazione continuativi e personalizzati in base ai ruoli aziendali



Azioni concrete per aumentare la postura cyber

Le domande da porsi

- 1. L'organizzazione è in grado di accorgersi subito che qualcosa di anomalo sta accadendo nei propri sistemi?
- 2. I dispositivi aziendali sono protetti in modo uniforme o rappresentano ancora il punto di ingresso più semplice per un attaccante?
- 3. Se un sistema viene compromesso, l'attacco può propagarsi liberamente?
- 4. È sempre noto chi accede ai sistemi, con quali privilegi e per quanto tempo?
- 5. Gli eventi di sicurezza vengono registrati e analizzati?
- 6. Le tecnologie di difesa sono in grado di rilevare comportamenti anomali?
- 7. I fornitori IT e cloud sono considerati parte del perimetro di rischio?

NEW: Le tecnologie di difesa sono in grado di rilevare attacchi perpetrati tramite sistemi AI multi-agent?
- 8. Quando si verifica un incidente, si è in grado di identificarlo e attivare rapidamente il processo di notifica e gestione?
- 9. Gli accessi sono considerati affidabili di default?
- 10. L'organizzazione è in grado di apprendere dagli incidenti e migliorare nel tempo le proprie difese?

Rilevazione

Endpoint

Segmentazione

Identità

Logging

IA

Ecosistema

Notifica

Zerotrust

Adattabilità

Le soluzioni in risposta (1/2)

R

E

S

I

L

I

E

N

Z

A

Definire un processo di **rilevazione e monitoraggio continuo**, creando le basi per individuare rapidamente eventi anomali e ridurre l'impatto anche di attacchi rapidi o automatizzati

Implementare la **segmentazione** di rete consente di isolare gli ambienti, ridurre il movimento laterale degli attaccanti e trasformare un incidente potenzialmente sistemico in un evento circoscritto

Centralizzare il **logging** permette di abilitare l'early detection e l'automazione della risposta, creando le condizioni per una gestione più rapida ed efficace degli incidenti

All'interno dell'**ecosistema dei fornitori e delle terze parti**, introdurre pratiche di gestione del rischio per prevenire l'impatto di incidenti esterni

Adottare un approccio **Zero Trust** significa eliminare la fiducia implicita, applicando una verifica continua e il principio del minimo privilegio per ridurre l'impatto degli attacchi

Le soluzioni in risposta (2/2)

R

S

L

E

Z

E

I

I

N

A

Un efficace presidio degli **endpoint** si basa su aggiornamenti continui, monitoraggio centralizzato e adozione di soluzioni specifiche per minimizzare i rischi di compromissione

Governare le identità significa introdurre una gestione delle **identità** e degli **accessi** e delle modalità di **autenticazione**, garantendo un controllo su utenti e privilegi

L'adozione di soluzioni basate sull'**Intelligenza Artificiale** per l'anomaly detection e la threat intelligence consente di ridurre i tempi di reazione e il carico operativo, rendendo la difesa più scalabile

Definire un processo di **notifica** strutturato per consentire di attivare rapidamente la risposta agli incidenti e supportare l'operatività interna

Costruire resilienza nel tempo richiede **adattabilità e formazione continua**, test e simulazioni periodiche, così da imparare dagli incidenti e migliorare costantemente processi, tecnologie e competenze

NEW: Strumenti AI per la sicurezza multi-agent

Le azioni concrete da implementare (1/2)

2. Presidio degli endpoint

- Distribuire **soluzioni EDR/XDR** sui dispositivi aziendali
- Centralizzare **patching**, aggiornamenti e monitoraggio degli endpoint

4. Governance delle identità

- Introdurre l'**autenticazione a più fattori** per accessi remoti, cloud e account privilegiati
- Implementare la gestione delle **identità** e degli **accessi (anche privilegiati)** per il governo e il tracciamento degli account amministrativi

1. Monitoraggio continuo

- Istituire un **SOC** interno o in outsourcing per il monitoraggio H24 degli eventi di sicurezza
- Definire **attività di controllo periodico** su log, alert e anomalie con use case chiari

3. Segmentazione di rete

- Implementare una **segmentazione logica della rete**
- Applicare **baseline di hardening** su server, firewall e apparati di rete (configurazioni sicure standard)

5. Logging centralizzato

- Centralizzare i log su una piattaforma **SIEM**
- Definire **regole di correlazione** e retention minime per supportare detection e analisi post-incidente

Le azioni concrete da implementare (2/2)

7. TPRM

- Censire **fornitori IT e cloud** critici con una classificazione del rischio
- Introdurre **requisiti di sicurezza contrattuali** e verifiche periodiche (questionari, attestazioni)

9. Zero Trust

- Eliminare la **fiducia implicita** tra reti e sistemi, introducendo controlli di accesso contestuali
- Applicare il **principio del minimo privilegio** su utenti, servizi e applicazioni

6. Intelligenza artificiale

- Integrare feed di **threat intelligence** aggiornati nei sistemi di sicurezza
- Utilizzare motori di **anomaly detection** basati su AI per ridurre falsi positivi e tempi di reazione

NEW: Implementare modelli di sicurezza AI multi-agent

8. Notifica e risposta agli incidenti

- Definire un **piano di risposta agli incidenti** con ruoli, contatti e flussi decisionali chiari
- Eseguire **esercitazioni periodiche** per testare tempi e coordinamento

10. Formazione continua

- Attivare **programmi di formazione** ricorrenti differenziati per ruolo (utente, IT, management)
- Analizzare **eventi e incidenti** per aggiornare controlli, processi e consapevolezza



ForgIA

AI nelle Aziende del Tessuto Imprenditoriale



ASSOLOMBARDA



Shape the future
with confidence

Tipi di Aziende che si affacciano all'AI



Legacy SMART(ER)

- Non cambiano i processi
- L'AI è solo per efficienza personale
- Le persone sono attori passive rispetto l'introduzione dell'AI



Augmented INTELLIGENT WORKPLACE

- I processi evolvono
- L'AI è uno strumento per l'efficienza e per il posizionamento
- Le persone sono formate e contribuiscono alla discovery e alla generazione di valore



Transformed BUSINESS MODEL DISRUPTION

- I processi vengono disegnati per l'AI
- L'AI è alla base della strategia aziendale
- Le attività delle persone sono orchestrate dall'AI e sono utili per prendere decisioni

I 3 Pilastri Organizzativi dell'AI



Adoption

GENERARE VALORE

- Valutazione della readiness
- Percorso di allineamento organizzativo e discovery dei casi d'uso
- Manifesto e Policy Iniziali



Governance

GESTIRE PROCESSI E RISCHIO

- AI Operating Model E2E
- Definizione delle Responsabilità (Owner, Risk, DPO, Infrastructure, ...)
- Gestione del lifecycle dei casi d'uso e delle policy



Compliance

ADESIONE A NORME E POLICY

- Controlli Interni e Classificazione Rischio
- Gap Analysis (EU AI Act, privacy, benchmark)
- Evidenze, Test, e Audit Trail

Alcuni Esempi di Use Case



Supporto alle Decisioni

L'AI supporta imprenditore, CFO, commerciale o operation manager con analisi, previsioni e raccomandazioni. La decisione resta umana.

- Agenti conversazionali
- Tool di Forecasting e Planning
- Supporto alla partecipazione a Gare



Automazioni Intelligenti

L'AI automatizza attività operative ripetitive o documentali, con approvazione umana.

- Automazione Ciclo Passivo
- Automazione Inserimento Ordini
- Riconciliazione Incassi



Agenti

L'AI non si limita ad analizzare o assistere: gestisce un flusso operativo end-to-end, interagendo con sistemi e utenti entro regole definite.

- Agente «Assistente Service di Primo Livello»
- Gestione sollecito pagamenti
- Onboarding nuovo fornitore

Limiti all'Adozione

NEL CONTESTO IMPRENDITORIALE ITALIANO



Ambientale

- Ricerca ROI immediato
- Bassa Maturità Digitale di Base
- Sponsorship debole
- Complessità nelle Integrazioni



Trusted Partners

- Spesso chi parla di AI nelle aziende sono i software vendor, limitando l'AI ad uno use case specifico



Conoscenza del Contesto

- Gli algoritmi e i modelli di frontiera sono estremamente generalisti, per essere efficaci in un contesto specifico devono essere «specializzati»

Rethinking Industry - forgIA

Viviana Palmieri, Senior Professional Transizione Digitale

aprile 2026



Obiettivo del progetto strategico **Rethinking Industry** è il **rafforzamento della competitività dell'industria**, favorendo l'adozione di soluzioni di Intelligenza Artificiale Generativa e Agentica.

A tal fine promuove la realizzazione di **forgIA, un ecosistema digitale condiviso**, sicuro e interoperabile, volto a sostenere lo sviluppo di applicazioni verticali ad alto impatto e a valorizzare i dati industriali in modo strutturato, **garantendo** al contempo la **sovranità del dato** e la **tutela della proprietà intellettuale**.

La **competitività e la resilienza** delle imprese dipendono sempre più dalla **capacità di valorizzare e condividere i dati**.

Le aziende che riescono a **creare ecosistemi digitali aperti**, dove il flusso informativo è continuo e sicuro, sono in grado di **anticipare i cambiamenti, ottimizzare i processi** e rispondere con agilità alle crisi.

Il dato non è solo una risorsa: è il motore dell'innovazione e della sostenibilità nel lungo periodo.

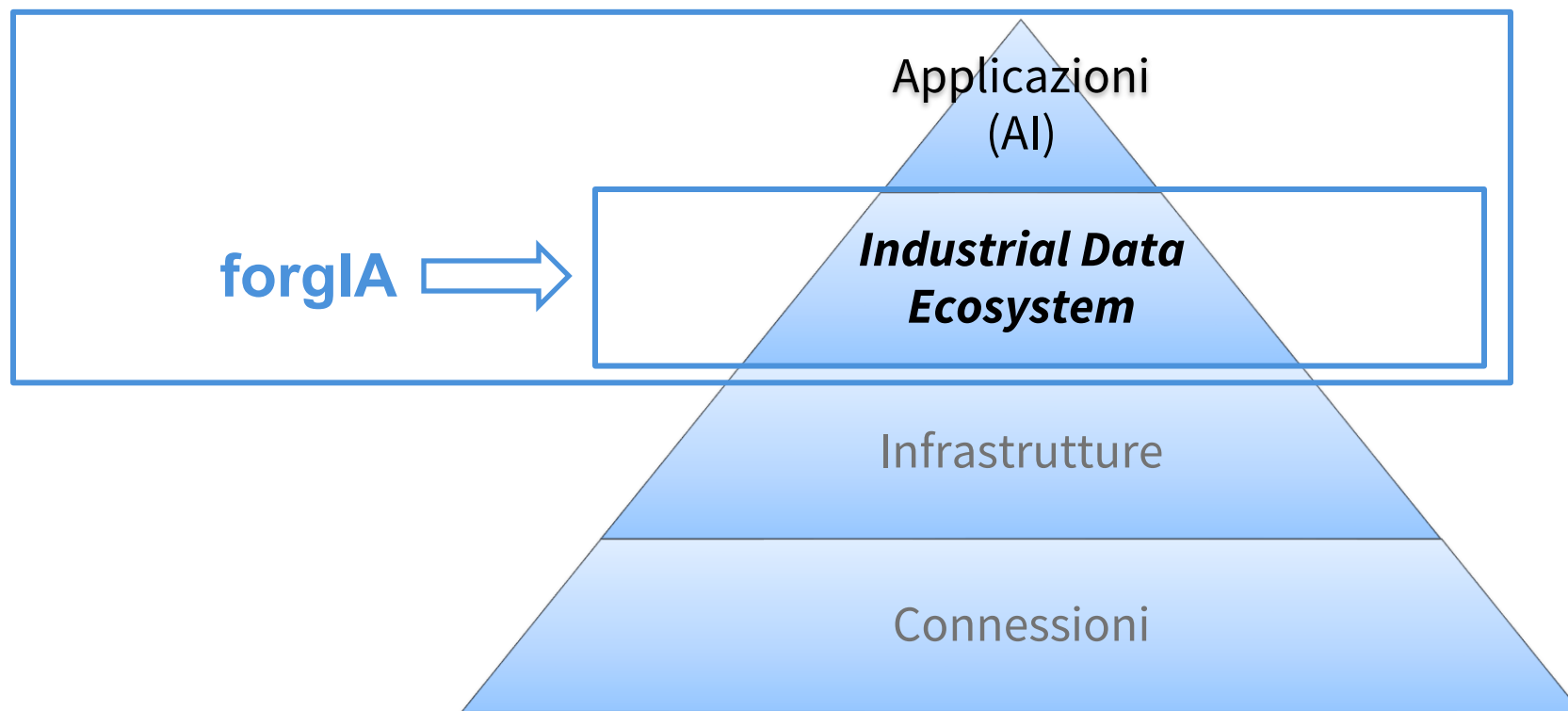


La visione su **forgIA**:
*ecosistema condiviso dalle filiere e dai distretti industriali,
volto a favorire la messa a disposizione di dati per «forgiare»
soluzioni di Intelligenza Artificiale*

Rethinking
Industry



forgIA



Attori chiave



ADVISORY BOARD

Cefriel: Centro di innovazione digitale e competenza avanzata che supporta imprese e istituzioni nella trasformazione tecnologica attraverso ricerca applicata, formazione e trasferimento di soluzioni digitali ad alto impatto. E' partner operativo del programma forgIA Industrial Data Ecosystem. **Cefriel**

AI USER

Aziende Associate che manifestano bisogni reali per lo sviluppo di casi d'uso basati sulla valorizzazione dei dati condivisi e l'applicazione dell'AI nei processi industriali

GRUPPO INNOVATION SERVICES

Il gruppo Innovation Services di Assolombarda è composto da oltre 1900 imprese che producono o forniscono servizi per la gestione delle imprese. Al suo interno troviamo: HPE, IBM, Accenture, NTT Data, Tecnimont, Cisco System,...

Iniziamo a dare i numeri

- **4 programmi strategici avviati**
- **30+ realtà candidate come *early adopters***
- **25+ *use cases* in approfondimento**
- **15 eventi dedicati programmati**
- **10 mentor per 6 aree focus**

4 Programmi Strategici:



Industrial Data Ecosystem



Accelerate



Academy

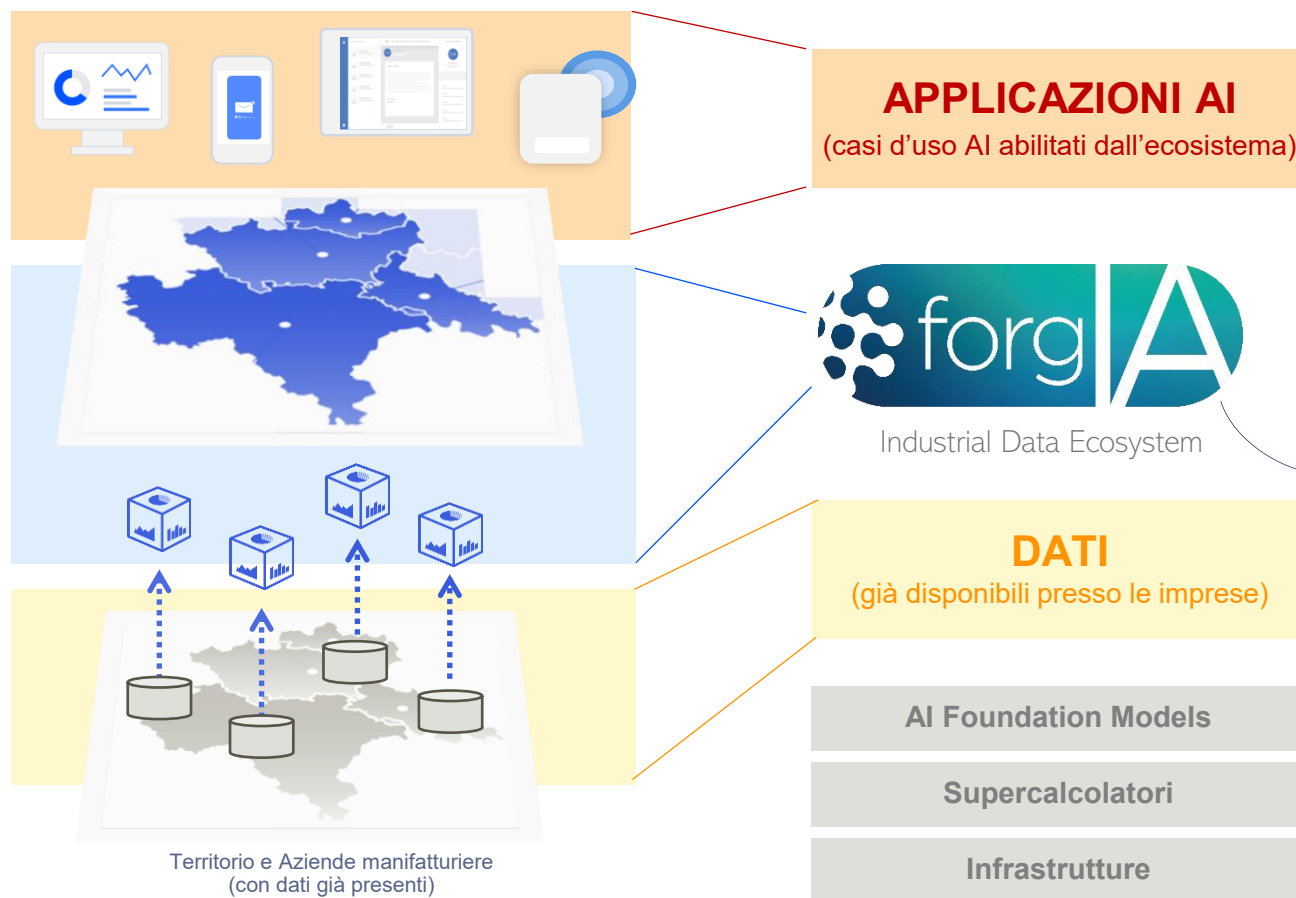


Leadership Initiative

Opportunità: Ecosistema Digitale per il “Rethinking Industry”

Impostazione strategica: abilitare soluzioni di **Generative & Agentic AI** nei settori manifatturiero e dei servizi a partire da un Ecosistema Digitale di collaborazione (forgIA)

Applicazioni Gen AI e Agentic AI “powered by” Ecosistema Digitale ForgIA



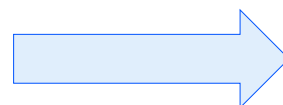
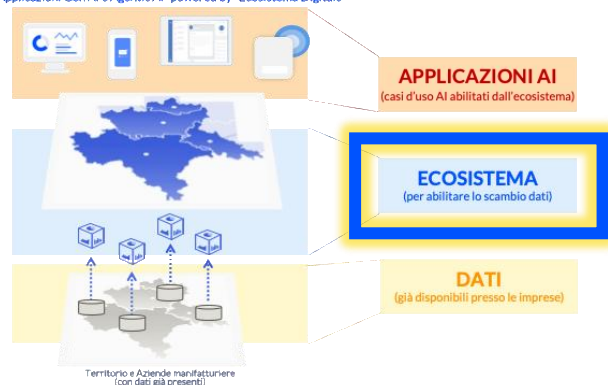
Ambiente di collaborazione per governare, promuovere e formalizzare, l'incontro fra:

- soggetti che vogliono **mettere a disposizione in modo sicuro flussi dati certificati** verso specifici partner approvati;
- soggetti che hanno **interesse ad accedere ai flussi dati certificati di altri soggetti**, al fine di innovare le proprie soluzioni digitali per clienti o dipendenti / creare nuovi servizi

BENEFICIO: sbloccare valore di business **addizionale dai propri dati** (“*unlocking additional business value*”), valorizzandoli ulteriormente all'interno di **nuove soluzioni AI augmented o AI native**

La “parte visibile” di un Ecosistema Digitale per il Rethinking Industry: Marketplace B2B di flussi dati

Applicazioni Gen AI e Agentic AI “powered by” Ecosistema Digitale



Regole di
partecipazione



Processi per
popolamento
contenuti e
richiesta d'uso di
flussi certificati

La «parte visibile» dell'ecosistema è rappresentata da un **marketplace B2B** all'interno del quale è disponibile il **catalogo dei flussi dati certificati** pubblicati, descritti nella forma di «**prodotto**» (data-as-a-product)

Il catalogo ha natura **operativa**, in quanto mette a disposizione i **processi per descrivere nuovi flussi dati** e per **richiedere l'autorizzazione all'accesso a flussi di altri soggetti**

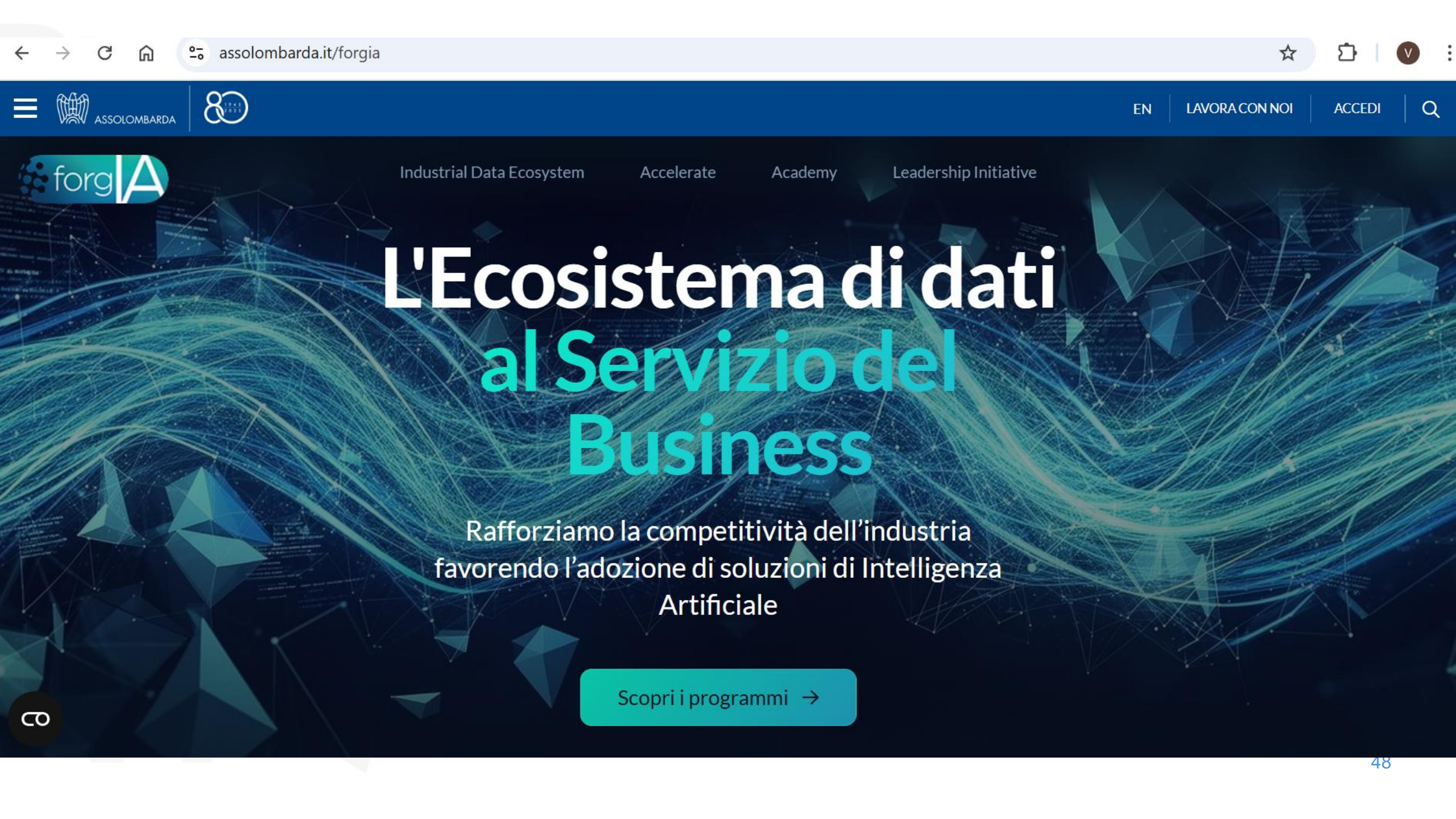


I flussi dati
«richiedibili» da altri
partecipanti



Le **soluzioni specifiche**
autorizzate all'uso di
specifici dati

Un Ambiente Digitale «affiancato» al mondo fisico, **abilitante lo scambio dati tra le imprese**



Industrial Data Ecosystem Accelerate Academy Leadership Initiative

L'Ecosistema di dati al Servizio del Business

Rafforziamo la competitività dell'industria
favorendo l'adozione di soluzioni di Intelligenza
Artificiale

Scopri i programmi →





ASSOLOMBARDA



www.assolombarda.it/forgia

**Scopri cosa può fare
forgIA per la tua azienda:**

Contattaci



forgia@assolombarda.it