L’Intelligenza Artificiale nella PA: dalle Linee Guida alle decisioni

Linee Guida AgID per l’adozione di IA nella Pubblica Amministrazione · v1.0
del 9 novembre 2026

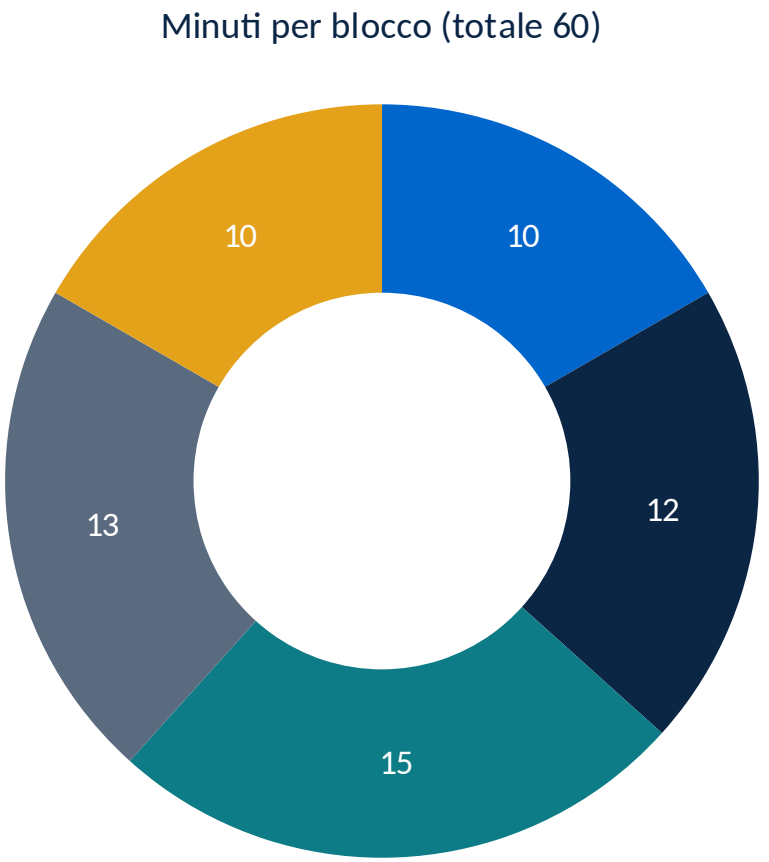


MODULO PER DIRIGENTI · 60 MINUTI

Relatore: Vincenzo Calabrò

Il percorso di oggi

1	**Il quadro di riferimento** Perché ora, a chi si applica, come si leggono le Linee Guida	10′
2	**Capire l’IA per governarla** Definizioni, ciclo di vita, ruoli, livelli di rischio, principi	12′
3	**Il modello organizzativo** Strategia, governance, casi d’uso, KPI, rischio e impatto	15′
4	**Conformità, dati e sicurezza** Obblighi, trasparenza, qualità dei dati, cybersicurezza	13′
5	**Competenze e prossimi passi** Cosa si chiede ai dirigenti e una roadmap di avvio	10′



Il messaggio da portare a casa

L’IA supporta. La PA decide, e ne risponde.

La responsabilità ultima delle decisioni, qualunque sia il livello di automazione, rimane in capo all’amministrazione. Per questo l’adozione dell’IA è prima di tutto una scelta di governo, non un acquisto tecnologico.

20

principi di adozione, in cinque famiglie

4

fasi del modello organizzativo, ciclo Plan-Do-Check-Act

150+

occorrenze di «DEVE / DEVONO» nel testo

Fonte: Linee Guida AgID, par. 3.4 (principio P.5 Responsabilità) e cap. 4. Conteggio delle occorrenze effettuato sul testo del documento.

01

Il quadro di riferimento

Perché ora, a chi si applica, come si leggono le Linee Guida

Come siamo arrivati qui

12 gen 2024
DPCM Piano triennale 2024-2026
prevede l'adozione di Linee Guida sull'IA nella PA

13 giu 2024
AI Act
Regolamento (UE) 2024/1689: regole armonizzate sull'IA

2 feb 2025
Divieti in vigore
si applicano gli usi vietati dell'art. 5 AI Act

23 set 2025
Legge 132/2025
disposizioni e deleghe al Governo in materia di IA

9 nov 2026
Linee Guida AgID v1.0
adozione dell'IA nella PA, versione definitiva

Fonte: Linee Guida AgID, Introduzione e nota 13. Le Linee Guida sono emanate secondo l'art. 71 del CAD.

A chi si rivolgono e come si leggono

A chi

A tutti i soggetti dell’art. 2, comma 2, del CAD: nel documento sono indicati come «PA».

Su cosa

Su tutti i sistemi e i modelli di IA definiti dall’art. 3 dell’AI Act e richiamati dall’art. 2 della Legge 132/2025.

Il «vocabolario» delle Linee Guida (ISO/IEC Directives)

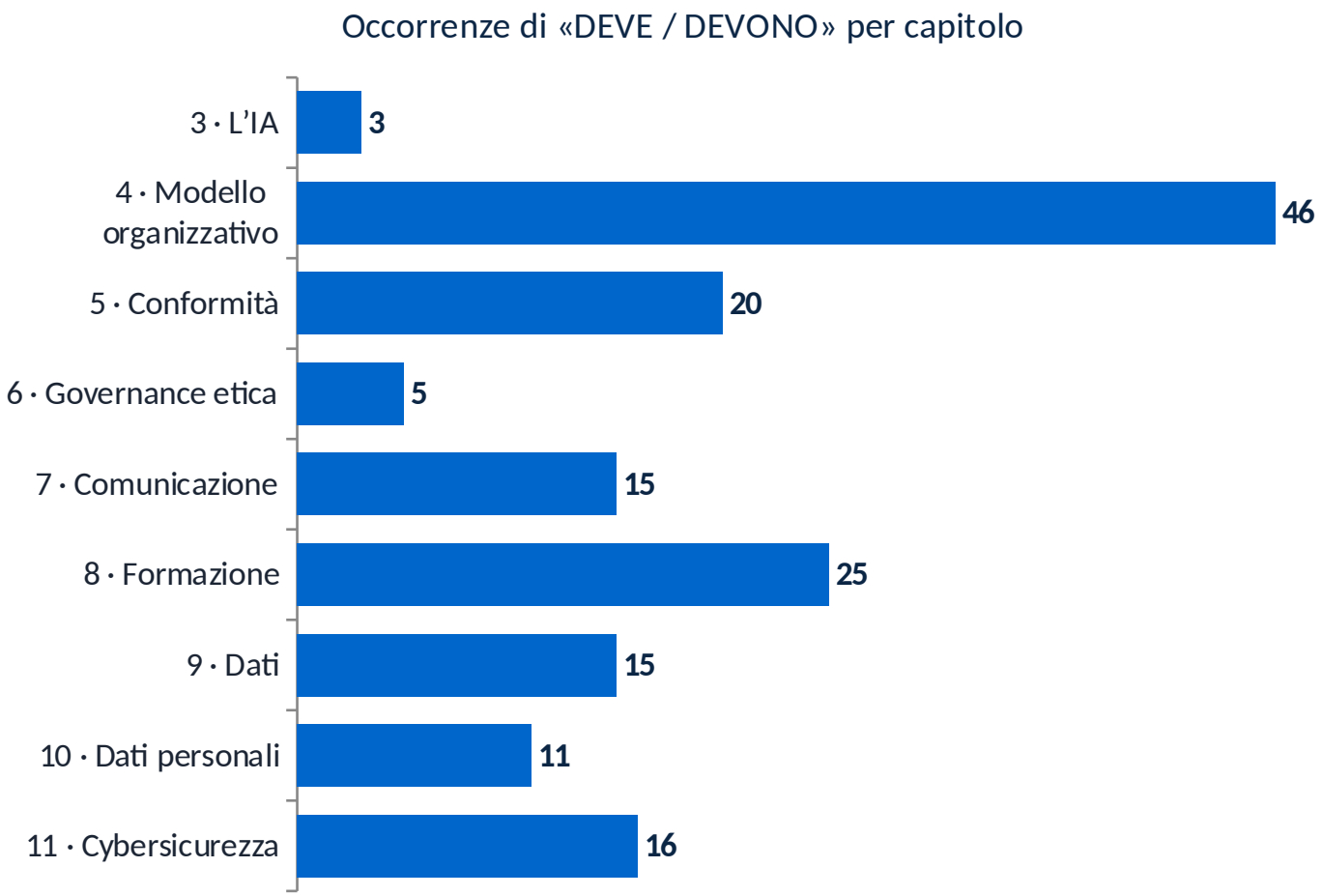
DEVE / DEVONO — Requisito obbligatorio. NON DEVE indica un divieto assoluto.

DOVREBBE — Le implicazioni vanno comprese e pesate prima di scegliere un’altra strada.

PUÒ / POSSONO — Facoltà: il lettore sceglie se applicare o meno l’indicazione.

Un disegno unico, tre documenti: Linee Guida adozione (oggi), Linee Guida sviluppo e Linee Guida procurement. Strumenti pratici di supporto sono pubblicati e aggiornati sul sito AgID.

Dove si concentrano gli obblighi



Elaborazione del relatore sul testo delle Linee Guida (46 occorrenze su 156 nei capitoli 3-11).

30%

degli obblighi si trova nel capitolo sul modello organizzativo.

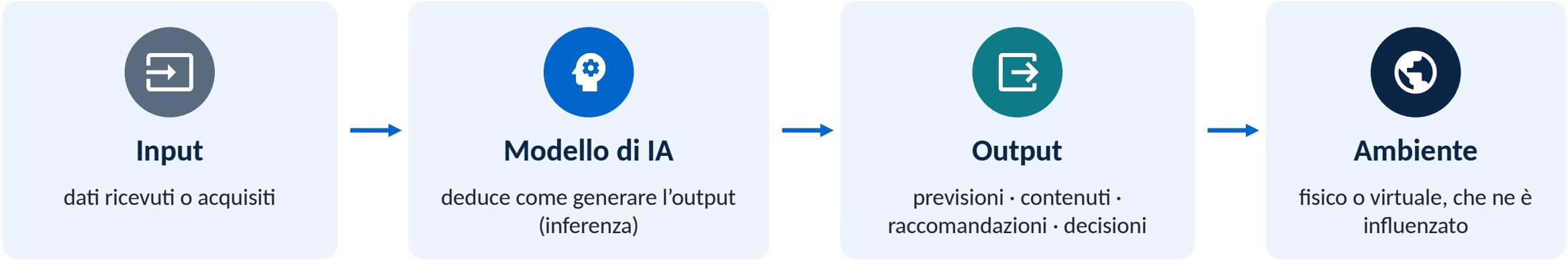
Il messaggio è netto: adottare l'IA significa anzitutto organizzarsi. Seguono conformità all'AI Act (cap. 5) e formazione (cap. 8), che insieme ai dati e alla sicurezza formano il cuore operativo del documento.

02

Capire l’IA per governarla

Definizioni, ciclo di vita, ruoli, rischio e principi

Che cos'è un «sistema di IA»



Autonomia variabile e adattabilità

Dal controllo umano diretto al funzionamento indipendente; alcuni sistemi apprendono e cambiano comportamento durante l'uso.

Modelli per finalità generali (GPAI)

Grandi modelli integrabili in molte applicazioni; quelli «a rischio sistemico» hanno un regime specifico (art. 51 AI Act).

Logica statistico-probabilistica

A differenza dei sistemi deterministici, gli output dell'IA generativa sono soggetti a margini di incertezza. Nei contesti ad alto impatto (diritti, equità, accesso ai servizi) affidabilità e robustezza vanno verificate con particolare attenzione.

Fonte: Linee Guida AgID, cap. 3; definizione dall'art. 3, punto 1, AI Act (allineata alla definizione OCSE).

Bias: tre origini, un solo rischio

Bias nei dati

I dati di addestramento o di test riflettono pregiudizi, lacune o rappresentazioni distorte della realtà.

Bias algoritmico

Le scelte tecniche e le ipotesi implementate nel modello introducono distorsioni nei risultati.

Bias umano

Pregiudizi impliciti o espliciti di progettisti e stakeholder entrano nella progettazione o nell'uso.

L'effetto: trattamenti ingiusti, risultati inaffidabili, discriminazioni verso individui o gruppi. **Cosa chiedere:** come vengono riconosciuti, mitigati e monitorati i bias, per tutto il ciclo di vita. Per i sistemi ad alto rischio l'art. 10 AI Act impone requisiti specifici di governance dei dati.

Fonte: Linee Guida AgID, cap. 3 (rif. ISO/IEC TR 24027) e cap. 9.

Il ciclo di vita di un sistema di IA (modello OCSE)



Pianificazione e design
obiettivi, contesto, requisiti misurabili

Raccolta e trattamento dati
acquisizione, qualità, conformità privacy

Costruzione o addestramento
scelta dei modelli, fine-tuning, transfer learning

Test, verifica e validazione
conformità a requisiti e aspettative

Messa a disposizione
integrazione nei processi, accessibilità

Operatività e monitoraggio
drift, anomalie, bias, riaddestramento

Ritiro / disattivazione
gestione sicura dei dati, documentazione

Perché interessa a un dirigente

Le decisioni non finiscono con il collaudo. Monitoraggio, riaddestramento e dismissione vanno previsti fin dall'inizio, nel piano operativo e nel contratto: un sistema di IA è un servizio da governare nel tempo, non un prodotto da installare.

Fonte: Linee Guida AgID, par. 3.1 (OECD AI Principles overview).

Chi fa cosa nella catena del valore

Fornitori di modelli
modelli di IA, anche GPAI

↓

Fornitori di infrastrutture
pipeline dati, rete, hardware, cloud, MLOps

↓

Fornitori di applicazioni
soluzioni verticali che adattano modelli esistenti

↓

Deployer
chi usa l'IA sotto la propria autorità: tipicamente la PA

Provider (fornitore): sviluppa o fa sviluppare un sistema o modello di IA e lo immette sul mercato o lo mette in servizio con il proprio nome o marchio.

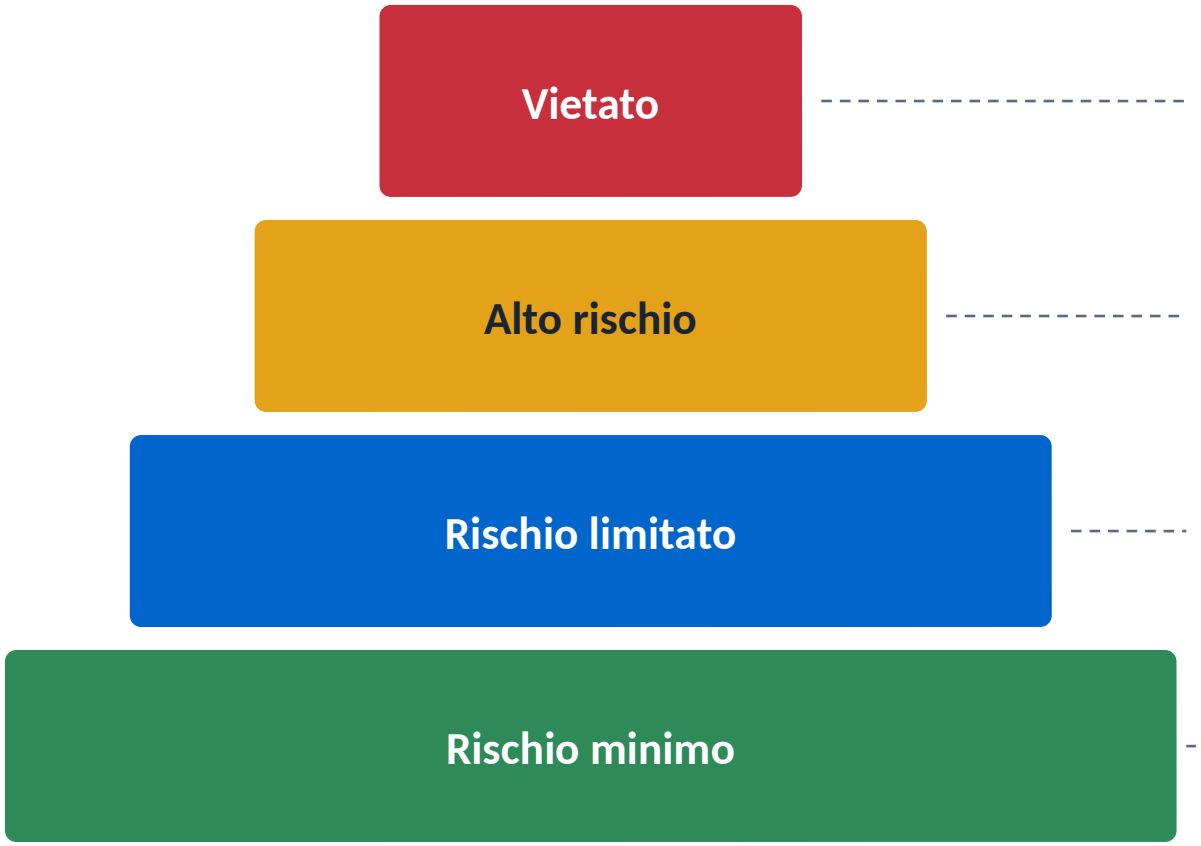
Deployer: utilizza un sistema di IA sotto la propria autorità (escluso l'uso personale non professionale).

Attenzione: il deployer può diventare provider (art. 25 AI Act)

- se appone il proprio nome o marchio su un sistema ad alto rischio già sul mercato;
- se vi apporta una modifica sostanziale e il sistema resta ad alto rischio;
- se ne modifica la finalità e il sistema diventa ad alto rischio.

Fonte: Linee Guida AgID, par. 3.2 e 5.1; AI Act art. 3 (definizioni 3 e 4) e art. 25.

Quattro livelli di rischio, quattro regimi diversi



Rischio inaccettabile (art. 5). Es.: tecniche subliminali o manipolative, social scoring. Divieti in vigore dal 2 febbraio 2025.

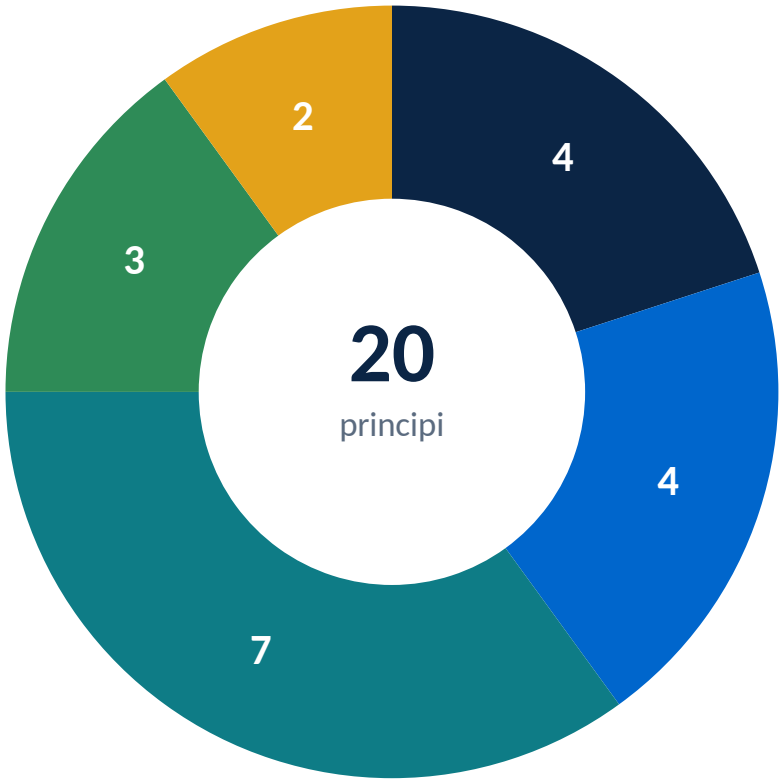
Rischi significativi per salute, sicurezza, diritti fondamentali, democrazia, Stato di diritto, ambiente. Classificazione: art. 6 e Allegato III.

Obblighi di trasparenza dell'art. 50: chi interagisce con l'IA deve saperlo.

Impatto trascurabile su interessi pubblici e diritti fondamentali.

Per tutti i sistemi: Carta dei diritti UE, CEDU, Convenzione quadro del Consiglio d'Europa sull'IA, Dichiarazione europea sui diritti digitali, Orientamenti etici AI HLEG.

20 principi in cinque famiglie



Conformità e governance (4)
P.1 Conformità normativa · P.2 Valori UE · P.3 Gestione del rischio · P.4 Dati personali

Etica e inclusione (4)
P.5 Responsabilità · P.6 Accessibilità e non discriminazione · P.7 Trasparenza e spiegabilità · P.8 Informazione

Qualità e affidabilità (7)
P.9 Qualità dei dati · P.10 Accuratezza · P.11 Robustezza · P.12 Cybersicurezza · P.13 Sorveglianza umana · P.14 Logging · P.15 Standard tecnici

Innovazione e sostenibilità (3)
P.16 Efficienza e qualità dei servizi · P.17 Innovazione e open source · P.18 Sostenibilità ambientale

Formazione e organizzazione (2)
P.19 Competenze · P.20 Organizzazione e infrastrutture

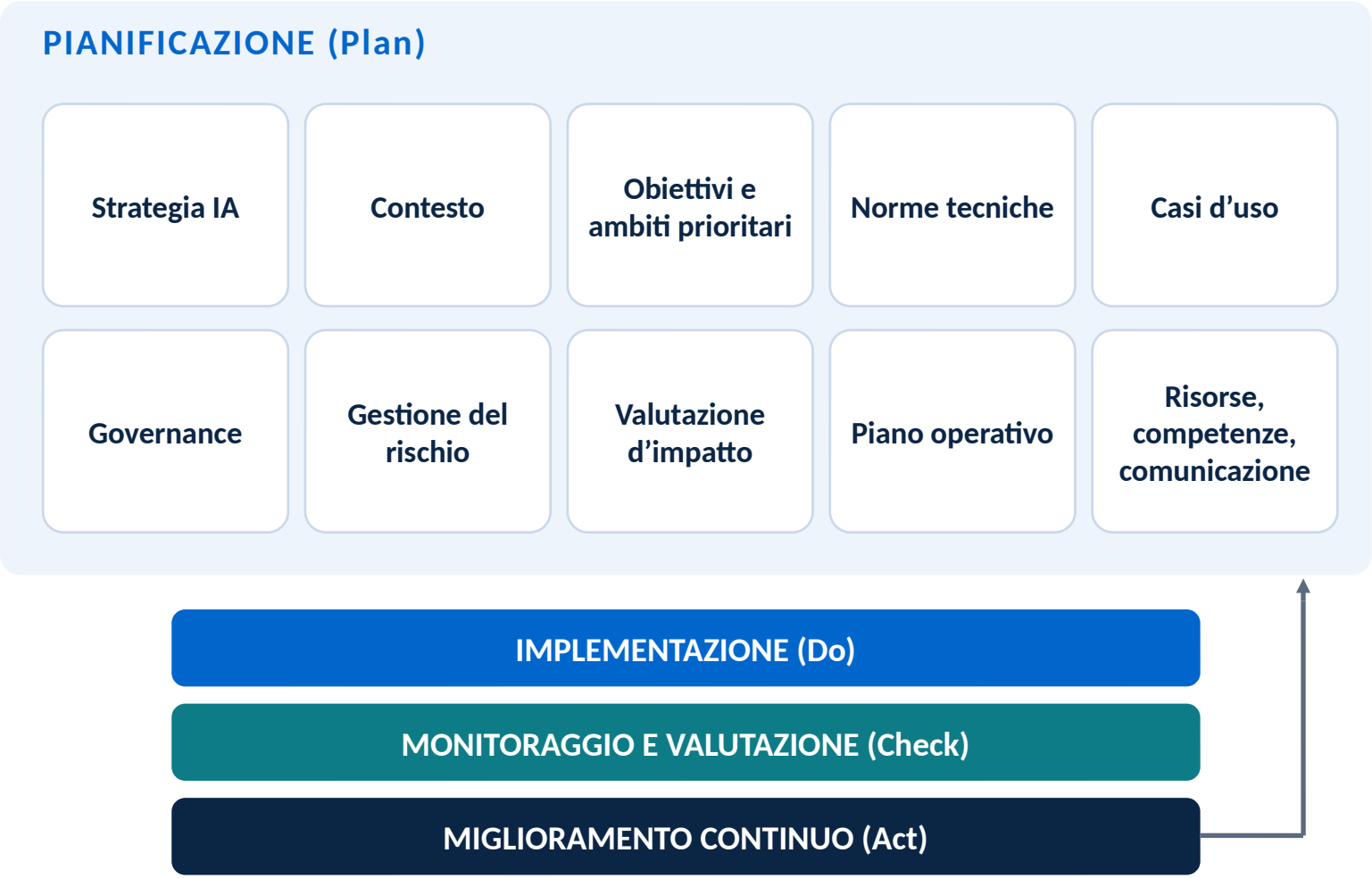
Fonte: Linee Guida AgID, par. 3.4. Per i sistemi ad alto rischio i principi sono rafforzati dai requisiti dell'AI Act.

03

Il modello organizzativo

Strategia, governance, casi d’uso, KPI, rischio e impatto

Un ciclo PDCA per governare l’IA



Fonte: Linee Guida AgID, cap. 4, Figura 4 (rielaborata).

Le basi del modello

DEVE esserci un modello organizzativo capace di reagire ai cambiamenti normativi e tecnologici.

ISO/IEC 42001:2023 come riferimento metodologico: utile, ma non dà presunzione di conformità all’AI Act.

Nei casi previsti dall’AI Act va adottato il sistema di gestione della qualità richiesto.

Rischio limitato o minimo: le fasi si POSSONO accorpare.

La strategia per l’IA: cosa deve contenere

La strategia DEVE…

- essere coerente con il contesto e allineata alla missione dell’ente;
- contenere obiettivi e azioni, con un approccio che coinvolga tutte le funzioni;
- contenere le misure di trasparenza sull’uso dell’IA;
- essere coerente con PIAO, strategia di data governance e Piano triennale;
- essere coordinata dal RTD e monitorata e aggiornata periodicamente.

Le azioni da includere

Qualità dei dati
migliorare dati e basi documentali con una data governance efficace

Competenze
su IA e protezione dei dati personali

Casi d’uso
individuare quelli a maggior beneficio

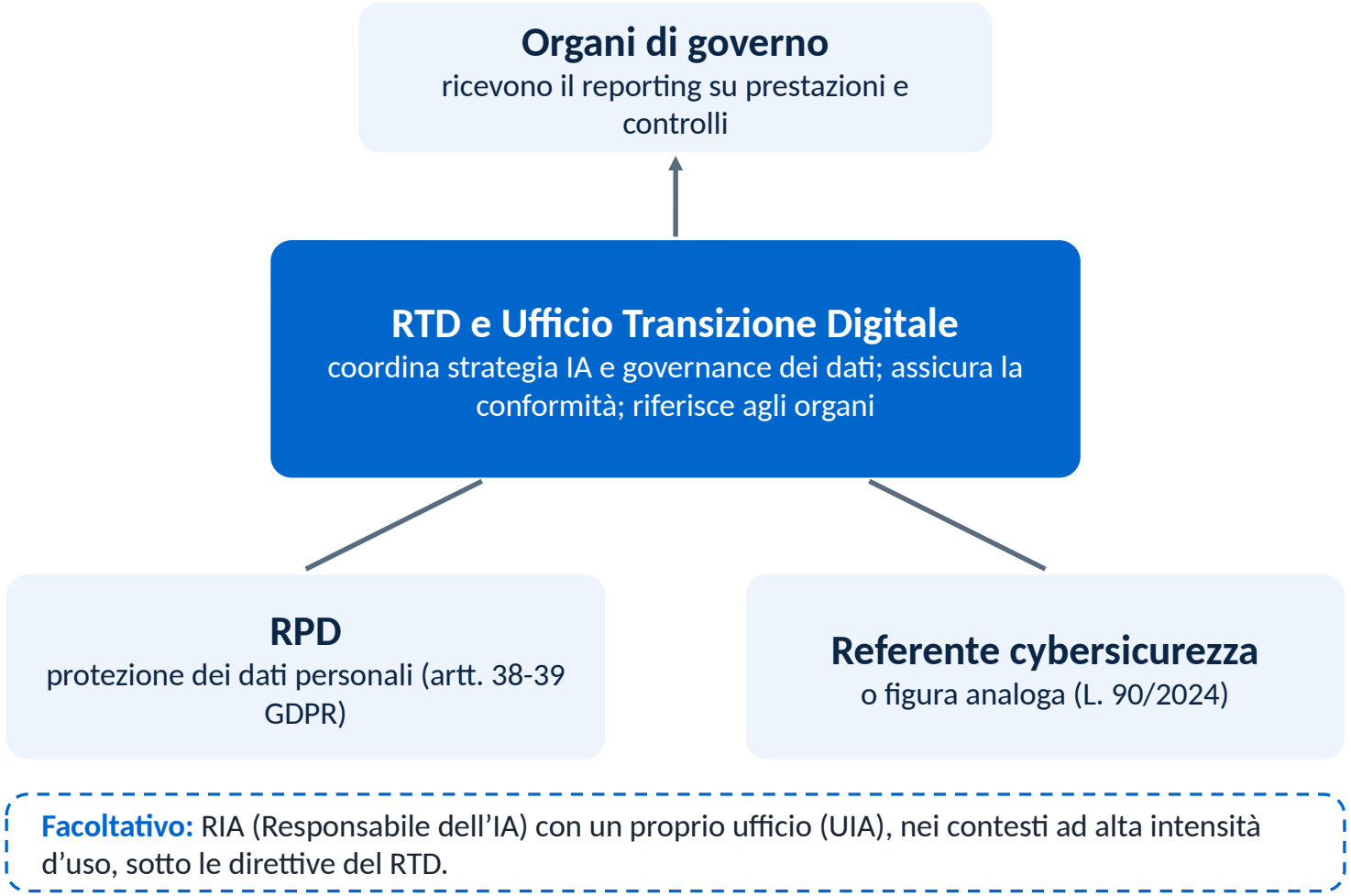
Esperienze altrui
valutare sperimentazioni già fatte da altre PA

Open source e open weight
con un orchestratore centralizzato multi-modello

Quick win e aggregazione
partire dai casi più semplici, anche in forma associata

Fonte: Linee Guida AgID, par. 4.1. La strategia PUÒ essere comune tra enti dello stesso tipo (es. comuni, università).

Governance: chi ne risponde



Facoltativo: RIA (Responsabile dell'IA) con un proprio ufficio (UIA), nei contesti ad alta intensità d'uso, sotto le direttive del RTD.

Fonte: Linee Guida AgID, par. 4.1, 4.6 e cap. 6.

Gli altri obblighi di governance

DEVONO essere definite procedure di governance per sviluppo e uso dell'IA, coerenti con strategia e PIAO.

PUÒ essere adottato un codice etico e di condotta per l'IA, che **DOVREBBE** diventare vincolante.

Il codice fissa anche le regole d'uso per i dipendenti, condivise con la dirigenza.

Dove l’IA porta più valore: gli ambiti prioritari

Efficienza operativa

- Supporto alle decisioni con modelli predittivi
- Gestione documentale: classificazione, archiviazione, ricerca
- Gestione della conoscenza da testi non strutturati

Servizi a cittadini e imprese

- Personalizzazione dei servizi
- Proattività: anticipare i bisogni
- Trasparenza sullo stato delle pratiche
- Accessibilità e contenuti nativamente accessibili
- Inclusione delle fasce deboli

Sicurezza e protezione dei dati

- Individuare minacce potenziali
- Protezione avanzata di dati e infrastrutture

La regola d’oro: impatto proporzionato a infrastrutture, competenze e risorse disponibili. Esigenze verificate e documentate, con analisi costi-benefici (art. 68 CAD).

Fonte: Linee Guida AgID, par. 4.3, basato sulla ricognizione AgID dei progetti IA nella PA avviata a settembre 2024.

Dal caso d’uso ai KPI

Ogni caso d’uso va documentato per tutto il ciclo di vita



Maturità misurabile con i Technology Readiness Level (ISO 16290); scheda caso d’uso ispirata alla ISO/IEC TR 24030.

Requisiti minimi da applicare (oltre ai 20 principi)

- **AI Act (cap. 5)**
- **Gestione e qualità dei dati (cap. 9)**
- **Protezione dei dati personali (cap. 10)**
- **Sicurezza cibernetica (cap. 11)**

KPI per ogni caso d’uso

- Prestazioni del modello
- Qualità dei dati
- Robustezza e affidabilità
- Efficienza computazionale
- Usabilità e accessibilità
- Impatto etico
- Conformità normativa
- Costo e sostenibilità

DEVONO essere monitorati lungo tutto il ciclo di vita.

Fonte: Linee Guida AgID, par. 4.5, 4.5.1, 4.5.2.

Piano operativo e risorse: lo stack da finanziare

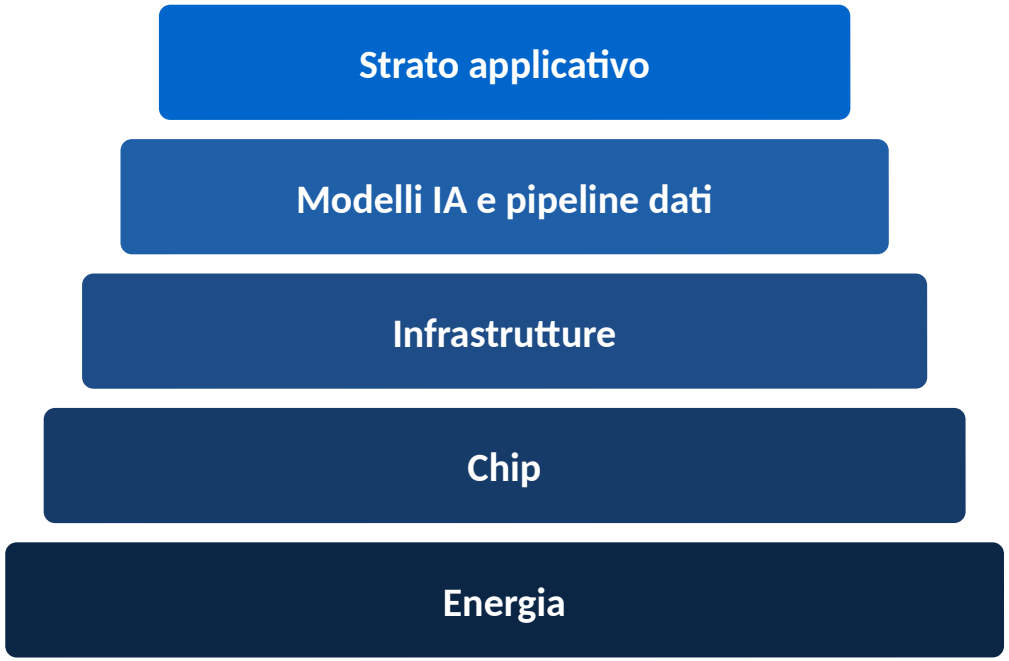
Il piano operativo DEVE...

- **definire le attività operative**
- **identificare le risorse richieste**
- **fissare i tempi di completamento**
- **assegnare responsabilità specifiche**
- **stabilire criteri di valutazione e monitoraggio**

...e includere gestione, procurement e sviluppo dei sistemi adottati o da adottare.

Fonte: Linee Guida AgID, par. 4.9 e 4.10 (stack tecnologico descritto nelle Linee Guida sviluppo).

Le risorse DEVONO coprire i cinque strati dello stack IA



Risorse finanziarie, tecnologiche e umane, adeguate a sviluppare, mantenere e migliorare con continuità.

Rischio e impatto: due valutazioni, un’unica regia

Gestione del rischio

DEVE esserci un sistema di gestione del rischio adeguato a finalità e contesto; conforme all’AI Act nei casi previsti.

- Riferimenti: UNI ISO 31000 e ISO/IEC 23894; norme armonizzate dove disponibili.
- Include i rischi per diritti e libertà legati ai dati personali (minimizzazione, privacy by design e by default).
- Se il sistema integra un GPAI, la classe di rischio può cambiare: va ricontrollata.

Valutazione d’impatto

FRIA (art. 27 AI Act) per l’alto rischio; integra la DPIA se già svolta.

DPIA (art. 35 GDPR) resta ferma quando ci sono dati personali.

DOVREBBE esserci una valutazione, anche semplificata, sui diritti fondamentali anche per il rischio minimo.

DEVONO essere documentati i risultati e condivisi con le parti interessate.

In fase di implementazione: entrambe le valutazioni si ripetono a intervalli pianificati e a ogni modifica significativa, con documentazione per tracciabilità e azioni correttive.

Fonte: Linee Guida AgID, par. 4.7, 4.8 e 4.11.

04

Conformità, dati e sicurezza

Obblighi, trasparenza, qualità dei dati, cybersicurezza

La conformità in quattro domande

1

È un sistema di IA?

Verifica con la definizione dell'art. 3 AI Act, anche per tecnologie già in uso.

2

Che livello di rischio?

Classifica secondo l'art. 6 AI Act: vietato, alto, limitato, minimo.

3

Che ruolo ho?

Fornitore o deployer; titolare o responsabile del trattamento (GDPR).

4

Quali obblighi si applicano?

Rischio + ruolo determinano le disposizioni dell'AI Act applicabili.

Anche per i sistemi a rischio limitato o minimo, le PA DEVONO:

- verificare che i dati siano trattati in conformità alle norme: protezione dei dati, trasferimenti verso Paesi terzi (artt. 44 ss. GDPR), diritto d'autore, normative di settore;
- garantire documentazione tecnica completa, utile a verificare trasparenza e spiegabilità, e aggiornata per tutto il ciclo di vita.

Fonte: Linee Guida AgID, cap. 5 e par. 5.2.

Alto rischio da deployer: i sette contenuti della FRIA

Processi della PA
in cui il sistema sarà utilizzato

Periodo e frequenza
di utilizzo del sistema

Persone e gruppi
verosimilmente interessati

Dati trattati
con attenzione ai dati personali

Rischi specifici
di danno per persone e diritti

Misure di risposta
governance interna e reclami

Sorveglianza umana
descrizione delle misure

Quando
prima dell'utilizzo, nei casi dell'art. 27 AI Act; può integrare la DPIA (art. 27, par. 4).

Se invece la PA è fornitore di un sistema ad alto rischio: monitoraggio post-commercializzazione documentato, gestione dei rischi riesaminata, informazioni comprensibili sul funzionamento, log automatici per tutto il ciclo di vita e documentazione tecnica conservata.

Fonte: Linee Guida AgID, par. 5.2.

Sorveglianza umana e documentazione

PA fornitore

DEVE progettare e sviluppare il sistema per un'efficace sorveglianza umana, con interfacce e strumenti di controllo adeguati.

PA deployer

DEVE adottare procedure e strumenti per monitorare, interpretare e, se serve, intervenire sulle decisioni generate dall'IA.

Chi sorveglia

RTD e UTD, con RPD e Referente cybersicurezza. Il personale incaricato deve avere competenza, esperienza e autorità.

Conservare la documentazione (art. 18 AI Act)

Dati, metadati e informazioni utili a verifiche, controlli e audit, per un periodo congruo e coerente con la conservazione del procedimento supportato dall'IA. Si applicano CAD e Linee Guida AgID sui documenti informatici.

Fonte: Linee Guida AgID, par. 5.3 e 5.4.

Trasparenza verso cittadini e imprese

L’informativa DEVE spiegare, in linguaggio semplice:

Cos’è e a cosa serve
tipo di IA impiegata e finalità del sistema

Come decide e con quale impatto
criteri, funzionamento, effetti su diritti e accesso ai servizi

Spiegazione delle decisioni
logica, dati e criteri determinanti (art. 22 GDPR)

Opposizione e intervento umano
canali, tempi di risposta, revisione da parte di un operatore

I tre principi cardine richiamati dal Garante

1. Conoscibilità
diritto di sapere che esiste una decisione automatizzata e di capirne la logica

2. Non esclusività
c’è sempre un intervento umano che può controllare, validare o smentire (human in the loop)

3. Non discriminazione
sistemi affidabili, verificati periodicamente, che riducono opacità ed errori

Fonte: Linee Guida AgID, cap. 7 e cap. 10; AI Act art. 50; GDPR artt. 12-14 e 22.

Dati: la qualità viene prima della quantità

Caratteristiche di qualità da garantire

Base (Linee Guida Open Data)

Accuratezza | Coerenza | Completezza | Attualità

In più, per l'IA (ISO/IEC 25012 e ISO/IEC 5259-2)

Rappresentatività | Bilanciamento | Tracciabilità | Disponibilità | Credibilità

- Pubblicare come open data i dataset pubblicabili, con licenze permissive (CC BY 4.0, CC0 o equivalenti).
- Fortemente raccomandato usare dataset istituzionali per addestrare i sistemi.
- Governance dei dati ricondotta a un'unica struttura di coordinamento (open data, art. 50-ter CAD, dati per l'IA).

IA in cloud e fornitori

DEVONO essere individuati fornitori e subfornitori della catena di erogazione.

DEVONO esserci garanzie che i fornitori non usino i dati per finalità proprie.

DEVE essere esplicitato ai responsabili del trattamento (art. 28 GDPR) il divieto di usare i dati per addestrare modelli destinati a terzi.

DEVE essere valutato se il modello è davvero anonimo.

Fonte: Linee Guida AgID, par. 9.2, 9.3 e cap. 10 (rif. parere EDPB n. 28/2024).

Cybersicurezza: nuove minacce, obiettivi chiari

Le quattro famiglie di attacco (tassonomia NIST)

Evasion attacks

input manipolati che ingannano il modello

Poisoning attacks

dati di addestramento «avvelenati»

Privacy attacks

ricostruzione di dati o del modello

Abuse attacks

uso distorto dell'IA generativa (frodi, malware, disinformazione)

Ciclo di gestione: sicurezza in ogni fase → audit e controlli di conformità → revisione continua delle misure.

Nove obiettivi di sicurezza (Linee Guida NCSC, sottoscritte anche da ACN)

1. Adottare l'IA in modo responsabile
2. Identificare e proteggere gli asset
3. Proteggere la supply chain
4. Proteggere modello e dati
5. Monitorare sistema e input
6. **Piano di risposta agli incidenti**
7. Formare il personale su minacce e rischi
8. Proteggere l'infrastruttura ICT
9. Proteggere identità e accessi (MFA)

Fonte: Linee Guida AgID, par. 11.1, 11.5 e 11.6. Le norme CEN/CENELEC JTC 21 DEVONO essere tenute in considerazione.

05

Competenze e prossimi passi

Cosa si chiede ai dirigenti e come partire

Cosa le Linee Guida chiedono ai dirigenti

Competenze adeguate alle responsabilità
per valutare opportunità, benefici, rischi e impatti dei progetti e garantire la conformità.

Obiettivi di performance
legati alla formazione su decision making e guida dei processi di adozione dell'IA.

Visione strategica e soft skills
leadership e change management, oltre alla comprensione di minacce e mitigazioni.

AI literacy per tutto il personale
competenza digitale di base (art. 4 AI Act), da pianificare e rendicontare nel PIAO.

Dove formarsi

- Syllabus: «Competenze digitali per la PA» e percorsi sull'IA per dirigenti e non specialisti
- Scuola Nazionale dell'Amministrazione e poli territoriali
- Formez PA e Università, anche con «PA 110 e lode»
- Community ReTe Digitale di AgID per RTD e UTD
- Percorsi su cybersicurezza dell'IA e protezione dei dati

Fonte: Linee Guida AgID, cap. 8 e par. 8.1; Direttiva del Ministro per la PA sulla formazione del 14 gennaio 2025.

Una roadmap di avvio in 100 giorni

Giorni 1-30
Organizzarsi

- Confermare la regia: RTD con RPD e Referente cybersicurezza
- Censire i sistemi di IA già in uso, inclusi quelli nei gestionali
- Classificarli per rischio e ruolo

Giorni 31-60
Decidere le regole

- Strategia IA coerente con il PIAO
- Codice di condotta con le regole d'uso per il personale
- Piano formativo: AI literacy per tutti

Giorni 61-100
Partire bene

- 1-2 quick win a basso rischio con KPI
- DPIA o FRIA dove necessarie
- Informative chiare per i cittadini

Proposta operativa del relatore, costruita sugli obblighi delle Linee Guida: tempi e sequenza vanno adattati a dimensione e maturità dell'ente.

Cinque domande per il prossimo comitato di direzione

- Sappiamo quali sistemi di IA stiamo già usando, anche dentro i software che abbiamo acquistato?
- Chi è il nostro punto di regia sull’IA, e RTD, RPD e Referente cybersicurezza lavorano davvero insieme?
- La nostra strategia IA è scritta, è nel PIAO e contiene misure di trasparenza?
- I nostri contratti vietano ai fornitori di usare i nostri dati per finalità proprie o per addestrare modelli per terzi?
- Il personale ha ricevuto una formazione di base sull’IA, e chi sorveglia i sistemi ha autorità per fermarli?

Domande costruite dal relatore sui requisiti dei capitoli 4, 5, 8, 9 e 10 delle Linee Guida.

Grazie per l’attenzione

Linee Guida AgID per l’adozione di IA nella PA · Modulo per dirigenti



Vincenzo Calabrò

Relatore

Domande, dubbi, casi concreti?
Continuiamo la conversazione su LinkedIn: inquadra il QR code.

linkedin.com/in/vincenzocalabro