Usare l’IA al lavoro: bene, in modo consapevole e sicuro

Le Linee Guida AgID per l’adozione di IA nella Pubblica Amministrazione spiegate a chi la usa ogni giorno

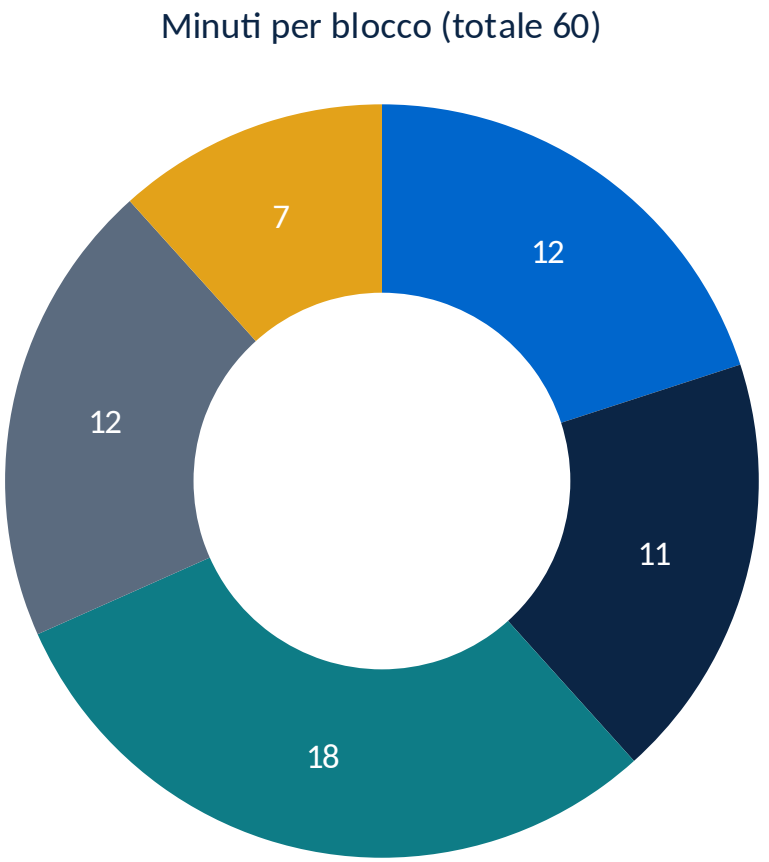


MODULO PER UTILIZZATORI · 60 MINUTI

Relatore: Vincenzo Calabrò

Il percorso di oggi

1	**Cos’è (e cosa non è) l’IA** Come ragiona, dove la incontri, perché può sbagliare	12′
2	**Le regole del gioco** Livelli di rischio, ruoli, principi, codice di condotta	11′
3	**Usarla bene ogni giorno** Verifica umana, trasparenza, diritti dei cittadini, buone pratiche	18′
4	**Dati, privacy e sicurezza** Cosa condividere, cosa no, come riconoscere gli attacchi	12′
5	**Chi chiamare e come crescere** Ruoli di riferimento, formazione, autoverifica finale	7′



Perché questo riguarda proprio te

L’AI literacy è diventata una competenza digitale di base.

Le PA DEVONO garantire che tutto il personale acquisisca un adeguato livello di alfabetizzazione sull’IA, per usarla in modo consapevole, corretto e responsabile.

Lo chiede l’AI Act

L’art. 4 impone a fornitori e deployer di sostenere l’alfabetizzazione di chi usa l’IA per loro conto.

Lo prevede la Direttiva 2025

La Direttiva del Ministro per la PA sulla formazione riconosce l’AI literacy come competenza digitale di base.

Ti protegge

Sapere come funziona l’IA significa sapere quando fidarsi, quando verificare e quando fermarsi.

Fonte: Linee Guida AgID, cap. 8 e par. 8.1; AI Act art. 4.

01

Cos’è (e cosa non è) l’IA

Come ragiona, dove la incontri, perché può sbagliare

Un sistema di IA, in parole semplici



Gli dai qualcosa

una domanda, un documento, dei dati



Lui «deduce»

elabora l'input sulla base di ciò che ha appreso dai dati



Ti restituisce

una previsione, un testo, un suggerimento o una decisione

La definizione ufficiale (art. 3 AI Act)

Un sistema automatizzato, con livelli di autonomia variabili, che può adattarsi dopo la messa in uso e che, per obiettivi espliciti o impliciti, deduce dall'input come generare output (previsioni, contenuti, raccomandazioni o decisioni) che possono influenzare ambienti fisici o virtuali.

Fonte: Linee Guida AgID, cap. 3 (definizione dell'AI Act, art. 3, punto 1, in sintesi).

Calcolatrice o oracolo? Né l’una né l’altro

Software deterministico

- Stesso input, sempre lo stesso output
- Segue regole esplicite, scritte da qualcuno
- Se sbaglia, l’errore si riproduce sempre uguale

IA generativa

- Logica statistico-probabilistica: lo stesso input può dare risposte diverse
- Output soggetti a margini di incertezza
- Può sbagliare con un tono sicuro e convincente

Quindi: l’output dell’IA è una bozza da verificare, non una verità da copiare. Più l’esito incide su diritti, equità o accesso ai servizi, più la verifica deve essere attenta.

Fonte: Linee Guida AgID, cap. 3.

Dove la incontri, spesso senza accorgertene

Applicazioni sviluppate per l'ente
soluzioni su misura per un procedimento o un servizio

Nuove versioni di gestionali e office
funzioni di IA integrate negli aggiornamenti dei software che già usi

Motori di ricerca basati su IA
risposte sintetiche al posto dell'elenco di link

App di IA generativa personali
con licenze individuali, gratuite o a pagamento

Social media
applicazioni di IA integrate nelle piattaforme

Attenzione al «fai da te»

Le Linee Guida invitano a essere consapevoli delle implicazioni quando si portano al lavoro le abitudini della vita privata.

Un account personale su un'app di IA non è uno strumento dell'ente: non sai dove finiscono i dati, chi li vede, se servono ad addestrare il modello.

Prima di usarla per lavoro, chiedi se è autorizzata.

Fonte: Linee Guida AgID, cap. 8 (AI literacy e AI awareness).

Bias: quando l’IA eredita i nostri pregiudizi

Bias nei dati

I dati di addestramento riflettono pregiudizi o lacune.

Esempio: un modello allenato su pratiche in cui un gruppo è sottorappresentato funzionerà peggio proprio per quel gruppo.

Bias nell’algoritmo

Scelte tecniche e ipotesi del modello distorcono i risultati.

Esempio: un criterio di priorità che sembra neutro ma penalizza chi ha percorsi non standard.

Bias nelle persone

Pregiudizi di chi progetta o usa il sistema entrano nel processo.

Esempio: accettare senza verifica gli output che confermano le nostre aspettative.

Fonte: Linee Guida AgID, cap. 3 (rif. ISO/IEC TR 24027). Esempi illustrativi del relatore.

Cosa può fare l’IA per il tuo ufficio

Gestione documentale

classificare, archiviare e ritrovare documenti più in fretta

Gestione della conoscenza

estrarre informazioni e concetti da testi non strutturati

Supporto alle decisioni

modelli predittivi per decisioni basate sui dati

Servizi più vicini alle persone

personalizzazione, proattività, informazioni chiare sullo stato delle pratiche

Accessibilità e inclusione

contenuti nativamente accessibili, attenzione alle fasce deboli

Sicurezza

individuare minacce a dati e infrastrutture

Fonte: Linee Guida AgID, par. 3.4 e 4.3.

02

Le regole del gioco

Rischio, ruoli, principi e codice di condotta

Non tutta l’IA è uguale: quattro livelli di rischio

		Cosa significa per te
Vietato	Mai: manipolazione subliminale, social scoring. Vietati dal 2 febbraio 2025.	**Se ti chiedono qualcosa del genere, fermati e segnala.**
Alto rischio	Sistemi che incidono su salute, sicurezza, diritti fondamentali (es. accesso a servizi essenziali).	**Procedure strutturate e sorveglianza umana formale.**
Rischio limitato	Obblighi di trasparenza (art. 50): chi interagisce con l’IA deve saperlo.	**Dichiara quando un testo o un’immagine sono generati dall’IA.**
Rischio minimo	Impatto trascurabile sui diritti.	**Usa il buon senso e le regole dell’ente.**

Fonte: Linee Guida AgID, par. 3.3 (classificazione dell’AI Act). Indicazioni pratiche a destra: sintesi del relatore.

Chi è responsabile di cosa

Provider (fornitore)
sviluppa il sistema o il modello e lo immette sul mercato con il proprio nome

↓

Deployer
l'ente che usa il sistema sotto la propria autorità: quasi sempre la tua amministrazione

↓

Tu, utilizzatore
usi lo strumento per conto dell'ente, secondo le sue regole

Il principio P.5: responsabilità

L'IA è uno strumento di supporto all'attività umana. La responsabilità ultima delle decisioni, qualunque sia il livello di automazione, rimane in capo alla PA.

Tradotto: «l'ha scritto l'IA» non è mai una giustificazione. Ciò che firmi o invii resta un atto dell'ente, di cui rispondi anche tu.

Fonte: Linee Guida AgID, par. 3.2 e 3.4 (P.5).

I principi che ti riguardano da vicino

P.5 Responsabilità
la decisione resta umana e dell'ente

P.6 Non discriminazione
trattamento equo, attenzione ai bias

P.7-P.8 Trasparenza
chi interagisce con l'IA deve saperlo

P.4 Dati personali
rispetto delle norme sulla protezione dei dati

P.10 Accuratezza
risultati corretti, errori individuati e corretti

P.12 Cybersicurezza
protezione da manomissioni e usi illeciti

P.13 Sorveglianza umana
possibilità di verificare, correggere, sostituire

P.14 Logging
le operazioni vengono tracciate e conservate

Fonte: Linee Guida AgID, par. 3.4 (selezione di 8 dei 20 principi).

Il codice di condotta del tuo ente

Le Linee Guida prevedono che ogni PA possa adottare un codice etico e di condotta per l'IA che:

introduce regole di utilizzo per i dipendenti
condivise con la dirigenza e i vertici amministrativi

aiuta a scegliere e usare i sistemi
integrando le norme applicabili

promuove una cultura condivisa
di responsabilità nell'uso dell'IA

viene rivisto periodicamente
per seguire tecnologia, norme e organizzazione

Tre domande da farti oggi

- Il mio ente ha un codice di condotta o regole d'uso dell'IA? Dove le trovo?
- Quali strumenti di IA sono autorizzati per il mio lavoro?
- Per quali attività o dati l'uso dell'IA è escluso o richiede cautele?

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

03

Usarla bene, ogni giorno

Verifica umana, trasparenza, diritti dei cittadini, buone pratiche

Human in the loop: l’ultima parola è tua

1. Conoscibilità

Chi è interessato da una decisione ha diritto di sapere che c’è un processo automatizzato e di capirne la logica.

2. Non esclusività

Nel processo deve esserci sempre un intervento umano capace di controllare, validare o smentire la decisione automatica.

3. Non discriminazione

Vanno usati sistemi affidabili, verificati periodicamente, che riducano opacità ed errori.

L’umano nel ciclo sei tu. Sorvegliare non significa dare un’occhiata: significa capire l’output, confrontarlo con le fonti e poterlo correggere o scartare. Se non sei in grado di farlo, non firmarlo.

Fonte: Linee Guida AgID, cap. 10 (principi richiamati dal Garante per la protezione dei dati personali) e par. 3.4 (P.13).

Cinque passi prima di usare un output dell’IA

1

Strumento autorizzato?

Usa solo sistemi messi a disposizione o approvati dall’ente.

2

Dati ammessi?

Inserisci solo i dati necessari; evita quelli personali se non previsto.

3

Richiesta chiara

Contesto, obiettivo, formato atteso: un buon prompt riduce gli errori.

4

Verifica

Controlla fatti, norme citate, numeri e nomi sulle fonti ufficiali.

5

Decidi e dichiara

Rivedi, correggi, assumi la responsabilità; indica l’uso dell’IA se richiesto.

Buona pratica del relatore, costruita su principi P.4, P.5, P.8, P.10 e P.13 delle Linee Guida e sulle regole del tuo ente.

Scrivere richieste efficaci (prompt)

✗ Così no

«Scrivimi una risposta al cittadino sul permesso.»

- Nessun contesto: quale permesso, quale normativa?
- Nessun vincolo: tono, lunghezza, destinatario
- L'IA «riempie i vuoti» inventando dettagli

✓ Così sì

«Sei un funzionario dell'ufficio SUAP. Scrivi una risposta cortese e chiara, in max 150 parole, a un cittadino che chiede i tempi per [procedimento]. Usa solo le informazioni nel testo che incollo sotto. Se un dato manca, scrivi "da verificare".»

Ruolo · compito · vincoli · fonte · cosa fare se manca un dato

Il prompt migliora la qualità, non elimina le allucinazioni: la verifica resta obbligatoria. Esempio illustrativo del relatore.

Trasparenza: dire quando c’è di mezzo l’IA

Interazione con l’IA
Le persone devono sapere quando stanno comunicando con una macchina anziché con un essere umano (es. chatbot).

Contenuti generati
Testi, immagini, audio o video sintetici DEVONO essere identificati chiaramente come generati artificialmente.

Informativa chiara
L’ente spiega finalità, criteri e conseguenze dell’uso dell’IA in linguaggio semplice e accessibile.

Esempio di dicitura

«Questa risposta è stata predisposta con il supporto di un sistema di intelligenza artificiale e verificata da un operatore dell’ufficio.»

Formula di esempio: la dicitura ufficiale la decide il tuo ente.

Perché conta: solo chi sa che c’è un sistema automatizzato può esercitare i propri diritti di accesso, rettifica e opposizione.

Fonte: Linee Guida AgID, cap. 7 (art. 50 AI Act). Dicitura: esempio del relatore.

Se un cittadino contesta una decisione

Ascolta

Il cittadino può opporsi a una decisione automatizzata e chiedere l'intervento umano.

Spiega

Fornisci informazioni chiare sulla logica, sui criteri e sui dati principali che hanno inciso sull'esito.

Riesamina

Una persona riesamina la decisione e, se necessario, la modifica.

Registra

Le segnalazioni alimentano il registro dei reclami e il monitoraggio del sistema.

Base normativa: art. 22 GDPR sulle decisioni automatizzate e informativa prevista dal cap. 7 delle Linee Guida. Le procedure, i canali e i tempi di risposta DEVONO essere indicati ai cittadini: verifica quali sono nel tuo ente.

Fonte: Linee Guida AgID, par. 7.2 e 5.2 (acquisizione e analisi dei reclami).

Hai notato qualcosa che non va? Segnalalo

Errori ricorrenti

risposte sbagliate sempre sullo stesso tema

Possibili discriminazioni

esiti diversi per casi simili, penalizzazioni di un gruppo

Comportamenti anomali

output strani, improvvisi cambi di qualità

Dati fuori posto

informazioni di altri utenti o dati che non dovresti vedere

Perché la tua segnalazione conta

Il monitoraggio dei sistemi di IA si basa anche sulla raccolta strutturata delle segnalazioni di utenti, cittadini e operatori della PA. Chi usa lo strumento ogni giorno vede per primo derive, bias e anomalie.

Un errore segnalato è un errore che non si ripete.

Fonte: Linee Guida AgID, par. 5.2 e 11.4.

04

Dati, privacy e sicurezza

Cosa condividere, cosa no, come riconoscere gli attacchi

Il semaforo dei dati

Rosso: non inserire

- Categorie particolari di dati (salute, opinioni, ecc.) e dati giudiziari (artt. 9-10 GDPR)
- Dati personali in strumenti non autorizzati o con account personali
- Informazioni riservate, credenziali, documenti classificati

Giallo: solo se previsto

- Dati personali in sistemi autorizzati, per finalità definite
- Solo i dati strettamente necessari (minimizzazione)
- Meglio anonimizzati o pseudonimizzati quando possibile

Verde: via libera

- Testi e normative pubbliche
- Open data e documenti già pubblicati
- Bozze prive di dati personali o riservati

Sintesi del relatore basata su cap. 10 (art. 5 GDPR, minimizzazione) e par. 9.3. Fa sempre fede la policy del tuo ente.

Privacy: i principi del GDPR valgono anche con l’IA

Liceità e trasparenza
serve una base giuridica e l’interessato va informato

Limitazione della finalità
i dati si usano per finalità determinate e compatibili

Minimizzazione
solo i dati necessari; anonimi o sintetici se possibile

Esattezza
dati corretti e aggiornati

Limitazione della conservazione
tempi di conservazione definiti

Sicurezza
misure adeguate al rischio, anche specifiche per l’IA

Da ricordare

- L’ente resta titolare del trattamento anche quando il sistema è del fornitore.
- Il RPD va coinvolto in ogni fase del ciclo di vita.
- Prima di trattare dati personali con l’IA, l’ente fa una DPIA, anche per sistemi non ad alto rischio.

Fonte: Linee Guida AgID, cap. 10 (art. 5 GDPR; art. 35 GDPR).

Come si attacca un sistema di IA

Evasion attacks
Input modificati in modo quasi invisibile ingannano il modello.

Esempio citato: piccoli adesivi su un segnale di stop che il modello non riconosce più.

Poisoning attacks
Qualcuno «avvelena» i dati di addestramento.

Esempio citato: etichette cambiate da spam a non-spam per far passare la posta indesiderata.

Privacy attacks
Interrogando il modello si ricostruiscono dati o informazioni su di esso.

Esempio: capire se i dati di una persona erano nel dataset (membership inference).

Abuse attacks
L'IA generativa viene piegata a frodi, malware o disinformazione.

Mitigazioni: filtraggio degli input, rilevamento di output anomali.

Fonte: Linee Guida AgID, par. 11.1 (tassonomia NIST, Adversarial Machine Learning, 2024).

Igiene di sicurezza: le abitudini che fanno la differenza

Accessi protetti

Usa l'autenticazione multi-fattore (MFA) e non condividere mai le credenziali.

Ruoli e permessi

Accedi solo a ciò che serve al tuo ruolo; segnala accessi impropri.

Fonti verificate

Niente plug-in, estensioni o modelli scaricati da fonti non verificate.

Occhio alle anomalie

Cambi improvvisi di comportamento possono indicare una compromissione.

Incidenti

In caso di sospetto incidente, avvisa subito: l'ente ha un piano di risposta.

Aggiornati

La formazione su minacce e rischi è uno degli obiettivi di sicurezza.

Fonte: Linee Guida AgID, par. 11.5 (obiettivi di sicurezza 3, 5, 6, 7 e 9).

05

Chi chiamare e come crescere

Ruoli di riferimento, formazione, autoverifica

Hai un dubbio? Ecco a chi rivolgerti

RTD e Ufficio Transizione Digitale
strategia IA, strumenti autorizzati, governance e sorveglianza dei sistemi

Responsabile protezione dati (RPD)
dati personali, DPIA, diritti degli interessati

Referente per la cybersicurezza
incidenti, attacchi, comportamenti sospetti

Il tuo dirigente
regole d'uso nel tuo ufficio, codice di condotta, priorità

Negli enti con un uso intenso dell'IA può esserci anche un Responsabile dell'IA (RIA), che opera seguendo le direttive del RTD.

Fonte: Linee Guida AgID, par. 4.1, 4.6 e 5.3.

Continuare a imparare

Syllabus
Percorso «Competenze digitali per la PA» e moduli sull'IA per dipendenti non specialisti

DigComp 3.0
Il quadro europeo delle competenze digitali, che integra l'IA, inclusa l'IA generativa

Formazione del tuo ente
Interventi mirati su temi specifici, pianificati e rendicontati nel PIAO

Cyber e privacy
Percorsi su sicurezza dell'IA e protezione dei dati personali, previsti nei piani formativi

AI literacy significa...

- sapere che l'IA esiste e influenza il lavoro (AI awareness);
- capire come e perché lo fa;
- conoscerne le implicazioni operative, normative ed etiche;
- saper gestire i rischi di sicurezza legati all'IA e ai dati.

Fonte: Linee Guida AgID, cap. 8 e par. 8.1.

Autoverifica: vero o falso?

1	Se l’IA ha prodotto un errore in un atto, la responsabilità è del fornitore del sistema.	V / F
2	Un testo generato dall’IA e inviato a un cittadino va identificato come tale.	V / F
3	Posso usare la mia app personale di IA per riassumere una pratica con dati sanitari.	V / F
4	Il cittadino può chiedere che una decisione automatizzata sia riesaminata da una persona.	V / F
5	Se un output sembra plausibile e ben scritto, posso considerarlo verificato.	V / F

Le risposte sono nelle note del relatore.

Sei cose da ricordare domani mattina

Decidi tu

L’IA supporta, la responsabilità resta all’ente e a chi firma.

Verifica sempre

Fatti, norme, numeri e nomi: controllali sulle fonti ufficiali.

Solo strumenti autorizzati

Niente account personali per attività di lavoro.

Meno dati possibile

Mai dati particolari o riservati fuori dalle regole dell’ente.

Dichiara l’IA

Chi riceve un contenuto generato deve poterlo sapere.

Segnala

Errori, bias e anomalie vanno riportati, non aggirati.

Sintesi del relatore dei contenuti del modulo.

Grazie per l’attenzione

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



Vincenzo Calabrò

Relatore

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

linkedin.com/in/vincenzocalabro