

Allegato A

Matrice di classificazione del rischio dei sistemi di Intelligenza Artificiale

1. Finalità dell'Allegato

La presente Matrice ha la finalità di:

- supportare le strutture regionali nella valutazione preventiva del rischio connesso all'utilizzo di sistemi di Intelligenza Artificiale;
- garantire un'applicazione uniforme, proporzionata e trasparente delle presenti Linee guida;
- individuare le misure di governance, controllo umano e monitoraggio adeguate al livello di rischio.

La classificazione del rischio è effettuata prima della messa in esercizio del sistema di IA e aggiornata in caso di modifiche rilevanti.

La Matrice è adottata in coerenza con la classificazione del rischio e dell'impatto definita dall'Agenzia per la Cybersicurezza Nazionale ai sensi della Determinazione n. 127437/2026, nonché con la disciplina NIS2 e il SGSI regionale.

2. Criteri di valutazione del rischio

La valutazione si basa sui seguenti criteri cumulativi, da analizzare nel contesto concreto di utilizzo del sistema.

Criterio	Descrizione
Ambito di utilizzo	Funzione amministrativa, supporto interno, servizio al cittadino
Tipo di procedimento	Procedimento vincolato, discrezionale, valutativo
Incidenza sui diritti	Assenza, incidenza indiretta, incidenza diretta su diritti/interessi
Grado di automazione	Supporto istruttorio, raccomandazione, automazione decisionale
Reversibilità degli effetti	Facilmente reversibili / difficilmente reversibili
Destinatari	Utenti interni / cittadini / imprese
Scala di utilizzo	Limitata / sistematica / massiva
Trasparenza e Comprensibilità	Alta / media / bassa
Possibili bias o discriminazioni	Assenti / potenziali / elevati

3. Classificazione del livello di rischio e impatto

La classificazione del livello di rischio e di impatto costituisce presupposto per l'individuazione delle misure di sicurezza, di governance e di monitoraggio, in coerenza con il SGSI e con gli adempimenti previsti dalla normativa NIS.

Sulla base dei criteri di cui al paragrafo 2, il sistema di Intelligenza Artificiale è classificato secondo una scala di rischio e di impatto coerente con la classificazione adottata dall'Agenzia per la Cybersicurezza Nazionale (ACN), ai sensi della Determinazione ACN n. 127437/2026, articolata nei seguenti livelli:

La classificazione del livello di rischio e di impatto di cui al presente Allegato è distinta e complementare rispetto alla classificazione dei sistemi di IA prevista dall'AI Act.

In particolare:

- la classificazione AI Act individua la tipologia giuridica del sistema (vietato, alto rischio, rischio limitato, minimo);

- la classificazione ACN valuta l'impatto operativo, organizzativo e di sicurezza del sistema nel contesto concreto di utilizzo.

Entrambe le classificazioni concorrono alla definizione delle misure di governance e controllo.

A. Rischio BASSO

Caratteristiche principali

- utilizzo per supporto interno o attività meramente strumentali;
- assenza di effetti diretti o indiretti su diritti o posizioni giuridiche;
- output utilizzato esclusivamente come ausilio operativo.

Esempi

- supporto alla redazione di testi interni;
- analisi statistiche descrittive;
- sistemi di ricerca e classificazione documentale.

Misure richieste

- informazione agli utenti interni sull'uso dell'IA;
- verifica di base di sicurezza e protezione dei dati;
- controllo umano sempre presente.

B. Rischio MEDIO

Caratteristiche principali

- interazione con cittadini, imprese o utenti esterni;
- incidenza indiretta sull'accesso ai servizi o sull'organizzazione delle attività;
- output che può orientare, ma non determinare, decisioni o priorità.

Esempi

- chatbot informativi;
- sistemi di supporto alla gestione delle istanze;
- prioritizzazione non vincolante delle pratiche.

Misure richieste

- obblighi di trasparenza verso gli utenti;
- possibilità di intervento umano effettivo;
- monitoraggio periodico delle prestazioni;
- gestione delle segnalazioni e dei reclami.

C. Rischio ALTO

Caratteristiche principali

- utilizzo in procedimenti amministrativi che incidono su diritti, benefici, sanzioni o accesso a servizi essenziali;
- rischio di discriminazioni, errori sistemici o effetti significativi;
- influenza rilevante sull'esito del procedimento, pur in presenza di controllo umano.

Esempi

- sistemi di valutazione automatizzata di requisiti;
- classificazione dei beneficiari;
- supporto avanzato a procedimenti discrezionali.

Misure obbligatorie

- utilizzo esclusivo di sistemi conformi all'AI Act;
- documentazione tecnica completa;
- supervisione umana rafforzata e documentata;
- formazione specifica degli operatori;

- tracciabilità e conservazione dei log;
- monitoraggio post-deployment continuativo;
- svolgimento delle valutazioni di impatto richieste (DPIA, FRIA, BIA)
- integrazione del sistema di IA nei processi di gestione del rischio e degli incidenti di sicurezza previsti dal SGSI regionale, con segnalazione tempestiva di eventi rilevanti.

La classificazione è effettuata sulla base di un'analisi motivata e documentata, conservata agli atti, ed è soggetta a riesame periodico, in particolare in caso di modifiche del contesto normativo, tecnologico o organizzativo.

4. Fattispecie vietate

Non rientrano nella classificazione del livello di rischio e di impatto i sistemi di Intelligenza Artificiale che costituiscono pratiche vietate ai sensi della normativa europea o risultano incompatibili con i principi costituzionali, i diritti fondamentali e la funzione pubblica.

Tali sistemi sono in ogni caso vietati e non possono essere adottati o utilizzati dalla Regione Basilicata, indipendentemente da ogni valutazione di mitigazione.

5. Coordinamento con gli altri allegati

La Matrice di classificazione del rischio:

- opera in coordinamento con il Glossario di Intelligenza Artificiale (Allegato B);
- supporta le attività di valutazione previste dal GDPR, dal PIAO e dalle politiche di gestione del rischio regionale.