



MIGLIORARE LA SICUREZZA, LA PRIVACY
E LA ROBUSTEZZA DEI MODELLI E DEI
SISTEMI DI INTELLIGENZA ARTIFICIALE
(SECUREAI) - (HORIZON-CL3-2026-02-CS-
ECCCC-02)

UNIONE EUROPEA

UNIONE EUROPEA

MIGLIORARE LA SICUREZZA, LA PRIVACY E LA ROBUSTEZZA DEI MODELLI E DEI SISTEMI DI INTELLIGENZA ARTIFICIALE (SECUREAI) - (HORIZON-CL3-2026-02-CS-ECCC-02)

SCADENZA

15/09/2026

AREA GEOGRAFICA:	EUROPEO
SETTORE ATTIVITÀ:	INNOVAZIONE
BENEFICIARI:	3 SOGGETTI GIURIDICI INDIPENDENTI IN 3 PAESI DIVERSI
SPESE FINANZIATE:	SPESE DIRETTAMENTE NECESSARIE ALLA REALIZZAZIONE DEL PROGETTO- PERSONALE
TIPO AGEVOLAZIONE:	CONTRIBUTO A FONDO PERDUTO
DOTAZIONE FINANZIARIA:	15.000.000 €

Finalità

Gli obiettivi riguardano:

- lo **sviluppo** di **tecnologie, strumenti e processi** che rafforzino la **cibersicurezza** utilizzando componenti tecnologiche di intelligenza artificiale, in particolare l'AI generativa;
- lo **sviluppo** di **nuovi strumenti e processi avanzati** per la **cibersicurezza operativa** in risposta a un panorama di minacce in rapida evoluzione e a un forte aumento degli attacchi informatici e delle vulnerabilità;
- lo **sviluppo** di **tecnologie avanzate** di tutela della privacy (Privacy Enhancing Technologies) per la condivisione sicura dei dati, l'elaborazione di dati personali e industriali e la creazione di spazi europei dei dati conformi al GDPR;
- la **valutazione** della **sicurezza** delle primitive di crittografia post-quantistica (PQC), incluse analisi di robustezza rispetto ad attaccanti quantistici;
- la **sicurezza** delle **implementazioni** di **algoritmi PQC**, con attenzione agli attacchi a canale laterale e di fault injection;
- l'**integrazione** di **algoritmi PQC** in protocolli di alto livello, con relativa analisi di sicurezza e contributo ai processi di standardizzazione e alle implementazioni open source.

Beneficiari

- Consorzio con almeno **3 soggetti giuridici indipendenti** in **3 Paesi diversi** (almeno 1 in Stato Membro UE + almeno 2 in altri Stati Membri o Paesi Associati)

Agevolazioni

- **Tipo di azione: IA - Innovation Action**
- **Tasso di finanziamento massimo (Horizon): 70%** dei costi ammissibili (**fino al 100% per enti non-profit**).

Cosa Finanzia

Il topic si aspetta progetti che sviluppino e validino, tra le altre cose:

- **Modelli IA robusti** contro attacchi avversari (adversarial training, robust optimisation, ecc.).
- **Rilevazione e mitigazione** di dataset manipolati/avvelenati (anomaly detection, provenance tracking, validazione automatica dati).

- **“Private AI”**: addestramento/uso IA in ambienti privacy-preserving (federated learning, secure aggregation, calcolo su dati cifrati, homomorphic encryption “quantum-safe”, secure inference, ecc.), per casi d’uso sensibili (PA, imprese).

Spese Ammissibili

- **personale, subcontratti, acquisti**, ecc.
- **indiretti**

Termini

Le domande possono essere presentate **dal 03 marzo 2026 al 15 settembre 2026**

Normativa

<https://tinyurl.com/257jdzy4>

Per Approfondimenti

<https://tinyurl.com/287q2rjq>



Per maggiori informazioni su questo bando, CLICCA QUI

Clausola di esclusione di responsabilità

Il presente documento di sintesi ha finalità illustrativa ed esemplificativa.

La Sef Sas non assume alcuna responsabilità per quanto riguarda il contenuto della scheda di sintesi e ricorda che fa fede, per una visione integrale ed esaustiva, unicamente la normativa e la modulistica di riferimento della misura agevolativa, pubblicata secondo le modalità previste dal bando