pertec

MINISTERO DELLE IMPRESE E DEL MADE IN ITALY

BANDO CYBER 4.0 PER I PROGETTI DI INNOVAZIONE TECNOLOGICA

PNRR

MINISTERO DELLE IMPRESE E DEL MADE IN ITALY

BANDO CYBER 4.0 PER I PROGETTI DI INNOVAZIONE TECNOLOGICA

PNRR

1. OBIETTIVI

Supportare i **progetti di innovazione tecnologica** e selezionare **proposte progettuali** che **incrementino la maturità tecnologica**, o Technology Readiness Level (TRL), di soluzioni innovative già esistenti.

2. SOGGETTI BENEFICIARI

Il bando è aperto a grandi imprese e alle **MPMI (micro, piccole e medie imprese),** anche in forma di Raggruppamento.

3. PROGETTI AMMISSIBILI

Il Bando intende supportare la realizzazione di progetti di maturità tecnologica in ciascuna delle seguenti aree tematiche e filoni di ricerca:

- N. **4 Aree tematiche**:
  - **A)** Cybersecurity Core;
  - **B)** Space;
  - **C)** Health;
  - **D)** Automotive;
- N. **12 Filoni di ricerca**, 3 per ogni area tematica.

Si riporta a seguire il dettaglio per ciascuna area tematica:

A) Cybersecurity Core

1) **Intelligenza artificiale**. Progetto e sperimentazione di strumenti e metodi basati sull'intelligenza artificiale per lo sviluppo di servizi innovativi per la cybersecurity di imprese e pubbliche amministrazioni, con particolare focus su: cyber intelligence, disinformazione, malware detection, sicurezza e affidabilità delle tecniche di machine learning, business process mining, collezione ed analisi di big data.
2) **Blockchain.** Sperimentazione della tecnologia blockchain per lo sviluppo di applicazioni industriali distribuite sicure in scenari digitali innovativi che abilitano le interazioni tra cittadini, imprese, pubbliche amministrazioni, e PMI, con particolare focus su: prevenzioni di frodi, tutela della privacy, tokenizzazione ed economia circolare.
3) **Crittografia e applicazioni**. Progetto e sperimentazione di strumenti e metodi basati sulla crittografia per lo sviluppo di servizi innovativi per la cybersecurity di imprese e pubbliche

amministrazioni, con particolare focus su: schemi di cifratura con funzionalità avanzate, sicurezza del software, sicurezza quantistica, cyber intelligence, software testing, vulnerability detection, sicurezza delle reti 5G.

B) Space

1) **Protezione di risorse critiche**. Definizione di soluzioni integrate, sviluppo prototipale delle componenti critiche e loro dimostrazione per preservare la disponibilità e l'integrità di elementi critici degli asset spaziali applicati a diversi casi d'uso e tipologie di missioni satellitari, anche con focus su tecniche di classificazione, rilevamento delle anomalie, profilazione del comportamento, e progetto di contromisure in tempo reale.
2) **Protocolli di comunicazione satellitari sicuri**. Sviluppo e prototipazione di soluzioni crittografiche avanzate, protocolli ed algoritmi specifici per le applicazioni spaziali ed in particolare volte ad incrementare la resilienza dei sistemi di comunicazione contro eavesdropping, jamming e accesso non autorizzato, in diversi scenari applicativi, con sicurezza post-quantum ed anche sfruttando i principi della meccanica quantistica.
3) **Sfruttamento dei dati satellitari**. Definizione di soluzioni volte all'utilizzo di dati e metadati da sensori spaziali eterogenei per la protezione in tempo reale di asset critici in orbita e a terra, ad esempio infrastrutture critiche, anche attraverso tecniche di intelligenza artificiale e della tecnologia blockchain.

C) Health

1) **Protezione dei dati**. Sviluppo ed implementazione di tecnologie volte a preservare la sicurezza e la riservatezza dei dati sensibili in applicazioni di telemedicina digitale avanzate (e.g., digital twins, monitoraggio dei pazienti, etc.), anche attraverso tecniche di intelligenza artificiale e della tecnologia blockchain.
2) **Tecnologie sicure per la telemedicina**. Sperimentazione e sviluppo di piattaforme tecnologiche hw/sw sicure per l'erogazione di servizi di telemedicina avanzati, con particolare focus su: prevenzione ed il monitoraggio di epidemie (anche attraverso modelli predittivi basati su machine learning), gestione di dispositivi medicali integrati, applicativi software di apprendimento, e gestione del clinical pathway.
3) **Anticontraffazione nel settore farmaceutico**. Identificazione e sviluppo di soluzioni tecnologiche innovative per l'anticontraffazione e la sicurezza dell'accesso a sistemi e prodotti farmaceutici (dalla produzione, al trasporto, allo stoccaggio, fino alla somministrazione all'utente finale). Le soluzioni dovranno preferibilmente basarsi su piattaforme tecnologiche condivise e scalabili, ed essere compatibili con requisiti di sostenibilità energetica, economica ed ambientale.

D) Automotive

1) **Sicurezza del veicolo**. Progettazione e sviluppo di tecnologie volte a preservare la protezione dei veicoli, dei loro occupanti e del traffico circostante, incluse architetture di sicurezza, sistemi di guida autonoma, sensori, attuatori, comunicazioni di bordo, raccolta e analisi di

dati finalizzati alla identificazione di possibili minacce, anche attraverso l'utilizzo della tecnologia blockchain.

2) **Sicurezza del software e delle stazioni di ricarica**. Progettazione e sviluppo di tecnologie volte ad assicurare la sicurezza dei sistemi software installati sui veicoli e delle piattaforme di ricarica, inclusa la certificazione degli aggiornamenti software, l'accuratezza-integrità-resilienza del posizionamento dei veicoli, e la protezione delle stazioni di ricarica dagli attacchi di tipo side channel, anche attraverso l'utilizzo della tecnologia blockchain.
3) **Sicurezza della persona**. Analisi del comportamento del conducente tramite lo studio di modelli di attenzione e segnali fisiologici (Elettroencefalografia-EEG, Elettrocardiogramma-ECG, etc.), sviluppo di tecniche e algoritmi per la rivelazione di sonnolenza e affaticamento del conducente utilizzando approcci di intelligenza artificiale. Anonimizzazione dei dati relativi.

4. SPESE AMMISSIBILI

Sono ammissibili le seguenti spese:

a) costi di **personale**: ricercatori, tecnici e altro personale ausiliario, nella misura in cui vengano impiegati nel progetto;
b) costi relativi a **strumentazione e attrezzature**, relativi consumabili e costi dei materiali, nella misura e per il periodo in cui vengano utilizzati per il progetto. Sono ammissibili le spese per il leasing di strumentazione e attrezzature;
c) costi per **collaborazioni e consulenze** per ricerca, sviluppo e innovazione con soggetti pubblici e privati;
d) costi per **l'acquisto di brevetti o licenze** acquisiti a normali condizioni di mercato;
e) costi per i **servizi di consulenza** e servizi equivalenti utilizzati esclusivamente ai fini del progetto;
f) **spese generali** calcolate nella misura forfettaria del **15%** dei costi di cui al precedente punto a).

Le proposte progettuali devono prevedere attività con una durata non superiore a 12 mesi a partire dalla data ufficiale di inizio progetto, eventualmente prorogabile fino ad un massimo di 3 (tre) mesi previa richiesta motivata a Cyber 4.0.

5. ENTITÀ DELL'AGEVOLAZIONE

L'importo complessivo delle risorse stanziate per questo bando è pari a **euro 2.500.000** così suddivisi per area tematica:

A) Cybersecurity Core: euro 1.000.000,00
B) Space: euro 500.000,00
C) Health: euro 500.000,00
D) Automotive: euro 500.000,00

L'agevolazione è concessa nella forma di **contributo a fondo perduto**, fino ad una quota massima erogabile di euro 400.000,00 per i progetti rientranti nell'area tematica Cybersecurity Core (A) e non superiore ad euro 300.000,00 per i progetti rientranti nelle altre aree tematiche elencate.

ATTIVITA'	% MAX DI INTENSITÀ DI AIUTO SUL TOTALE DEI COSTI AMMISSIBILI		
	MICRO E PICCOLE IMPRESE	MEDIE IMPRESE	GRENDI IMPRESE
RICERCA INDUSTRIALE (RI)	70% Art. 25 GBER	60% Art. 25 GBER	50% Art. 25 GBER
SVILUPPO SPERIMETALE (SS)	45% Art. 25 GBER	35% Art. 25 GBER	25% Art. 25 GBER

6. PRESENTAZIONE DELLE DOMANDE

La domanda di partecipazione dei progetti deve essere inviata entro e non oltre le ore **14.00** del **30 maggio 2024**.

La procedura di selezione delle domande e **valutazione dei progetti** sarà di tipo **valutativo a graduatoria.** Sono elementi di premialità la partecipazione al progetto di Piccole-Medie Imprese e il coinvolgimento nel progetto di **almeno un Ente di Ricerca in qualità di fornitore.**

pertec

PERTEC SRL

Sede legale e operativa: Viale Virgilio, n. 58/i – 41123 Modena (MO) –
Tel. 059-460732 – email: marketing@pertec.it - www.pertec.it