# Bando Cyber 4.0

*Bandi per progetti di ricerca e innovazione per supportare il potenziale innovativo delle PMI in ambito cyber e nelle sue declinazioni tematiche: e-health, automotive e spazio.*

Cyber 4.0, uno degli 8 centri di competenza ad alta specializzazione riconosciuti e finanziati dal Ministero delle Imprese e del Made in Italy, è un partenariato pubblico-privato, con capofila l'università La Sapienza di Roma, che include più di 40 soci provenienti dal mondo dell'Università e della ricerca, da istituzioni pubbliche, dal mondo privato – grandi aziende e pmi specializzate, associazioni e fondazioni.

Il presente Bando, finanziato con risorse PNRR pari a 2,6 milioni di euro, intende supportare la realizzazione di progetti nelle seguenti 4 aree tematiche e filoni di ricerca: Cybersecurity Core; Space; Health; Automotive, da parte di imprese di ogni dimensione.

N. 12 Filoni di ricerca (n. 3 per ogni 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 traì 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.

**Finanza agevolata ed innovazione**
*Francesco Angeletti*
Tel. 071 29048218

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, risultando quindi a basso impatto per un'adozione massiva da parte sia di operatori pubblici che privati.

**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-integritàresilienza 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, Elettrocardiogrammaecg, etc.), sviluppo di tecniche e algoritmi per la rivelazione di sonnolenza e affaticamento del conducente utilizzando approcci di intelligenza artificiale. Anonimizzazione dei dati relativi.

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

Tutti i progetti dovranno utilizzare una o più tecnologie sulle quali Cyber 4.0 abitualmente opera e/o competenze del Centro di Competenza, includendo Cyber 4.0 come fornitore di servizi e per un importo pari almeno al 20% dei costi totali di progetto.

La domanda di presentazione dei progetti deve essere inviata all'indirizzo cyber4.0@pec.it entro e non oltre le ore 14.00 del 30/09/2023, data di scadenza del bando.

Per maggiori informazioni:

https://www.cyber40.it/bandi/bando-1-2023/