Pianificazione urbana resiliente e sicura e nuovi strumenti per le entità territoriali dell'UE

Resilient and secure urban planning and new tools for EU territorial entities

TOPIC ID:
HORIZON-CL3-2024-INFRA-01-02

Ente finanziatore:
Commissione europea
Programma quadro Horizon Europe (HORIZON)

Obiettivi ed impatto attesi:
I risultati dei progetti dovrebbero contribuire a tutti i seguenti risultati:
- Valutazione della resilienza di un ambiente urbano e periurbano, identificazione dei punti deboli e raccomandazioni per la modifica dei processi organizzativi;
- Creazione di nuovi strumenti e aggiornamenti efficienti in termini di costi per la sicurezza delle infrastrutture urbane, con la possibilità di mettere in comune e condividere sistemi di sicurezza complessi, tenendo conto dei bilanci limitati delle autorità locali;
- Miglioramento dell'efficienza delle forze di sicurezza e dei servizi di emergenza (polizia, vigili del fuoco, paramedici...) a beneficio dei cittadini e dei residenti europei;
- Promozione delle migliori pratiche, creazione di uno strumento/soluzione di supporto decisionale sovrano dell'UE e diffusione di strumenti e capacità efficaci tra gli enti dei diversi territori dell'UE, nonostante le loro dimensioni e la loro ubicazione.

Ambito di applicazione:
I territori europei si stanno trasformando in sistemi più connessi e complessi di servizi e infrastrutture diversi, potenziati dalle tecnologie e dalla crescente digitalizzazione. Questo cambiamento nelle aree urbane europee comporta nuove opportunità ma anche nuove minacce per le autorità e per il loro rapporto con i cittadini e i residenti. È quindi fondamentale per la resilienza delle nostre aree urbane e per il benessere dei cittadini che questi servizi siano affidabili e sicuri.
Le infrastrutture classiche su larga scala hanno una lunga tradizione di implementazione dei principi di Safety-by-design e Security-by-design nella pianificazione dei loro asset. Tuttavia, poiché sempre più infrastrutture a livello locale diventano vulnerabili, la ricerca sulla sicurezza può sostenere la loro protezione con nuovi approcci di "Security-by-design".[1]. Alla luce dei bilanci limitati di molte amministrazioni locali, si potrebbero esplorare migliori conoscenze e processi innovativi di sicurezza per le infrastrutture urbane esistenti, dotate di tecnologie di connettività avanzate e sistemi cooperativi.
I territori dell'UE, nonostante le loro dimensioni e la loro ubicazione, soffrono della mancanza di strumenti dedicati, sovrani e affidabili, per migliorare il coordinamento dei primi soccorritori locali e la copertura della sicurezza, come la preparazione del personale operativo, gli interventi sul campo e gli strumenti di previsione. Anche se esistono già alcuni strumenti complessi, è chiaro che non esistono soluzioni generiche, economiche e facili da usare per le autorità locali. Pertanto, è necessario creare nuovi strumenti che siano progettati in modo semplice e che vengano utilizzati in modo efficace.
Strumenti di pianificazione urbana resilienti e sicuri per lo sviluppo di approcci olistici che mettano in rete

i diversi livelli organizzativi, i livelli di sensori e comunicazione e le sale dati sono molto pertinenti. Questi strumenti dovrebbero valutare la resilienza dei territori urbani e periurbani, identificare i punti deboli e raccomandare modifiche ai processi organizzativi, ai sensori e alle infrastrutture di comunicazione. Gli spazi abitativi sicuri urbani e rurali, le soluzioni tecniche, i livelli organizzativi e le sale dati devono essere più strettamente collegati. È evidente la necessità di sviluppare strumenti per le strategie di recupero e di previsione proattiva per gli ambienti urbani e periurbani. Gli strumenti tattici dovrebbero includere la modellazione dei centri urbani e delle aree rurali, gli strumenti di previsione, una migliore consapevolezza della situazione globale e la pianificazione quotidiana e la gestione delle crisi (ad esempio, simulazione, formazione).
Le proposte devono includere un elevato livello di fiducia nella gestione e nella condivisione dei dati, fornire soluzioni ai problemi di cybersecurity e tenere conto di nuovi tipi di minacce. Le soluzioni proposte devono suggerire architetture condivise fidate, raccolta di dati fidata, calcolo sicuro sui dati e sui processi di gestione, capacità di modellazione, hypervisor che supporti la consapevolezza situazionale globale con API aperte e fidate, motori di elaborazione dei dati fidati e, ad esempio, strumenti di intelligenza artificiale. Se gli strumenti includono l'elaborazione di dati personali, si dovrebbe considerare di includere una valutazione del rischio o dell'impatto sulla privacy degli individui e della società.
La sperimentazione e/o il pilotaggio degli strumenti e delle soluzioni sviluppate in un contesto reale e la partecipazione di una o più autorità locali rilevanti rappresentano un vantaggio; in ogni caso, le azioni devono prevedere come facilitare l'adozione, la replica nei diversi contesti e l'up-scaling delle capacità - cioè soluzioni, strumenti, processi e altro - che saranno sviluppate dal progetto.
Questo tema richiede il contributo efficace delle discipline SSH e il coinvolgimento di esperti SSH, delle istituzioni e l'inclusione di competenze SSH rilevanti, al fine di produrre effetti significativi e significativi che rafforzino l'impatto sociale delle relative attività di innovazione.
Condizioni specifiche dell'argomento:
Si prevede che le attività raggiungano il TRL 6-8 entro la fine del progetto - si veda l'Allegato generale B.

Criteri di eleggibilità:
Qualsiasi soggetto giuridico, indipendentemente dal suo luogo di stabilimento, compresi i soggetti giuridici di Paesi terzi non associati o di organizzazioni internazionali (comprese le organizzazioni internazionali di ricerca europee) è ammesso a partecipare (indipendentemente dal fatto che sia ammissibile o meno al finanziamento), a condizione che siano state soddisfatte le condizioni stabilite dal regolamento Horizon Europe e qualsiasi altra condizione stabilita nel tema specifico del bando. Per "soggetto giuridico" si intende qualsiasi persona fisica o giuridica costituita e riconosciuta come tale ai sensi del diritto nazionale, del diritto dell'UE o del diritto internazionale, dotata di personalità giuridica e che può, agendo in nome proprio, esercitare diritti ed essere soggetta a obblighi, oppure un soggetto privo di personalità giuridica. I beneficiari e gli enti affiliati devono registrarsi nel Registro dei Partecipanti prima di presentare la domanda, per ottenere un codice di identificazione dei partecipanti (PIC) ed essere convalidati dal Servizio Centrale di Convalida prima di firmare la convenzione di sovvenzione. Per la convalida, durante la fase di preparazione della sovvenzione, verrà chiesto loro di caricare i documenti necessari che dimostrino il loro status giuridico e la loro origine. Un PIC convalidato non è un prerequisito per presentare una domanda.
Questo tema richiede il coinvolgimento attivo, in qualità di beneficiari, di almeno 2 autorità governative

locali o regionali di 2 diversi Stati membri dell'UE o Paesi associati. Per questi partecipanti, i richiedenti devono compilare la tabella "Informazioni sugli operatori della sicurezza" nel modulo di domanda con tutte le informazioni richieste, seguendo il modello fornito nello strumento informatico di presentazione. Se i progetti utilizzano dati e servizi di osservazione della terra, posizionamento, navigazione e/o tempistica correlati basati su satelliti, i beneficiari devono utilizzare Copernicus e/o Galileo/EGNOS (possono essere utilizzati anche altri dati e servizi).

Contributo finanziario:
Contributo UE previsto per progetto La Commissione stima che un contributo UE di circa 6,00 milioni di euro consentirebbe di affrontare adeguatamente questi risultati.
Tuttavia, ciò non preclude la presentazione e la selezione di una proposta che richieda importi diversi.
Budget indicativo Il budget indicativo totale per il tema è di 6,00 milioni di euro.
Tipo di azione Azioni di innovazione

Scadenza:
20 novembre 2024 17:00:00 ora di Bruxelles

Ulteriori informazioni:
wp-6-civil-security-for-society_horizon-2023-2024_en.pdf (europa.eu)