Implementazione della rete di centri di coordinamento nazionale con gli Stati membri

Deploying the Network of National Coordination Centres with Member States

TOPIC ID: DIGITAL-ECCC-2022-CYBER-03-NAT-COORDINATION
Ente finanziatore: Commissione europea, Digital Europe Programme (DIGITAL)

Obiettivi ed impatto attesi: Con la creazione del Centro di competenza europeo per l'industria, la tecnologia e la ricerca in materia di cibersicurezza (Regolamento (UE) 2021/887), i Centri nazionali di coordinamento - che lavorano insieme attraverso una rete - contribuiranno a raggiungere gli obiettivi di questo regolamento e a promuovere la Comunità di competenza in materia di cibersicurezza in ogni Stato membro, contribuendo ad acquisire le capacità necessarie.
I Centri nazionali di coordinamento (NCC) sosterranno lo sviluppo di capacità in materia di cibersicurezza a livello nazionale e, se del caso, regionale e locale.
Essi mirano a promuovere la cooperazione transfrontaliera e a preparare azioni congiunte come definito nel regolamento del Centro di competenza industriale, tecnologico e di ricerca e della rete europea in materia di cibersicurezza.

Il Centro di coordinamento nazionale deve svolgere i seguenti compiti:
- fungere da punti di contatto a livello nazionale per la Comunità di competenza per la cibersicurezza al fine di sostenere il Centro europeo di competenza industriale, tecnologica e di ricerca in materia di cibersicurezza nel raggiungimento dei suoi obiettivi e missioni, in particolare nel coordinamento della Comunità di competenza per la cibersicurezza attraverso il coordinamento dei suoi membri nazionali

- fornire competenze e contribuire attivamente ai compiti strategici del Centro europeo di competenza industriale, tecnologica e di ricerca sulla cibersicurezza, tenendo conto delle sfide nazionali e regionali rilevanti per la cibersicurezza in diversi settori;

- promuovere, incoraggiare e facilitare la partecipazione della società civile, dell'industria, in particolare delle start-up e delle PMI, delle comunità accademiche e di ricerca e di altri attori a livello di Stati membri a progetti transfrontalieri e ad azioni di cibersicurezza finanziate attraverso tutti i programmi pertinenti dell'Unione;

- fornire assistenza tecnica alle parti interessate sostenendole nella fase di presentazione delle domande per i progetti gestiti dal Centro europeo di competenza industriale, tecnologica e di ricerca sulla cibersicurezza, nel pieno rispetto delle norme di sana gestione finanziaria, in particolare in materia di conflitto di interessi. Ciò dovrebbe avvenire in stretto coordinamento con i pertinenti PCN istituiti dagli Stati membri, come quelli finanziati nell'ambito del tema Horizon Europe: "HORIZON-CL3-2021-SSRI-01-03: National Contact Points (NCPs) in the field of security and cybersecurity";

- cercare di stabilire sinergie con le attività pertinenti a livello nazionale, regionale e locale, ad esempio affrontando il tema della cybersecurity nelle politiche nazionali in materia di ricerca, sviluppo e innovazione nel settore, e in particolare nelle politiche indicate nelle strategie nazionali di cybersecurity;

- se del caso, attuare azioni specifiche per le quali sono state concesse sovvenzioni dal Centro europeo di competenza industriale, tecnologica e di ricerca sulla cibersicurezza, anche attraverso la fornitura di sostegno finanziario a terzi in linea con l'articolo 204 del regolamento (UE, Euratom) 2018/1046 alle condizioni specificate nelle convenzioni di sovvenzione in questione; tale sostegno dovrebbe in particolare mirare a rafforzare l'adozione e la diffusione di soluzioni di cibersicurezza all'avanguardia (in particolare da parte delle PMI);

- promuovere e diffondere i risultati pertinenti del lavoro della rete, della comunità di competenza in materia di cibersicurezza e del centro di competenza a livello nazionale, regionale o locale;

- valutare le richieste di entrare a far parte della comunità di competenza in materia di cibersicurezza da parte di entità stabilite nello stesso Stato membro del centro nazionale di coordinamento;

- sostenere e promuovere il coinvolgimento dei soggetti interessati nelle attività del Centro europeo di competenza industriale, tecnologica e di ricerca in materia di cibersicurezza, della rete dei Centri nazionali di coordinamento e della Comunità di competenza in materia di cibersicurezza e monitorare, se del caso, il livello di impegno nelle azioni assegnate per la ricerca, gli sviluppi e le applicazioni in materia di cibersicurezza.

Le proposte dovranno specificare ulteriormente le attività sopra elencate ed eventualmente altre attività pertinenti. Il finanziamento può coprire il rafforzamento delle capacità e il funzionamento dei Centri nazionali di coordinamento per un massimo di 2 anni. Le proposte devono dimostrare di essere in grado di coordinare le rispettive attività con i pertinenti Digital Innovation Hub europei creati ai sensi dell'articolo 16 del regolamento che istituisce il programma Europa digitale.

Criteri di eleggibilità: Per essere ammissibili, i richiedenti (beneficiari ed enti affiliati) devono:
- essere persone giuridiche (enti pubblici o privati) - essere stabiliti in uno dei Paesi ammissibili, ossia:
- Stati membri dell'UE (compresi i Paesi e territori d'oltremare (PTOM)) per tutti i temi
- Paesi SEE (Norvegia, Islanda, Liechtenstein) per tutti i temi.
I beneficiari e gli enti affiliati devono registrarsi nel Registro dei partecipanti - prima di presentare la proposta - e dovranno essere convalidati dal Servizio centrale di convalida (REA Validation).
Per la convalida, sarà richiesto loro di caricare documenti che dimostrino lo status giuridico e l'origine.
Si ricorda che tutti i temi di questo bando sono soggetti a restrizioni per motivi di sicurezza,

pertanto i soggetti non devono essere controllati direttamente o indirettamente da un Paese che non sia un Paese ammissibile. Tutti i soggetti dovranno compilare e presentare una dichiarazione sulla proprietà e sul controllo.

Contributo finanziario: La Commissione ritiene che un contributo dell'UE fino a circa 1 milione di euro sia appropriato per lo sviluppo delle capacità e il funzionamento dei Centri nazionali di coordinamento per un periodo di 2 anni. La Commissione ritiene inoltre che, nell'ambito della stessa proposta, i candidati possano richiedere un altro milione di euro da fornire sotto forma di sostegno finanziario a terzi, con l'obiettivo di sostenere l'adozione e la diffusione di soluzioni all'avanguardia in materia di sicurezza informatica (in particolare da parte delle PMI).

Tipo di azione e tasso di finanziamento Simple Grants — 50% funding rate.
Importo totale della call DIGITAL-ECCC-2022- CYBER-03-NATCOORDINATION EUR 22 milioni di euro.
I parametri della sovvenzione (importo massimo della sovvenzione, tasso di finanziamento, costi totali ammissibili, ecc.) saranno stabiliti nella Convenzione di sovvenzione

La sovvenzione assegnata potrebbe essere inferiore all'importo richiesto. Si raccomanda vivamente di rispettare il budget minimo per ogni argomento sopra elencato

Scadenza: 24 gennaio 2023 17:00:00 ora di Bruxelles

Ulteriori informazioni:
call-fiche_digital-eccc-2022-cyber-03_en.pdf (europa.eu)