



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-2022-CYBER-02-NAT-COORDINATION

Ente finanziatore: Commissione europea, Programma Digital Europe

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

Il Centro di coordinamento nazionale dovrebbe realizzare i seguenti interventi :

- agire come punti di contatto a livello nazionale per la Cybersecurity Competence Community per supportare il Centro Europeo di Competenza per la Cybersecurity Industriale, Tecnologica e di Ricerca nel raggiungimento dei suoi obiettivi e missioni, in particolare nel coordinare la Cybersecurity Competence Community attraverso il coordinamento dei suoi membri nazionali;
- fornire competenze e contribuire attivamente ai compiti strategici del Centro Europeo di Competenza Industriale, Tecnologico e di Ricerca sulla Cybersecurity, tenendo conto delle sfide nazionali e regionali rilevanti per la cybersecurity in diversi settori;
- promuovendo, incoraggiando e facilitando 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 degli Stati membri ai progetti transfrontalieri e alle azioni di cybersecurity finanziate attraverso tutti i programmi pertinenti dell'Unione;
- fornire assistenza tecnica alle parti interessate, sostenendo le parti interessate nella loro fase di candidatura per i progetti gestiti dal Centro europeo di competenza per l'industria, la tecnologia e la ricerca sulla cibersecurity, e nel pieno rispetto delle regole di sana gestione finanziaria, in particolare sul conflitto di interessi. Questo dovrebbe essere fatto 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: Punti di contatto nazionali (PCN) nel campo della sicurezza e della cibersecurity"; cercando di stabilire sinergie con attività pertinenti a livello nazionale, regionale e locale, come affrontare la sicurezza informatica nelle politiche nazionali di ricerca, sviluppo e innovazione nel settore, e in particolare in quelle politiche dichiarate

nelle strategie nazionali di sicurezza informatica;

- se del caso, attuare azioni specifiche per le quali sono state concesse sovvenzioni dal Centro europeo di competenza per l'industria, la tecnologia e la 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 interessate; tale sostegno dovrebbe in particolare mirare a rafforzare l'adozione e la diffusione di soluzioni all'avanguardia in materia di cibersicurezza (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 sulla Cybersecurity da parte di entità stabilite nello stesso Stato membro del Centro di Coordinamento Nazionale
 - sostenendo e promuovendo il coinvolgimento di entità rilevanti nelle attività derivanti dal Centro di Competenza Europeo per l'Industria, la Tecnologia e la Ricerca sulla Cybersecurity, dalla Rete dei Centri di Coordinamento Nazionale e dalla Comunità di Competenza sulla Cybersecurity, e monitorando, come appropriato, il livello di impegno nelle azioni assegnate per la ricerca, gli sviluppi e le implementazioni sulla cybersecurity.
- E' atteso che le proposte specifichino ulteriormente le attività sopra elencate ed eventualmente altre attività pertinenti. Il finanziamento può coprire lo sviluppo delle capacità e il funzionamento dei centri di coordinamento nazionali per un massimo di 2 anni.

Le proposte dovranno inoltre 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 Digital Europe.

Criteri di eleggibilità: Il presente invito si rivolge esclusivamente ai centri di coordinamento nazionali che sono stati riconosciuti dalla Commissione come aventi la capacità di gestire fondi per realizzare la missione e gli obiettivi stabiliti nel regolamento che istituisce il centro di competenza industriale, tecnologico e di ricerca europeo sulla cybersecurity e la rete dei centri di coordinamento nazionali.

Tale centro di coordinamento nazionale deve agire come coordinatore, ma altri beneficiari possono unirsi per formare un consorzio.

I beneficiari e gli enti affiliati devono registrarsi nel Registro dei Partecipanti prima di presentare la loro domanda, al fine di ottenere un codice di identificazione del partecipante (PIC) ed essere convalidati dal Servizio Centrale di Convalida (REA Validation) prima di firmare la convenzione di sovvenzione. Per la convalida, sarà chiesto loro di caricare i documenti necessari che dimostrano il loro status giuridico e la loro origine durante la fase di preparazione della sovvenzione.

Schema di finanziamento: La Commissione ritiene appropriato un contributo dell'UE fino a circa 1 milione di euro per lo sviluppo delle capacità e il funzionamento dei centri nazionali di

coordinamento per 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, allo scopo di sostenere l'adozione e la diffusione di soluzioni all'avanguardia in materia di sicurezza informatica (in particolare da parte delle PMI).

Budget totale per il bando 33 milioni di euro

Scadenza: 17 May 2022

Ulteriori informazioni:

[digital2022cyber02cybersecurityandtrustpdf1644503104-en.pdf \(europa.eu\)](#)