

Standardizzazione nel settore della sicurezza informatica

Standardisation in the area of Cybersecurity

TOPIC ID: DIGITAL-ECCC-2023-DEPLOY-CYBER-04-STANDARDISATION

Ente finanziatore: Commissione europea, Programma Digital Europe

Obiettivi ed impatto attesi:

Risultati attesi:

Organizzazione di eventi, workshop, consultazioni con le parti interessate e produzione di libri bianchi, tutti volti a promuovere lo sviluppo di standard armonizzati e la conformità ai requisiti derivanti dal quadro legislativo sopra menzionato.

Sostegno alla partecipazione di esperti europei di rilievo ai forum europei e internazionali per la standardizzazione della cybersecurity.

Obiettivo:

L'obiettivo di questo tema è sostenere l'ulteriore standardizzazione nel settore della cybersecurity, in particolare in vista dell'attuazione della proposta di regolamento sulla Cyber Resilience Act (CRA), in particolare al fine di migliorare la consapevolezza e coinvolgere le parti interessate in tale lavoro di standardizzazione.

Ambito di applicazione:

L'obiettivo è garantire un'ampia partecipazione delle parti interessate alle attività di standardizzazione nel settore della sicurezza informatica, in particolare in relazione allo sviluppo di standard armonizzati che facilitino l'attuazione della legge sulla resilienza informatica. Ciò può avvenire sotto forma di incontri, workshop e attività di collaborazione, coinvolgendo sia il settore privato che quello pubblico.

La proposta di legge sulla resilienza informatica (Cyber Resilience Act, CRA) mira a migliorare il funzionamento del mercato interno imponendo che tutti i prodotti con elementi digitali (hardware e software) siano resi disponibili sul mercato solo se soddisfano specifici requisiti essenziali di sicurezza informatica. Per facilitare l'attuazione del CRA, saranno sviluppate norme armonizzate che, se rispettate, faranno scattare la presunzione di conformità ai requisiti essenziali di cibersicurezza del CRA a cui corrispondono. Ciò sarà complementare alle azioni dei Centri nazionali di coordinamento, che svolgeranno un ruolo fondamentale nel ridurre le ricadute negative transfrontaliere e i conseguenti costi per la società per mitigare i rischi associati ai prodotti non sicuri.

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))
- Paesi non appartenenti all'UE (ad eccezione dei temi con restrizioni; vedi sotto):
- Paesi SEE elencati e Paesi associati al Programma Europa Digitale o Paesi che sono in trattative in corso per un accordo di associazione e in cui l'accordo entra in vigore prima della firma della sovvenzione

(insieme “Paesi associati al DEP”, vedi elenco dei Paesi partecipanti)

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. Altre entità possono partecipare in altri ruoli del consorzio, come partner associati, subappaltatori, terze parti che forniscono contributi in natura, ecc.

I candidati devono possedere il know-how, le qualifiche e le risorse necessarie per attuare con successo i progetti e contribuire con la loro quota (compresa una sufficiente esperienza in progetti di dimensioni e natura comparabili). Questa capacità sarà valutata insieme al criterio di aggiudicazione “Attuazione”, sulla base della competenza e dell'esperienza dei richiedenti e dei loro team di progetto, comprese le risorse operative (umane, tecniche e di altro tipo) o, eccezionalmente, le misure proposte per ottenerle entro l'inizio dell'attuazione del progetto.

Soggetti interessati Questo tema si rivolge ai soggetti interessati alla standardizzazione della cybersecurity (in particolare agli organismi di standardizzazione europei e agli organismi di valutazione della conformità), agli operatori industriali, comprese le PMI e le start-up, e agli attori rilevanti che svolgono un ruolo nel processo di standardizzazione europeo e nell'attuazione del Cyber Resilience Act e del Cybersecurity Act. La composizione di consorzi multipaese non è obbligatoria per questo tema, ma contribuirà positivamente all'impatto dell'azione.

Contributo finanziario: Tipo di azione e tasso di finanziamento Azioni di coordinamento e supporto - tasso di finanziamento del 100%. Budget massimo per progetto :per l'argomento DIGITAL-ECCC-2023-DEPLOY-CYBER-04-STANDARDISATION: fino a 3 milioni di EUR per progetto.

Scadenza: 26 Settembre 2023 17:00:00 Brussels time

Ulteriori informazioni: [call-fiche_digital-eccc-2023-deploy-cyber-04_en.pdf \(europa.eu\)](#)