

Rafforzamento delle capacità e delle competenze dell'UE in materia di cibersicurezza, in linea con i requisiti normativi

Strengthening EU cybersecurity capacities & capabilities in line with legislative requirements

TOPIC ID:

DIGITAL-ECCC-2027-DEPLOY-CYBER-11-EULEG

Ente finanziatore:

Commissione europea
Programma Europa Digitale

Obiettivi ed impatto attesi:

Obiettivi

L'obiettivo del topic è sostenere l'ecosistema europeo nel rafforzamento delle capacità di cibersicurezza e nell'attuazione, secondo un approccio omogeneo, del quadro normativo europeo, con particolare riferimento a CRA, NIS 2 Directive, GDPR, DORA, Cybersecurity Act e agli specifici requisiti dell'AI Act. In coerenza con il Digital Education Action Plan e a sostegno di iniziative quali la Cybersecurity Skills Academy, saranno promosse attività volte ad affrontare le sfide della cibersicurezza e la carenza di competenze specialistiche. Formazione pratica, coinvolgimento di giovani professionisti e promozione della diversità contribuiranno a sviluppare una forza lavoro in grado di rispondere alle esigenze normative e operative e all'evoluzione delle minacce informatiche.

L'attuazione della legislazione UE in materia di cibersicurezza richiede un rafforzamento continuo del livello di sicurezza nei settori pubblico e privato, tenendo conto dei differenti livelli di maturità dei singoli settori. A tal fine, risultano particolarmente rilevanti strumenti di empowerment e autovalutazione, accompagnati da investimenti e iniziative comuni a livello europeo.

La sicurezza e la protezione dei dati devono essere integrate nella progettazione e nello sviluppo dei prodotti e dei servizi ICT.

Ambito di applicazione

La normativa europea in materia di cibersicurezza introduce nuove responsabilità e obblighi per gli stakeholder interessati, i sistemi ICT, le Operational Technology e i produttori IoT. L'azione intende sostenere concretamente l'attuazione di tali obblighi, anche attraverso forme di supporto finanziario e organizzativo.

Le proposte devono riguardare almeno uno degli atti normativi ammissibili in materia di cibersicurezza, potendo interessarne anche più di uno.

Particolare attenzione sarà dedicata alla cooperazione transfrontaliera, alla diversità della forza lavoro e alla partecipazione delle donne e degli altri gruppi sottorappresentati nel settore della cibersicurezza. Le attività dovranno contribuire allo sviluppo delle capacità, alla sensibilizzazione e all'adozione del quadro normativo europeo.

In linea con il Digital Education Action Plan, le attività dovranno inoltre contribuire alla formazione della nuova generazione di professionisti della cibersicurezza, offrendo a giovani professionisti e studenti esperienze pratiche utili a ridurre il divario di competenze e a prepararli all'applicazione dei nuovi requisiti normativi.

Certificazione e valutazione della cibersicurezza

La valutazione di prodotti e servizi costituisce una fase essenziale del processo europeo di certificazione della cibersicurezza. L'evoluzione delle minacce, la crescente sofisticazione degli attacchi e l'aumento delle dimensioni e della complessità dei sistemi informativi richiedono procedure di valutazione rapide, sicure, replicabili e interoperabili.

L'azione prevede il rafforzamento delle capacità delle autorità nazionali di certificazione della cibersicurezza per lo svolgimento della sorveglianza del mercato e la supervisione degli organismi e delle procedure di valutazione della conformità, assicurando il riconoscimento reciproco tra gli Stati membri. È inoltre previsto il rafforzamento delle capacità dei CABs e dei laboratori di certificazione, affinché possano soddisfare i requisiti del Cybersecurity Act e del CRA, anche per quanto riguarda la verifica delle dichiarazioni di conformità dei fornitori.

L'azione comprende lo sviluppo di strumenti a supporto dei processi di certificazione e valutazione, inclusa una piattaforma software di "Certification and Evaluation as a Service", nonché il sostegno alla creazione di hub nazionali o interregionali di esperti. Lo sviluppo dovrebbe coinvolgere gli stakeholder pertinenti, inclusi CBs, CABs e rappresentanti dei clienti.

La piattaforma potrà facilitare la gestione della documentazione relativa ai processi di certificazione, accelerare lo scambio di informazioni tra gli organismi coinvolti e contribuire all'armonizzazione e standardizzazione della documentazione e degli strumenti utilizzati a livello europeo.

Principali attività

L'azione può comprendere:

- sostegno all'attuazione della legislazione UE in materia di cibersicurezza, al fine di aumentare il livello di sicurezza informatica in Europa;
- sostegno alle PMI per rafforzarne la resilienza informatica, con particolare attenzione agli obblighi derivanti da NIS 2, CRA e Cybersecurity Act, anche mediante linee guida operative e strumenti di facile utilizzo per verificare la conformità delle soluzioni ai nuovi requisiti normativi, tenendo conto degli standard aperti;
- sviluppo di piattaforme di reporting per NIS 2, ad esempio per la segnalazione degli incidenti, e per il CRA, comprese piattaforme uniche per la segnalazione delle vulnerabilità;
- azioni di breve e lungo periodo finalizzate a preparare i professionisti alla corretta attuazione dei requisiti introdotti dalla nuova normativa UE;

- programmi per promuovere diversità e pari opportunità, con percorsi specifici rivolti ai giovani europei, accesso a contenuti formativi e opportunità di partecipazione a cybersecurity challenges;
- iniziative di cooperazione transfrontaliera e intersettoriale tra autorità nazionali e regionali, finalizzate ad aumentare la resilienza informatica e i livelli di maturità della cibersicurezza mediante metodologie comuni;
- progettazione e valutazione di piattaforme formative e strumenti per lo scambio tra Paesi, programmi di benchmarking e assessment, materiali formativi, scambi tra pari e fellowship;
- programmi di collaborazione transfrontaliera che consentano a team paneuropei di partecipare a competizioni internazionali di cibersicurezza, con accesso a strumenti avanzati, mentoring e formazione alla leadership.

Rafforzamento delle capacità e cooperazione

Oltre al sostegno alle autorità nazionali di certificazione della cibersicurezza, ai CABs e agli organismi nazionali di accreditamento, l'azione accompagnerà la progressiva attuazione della NIS 2 Directive.

Le autorità competenti dovranno rafforzare le proprie capacità in materia di audit e compliance, al fine di verificare che le entità essenziali e importanti rispettino i propri obblighi. Dovranno inoltre essere previste attività di formazione, sensibilizzazione e costruzione della fiducia, volte a facilitare la condivisione delle informazioni e delle conoscenze.

Nel complesso, l'azione mira ad aumentare la collaborazione tra le autorità nazionali e tra queste e gli stakeholder, in particolare le PMI, sostenendo anche le strutture previste dalla NIS Directive che devono conformarsi al CRA. Ciò comprende, tra l'altro, Software Bill of Materials, contributi e prototipi aperti per la CRA Single Reporting Platform, processi CVD e automazione dei security advisory, come CSAF.

L'obiettivo finale è aumentare il livello di maturità della cibersicurezza attraverso lo sviluppo e l'attuazione di metodologie comuni, favorendo l'implementazione dei processi di cibersicurezza e l'adozione di prodotti e servizi da parte delle entità interessate.

Criteri di eleggibilità:

Ammissibilità delle candidature

Le candidature saranno considerate ammissibili solo se il loro contenuto corrisponde interamente (o almeno in parte) alla descrizione del topic per il quale sono presentate.

Partecipanti ammissibili (Paesi ammissibili)

Per essere ammissibili, i richiedenti (beneficiari ed entità affiliate) devono:

- essere entità giuridiche (organismi pubblici o privati);
- essere stabiliti in uno dei Paesi ammissibili, vale a dire:
 - Stati membri dell'UE (compresi i Paesi e territori d'oltremare – PTOM);
 - Paesi SEE (Norvegia, Islanda, Liechtenstein).

I beneficiari e le entità affiliate devono registrarsi nel Participant Register — prima della presentazione della proposta — e dovranno essere convalidati dal Central Validation Service (REA Validation). Ai fini della convalida, sarà loro richiesto di caricare documenti attestanti lo status giuridico e l'origine.

Altre entità possono partecipare ricoprendo altri ruoli all'interno del consorzio, quali partner associati, subappaltatori, terzi che forniscono contributi in natura, ecc. (cfr. sezione 13).

Si tenga presente che tutti i topic del presente invito sono soggetti a restrizioni per motivi di sicurezza;

pertanto, le entità non devono essere direttamente o indirettamente controllate da un Paese che non sia un Paese ammissibile. Tutte le entità¹⁷ dovranno compilare e presentare una dichiarazione relativa alla proprietà e al controllo.

Inoltre

- la partecipazione a qualsiasi titolo (in qualità di beneficiario, entità affiliata, partner associato, subappaltatore o destinatario di sostegno finanziario a terzi) è limitata alle entità stabilite e controllate da Paesi ammissibili;
- le attività del progetto (compresi i lavori subappaltati) devono svolgersi nei Paesi ammissibili (cfr. la sezione relativa alla localizzazione geografica di seguito e la sezione 10);
- il Grant Agreement può prevedere restrizioni in materia di diritti di proprietà intellettuale (IPR) (cfr. sezione 10).

Contributo finanziario:

Budget disponibile

Il budget disponibile stimato per la call è pari a 20.000.000 EUR

La disponibilità del budget della call dipende ancora dall'adozione definitiva della modifica del Programma di lavoro 2025-2027.

Forma della sovvenzione, tasso di finanziamento e importo massimo della sovvenzione

I parametri della sovvenzione (importo massimo della sovvenzione, tasso di finanziamento, costi ammissibili totali, ecc.) saranno stabiliti nella Convenzione di sovvenzione (Grant Agreement) (Scheda dati, punto 3 e articolo 5).

Budget del progetto (importo della sovvenzione richiesta)

Il contributo UE richiesto dovrebbe essere compreso tra 3 milioni di EUR e 5 milioni di EUR per progetto. Tuttavia, potranno essere prese in considerazione anche proposte che richiedano importi diversi, purché ciò sia debitamente giustificato.

La sovvenzione concessa potrà essere inferiore all'importo richiesto.

Forma della sovvenzione e costi ammissibili

Tipologia di azione e tasso di finanziamento

Sovvenzioni semplici (Simple Grants) — tasso di finanziamento del 50%.

La sovvenzione assumerà la forma di una sovvenzione basata sul budget a costi effettivi misti (budget-based mixed actual cost grant: costi effettivi, con elementi basati su costi unitari e tassi forfettari).

Ciò significa che saranno rimborsate ESCLUSIVAMENTE determinate tipologie di costi (costi ammissibili) e i costi effettivamente sostenuti per il progetto (NON i costi preventivati).

Per i costi unitari e i tassi forfettari, potranno essere imputati gli importi calcolati secondo le modalità indicate nella Convenzione di sovvenzione (cfr. articolo 6 e Allegati 2 e 2a).

Tasso di finanziamento

Divieto di profitto

Le sovvenzioni NON possono generare un profitto, vale a dire un'eccedenza dei ricavi + sovvenzione UE rispetto ai costi.

Le organizzazioni a scopo di lucro devono dichiarare i propri ricavi e, qualora si realizzi un profitto, questo sarà dedotto dall'importo finale della sovvenzione (cfr. articolo 22.3).

Riduzione dell'importo finale della sovvenzione

Si tenga inoltre presente che l'importo finale della sovvenzione potrà essere ridotto in caso di mancato rispetto della Convenzione di sovvenzione, ad esempio in caso di attuazione non corretta, violazione degli obblighi, ecc.

Scadenza:

14 Gennaio 2027 17:00:00 Brussels time

Ulteriori informazioni:

[8e1d6074-95ed-4b23-8bd3-2ca42b096411_en](#)