DIGITAL-ECCC-2023-DEPLOY-CYBER-04-EULEGISLATION - Sostegno all'attuazione della legislazione dell'UE in materia di sicurezza informatica e delle strategie nazionali in materia di cybersicurezza

PROGRAMMA DI FINANZIAMENTO	**DIGITAL**
TITOLO BANDO (ITA/ENG)	• DIGITAL-ECCC-2023-DEPLOY-CYBER-04- EULEGISLATION Sostegno all'attuazione della legislazione dell'UE in materia di sicurezza informatica e delle strategie nazionali in materia di cybersicurezza • DIGITAL-ECCC-2023-DEPLOY-CYBER-04- EULEGISLATION Support for implementation of EU legislation on cybersecurity and national cybersecurity strategies
DATA DI SCADENZA	**26 settembre 2023 ore 17:00**
ENTE FINANZIATORE	**Commissione Europea**
BUDGET (€)	30.000.000
CO-FINANZIAMENTO UE (€) PER OGNI PROGETTO	50%
DURATA	36 mesi
SETTORE SPECIFICO/TEMATICA/PRIORITÀ	Legislazione, sicurezza informatica

DESCRIZIONE	La presente iniziativa si focalizza sull'enfatizzare lo sviluppo delle competenze e il potenziamento della cooperazione nell'ambito della sicurezza informatica a livello tecnico, operativo e strategico, all'interno del quadro della legislazione europea vigente e delle proposte relative alla sicurezza informatica. In particolare, si presta attenzione alla direttiva NIS2 (direttiva (UE) 2022/2555), alla legge sulla cybersicurezza e alla proposta di legge sulla resilienza informatica, nonché alla direttiva sugli attacchi contro i sistemi informativi (direttiva 2013/40). Il sistema integrerà il lavoro dei Centri di Operazioni per la Sicurezza (SOC) nel contesto del rilevamento delle minacce. Questa iniziativa rappresenta una continuazione delle attività attualmente sostenute nell'ambito del precedente Programma di lavoro digitale. L'obiettivo principale è inoltre quello di potenziare la preparazione dell'industria e del mercato per adeguarsi ai requisiti di cybersecurity stabiliti nella proposta di regolamento sui requisiti di sicurezza informatica per i prodotti con componenti digitali, comunemente noto come "Cyber Resilience Act". Questa misura mira a garantire una maggiore sicurezza dei prodotti hardware e software attraverso l'implementazione di normative più stringenti.
OBIETTIVI	Le proposte dovranno perseguire almeno uno dei seguenti obiettivi: 1. Promuovere lo sviluppo della fiducia tra gli Stati membri. 2. Favorire una cooperazione operativa efficace tra le organizzazioni responsabili della sicurezza informatica dell'Unione Europea o degli Stati membri, con particolare attenzione alla cooperazione dei CSIRT o degli operatori di servizi essenziali, inclusi gli enti pubblici. 3. Potenziare i processi e i mezzi di sicurezza e notifica per gli Operatori di Servizi essenziali e per i fornitori di servizi digitali nell'Unione Europea. 4. Migliorare la segnalazione degli attacchi informatici alle autorità di polizia, in conformità con quanto previsto dalla direttiva sugli attacchi ai sistemi informativi. 5. Rafforzare la sicurezza delle reti e dei sistemi informativi nell'Unione Europea. 6. Favorire un maggiore allineamento delle implementazioni degli Stati membri con la NIS2 (Direttiva (UE) 2022/2555). 7. Sostenere l'attuazione della certificazione della sicurezza digitale, coerentemente con quanto stabilito dalla legge sulla cybersecurity.

ATTIVITÀ	Le attività pianificate saranno incentrate sui seguenti aspetti prioritari: 1. Implementazione, validazione, sperimentazione e diffusione di tecnologie, strumenti e soluzioni informatiche, nonché di processi e metodi per il monitoraggio e la gestione degli incidenti di sicurezza informatica. 2. Promozione della collaborazione, comunicazione, sensibilizzazione, scambio di conoscenze e formazione tra organizzazioni pubbliche e private che operano nell'ambito dell'attuazione della NIS2 (Direttiva (UE) 2022/2555). 3. Promozione di schemi di gemellaggio che coinvolgano organizzazioni di almeno due Stati membri diversi, al fine di agevolare la diffusione e l'adozione di tecnologie, strumenti, processi e metodi per una collaborazione transfrontaliera efficace volti a prevenire, individuare e contrastare gli incidenti di sicurezza informatica. 4. Adozione di misure di solidità e resilienza nel campo della cybersecurity, al fine di potenziare la capacità dei fornitori di lavorare sistematicamente con informazioni rilevanti per la sicurezza informatica. 5. Assicurare che i produttori migliorino la sicurezza dei prodotti con elementi digitali fin dalla fase di progettazione e sviluppo, e durante tutto il loro ciclo di vita. 6. Garantire un quadro coerente di cybersecurity per agevolare la conformità dei produttori di hardware e software. 7. Migliorare la trasparenza riguardante le proprietà di sicurezza dei prodotti con elementi digitali. 8. Consentire alle aziende di tutti i settori e ai consumatori di utilizzare prodotti con elementi digitali in modo sicuro.
CHI PUÒ PRESENTARE IL PROGETTO	Tutte le entità interessate
MODALITÀ DI PARTECIPAZIONE	Funding and tenders portal
LINK A DOCUMENTAZIONE	**https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/digital/wp-call/2023/call-fiche_digital-eccc-2023-deploy-cyber-04_en.pdf**
LINK AD EVENTUALI	**https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-**

APPROFONDIMENTI	**2027/common/guidance/om_en.pdf**