Finanziato dall'Unione europea NextGenerationEU

MUR

Italiadomani
PIANO NAZIONALE DI RIPRESA E RESILIENZA

SERICS
SECURITY AND RIGHTS IN THE CYBERSPACE

Dibris
Dipartimento di Informatica, Bioingegneria, Robotica e Ingegneria dei Sistemi

Università di Genova

UNIVERSITÀ DEGLI STUDI GENOVA

DIBRIS – Dipartimento di Informatica Bioingegneria Robotica e Ingegneria dei Sistemi

SCHEDA PROGETTO

Responsabile del progetto e dell'esecuzione del contratto:
Prof. Alessandro Armando (Professore Ordinario – Area scientifico-disciplinare ING-INF/05)

Obiettivo del progetto:
Uno dei problemi più urgenti che le Organizzazioni devono affrontare riguarda la sfida di assolvere efficacemente ai propri doveri di sicurezza in risposta alle stringenti normative europee e italiane in materia di Cybersicurezza. Questa problematica assume particolare gravità per entità incluse nel Perimetro di Sicurezza Nazionale, esteso a seguito dell'introduzione della direttiva europea NIS 2.
La normativa in vigore, pur imponendo alle Organizzazioni obbligazioni precise e inderogabili, lascia a queste ultime il compito di identificare e gestire le misure tecniche e organizzative adeguate a mitigare il rischio cyber a cui sono soggette, considerando il proprio contesto operativo, le necessità aziendali e gli obiettivi specifici. Un'ulteriore complessità emerge dal fatto che, nonostante la legislazione europea stabilisca le basi per gli schemi di certificazione, essa non fornisce indicazioni dettagliate sull'implementazione pratica, demandando alle singole entità la responsabilità di allinearsi agli standard o alle migliori pratiche ritenuti più opportuni.
Nel contesto italiano, il Framework nazionale di Cyber Security, nato per supportare le organizzazioni e le PMI, è basato sul NIST CSF 1.1 ed è esplicitamente menzionato dalla normativa che portato all'istituzione del Perimetro Nazionale di Cybersicurezza. Tuttavia, esso fornisce supporto alle organizzazioni che intendono avviare o migliorare il proprio programma di gestione del cyber-risk e non è pensato per supportare un iter certificazione.
Queste sfide diventano ancor più pressanti per quelle Organizzazioni, come ad esempio le PMI, che non godono di adeguate competenze interne o di risorse finanziarie sufficienti per condurre un'analisi approfondita dei propri sistemi organizzativi, dei rischi legati alle minacce informatiche e per l'adozione di efficaci misure di difesa tecniche e organizzative. La mancanza di azione si traduce in un aumento del rischio, soprattutto alla luce dell'estensione del perimetro di sicurezza delineato dalla Direttiva NIS 2, entrata in vigore il 17 gennaio 2023 e che dovrà essere recepita dagli Stati Membri entro l'Ottobre 2024.
Al fine di fornire strumenti operativi coerenti con le normative vigenti si vuole promuovere lo studio e la realizzazione di una PdR adottabile in modo pragmatico anche dalle Organizzazioni più piccole meno strutturate ed in linea con i principali standard nazionali e internazionali per la sicurezza delle informazioni e delle infrastrutture critiche dal rischio cyber. L'obiettivo finale di questa azione è quello di migliorare la sicurezza di tutte le organizzazioni supportandole nel muovere i primi passi all'interno di un percorso in grado di mitigare il rischio cyber, migliorare la sicurezza all'interno della catena del valore (sia delle aziende sia della PA) rendendo al tempo stesso più sicuro e competitivo l'intero sistema paese.
Sulla base delle precedenti argomentazioni, l'attività prevede l'armonizzazione e la convergenza in una pre-norma UNI certificabile, denominata Prassi di Riferimento, dello standard ISO/IEC 27001 e del Framework NIST CSF.
L'attività sarà svolta nell'ambito di un Tavolo di Lavoro UNI al quale parteciperanno diversi Organi Istituzionali Italiani e Pubbliche Amministrazioni.

Oggetto della prestazione:
Attività di consulenza: "*Estensione ed armonizzazione, in ottica di certificabilità, dei requisiti della norma UNI EN ISO/IEC 27001 e del Framework NIST CSF*".

Descrizione dettagliata della prestazione:
Nell'ambito del contesto sopradescritto, sono richieste le attività e i risultati di seguito dettagliati:

1. analisi comparativa del Cybersecurity Framework v. 2.0 del NIST (CSF 2.0) rispetto alla versione 1.1

2. analisi comparativa della norma UNI EN ISO/IEC 27001:2022 e del CSF 2.0
3. studio di fattibilità la mappatura del NIST CSF 2 con la norma ISO/IEC 27001:2022
4. analisi e ricerca dei controlli UNI EN ISO/IEC non mappati e/o non mappabili rispetto alle funzioni Core del CSF 2.0
5. identificazione di possibili soluzioni operative atte ad armonizzare i controlli UNI EN ISO/IEC non mappati e/o non mappabili rispetto alle funzioni Core del CSF 2.0
6. redazione di un rapporto tecnico di sintesi delle attività indicate ai punti precedenti

Competenze richieste al prestatore:

- Diploma di laurea quinquennale in Fisica, Informatica, Ingegneria Informatica, Ingegneria Elettronica, Ingegneria delle Telecomunicazioni, Ingegneria Gestionale e Matematica conseguita ai sensi della normativa previgente al D.M. 3 Novembre 1999, no. 509 oppure titolo equipollente ai sensi del Decreto interministeriale del 9 luglio 2009
- Esperienza, anche in ambito accademico, in istituzioni o enti, pubblici o privati, anche a supporto di studi e ricerche nel settore di riferimento di almeno 2 anni;
- Conoscenze e competenze documentabili attraverso il curriculum ed acquisite tramite attività di ricerca o esperienze lavorative nei seguenti ambiti:
  - Cybersecurity
  - Cyber-risk management
  - Information Security

Durata della prestazione:
La prestazione dovrà essere conclusa entro 6 mesi.

Compenso:
Compenso lordo per l'intero periodo contrattuale: euro 8.000,00 (ottomila/00) + IVA (se dovuta) e comprensivi di oneri previdenziali e assistenziali a carico del prestatore, se dovuti.
Modalità di pagamento: in due rate, euro 4.000,00 (quattromila/00) + iva (se dovuta) e comprensivi di oneri previdenziali e assistenziali a carico del prestatore (se dovuti) dopo tre mesi dall'inizio del contratto - euro 4.000,00 (quattromila/00) + iva (se dovuta) e comprensivi di oneri previdenziali e assistenziali a carico del prestatore (se dovuti), a saldo, a conclusione del contratto.

Natura Fiscale della prestazione:
Prestazione unica ad esecuzione pressoché istantanea:

- lavoro autonomo – redditi diversi (art. 67, comma 1, lett. l, D.P.R. 917/86 TUIR);
- lavoro autonomo – redditi di lavoro autonomo- professionisti abituali (art. 53, comma 1, D.P.R. 917/86 TUIR).

Il Responsabile del progetto e dell'esecuzione del contratto
(prof. Alessandro Armando)

(*Documento firmato*