IRE ISTITUTO NAZIONALE TUMORI REGINA ELENA ISG ISTITUTO DERMATOLOGICO SAN GALLICANO
ISTITUTI DI RICOVERO E CURA A CARATTERE SCIENTIFICO

UOC Acquisizione Beni e Servizi

Il dirigente della UOC Acquisizione Beni e Servizi

in virtù della delega conferita con deliberazione N°232/2015

HA ASSUNTO LA PRESENTE DETERMINAZIONE

N. 760 del 18/08/2023

OGGETTO: Affidamento, ai sensi dell'art. 50, comma 1, lett. b), D. Lgs. 36/2023, previa pubblicazione manifestazione di interesse, del servizio un servizio di consulenza per attività di Vulnerability Scan di due web application (tra cui la piattaforma EDUMEET) alla Società Moveax S.r.l. Fondi Commissione Europea, Cod. IFO 22/07/R/30, responsabile Dr. Andrea Pace - CUP: H83C22000670006 - CIG: ZD23C2C20C.

Esercizi/o e conto 2023 - Conto 502020197 x € 28.914,00 Iva inclusa Centri/o di costo 3020750

- Importo presente Atto: € 28.914,00

- Importo esercizio corrente: € 28.914,00

Budget

- Assegnato: € 539287,70

- Utilizzato: € 162119,64

- Residuo: € 348254,06

Autorizzazione n°: 2023/1957

Servizio Risorse Economiche: **Giovanna Evangelista**

UOC Acquisizione Beni e Servizi Proposta n° DT-791-2023

L'estensore

Fabrizio Caputo

Il Responsabile del Procedimento

Andrea Scotti

Il Dirigente della UOC Acquisizione Beni e Servizi

Andrea Scotti

La presente determinazione si compone di n° 4 pagine e dei seguenti allegati che ne formano parte integrante e sostanziale:
n°1 RICHIESTA SERVIZIO + OFFERTA ECONOMICA

Il Dirigente della UOC Acquisizione Beni e Servizi

Visto	il Decreto Legislativo 30 dicembre 1992, n. 502 e ss.mm.ii.;
Visto	il Decreto Legislativo 16 ottobre 2003, n. 288 e ss.mm.ii.;
Vista	la Legge Regionale 23 gennaio 2006, n. 2;
Visto	il decreto legislativo 31.03.2023, n. 36 e ss.mm.ii.;
Visto	l'Atto Aziendale adottato con deliberazione IFO n.153 del 19.02.2019, ed approvato dalla Regione Lazio con DCA n. U00248 del 02.07.2019, modificato e integrato con deliberazioni n. 1254 del 02.12.2020, n. 46 del 21/01/2021 e n. 380 del 25.03.2021, approvate dalla Direzione Salute ed Integrazione Sociosanitaria della Regione Lazio, con Determinazione n. G03488 del 30.03.2021;
Premesso che	che, in esecuzione della deliberazione n. 982 del 29/12/2022, è in corso di svolgimento il progetto finanziato dall'Unione Europea dal titolo "*Joint action on strengthening ehealth including telemedicine and remote monitoring for health care systems for cancer prevention and care*"; cod. IFO 22/07/R/30, di cui è responsabile il Dr. Andrea Pace;
Considerato che	il Dr. Andrea Pace con nota di protocollo n°8021 del 15/06/2023, ha richiesto l'attivazione di un servizio di consulenza per attività di Vulnerability Scan di due web application (tra cui la piattaforma EDUMEET) e predisposizione delle linee guida di Software sicuro per il progetto europeo di Joint Action, acronimo e-CAN; al fine di individuare operatori economici interessati a presentare offerta per il predetto servizio, gli I.F.O. in data 20.06.2023 hanno indetto una manifestazione d'interesse pubblicata sul sito www.ifo.it per la durata di quindici giorni naturali e consecutivi;

alla scadenza della suddetta manifestazione, hanno mostrato interesse a partecipare le seguenti Società:

- CyberCoaching S.r.l.;
- Moveax S.r.l.;

entrambe le offerte sono state sottoposta a valutazione tecnica della Dr. Andrea Pace – responsabile UOSD Neurologia IRE, con esito positivo;

e selezionato tra quest'ultime il preventivo presentato dalla Moveax S.r.l. che è parte integrante e sostanziale del presente provvedimento, in quanto contenente l'offerta economicamente più vantaggiosa;

Preso atto del parere favorevole del Direttore Scientifico dell'Istituto Regina Elena, apposto in calce alla richiesta citata;

Accertata la disponibilità sul fondo individuato in premessa;

Esperiti i controlli sulla richiesta presentata dal responsabile del progetto;

Tenuto conto che la spesa complessiva di 28.914,00 Iva inclusa, graverà sul sul Fondo Commissione Europea, cod. IFO 22/07/R/30 responsabile Dr. Andrea Pace, che presenta la necessaria disponibilità;

Attestato che il presente provvedimento, a seguito dell'istruttoria effettuata, nella forma e nella sostanza è totalmente legittimo e utile per il servizio pubblico, ai sensi dell'art. 1 della legge 20/94 e successive modifiche, nonché alla stregua dei criteri di economicità e di efficacia di cui all'art. 1, primo comma, della legge 241/90, come modificata dalla legge 15/2005;

Determina

per i motivi di cui in narrativa che si intendono integralmente confermati di:

1) affidare, ai sensi dell'art. 50, comma 1, lett. b), D. Lgs. 36/2023, il servizio di consulenza, tramite il Mercato della Pubblica Amministratore (M.E.P.A), a seguito di invio telematico tramite NSO (Nodo Smistamento Ordini) della Regione Lazio, che forma parte integrante e sostanziale della presente determinazione, alla società:

- Moveax S.r.l. 28.914,00 Iva inclusa;

2) far gravare che la spesa complessiva di € 6.100,00 Iva inclusa, sul sul Fondo Commissione Europea, cod. IFO 22/07/R/30 responsabile Dr. Andrea Pace, che presenta la necessaria disponibilità;

Cod. IFO RC 22/07/R/30

- assegnato:	€	539.287,70
- utilizzato:	€	162.119,64
- presente atto:	€	28.914,00
- residuo:	€	348.254,06

3) attribuire il costo di produzione alla Contabilità Generale con imputazione al relativo al Centro di Costo 3020750 - Conto 502020197 x € 28.914,00 Iva inclusa.

4) stipulare il contratto, ai sensi dell'art. 18, comma 1 del D.Lgs. 36/202023.

La UOC Acquisizione Beni e Servizi curerà tutti gli adempimenti per l'esecuzione della presente determinazione.

Il Dirigente della UOC Acquisizione Beni e Servizi

Andrea Scotti

Documento firmato digitalmente ai sensi del D.Lgs 82/2005 s.m.i. e norme collegate

CIG ZD23C2C20C

ifo_058.IFO_AOO.REGISTRO UFFICIALE.0008021.15-06-2023

IRE
ISTITUTO NAZIONALE TUMORI
REGINA ELENA
ISTITUTO DI RICOVERO E CURA A CARATTERE SCIENTIFICO

Al Direttore Scientifico

OGGETTO: Richiesta acquisizione di un servizio per la fornitura di una consulenza per attività di Vulnerability Scan di due web application (tra cui la piattaforma EDUMEET) e predisposizione di linee guida di Software sicuro, per il progetto europeo di Joint Action, acronimo e-CAN.

Nell'ambito del progetto eCAN JA finanziato dalla Commissione Europea, avviato in data 15/09/2022, l'utilizzo della piattaforma software EDUMEET, resa disponibile ai vari partner esecutori, per effettuare le attività di Teleconsultation previste, nell'ambito del WP6, Task 6.1 "Data and systems security in tele-consultations and tele monitoring" e task 6.3 "Guideline and recommendations production" di cui IFO-IRE è coordinatore, è richiesta un'azione di "Vulnerability Assessment (black box)", per la sicurezza informatica delle attività previste.

Edumeet è un software sviluppato per il National Research and Education Network, già ampiamente utilizzato in diversi progetti europei e sviluppato con fondi comunitari. La piattaforma Cloud provider centralizzata che utilizzerà tale software sarà gestita dal partner Affiliato Ospedale San Raffaele di Milano.

IFO-IRE ha necessità di esternalizzare l'attività di implementare la sicurezza informatica del sistema adottato che richiede un expertise specialistico, perché l'obiettivo di tale attività consiste nella ricerca e analisi di eventuali vulnerabilità informatiche presenti nella piattaforma EDUMEET, con conseguente suggerimento dei passi di mitigazione. La ricerca di vulnerabilità deve essere svolta in modalità BLACK BOX cioè simulando l'attività di un attaccante che non può disporre del codice sorgente della piattaforma.

Con la presente pertanto, chiedo l'avvio delle procedure amministrative e l'iter idoneo, per l'assegnazione di una fornitura di servizio di cui all'oggetto, la cui spesa dovrà gravare sui fondi del progetto europeo del quale sono Responsabile, dal titolo *"e-CAN - Joint Action on strengthening ehealth including telemedicine and remote monitoring for health care systems for cancer prevention and care"*, delibera n° 982 del 29/12/2022, CUP H83C22000670006, codice IFO 22/07/R/30.

A seguire, si elencano alcuni degli elementi (non a titolo esaustivo) che dovrà prevedere il capitolato tecnico per la richiesta delle offerte:

- Svolgimento dei seguenti test:
  - *Ricerca e test di vulnerabilità nella validazione dell'input* al fine di rilevare eventuali vulnerabilità di tipo XSS (Cross-site scripting), SQL injection e command injection, utilizzando tool di scanning e/o fuzzer.
  - *Port scanning del server web con Nmap* al fine di individuare Porte/servizi critici che vengono aperti in fase di installazione del server
  - *Ricerca e test di vulnerabilità di tipo authorization* al fine di rilevare eventuali vulnerabilità di tipo directory traversal e forceful browsing utilizzando tool di fuzzing
  - *Ricerca e test di vulnerabilità nel sistema di autenticazione* attraverso la simulazione di attacchi di tipo username enumeration e brute force
  - *Ricerca e test di vulnerabilità lato client:* test su URL Redirection e Cross Origin Resource Sharing (CORS
  - *Ricerca e test di vulnerabilità nella gestione delle sessioni*: verificando la robustezza ad attacchi di tipo CSRF (Cross-site Request Forgery).

1. Al termine dell'attività di analisi le eventuali vulnerabilità individuate per ogni applicazione dovranno essere classificate assegnandogli un livello di gravità e per ogni vulnerabilità dovranno essere

moveax|

Specifica dei costi del servizio

Voce di costo	Importo
Test di vulnerability scan (Schede servizi 1-4) per App. 1	10.000€
Test di vulnerability scan (Schede servizi 1-4) per App. 2	10.000€
Report di valutazione delle vulnerabilità	0€
Supporto allo sviluppo del Piano di sicurezza	3.700€
Importo totale	**23.700**

* Tutti i prezzi sono da intendersi iva esclusa.

** La presente offerta non include costi di eventuali trasferte richieste dal cliente, tutta l'attività si svolgerà da remoto.