Via Giuseppe Grezar, 14
00142 Roma – RM
Tel. 06 98 9581
www.agenziaentrateriscossione.gov.it

Prot n. 10718730 del 27/11/2023

Progetto tecnico ai sensi art. 23 comma 15 D. Lgs. n. 50/2016

Acquisizione servizi di formazione e security awareness in adesione all'AQ Consip ID 2296 - "Servizi di sicurezza da remoto, di compliance e controllo", lotto 1

Sommario

Premessa 3
Fabbisogno 4
Quadro economico complessivo 6
Indicazioni per la stesura del DUVRI di cui al D. Lgs. n. 81/2008 7
Costo della Manodopera 7
Clausola sociale 8
Garanzie 8
Subappalto 8
Penali 8
Modalità di fatturazione 8
Modalità acquisitiva 9
Conclusioni 9

Premessa

Agenzia delle entrate-Riscossione (di seguito per brevità AdeR o Ente) è impegnata costantemente nel miglioramento del livello di sicurezza del patrimonio informativo gestito (dati e asset), per il corretto esercizio delle attività istituzionali inerenti la riscossione e l'amministrazione dei processi corporate, in conformità alle prescrizioni di legge ed alle linee guida di vigenti.

La rilevante crescita degli attacchi di tipo cyber e il peggioramento degli scenari internazionali hanno reso centrale il concetto della cyber security per preservare la continuità del business aziendale, attraverso processi di prevenzione e di protezione.

L'adozione di sistemi e misure di protezione (antivirus/antimalware, intrusion prevention/detection, firewall, proxy, etc.) non è di per sé sufficiente a prevenire e a mettere al sicuro l'Ente dagli attacchi informatici; il fattore umano rappresenta un rischio elevato, legato alle "vulnerabilità" del comportamento delle persone, sfruttate dai criminali mediante tecniche di social engineering, sempre più sofisticate.

La consapevolezza dei comportamenti da tenere e la formazione in ambito cyber security, sono elementi essenziali per la tutela del patrimonio informativo dell'Ente.

Per indirizzare correttamente il comportamento dei dipendenti-utenti, occorre impostare un adeguato percorso di training e awareness.

Il progetto formativo rappresentato nel presente documento si configura come un'iniziativa finalizzata a rafforzare la consapevolezza dei dipendenti-utenti di AdeR, in merito ai rischi e alle vulnerabilità nell'ambito della sicurezza ICT.

Trattandosi di iniziativa attinente anche al tema della formazione, è stata rappresentata l'esigenza al Responsabile della Struttura "Gestione Risorse Umane". Quest'ultimo, non ricorrendo elementi tipici della formazione, ovvero lezioni in aula o a distanza, feedback iniziali e finali e valutazione finale della fruizione della formazione dei discenti, non ha ritenuto di allocare sul proprio budget l'iniziativa in questione. Pertanto, trattandosi essenzialmente di temi legati all'awareness ed alla consapevolezza in ambito di sicurezza ICT e di attività specialistiche ad essa connesse, il budget di riferimento è stato correttamente individuato nell'ambito del Settore "Esercizio Sistemi ICT".

Dall'analisi degli strumenti acquisitivi messi a disposizione da Consip è emerso che il lotto 1[1] dell'Accordo Quadro Consip ID 2296[2]- Servizi di sicurezza da remoto, di compliance e controllo - soddisfa pienamente il fabbisogno definito.

[1] In caso di appartenenza al comparto della Pubblica Amministrazione Centrale (cd. PAC), come nel caso di AdeR, l'affidamento è stato attribuito all'operatore economico RTI costituito TELECOM ITALIA S.P.A. - NETGROUP S.P.A., REEVO S.P.A., KPMG ADVISORY S.P.A., ALMAVIVA -THE ITALIAN INNOVATION COMPANY S.P.A..

[2] Gara bandita il 09/09/2021 (Pubblicazione bando su GUUE n. S 178 del 14/09/2021, Pubblicazione bando su GURI n. 108 del 17/09/2021), ai sensi dell'art. 4, comma 3 quater del d.l. 95/2012.

Pertanto:

- in data 20/10/2023, come previsto dall'Accordo Quadro Consip ID 2296, AdeR ha trasmesso al fornitore aggiudicatario - RTI TIM - il Piano dei Fabbisogni definito a valle del completamento della analisi effettuata internamente (prot. AdeR n. 9889656 del 20/10/2023);
- in data 08/11/2023, quindi nei termini previsti dall'Accordo Quadro Consip ID 2296, l'RTI TIM ha trasmesso ad AdeR il Piano Operativo afferente al relativo Piano dei Fabbisogni (Prot. AdeR n. 10317219 del 08/11/2023);
- in data 20/11/2023, a integrazione del Piano Operativo, l'RTI TIM ha trasmesso l'annesso "Valorizzatore economico (Prot. AdeR n. 10565536 del 20/11/2023).

Ciò premesso e in considerazione:

- degli standard di sicurezza adottati da AdeR, coerentemente alle misure di Sicurezza definite da AgID;
- dell'efficacia, a far tempo dal 25 maggio 2018, del regolamento generale sulla protezione dei dati (RGPD, in inglese GDPR, General Data Protection Regulation- Regolamento UE 2016/679), pubblicato sulla Gazzetta Ufficiale Europea il 4 maggio 2016;
- dell'evoluzione del programma di awareness nell'ambito del Sistema di Gestione per la Sicurezza delle Informazioni (SGSI) adottato da AdeR,

risulta necessario provvedere all'approvvigionamento dei servizi di seguito descritti.

Fabbisogno

Dall'analisi dei servizi disponibili nell'ambito del lotto 1 dell'AQ ID 2296, è stata individuata la soluzione di seguito descritta e analiticamente riportata nell'allegato Piano Operativo (Allegato "A"), risultato conforme rispetto al Piano dei Fabbisogni definito da AdeR.

Il servizio "Formazione e Security awareness" è mirato a sensibilizzare il personale dell'Ente su molteplici aspetti della sicurezza delle informazioni, incrementando il livello di consapevolezza ed innalzando conseguentemente il livello di sicurezza per la protezione dei dati critici e personali gestiti. Lo scopo del servizio è quello di sviluppare negli utenti le competenze essenziali, le tecniche e i metodi fondamentali per prevenire il più possibile gli incidenti di sicurezza e reagire al meglio a fronte del verificarsi degli stessi.

Il servizio definito è basato su:

- **Campagne di Phishing**. Il Phishing rappresenta il principale veicolo utilizzato dagli attaccanti per accedere alle informazioni e dati presenti sui nostri dispositivi sia laptop che mobile. Attacchi affini, come lo Smishing, il Vishing

ed il QRishing sono sempre più spesso utilizzati con gli stessi scopi anche per rendere più credibili le e-mail malevoli inviate. In ottica di miglioramento continuo ed al fine di monitorare e valutare l'efficacia delle attività di user awareness, le Campagne di Phishing su tutto il personale sono svolte per raggiungere i seguenti obiettivi:

  - Awareness: attività volta ad aumentare la consapevolezza del personale rispetto ai rischi legati alle attività di Phishing, Smishing, Vishing, QRishing.
  - Risk Evaluation: misurare il rischio associato alle minacce, evidenziando le possibili conseguenze di un eventuale attacco.
  - Threat Identification: incrementare la capacità di individuare questa tipologia di attacchi, limitando al minimo i possibili danni che potrebbero causare.
  - Nel corso della durata contrattuale, sono richieste in totale 12 Campagne di Phishing (circa 4 all'anno).

- **Pillole di Sicurezza e Newsletter Periodiche.** L'erogazione di Pillole di Sicurezza e Newsletter, a cadenza periodica, concorre a mantenere alta la focalizzazione dell'attenzione sulle esigenze di presidio relative ai rischi connessi alle principali tematiche della Cyber Security. Sia le Pillole di Sicurezza che le Newsletter sono composte da un breve contributo redazionale di circa 1.000/1.500 caratteri e condivisa con cadenza periodica via e-mail a tutti i dipendenti della Pubblica Amministrazione. Gli argomenti trattati sono proposti nell'ambito di un piano coordinato con gli interventi formativi inclusi nel Servizio di Formazione e Awareness in coerenza con le caratteristiche del contesto di riferimento dell'Ente. L'obiettivo è quello di portare all'attenzione degli utenti fatti ed eventi di tipo Cyber recenti e realmente accaduti fornendo anche consigli su come ciascun dipendente può difendersi e prevenire eventuali attacchi. Nel corso della durata contrattuale, sono richieste in totale 12 Pillole di Sicurezza e Newsletter (complessivamente 4 all'anno).
- **Cyber Security Journal:** La tematica delle minacce di Cyber Security non ha un impatto esclusivamente sulle infrastrutture tecnologiche ma anche sulle persone. Infatti, più del 59% degli attacchi Cyber vanno a buon fine a causa dell'errore umano (es. apertura di un link nell'email di phishing, uso improprio dello smartphone, etc.). I Cyber Security Journal hanno quindi lo scopo di raccogliere informazioni e notizie a livello globale e nell'ambito delle Pubbliche Amministrazioni relativamente alle principali minacce Cyber, andando a sensibilizzare i dipendenti riguardo i principali rischi e su come difendersi. Un altro importante obiettivo dei Cyber Security Journal è quello di coniugare tematiche complesse come gli attacchi reali e la storyline degli eventi occorsi, con esempi legati alla vita di tutti i giorni. L'unione di complessità e quotidianità risulta fondamentale per aumentare la consapevolezza dei dipendenti delle Pubbliche Amministrazioni che loro stessi rappresentano la prima linea di difesa contro gli attacchi Cyber e che i loro comportamenti, molto spesso, possono causare incidenti di sicurezza

anche gravi. Nel corso della durata contrattuale, sono richiesti 9 Cyber Security Journal (3 all'anno).

- **Monitoraggio e Reporting:** Le attività formative necessitano di un continuo monitoraggio con l'obiettivo di valutare l'efficacia delle strategie formative e identificare eventuali lacune o aree di miglioramento consentendo quindi l'identificazione di eventuali azioni correttive da implementare. È pertanto richiesta l'attività di Monitoraggio e Reporting con l'obiettivo di presentare i risultati delle campagne di Phishing e lo status report delle attività di formazione svolte. Si richiede la formalizzazione di Report su base bimestrale, qualora necessario potrà essere concordata con l'Amministrazione una maggiore frequenza di analisi e rilascio di Report.

Nel prospetto che segue è riportata la previsione di spesa da sostenere nell'ambito del nuovo contratto esecutivo da stipulare in adesione al lotto 1 dell'AQ Consip ID 2296, applicando le tariffe previste nel medesimo AQ e per una durata di 36 (trentasei) mesi.

Cod. Serv.	Servizio	Fascia di acquisizione	Unità di misura	Tipologia remunerazione	Quantità	Importo Unitario [€]	Durata Contrattuale (Mesi)	Importo Totale del servizio [€]
L1.S9	Servizio di Formazione e Security awareness	Team Ottimale	gg/p	gg/p	750	231 €	36	173.250,00 €
	Servizio di Formazione e Security awareness	Team Ottimale	gg/p	gg/p		231 €		
	Servizio di Formazione e Security awareness	Team Ottimale	gg/p	gg/p		231 €		- €
	Servizio di Formazione e Security awareness	Team Ottimale	gg/p	gg/p		231 €		- €
							IMPORTO TOTALE CONTRATTO (KPMG - L1.S9) =	173.250,00 €

Le sessioni di formazione saranno erogate da remoto, la metrica di servizio è espressa in giorni/persona del Team ottimale (pari a 8 ore lavorative), la modalità di remunerazione è di tipo "Progettuale" (a corpo).

Quadro economico complessivo

Il quadro economico complessivo degli oneri dell'appalto risultante pari a 175.398,30 €, come dettagliato nella tabella seguente, è stato determinato sulla base del valore dell'acquisizione dei nuovi servizi pari a € 173.250,00, del contributo da corrispondere a Consip S.p.A., pari a € 1.386,00, calcolato sulla base di quanto riportato all'art. 19.2 del contratto esecutivo, e dell'IVA indetraibile (2%) calcolata al netto del contributo Consip, pari a € 762,30.

Quadro economico degli oneri complessivi della procedura acquisitiva			
A	**Servizi**		**importi dati in €**
A1	Importo		173.250,00
A2	Costi per l'eliminazione delle interferenze		
	Totale a		**173.250,00**
B	**Somme a disposizione dell'amministrazione**		
B1	Spese per le commissioni giudicatrici		

B2	Pagamento contributo per procedura di gara anac		
B3	Spese per pubblicità legale		
B4	Altri costi eventuali riferibili all'appalto - contributo Consip fuori campo IVA, conformemente alla misura prevista dall'articolo 2, lettera a), del D.P.C.M. 23 giugno 2010 (8 per mille del valore del contratto esecutivo sottoscritto)		1.386,00
	Totale b		**1.386,00**
	Totale (a+b)		**174.636,00**
C	**Iva (*)**		
C1	IVA sul servizio (2% indetraibile))		762,30
C2	IVA su costi per la sicurezza di natura interferenziali (2% indetraibile)		
C3	IVA sulle somme a disposizione dell'Amministrazione (2%) (voce B3)		
	Totale C		**762,30**
	TOTALE COMPLESSIVO DELL'APPALTO (A+B+C)		**175.398,30**

(*) Il pro-rata di detrazione dell'IVA è indicato in base al dato definitivo del 2022. La percentuale potrebbe variare negli anni seguenti.

L'impegno di spesa complessivo trova copertura nel Budget Economico relativo al triennio 2023-2025 deliberato dal Comitato di Gestione di AdeR del 27 ottobre 2022 e risulta coerente anche con quanto previsto nel Budget Economico 2024-2026 deliberato dal Comitato di gestione di AdeR del 26 ottobre 2023.

L'iniziativa acquisitiva è inserita dall'Ufficio Pianificazione Acquisti e Monitoraggio Contratti nella programmazione dell'Ente in vigore alla data col codice pianificazione interno 2023.9.001.I.

Indicazioni per la stesura del DUVRI di cui al D. Lgs. n. 81/2008

Stante la natura intellettuale dei servizi oggetto di gara, ai sensi dell'art. 26, comma 3 bis del D. Lgs. 81/2008, non si renderà necessario predisporre il Documento Unico di Valutazione dei Rischi da Interferenza (DUVRI); conseguentemente l'importo degli oneri della sicurezza connessi ai rischi da interferenza è pari a zero.

Costo della Manodopera

Trattandosi di solo servizi di natura intellettuale, ai sensi di quanto disposto dall'ANAC nella delibera n. 1228 del 22 novembre 2017, non sussiste l'obbligo di indicare i costi della manodopera.

Clausola sociale

Trattandosi di servizi di natura intellettuale, non trova applicazione l'art. 50 del D. Lgs. n. 50/2016.

Garanzie

Secondo quanto disposto all'articolo 12 "GARANZIA DELL'ESATTO ADEMPIMENTO" del contratto esecutivo, il fornitore presenterà la garanzia definitiva antecedentemente la sottoscrizione dello stesso.

Per quanto concerne la RCT, per la specifica attività del servizio erogato non si necessita di specifica polizza. Pertanto, a norma dell'art. 17 del contratto esecutivo "il Fornitore assume in proprio ogni responsabilità per infortunio o danni eventualmente subiti da parte di persone o di beni, tanto del Fornitore quanto dell'Amministrazione o di terzi, in dipendenza di omissioni, negligenze o altre inadempienze attinenti all'esecuzione delle prestazioni contrattuali ad esso riferibili, anche se eseguite da parte di terzi".

Subappalto

Il fornitore si è riservato di affidare in subappalto, nella misura non superiore al 50% dell'importo dell'Accordo Quadro, l'esecuzione delle seguenti prestazioni:

- omissis ..
- **Formazione e security awareness**
- ..omissis..

salvo quanto previsto dall'art. 105, comma 12, del d. lgs. n. 50/2016.

Penali

L'Amministrazione potrà applicare al Fornitore le penali dettagliatamente descritte e regolate nel contratto esecutivo.

Per le modalità di contestazione ed applicazione delle penali vale tra le Parti quanto stabilito all'articolo 9 del contratto esecutivo.

Modalità di fatturazione

La fatturazione dei corrispettivi maturati dall'Aggiudicatario per le attività prestate, avrà cadenza bimestrale secondo quanto disposto all'articolo 11 "Fatturazione e Pagamenti" del contratto esecutivo.

Modalità acquisitiva

Tenuto conto della natura dei servizi oggetto dell'affidamento, si ritiene che l'approvvigionamento dei servizi ICT possa essere fatto aderendo all'AQ Consip ID 2296 - "Servizi di sicurezza da remoto, di compliance e controllo", lotto 1.

Va sottolineato che l'acquisizione del servizio descritto mediante adesione all'AQ menzionato deve avvenire ai sensi dell'art. 1, comma 512 della L. 28 dicembre 2015, n. 208 (legge di stabilità 2016) atteso che i servizi previsti da detto contratto quadro sono idonei al soddisfacimento dello specifico fabbisogno acquisitivo rappresentato nel presente documento.

L'iniziativa, inoltre, non è in contrasto con la citata legge neppure sotto l'altro profilo dell'obbligo del risparmio di spesa; ciò per effetto dell'esimente espressamente prevista all'art. 1, comma 515, che esclude da tale obbligo "la spesa effettuata tramite Consip S.p.A.".

Al fine di aderire al suddetto AQ, occorrerà trasmettere all'indirizzo PEC aq.sicurezzadaremoto@pec.telecomitalia.it del RTI Telecom Italia S.p.A. aggiudicatario, il Piano operativo approvato ed il Contratto esecutivo compilato e sottoscritto sulla base dell'apposito template.

Conclusioni

Sulla base delle considerazioni svolte, si rende necessario acquisire i servizi secondo le specifiche tecniche ed economiche riportate nel Piano Operativo allegato alla presente, mediante la stipula di un contratto esecutivo in adesione all'AQ Consip ID 2296 - "Servizi di sicurezza da remoto, di compliance e controllo", lotto 1.

La durata sarà di 36(trentasei) mesi e il massimale di spesa sarà pari a € 173.250,00, oltre IVA.

Il totale complessivo degli oneri dell'appalto sarà pari a € 175.398,30, , comprensivo del contributo da corrispondere a Consip S.p.A. e dell'IVA indetraibile.

Allegati:

- Allegato A - Piano Operativo_ADER_v1.0.

Il Responsabile del Procedimento
Valerio Ricciardi
(Firmato digitalmente)