Sardegna IT

REGIONE AUTÒNOMA DE SARDIGNA
REGIONE AUTONOMA DELLA SARDEGNA

ISTRUTTORIA DI ACQUISTO PER FORNITURE DI BENI E SERVIZI

Acronimo di progetto	e-HEALTH-2020
Denominazione dell'incarico	Interventi per lo sviluppo dei sistemi e per l'erogazione dei servizi di sanità elettronica in Sardegna
Rif. Incarico	Lettera di incarico, sottoscritta in data 20.06.2017, ns. prot. n. 1923 del 20.06.2017 Appendice integrativa n. 1, sottoscritta in data 27.10.2017 approvata con nota RAS ns. prot.n. 3341 del 02.11.2017
Rif. Piano Operativo	PoP vers. 2.0
Rif. Intervento / attività	9.0 - Altre somme a budget per ulteriori esigenze di supporto, realizzazione sistemi informativi, acquisizione di infrastrutture, tecnologie HW e licenze SW, servizi professionali, comunemente condivisibili tra i diversi interventi in essere e/o di integrazione con i sistemi e le infrastrutture RAS del CED/CSR o altri interventi di interesse sull'E-HEALTH
Rif. Budget	9.1.0 - Altre somme a Budget Bilancio regionale Titolo II euro 412.238,36
Oggetto acquisizione	Servizi di Vulnerability Assessment / Penetration Test, Cyber Security, scanning
Codifica interna (ove pertinente)	
Motivazione, descrizione, scadenze	A Maggio del 2018 è entrato in vigore il GDPR (General Data Protection Regulation). Tale regolamento prevede che i titolari dei dati si preoccupino di rendere/far rendere i sistemi sicuri e adottino le necessarie azioni per limitare i possibili casi di accesso malevolo ai dati personali e sensibili di cittadini e dipendenti. Il Rapporto CLUSIT 2017 sulla sicurezza ICT in Italia ha evidenziato che In ambito Pubblica Amministrazione, la Sanità è stata quella che registra un incremento più forte di attacchi. "*Questo non stupisce perché la Sanità, con i dati sensibili che gestisce, rappresenta probabilmente un bersaglio molto appetibile per i cyber-criminals. Per poter contrastare gli attacchi di ransomware è necessario sviluppare programmi di awareness mirati per gli utilizzatori dei sistemi informativi della PA e, nel contempo, implementare le necessarie misure di sicurezza (es. backup frequenti dei dati) per contenere gli impatti degli attacchi. Se non si attueranno delle misure urgenti in tal senso, esiste il rischio concreto che tale fenomeno perduri …*". Nel periodo Maggio – Settembre 2018 si sono verificati diversi casi di possibili eventi di data breach sul sistema di posta dell'Azienda per la Tutela della Salute (ATS) gestito da Sardegna IT. Il titolare dei dati, ATS ha richiesto la verifica sulla vulnerabilità del nuovo sistema di posta, gestito da Sardegna IT, e al contempo di verificare se ci sono in atto azioni di hacker che abbiano come obiettivo la ATS e in generale il Servizio Sanitario Regionale. E' necessario quindi intraprendere, con urgenza, azioni atte a verificare lo stato del sistema di posta e l'eventuale interesse di hacker. La verifica consentirà altresì di rispondere ad eventuali richieste di verifica da parte del garante della privacy che potrebbe promuovere ispezioni in conseguenza alle segnalazioni di possibili data breach sul sistema di Posta comunicate dalla ATS. Anche l'Assessorato Igiene e Sanità della Regione Sardegna richiede che i sistemi informativi sanitari regionali promossi dalla Regione siano sicuri rispetto a possibili accessi malevoli a dati sensibili. Tali sistemi registrano dati molto sensibili pertanto è indispensabile verificare se siano vulnerabili. I servizi che devono essere richiesti in particolare sono: - Vulnerability Assessment e Penetration Test per il sistema di Posta ATS: VA e PT ESTERNO in modalità Black Box. Il perimetro di questo test sono tutti i sistemi esposti su internet, server o dispositivi tra cui i server dei nomi di dominio (DNS), server di posta, server Web o firewall. L'obiettivo è quello di scoprire se un aggressore esterno può entrare e quanto può ottenere una volta che hanno guadagnato l'accesso. - Vulnerability Scanning su perimetro sanità per un periodo di 3 mesi: L'obiettivo è quello di identificare le principali vulnerabilità presenti sui sistemi che possono essere oggetto di attacchi. Viene eseguita una scansione utilizzando uno strumento di scansione che cerca di mappare le principali vulnerabilità presenti sui sistemi assegnando per ognuna di esse uno scoring CVE. L'attività, condotta secondo la metodologia OSSTMM sugli indirizzi IP e URL specificati da Sardegna IT (Perimetro) - Cyber Intelligence su perimetro sanità per un periodo di 3 mesi: Questo servizio consta di un monitoraggio giornaliero eseguito specificatamente per il perimetro sanità della Regione Sardegna. In caso di riscontro di informazioni che possono essere ricondotte ad una generica minaccia, viene immediatamente data segnalazione a SardegnaIT, tramite mail o contatto telefonico e contemporaneamente viene acquisita l'evidenza secondo metodologie forensi. L'attività dovrà essere svolta adottando standard internazionali riconosciuti riguardo alle attività in ambito IT Security. Si è stimato che i servizi richiesti possano essere ricompresi in una fascia di prezzo di circa € 30.000,00 oltre IVA.
Modalità acquisizione	Procedura negoziata senza previa pubblicazione del bando di gara, da esperirsi ai sensi dell'art. 36, comma 2, lettera a) del D.lgs. 50/2016.

Modalità di scelta del fornitore	Quanto espresso nel paragrafo "*Motivazione, descrizione, scadenze*" porta a rilevare: - la necessità di attivazione urgente dei servizi e ciò fa ritenere che un possibile ricorso a una procedura o al lotto CONSIP SPC ritarderebbe l'avvio del servizio oltre l'urgenza dettata dalla verifica sulla possibilità di vulnerabilità in considerazione della frequenza di accesso anomalo alle caselle di e-mail sugli utenti ATS riscontrato a partire da Giugno 2018. - considerazioni di evidenti opportunità di limitazione della diffusione della notizia dell'attivazione del servizio per non vanificare l'efficacia del servizio stesso, Per la scelta del fornitore sono state interpellate 3 aziende leader nel settore di cui trattasi e precisamente è stata richiesta un'offerta per i servizi sotto identificati a: - Abissi s.r.l. Via Togliatti 78 - 09028 Sestu (CA), P.IVA e C.F. 03524690926, email: info@abissi.eu - Adora ICT s.r.l. Viale Europa, 55 – 00144 Roma, P.IVA e C.F. 08590111004, email: info@adora-ict.com - ISGroup SRL Vicolo Miracoli, 1 - 37121 Verona (VR), P.IVA 04164220230, email: sales@isgroup.it Servizi richiesti e offerti: - Vulnerability Assessment e Penetration Test per il sistema di Posta ATS: VA e PT ESTERNO in modalità Black Box. Il perimetro di questo test sono tutti i sistemi esposti su internet, server o dispositivi tra cui i server dei nomi di dominio (DNS), server di posta, server Web o firewall. L'obiettivo è quello di scoprire se un aggressore esterno può entrare e quanto può ottenere una volta che hanno guadagnato l'accesso. - Vulnerability Scanning su perimetro sanità per un periodo di 3 mesi: L'obiettivo è quello di identificare le principali vulnerabilità presenti sui sistemi che possono essere oggetto di attacchi. Viene eseguita una scansione utilizzando uno strumento di scansione che cerca di mappare le principali vulnerabilità presenti sui sistemi assegnando per ognuna di esse uno scoring CVE. L'attività, condotta secondo la metodologia OSSTMM sugli indirizzi IP e URL specificati da Sardegna IT (Perimetro) - Cyber Intelligence su perimetro sanità per un periodo di 3 mesi: Questo servizio consta di un monitoraggio giornaliero eseguito specificatamente per il perimetro sanità della Regione Sardegna. In caso di riscontro di informazioni che possono essere ricondotte ad una generica minaccia, viene immediatamente data segnalazione a SardegnaIT, tramite mail o contatto telefonico e contemporaneamente viene acquisita l'evidenza secondo metodologie forensi. L'attività dovrà essere svolta adottando standard internazionali riconosciuti riguardo alle attività in ambito IT Security. Le aziende interpellate hanno fornito i seguenti prezzi: - Abissi ha presentato una offerta per i servizi richiesti più un altro senza ulteriori oneri per un importo pari a 17.800,00 € - Adora ICT ha presentato una offerta per i servizi richiesti per un importo pari a € 33.600,00 - ISGroup SRL ha presentato 3 offerte per i servizi richiesti secondo differenti granularità per i servizi richiesti per un importo pari a: • 40.156,00 € per una proposta denominata FULL • 29.656,00 € per una proposta denominata Medium • 25.756,00 € per una proposta denominata small Alla luce di quanto esposto, si propone di affidare il servizio alla società Abissi S.r.l. in quanto ha presentato una proposta tecnica completa e congruente con le attese di Sardegna IT ed ha altresì offerto il prezzo più basso fra tutte le società interpellate includendo nell'offerta, senza ulteriori oneri, un servizio di VA/PT aggiuntivo. Il fornitore proposto presenta altresì: - vicinanza geografica con la sede di Sardegna IT, - esperienza acquisita con altri Clienti di grandi dimensioni (fra i quali sono compresi Magneti Marelli, Iveco, HDI, Barilla, Arborea, Wind, Unieuro, Ansaldo Energia, Alitalia, Aeroporti di Roma, Lottomatica, BNL, BPER), - esperienza specifica di almeno 10 anni maturata dal personale tecnico che si dovrà occupare del servizio.
Importo previsto	17.800,00 € Iva Esclusa

Modalità fatturazione e pagamento	Pagamento mediante bonifico bancario, 30gg DFFM
Validazione e idoneità tecnica	La fornitura richiesta è identificata come indicato nelle "Descrizione e/o specifiche di dettaglio tecnico e dimensionale" ed è idonea e coerente con quanto previsto dall'incarico e/o piano operativo e/o altra documentazione già approvata regolamentante l'incarico per cui viene acquisita

	Rif. PO	Budget assegnato	Budget già impegnato	Budget disponibile	Budget da impegnarsi
Budget e copertura della spesa	*PoP vers. 2.0* 9.1.0 - Altre somme a Budget Bilancio regionale Titolo II euro 412.238,36	412.238,36 € Iva Esclusa	*158.258,58 € Iva Esclusa*	*253.979,78 € Iva Esclusa*	*17.800,00 € Iva Esclusa*

	Responsabile di incarico	Data richiesta	Firma
Richiesta acquisto formulata da	*Valter Degiorgi*	18/10/2018	Valter Degiorgi

	ROP di progetto	Data richiesta	Firma
Verifica copertura attestata da	*Alberto Dessena*	18/10/2018	Alberto Dessena

	Responsabile di incarico	Data approvazione	Firma
Richiesta verificata e autorizzata da	*Valter Degiorgi*	18/10/2018	Valter Degiorgi