Piano dei Fabbisogni

"AgID progetto CERT-PA"

"SERVIZI DI GESTIONE DELLE IDENTITÀ DIGITALI

E

SICUREZZA APPLICATIVA"

(Servizi di cloud computing, di sicurezza, di realizzazione di portali e servizi online e di cooperazione applicativa per le pubbliche amministrazioni – Lotto 2)

Maggio 2018

INDICE

1. DATI ANAGRAFICI AMMINISTRAZIONE

Ragione sociale Amministrazione:	Agenzia per l'Italia Digitale
Indirizzo	Via Liszt, 21
CAP	00144
Comune	Roma
Provincia	Roma
Regione	Lazio
Codice Fiscale	97735020584
Codice IPA	AGID
Indirizzo mail	protocollo@pec.agid.gov.it
PEC (SÌ/NO)	SÌ

Referente Amministrazione	Francesco Tortorelli
Ruolo	Dirigente Responsabile Area "Architetture, standard e infrastrutture"
Telefono	0685264435
Indirizzo mail	tortorelli@agid.gov.it
PEC	protocollo@pec.agid.gov.it

2. DESCRIZIONE DELLE ESIGENZE

Il presente documento ha lo scopo di descrivere le esigenze dell'Agenzia per l'Italia Digitale, di seguito AgID, nell'ambito dei servizi offerti dal Contratto quadro SPC - Lotto 2 relativo alla fornitura di servizi di Identità Digitale e Sicurezza Applicativa, così come previsti nel Contratto Quadro [DA-1], stipulato da AgID/Consip ed il RTI composto da:

- Leonardo-Finmeccanica S.p.A. (mandataria)
- IBM Italia S.p.A. (mandante)
- Sistemi Informativi S.r.l. (mandante)
- Fastweb S.p.A. (mandante)

Il presente Piano dei Fabbisogni richiede in particolare l'attivazione dei servizi di seguito descritti:

- L2.S3.7 Next Generation Firewall Management
- L2.S3.9 Servizi professionali

2.1 L2.S3.7 NEXT GENERATION FIREWALL MANAGEMENT

A tutela della piattaforma di trasmissione automatizzata degli IOC (cfr. 2.2.2) dovrà essere previsto un servizio di sicurezza NGFW con throughput fino a 200 Mbps per la durata di 36 mesi.

2.2 L2.S3.9 SERVIZI PROFESSIONALI

AgID intende dotarsi di attività erogabili nell'ambito del contratto, di cui ai servizi L2.S3.9 (Servizi professionali) per le attività di seguito elencate.

A. Nell'ambito del progetto INFOSEC, servizi di progettazione e supporto allo sviluppo di una piattaforma di aggregazione di dati.
B. Servizi di progettazione per la definizione degli standard per la condivisione degli IOC e la relativa gestione dell'infrastruttura operativa.
C. Servizi di progettazione e sviluppo delle componenti di sicurezza del portale riservato del CERT-PA.
F. Supporto al modello di Ingaggio delle Regioni per il CERT-PA.

Le attività dovranno essere erogate a task in base ad obiettivi temporali prefissati e potranno essere svolte sia presso la sede del cliente sia presso una delle sedi del RTI. È richiesta l'effettiva presenza presso le sedi di AgID solo per il personale del fornitore che dovrà interfacciarsi direttamente con i referenti di AgID per la raccolta dei requisiti e per le riunioni relative allo stato di avanzamento dei lavori. Il resto delle attività potranno essere erogate dalla sede del fornitore o da altra sede da concordare con l'Amministrazione stessa.

2.2.1 SUPPORTO ALLA DEFINIZIONE E SVILUPPO DI UNA CYBER SECURITY KNOWLEDGE BASE

L'Amministrazione richiede servizi professionali H8 a supporto della realizzazione di una capacità di Cyber Security Knowledge Base nella quale verranno raccolte le informazioni sulle infrastrutture realizzate nel dominio della Pubblica amministrazione e sugli eventi di sicurezza occorsi nel tempo al loro interno.

Si richiede, a tale scopo, la fornitura di servizi di progettazione e sviluppo di un sistema informativo per l'archiviazione e l'interrogazione d'informazioni relative alla sicurezza (vulnerabilità, minacce, incidenti, ecc.). Il mix di risorse offerte dovrà possedere:

- conoscenza delle architetture di sicurezza di sistemi informativi;
- capacità di progettazione di componenti di sicurezza infrastrutturali e applicative;
- conoscenza delle piattaforme di sicurezza utilizzate per l'erogazione dei servizi web;
- conoscenza dei principi di sicurezza applicativa;
- conoscenza di architetture web oriented e SOA;
- conoscenza di DB relazionali e RDBMS;
- conoscenza delle linee guida per la produzione di codice sicuro;
- ottima conoscenza del linguaggio PHP5;
- conoscenza del linguaggio PHP7 (nessuna esperienza specifica richiesta);
- esperienza nell'implementazione progettuale con pattern architetturale MVC;

- comprovata esperienza pluriennale nell'uso del framework PHP;
- profonda conoscenza di SQL e ODBC;
- esperienza di sviluppo in ambiente LAMP;
- approfondita conoscenza tecnica e progettuale di HTML5, CSS3 e Javascript;
- esperienza in progettazione e sviluppo di Web Services (SOAP, XML-RPC, REST);
- esperienza nell'uso dei sistemi di controllo di versione e conoscenza dei sistemi distribuiti Git e Bazaar;
- esperienza con Zend Framework, a partire dalla versione 1.10,
- conoscenza DBMS Oracle, MySQL e Postgres;
- esperienze in progettazione di database con implementazione del modello ER;
- esperienza nella progettazione e realizzazione di processi ETL.

Sono inoltre gradite esperienze nell'uso di framework e librerie CSS e JavaScript.

Si richiede l'erogazione del servizio per una durata di 36 mesi.

2.2.2 SERVIZI PER LA PIATTAFORMA DI TRASMISSIONE AUTOMATIZZATA DEGLI IOC

L'Amministrazione intende potenziare le proprie capacità di information sharing con le strutture nazionali di Cyber Security tramite una piattaforma per la trasmissione automatizzata degli IOC. Allo scopo richiede l'erogazione di servizi professionali per la gestione operativa e la sicurezza della piattaforma di *information sharing* **MineMeld** per la condivisione delle informazioni sugli indicatori di compromissione (IOC) con la piattaforma del CERT-PA INFOSEC (https://infosec.cert-pa.it) ed ai referenti delle PA.

Nell'ambito dei suddetti servizi professionali, AgID richiede il supporto specialistico per il progetto e lo sviluppo della piattaforma di condivisione IOC. In particolare, oltre alle competenze di Information Security, sono necessarie specifiche esperienze di sviluppo software in ambiente Python.

Si richiede l'erogazione del servizio per una durata di 36 mesi.

2.2.3 ADEGUAMENTO DELLA PIATTAFORMA DI INFOSHARING RISERVATA DEL CERT-PA

I servizi professionali richiesti hanno come oggetto la revisione della piattaforma di infosharng riservata del CERT-PA fruibile da rete Infranet, al fine di migliorare il livello di sicurezza globale. L'attuale soluzione utilizza Liferay Portal Community Edition 6.2 CE GA2 in bundle con Tomcat in configurazione standalone.

Si richiede di migrare il portale su Liferay Portal Enterprise Edition con Tomcat e database MySQL. Tutte le componenti software dovranno garantire il massimo livello di patching disponibile al fine di limitare qualunque problema di sicurezza. Inoltre tutti i contenuti, ove possibile, dovranno essere gestiti tramite le funzionalità del CMS. L'infrastruttura per l'erogazione dei servizi richiesti, compresa quella necessaria all'installazione di Liferay Portal Enterprise Edition, sarà messa a disposizione da AgID.

Di seguito si riassumono i requisiti di carattere generale che dovranno essere soddisfatti dal Fornitore nell'erogazione dei servizi professionali specialistici richiesti:

- ove possibile, utilizzare le funzionalità standard fornite da Liferay Portal in sostituzione delle componenti custom;
- utilizzare plugin/portlet forniti da Liferay Portal;
- eventuali sviluppi custom dovranno utilizzare le API standard di Liferay Portal Enterprise Edition;
- eventuale codice custom dovrà comunque rispettare stringenti criteri di sicurezza quali:
    - verifica statica della sicurezza del codice,
    - conformità alle norme OWASP.

Un elemento di sicurezza caratterizzante la soluzione è la gestione degli avvisi; questi dovranno essere cifrati automaticamente dal sistema, utilizzando la chiave pubblica dell'utente accreditato (preventivamente caricata sul portale tramite l'interfaccia preposta). Si raccomanda di porre particolare attenzione alla gestione delle chiavi pubbliche degli utenti.

La condivisione di documenti tra CERT-PA e utenti dovrà essere realizzata tramite la funzione di *data-sharing*. Ogni documento avrà il proprio insieme di autorizzazioni.

Anche la funzionalità di ricerca dovrà rispettare i criteri di sicurezza imposti dalle ACL applicate ai documenti. In particolare, non dovrà essere consentita la ricerca di documenti su cui l'utente non ha i permessi.

La piattaforma di infosharing riservata del CERT-PA deve essere conforme ai requisiti relativi all'accessibilità previsti per legge e deve rispettare gli usuali canoni di usabilità al fine di raggiungere gli obiettivi prefissati con efficacia, efficienza, soddisfazione da parte dell'utente. Il sito dovrà inoltre fornire un'interfaccia responsive che consenta di fruire i contenuti anche da dispositivi mobili (utilizzando framework di sviluppo quali, ad esempio, Bootstrap).

Si richiede l'erogazione del servizio per una durata di 36 mesi.

2.2.4 SUPPORTO AL MODELLO DI INGAGGIO DELLE REGIONI PER IL CERT-PA

L'Amministrazione richiede servizi professionali H8 per il supporto alla definizione del modello di ingaggio dei CERT di prossimità da/verso il CERT-PA e la revisione della procedura di Incident Response.

Si richiede l'erogazione del servizio per una durata di 12 mesi nell'ambito della durata complessiva del contratto esecutivo.

3. SERVIZI RICHIESTI

Per il soddisfacimento dei fabbisogni individuati nel presente documento l'Amministrazione stima un costo massimo complessivo di € 1.740.000,00 (IVA esclusa).

4. RIEPILOGO SERVIZI RICHIESTI

La PA fornisce una stima delle quantità richieste nella tabella sotto indicata.

SERVIZI DI SICUREZZA (I2.S3)										
							2018	2019	2020	2021
Codice	**Descrizione**	**Tipologia d'erogazione**	**Valutazione economica**	**Metrica**	**Fascia**		**Nun.tà**	**Nun.tà**	**Nun.tà**	**Nun.tà**
L2.S3.7	WEB APPLICATION FIREWALL MANAGEMENT E NEXT GENERATION FIREWALL MANAGEMENT	As a service	A canone (annuale)	throughput / anno	Fascia 1: throughput fino a 50 Mbps		**0**	**0**	**0**	**0**
					Fascia 2: throughput fino a 200 Mbps		**1**	**1**	**1**	**0**
					Fascia 3: throughput fino a 500 Mbps		**0**	**0**	**0**	**0**
							2018	**2019**	**2020**	**2021**
ID SPC	**Descrizione**			**Metrica**	**Servizio**	**Figura professionale**	**Nun.tà**	**Nun.tà**	**Nun.tà**	**Nun.tà**
L2.S3.9	Servizi PROFESSIONALI	On premise - Normale orario di lavoro (8 ore)	A corpo (gg/uu)	giorno/uomo	H8	Capo progetto	**361**	**131**	**100**	**0**
						Security Architect	**1.463**	**499**	**325**	**0**
						Specialista di tecnologia/prodotto Senior	**1.112**	**372**	**248**	**0**
						Specialista di tecnologia/prodotto	**95**	**190**	**190**	**0**
		On premise - Orario continuativo H24		giorno/uomo	H24	Specialista di tecnologia/prodotto Senior (H24)	**16**	**16**	**16**	**0**
						Specialista di tecnologia/prodotto (H24)	**0**	**0**	**0**	**0**