Agenzia per l'Italia Digitale
Presidenza del Consiglio dei Ministri

DETERMINAZIONE N. 92 /2017

Oggetto
Avvio della procedura comparativa per la selezione di collaboratori con rapporto di lavoro coordinato e continuativo da impegnare nel progetto CERT-PA presso l'Area "Sicurezza e CERT-PA" .

IL DIRETTORE GENERALE

VISTI gli articoli 19 (Istituzione dell'Agenzia per l'Italia Digitale), 21 (Organi e statuto), 22 (Soppressione di DigitPA e dell'Agenzia per la diffusione delle tecnologie per l'innovazione; successione dei rapporti e individuazione delle effettive risorse umane e strumentali) del decreto legge n. 83 del 22 giugno 2012, recante "Misure urgenti per la crescita del Paese", convertito, con modificazioni, nella legge n. 134 del 7 agosto 2012 e s.m.i. e l'articolo 14-bis (Agenzia per l'Italia digitale) del decreto legislativo n.82 del 7 marzo 2005 (Codice dell'amministrazione digitale) e s.m.i.

VISTO il decreto del Presidente del Consiglio dei Ministri dell'8 gennaio 2014 (pubblicato sulla GURI n. 37 del 14 febbraio 2014), che ha approvato lo Statuto dell'Agenzia per l'Italia Digitale (AgID);

VISTO il decreto del Presidente del Consiglio dei Ministri del 30 aprile 2015, registrato alla Corte dei conti in data 10 giugno 2015 al n.1574, con il quale il dott. Antonio Francesco Maria Samaritani è stato nominato, per la durata di un triennio, Direttore Generale dell'Agenzia per l'Italia Digitale con decorrenza dalla data del predetto decreto;

VISTO l'art. 7, comma 6 del decreto legislativo 30 marzo 2001, n. 165, concernente la disciplina delle collaborazioni esterne nella pubblica amministrazione;

VISTO l'art. 1, comma 188, della legge n. 266/2005 che consente all'Agenzia per l'Italia Digitale, la stipula di contratti di collaborazione coordinata e continuativa per l'attuazione di progetti di innovazione tecnologica i cui oneri non risultino a carico degli stanziamenti previsti per il funzionamento;

VISTO altresì l'art. 17, comma 30, del decreto legge 1° luglio 2009, n. 78, recante "Provvedimenti anticrisi, nonché proroga di termini", come modificato dalla legge di conversione 3 agosto 2009, n. 102, che ha sottoposto al controllo preventivo di legittimità della Corte dei Conti gli atti e i contratti concernenti sia le collaborazioni esterne di cui all'art. 7, comma 6, del d.lgs. n. 165/2001, sia gli studi e consulenze di cui all'art. 1, comma 9, della legge 23 dicembre 2005, n. 266;

CONSIDERATO che, nella nota prot. reg. int. n. 71 del 2 marzo 2017 il responsabile dell'Area Sicurezza e CERT-PA, dott. Mario Terranova ha richiesto di acquisire otto risorse professionali, previa ricognizione interna tra il personale eventualmente in possesso delle competenze necessarie e, in caso di esito negativo della ricognizione stessa, di procedere attraverso la selezione di collaborazioni coordinate e continuative;

CONSIDERATO che, a seguito della ricognizione interna effettuata, non sono state ravvisate risorse idonee con le competenze richieste, come da nota del Responsabile l'Area "Organizzazione e gestione del personale", datata 20 marzo 2017;

TENUTO CONTO della conseguente nota prot. reg. int. 228 del 3 aprile 2017 con la quale la Responsabile dell'Area "Sicurezza e CERT-PA" ha proposto al Direttore Generale la pubblicazione sul sito web dell'Agenzia dell'Avviso n. 4/2017 per l'avvio di procedure comparative per la selezione di n. 8 collaboratori con rapporto di lavoro coordinato e continuativo per l'Area Sicurezza e CERT-PA;

RITENUTO di approvare la citata proposta e avviare le conseguenti procedure comparative mediante pubblicazione sul sito web dell'Ente del relativo avviso;

DETERMINA

1. L'avvio di procedure comparative per la selezione delle seguenti risorse professionali esterne:

   Modulo A: un profilo Super senior (*Esperto di sicurezza cibernetica*), Consulente con esperienza lavorativa superiore a 10 anni, come descritti nel Modulo A. In considerazione dell'elevatissima competenza richiesta, che per altro esclude la possibilità di impegno a tempo pieno, il compenso annuo da corrispondere è pari a € 50.000,00, oltre oneri riflessi e IVA se dovuta.;

   Modulo B: tre profili Senior (Analisti di sicurezza cibernetica), Consulenti con esperienza lavorativa superiore a 10 anni, come descritti nel Modulo B. In considerazione dell'elevatissima specializzazione richiesta e dell'esigenza di assicurare la reperibilità h:24, il compenso annuo da corrispondere - in base ai compensi minimi riconosciuti a figure professionali che svolgono analoghe attività - è pari a € 58.000,00, oltre oneri riflessi e IVA se dovuta;

   Modulo C: tre profili Junior (Analisti di sicurezza cibernetica), Consulenti con esperienza lavorativa oltre tre anni fino a cinque, come descritti nel Modulo C. da impegnare per 36 mesi a tempo pieno e con reperibilità h24 - per le attività di supporto del CERT-PA, il compenso annuo da corrispondere - in base ai compensi minimi riconosciuti a figure professionali che svolgono analoghe attività - è pari a € 30.000,00, oltre oneri riflessi e IVA se dovuta;

   Modulo D: un profilo Senior (Analista programmatore), Consulente con esperienza lavorativa oltre cinque anni fino a dieci, come descritti nel Modulo D. da impegnare per 36

Agenzia per l'Italia Digitale
Presidenza del Consiglio dei Ministri

AVVISO 4/2017: Procedure comparative per il conferimento di n. 8 incarichi di collaborazione coordinata e continuativa da impegnare nel progetto CERT-PA presso l'Area "Sicurezza e CERT-PA".

PREMESSA

Gli obiettivi definiti per il biennio 2016-2018 dal Piano nazionale per la protezione cibernetica e la sicurezza informatica (PN), le nuove disposizioni della direttiva europea NIS e le indicazioni della direttiva 1 agosto 2015, richiedono l'adeguamento della struttura tecnico-operativa del CERT-PA.
I citati obiettivi posti in capo ad AgID richiedono lo sviluppo e l'implementazione del CERT-PA quale soggetto preposto al trattamento degli incidenti di sicurezza informatica per tutte le pubbliche amministrazioni, in uno scenario di collaborazione con i CERT della pubblica amministrazione a livello europeo ed internazionale e di cooperazione con le analoghe strutture di rilevanza nazionale, il CERT Nazionale ed il CERT Difesa.

L'esigenza di consolidare e aumentare la capacità operativa del CERT-PA per la prevenzione e reazione ad eventi cibernetici in tutto il dominio della pubblica amministrazione, per l'adeguamento alle disposizioni comunitarie e per gli adempimenti indicati dal PN è determinata dalla necessità di:

- continuare a garantire l'erogazione dei servizi in atto alle amministrazioni già utenti;
- accelerare le azioni per consentire lo sviluppo del CERT-PA estendo i servizi a tutte le pubbliche amministrazioni, in linea con gli obiettivi definiti dal PN;
- di implementare l'infrastruttura ed i servizi erogati, completando la definizione delle procedure operative, accrescendo la competenza del personale e creando un'opportuna rete di rapporti a livello nazionale ed internazionale.

È perciò necessario disporre di competenze ed esperienze consolidate sugli aspetti chiave della sicurezza informatica, congiunte alla capacità di trasferimento agli altri ed una conoscenza profonda del panorama della sicurezza cibernetica internazionale.

Con determinazione del Direttore Generale n. …del ….. è indetta pertanto una procedura comparativa per la selezione dei seguenti profili professionali:

- 1 **Profilo Super senior (*Esperto di sicurezza cibernetica*)**, Consulente con esperienza lavorativa superiore a 10 anni, come descritti nel Modulo A. In considerazione dell'elevatissima competenza richiesta, che per altro esclude la possibilità di impegno a tempo pieno, il compenso annuo da corrispondere è pari a € 50.000,00, oltre oneri riflessi e IVA se dovuta a carico dell'Agenzia.
- **3 Profili Senior (*Analisti di sicurezza cibernetica*)**, Consulenti con esperienza lavorativa superiore a 10 anni, come descritti nel Modulo B. In considerazione dell'elevatissima specializzazione richiesta e dell'esigenza di assicurare la reperibilità h:24, il compenso annuo da corrispondere - in base ai compensi minimi riconosciuti a figure professionali che svolgono analoghe attività - è pari a € 58.000,00, oltre oneri riflessi e IVA se dovuta a carico dell'Agenzia.

- **3 Profili Junior** (***Analisti di sicurezza cibernetica***), Consulenti con esperienza lavorativa oltre tre anni fino a cinque, come descritti nel Modulo C. da impegnare per 36 mesi a tempo pieno e con reperibilità h24 - per le attività di supporto del CERT-PA, il compenso annuo da corrispondere - in base ai compensi minimi riconosciuti a figure professionali che svolgono analoghe attività - è pari a € 30.000,00, oltre oneri riflessi e IVA se dovuta a carico dell'Agenzia.
- **1 Profilo Senior** (***Analista programmatore***), Consulente con esperienza lavorativa oltre cinque anni fino a dieci, come descritti nel Modulo D. da impegnare per 36 mesi a tempo pieno - per le attività di sviluppo del CERT-PA, il compenso annuo da corrispondere - in base ai compensi minimi riconosciuti a figure professionali che svolgono analoghe attività - è pari a € 40.000,00, oltre oneri riflessi e IVA se dovuta.

CRITERI DI SELEZIONE E VALUTAZIONE

Ai sensi del decreto legge 24 giugno 2014, n. 9, sono esclusi dalla partecipazione i candidati collocati in quiescenza nella qualità di lavoratore privato o pubblico.

I curricula pervenuti saranno selezionati in base alla rispondenza ai "Requisiti minimi" indicati nella descrizione di ciascun Modulo e di ciascun Profilo.

I candidati che avranno presentato domanda entro la data indicata dal presente Avviso e il cui curriculum risponda ai requisiti minimi indicati nella descrizione dei profili, saranno convocati, per posta elettronica, per un colloquio di valutazione comparativa effettuato da un'apposita Commissione all'uopo nominata.

Nel corso del colloquio saranno valutati:

- la rispondenza delle esperienze curriculari rispetto ai "Requisiti minimi" richiesti;
- le "Competenze e conoscenze specifiche" e la conseguente attinenza delle esperienze lavorative rispetto alle tematiche specificate nell'oggetto dell'incarico;
- i requisiti preferenziali.

Il punteggio massimo complessivo che potrà essere assegnato a ciascun candidato è di 30 punti, attribuibili, sulla base del curriculum e del colloquio, come indicato di seguito nella descrizione di ciascun modulo. Saranno considerati idonei i candidati che avranno ottenuto una valutazione pari o superiore a 18 punti.

Una volta completata la fase di valutazione comparativa, la Commissione predisporrà la graduatoria finale dei candidati idonei, ai fini del conferimento dell'incarico di collaborazione da parte del Direttore generale.

La conclusione della procedura comparativa di valutazione sarà resa nota sul sito AgID.

La graduatoria rimarrà efficace per un termine di un anno dalla data di pubblicazione della graduatoria stessa sul sito istituzionale.

CARATTERISTICHE DEGLI INCARICHI:

Durata:

- L'incarico relativo al Profilo Super senior (Esperto di sicurezza cibernetica Modulo A) ha una durata di trentasei mesi con impegno part time. L'efficacia del contratto di collaborazione è subordinata all'esito

del controllo preventivo della Corte dei Conti, di cui all'art. 3 della legge n. 20/1994 e s.m.i. e agli obblighi di cui all'art. 3 comma 18 della legge n. 244 del 2007.

- Gli incarichi relativi ai profili Senior (Analisti di sicurezza cibernetica Modulo B), Profili Junior (Analisti di sicurezza cibernetica Modulo C) e Profilo Senior (Analista programmatore Modulo D) hanno una durata di trentasei mesi con impegno full time. L'efficacia del contratto di collaborazione è subordinata all'esito del controllo preventivo della Corte dei Conti, di cui all'art. 3 della legge n. 20/1994 e s.m.i. e agli obblighi di cui all'art. 3 comma 18 della legge n. 244 del 2007.

Luogo di svolgimento e modalità di realizzazione:

Tutti gli incarichi saranno svolti necessariamente presso la sede dell'Agenzia per l'Italia Digitale, sita in Roma, ed eventualmente anche presso le sedi dei fornitori o di altri soggetti indicati dall'Agenzia, comunque all'interno del Comune di Roma, fatte salve partecipazioni saltuarie ed occasionali ad attività progettuali in altri luoghi del territorio nazionale o europeo.

PROFILI RICHIESTI

MODULO A

Profilo A1 – risorsa super senior con più di 10 anni di esperienza lavorativa - per consolidare e aumentare la capacità operativa del CERT-PA per la prevenzione e reazione ad eventi cibernetici in tutto il dominio della pubblica amministrazione, per l'adeguamento alle disposizioni comunitarie e per gli adempimenti indicati dal PN per:

- continuare a garantire l'erogazione dei servizi in atto alle amministrazioni già utenti;
- accelerare le azioni per consentire lo sviluppo del CERT-PA estendendo i servizi a tutte le pubbliche amministrazioni, in linea con gli obiettivi definiti dal PN;
- implementare l'infrastruttura ed i servizi erogati, completando la definizione delle procedure operative, accrescendo la competenza del personale e creando un'opportuna rete di rapporti a livello nazionale ed internazionale.

Oggetto dell'incarico

L'incarico consisterà nel supportare il CERT-PA nello svolgimento delle attività connesse allo sviluppo ed alla conduzione dei servizi del CERT-PA, di seguito indicate:

- servizi di analisi e di indirizzamento, finalizzati a supportare la definizione dei processi di gestione della sicurezza e lo sviluppo di metodologie e di metriche valutative per il governo della sicurezza cibernetica;
- servizi proattivi, aventi come scopo la raccolta e l'elaborazione di dati significativi ai fini della sicurezza cibernetica, l'emanazione di bollettini e segnalazioni di sicurezza, l'implementazione e la gestione di basi dati informative;
- servizi reattivi, aventi come scopo la gestione degli allarmi di sicurezza ed il supporto ai processi di gestione e risoluzione degli incidenti di sicurezza che avvengono all'interno del dominio delle PA;
- servizi di formazione e comunicazione, finalizzati a promuovere la cultura della sicurezza cibernetica favorendo il grado di consapevolezza e competenza all'interno delle PA, attraverso la condivisione di informazioni relative a specifici eventi in corso ed a nuovi scenari di rischio, concernenti specifiche tematiche di sicurezza delle informazioni.

Requisiti delle risorse professionale

Requisiti minimi

- almeno 10 anni di documentata esperienza lavorativa come consulente sulla sicurezza informatica per pubbliche amministrazioni o grandi aziende nazionali o multinazionali;
- specifica esperienza lavorativa come docente o formatore su tematiche che riguardano gli aspetti organizzativi della sicurezza;
- buona conoscenza della lingua inglese, parlata e scritta, con particolare riferimento al contesto di tipo tecnico-scientifico;

Conoscenze e competenze specifiche

- sicurezza organizzativa (analisi del rischio, business impact analysis, procedure di sicurezza, etc.);
- tecniche per la conduzione di attacchi informatici sia a livello di software di base che applicativo;
- misure di contrasto degli attacchi informatici a livello preventivo e di contenimento;
- correlazione degli eventi e strumenti per l'individuazione degli incidenti informatici;
- analisi forensica ed aspetti legali della criminalità informatica;
- formazione nel settore della sicurezza informatica;
- organizzazioni internazionali operanti nel settore della sicurezza cibernetica.

Requisiti preferenziali

- specifica esperienza in organizzazioni o istituzioni nazionali o europee preposte alla definizione delle strategie di sicurezza cibernetica ed allo sviluppo e divulgazione della cultura sulla sicurezza delle informazioni;
- specifica esperienza in organizzazioni o istituzioni nazionali o europee impegnate in attività connesse al contrasto del cybercrime e del cyberterrorismo;
- documentata esperienza lavorativa pluriennale come formatore, docente o divulgatore culturale su tematiche tecniche, sociali e legali connesse alla sicurezza cibernetica.

Criteri di valutazione

Area di valutazione	Punteggio massimo	Suddivisione del punteggio	
Conoscenze e competenze specifiche	massimo 21 punti	sicurezza organizzativa (analisi del rischio, business impact analysis, procedure di sicurezza, etc.)	0-4
		tecniche per la conduzione di attacchi informatici sia a livello di software di base che applicativo	0-2
		misure di contrasto degli attacchi informatici a livello preventivo e di contenimento	0-2
		correlazione degli eventi e strumenti per l'individuazione degli incidenti informatici	0-2
		analisi forensica ed aspetti legali della criminalità informatica	0-3
		formazione nel settore della sicurezza informatica	0-4
		organizzazioni internazionali operanti nel settore della sicurezza cibernetica	0-4
Requisiti preferenziali	massimo 9 punti	specifica esperienza in organizzazioni o istituzioni nazionali o europee preposte alla definizione delle strategie di sicurezza cibernetica ed allo sviluppo e divulgazione della cultura sulla sicurezza delle informazioni	0-3
		specifica esperienza in organizzazioni o istituzioni nazionali o europee impegnate in attività connesse al contrasto del *cybercrime* e del *cyberterrorismo*	0-3
		documentata esperienza lavorativa pluriennale come formatore, docente o divulgatore culturale su tematiche tecniche, sociali e legali connesse alla sicurezza cibernetica	0-3

MODULO B

Profilo B1 –risorse senior (esperti) con più di 10 anni di esperienza lavorativa - per consolidare e aumentare la capacità operativa del CERT-PA per la prevenzione e reazione ad eventi cibernetici in tutto il dominio della pubblica amministrazione, per l'adeguamento alle disposizioni comunitarie e per gli adempimenti indicati dal PN per:

- continuare a garantire l'erogazione dei servizi in atto alle amministrazioni già utenti;
- accelerare le azioni per consentire lo sviluppo del CERT-PA estendendo i servizi a tutte le pubbliche amministrazioni, in linea con gli obiettivi definiti dal PN;
- implementare l'infrastruttura ed i servizi erogati, completando la definizione delle procedure operative, accrescendo la competenza del personale e creando un'opportuna rete di rapporti a livello nazionale ed internazionale.

Oggetto dell'incarico

L'incarico consisterà nel supportare il CERT-PA nello svolgimento delle attività connesse allo sviluppo ed alla conduzione dei servizi del CERT-PA, di seguito indicate:

- servizi di analisi e di indirizzamento, finalizzati a supportare la definizione dei processi di gestione della sicurezza e lo sviluppo di metodologie e di metriche valutative per il governo della sicurezza cibernetica;
- servizi proattivi, aventi come scopo la raccolta e l'elaborazione di dati significativi ai fini della sicurezza cibernetica, l'emanazione di bollettini e segnalazioni di sicurezza, l'implementazione e la gestione di basi dati informative;
- servizi reattivi, aventi come scopo la gestione degli allarmi di sicurezza ed il supporto ai processi di gestione e risoluzione degli incidenti di sicurezza che avvengono all'interno del dominio delle PA;
- servizi di formazione e comunicazione, finalizzati a promuovere la cultura della sicurezza cibernetica favorendo il grado di consapevolezza e competenza all'interno delle PA, attraverso la condivisione di informazioni relative a specifici eventi in corso ed a nuovi scenari di rischio, concernenti specifiche tematiche di sicurezza delle informazioni.

Requisiti della risorsa professionale

Requisiti minimi

- almeno 9 anni di documentata esperienza lavorativa in ambito sicurezza cibernetica;
- nell'ambito della precedente esperienza, almeno 5 anni come analista di sicurezza presso presidi di Computer Emergency Response Team o strutture comparabili a contesti ad alta complessità e dinamicità, sia in termini tecnologici che organizzativi;
- buona conoscenza della lingua inglese, parlata e scritta, con particolare riferimento al contesto di tipo tecnico-scientifico;

Conoscenze e competenze specifiche

- conoscenza ed esperienza nella configurazione delle principali piattaforme di sicurezza perimetrale, quali piattaforme Firewall, piattaforme IPS/IDS, piattaforme Antivirus centralizzate, piattaforme di network anomaly detection per la protezione da attacchi di tipo DoS, piattaforme di URL filtering;
- conoscenza delle principali tecniche utilizzate per la conduzione di attacchi informatici, sia a livello di sistema operativo che applicativo (tecniche di buffer overflow, tecniche di injection, attacchi di spoofing, attacchi al DNS, tecniche utilizzate dalle principali botnet, ecc.);
- conoscenza principali tematiche di sicurezza tecnologica in ambiente Web. In particolare: principi di sviluppo sicuro del codice e meccanismi di protezione dai principali attacchi progettati per il protocollo HTTP (attacchi tipo XSS, attacchi tipo CSRF, attacchi di SQL Injection su protocollo HTTP, ecc.);
- conoscenza delle principali tematiche di sicurezza organizzativa, quali analisi dei rischi, business impact analysis, definizione procedure di sicurezza, ecc.;
- conoscenza delle principali piattaforme di controllo accessi e autorizzazione. In particolare, piattaforme di strong authentication e sistemi di cifratura forte per sistemi client e server;
- conoscenza dei principali tool open source per l'assessment tecnologico e l'analisi delle vulnerabilità (nmap, sqlmap, nessus, hping, ecc.);
- conoscenza dei principali sistemi operativi (Windows, Unix, Linux) ed in particolare dei principi e delle tecniche di hardening per tali piattaforme;
- conoscenza delle principali tecniche utilizzate per lo sfruttamento delle vulnerabilità e la conduzione di attacchi informatici, sia a livello di sistema operativo che applicativo (tecniche di buffer overflow, tecniche di injection, attacchi di spoofing, attacchi al DNS, tecniche utilizzate dalle principali botnet, ecc.). In particolare, conoscenza delle principali metodologie di assessment tecnologico e Penetration Testing, quali OSSTMM e OWASP Testing Guide;
- conoscenza delle piattaforme di correlazione eventi per l'analisi e la classificazione degli eventi di sicurezza;
- conoscenza delle tecniche di analisi e classificazione del malware (analisi statica, reverse engineering del codice, analisi dinamica);
- linguaggio SQL e principali linguaggi di shell scripting in ambiente Windows/Unix (perl, python, shell scripting.

Requisiti preferenziali

- specifica esperienza continuativa nell'ambito del progetto CERT-PA;
- conoscenza della normativa e dell'organizzazione vigente in materia di sicurezza cibernetica in ambito nazionale ed europeo;
- specifica esperienza nell'erogazione di corsi di formazione in tematiche relative alla sicurezza cibernetica.

Criteri di valutazione

Area di valutazione	Punteggio massimo	Suddivisione del punteggio	
Conoscenze e competenze specifiche	massimo 21 punti	conoscenza ed esperienza nella configurazione delle principali piattaforme di sicurezza perimetrale, quali piattaforme Firewall, piattaforme IPS/IDS, piattaforme Antivirus centralizzate, piattaforme di network anomaly detection per la protezione da attacchi di tipo DoS, piattaforme di URL filtering	0-2
		conoscenza delle principali tecniche utilizzate per la conduzione di attacchi informatici, sia a livello di sistema operativo che applicativo (tecniche di buffer overflow, tecniche di injection, attacchi di spoofing, attacchi al DNS, tecniche utilizzate dalle principali botnet, ecc.)	0-2
		conoscenza principali tematiche di sicurezza tecnologica in ambiente Web. In particolare: principi di sviluppo sicuro del codice e meccanismi di protezione dai principali attacchi progettati per il protocollo HTTP (attacchi tipo XSS, attacchi tipo CSRF, attacchi di SQL Injection su protocollo HTTP, ecc.)	0-2
		conoscenza delle principali tematiche di sicurezza organizzativa, quali analisi dei rischi, business impact analysis, definizione procedure di sicurezza, ecc.	0-2
		conoscenza delle principali piattaforme di controllo accessi e autorizzazione. In particolare, piattaforme di strong authentication e sistemi di cifratura forte per sistemi client e server	0-2
		conoscenza dei principali tool open source per l'assessment tecnologico e l'analisi delle vulnerabilità (nmap, sqlmap, nessus, hping, ecc.)	0-2
		conoscenza dei principali sistemi operativi (Windows, Unix, Linux) ed in particolare dei principi e delle tecniche di hardening per tali piattaforme;	0-1
		conoscenza delle principali tecniche utilizzate per lo sfruttamento delle vulnerabilità e la conduzione di attacchi informatici, sia a livello di sistema operativo che applicativo (tecniche di buffer overflow, tecniche di injection, attacchi di spoofing, attacchi al DNS, tecniche utilizzate dalle principali botnet, ecc.). In particolare, conoscenza delle principali metodologie di assessment tecnologico e Penetration Testing, quali OSSTMM e OWASP Testing Guide	0-2
		conoscenza delle piattaforme di correlazione eventi per l'analisi e la classificazione degli eventi di sicurezza;	0-2
		conoscenza delle tecniche di analisi e classificazione del malware (analisi statica, reverse engineering del	0-2

		codice, analisi dinamica);	
		linguaggio SQL e principali linguaggi di shell scripting in ambiente Windows/Unix (perl, python, shell scripting.	0-2
Requisiti preferenziali	massimo 9 punti	specifica esperienza continuativa nell'ambito del progetto CERT-PA	0-4
		conoscenza della normativa e dell'organizzazione vigente in materia di sicurezza cibernetica in ambito nazionale ed europeo	0-2
		specifica esperienza nell'erogazione di corsi di formazione in tematiche relative alla sicurezza cibernetica	0-3

MODULO C

Profilo C1 –risorse Junior per consolidare e aumentare la capacità operativa del CERT-PA per la prevenzione e reazione ad eventi cibernetici in tutto il dominio della pubblica amministrazione, per l'adeguamento alle disposizioni comunitarie e per gli adempimenti indicati dal PN per:

- continuare a garantire l'erogazione dei servizi in atto alle amministrazioni già utenti;
- accelerare le azioni per consentire lo sviluppo del CERT-PA estendendo i servizi a tutte le pubbliche amministrazioni, in linea con gli obiettivi definiti dal PN;
- implementare l'infrastruttura ed i servizi erogati, completando la definizione delle procedure operative, accrescendo la competenza del personale e creando un'opportuna rete di rapporti a livello nazionale ed internazionale.

Oggetto dell'incarico

L'incarico consisterà nel supportare il CERT-PA nello svolgimento delle attività connesse allo sviluppo ed alla conduzione dei servizi del CERT-PA, di seguito indicate:

- Supporto alle attività di analisi e di indirizzamento;
- Supporto per i servizi proattivi, aventi come scopo la raccolta e l'elaborazione di dati significativi ai fini della sicurezza cibernetica, l'emanazione di bollettini e segnalazioni di sicurezza, l'implementazione e la gestione di basi dati informative;
- supporto ai processi di gestione e risoluzione degli incidenti di sicurezza che avvengono all'interno del dominio delle PA;
- servizi di formazione e comunicazione, finalizzati a promuovere la cultura della sicurezza cibernetica favorendo il grado di consapevolezza e competenza all'interno delle PA, attraverso la condivisione di informazioni relative a specifici eventi in corso ed a nuovi scenari di rischio, concernenti specifiche tematiche di sicurezza delle informazioni.

Requisiti della risorsa professionale

Requisiti minimi

- Almeno 3 anni di esperienza lavorativa di cui 2 in ambito sicurezza cibernetica;
- buona conoscenza della lingua inglese, parlata e scritta, con particolare riferimento al contesto di tipo tecnico-scientifico;

Conoscenze e competenze specifiche

- conoscenza delle principali tecniche utilizzate per la conduzione di attacchi informatici, sia a livello di sistema operativo che applicativo (tecniche di buffer overflow, tecniche di injection, attacchi di spoofing, attacchi al DNS, tecniche utilizzate dalle principali botnet, ecc.);
- conoscenza principali tematiche di sicurezza tecnologica in ambiente Web.
- conoscenza delle principali piattaforme di controllo accessi e autorizzazione.
- conoscenze di base dei principali tool open source per l'assessment tecnologico e l'analisi delle vulnerabilità (nmap, sqlmap, nessus, hping, ecc.);

- conoscenza dei principali sistemi operativi (Windows, Unix, Linux) ;
- conoscenze di base delle principali metodologie di assessment tecnologico e Penetration Testing, quali OSSTMM e OWASP Testing Guide;
- avere esperienza nell'utilizzo di almeno una piattaforma di correlazione eventi per l'analisi e la classificazione degli eventi di sicurezza;
- conoscenze di base delle principali tecniche di analisi e classificazione del malware.

Requisiti preferenziali

- specifica esperienza continuativa in ambito di sicurezza informatica;
- conoscenza della normativa e dell'organizzazione vigente in materia di sicurezza cibernetica in ambito nazionale ed europeo;

Criteri di valutazione

Area di valutazione	Punteggio massimo	Suddivisione del punteggio	
Conoscenze e competenze specifiche	massimo 21 punti	conoscenza delle principali tecniche utilizzate per la conduzione di attacchi informatici, sia a livello di sistema operativo che applicativo (tecniche di buffer overflow, tecniche di injection, attacchi di spoofing, attacchi al DNS, tecniche utilizzate dalle principali botnet, ecc.)	0-3
		conoscenza principali tematiche di sicurezza tecnologica in ambiente Web.	0-3
		conoscenza delle principali tematiche di sicurezza organizzativa, quali analisi dei rischi, business impact analysis, definizione procedure di sicurezza, ecc.	0-2
		conoscenza delle principali piattaforme di controllo accessi e autorizzazione.	0-2
		conoscenza dei principali tool open source per l'assessment tecnologico e l'analisi delle vulnerabilità (nmap, sqlmap, nessus, hping, ecc.)	0-3
		conoscenza dei principali sistemi operativi (Windows, Unix, Linux);	0-2
		conoscenza delle principali metodologie di assessment tecnologico e Penetration Testing, quali OSSTMM e OWASP Testing Guide	0-2
		conoscenza delle piattaforme di correlazione eventi per l'analisi e la classificazione degli eventi di sicurezza;	0-2
		conoscenza delle tecniche di analisi e classificazione del malware;	0-2
Requisiti preferenziali	massimo 9 punti	conoscenza della normativa e dell'organizzazione vigente in materia di sicurezza cibernetica in ambito nazionale ed europeo	0-4
		specifica esperienza continuativa in ambito di sicurezza informatica	0-5

MODULO D

Profilo D1 –risorsa Senior (Analista Programmatore) con più di 5 anni di esperienza lavorativa - per assicurare lo sviluppo dei progetti del CERT-PA in modalità continuativa al fine di poter conseguire i risultati richiesti dalle strutture Nazionali di Cyber Security.

Oggetto dell'incarico

Il CERT-PA, nel quadro degli adempimenti richiesti dai tavoli tecnici nazionali Nucleo di Sicurezza Cibernetica e Tavolo Tecnico Cyber, ha avviato:

- il progetto INFOSEC relativo a definire e sviluppare una piattaforma di aggregazione di dati attraverso la quale sarà possibile erogare servizi informativi, operativi e costituire il National Vulnerability Database Italiano;
- il progetto per la definizione degli standard per la trasmissione automatizzata degli IOC e la relativa definizione di infrastruttura operativa.

L'incarico consisterà nel:

- supporto alle attività di analisi dei dizionari relativi alla costituzione del NVD Italiano;
- supporto nello sviluppo di codice per i servizi online, aventi come scopo la raccolta e l'elaborazione di dati significativi ai fini della sicurezza cibernetica, l'implementazione e la gestione di basi dati informative;
- supporto nello sviluppo dei processi automatizzati per lo scambio dei dati.

La risorsa da acquisire può essere classificata come "Analista senior" e deve avere esperienza professionale pluriennale come Analista programmatore con particolare competenza sui seguenti temi:

- Progettazione e sviluppo di WebServices (SOAP, XML-RPC, REST)
- Uso di sistemi di controllo di versione.;
- implementazione progettuale con pattern architetturale MVC
- sviluppo in ambiente LAMP;

Requisiti della risorsa professionale

Requisiti minimi

- almeno 5 anni di documentata esperienza lavorativa come analista programmatore;
- buona conoscenza della lingua inglese, parlata e scritta, con particolare riferimento al contesto di tipo tecnico-scientifico;

Conoscenze e competenze specifiche

- Ottima conoscenza linguaggio PHP5
- Conoscenza linguaggio PHP7 (nessuna esperienza specifica richiesta)
- Esperienza nell'implementazione progettuale con pattern architetturale MVC
- Comprovata esperienza pluriennale nell'uso di 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 WebServices (SOAP, XML-RPC, REST)
- Esperienza nell'uso di sistemi di controllo di versione.

Requisiti preferenziali

- aver partecipato attivamente a progetti di sviluppo di dimensioni rappresentate da gruppi di lavoro di tre o più soggetti, con linguaggio di sviluppo prevalente in PHP5
- esperienza con Zend Framework, versione >= 1.10.
- conoscenza delle piattaforme:
  - git
  - Bazaar
- conoscenza DBMS Oracle, MySQL, Postgres
- Esperienze in progettazione di database con implementazione del Modello ER
- Esperienza nella progettazione e realizzazione di processi ETL
- Gradite esperienze nell'uso di framework e librerie CSS e JavaScript

Criteri di valutazione

Area di valutazione	Punteggio massimo	Suddivisione del punteggio	
Conoscenze e competenze specifiche	massimo 21 punti	Conoscenza linguaggio PHP5	0-3
		Conoscenza linguaggio PHP7	0-1
		Esperienza nell'implementazione progettuale con pattern architetturale MVC	0-2
		Esperienza nell'uso di framework PHP	0-3
		Conoscenza di SQL e ODBC	0-3
		Esperienza di sviluppo in ambiente LAMP	0-2
		Conoscenza tecnica e progettuale di HTML5, CSS3 e JavaScript	0-3
		Esperienza in progettazione e sviluppo di WebServices (SOAP, XML-RPC, REST)	0-3
		Esperienza nell'uso di sistemi di controllo di versione.	0-1
Requisiti preferenziali	massimo 9 punti	Esperienze relative a progetti di sviluppo di dimensioni rappresentate da gruppi di lavoro di tre o più soggetti, con linguaggio di sviluppo prevalente in PHP5	0-3
		esperienza con Zend Framework, versione >= 1.10	0-3
		conoscenza delle piattaforme: GIT - BAZAR	0-3

MODALITA' DI PARTECIPAZIONE

I candidati agli Avvisi sopra indicati dovranno inoltrare la richiesta di partecipazione predisposta secondo il fac-simile allegato (Modulo di iscrizione), con accluso curriculum in formato europeo, all'indirizzo di posta certificata dell'Agenzia per l'Italia digitale protocollo@pec.agid.gov.it entro le ore 16,00 del giorno .....2017.

In alternativa, la stessa documentazione potrà essere consegnata direttamente a:

Agenzia per l'Italia Digitale – Sezione Protocollo e archivio

Viale Liszt, 21 – 00144 Roma

La consegna può essere effettuata esclusivamente nel seguente orario: dal lunedì al giovedì dalle ore 10,00 alle ore 13,00 e dalle ore 15,00 alle ore 16,00 e il venerdì dalle ore 10,00 alle ore 13,00 e dalle ore 15,00 alle ore 15,30. La Sezione Protocollo e Archivio rilascerà apposita ricevuta.

Non saranno prese in considerazione domande di partecipazione presentate con modalità diverse, ovvero oltre il termine indicato.

Si precisa che i candidati dovranno presentare la propria candidatura per un solo profilo.

Le domande che non indicheranno per quale profilo ci si candida o che indicheranno più profili saranno escluse.

RESPONSABILE DEL PROCEDIMENTO

È responsabile del procedimento l'Ing. Mario Terranova, Area Sicurezza e CERT-PA, Agenzia per l'Italia Digitale.

mesi a tempo pieno - per le attività di sviluppo del CERT-PA, il compenso annuo da corrispondere - in base ai compensi minimi riconosciuti a figure professionali che svolgono analoghe attività - è pari a € 40.000,00, oltre oneri riflessi e IVA se dovuta;

2. la pubblicazione sul sito web dell'AgID dell'Avviso n. 4/2017 – di seguito allegato e parte integrante della presente determinazione – che definisce requisiti e caratteristiche delle risorse professionali di cui al punto 1, nonché le modalità di svolgimento della citata procedura comparativa;
3. la nomina del dott. Mario Terranova quale Responsabile Unico del Procedimento;
4. l'imputazione dell'onere della spesa come segue:

MODULO A

Profilo A1: per una risorsa, un importo complessivo di € 200.250,00 oneri e imposte a carico dell'Amministrazione inclusi, a valere sui fondi della voce progettuale "CERT PA" Ob.fu. 1.02.13.02.

MODULO B

Profilo B1: per tre risorse, un importo complessivo di € 696.870,00 oneri e imposte a carico dell'Amministrazione inclusi, a valere sui fondi della voce progettuale "CERT PA" Ob.fu. 1.02.13.02.

MODULO C

Profilo C1: per tre risorse, un importo complessivo di € 360.450,00 oneri e imposte a carico dell'Amministrazione inclusi, a valere sui fondi della voce progettuale "CERT PA" Ob.fu. 1.02.13.02.

MODULO D

Profilo D1: per una risorsa, un importo complessivo di € 160.200,00 oneri e imposte a carico dell'Amministrazione inclusi, a valere sui fondi della voce progettuale "CERT PA" Ob.fu. 1.02.13.02.

5. la disciplina dei suddetti incarichi mediante la stipula di appositi contratti di collaborazione coordinata e continuativa, in esito all'approvazione dei piani di programmazione, anche finanziaria, di AgID da parte delle amministrazioni vigilanti, secondo la normativa vigente.

Roma, - 4 APR. 2017

Antonio Samaritani