CAPITOLATO

Adeguamento infrastruttura Firewall Checkpoint con manutenzione triennale (2024-2026) e aggiornamento di n. 90 licenze per autenticazione a 2 fattori (RSA) e relativo servizio di manutenzione annuale

CPV: 72260000-5

CODICE NUTS: ITH53

1) Oggetto del servizio

Il sistema informativo della Provincia di Reggio Emilia da diversi anni è protetto da un'infrastruttura firewall fisica, installata presso la propria sala macchine, composta da n.2 Appliance Check Point 5800 con bundle Next Generation Extraction Appliance (NGTX): SG5800NGTX e SG5800NGTX-HA e n.1 Virtual Appliance Security Management Server Check Point.
Il sistema, **associato all'account ID Check Point: 7963692,** opera utilizzando i servizi garantiti dalle seguenti licenze:

- n.1 CPEBP-NGTX Enterprise Based Protection - Next Generation Threat Extraction Package Including IPS APCL URLF AV ABOT ASPM TX and TE b;
- n.1 CPSB-EVS-5-1Y SmartEvent and SmartReporter blade for 5 gateways (Smart-1 & open server);
- n.1 CPCES-CO-STANDARDPRO Standard Pro Collaborative Enterprise Support;
- n.1 CPCES-CO-STANDARDPRO-ADD Standard Pro Collaborative Enterprise Support.

Il Firewall fisico garantisce i seguenti servizi:

- l'accesso alla rete interna e alla navigazione Internet a circa 400 postazioni utenti l'accesso a banche dati raggiungibili mediante internet ed SPC (Servizio Pubblico di Connettività) come l'INSP, Agenzia delle Entrate, ANAC, Prefettura-BDNA, Agid, Sitar, Sistema Informativo Lavoro e Portale lavoro della Regione Emilia Romagna, sistema regionale di gestione delle autorizzazioni ai trasporti eccezionali e della formazione professionale, centrali di acquisto Mepa ed Intercenter, ACI e Motorizzazione civile;
- l'accesso riservato dalla rete SisTER dei Comuni ai server che erogano il back office di SUAP, Rilfedeur, Moka e le elezioni on line;
- servizio di firewall alla rete SisTER dei Comuni, per proteggere la rete interna e le pubblicazioni su internet per i comuni che non sono dotati di apparati di protezione o non hanno un'uscita Internet dedicata ed utilizzano la rete SisTER come connettività principale;
- servizio di firewall IPS (Intrusion Prevent System) per la navigazione internet dell'Ente e per tredici comuni;
- accesso protetto da Internet verso i server della DMZ, come per la protezione del servizio di posta elettronica mediante il servizio di relay provinciale per dieci comuni.

Considerato che:

- nel corso del 2023 l'infrastruttura server Vmware dell'Ente è stata trasferita presso i DatacentER di Lepida Scpa e per garantire maggiore protezione dei server e migliorare le performance di accesso ad internet è necessario dotarsi anche in

DatacentER di un dispositivo di protezione firewall e di un accesso ad Internet dedicato ai server;
- gli unici server rimasti nella sala macchine dell'Ente sono i server della DMZ, che per essere trasferiti in DatacentER devono necessariamente essere separati dal resto dell'infrastruttura attraverso un dispositivo di protezione firewall;
- la raggiungibilità del DatacentER è garantita da un collegamento punto-punto consegnato sul Pals provinciale, sul quale sono consegnati anche altri servizi quali: connettività internet, rete SistER dei Comuni, libreria backup e tutti questi servizi devono essere separati dalla rete client e dalla rete server DatacentER mediante dispositivi di protezione firewall;
- i firewall fisici attuali sono ormai fuori supporto e i relativi servizi sono in scadenza il 9 febbraio 2024, devono pertanto essere rinnovati entro tale data.

Per le motivazioni sopra descritte si ritiene necessario migrare l'attuale infrastruttura di firewall fisico verso una soluzione virtuale, installata presso l'infrastruttura VMware dell'Ente in DatacentER, mantenendo lo stesso software CheckPoint e la stessa management server di gestione, consentendo così la migrazione delle attuali policy di sicurezza in modo automatico e senza disservizi, oltre a garantire autonomia nella gestione da parte del personale interno all'Ente, già opportunamente formato su tale sistema.
La soluzione virtuale in DatacentER permetterà quindi la protezione dell'attuale infrastruttura server, la migrazione dei server della DMZ, la consegna in DatacentER di tutti i servizi ora erogati sul Pals provinciale, la connettività Internet della Rete SisTER dei Comuni e del backup, migliorando sia gli aspetti di sicurezza che di performance di tutte le reti.

Si richiede pertanto una soluzione completamente virtuale, comprensiva di manutenzione triennale dalla data del collaudo, con le seguenti componenti software e licenze CheckPoint :
- n.2 CPSG-VSEC-VEN-BUN-NGTX-3Y: per attivare l'istanza virtuale clusterizzata nella farm VMware dell'Ente, così da garantire i medesimi servizi attualmente erogati dagli appliance fisici, per 3 anni;
- n.2 CPSB-MOB-50: per garantire almeno 50 utenti contemporanei collegati in VPN, da accesso mobile per il cluster;
- n.1 CPSM-NGSM5: per rinnovare l'attuale licenza della *Management server* per 5 gateway (in scadenza il 9 febbraio 2024) portandola alla medesima scadenza triennale di tutta l'infrastruttura firewall;
- CPCES-CO-PREMIUM: per attivare il supporto Premium Collaborative, come presente nell'attuale infrastruttura.

Dovranno inoltre essere previste almeno le seguenti attività:
- la creazione di n.2 virtual machine firewall sull'infrastruttura VMware in DatacentER in stretta collaborazione con il personale dell'Ente e il personale di Lepida;
- la migrazione delle configurazioni da firewall fisico on-premise a virtuale in DatacentER;
- la migrazione della linea internet e della rete SisTER dalla sala macchine locale al DatacentER;
- l'attivazione del cluster virtuale in DatacentER;
- test e collaudo nuova infrastruttura con produzione di documentazione ad hoc;
- la dismissione cluster on-premise.

Si precisa che le attività di migrazione potranno anche essere svolte, gradualmente, per successivi step, potendo utilizzare in DatacentER la connettività Internet dedicata e le classi di indirizzi IP pubblici riservati alla Provincia di Reggio Emilia.

Considerando inoltre che già da anni, per aumentare il livello di sicurezza e protezione negli accessi in VPN, è stata attivata l'autenticazione a 2 fattori mediante il software RSA che consente un alto grado di integrazione con la VPN del software Checkpoint e che le attuali 90 licenze sono in scadenza il 12 gennaio 2024, si richiede:

- di procedere al rinnovo annuale della manutenzione delle licenze *ID Plus E2 perU 1Mo*
- di integrare questa soluzione anche sulla nuova infrastruttura virtuale oltre che sull'attuale infrastruttura fisica.

2) Tempi massimi per il rinnovo

- Il nuovo firewall virtuale, comprensivo delle componenti di dettaglio sopra indicate, dovrà essere attivato a partire dai primi giorni di gennaio 2024 e collaudato entro il 9 febbraio 2024, così da completare le attività prima della scadenza dell'attuale sistema e garantirne la manutenzione triennale da tale data.
- Le licenze RSA (*ID Plus E2 perU 1Mo)* dovranno invece essere rinnovate entro la scadenza del 12/01/2024, pertanto il rinnovo annuale, dovrà avvenire entro e non oltre tale data.

3) Presentazione dell'offerta

Il contratto verrà perfezionato sul Mercato elettronico della Pubblica amministrazione, mediante trattativa diretta, con tempistiche che possano garantire il rinnovo in oggetto nei termini previsti.
La presentazione dell'offerta da parte dell'Impresa implica l'accettazione incondizionata di tutte le condizioni e norme contenute nel presente Documento che sarà parte integrante del contratto che verrà stipulato con l'impresa affidataria.

4) Affidamento e Stipula del Contratto

Il Responsabile Unico del Progetto, ing. Ilenia Incerti, preso atto dei preventivi pervenuti entro il termine suddetto, darà seguito alla trattativa diretta e alla successiva adozione dell'atto necessario per l'affidamento del servizio.

Si precisa che la Provincia si riserva il diritto:

- di non procedere all'indizione della trattativa diretta nel caso in cui nessuno dei preventivi presentati venga ritenuto conveniente o idoneo;
- di procedere all'affidamento anche in presenza di un solo preventivo valido, purché ritenuto congruo;
- di sospendere, di revocare, re-indire e/o non aggiudicare l'affidamento motivatamente.

Il Contratto si intenderà validamente perfezionato al momento in cui il Documento di stipula firmato digitalmente verrà caricato a Sistema (art. 52 delle Regole del Sistema di e-Procurement).

5) Garanzia definitiva

Contestualmente alla presentazione dell'offerta, in risposta alla trattativa diretta sul Mercato elettronico della Pubblica amministrazione, l'affidatario dovrà presentare la garanzia definitiva ai sensi dell'art. 53, comma 4 del D.Lgs. 36/2023: l'impresa pertanto è

tenuta, a costituire una garanzia, pari al 5% dell'importo contrattuale, sotto forma di fidejussione, costituita con le modalità di cui all'art. 117 del Codice.

6) Fattura e Pagamento
La fatturazione dovrà essere separata relativamente ai due servizi:

a) la fattura relativa al nuovo firewall virtuale potrà essere emessa a seguito di approvazione da parte dell'amministrazione del documento di collaudo;
b) la fattura per il rinnovo della manutenzione delle licenze RSA potrà avvenire in seguito alla comunicazione di affidamento del servizio, così da consentirne il rinnovo nelle tempistiche previste.

Si precisa che su ogni fattura deve essere operata la ritenuta dello 0,5% ai sensi dell'art. 11, comma 6 del D. Lgs. n. 36/2023; tali ritenute saranno svincolate solo in fase di liquidazione finale, in seguito all'approvazione, da parte del committente, della verifica di conformità, e previa acquisizione del documento unico di regolarità contributiva.

Le fatture dovranno essere intestate a: Provincia di Reggio Emilia - Corso Garibaldi, 59 - 42121 Reggio Emilia ed inviarla tramite il sistema di fatturazione elettronica, come da Decreto Ministeriale 3 aprile 2013 n. 55, utilizzando il codice ufficio: UF1I87.

Oltre al "Codice Univoco Ufficio", che deve essere inserito obbligatoriamente nell'elemento "Codice Destinatario" del tracciato della fattura elettronica, si devono altresì indicare nella fattura i seguenti dati:

- CIG, obbligatoriamente inserito nel campo dedicato
- numero/i del buono d'ordine;
- il codice IBAN completo su cui effettuare il pagamento;
- la scadenza della fattura.

In mancanza di tali elementi, la fattura verrà rifiutata dal sistema e il pagamento sarà effettuato a 30 giorni dal ricevimento della fattura.
Inoltre, per ogni pagamento, sarà necessaria l'acquisizione del DURC (Documento Unico di Regolarità Contributiva).
Ai sensi della L.136/2010, ai fini della tracciabilità dei flussi finanziari, nella documentazione da presentare a seguito dell'affidamento, si dovrà indicare, uno o più conti correnti bancari o postali, accesi presso banche o presso la società Poste italiane Spa, dedicati, anche non in via esclusiva, a tutta la gestione contrattuale. Tutti i movimenti finanziari relativi al servizio oggetto del contratto dovranno essere registrati sul conto corrente dedicato e dovranno essere effettuati esclusivamente tramite lo strumento del bonifico bancario o postale, ovvero con altri strumenti di pagamento idonei a consentire la piena tracciabilità delle operazioni.

Gli strumenti di pagamento devono riportare, in relazione a ciascuna transazione posta in essere per il presente contratto, il Codice Identificato della Gara (CIG) che sarà comunicato nella successiva Trattativa Diretta.
E' fatto obbligo di provvedere a comunicare ogni modifica relativa alle generalità e al codice fiscale delle persone delegate ad operare sul suddetto c/c dedicato. A pena di nullità assoluta, l'impresa, assume gli obblighi di tracciabilità dei flussi finanziari di cui alla legge sopra citata.
L'assunzione degli obblighi di tracciabilità dei flussi finanziari deve essere riportata in tutti i contratti sottoscritti a qualsiasi titolo interessate al servizio di cui al presente contratto e la Provincia può verificare in ogni momento tale adempimento.

Il soggetto che ha notizia dell'inadempimento della propria controparte agli obblighi di tracciabilità finanziaria di cui alla Legge 136/2010, ne deve dare immediata comunicazione alla Provincia di Reggio Emilia e alla Prefettura-Ufficio territoriale del Governo di Reggio Emilia.

6) Penali e Risoluzione.

La stazione appaltante, tenuto conto di quanto indicato dall'art. 126 del D.lgs. 36/2023, applicherà una penale il cui valore sarà pari allo 0,3 per mille dell'ammontare netto contrattuale, fino ad un massimo del 10%, per ogni giorno di ritardo rispetto alle scadenze indicate.

In caso di inottemperanza agli obblighi derivanti dal presente Capitolato fermo restando l'applicazione delle penali previste, la Provincia può inoltrare lettera di diffida all'impresa; qualora queste non provvedano a fornire la prestazione dovuta, entro sette giorni dal ricevimento dalla comunicazione, il committente ha facoltà di risolvere "ipso-facto et jure" il contratto, mediante semplice dichiarazione stragiudiziale intimata (ex Art. 1456 c.c.) a mezzo PEC; in tal caso, l'impresa dovrà corrispondere alla Provincia il 10% del valore del contratto, quale indennizzo per i danni subiti; saranno inoltre annullati i pagamenti non ancora eseguiti.

La Provincia può risolvere altresì il contratto nei casi indicati all'Art. 122 del Codice dei contratti e recedere dallo stesso ai sensi dell'Art. 123 del Codice.

L'impresa non può recedere dal contratto.

7) Sicurezza sul lavoro e costo del lavoro

Trattandosi di affidamento di attività principalmente di natura intellettuale, non sono previsti rischi da interferenza né oneri per la sicurezza.

Per l'esecuzione del servizio, l'Impresa affidataria si obbliga ad avvalersi di personale di adeguata professionalità e ad ottemperare a tutti gli obblighi verso i propri dipendenti occupati nelle attività contrattuali e ad applicare le condizioni normative e retributive non inferiori a quelle dei contratti collettivi ed integrativi di lavoro applicabili, alla data di stipula del Contratto, come precisato all'articolo 4 delle "Condizioni generali di contratto relative alla prestazione di servizi" redatte da Consip S.p.A.

8) Obbligo alla riservatezza

- Il Fornitore ha l'obbligo di mantenere riservati i dati e le informazioni, ivi comprese quelle che transitano per le apparecchiature di elaborazione dati, di cui venga in possesso e comunque a conoscenza, anche tramite l'esecuzione del contratto, di non divulgarli in alcun modo e in qualsiasi forma, di non farne oggetto di utilizzazione a qualsiasi titolo per scopi diversi da quelli strettamente necessari all'esecuzione del contratto e di non farne oggetto di comunicazione o trasmissione senza l'espressa autorizzazione dell'Amministrazione.
- L'obbligo di cui al precedente comma sussiste, altresì, relativamente a tutto il materiale originario o predisposto in esecuzione del contratto.
- L'obbligo di cui ai commi 1 e 2 non concerne i dati che siano o divengano di pubblico dominio.
- Il Fornitore è responsabile per l'esatta osservanza da parte dei propri dipendenti, consulenti e collaboratori, nonché di subappaltatori e dei dipendenti, consulenti e collaboratori di questi ultimi, degli obblighi di segretezza di cui ai punti 1, 2 e 3 e risponde nei confronti dell'Amministrazione per eventuali violazioni dell'obbligo di riservatezza commesse dai suddetti soggetti.

- Il Fornitore può utilizzare servizi di cloud pubblici ove memorizzare i dati e le informazioni trattate nell'espletamento dell'incarico affidato, solo previa autorizzazione dell'Ente.
- In caso di inosservanza degli obblighi descritti nei punti da 1 a 5, l'Amministrazione ha facoltà di dichiarare risolto di diritto il contratto, fermo restando che il Fornitore sarà tenuto a risarcire tutti i danni che ne dovessero derivare.
- Il Fornitore potrà citare i termini essenziali del contratto nei casi in cui fosse condizione necessaria per la partecipazione del Fornitore stesso a gare e appalti, previa comunicazione all'Amministrazione delle modalità e dei contenuti di detta citazione.
- Sarà possibile ogni operazione di auditing da parte dell'Amministrazione attinente le procedure adottate dal Contraente in materia di riservatezza e degli altri obblighi assunti dal presente contratto.
- Il Fornitore non potrà conservare copia di dati dell'Amministrazione, né alcuna documentazione inerente ad essi dopo la scadenza del Contratto e dovrà, su richiesta, ritrasmetterli all'Amministrazione.
- Il Fornitore, successivamente all'aggiudicazione, verrà designato Responsabile del trattamento di dati personali ai sensi dell'art. 28 del GDPR (Regolamento Privacy UE 2016/679).

9) Obblighi derivanti dal Codice di comportamento dei dipendenti della Provincia di Reggio Emilia.

L'impresa con riferimento alle prestazioni oggetto del presente contratto, si impegna ad osservare e far osservare ai propri collaboratori a qualsiasi titolo, per quanto compatibili con il ruolo e l'attività volta, gli obblighi di condotta previsti dal codice di comportamento dei dipendenti della Provincia di Reggio Emilia, approvato con decreto presidenziale n. 116/2021. A tal fine si dà atto che l'amministrazione ha informato il contraente che sul sito dell'Amministrazione Provinciale è pubblicato il codice di comportamento.

Il professionista si impegna a rendere edotti dei contenuti dello stesso i propri collaboratori a qualsiasi titolo e a fornire prova dell'avvenuta comunicazione. La violazione da parte dell'impresa degli obblighi di cui al codice di comportamento dei dipendenti della Provincia di Reggio Emilia costituisce motivo di risoluzione di diritto del contratto, ai sensi dell'art. 1456 del Codice Civile. L'amministrazione verificata l'eventuale violazione, contesta per iscritto il fatto assegnando un termine non superiore a dieci giorni per la presentazione di eventuali controdeduzioni. Ove queste non fossero presentate o risultassero non accoglibili, procederà alla risoluzione del contratto, fatto salvo il risarcimento dei danni.

10) Divergenze

La competenza a conoscere delle controversie derivanti dall'esecuzione del contratto spetta, ai sensi dell'art. 20 del codice di procedura civile, al giudice del luogo dove il contratto è stato stipulato. E' escluso, pertanto, il deferimento al giudizio arbitrale delle eventuali controversie contrattuali.

11) Disposizioni finali

Il servizio, di cui al presente disciplinare, si configura a tutti gli effetti come rapporto stipulato e regolato, per quanto non disciplinato dal presente atto, dagli artt. 2222 e seguenti del Codice Civile.

Il Responsabile Unico del Progetto, ai sensi dell'art. 15 del D.Lgs. n. 36/2023, è l'ing. Ilenia Incerti, Responsabile dell'U.O. Sistemi Informativi del Servizio Bilancio.

12) Norme sull'anticorruzione

L’affidatario, a decorrere dall’entrata in vigore del comma 16 ter dell’art. 53 del D.Lgs. n. 165/2001 (28.11.2012), non dovrà aver affidato incarichi o lavori retribuiti, di natura autonoma o subordinata, a ex dipendenti delle pubbliche amministrazioni di cui all’art.1, comma 2, del medesimo decreto, entro tre anni dalla loro cessazione dal servizio, se questi avevano esercitato, nei suoi confronti, poteri autoritativi o negoziali in nome e per conto dell’Amministrazione di appartenenza. Ai sensi degli artt. 94, 95, 97 e 98 del Dlgs. 36/2023 è fatto obbligo ai partecipanti alla richiesta di preventivi di comunicare ogni situazione di conflitto di interesse, anche potenziale, che dovesse manifestarsi nel corso della procedura.

Per ogni ulteriore informazione di carattere tecnico è possibile rivolgersi a Daniela Galeazzi (tel. 0522 444161; d.galeazzi@provincia.re.it) o Ilenia Incerti (tel. 0522 444137; i.incerti@provincia.re.it).

Reggio Emilia, 29/11/2023

La Responsabile
U.O. Sistemi informativi
(f.to Ing. Ilenia Incerti)

Documento sottoscritto con modalità digitale ai sensi dell'art. 21 del d.lgs. 82/2005.