PROVINCIA
DI REGGIO EMILIA

DETERMINAZIONE DIRIGENZIALE
N. 795 DEL 06/12/2016

OGGETTO

ACQUISTO ED ATTIVAZIONE DI UN SISTEMA DI SICUREZZA PER LA RETE PROVINCIALE

Servizio Bilancio

IL DIRIGENTE

Premesso che con decreto del Presidente n. 131 del 04/08/2016, successivamente modificato con decreti del Presidente n. 172 del 05/10/2016 e n. 243 del 29/11/2016, è stato approvato il Piano Esecutivo di Gestione per l'esercizio 2016 ed è stata affidata ai dirigenti dei centri di responsabilità l'adozione di tutti i provvedimenti di contenuto gestionale necessari per assicurare il perseguimento degli obiettivi assegnati;

Visto il Decreto del Presidente n. 45 del 31/03/2015 con il quale conferisce il potere di firma del dirigente del Servizio Bilancio;

dato atto che l'U.O. Sistemi Informativi del Servizio Bilancio ha tra le proprie funzioni quella di garantire la sicurezza della rete provinciale;

considerato che:
- con deliberazione della Giunta Provinciale n. 133 del 2.5.2000, è stato approvato il progetto della rete telematica territoriale della Provincia di Reggio Emilia, che ha consentito di realizzare una rete di trasmissione dati 'protetta' tra i comuni e la Provincia di Reggio Emilia consentendo l'interoperabilità e lo scambio di dati in formato digitale tra le pubbliche amministrazioni del territorio provinciale; tale rete si è evoluta negli anni ed è stata integrata nella rete Lepida regionale;
- con la creazione della rete telematica è stato costruito un modello topologico che ha visto la Provincia come snodo di collegamento della rete dei comuni verso il mondo Internet e la rete regionale e questo ha richiesto che nella realizzazione di tale rete fossero acquisiti e configurati adeguati apparati di protezione per la sicurezza della rete e dei dati degli enti coinvolti;
- in particolare è stato implementato uno strumento di firewall che ha garantito in questi anni la protezione della rete dalle minacce alla sicurezza: vista la criticità del servizio era stato individuato un prodotto leader di mercato che offrisse tutte le migliori garanzie di sicurezza e stabilità;
- negli anni il sistema è stato adeguato alle evoluzioni tecnologiche, alle mutate caratteristiche della rete telematica regionale e al costante aumento delle minacce informatiche; in particolare con determinazione n. 853/2008 è stato acquisito un sistema firewall costituito da due apparati di rete Nokia, con l'aggiornamento del software Checkpoint all'ultima versione, associato ad un diverso sistema di controllo della navigazione;

dato atto che:
- al 31 dicembre 2016 gli apparati firewall non verranno più supportati dalla casa madre a livello di manutenzione hardware e software; si rende necessario sostituire tale sistema, perché in caso di guasto e/o malfunzionamento non sarebbe garantito in alcun modo il suo ripristino;
- il sistema di sicurezza informatica dell'Ente è negli anni sempre più importante e cruciale per via della crescente informatizzazione dei servizi che vede una maggiore esposizione alla rete internet per l'accesso alle banche dati esterne e della parallela diffusione e specializzazione delle minacce alla sicurezza, non si può pertanto rischiare

il malfunzionamento del principale strumento utilizzato per la sicurezza perimetrale della rete;

considerato inoltre che:
- tale infrastruttura deve assicurare la sicurezza della rete locale della Provincia, l'accesso ad applicazioni erogate dalla Provincia ai comuni del territorio e la protezione della rete dei comuni che sono protetti in parte dei loro servizi dagli apparati di sicurezza della Provincia, come meglio dettagliato nel progetto allegato, si ritiene indispensabile acquisire una infrastruttura diffusa e leader di mercato, che presenti tutte le migliori caratteristiche funzionali e che garantisca, anche rispetto alle valutazioni comparative effettuate da organismi internazionali, le migliori prestazioni e adeguamenti alla continua mutazione dei rischi informatici. La diffusione dello strumento potrà dare garanzia che su di esso possano operare una molteplicità di imprese con sedi operative tali da poter intervenire presso la sede della Provincia tempestivamente in caso di grave guasto;
- sono stati analizzati diversi prodotti di mercato ed oltre alla possibilità di aggiornare la soluzione esistente con appliance e tecnologia Check Point, si è individuata la soluzione “denominata PA 3020” in HA di Palo Alto Network come quella più corrispondente alle caratteristiche e funzionalità richieste, il fornitore dovrà quindi proporre un progetto di migrazione dall'attuale soluzione ad una piattaforma tra quelle indicate o equivalente a livello di prestazioni, funzionalità e caratteristiche tecniche, con tutti i servizi attivi richiesti per un anno;
- il sistema che si andrà ad implementare dovrà essere gestito da personale interno all'Ente che ha competenza sull'attuale sistema in uso, pertanto la fornitura dovrà prevedere 'attività di training on the job' durante le attività di installazione, configurazione e migrazione delle configurazioni dell'attuale sistema firewall, così da acquisire competenze da gestire il nuovo sistema che si va ad implementare;

dato atto che:
- al momento presente, nell'ambito del programma "Acquisti in Rete della PA", attuato dal Ministero dell’Economia e delle Finanze attraverso la gestione di Consip S.p.A, a norma dell'articolo 26 della legge 23 dicembre 1999, n. 488 "Legge finanziaria 2000", relativamente alla categoria “Telecomunicazioni, elettronica e servizi accessori ”, è attiva la convenzione “Reti Locali 5“ che propone dispositivi di sicurezza, ma tali apparati e servizi software non si ritengono adeguati, relativamente a funzionalità, diffusione sul mercato, presenza di aziende sul territorio italiano con esperienza nella loro manutenzione, configurazione e migrazione da precedenti sistemi di sicurezza così come meglio dettagliato nel progetto allegato, inoltre in data 16 Novembre 2016 è stato comunicato sulla piattaforma Consip che tale convenzione ha esaurito il massimale del Lotto2, comprensivo di estensioni 6° e 7° quinto;
- al momento presso la Centrale di committenza regionale Intercent-ER è presente la convenzione 'Servizi convergenti ed integrati di trasmissione dati e voce su reti fisse e mobili' che propone a listino, tra i servizi aggiuntivi e non previsti inizialmente, alcune licenze di sistemi di protezione dati, ma si ritiene che non siano adeguati relativamente alle funzionalità e ai costi, così come indicati su tali listini;

considerato quindi che:
- per l’individuazione dell'operatore economico si intende procedere, a norma dell’art. 36, comma 2, lett. b del D.Lgs.vo n. 50/2016, con l'attivazione di una richiesta di offerta

(RdO), nell'ambito del Mercato Elettronico della Pubblica Amministrazione (MePA), all'interno del programma "Acquisti in Rete della PA" per quindici giorni, con aggiudicazione sulla base del criterio dell'offerta economicamente più vantaggiosa, individuata sulla base del migliore rapporto qualità/prezzo a norma dell'art. 95 del decreto precitato;
- le ditte invitate a partecipare alla suddetta RdO saranno selezionate sulla base di comprovata esperienza professionale in ambito di sicurezza informatica, certificati rispetto ai prodotti individuati come leader di mercato e che possono garantire un presidio territoriale tale da garantire interventi tempestivi anche in loco;
- il prodotto offerto dovrà possedere almeno le caratteristiche minime specificate nel capitolato, ufficialmente documentate dalla casa madre. Inoltre essa dovrà documentare di essere un partner autorizzato del prodotto offerto e possedere adeguate competenze ed esperienze pregresse relative a progetti analoghi di implementazione dell'infrastruttura e di migrazione delle configurazioni attualmente presenti sul nostro sistema firewall;

dato atto inoltre che:
- con riferimento alla Legge n. 123 del 03/08/2007 e alla successiva determinazione n. 3 del 05/03/2008 sulla "Sicurezza nell'esecuzione degli appalti relativi a servizi e forniture. Predisposizione del documento unico di valutazione dei rischi (DUVRI) e determinazione dei costi della sicurezza" (emanata dall'AVCP - AUTORITA' per la Vigilanza sui contratti pubblici di lavori, servizi e forniture), si dichiara che la fornitura in oggetto non prevede rischi da "interferenze" in merito alla sicurezza, in quanto trattasi di mera fornitura, e pertanto non è necessaria la redazione del documento unico di valutazione dei rischi (DUVRI);
- si provvederà ad ottemperare agli obblighi di tracciabilità dei flussi finanziari previsti dalla legge 13 agosto 2010, n. 136 "Piano straordinario contro le mafie, nonché delega al governo in materia di normativa antimafia" e successive modificazioni e integrazioni;

atteso che:
- l'acquisto dell'impianto di sicurezza sarà effettuato nelle forme, nei modi ed alle condizioni di cui al Capitolato, allegato al presente atto, quale parte integrante e sostanziale;
- la base d'asta per tale fornitura è pari a netti € 39.900,00;
- la spesa complessiva di € 39.900,00, IVA esclusa, pari a complessivi € 48.678,00, IVA compresa trova imputazione:
  - ✓ per € 14.132,42 alla Missione 01, Programma 08, codice del Piano dei Conti Integrato 2.02.01.07.999 ed al corrispondente capitolo 4613, Articolo 1, "Acquisto attrezzature e procedure informatiche – Hardware", finanziato con mutuo, del PEG 2016, con esigibilità anno 2016;
  - ✓ per € 34.545,58, alla Missione 01, Programma 08, codice del Piano dei Conti Integrato 2.02.01.07.999 ed al corrispondente capitolo 4613, Articolo 1, "Acquisto attrezzature e procedure informatiche – Hardware", finanziato con avanzo vincolato, del PEG 2016, con esigibilità anno 2016;
- l'attività è prevista nell'obiettivo gestionale R02G5OG2 "Attività gestionale dei sistemi informativi" del PEG 2016;
- il Codice Identificativo Gara (C.I.G.), e il Codice Unico del Progetto (CUP), ai sensi dell'art. 3, comma 5, della legge 13 agosto 2010, n. 136 "Piano straordinario contro le mafie, nonché delega al Governo in materia di normativa antimafia" (di seguito L.

136/2010) e successive modificazioni e integrazioni, per la gestione del contratto sono i seguenti:
  - ✓ C.I.G. Z211C54496, C.U.P. C89G16000750003;
- il Responsabile Unico del Procedimento, ai sensi dell'art. 31 del D.Lgs.vo n. 50/2016, nonché direttore dell'esecuzione del Contratto, ai sensi dell'art. 101 del decreto stesso, è la Dott.ssa Claudia Del Rio, Dirigente del Servizio Bilancio;

Accertata, ai sensi dell'art. 147-bis del D.Lgs. 267/2000, la regolarità amministrativa del presente atto e acquisito il parere del Segretario Generale ai sensi del comma 517 dell'art. 1 della l. 208/2015;

DETERMINA

- di procedere con l'acquisto di un nuovo sistema di sicurezza per la rete provinciale;

- di indire, per tale fornitura, una Richiesta di Offerta (RdO) tramite il Mercato Elettronico della Pubblica Amministrazione (MePA) con aggiudicazione ai sensi dell'art. 95, comma 2, del D. Lgs. 50/2016 secondo il criterio dell'offerta economicamente più vantaggiosa sulla base del migliore rapporto qualità/prezzo;

- di approvare il relativo Capitolato, allegato alla presente determinazione dirigenziale, quale parte integrante e sostanziale della stessa;

- di dare atto che:
  - ✓ la base d'asta per tale fornitura è pari a netti € 39.900,00;
  - ✓ la spesa complessiva di € 39.900,00, IVA esclusa, pari a complessivi € 48.678,00, IVA compresa trova imputazione:
    - per € 14.132,42 alla Missione 01, Programma 08, codice del Piano dei Conti Integrato 2.02.01.07.999 ed al corrispondente capitolo 4613, Articolo 1, "Acquisto attrezzature e procedure informatiche – Hardware", finanziato con mutuo, del PEG 2016, con esigibilità anno 2016;
    - per € 34.545,58, alla Missione 01, Programma 08, codice del Piano dei Conti Integrato 2.02.01.07.999 ed al corrispondente capitolo 4613, Articolo 1, "Acquisto attrezzature e procedure informatiche – Hardware", finanziato con avanzo vincolato, del PEG 2016, con esigibilità anno 2016
  - ✓ l'attività è prevista nell'obiettivo gestionale R02G5OG2 "Attività gestionale dei sistemi informativi" del PEG 2016;
  - ✓ il Codice Identificativo Gara (C.I.G.), e il Codice Unico del Progetto (CUP), ai sensi dell'art. 3, comma 5, della legge 13 agosto 2010, n. 136 "Piano straordinario contro le mafie, nonché delega al Governo in materia di normativa antimafia" (di seguito L. 136/2010) e successive modificazioni e integrazioni, per la gestione del contratto sono i seguenti:
    C.I.G. Z211C54496; C.U.P. C89G16000750003;

- di dichiarare che il il Responsabile Unico del Procedimento, ai sensi dell'art. 31 del D.Lgs.vo n. 50/2016, nonché direttore dell'esecuzione del Contratto, ai sensi dell'art. 101 del decreto stesso, è la Dott.ssa Claudia Del Rio, Dirigente del Servizio Bilancio;

- di dare infine atto che, ai sensi e per gli effetti di cui all'art. 192 del D. Lgs. 18 Agosto 2000, n. 267:
  - ✓ il fine e l'oggetto del contratto che si andrà a stipulare, sono descritti nella premessa del presente atto e consistono nel dotare l'Ente di un nuovo sistema di sicurezza per la rete provinciale;
  - ✓ le clausole ritenute essenziali sono quelle inerenti al prezzo, alla tempistica e alle modalità di esecuzione del servizio, alle modalità di fatturazione e pagamento, le penali, clausole tutte contenute e più dettagliatamente descritte nel Capitolato allegato al presente atto;
  - ✓ il servizio viene aggiudicato a norma dell'art. 36, comma 2, lett. B, del D.Lgs.vo n. 50/2016, a seguito di Richiesta di Offerta pubblicata sul Mercato Elettronico della Pubblica Amministrazione (MEPA) realizzato da Consip S.p.A., ai sensi dell'art. 95, comma 2 del D. LGS 50/2016;
  - ✓ la verifica dei requisiti fissati dall'articolo 80 del D.Lgs.vo n. 50/2016 potrà essere svolta con metodo tradizionale;
  - ✓ il contratto verrà stipulato secondo le modalità attive sulla piattaforma del Mercato Elettronico della P.A di Consip; parte integrante del contratto sarà il Capitolato allegato alla RdO;
  - ✓ il contratto sarà sottoposto a condizione risolutiva nel caso di disponibilità di convenzione Consip o della Centrale di committenza regionale (Intercent-ER), adeguate alle esigenze espresse sul capitolato. In alternativa, a norma di quanto disposto dal comma 7 dell'articolo 9 del D.L. 66/2014, l'Impresa aggiudicataria dovrà adeguare i prezzi proposti in sede di gara, al parametro di *benchmark* di Consip o di Intercent-ER, se più favorevole;
  - ✓ nel contratto che verrà stipulato verrà precisato che il fornitore si impegna ad osservare e a fare osservare ai propri collaboratori gli obblighi di condotta previsti dal Codice di comportamento dei dipendenti della Provincia di Reggio Emilia, approvato con delibera n. 23 del 11/02/2014 reperibile sul sito web della Provincia all'indirizzo: http://www.provincia.re.it/page.aspIDCategoria=703&IDSezione=26591&ID=529565
  - ✓ in ragione delle recenti disposizioni normative, in materia di riordino delle Province il contratto riporterà fra le proprie clausole quella secondo cui potrà rendersi necessario modificare in tutto o in parte o cedere il contratto, in seguito a provvedimenti legislativi che comportino l'abolizione delle Province o la redistribuzione delle relative competenze, tutto ciò senza che la Ditta affidataria possa vantare, nei confronti dell'ente, alcunché per danno emergente o per lucro cessante.

Reggio Emilia, lì 06/12/2016

IL DIRIGENTE DEL
Servizio Bilancio
F.to DEL RIO CLAUDIA

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

(da sottoscrivere in caso di stampa)
Si attesta che la presente copia, composta di n. ... fogli, è conforme in tutte le sue componenti al corrispondente atto originale firmato digitalmente conservato agli atti con n ..... del .....
Reggio Emilia, lì.....Qualifica e firma .....

PROVINCIA
DI REGGIO EMILIA

Reggio Emilia, lì 05/12/2016

Il sottoscritto Segretario Generale, visti i commi da 512 a 516 dell'art. 1 della l. 208/2015, preso atto che la fornitura viene acquisita con le modalità di cui al citato comma 512, dichiara che non sussiste la necessità dell'autorizzazione prevista dal successivo comma 516.

IL SEGRETARIO GENERALE
(Dott. Alfredo L. Tirabassi)

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

U.O. Sistemi Informativi – Corso Garibaldi, 59 - Tel 0522.444120 - Fax 0522.444159 - sistemi.informativi@provincia.re.it
Provincia di Reggio Emilia - Corso Garibaldi, 59 - 42121 Reggio Emilia - c.f. 00209290352 - Tel. 0522.444111 - www.provincia.re.it

PROVINCIA
DI REGGIO EMILIA

CAPITOLATO
Acquisto sistema di sicurezza per la rete provinciale

CIG: Z211C54496

CUP: C89G16000750003

CPV: 32000000

CODICE NUTS: ITD53

1) Oggetto

Il presente capitolato ha per oggetto l'acquisto e le relative attività per l'attivazione di un sistema di sicurezza per la rete provinciale

2) Importo Base d'asta: € 39.900,00 al netto di I.V.A.

3) Descrizione della situazione attuale:

La rete telematica territoriale della Provincia di Reggio Emilia è stata progettata nel corso del 2000 e ha consentito di realizzare una rete di trasmissione dati 'protetta' tra i comuni e la Provincia di Reggio Emilia garantendo l'interoperabilità e lo scambio di dati in formato digitale tra le pubbliche amministrazioni del territorio provinciale; tale rete si è evoluta negli anni ed è stata integrata nella rete Lepida regionale. Con la creazione della rete telematica è stato costruito un modello topologico che ha visto la Provincia come snodo di collegamento della rete dei comuni verso il mondo Internet e la rete regionale e questo ha richiesto che nella realizzazione di tale rete fossero acquisiti e configurati adeguati apparati di protezione per la sicurezza della rete e dei dati degli enti coinvolti; negli anni il sistema è stato adeguato alle evoluzioni tecnologiche, alle mutate caratteristiche della rete telematica regionale e all'aumento costante delle minacce alla sicurezza.
L'attuale infrastruttura di sicurezza dell'Ente è composta da un firewall CheckPoint R77.30, che garantisce servizi di IPS, VPN IPSEC ed SSL, installato su una coppia di appliance IP560 e da un sistema di webfiltering per i contenuti http separato, Fortigate 200A. Il traffico di rete sul protocollo http viene poi ispezionato per possibili virus, mediante il servizio IWSVA di TrendMicro, non viene attualmente ispezionato il traffico https.

Attualmente la rete provinciale garantisce:

- l'accesso alla rete interna e alla navigazione a circa 400 postazioni utenti, utilizzano infatti la rete provinciale anche dipendenti regionali che operano dagli uffici provinciali e tutti necessitano costantemente di accedere a banche dati raggiungibili mediante internet (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, etc);
- l'accesso a sistemi informativi provinciali, sia ad accesso riservato agli uffici comunali (back office dello SUAP, di Rilfedeur e delle elezioni; strumenti di gestione della

cartografia, dns) sia aperti a tutti (software di segnalazione per i cittadini, consultazione delle tornate elettorali, catalogo delle biblioteche provinciali, cartografia provinciale, etc), installati presso la sala macchine della Provincia;
- servizio di firewall per la rete interna e le pubblicazioni su internet per quattro comuni che non hanno un proprio apparato di protezione;
- servizio di firewall per la navigazione internet per tredici comuni che hanno un proprio apparato firewall per la rete interna, ma accedono a Internet mediante la rete provinciale;
- protezione del servizio di posta elettronica mediante il servizio di relay provinciale per dieci comuni;
- protezione del servizio di videosorveglianza di un comune

4) Prestazione richiesta

I concorrenti dovranno formulare una relazione descrittiva che presenti il sistema di sicurezza che intendono proporre, sulla base delle caratteristiche tecniche minime come dettagliate dal produttore, l'implementazione e configurazione che intendono effettuare sul sistema perché sia rispondente alle necessità dell'Ente, come sotto dettagliate.
Dovrà inoltre essere presente un crono programma che specifichi le modalità e le tempistiche per la conversione delle configurazioni e delle regole attualmente presenti sul sistema firewall per garantire il minimo disservizio: tali attività dovranno essere effettuate in affiancamento al personale interno all'Ente, che si occuperà poi della gestione del sistema a regime.
I requisiti del sistema proposto, dovranno tener conto delle caratteristiche della rete dell'Ente come descritte al punto precedente, considerando che il traffico che transita dal firewall continuerà ad aumentare in quanto sempre più risorse e banche dati devono essere raggiungibili sulla rete internet per l'ordinaria attività degli uffici e che sempre più l'accesso a tali banche dati dovrà essere protetto e quindi transitare cifrato (https); sulla base di tali considerazioni, si sono analizzate le varie soluzioni presenti sul mercato, dando rilievo alle infrastrutture proposte dai leader di mercato, anche sulle base delle analisi effettuate da enti certificatori internazionali, quali Gartner e nss Labs.
Si sono individuate le caratteristiche tecniche e le funzionalità minime che deve prevedere la soluzione proposta, che si elencano sinteticamente di seguito:

- il sistema proposto deve essere configurato in **alta affidabilità**, tramite due dispositivi fisici distinti;
- il sistema e gli apparati proposti dovranno disporre, in maniera integrata, di tutte le diverse funzioni di sicurezza caratterizzanti un "***Next-Generation Firewall****",* ovvero garantire le funzionalità di: **Firewall/VPN di base con l'aggiunta di funzionalità di identificazione delle applicazioni e identificazione dell'utente, oltre ai servizi di Intrusion Prevention System (IPS), Antivirus, Anti-Spyware, Web/URL Filtering, Application Control ed Advanced Threat Protection/Detection**, senza necessità di utilizzare alcun modulo software o hardware aggiuntivo o ulteriore apparato esterno. Queste ultime funzionalità dovranno poter essere implementate ed attivate secondo i diversi profili legati alle singole regole di accesso definite sul sistema;
- la fornitura dovrà prevedere le **licenze e la manutenzione hardware e software annuale** per garantire le funzionalità sopra descritte;
- il sistema così configurato, con tutti i servizi attivi e configurati, dovrà garantire almeno il parametro di ***Threat prevention throughput (Firewall,Application Control, Url Filtering, IPS, Antivirus)*** **pari o superiore ad 1 Gbps**;

- il sistema dovrà disporre di un complesso di correlazioni di oggetti ed eventi relativi a tutte le diverse funzioni di sicurezza sopra descritte che sia integrato sullo stesso apparato del firewall e che garantisca una vista in tempo reale delle attività sospette e degli eventi relativi ad attività malevole;
- gli apparati dovranno disporre, di un servizio **"*Advanced Threat Protection/Detection*"** in Cloud con le seguenti caratteristiche:
  - ricezione e analisi proattiva di molteplici tipologie di file (es. "jar", "PE", "flash","pdf", file Microsoft Office, pacchetti android e della copia di file eseguibili "exe") sospetti in transito sull'apparato firewall stesso;
  - integrazione con l'apparato firewall sia in termini operativi che di gestione del servizio stesso;
  - verifica, analisi e report dettagliato dell'eventuale comportamento malevolo all'apertura o all'esecuzione dello stesso file sospetto;

- dovrà essere presente un **tool di migrazione** automatico che consenta di recuperare le configurazioni relativamente ad oggetti, host, network e regole presenti sull'attuale sistema Check Point;

Sulla base delle esigenze sopra indicate, sono stati analizzati diversi prodotti di mercato ed oltre **alla possibilità di aggiornare la soluzione esistente con appliance e tecnologia Check Point, si è individuata la soluzione "denominata PA 3020" in HA di Palo Alto Network** come quella più corrispondente alle caratteristiche e funzionalità richieste, il fornitore dovrà quindi proporre un progetto di migrazione dall'attuale soluzione ad una piattaforma tra quelle indicate o equivalente a livello di prestazioni, funzionalità e caratteristiche tecniche, con tutti i servizi attivi richiesti per un anno.

5) Installazione e migrazione sul nuovo sistema di sicurezza

La fornitura dovrà inoltre prevedere:

- tutti i componenti accessori (cavi, terminatori, viti, …) necessari alla corretta installazione e funzionamento dell'infrastruttura;
- l'installazione fisica degli apparati e la loro configurazione software;
- le licenze e la manutenzione hardware e software adeguate all'implementazione del progetto proposto, all'ultima versione disponibile e stabile, comprensive di un anno di manutenzione;
- il ripristino di tutte le configurazioni che riguardano le dmz, le policy, le regole di Qos, le regole di address space, le Vpn, i certificati, i backup automatici, il salvataggio dei log etc.;

La ditta aggiudicataria concorderà insieme ai referenti dell'UO Sistemi Informativi della Provincia di Reggio Emilia un piano di implementazione e avviamento che preveda le fasi di installazione, configurazione e relativa migrazione dal vecchio al nuovo sistema per raggiungere il completo funzionamento dell'intero (Connettività, VPN, Qualite of Service etc. etc.), che sarà certificato dalla stessa ditta attraverso un documento di collaudo.

6) Sopralluogo

I concorrenti sono tenuti ad effettuare un sopralluogo preventivo nelle aree/luoghi nei quali sarà realizzato il servizio, al fine di valutarne problematiche e complessità in relazione alla predisposizione dell'offerta. Per effettuare tale sopralluogo i concorrenti devono concordare un appuntamento con il referente della Provincia individuato nella Sig.ra

Daniela Galeazzi, reperibile ai seguenti recapiti telefonici 0522444161 - fax 0522444159 - posta elettronica d.galeazzi@provincia.re.it. Detto referente redigerà apposito attestato di sopralluogo. Una copia dello stesso verrà consegnata alla ditta concorrente, che dovrà allegarlo a pena di esclusione alla “documentazione amministrativa”.

Saranno escluse le Ditte che non avranno effettuato il sopralluogo richiesto.

7) Luogo e tempi di consegna

La consegna e l’installazione del sistema operativo e del software deve essere effettuata presso la Sala Macchine dell'UO Sistemi Informativi, sita in Reggio Emilia, Piazza S. Giovanni, 4, entro 45 (quarantacinque) giorni naturali e consecutivi dal ricevimento dell’ordine da parte di questa Provincia. Tale termine potrà essere prorogato, ad insindacabile giudizio di questa Provincia, qualora intervenissero cause ostative non dipendenti dalla Ditta aggiudicataria. La Ditta aggiudicataria deve effettuare la consegna dei prodotti con costi a suo carico e a proprio rischio.

L’installazione del sistema operativo e del software dovrà essere fatta alla presenza del personale incaricato dell'UO Sistemi Informativi.

8) Garanzia di funzionamento

La ditta dovrà garantire i seguenti punti:

- funzionamento dell'intero sistema, ovvero l'offerta deve essere "chiavi in mano";
- dovrà farsi carico di qualunque imprevisto o problema sorga in fase di installazione, messa a punto e collaudo dell'intero sistema;
- dovrà prevedere un supporto di assistenza sistemistica "post-installazione" con personale qualificato in affiancamento all'UO Sistemi Informativi della Provincia per risolvere eventuali anomalie o malfunzionamenti.

9) Collaudo.

Il collaudo dei sistemi oggetto della fornitura sarà effettuato dopo la consegna e l'installazione presso la sede indicata nel **punto 7** da parte del Responsabile dell'UO Sistemi Informativi. Si procederà al collaudo entro 45 giorni naturali e consecutivi dalla data di consegna dei sistemi. I beni rifiutati al collaudo ferma restando l'applicazione delle penalità di cui al **punto 19** dovranno essere sostituiti a cura e spese della Ditta aggiudicataria entro e non oltre 15 giorni naturali e consecutivi dalla data di comunicazione del mancato collaudo.

10) Garanzia.

La garanzia dei sistemi oggetto della fornitura dovrà avere una durata di mesi 12 (dodici) on-site dalla data di collaudo e dovrà essere compresa nel prezzo offerto.

11) Modalità di scelta del contraente e requisiti di partecipazione

La selezione degli operatori economici avverrà facendo ricorso al Mercato Elettronico di Consip SPA, ai sensi dell'art. 37, Comma 1, del D. Lgs n. 50/2016.

I soggetti partecipanti alla gara non devono essere incorsi in alcuno dei motivi di esclusione di cui all'art. 80 del D.Lgs. n. 50/2016.

In caso di soccorso istruttorio si applica la disciplina dell'art. 83, comma 9 del decreto precitato, applicando una penale pari all'1 per mille del valore di gara.

12) Presentazione dell'offerta.
L'offerta andrà presentata entro quindici giorni con decorrenza dalla data di avvio della procedura concorrenziale, secondo il procedimento generato dal sistema MePA.

L'offerta formulata ha una validità di 60 giorni dalla scadenza dei termini di presentazione delle offerte.

Nell'offerta economica l'operatore dovrà indicare i propri costi aziendali concernenti l'adempimento delle disposizioni in materia di salute e sicurezza sui luoghi di lavoro.

La presentazione dell'offerta da parte delle Imprese partecipanti implica l'accettazione incondizionata di tutte le condizioni e norme contenute nel presente Capitolato; tale Capitolato è parte integrante del contratto che verrà stipulato con la ditta aggiudicataria oltre a quelle definite nelle "Condizioni generali di contratto relative alla prestazione di servizi per l'informatica e le telecomunicazioni" redatte da Consip S.p.A. relativamente al Bando ICT 2009 di Abilitazione al Mercato Elettronico della Pubblica Amministrazione.
Per la Provincia di Reggio Emilia il rapporto obbligatorio sorgerà solo dopo l'intervenuta esecutività della Determinazione Dirigenziale che disponga l'aggiudicazione definitiva della fornitura.

13) Cauzioni
Unitamente all'offerta, la Ditta dovrà prestare un'unica cauzione provvisoria anche mediante fideiussione bancaria o assicurativa o rilasciata dagli intermediari finanziari iscritti nell'elenco speciale di cui all'art. 93 del D.Lgs 50/2016, del valore minimo del 2% dell'importo della base d'asta. La cauzione provvisoria non potrà essere costituita, allegando all'offerta denaro contante, assegni bancari o circolari. La cauzione provvisoria dovrà prevedere espressamente quanto segue:

a) La rinuncia al beneficio della preventiva escussione del debitore principale e la sua operatività entro 15 giorni a semplice richiesta scritta della stazione appaltante;
b) La rinuncia all'eccezione di cui all'art. 1957 comma 2 del Codice Civile;
c) Validità per almeno 180 giorni dalla data di presentazione dell'offerta;
d) Impegno del fideiussore a rilasciare la garanzia di cui all'art. 103 del D.Lgs. 50/2016 (cauzione definitiva).

Alla Ditta aggiudicataria verrà inoltre richiesta la costituzione di una cauzione definitiva mediante fideiussione bancaria o assicurativa secondo la disciplina di cui all'art. 103 del D.Lgs.vo n. 50/2016.

In caso di riduzione della cauzione, secondo quanto indicato dall'articolo precitato, il concorrente dovrà autodichiarare, sotto la propria responsabilità, in quale fattispecie rientra.

14) **Aggiudicazione.**
La fornitura in oggetto verrà assegnata secondo il criterio dell'offerta economicamente più vantaggiosa, secondo il miglior rapporto qualità/prezzo, ai sensi dell'art. 95 comma 2, del D.Lgs.vo n. 50/2016, sulla base dell'applicazione dei seguenti criteri e coefficienti:

- elemento prezzo, punteggio massimo 20/100
- elemento qualità, punteggio massimo 80/100

OFFERTA TECNICA: massimo punti 80

L'offerta tecnica è costituita da una RELAZIONE DESCRITTIVA, composta da massimo n. 8 facciate di formato A4 redatte con carattere Arial di dimensione 12 pt., interlinea 1 in formato pdf. Sono esclusi da tale computo le pagine relative ai curricula professionali del personale che sarà adibito al servizio.

La sopracitata relazione descrittiva dovrà articolarsi secondo i seguenti punti:

1) Caratteristiche del prodotto che si intende proporre e metodologie del servizio proposto

- descrizione della soluzione tecnologica che si intende proporre, comprensiva del codice delle licenze che si intende fornire e delle metodologie che si intendono utilizzare per la migrazione dalle attuali configurazioni e regole;
- formulazione piano temporale delle azioni necessarie per realizzare i suddetti interventi;
- indicazione dell'esperienza e professionalità del personale che sarà adibito al servizio, da desumere dagli allegati curricula professionali, specificandone il numero;

2) Elencazione e descrizione migliorie offerte rispetto alle prestazioni previste dal presente Capitolato, senza oneri aggiuntivi per la Provincia.

La commissione di gara che procederà all'esame delle offerte tecniche, nel suo plenum, redigerà la graduatoria in base al criterio dell'offerta economicamente più vantaggiosa, applicando il metodo aggregativo-compensatore di cui "alle Linee Guida attuative del nuovo Codice degli Appalti e delle Concessioni" deliberate da ANAC con atto n. 1005 del 21 settembre 2016 con la riparametrazione per i sub criteri a), b), c) relativi al criterio A) e per i criteri B) e C), tenuto conto della seguente articolazione:

Criteri di valutazione dell'offerta tecnica:

CRITERIO A: **Caratteristiche e metodologie del servizio proposto, articolate nei seguenti subcriteri:**	**Max punti 65**
Subcriterio a: proposta progettuale d'insieme, caratteristiche della soluzione proposta comprensive del codice delle licenze che si intende fornire e dettaglio tecnico/organizzativo delle modalità di migrazione. Saranno valutate in questa categoria anche le modalità di intervento, tempo di fermo dei servizi garantiti verso Internet, le procedure per il salvataggio e il ripristino dei log e delle configurazioni.	max 40 punti
Subcriterio b: assistenza post installazione (durata, modalità di erogazione del servizio e SLA)	max 15 punti
Subcriterio c: struttura organizzativa della ditta con particolare riferimento, anche se non esclusivo, a certificazioni attinenti ai servizi richiesti ed esperienza e professionalità del personale che sarà adibito al servizio, da desumere dagli allegati curricula professionali, specificandone il numero	max 10 punti
CRITERIO B: Chiarezza e completezza della relazione tecnica	**Max punti 5**
CRITERIO C: migliorie liberamente proposte relativamente ai	**Max punti 10**

risultati attesi, ai tempi di realizzazione, o altre proposte migliorative, quali ad esempio la percentuale di sconto attuata sulla manutenzione hardware e software per il secondo anno sul prezzo di listino	
Totale PUNTI	**80**

Punteggio massimo assegnato per la parte qualitativa Q(i) (punti max 80) è valutato con un metodo multicriterio, applicato secondo la seguente formula:

Q(i) = A(i)+B(i)+C(i)
Q(i) = punteggio complessivo assegnato all'offerta i-esima
A(i) = punteggio assegnato all'offerta i-esima per le 'Caratteristiche e le metodologie del servizio proposto'
B(i) = punteggio assegnato all'offerta i-esima per la 'Chiarezza e completezza della relazione tecnica'
C(i) = punteggio assegnato all'offerta i-esima per le 'migliorie liberamente proposte relativamente ai risultati attesi, ai tempi di realizzazione, o altre proposte migliorative quali ad esempio la percentuale di sconto attuata sulla manutenzione hardware e software per il secondo anno sul prezzo di listino'

1**) A(i) = punteggio assegnato all'offerta i-esima per le Caratteristiche e le metodologie del servizio proposto**

Poiché questo elemento di valutazione viene valutato ricorrendo a dei sub criteri si applicano per ciascuno dei sub criteri le seguenti formule:

sub criterio a) proposta progettuale d'insieme, caratteristiche della soluzione proposta comprensive del codice delle licenze che si intende fornire e dettaglio tecnico/organizzativo delle modalità di migrazione. Saranno valutate in questa categoria anche le modalità di intervento, tempo di fermo dei servizi garantiti verso Internet, le procedure per il salvataggio e il ripristino dei log e delle configurazioni.

Aa(i) = 40*aa(i)/aa(max)

Aa(i): punteggio attribuito all'i-esimo concorrente per il sub criterio a)

aa(i):punteggio attribuito per la valutazione del sub criterio a)

aa(max): punteggio massimo fra quelli attribuiti per la valutazione delle medesime caratteristiche proposte dal concorrente per il presente elemento di valutazione;

sub criterio b) assistenza post installazione (durata, modalità di erogazione del servizio e SLA)

Ab(i) = 15*ab(i)/ab(max)

Ab(i): punteggio attribuito all'i-esimo concorrente per il sub criterio b)

ab(i): punteggio attribuito per la valutazione del sub criterio b)

ab(max): punteggio massimo fra quelli attribuiti per la valutazione delle medesime caratteristiche proposte dal concorrente per il presente elemento di valutazione;

sub criterio c) struttura organizzativa della ditta con particolare riferimento, anche se non esclusivo, a certificazioni attinenti ai servizi richiesti ed esperienza e professionalità del personale che sarà adibito al servizio, da desumere dagli allegati curricula professionali, specificandone il numero

Ac(i) = 10*ac(i)/ac(max)

Ac(i): punteggio attribuito all'i-esimo concorrente per il sub criterio c)

ac(i): punteggio attribuito per la valutazione del sub criterio c)

ac(max): punteggio massimo fra quelli attribuiti per la valutazione delle medesime caratteristiche proposte dal concorrente per il presente elemento di valutazione

2) **B(i) = punteggio assegnato all'offerta i-esima per la Chiarezza e completezza della relazione tecnica calcolato in base alle indicazioni e alla formula seguente:**

B(i) = 5*b(i)/b(max)

Dove:

B(i): punteggio attribuito all'i-esimo concorrente per il criterio B

b(i): punteggio attribuito per il criterio B;

b(max):punteggio massimo fra quelli attribuiti per il criterio B.

3**) C(i) = punteggio assegnato all'offerta i-esima per le migliorie liberamente proposte relativamente ai risultati attesi, ai tempi di realizzazione, o altre proposte migliorative, quali ad esempio la percentuale di sconto attuata sulla manutenzione hardware e software per il secondo anno sul prezzo di listino,calcolato in base alla formula seguente:**

C(i) = 10*c(i)/c(max)

Dove:

C(i): punteggio attribuito all'i-esimo concorrente per il criterio C

c(i): punteggio attribuito per la valutazione del criterio C

c(max):punteggio massimo fra quelli attribuiti per la valutazione del criterio C.

Verrà attribuito, dalla Commissione nel suo plenum, un punteggio variabile da 0 a 10, da valutare in base alla documentazione presentata.

Si precisa inoltre che la Commissione non procederà all'apertura delle buste contenenti le offerte economiche relative a ditte che non abbiano raggiunto, in ordine ai parametri relativi all'offerta tecnica, almeno il punteggio di 55 su 80.

OFFERTA ECONOMICA: massimo punti 20

Gli operatori economici partecipanti alla gara dovranno indicare, compilando l'apposito modulo su MEPA, il prezzo che intendono applicare sull'importo posto a base di gara. Sulla base del prezzo presentato la stazione appaltante calcolerà l'offerta economica in valore numerico di ogni singolo operatore economico.

Sono ammesse offerte economiche pari alla base d'asta

Per valutare il prezzo di ogni singolo offerente si procede nel seguente modo:

Prezzo P(i) (punti max 20)

P(i) = Omi/Oi x R(max)

dove :

P(i) = punteggio del singolo partecipante

Omi = Offerta migliore tra quelle pervenute in valore numerico come sopra determinato

Oi= Offerta del partecipante di cui viene calcolato il risultato in valore numerico come sopra determinato

R(max)= Risultato economico massimo (pari a 20)

L'offerta di ciascun candidato viene messa in relazione inversamente proporzionale all'offerta migliore. L'offerta migliore prende il massimo del punteggio economico previsto e a tutte le altre viene attribuito un punteggio inferiore proporzionalmente a quanto è peggiore l'offerta fatta.

L'aggiudicazione avverrà a favore dell'Impresa che avrà ottenuto il punteggio più elevato, sommando Q(i), per la parte qualitativa, al punteggio ottenuto per la parte prezzo P(i).

Si procederà alla valutazione della congruità delle offerte in relazione alle quali sia i punti relativi al prezzo sia la somma dei punti relativi a tutti gli altri elementi di valutazione, siano entrambi pari o superiori ai quattro quinti dei corrispondenti punti massimi previsti (art. 97, comma 3 del D.Lgs 50/2016), prima della riparametrazione.

L'offerta anomala verrà determinata ai sensi dell'art. 97 del D.Lgs. 50/2016.

Il servizio verrà assegnato anche in presenza di una sola offerta, purché ritenuta valida ed idonea.

In caso di offerte uguali si procederà al sorteggio per designare l'aggiudicatario della fornitura.

La Provincia si riserva la facoltà, a suo insindacabile giudizio, di procedere o meno alla aggiudicazione.

In caso di mancata aggiudicazione, le Imprese partecipanti alla presente Richiesta di Offerta non vanteranno nei confronti della Provincia di Reggio Emilia alcun diritto di rimborso spese o risarcimento danni, sia per danno emergente, sia per lucro cessante.

Qualora non venga presentata alcuna offerta la Provincia potrà sondare a suo piacimento il libero mercato procedendo ai sensi dell'art. 36, comma 2, lett. a) del D.Lgs.vo n. 50/2016.

15) Stipula del contratto e assolvimento imposta di bollo

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).
Il documento di accettazione firmato dal Punto Ordinante dell'Ente conterrà tutti i dati essenziali del contratto: amministrazione aggiudicatrice, fornitore aggiudicatario, oggetto della fornitura, dati identificativi, tecnici ed economici dell'oggetto offerto, informazioni per la consegna e fatturazione ecc. e pertanto tale documento di accettazione dell'offerta deve essere assoggettato ad imposta di bollo che dovrà essere assolta da parte dell'aggiudicatario in modo virtuale ovvero assolta secondo le modalità previste dall'art. 15 D.P.R. 26 ottobre 1972, n. 642 ovvero assolta in base alle modalità individuate dalla lettera a) dell'art. 3 D.P.R. 26 ottobre 1972, n. 642 e cioè mediante versamento all'intermediario convenzionato con l'Agenzia delle Entrate che rilascia apposito contrassegno, vale a dire, con apposizione di marca da bollo da € 16,00 su copia del contratto, annullata con timbro e firma della ditta, che dovrà essere inviato in copia al punto ordinante (fax 0522/444159 o mail: sistemi.informativi@provincia.re.it).

Qualora si verifichi la fattispecie di cui all'ultimo comma dell'articolo precedente il contratto verrà concluso ai sensi dell'art. 32, comma 14 del D.Lgs.vo n. 50/2016 mediante scrittura privata.

16) Oneri per la sicurezza

In considerazione della tipologia di servizio, le cui attività ricadono nell'applicazione dell'art. 26 del D. Lgs. 81/08 e s.m.i., vista l'analisi svolta, non è stata rilevata la presenza di contatti rischiosi o pericolosi e pertanto gli oneri della sicurezza volti ad eliminare le interferenze si ritengono pari a zero e quindi non è necessaria la redazione del DUVRI.

Gli operatori economici dovranno indicare, in sede di presentazione dell'offerta economica, gli oneri di sicurezza aziendali.

17) Certificazione

I prodotti offerti dovranno essere conformi alle normative vigenti in materia con particolare riferimento alle disposizioni del Decreto Legislativo n. 626 del 19.9.1994 e successive modificazioni ed integrazioni, nonché alle norme internazionali relative alla sicurezza (ergonomia contro i danni alla salute degli utenti, protezione da incidenti meccanici, shock elettrici, fuoco, radiazioni ecc.).

18) Subappalto e cessione del contratto

In caso di sub appalto si applica la disciplina dell'art. 105 del D.Lgs. n. 50/2016.
E' vietato al soggetto appaltatore aggiudicatario di cedere il contratto.

19) Penali.
La Provincia ha la facoltà di applicare le seguenti penali:
1.*Ritardo nella consegna dei beni*
Nel caso di ritardo nella consegna, totale o parziale, in considerazione dell'importanza della fornitura per l'Ente, la Ditta aggiudicataria potrà essere assoggettata, a discrezione esclusiva della Provincia, alla penale di € 500,00 IVA esclusa, per ognuno dei primi 7 giorni naturali e consecutivi di ritardo e del 1% (uno per cento) dell'importo, IVA esclusa, della fornitura ad essa aggiudicata per ognuno dei successivi giorni naturali e consecutivi susseguenti ai primi 7 giorni. La penale si applica in proporzione all'importo dei beni consegnati in ritardo. Se l'importo dei beni consegnati in ritardo è superiore al 20% dell'importo contrattuale, l'importo della penale si applica sul prezzo netto del contratto.

2. *Altre inadempienze*
Nel caso di altre inadempienze nell'esecuzione di prestazioni contrattuali non previste nel punto precedente la Ditta aggiudicataria è assoggettata a penale rapportata in ragione delle loro gravità all'importo delle prestazioni non eseguite o non esattamente eseguite, fino ad un massimo del 10% dell'importo netto della fornitura. La penalità deve essere notificata alla Ditta aggiudicataria mediante PEC e sarà addebitata sui crediti vantati dalla Ditta dipendenti dal contratto relativo alla fornitura in questione. Per l'incasso delle penali può essere escussa anche la cauzione di cui al precedente **punto 13**

20) **Obbligo alla riservatezza.**
La ditta aggiudicataria sarà tenuta a mantenere segreti tutti i dati di qualsiasi natura di cui venga a conoscenza nell'esecuzione della fornitura in oggetto, essendo gli stessi considerati riservati a tutti gli effetti di legge e sottoposti come tali al trattamento del D Lgs n. 196 del 30 giugno 2003.
La ditta aggiudicataria dovrà altresì impegnarsi a dare istruzioni al proprio personale affinché tutti i dati relativi sia all'attività dell'Ente che a quella dei suoi utenti di cui venga a conoscenza, siano considerati riservati e come tali trattati.

21) **Obblighi di tracciabilità ex L. 136/2010.**.
Ai sensi della L.136/2010, ai fini della tracciabilità dei flussi finanziari, nella documentazione da presentare a seguito di aggiudicazione, 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.

Ai fini della tracciabilità dei flussi finanziari, gli strumenti di pagamento dovranno riportare, in relazione a ciascuna transazione posta in essere, il codice identificativo gara (CIG), attribuito dall' Autorità Nazionale Anticorruzione (A.N.A.C.).
Dovranno inoltre essere comunicati le generalità e il codice fiscale delle persone delegate ad operare sul suddetto c/c dedicato, entro 7 gg. dalla loro accensione o, nel caso di c/c già esistente, dalla sua prima utilizzazione in operazioni finanziarie relative alla presente commessa pubblica. E' fatto obbligo di provvedere altresì a comunicare ogni modifica ai dati trasmessi. A pena di nullità assoluta, la ditta assumerà gli obblighi di tracciabilità dei flussi finanziari di cui alla legge sopra citata.

L'assunzione degli obblighi di tracciabilità dei flussi finanziari dovrà essere riportata in tutti i contratti sottoscritti con i subappaltatori ed i subcontraenti della filiera delle imprese a qualsiasi titolo interessate al servizio/lavoro/fornitura di cui al presente Capitolato e la Provincia potrà verificare in ogni momento tale adempimento.
Il mancato utilizzo del bonifico bancario o postale, ovvero degli altri strumenti idonei a consentire la piena tracciabilità delle operazioni, determinerà la risoluzione di diritto del contratto.

L'appaltatore, il subappaltatore o il subcontraente che ha notizia dell'inadempimento della propria controparte agli obblighi di tracciabilità finanziaria di cui alla Legge 136/2010, ne darà immediata comunicazione alla Provincia di Reggio Emilia e alla Prefettura-Ufficio territoriale del Governo di Reggio Emilia.

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

Il contraente con riferimento alla prestazione 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 svolta, gli obblighi di condotta previsti dal codice di comportamento dei dipendenti della Provincia di Reggio Emilia approvato con delibera n. 23 del 11/02/2014. A tal fine si dà atto che l'amministrazione ha informato il contraente che sul sito della Provincia di Reggio Emilia è pubblicato il codice di comportamento al seguente indirizzo:

http://www.provincia.re.it/page.asp?IDCategoria=703&IDSezione=26591&ID=529565.

Il Contraente 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 del contraente degli obblighi di cui al codice di comportamento dei dipendenti della Provincia di Reggio Emilia approvato con delibera di Giunta provinciale n. 23 del 11/02/2014 costituisce motivo di risoluzione di diritto del contratto ai sensi dell'art. 1456 codice civile. Il Responsabile del procedimento verificata la 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 dl contratto, fatto salvo il risarcimento dei danni

23) **Fatturazione e pagamento**

La fatturazione potrà avvenire a seguito della protocollazione dell'attestazione del collaudo.

La ditta dovrà emettere regolare fattura intestata 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:

- CUP e CIG, ove previsti;
- numero/i del buono/i 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.
Il pagamento sarà effettuato a 30 giorni dal ricevimento della fattura

24) **Clausole di salvaguardia**
Il contratto è sottoposto a condizione risolutiva nel caso di disponibilità di convenzione Consip o della Centrale di committenza regionale (Intercent-ER) adeguate alle esigenze espresse sul capitolato . In alternativa, a norma di quanto disposto dal comma 7 dell'articolo 9 del D.L. 66/2014, l'Impresa aggiudicataria dovrà adeguare i prezzi proposti al parametro di *benchmark* delle Convenzioni Consip o della centrale di Committenza regionale Intercent-ER, se più favorevole.
Si precisa inoltre, che il contratto potrà essere modificato in tutto o in parte, ceduto o revocato in relazione all'emanazione di provvedimenti legislativi che comportino la trasformazione delle Province ed il trasferimento delle attuali competenze ad altri enti.

25) Risoluzione del Contratto
Qualora nel corso dell'erogazione del servizio richiesto al presente appalto, la stazione appaltante accerti che la suddetta erogazione non procede secondo le condizioni stabilite, può fissare un termine perentorio entro il quale la Ditta aggiudicataria deve conformarsi a tali condizioni. Trascorso inutilmente il termine, la stazione appaltante si riserva la facoltà di risolvere il contratto. La risoluzione opera in ogni caso di inadempimento degli obblighi contrattuali assunti dalla Ditta aggiudicataria.
La risoluzione comporta in ogni caso l'escussione della cauzione oltre all'eventuale risarcimento danni. In tale caso, la stazione appaltante si riserva di rivolgersi ad altro fornitore e le maggiori spese derivanti saranno a carico della Ditta aggiudicataria.

Qualora il fornitore non osservi anche uno solo degli obblighi assunti o si renda colpevole di gravi inadempienze quali ad es: ripetuti ritardi nell'esecuzione del servizio, ovvero, reiterata non conformità dei servizi prestati rispetto alle indicazioni del presente Capitolato o qualunque altra inadempienza, ritenuta ad insindacabile giudizio dell'Amministrazione grave, quindi non prevista, ma che si dovesse verificare durante l'esecuzione contrattuale l'Ente avrà la facoltà di risolvere "ipso-facto et jure" il contratto, mediante semplice dichiarazione stragiudiziale intimata (ex art. 1456 c.c.) a mezzo lettera raccomandata con avviso di ricevimento, salvo in ogni caso il risarcimento del danno.

La cauzione definitiva verrà incamerata a titolo di penale e di indennizzo, salvo il risarcimento dei maggiori danni. E' facoltà dell'Ente, in caso di risoluzione del contratto, rivolgersi per l'esecuzione dei servizi oggetto del presente Capitolato, alla ditta seconda classificata.

Per tutto quanto non previsto si applica la disciplina di cui all'art. 108 del D.Lgs. n. 50/2016.

26) Recesso
Relativamente al recesso si applica l'art. 109 del D.Lgs.vo n. 50/2016.

27) Controversie
In caso di contenzioso si applica l'art. 204 del D.Lgs.vo n. 50/2016; per I rimedi alternativi alla giurisdizione si fa riferimento alla parte VI, titolo I, capo II del decreto medesimo.

28) **Rinvio**.
Per tutto quanto non previsto nel presente Capitolato, sono applicabili le disposizioni contenute nel D. Lgs. 50/2016, nonché le altre leggi e regolamenti vigenti in materia, in quanto applicabili.

29) **Responsabile unico del procedimento e direttore per l'esecuzione del contratto**
Il Responsabile Unico del Procedimento, ai sensi dell'art. 31 del D.Lgs.vo n. 50/2016, nonché direttore dell'esecuzione del Contratto, ai sensi dell'art. 101 del decreto stesso, è la Dott.ssa Claudia Del Rio, Dirigente del Servizio Bilancio.

Per ogni ulteriore informazione di carattere tecnico è possibile rivolgersi al sig. Denis Manzini (tel. 0522/444157, d.manzini@provincia.re.it) o in alternativa alla dott.ssa Daniela Galeazzi (tel. 0522/444161; d.galeazzi@provincia.re.it).

Reggio Emilia, 05/12/2016

La Dirigente
Servizio Bilancio
(F.to dott.ssa Claudia Del Rio)

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

PROGETTO

Acquisto ed attivazione di un sistema di sicurezza per la rete provinciale (a norma dell'art. 37, comma 1 del D.Lgs.vo n. 50/2016, con l'attivazione di una richiesta di offerta (RdO), nell'ambito del Mercato Elettronico della Pubblica Amministrazione (MePA))

La Provincia, per garantire la funzionalità dei propri uffici e degli uffici dei comuni che utilizzano la rete provinciale, ha la necessità di adottare tutte le misure di sicurezza e prevenzione così da ridurre al minimo il rischio di malfunzionamenti ed interruzioni di servizio.

Con deliberazione della Giunta Provinciale n. 133 del 2.5.2000, è stato approvato il progetto della prima rete telematica territoriale della Provincia di Reggio Emilia, che ha consentito di realizzare una rete di trasmissione dati 'protetta' tra i comuni e la Provincia di Reggio Emilia consentendo l'interoperabilità e lo scambio di dati in formato digitale tra le pubbliche amministrazioni del territorio provinciale; tale rete si è evoluta negli anni ed è stata integrata nella rete Lepida regionale. Con la creazione della rete telematica è stato costruito un modello topologico che ha visto la Provincia come snodo di collegamento della rete dei comuni verso il mondo Internet e la rete regionale e questo ha richiesto che nella realizzazione di tale rete fossero acquisiti e configurati adeguati apparati di protezione per la sicurezza della rete e dei dati degli enti coinvolti ed in coerenza con le tecnologie disponibili in quegli anni, è stato implementato uno strumento di firewall leader di mercato che ha garantito la massima sicurezza e stabilità.

Negli anni il sistema è stato adeguato alle evoluzioni tecnologiche, alle mutate caratteristiche della rete telematica regionale e all'aumento costante delle minacce alla sicurezza; in particolare con determinazione n. 853/2008 è stato acquisito un sistema firewall costituito da due apparati di rete Nokia/CheckPoint IP 560, aggiornato ora alla release software R 77.30: tale sistema al 31 dicembre 2016 non verrà più supportato dalla casa madre a livello di manutenzione hardware; si rende pertanto necessario sostituirlo, perché in caso di guasto e/o malfunzionamento non sarebbe garantito in alcun modo il suo ripristino.

Il sistema di sicurezza informatica dell'Ente negli anni è diventato sempre più importante e cruciale per via della crescente informatizzazione dei servizi in termini di apparati e sistemi informatici e della parallela diffusione e specializzazione delle minacce alla sicurezza: per l'operatività quotidiana degli uffici è necessario accedere a banche dati raggiunte tramite la rete Internet e molte di queste banche dati sono pubblicate con comunicazioni di tipo cifrato, proprio a causa dell'aumento delle minacce, che richiedono però tempi di controllo maggiori. Molte minacce arrivano poi dai file allegati o dai link inseriti nelle e-mail, strumento sempre più diffuso e indispensabile per tutti i dipendenti dell'Ente: è quindi fondamentale che tutte queste attività transitino dagli apparati di sicurezza garantendone la protezione da tutte le minacce presenti sulla rete internet e nelle mail, assicurando al contempo tempi di accesso soddisfacenti.

Attualmente la rete provinciale garantisce:

- l'accesso alla rete interna e alla navigazione a circa 400 postazioni utenti, utilizzano infatti la rete provinciale anche dipendenti regionali che operano dagli uffici provinciali e tutti necessitano costantemente di accedere a banche dati raggiungibili mediante internet (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, etc);

- l'accesso a sistemi informativi provinciali, sia ad accesso riservato agli uffici comunali (back office dello SUAP, di Rilfedeur e delle elezioni; strumenti di gestione della cartografia, dns) sia aperti a tutti (software di segnalazione per i cittadini, consultazione delle tornate elettorali, catalogo delle biblioteche provinciali, cartografia provinciale, etc), installati presso la sala macchine della Provincia;
- servizio di firewall per la rete interna e le pubblicazioni su internet per quattro comuni che non hanno un proprio apparato di protezione;
- servizio di firewall per la navigazione internet per tredici comuni che hanno un proprio apparato firewall per la rete interna, ma accedono a Internet mediante la rete provinciale;
- protezione del servizio di posta elettronica mediante il servizio di relay provinciale per dieci comuni;
- protezione del servizio di videosorveglianza di un comune

Vista quindi la molteplicità e criticità di comunicazioni gestite dalla rete provinciale, si ritiene indispensabile acquisire un'infrastruttura diffusa e leader di mercato, che presenti tutte le migliori caratteristiche funzionali e che assicuri, anche rispetto alle valutazioni comparative effettuate da organismi internazionali, le migliori prestazioni e adeguamenti alla continua mutazione dei rischi informatici.
La scelta di uno strumento molto diffuso, potrà inoltre dare garanzia nel tempo, che su di esso possano operare una molteplicità di imprese con sedi operative tali da poter intervenire presso la sede della Provincia tempestivamente in caso di grave guasto.

Si sono individuate una serie di caratteristiche e funzionalità minime che dovrà garantire lo strumento che si va ad acquisire, così da assicurare i servizi sopra descritti, in particolare la soluzione proposta deve garantire le seguenti funzionalità:

- il sistema proposto deve essere configurato in **alta affidabilità**, tramite due dispositivi fisici distinti;
- il sistema e gli apparati proposti dovranno disporre, in maniera integrata, di tutte le diverse funzioni di sicurezza caratterizzanti un "***Next-Generation Firewall****",* ovvero garantire le funzionalità di: **Firewall/VPN di base con l'aggiunta di funzionalità di identificazione delle applicazioni e identificazione dell'utente, oltre ai servizi di Intrusion Prevention System (IPS), Antivirus, Anti-Spyware, Web/URL Filtering, Application Control ed Advanced Threat Protection/Detection**, senza necessità di utilizzare alcun modulo software o hardware aggiuntivo o ulteriore apparato esterno. Queste ultime funzionalità dovranno poter essere implementate ed attivate secondo i diversi profili legati alle singole regole di accesso definite sul sistema;
- la fornitura dovrà prevedere le **licenze e la manutenzione hardware e software annuale** per garantire le funzionalità sopra descritte;
- il sistema così configurato, con tutti i servizi attivi e configurati, dovrà garantire almeno il parametro di ***Threat prevention throughput (Firewall,Application Control, Url Filtering, IPS, Antivirus)*** **pari o superiore ad 1 Gbps**;
- il sistema dovrà disporre di un complesso di correlazioni di oggetti ed eventi relativi a tutte le diverse funzioni di sicurezza sopra descritte che sia integrato sullo stesso apparato del firewall e che garantisca una vista in tempo reale delle attività sospette e degli eventi relativi ad attività malevole;
- gli apparati dovranno disporre, di un servizio **"*Advanced Threat Protection/Detection*"** in Cloud con le seguenti caratteristiche:
  - ricezione e analisi proattiva di molteplici tipologie di file (es. "jar", "PE",

"flash",“pdf”, file Microsoft Office, pacchetti android e della copia di file eseguibili “exe”) sospetti in transito sull’apparato firewall stesso;
    - integrazione con l’apparato firewall sia in termini operativi che di gestione del servizio stesso;
    - verifica, analisi e report dettagliato dell’eventuale comportamento malevolo all’apertura o all'esecuzione dello stesso file sospetto;

- dovrà essere presente un **tool di migrazione** automatico che consenta di recuperare le configurazioni relativamente ad oggetti, host, network e regole presenti sull'attuale sistema Check Point;

Sulla base delle esigenze sopra indicate, sono stati analizzati diversi prodotti di mercato ed oltre **alla possibilità di aggiornare la soluzione esistente con appliance e tecnologia Check Point, si è individuata la soluzione “denominata PA 3020” in HA di Palo Alto Network** come quella più corrispondente alle caratteristiche e funzionalità richieste, il fornitore dovrà quindi proporre un progetto di migrazione dall'attuale soluzione ad una piattaforma tra quelle indicate o equivalente a livello di prestazioni, funzionalità e caratteristiche tecniche, con tutti i servizi attivi richiesti per un anno.

I concorrenti dovranno **formulare una relazione descrittiva** che presenti dettagliatamente il sistema di sicurezza che intendono proporre, sulla base delle caratteristiche tecniche minime come dettagliate dal produttore, l'implementazione e configurazione che intendono effettuare sul sistema perché sia rispondente alle necessità dell'Ente. Dovrà inoltre essere presente un crono programma che dettagli le modalità e le tempistiche per la conversione delle configurazioni e delle regole attualmente presenti sul sistema firewall per garantire il minimo disservizio: tali attività dovranno essere effettuate in affiancamento al personale interno all'Ente, che si occuperà poi della gestione del sistema a regime.

dato atto che:

- al momento presente, nell'ambito del programma "Acquisti in Rete della PA", attuato dal Ministero dell’Economia e delle Finanze attraverso la gestione di Consip S.p.A, a norma dell'articolo 26 della legge 23 dicembre 1999, n. 488 "Legge finanziaria 2000", relativamente alla categoria “Telecomunicazioni, elettronica e servizi accessori ”, è attiva la convenzione “Reti Locali 5 – Lotto 2“ che propone dispositivi di sicurezza, ma si valuta di non procedere all'acquisizione di tali apparati in quanto:
    - ✓ in data 16 novembre 2016 sul programma "Acquisti in Rete della PA" è stata pubblicata una segnalazione che precisa che '*in data 16/11/2016, relativamente al Lotto 2 della convenzione Reti Locali 5, si è verificato l’esaurimento del massimale,* comprensivo di estensioni 6° e 7° quinto;
    - ✓ i sistemi di sicurezza e relativi servizi software presenti in convenzione non si ritengono adeguati, relativamente a funzionalità, diffusione sul mercato, presenza di aziende sul territorio italiano con esperienza nella loro configurazione e migrazione dal precedente sistemi di sicurezza CheckPoint, attualmente in uso, in particolare:
        - ✗ i dispositivi presenti in convenzione, comprendono quattro soluzioni, dalla fascia base (meno performante) alla fascia top (con grandi prestazioni), e nella comparazione si valuta sempre il sistema di fascia top, denominato USG6650;
        - ✗ il prodotto in convenzione è poco diffuso in Italia al momento e le aziende che possono garantire assistenza e raggiungere in tempi stretti la sede della Provincia in caso di malfunzionamenti gravi e bloccanti sono limitate (l'acquisto di un prodotto più diffuso e presente nel territorio ci dà molte più garanzie in tal senso);

- ✗ rispetto ai sistemi di valutazione internazionale dei prodotti di questa tipologia il prodotto in convenzione è in possesso delle certificazioni ICSA Labs e NSS Labs, ma per Gartner (www.gartner.com) è un prodotto ancora di nicchia, indicato nelle situazioni in cui gli apparati di rete e di amministrazione sono del medesimo costruttore, invece la Provincia non possiede alcun altro prodotto Huawei;
- ✗ non risulta avere integrata la funzionalità di 'a*dvanced threat protection',* come sopra descritta tra le funzionalità di grande importanza nella soluzione che si intende acquisire;

b) al momento presso la Centrale di committenza regionale Intercent-ER è presente la convenzione 'Servizi convergenti ed integrati di trasmissione dati e voce su reti fisse e mobili' che propone a listino, tra i servizi aggiuntivi e non previsti inizialmente, alcune licenze di sistemi di protezione dati, ma si ritiene che non siano adeguati relativamente alle funzionalità e ai costi, così come indicati su tali listini;

L'aggiudicatario dovrà dimostrare di avere esperienza in precedenti migrazioni da sistema firewall CheckPoint esistente alla soluzione proposta e dovrà indicare una proposta di pianificazione delle attività tale da garantire il minimo disservizio.
La ditta dovrà inoltre indicare con precisione il livello di assistenza proposto, successivo alle attività di migrazione, ovvero specificare le modalità con cui sarà possibile segnalare le problematiche evidenziate dal sistema e i tempi di presa in carico, sulla base della gravità del problema riscontrato e dovrà specificare la durata di tale servizio compresa nella fornitura.

Con riferimento alla Legge n. 123 del 03/08/2007 e alla successiva determinazione n. 3 del 05/03/2008 sulla “Sicurezza nell'esecuzione degli appalti relativi a servizi e forniture. Predisposizione del documento unico di valutazione dei rischi (DUVRI) e determinazione dei costi della sicurezza” (emanata dall'AVCP - AUTORITA' per la Vigilanza sui contratti pubblici di lavori, servizi e forniture), trattandosi di affidamento di attività principalmente di natura intellettuale, non sono previsti rischi da interferenza né oneri per la sicurezza.

L'azienda affidataria del servizio dovrà poi dichiarare l'entità dei costi generali per gli adempimenti in materia di sicurezza che sostiene.

La base d'asta ammonta a € 39.900,00.

Per ogni altro dettaglio si rimanda al Capitolato.

PROVINCIA
DI REGGIO EMILIA

Visto, si attesta con esito FAVOREVOLE la regolarità contabile e la copertura finanziaria della spesa della determina N. 795 del 06/12/2016.

Reggio Emilia, lì 06/12/2016

IL DIRIGENTE DEL SERVIZIO BILANCIO

F.to DEL RIO CLAUDIA