Bollettino Ufficiale della Regione Campania n° 07 del 10 febbraio 2003

REGIONE CAMPANIA - AGC Ricerca Scientifica ed Informatica Settore Analisi Progettazione e Gestione Sistemi Informativi e Settore CRED - **Bando di gara: Appalto concorso per la fornitura di un sistema di sicurezza caratterizzato da una piattaforma di applicazioni e servizi per la gestione avanzata della sicurezza ed il controllo delle risorse in rete della Giunta Regionale della Campania - Importo: Euro 610.000,00, oltre IVA.**

1. Ente appaltante: Regione Campania – A.G.C. Ricerca Scientifica, Statistica, Sistemi Informativi ed Informatica – via Don Bosco n. 9/E – Napoli.

Responsabile del procedimento Pastore Eugenio

Telefono: 081/7514954 Fax: 081/7515424;

2. Procedura di aggiudicazione: Appalto concorso ai sensi dell'art. 19, comma 1, lett. b) del D.Lgs. n. 358/92, così come modificato dal D.Lgs 402/98.

3. a) Luogo della consegna: Uffici della Giunta Regionale della Campania;

b) Categoria del servizio e descrizione: Fornitura di un di un Sistema di Sicurezza caratterizzato da una piattaforma di applicazioni e servizi per la gestione avanzata della sicurezza e il controllo delle risorse in rete della Giunta Regionale della Campania, e quant'altro richiesto nel Capitolato Speciale di Appalto e Disciplinare Tecnico che viene pubblicato sul Bollettino Ufficiale della Regione Campania contestualmente al bando;

c) l'offerta deve essere presentata esclusivamente per la totalità della fornitura.

4. Termini ultimi di consegna:

a) Realizzazione: entro 60 (sessanta) giorni naturali, successivi e continui, a partire dalla data di consegna dei lavori.;

5. a)Uffici regionali incaricati di dare informazioni:

- presso il Settore CRED potranno essere richiesti chiarimenti tecnici inerenti la gara;

-presso l'A.G.C. Ricerca Scientifica, Statistica, Sistemi Informativi ed Informatica potranno essere consultabili i documenti amministrativi inerenti la gara;

b) Termine per la richiesta di documenti e/o chiarimenti: fino a dieci giorni prima del termine ultimo per la presentazione delle offerte.

6. Tempi e modalità delle domande e delle offerte:

a) Modalità di presentazione della domanda e dell'offerta: vedi art. 7 del Capitolato Speciale di Appalto;

b) Termine ultimo per la ricezione delle domande: entro il 37° giorno **dalla data di spedizione del bando di gara alla G. U. C. E.;**

c) Termine ultimo per la ricezione delle offerte: entro il 40° giorno successivo alla data di spedizione della lettera di invito;

d) Luogo di presentazione delle offerte: A.G.C. Ricerca Scientifica, Statistica, Sistemi Informativi ed Informatica;

e) Lingua: italiano.

7. a) Persone ammesse ad assistere all'apertura delle offerte economiche: Un legale rappresentante pro-tempore dell'Impresa offerente;

b) Data, ora e luogo dell'apertura delle offerte economiche: verrà comunicata tramite fax a tutte le Ditte invitate.

8. Eventuali cauzioni e garanzie: vedi art. 17 del Capitolato Speciale.

9. Modalità di pagamento: vedi art. 24 del Capitolato Speciale.

10. Alla gara possono partecipare Società, Ditte individuali e Raggruppamenti di Imprese; la forma giuridica che dovrà assumere il Raggruppamento d'Imprese è quella di Raggruppamento Temporaneo di Imprese.

11. Requisiti tecnico- finanziari minimi e Requisiti di legge: vedi art. 5 del Capitolato Speciale.

12. Periodo di tempo durante il quale l'offerente è vincolato alla propria offerta: fino a dodici mesi dalla data di aggiudicazione definitiva.

13. Criteri di aggiudicazione: l'offerta economicamente più vantaggiosa.

14. Altre informazioni:

a. nella domanda le Ditte dovranno indicare la partita IVA;

b. i documenti di tutte le Ditte saranno acquisiti agli atti dell'Ente Appaltante e non saranno restituiti alle Ditte interessate;

c. la richiesta di invito non vincola l'Amministrazione appaltante;

d. si procederà all'aggiudicazione anche nel caso in cui uno solo dei progetti-offerta sarà ritenuto idoneo dalla Commissione Giudicatrice;

e. sarà escluso dalla gara il concorrente che produrrà dichiarazioni non conformi alle prescrizioni e alle norme dettate dal Capitolato Speciale di Appalto e al Disciplinare Tecnico, allegati alla lettera di invito.

15. Data di invio del bando alla G.U.C.E.: 6 febbraio 2003

16. 16. Data di ricevimento del bando: 6 febbraio 2003

17. Data di pubblicazione del bando sul BURC: 10 febbraio 2003

ALLEGATO A

**ASSESSORATO ALL'UNIVERSITA' E
RICERCA SCIENTIFICA, INNOVAZIONE TECNOLOGICA E NUOVA ECONOMIA, SISTEMI INFORMATIVI
E STATISTICA, MUSEI E BIBLIOTECHE**

CAPITOLATO SPECIALE

Appalto-concorso per la fornitura di un Sistema di Sicurezza caratterizzato da una piattaforma di applicazioni e servizi per la gestione avanzata della sicurezza ed il controllo delle risorse in rete della Giunta Regionale della Campania.

Napoli, addì 3/12/2002

ART.37 - FORO COMPETENTE

ART. 1 – OGGETTO DELLA GARA

L'oggetto del presente appalto concorso consiste nell'acquisizione di un Sistema di Sicurezza caratterizzato da una piattaforma di applicazioni e servizi per la gestione avanzata della sicurezza e il controllo delle risorse in rete della Giunta Regionale della Campania (di seguito Regione Campania).

Prerogativa di tale fornitura sarà quella di integrarsi perfettamente con l'infrastruttura di rete preesistente nonché di essere aperta alle probabili evoluzioni dei sistemi in ragione dell'evoluzione tecnologica e delle nuove forme di minaccia che verranno riscontrate.

La fornitura dovrà comprendere e garantire:

a) l'implementazione, in seno all'attuale sistema informatico e telematico della Regione Campania, di una piattaf**orma di applicazioni e servizi** per la gestione della sicurezza ed il controllo delle risorse costituita dalle seguenti componenti di base:

- i s**erver/Workstation** costituenti la piattaforma Hardware del "Sistema" di gestione della sicurezza della Infrastruttura di rete della Regione Campania così come individuati nel Disciplinare Tecnico;

- il Sistema di **Intrusion Detection** (IDS) e Risk Analysis;

- il Sistema di **Antivirus Centralizzato**;

- il Sistema di **Strong Authentication** per tutti gli accessi alle risorse di rete, con l'individuazione dei profili utente e dei privilegi ad essi attribuiti;

- il Sistema di **Configuration Management** centralizzato per tutte le stazioni di lavoro in rete;

- il Sistema di **Content Filtering** intelligente per gli accessi verso Internet;

- il Sistema di A**utenticazione di Dominio** MS e File server Centralizzato;

- il Load Balancing sui Firewall di Front-end a fronte di migliorarne la tolleranza al carico e garantirne la scalabilità per i volumi di utenza futuri;

b) almeno 500 (cinquecento) ore di addestramento del personale della Regione Campania mediante training on the job;

c) la manutenzione in g**aranzia** di tutte le componenti per un anno dall'avvenuto positivo collaudo.

Sono pertanto compresi e garantiti nella fornitura di cui al presente appalto-concorso:

• l'implementazione, in seno all'attuale sistema informatico e telematico della Regione Campania, di una pia**ttaforma di applicazioni e servizi** per la gestione della sicurezza ed il controllo delle risorse costituita dalle seguenti componenti di base:

- i s**erver/Workstation** costituenti la piattaforma Hardware del "Sistema" di gestione della sicurezza della Infrastruttura di rete della Regione Campania, così come individuati nel Disciplinare Tecnico;

- il Sistema di **Intrusion Detection** (IDS) e Risk Analysis;

- il Sistema di **Antivirus Centralizzato**;

- il Sistema di **Strong Authentication** per tutti gli accessi alle risorse di rete, con l'individuazione dei profili utente e dei privilegi ad essi attribuiti;

- il Sistema di **Configuration Management** centralizzato per tutte le stazioni di lavoro in rete;

- il Sistema di **Content Filtering** intelligente per gli accessi verso Internet;

- il Sistema di A**utenticazione di Dominio** MS e File server Centralizzato;

- il Load Balancing sui Firewall di Front-end a fronte di migliorarne la tolleranza al carico e garantirne la scalabilità per i volumi di utenza futuri;

• almeno 500 (cinquecento) ore di addestramento del personale della Regione Campania mediante training on the job;

• la manutenzione in gar**anzia** di tutte le componenti per un anno dall'avvenuto positivo collaudo.

E' a carico dell'aggiudicatario, e compreso nell'importo dell'appalto, anche quanto segue:

• l'installazione, allacciamento, stoccaggio, collegamento ed avviamento dei prodotti, attrezzature o programmi, tutto incluso e nulla escluso, per rendere completo e funzionale l'intera fornitura;

• le risorse umane e i materiali di consumo necessari alla installazione e configurazione dei prodotti hardware e software;

• la fornitura di dettagliate descrizioni tecniche e manuali d'uso, sia su carta che su supporto magnetico, idonei ad assicurare una completa conoscenza dei prodotti hardware e software;

• l'imballaggio, il trasporto nel rispetto della normativa vigente, la pulizia dei locali oggetto degli interventi ed in generale tutto quanto necessario, nulla escluso, per la consegna chiavi in mano dell'intera fornitura.

ART. 2 – CORRISPETTIVO DELL'APPALTO

L'importo presunto per il presente appalto "chiavi in mano" è determinato in Euro 610.000,00, oltre IVA.

Il corrispettivo di aggiudicazione sarà quello risultante dall'offerta prescelta e sono escluse offerte in aumento.

ART. 3 – FORME DI ACQUISIZIONE E DOCUMENTAZIONE

Tutte le apparecchiature hardware sono acquisite in proprietà dalla Regione Campania.

Il software di sistema e di base sarà acquisito in licenza d'uso a tempo illimitato.

Il software applicativo utilizzato per l'implementazione dei Sistemi richiesti sarà acquisito in proprietà dalla Regione Campania all'atto dell'avvenuto positivo collaudo senza oneri finanziari e/o economici aggiuntivi per l'Ente.

Tutto il software applicativo potrà essere costituito da software già prodotto, da COTS (componenti in commercio acquisiti dal mercato) e da componenti che verranno sviluppate ad hoc per la Regione Campania, richiedendosi altresì che:

• per le componenti già prodotte, la Regione Campania acquisisca tutti i diritti eccetto quello di cessione a terzi;

• per i COTS, la Regione Campania acquisisca la licenza d'uso per un periodo illimitato. Qualora tale diritto non sia riconosciuto dal produttore di un COTS, la licenza d'uso si intende rilasciata almeno fino alla fine della fornitura del Servizio;

• per le componenti prodotte ad hoc, la Regione Campania acquisisca il diritto di proprietà e, per l'effetto, tutti diritti e facoltà provenienti dall'esclusività del diritto stesso.

La Ditta aggiudicataria dovrà fornire alla Regione Campania la documentazione descrittiva di tutte le componenti del software di base e del software applicativo utilizzati per la presente fornitura, su supporto cartaceo e CD-ROM. Per tutte le componenti del software applicativo dovrà essere consegnato, oltre ai documenti e i deliverables del processo di produzione del software, il codice sorgente.

ART. 4 – TEMPI DI REALIZZAZIONE

L'intero appalto deve essere realizzato nell'arco temporale di 60 (sessanta) giorni naturali, successivi e continui, a partire dalla data di consegna dei lavori. Tale data deve risultare da apposito verbale di consegna lavori, debitamente sottoscritto dai rappresentanti delle parti. Tale adempimento iniziale deve avvenire entro e non oltre il termine massimo di 30 (trenta) giorni naturali, successivi e continui a far data dalla comunicazione scritta da parte della Regione Campania di avvenuta aggiudicazione dell'appalto.

La sede di trattazione tecnica e di riferimento è l'Area di Ricerca Scientifica (Settore "C.R.E.D."), precisamente, Via Don Bosco 9/E – Napoli.

La Regione Campania, in ottemperanza della Legge 241/1990, ha designato il Responsabile del Procedimento che rappresenterà l'Ente per gli adempimenti connessi a tale appalto.

ART. 5 – REQUISITI PER LA PARTECIPAZIONE ALL'APPALTO

1. Requisiti tecnico-finanziari

Saranno ammesse a partecipare alla gara di appalto per l'acquisizione del servizio le Ditte che dimostreranno di possedere i seguenti requisiti di capacità finanziaria e tecnica:

a) fatturato, a netto di IVA, di almeno 2.000.000,00 Euro nell'ultimo triennio, per attività di sviluppo ed implementazione conto terzi di Sistemi hardware e Software;

b) fatturato, a netto di IVA, di almeno 1.000.000,00 Euro nell'ultimo triennio, per forniture di Sistemi di gestione della sicurezza delle intranet;

c) aver fornito e gestito nell'ultimo triennio almeno un Sistema per la gestione della Sicurezza di dimensioni comparabili al Sistema oggetto del presente appalto;

d) possedere una certificazione ISO 9000 per tutte le tipologie di servizi offerti.

2. Requisiti di legge

Per essere ammessa a partecipare alla gara la Ditta interessata deve produrre una domanda di partecipazione, redatta su carta legale e sottoscritta dal titolare o dal legale rappresentante pro-tempore dell'Impresa ed autenticata con le modalità di cui è al DPR 445/2000 e successive modificazioni ed integrazioni, nella quale si attesta:

a. di non trovarsi e di essere in regola rispettivamente con quanto previsto dalle lettere a), b), c), d), e), f), di cui all'art. 11 del D.Lgs 358/92, così come modificato dal D.Lgs 402/98;

b. di non essere stato sottoposto a misure di prevenzione e di non essere a conoscenza dell'esistenza a suo carico e dei propri conviventi di procedimenti in corso per l'applicazione di una delle misure di prevenzione di cui alla L.55/90 e di trovarsi nella capacità di contrattare con le PP.AA. (Pubbliche Amministrazioni);

c. di essere iscritta alla CCIAA (Camera di Commercio Industria Artigianato e Agricoltura) da almeno un triennio per le attività oggetto dell'appalto;

d. l'accettazione incondizionata di tutte le clausole previste dal bando;

e. di aver preso visione del Capitolato Speciale di Appalto e del relativo Disciplinare Tecnico quale parte integrante del Capitolato stesso e di accettarne senza riserva alcuna tutte le condizioni;

f. di trovarsi nelle condizioni di cui alle lettere a), b), c), d), del precedente punto 1. relativo ai requisiti tecnico-finanziari.

ART. 6 – PERIODO DURANTE IL QUALE L'OFFERENTE E' VINCOLATO ALLA PROPRIA OFFERTA

Fino a 12 (dodici) mesi dalla data dell'aggiudicazione definitiva ai sensi e agli effetti dell'art. 1329 c.c..

ART. 7 – MODALITA' E TERMINI DI PRESENTAZIONE DELLA DOMANDA E DELL'OFFERTA

Sono ammesse a partecipare alla preselezione le Ditte che, ritenendosi in possesso di tutti i requisiti prescritti dal presente Capitolato, faranno pervenire, alla Regione Campania – A.G.C. Ricerca Scientifica, Statistica, Sistemi Informativi ed Informatica – via Don Bosco n. 9/E – Napoli, a mezzo servizio postale con raccomandata A.R. o anche con consegna a mano purché l'affrancatura sia stata preventivamente annullata dall'ufficio postale, domanda di partecipazione, con indicazione del mittente e la scritta **"Domanda di partecipazione per l'appalto-concorso per la fornitura di un Sistema di Sicurezza caratterizzato da una piattaforma di applicazioni e servizi per la gestione avanzata della sicurezza ed il controllo delle risorse in rete della Giunta Regionale della Campania",** entro il 37° giorno (trentasettesimo) giorno dalla data di spedizione del bando di gara per la pubblicazione sulla Gazzetta Ufficiale della Comunità Europea. In conformità con le prescrizioni del bando, le domande devono essere corredate dagli elementi necessari ai fini della scelta dei soggetti da invitare.

Possono presentare offerte le Ditte invitate al seguito della preselezione di cui sopra. Le offerte, redatte in conformità con il presente Capitolato, vanno racchiuse in un plico sigillato con ceralacca e firmato sui lembi di chiusura, con indicazione del mittente e la seguente scritta: "**Offerta per** l'**appalto-concorso per la fornitura di Sistema di Sicurezza caratterizzato da una piattaforma di applicazioni e servizi per la gestione avanzata della sicurezza ed il controllo delle risorse in rete della Giunta Regionale della Campania",** nel quale dovranno essere inseriti:

a) una busta contenente l'autocertificazione attestante il possesso dei requisiti di capacità finanziaria e tecnica prescritti nel presente Capitolato in conformità a quanto previsto dagli artt. 13 e 14 del D.Lgs 358/92, così come modificato dal D.Lgs 402/98. Tale documentazione non dovrà in alcun modo riportare indicazione sui costi, pena esclusione;

b) una busta, contenente l'offerta tecnica, sigillata con ceralacca e controfirmata sui lembi di chiusura, con l'indicazione del mittente e l'oggetto della gara. L'offerta tecnica, regolarmente sottoscritta in tutte le sue parti, deve contenere, pena esclusione:

• presentazione della Ditta e referenze generali e specifiche, con particolare riferimento a soluzioni analoghe a quelle previste dal presente Appalto;

• elenco in cui siano puntualmente identificati tutti gli oggetti componenti il Servizio;

• Progetto Tecnico, che deve includere appositi e specifici capitoli:

- la descrizione dettagliata delle caratteristiche tecniche delle apparecchiature offerte;

- la descrizione tecnica e funzionale del Sistema Intrusion Detection;

- la descrizione tecnica e funzionale del Sistema Antivirus Centralizzato;

- la descrizione tecnica e funzionale del Sistema di Strong Authentication;

- la descrizione tecnica e funzionale del Sistema di Configuration Management;

- la descrizione tecnica e funzionale del Sistema di Content Filtering;

- la descrizione tecnica e funzionale del Sistema di Autenticazione di Dominio;

- il Piano di implementazione del Load Balancing sui Firewall di Front-end;

- il Piano dettagliato delle modalità di integrazione dei nuovi apparati sull'infrastruttura intranet preesistente;

- il Piano di addestramento del personale della Regione Campania con le modalità di cui al presente Appalto;

- il Piano di installazione, messa in esercizio, configurazione, fornitura e posa in opera di ogni componente software e hardware dell'intera fornitura;

• la dichiarazione con la quale i concorrenti attestano:

• di aver esaminato gli elaborati di gara;

• di essersi recati sul luogo di esecuzione dei lavori;

• di aver preso conoscenza delle condizioni locali e delle eventuali preesistenze utilizzabili ai fini della implementazione del Sistema richiesto, nonché di tutte le circostanze generali e particolari suscettibili di influire sulla determinazione dei prezzi, sulle condizioni contrattuali e sulla fornitura dell'appalto;

• di essere a conoscenza dell'infrastruttura Intranet della Giunta Regionale della Campania e che questa può essere messa in completa sicurezza grazie alla soluzione tecnica proposta;

• di aver giudicato il Servizio attuabile, gli elaborati di gara adeguati ed il prezzo a base della gara remunerativo e tale da indurre offerte in ribasso.

L'offerta tecnica dovrà essere corredata da tutta la documentazione tecnica ritenuta opportuna per la sua corretta valutazione. Per consentire una migliore consultazione, l'offerta tecnica dovrà essere fornita anche in formato elettronico PDF e non dovrà in alcun modo riportare indicazioni sui costi, pena esclusione;

c) una busta, contenente l'offerta economica, sigillata con ceralacca e controfirmata sui lembi di chiusura con l'indicazione del mittente e l'oggetto della gara. L'offerta economica, regolarmente sottoscritta, deve essere redatta in carta da bollo e in lingua italiana e, pena esclusione, deve contenere l'importo complessivo richiesto per la fornitura "chiavi in mano" dell'appalto, espresso in cifre e in lettere al netto di IVA, nonché la sua ripartizione nei singoli importi espressi in cifra ed in lettere, al netto di IVA, relativi ai singoli sottosistemi offerti (alias elenco prezzi). Nel caso di discordanza tra un importo in cifre ed il suo corrispondente in lettere farà fede quest'ultimo. In caso di discordanza tra l'importo complessivo e la sommatoria dei singoli importi farà fede l'importo più vantaggioso per l'Amministrazione. Tale plico dovrà pervenire, a pena di esclusione, all'A.G.C. Ricerca Scientifica, Statistica, Sistemi Informativi ed Informatica entro il 40° (quarantesimo) giorno successivo alla data di spedizione della lettera d'invito.

Fino a 10 (dieci) giorni prima del termine ultimo per la presentazione delle offerte sarà possibile richiedere chiarimenti e/o consultare documenti tecnici e/o amministrativi rispettivamente presso il CRED e l'A.G.C. Ricerca Scientifica, Statistica, Sistemi Informativi ed Informatica.

Alla gara possono partecipare società, Ditte individuali e raggruppamenti di imprese.

Nel caso del raggruppamento apposito e temporaneo di imprese:

• l'offerta congiunta deve essere sottoscritta da tutte le imprese appositamente e temporaneamente raggruppate e contenere l'impegno che, in caso di aggiudicazione, le stesse imprese si conformeranno interamente e letteralmente alla normativa di cui all'art. 10 del D. Lgs. n. 358/92, così come modificato dal D.Lgs 402/98;

• con riferimento ai requisiti di cui al punto 1 dell'art. 5 del presente Capitolato:

- il requisito a) deve essere posseduto in misura non inferiore al 80% da una delle Ditte partecipanti al raggruppamento;

- il requisito b) deve essere posseduto in misura non inferiore al 80% da almeno una delle Ditte partecipanti al raggruppamento;

- il requisito c) deve essere posseduto da almeno una delle Ditte partecipanti al raggruppamento;

- la certificazione ISO 9000 (requisito d)) deve essere posseduta da tutte le Ditte partecipanti e deve essere tale che l'oggetto della certificazione posseduta da ciascuna Ditta includa la fornitura di beni e servizi che competono ad essa nell'ambito del raggruppamento;

• le Ditte partecipanti al raggruppamento dovranno presentare in sede di offerta, per quanto di propria competenza, l'autocertificazione attestante che il raggruppamento possiede, nei termini su indicati, i requisiti di cui all'art. 5.

L'Amministrazione si riserva di verificare, in ogni tempo, la rispondenza delle dichiarazioni e certificazioni prodotte con i requisiti di legge, tecnici e finanziari posseduti.

Nessun compenso e rimborso spetta alle Ditte offerenti per la predisposizione del progetto-offerta e per la presentazione di documenti e di quant'altro ritenuto utile ai fini della migliore valutazione dell'offerta.

ART. 8 – DOCUMENTAZIONE RICHIESTA ALLA DITTA AGGIUDICATARIA

La Ditta aggiudicataria dovrà produrre le seguenti certificazioni:

a) cauzione di cui è all'art. 17 del presente Capitolato;

b) atto notarile attestante la costituzione dell'associazione temporanea di impresa, se del caso.

L'Amministrazione provvederà all'aggiudicazione definitiva solo dopo la verifica della sussistenza dei requisiti di cui è all'art. 5.

Qualora le verifiche risultassero insoddisfacenti, l'Amministrazione procederà ad aggiudicare l'affidamento dell'appalto alla Ditta che segue in graduatoria, fermo restante analoga verifica.

ART. 9 – DATA DI SPEDIZIONE ALLA GAZZETTA UFFICIALE DELLE COMUNITA' EUROPEE

Il bando relativo alla presente gara di appalto è stato spedito alla Gazzetta Ufficiale delle Comunità Europee in data **6 febbraio 2003**.

ART. 10 – MODALITA' DI CONFERIMENTO DELL'APPALTO

La gara sarà espletata con le modalità dell'appalto concorso e sarà aggiudicata a favore dell'offerta economicamente più vantaggiosa ai sensi e agli effetti dell'art. 19, comma 1, lett. b) del D.Lgs. n. 358/92, così come modificato dal D.Lgs 402/98, con le modalità espresse nel seguito.

L'aggiudicazione della fornitura sarà effettuata a giudizio insindacabile dell'Amministrazione Regionale, con provvedimento amministrativo, su proposta della Commissione Giudicatrice, di cui è all'art. 11 del presente Capitolato, all'uopo costituita.

La Commissione, cui compete di formulare la proposta di aggiudicazione, escluderà tutte le Ditte che avranno prodotto un progetto-offerta ritenuto inadeguato rispetto alle specifiche definite nel presente Capitolato e nel Disciplinare Tecnico. La Commissione, per individuare l'offerta più vantaggiosa, formulerà una graduatoria tra i soli progetti-offerta ritenuti idonei.

La fornitura sarà aggiudicata anche nel caso in cui uno solo dei progetti-offerta pervenuti sarà ritenuto idoneo dalla Commissione.

Ciascuna offerta sarà inclusa nella graduatoria in base ad un punteggio risultante dalla somma di due distinti punteggi parziali, detti, rispettivamente, punteggio tecnico e punteggio economico.

Calcolo del punteggio tecnico

Il punteggio tecnico dell'offerta sarà calcolato in funzione del suo valore tecnico, che è la misura in cui il progetto tecnico definitivo dell'offerta risponde ad un predefinito insieme di criteri di valutazione.

Per calcolare il valore tecnico la Commissione, per ciascun criterio di valutazione, esprimerà il livello di soddisfacimento mediante un punteggio variabile in base al tipo di criterio. Nel seguito sono elencati i punteggi massimi attribuibili per ognuno dei criteri. Il totale del punteggio raggiunto costituirà il valore tecnico dell'offerta. Alla Ditta che avrà conseguito il valore tecnico più alto verrà attribuito il punteggio tecnico di 70 ed alle altre Ditte un punteggio tecnico decrescente e proporzionale al valore tecnico conseguito.

I criteri che saranno utilizzati per calcolare il valore tecnico dell'offerta sono i seguenti:

• qualità e completezza della descrizione dettagliata delle caratteristiche tecniche delle apparecchiature offerte (max. 20 punti);

• qualità e completezza della descrizione tecnica e funzionale del Sistema di Intrusion Detection (max. 20 punti);

• qualità e completezza della descrizione tecnica e funzionale del Sistema Antivirus Centralizzato (max. 20 punti);

• qualità e completezza della descrizione tecnica e funzionale del Sistema di Strong Authentication (max. 20 punti);

• qualità e completezza della descrizione tecnica e funzionale del Sistema di Configuration Management (max. 20 punti);

• qualità e completezza della descrizione tecnica e funzionale del Sistema di Content Filtering (max. 20 punti);

• qualità e completezza della descrizione tecnica e funzionale del Sistema di Autenticazione di Dominio (max. 20 punti);

• qualità e completezza del Piano di implementazione del Load Balancing sui Firewall di Front-end (max. 20 punti);

• qualità e completezza del Piano dettagliato delle modalità di integrazione dei nuovi apparati sull'infrastruttura intranet preesistente (max. 20 punti);

• qualità e completezza del Piano di addestramento del personale della Regione Campania (max. 30 punti);

• qualità e completezza del Piano di installazione, messa in esercizio, configurazione, fornitura e posa in opera di ogni componente software e hardware (max. 30 punti).

La Commissione riterrà non idonei quei progetti offerta che dovessero ottenere un valore tecnico inferiore al 60% della somma dei punteggi massimi definiti per i criteri sopra riportati. Verranno, altresì, ritenuti non idonei progetti-offerta che dovessero ottenere anche in uno solo dei criteri elencati, un punteggio inferiore al 40% del numero massimo di punti previsti per lo specifico criterio.

Calcolo del punteggio economico

Terminate le operazioni per l'attribuzione del punteggio tecnico delle offerte, la Commissione procederà all'apertura delle buste contenenti le offerte economiche delle sole Ditte il cui progetto-offerta è risultato idoneo e attribuirà a dette offerte il punteggio economico calcolato, per ogni offerta, con la seguente formula:

$Po = (30 \times Ioem / Io)$

Dove:

Po = Punteggio dell'offerta

30 = Punteggio da attribuire alla Offerta Economica Minima per l'intera fornitura

Ioem = Importo dell'Offerta Economica Minima

Io = Importo della Generica Offerta Economica per l'intera fornitura

Terminate anche le operazioni per l'attribuzione del punteggio economico, la Commissione costruirà la graduatoria delle Ditte sulla base della somma dei punteggi tecnici ed economici e proporrà di aggiudicare l'appalto a favore della Ditta che avrà ottenuto il massimo punteggio e che quindi avrà formulato l'offerta ritenuta più vantaggiosa. A parità di punteggio complessivo si proporrà l'aggiudicazione a favore della Ditta che avrà il maggiore punteggio tecnico. A parità anche del punteggio tecnico si procederà a sorteggio.

L'Amministrazione si riserva la facoltà di chiedere alla Ditta che avrà presentato l'offerta prescelta, l'inserimento di tutte le varianti che riterrà necessarie per rendere il Servizio proposto più confacente alle proprie esigenze.

L'aggiudicazione non è impegnativa che per la sola Ditta aggiudicataria.

Ai sensi del D.Lgs. 358/1992, così come modificato dal D.Lgs 402/98, in caso di offerta economica manifestamente ed anormalmente bassa, l'Amministrazione si riserva di richiedere all'Impresa, prima dell'aggiudicazione definitiva, tutte le giustificazioni del caso e, qualora queste non siano ritenute valide e sufficienti, si riserva altresì la facoltà di rigettare l'offerta, escludendo la detta Impresa dalla gara. Si precisa che la Regione Campania riterrà anormalmente bassa l'offerta che presenti una percentuale di ribasso superiore ad un quinto della media aritmetica dei ribassi delle offerte ammesse.

Qualora tutte le offerte prodotte dalle Ditte concorrenti risultino inappropriate, l'Amministrazione si riserva la facoltà, ai sensi e agli effetti dell'art. 9, comma 4, del D.Lgs. 358/1992, così come modificato dal D.Lgs. 402/98, di aggiudicare a trattativa privata la presente fornitura.

L'Amministrazione si riserva, infine, la facoltà di non procedere all'aggiudicazione.

ART. 11 - COMMISSIONE GIUDICATRICE

L'Amministrazione Regionale, provvederà a costituire la Commissione Giudicatrice entro 20 giorni solari dalla scadenza per la presentazione delle offerte.

Art. 12 - CERTIFICAZIONE

Prima della consegna dei prodotti oggetto della fornitura dovrà essere rilasciato un certificato di garanzia attestante l'originalità dei prodotti, che gli stessi sono nuovi di fabbricazione e d'uso e che possono essere liberamente forniti dall'aggiudicatario.

La Ditta dovrà, altresì, presentare le licenze d'uso illimitate per i prodotti già presenti sul mercato a favore dell'Ente Regione.

ART. 13 - RISPONDENZA ALLE NORMATIVE

L'appalto è soggetto alla piena ed intera osservanza di tutte le norme di leggi, decreti e regolamenti vigenti o che siano emanati in corso d'opera per appalti di forniture di beni e servizi.

In particolare le apparecchiature oggetto della fornitura dovranno essere conformi alla normativa vigente in materia di sicurezza e di sanità (legge n. 626/94, D.Lgs n. 494/96 e legge n. 46/90 e loro modificazioni e/o integrazioni) ed alle seguenti prescrizioni di carattere tecnico-normativo:

- progettate e costruite secondo le norme tecniche di sicurezza europee EN 60950;
- Conformi ai requisiti ergonomici di usabilità secondo i parametri tecnici della norma ISO 9241 parte 3;
- Conformi alle norme EN 55022 ed EN50082-1 relative ai radiodisturbi;
- Conformi alla norma EPA per il risparmio energetico.

Tutti i sistemi, inoltre, dovranno essere conformi alla Circolare Ministeriale N. 51223 del 21/5/1990 relativa agli "Indirizzi di normalizzazione nell'area delle tecnologie dell'informazione nella P.A.".

Tutte le lavorazioni per la realizzazione dell'intera fornitura dovranno essere eseguite nel pieno rispetto di tutta la normativa vigente in materia di sicurezza.

Conseguentemente la Ditta aggiudicataria dovrà fornire tutte le prescritte certificazioni per i componenti la fornitura.

ART. 14 - BREVETTI E DIRITTI D'AUTORE

L'Amministrazione non assume alcuna responsabilità nel caso che la Ditta abbia usato, nell'esecuzione della fornitura, dispositivi o soluzioni tecniche di cui altri abbiano ottenuto la privativa.

La Ditta aggiudicataria, pertanto, dovrà assumersi tutte le responsabilità eventualmente derivanti dall'adozione di dispositivi o soluzioni tecniche che violino brevetti e diritti di autore, sollevandone espressamente l'Amministrazione.

La Ditta assume l'obbligo di tenere indenne l'Amministrazione da tutte le rivendicazioni, le responsabilità, le perdite e i danni pretesi da qualsiasi persona, nonché da tutti i costi, le spese o le responsabilità ad essi relativi (compresi gli onorari di avvocati in equa misura) a seguito di qualsiasi marchio italiano o straniero, derivante o che si pretendesse derivare dalla fabbricazione, vendita, gestione od uso di uno o più prodotti oggetto della presente fornitura.

Ciascuna parte si obbliga a dare immediato avviso all'altra di qualsiasi azione di rivendicazione o questione di terzi, di cui al precedente comma, di cui sia venuto a conoscenza.

Qualora il fornitore riceva comunicazione scritta di qualsiasi azione o rivendicazione per la quale esso sia tenuto a lasciare indenne l'Amministrazione, il fornitore garantisce, senza limitazione alcuna e a proprie spese, l'Amministrazione contro tali azioni o rivendicazioni e pagherà i costi, i danni e gli onorari degli avvocati posti a carico dell'Amministrazione in qualsiasi di tali azioni o rivendicazioni, fermo restando che il fornitore avrà il diritto di essere sentito circa l'eventualità di tali azioni o rivendicazioni. L'Amministrazione può svolgere a spese del fornitore tutti i passi che potranno essere ragionevolmente richiesti dal fornitore in relazione a tali transazioni o difese.

Nel caso di sentenza provvisoria o definitiva contro l'uso o la gestione da parte dell'Amministrazione di una o più componenti hardware e/o software oggetto del presente appalto, a causa di pretesa violazione, ovvero nel caso in cui, a parere del fornitore, vi siano possibilità che uno o più componenti dell'intera fornitura siano oggetto di rivendicazione per violazione, il fornitore, a sua responsabilità e a sue spese, potrà:

• modificare il componente e/o i componenti in modo da eliminare la violazione;

• ottenere per l'Amministrazione il diritto di continuare la fornitura del Servizio;

• sostituire il componente e/o i componenti in violazione con altri aventi la stessa capacità e che, in ogni caso, soddisfino le esigenze dell'Amministrazione, garantendo tutte le possibili prestazioni svolte o da svolgere con essi sino alla data in cui verranno esercitate tali rivendicazioni, secondo la soluzione meno impegnativa.

• Ritirare il componente e/o i componenti e rifondere le somme versate al fornitore, salvo una adeguata riduzione per l'uso, i danni e l'obsolescenza.

ART. 15 – RISCHI

Sono a carico del fornitore i rischi di perdite e di danni durante il trasporto dei prodotti ordinati e la sosta presso l'Amministrazione ad eccezione delle perdite e dei danni imputabili all'Amministrazione.

ART. 16 – DANNI

Nei casi di danni, deterioramenti o perdite totali o di parte delle apparecchiature, con conseguente loro indisponibilità, a causa di forza maggiore o per eventi non imputabili all'Amministrazione, al fornitore non è dovuto alcun indennizzo, rimborso spese o corrispettivo, inoltre:

• l'Amministrazione assume l'obbligo di informare il fornitore immediatamente, anche per telefono, e comunque non oltre 24 ore, dal momento in cui ha avuto conoscenza del verificarsi dell'evento dannoso;

• Il fornitore per contro, assume l'obbligo di intervenire per riparare le apparecchiature guaste o deteriorate o sostituire quelle non più utilizzabili subito dopo la cessazione delle cause che hanno provocato i danni, entro un termine da determinarsi d'intesa con l'Amministrazione;

• l'Amministrazione potrà utilizzare le apparecchiature poste progressivamente in condizioni di funzionamento.

ART. 17 - DEPOSITO DI GARANZIA

La Ditta aggiudicataria dovrà, ai sensi della normativa vigente, presentare all'A.G.C. Ricerca Scientifica, Statistica, Sistemi Informativi ed Informatica della Giunta Regionale della Campania una cauzione che sarà costituita da polizza assicurativa o fideiussione bancaria irrevocabile, incondizionata ed escutibile a prima richiesta a favore della Regione Campania, di importo pari al 10% di quello di aggiudicazione. La cauzione resterà vincolata fino alla scadenza del periodo di garanzia, e comunque non prima che siano state definite tutte le eventuali contestazioni e vertenze che fossero in corso tra le Parti.

Lo svincolo della cauzione verrà effettuato a domanda e a spese dell'Impresa aggiudicataria, nella quale la medesima dichiarerà di non aver altro da pretendere dall'Amministrazione.

ART. 18 - STIPULA DEL CONTRATTO

Il contratto dovrà essere stipulato entro 45 (quarantacinque) giorni naturali, successivi e continui a far data dalla comunicazione scritta da parte della Regione Campania di avvenuta aggiudicazione dell'appalto.

La Ditta aggiudicataria dovrà presentarsi per la stipula del contratto entro il termine assegnato con la lettera di notifica dell'aggiudicazione.

Faranno parte integrante del contratto il presente Capitolato con relativo Disciplinare Tecnico, ed il progetto-offerta presentato dalla Ditta.

ART. 19 – COLLAUDO

L'Amministrazione regionale provvederà con apposita Commissione di cui al successivo art. 20 ad effettuare il collaudo in corso d'opera del sistema. Il collaudo è finalizzato alla verifica che il Sistema risponda a quanto previsto in sede di offerta e nei successivi documenti progettuali predisposti durante la sua realizzazione.

Le operazioni di collaudo saranno condotte dai tecnici della Ditta, senza oneri aggiuntivi per l'Amministrazione Regionale, alla presenza della Commissione che dovrà rilasciare il certificato di avvenuto positivo collaudo.

Le operazioni di collaudo dovranno essere definite preventivamente in un Piano di Collaudo predisposto dalla Ditta e accettato dalla Commissione. In caso di non superamento, anche parziale, del collaudo, la Ditta dovrà provvedere entro ulteriori 10 (dieci) giorni solari ad effettuare i lavori necessari e/o fornire quanto necessario al superamento del collaudo. Trascorso tale termine l'Amministrazione applicherà una penale pari a Euro 1.000,00 per ogni giorno di ritardo. Qualora le penali raggiungano

l'importo di Euro 16.000,00 l'Amministrazione si riserva di avvalersi sulla cauzione per il danno subito e di avviare contestualmente le procedure per la risoluzione del contratto ai sensi dell'art. 1662 c.c., comma 2.

ART. 20 - COMMISSIONE DI COLLAUDO

L'Amministrazione provvederà a nominare, entro 20 giorni solari dalla dall'aggiudicazione definitiva, la Commissione Regionale di Collaudo composta da tre tecnici di specifica qualificazione professionale commisurata alla tipologia e categoria degli interventi, alla loro complessità ed all'importo.

La Commissione di collaudo nell'esercizio delle sue attività dovrà avvalersi della struttura di Help Desk di cui è dotato l'Ente Regione Campania.

La Commissione dovrà rimettere all'Amministrazione, entro 30 (trenta) giorni lavorativi dalla comunicazione scritta di pronto per la messa in esercizio dell'intero Sistema fatta dalla Ditta aggiudicataria, il certificato di collaudo finale.

ART. 21 - DIREZIONE DEI LAVORI

L'Amministrazione si riserva la facoltà di istituire un ufficio per la direzione dei lavori.

ART. 22 – RESPONSABILITA' DELL'APPALTO

La Ditta è responsabile per ogni parte, nessuna esclusa o riservata, della redazione del progetto e della sua esecuzione, nonché dell'attività di formazione ai dipendenti dell'Ente.

Restano a carico della Ditta tutte le attività, e gli eventuali oneri economici consequenziali, per l'attuazione di quanto disposto dalla normativa vigente (legge 46/90, legge 626/94, D. lgs. 494/96, etc.) in materia di sicurezza sui lavori per tutte le fasi di espletamento dell'intero Servizio.

La Ditta aggiudicataria, ad aggiudicazione avvenuta, provvederà a nominare un proprio Responsabile con la precisa responsabilità di seguire tutte le fasi di realizzazione, di esecuzione, di formazione e di verifica dell'intero Sistema nel rispetto di tutte le norme di leggi, decreti e regolamenti italiani e comunitari vigenti o che siano emanati in corso d'opera, per gli appalti di che trattasi.

ART. 23 – SUBAPPALTO

Per il subappalto della presente fornitura si rinvia all'art.18, lex 55/1990 e successive modifiche ed integrazioni.

La Ditta è tenuta ad indicare in sede di offerta i servizi e gli interventi che intende subappaltare; la mancanza di tale indicazione comporterà, in caso di aggiudicazione, l'impossibilità di ottenere l'autorizzazione al subappalto.

ART. 24 - MODALITA' E CONDIZIONI DI PAGAMENTO

Il pagamento del corrispettivo dell'appalto avverrà con le seguenti modalità:

- l'intero importo sarà corrisposto, previa presentazione di regolare fattura al Settore CRED dell'A.G.C. Ricerca Scientifica ed Informatica, al rilascio del certificato di avvenuto positivo collaudo definitivo dell'intera fornitura.

ART. 25 – PENALI

In caso di ritardata esecuzione della realizzazione del Sistema rispetto ai tempi previsti, l'Amministrazione applicherà una penale pari a Euro 2.000,00 per ogni giorno di calendario di ritardo fino ad un massimo di Euro 60.000,00 oltre il quale l'Amministrazione si riserva di avvalersi sulla cauzione e di avviare le procedure per la risoluzione del contratto (ex art. 1662 c.c., comma 2).

ART. 26 - RISERVATEZZA

La Ditta aggiudicataria assumerà l'obbligo di agire in modo che il proprio personale dipendente, incaricato di eseguire le prestazioni contrattuali, mantenga riservati i dati e le informazioni, comprese quelle sui programmi, di cui venga in possesso, non li rilevi senza ordine della legittima autorità, non li divulghi e non ne faccia oggetto di sfruttamento (Legge 675/96).

La Ditta aggiudicataria avrà la responsabilità di attuare le operazioni di sicurezza sui dati e sui programmi mediante la duplicazione e il mantenimento di copie delle banche dati, delle registrazioni statistiche e di qualsiasi altra informazione necessaria per la fornitura del servizio e della sua continuità. La Ditta aggiudicataria si farà, altresì, carico dell'integrità fisica dei dati di proprietà esclusiva dell'Ente, perdite e calamità o per ogni evento distruttivo.

ART. 27 - ONERI A CARICO DELL'AMMINISTRAZIONE

L'Amministrazione si impegna a rendere disponibili i locali per la installazione delle componenti HW oggetto della fornitura.

E', invece, a carico della Ditta aggiudicataria quant'altro necessario per la realizzazione, per la esecuzione e per il corretto funzionamento dell'intera fornitura, ivi incluso lo stoccaggio dei materiali.

ART. 28 – RISOLUZIONE

Il rapporto contrattuale viene risolto "ipso iure" nei seguenti casi:

• sospensione della prestazione per fatto dell'Impresa aggiudicataria;

• fallimento dell'Impresa aggiudicataria o della mandataria;

• mancata costituzione del deposito di garanzia;

• non veridicità di parte o di tutto quanto contenuto nel progetto-offerta;

• inadempienza alle clausole e condizioni del contratto ai sensi dell'art. 1453 e successivi del codice civile;

• nei casi previsti dall'art. 37, 1° comma, del Capitolato Generale dello Stato.

La risoluzione nei casi previsti dal presente articolo comporta come conseguenza l'incameramento a titolo di penale della cauzione prestata, salvo il risarcimento dei maggiori danni consequenziali.

ART. 29 - ESECUZIONE IN DANNO

In caso di risoluzione, revoca o di grave inadempienza dell'Impresa aggiudicataria, l'Amministrazione si riserva il diritto di affidare a terzi la realizzazione di quanto oggetto dell'appalto con addebito della differenza a carico della Impresa stessa.

L'affidamento avviene con trattativa privata o, entro i limiti prescritti, in economia, stante l'esigenza di limitare le conseguenze dei ritardi connessi con la risoluzione del contratto.

L'affidamento a terzi viene notificato all'Impresa aggiudicataria inadempiente nelle forme prescritte con l'indicazione dei nuovi termini di esecuzione degli incarichi affidati e degli importi relativi.

All'Impresa aggiudicataria inadempiente sono addebitate le spese sostenute in più dall'Amministrazione rispetto a quelle previste dal contratto risolto.

Esse sono prelevate da eventuali crediti dell'Impresa.

Nel caso di minore spesa, nulla compete all'Impresa aggiudicataria inadempiente.

L'esecuzione in danno non esime l'Impresa dalle responsabilità civili e penali in cui la stessa possa incorrere a norma di legge per i fatti che hanno motivato la risoluzione.

ART. 30 - OBBLIGHI E RESPONSABILITA'

La Ditta aggiudicataria ha l'obbligo di segnalare immediatamente tutte quelle circostanze e fatti che, rilevanti nell'espletamento del suo compito, possano pregiudicare il regolare svolgimento dei servizi. Inoltre, si obbliga a rilevare l'Amministrazione da qualunque azione che possa esserle attentata da terzi o per mancato adempimento degli obblighi contrattuali o per trascuratezza o colpa nell'adempimento dei medesimi.

La Ditta aggiudicataria è esclusiva responsabile dell'osservanza di tutte le disposizioni normative e legislative italiane e comunitarie relative alla realizzazione e all'installazione dell'intero Sistema nonché alla tutela infortunistica del proprio personale addetto ai lavori di cui all'appalto. E' fatto carico alla Ditta aggiudicataria di dare piena attuazione agli obblighi delle assicurazioni sociali e ad ogni patto di lavoro stabilito per il personale stesso, ivi compreso quello economico nazionale di categoria.

ART. 31 – INVARIABILITA' DEI PREZZI

Nei prezzi offerti e contrattualmente fissati si intendono compresi e compensati tutti gli oneri di cui all'appalto, tutto incluso e nulla escluso, per la completa attuazione dell'appalto. La Ditta aggiudicataria, pertanto, non avrà diritto alcuno di pretendere sovrapprezzi o indennità di alcun genere per aumento dei costi, perdite o qualsiasi altra sfavorevole circostanza che possa verificarsi dopo la data dell'offerta.

ART. 32 - AUMENTO, DIMINUZIONE E VARIAZIONI DELLA FORNITURA

L'Amministrazione si riserva la facoltà di estendere o diminuire l'intero appalto nel limite di un quinto del prezzo di aggiudicazione.

Oltre al quinto d'obbligo previsto dall'art. 11 della legge di contabilità generale dello Stato la Ditta Aggiudicataria sarà tenuta anche a quanto previsto dal Decreto Ministeriale 28 ottobre 1985, art. 27, comma 3, essendo in facoltà dell'Amministrazione richiedere un aumento od una diminuzione dell'intera

fornitura fino alla concorrenza di due quinti dell'importo complessivo con riferimento all'oggetto del presente appalto.

ART. 33 - RESPONSABILITA' CIVILE

La Ditta aggiudicataria assume in proprio ogni responsabilità per infortuni o danni eventualmente subiti da parte di persone o di beni, tanto della stessa Ditta aggiudicataria quanto dell'Amministrazione o di terzi, in dipendenza di omissioni, negligenze o altre inadempienze attinenti all'esecuzione delle prestazioni contrattuali ad esso riferibili, anche se eseguite da parte di terzi.

ART. 34 - AUTORIZZAZIONI E PERMESSI

Restano a carico della Ditta aggiudicataria tutte le spese, oneri, formalità, permessi, licenze, visti, nulla escluso per l'esecuzione dell'appalto.

ART. 35 – ADEGUAMENTO TECNOLOGICO

Tutte le apparecchiature (componenti) utilizzate per l'attuazione del Servizio dovranno essere di corrente produzione e di produttori certificati ISO 9001 o 9002, dovranno corrispondere ai più avanzati requisiti tecnici offerti dal mercato.

ART. 36 – MANUTENZIONE IN GARANZIA

Tutte le componenti fornite dovranno essere coperte dal servizio di manutenzione in garanzia per un periodo di un anno. I prodotti che risulteranno difettosi nel periodo considerato dovranno essere prontamente sostituiti con componenti nuovi entro 12 ore solari. Per ogni ora di ritardo per il regolare funzionamento dei prodotti difettosi sarà applicata una penale pari a 5.000,00 Euro. La garanzia dovrà essere inviata direttamente dal produttore, e dovrà coprire eventuali costi di manodopera necessari per la sostituzione di componenti difettosi.

ART. 37 - FORO COMPETENTE

Per qualsiasi controversia tra le parti, relativa all'interpretazione e/o esecuzione di un eventuale ordine, sarà competente, in via esclusiva, il Foro di Napoli.

ALLEGATO "A1"

ASSESSORATO ALL'UNIVERSITA' E RICERCA SCIENTIFICA, INNOVAZIONE TECNOLOGICA E NUOVA ECONOMIA, SISTEMI INFORMATIVI E STATISTICA, MUSEI E BIBLIOTECHE

DISCIPLINARE TECNICO

Appalto-concorso per la fornitura di un Sistema di Sicurezza caratterizzato una piattaforma di applicazioni e servizi per la gestione avanzata della sicurezza ed il controllo delle risorse in rete della Giunta Regionale della Campania

Napoli, addì 3/12/2002

1 - PREMESSA

L'Ente Regione Campania~~,~~ ha recentemente realizzato il livello infrastrutturale della propria rete **Intranet** dotando le sue principali sedi dislocate sull'intero territorio regionale di una infrastruttura di reti locali di campo e di edificio per la trasmissione dati ad alte prestazioni ed interconnettendo fra loro tali reti locali. Sono stati gli applicativi software, l'hardware integrativo e i servizi necessari per la realizzazione di un primo livello applicativo relativo ad Internet, Intranet e Extranet.

La connessione in rete di un calcolatore comporta però la visibilità dello stesso a tutti gli utenti collegati alla rete. L'utenza che quindi può accedere al calcolatore ed usufruire dei servizi/applicazioni da questo erogati si allarga enormemente. Nel caso in cui la rete in questione sia Internet il numero di potenziali utenti è smisurato. L'esperienza di questi anni ci insegna che tutto ciò può comportare notevoli vantaggi ma anche alcuni rischi. Tra i potenziali utenti della rete si nascondono infatti persone che, per diversi motivi, sono interessate a compromettere il buon funzionamento dei sistemi, accedere o modificare senza l'adeguata autorizzazione informazioni riservate.

Alla luce di tali considerazioni e in ottemperanza al Documento Programmatico sulla Sicurezza Informatica della Giunta Regionale della Campania l'Ente intende ora acquisire un Sistema di Sicurezza caratterizzato da una piattaforma di applicazioni e servizi per la gestione avanzata della sicurezza e il controllo delle risorse in rete della Giunta Regionale della Campania (di seguito Regione Campania).

2 - GENERALITA'

L'oggetto del presente appalto concorso consiste nell'acquisizione di un Sistema di Sicurezza caratterizzato da una piattaforma di applicazioni e servizi per la gestione avanzata della sicurezza e il controllo delle risorse in rete della Regione Campania.

La fornitura dovrà comprendere e garantire:

a) l'implementazione, in seno all'attuale sistema informatico e telematico della Regione Campania, di una **piattaforma di applicazioni e servizi** per la gestione della sicurezza ed il controllo delle risorse costituita dalle seguenti componenti di base:

• i **server/Workstation** costituenti la piattaforma Hardware del "Sistema" di gestione della sicurezza della Infrastruttura di rete della Regione Campania così come individuati nel presente documento;

• il Sistema di **Intrusion Detection** (IDS) e Risk Analysis;

• il Sistema di **Antivirus Centralizzato**;

• il Sistema di **Strong Authentication** per tutti gli accessi alle risorse di rete, con l'individuazione dei profili utente e dei privilegi ad essi attribuiti;

• il Sistema di **Configuration Management** centralizzato per tutte le stazioni di lavoro in rete;

• il Sistema di **Content Filtering** intelligente per gli accessi verso Internet;

• il Sistema di **Autenticazione di Dominio** MS e File server Centralizzato;

• il Load Balancing sui Firewall di Front-end a fronte di migliorarne la tolleranza al carico e garantirne la scalabilità per i volumi di utenza futuri;

b) almeno 500 (cinquecento) ore di addestramento del personale della Regione Campania mediante training on the job;

c) la manutenzione in **garanzia** di tutte le componenti per un anno dall'avvenuto positivo collaudo.

3 - DESCRIZIONE DELLE PREESISTENZE

3.1 - L'INFRASTRUTTURA DI RETE

L'attuale infrastruttura telematica della Regione Campania si articola in accordo ad un modello parzialmente hub-and-spoke a partire da un Centro Stella posto nella sede di Napoli di Via Don Bosco, che funge da hub verso le sedi periferiche extra urbane della Regione Campania collegate tramite flussi Frame-relay forniti da PathNet/Telecom terminati su un router Cisco 7513 e partecipa in qualità di nodo principale ad una MAN in topologia BMA full meshed realizzata attraverso il servizio Ethernity con le sedi della Regione Campania posizionate sul territorio metropolitano.

La sede di via Don Bosco fornisce la connettività verso Internet tramite due Flussi a 8 Mbs (4x2IMA) forniti da Telecom Italia, terminati su due router Cisco della famiglia 3600, configurati in load-balancing verso internet ed in HSRP verso la rete interna ove è installata una coppia di Firewall in tecnologia Cisco modello PIX 525 nella configurazione Fullstate failover che, in accordo alle politiche attualmente previste, partiziona la rete in quattro domini, o zone, di sicurezza: una zona definita outside verso Internet, una zona demilitarizzata definita DMZ che ospita i principali servizi di rete a visibilità globale (WWW, news etc.), una zona sicura definita SERVER-FARM destinata ad ospitare i principali servizi informatici a visibilità interna e una zona inside verso la intranet regionale.

Per il sistema sopra descritto si richiede l'introduzione delle nuove funzionalità dettagliate nel seguito.

4 - CARATTERISTICHE DELLA FORNITURA

4.1 - FUNZIONALITA' DI GESTIONE DELLA SICUREZZA E DEL CONTROLLO DELLE RISORSE

La Ditta Aggiudicataria dovrà procedere all'implementazione, in seno all'attuale sistema informatico e telematico della Regione Campania, di un Sistema di Sicurezza caratterizzato da una piattaforma di applicazioni e servizi per la gestione della sicurezza ed il controllo delle risorse costituita dalle seguenti componenti di base:

• Sistema IDS (Intrusion Detection System) e Risk Analysis;

• Sistema Antivirus Centralizzato;

• Sistema di Strong Authentication per tutti gli accessi alle risorse di rete, con l'individuazione dei profili utente e dei privilegi ad essi attribuiti;

• Sistema di Configuration Management centralizzato per tutte le stazioni di lavoro in rete;

• Sistema di Content Filtering intelligente per gli accessi verso Internet;

• Sistema di Autenticazione di Dominio MS e File server Centralizzato;

• Load Balancing sui Firewall di Front-end a fronte di migliorarne la tolleranza al carico e garantirne la scalabilità per i volumi di utenza futuri.

L'ambiente di gestione dovrà essere multivendor, strutturato al fine di massimizzare i benefici ricavabili da differenti prodotti e tale da offrire una soluzione completa e competitiva.

I moduli Software e Hardware dovranno essere selezionati tra gli ambienti leader di mercato in ciascun settore.

I requisiti minimali delle singole componenti vengono definiti in seguito.

4.2 – REQUISITI TECNICI DELLA PIATTAFORMA

Nel presente paragrafo sono individuate le caratteristiche tecniche generali e minimali delle apparecchiature richieste mentre nei paragrafi successivi verranno descritte le funzionalità richieste ai singoli sottosistemi.

PIATTAFORMA HARDWARE E SOFTWARE

La soluzione richiesta dovrà essere basata su una piattaforma hardware e software con le seguenti caratteristiche:

• le macchine (server/Workstation) del sistema di gestione dovranno appartenere all'ultima generazione di modelli nell'ambito del catalogo dello specifico costruttore;

• laddove necessario le macchine dovranno essere dotate di doppia scheda di rete e disk-array di capacità adeguata;

• il sistema operativo dovrà corrispondere ad uno dei sistemi più diffusi sul mercato;

• il protocollo di rete per tutti i componenti della soluzione proposta dovrà essere TCP/IP;

• il server di gestione dovrà supportare il protocollo NTP per la propria sincronizzazione data/ora con un server di riferimento.

SCALABILITÀ DEL SISTEMA

Il sistema dovrà essere capace di adeguarsi ad un numero crescente di elementi gestiti e di posti operatore. In ogni caso il presente progetto dovrà essere dimensionato per un carico attuale di 2600 utenti scalabile fino a 10000 utenti, basandosi su macchine le cui caratteristiche fisiche (processori, RAM, memoria di massa) siano espandibili ma che lascino contestualmente inalterate le caratteristiche del sistema.

4.3 – SISTEMA DI INTRUSION DETECTION E RISK MANAGEMENT

Il sistema richiesto dovrà permettere di rilevare eventuali attacchi ricevuti sia dall'interno che dall'esterno mantenendo traccia degli stessi a scopo di una successiva analisi "forensics", chiudendo le connessioni a rischio ed eventualmente riconfigurando i firewall.

Il sistema di Intrusion Detection deve prevedere tre sonde network sensor, tre sonde Server/Os Sensor e la relativa console di management. Il sistema di management dovrà consentire una gestione integrata e centralizzata di tutte le sonde installate sulla rete.

La piattaforma di Risk Management dovrà consentire di testare le vulnerabilità di alcuni dei sistemi attestati sulla rete (DNS, Server Web, ecc…), di produrre una reportistica dettagliata in grado di mostrare le caratteristiche della macchina analizzata e di individuare alcune possibili soluzioni per rimuovere le criticità riscontrate. REQUISITI TECNICO/FUNZIONALI

Il Sistema di IDS e il relativo sistema di management dovrà consentire di supportare i seguenti requisiti:

- configurazione delle policy di sicurezza dei sensori per l'identificazione degli attacchi;

- alerts in tempo reale degli eventi sospetti rilevati dai sensori;

- attuazione di contromisure (e-mail, blocco dell'IP dell'attaccante sui fw, chiusura porta utilizzata ecc…) in tempo reale in funzione della sensor's security policy configurata;

- aggiornamento programmato e/o spot del software;

- aggiornamento automatico degli attack signatures verso i sensori;

- capacità di analisi del traffico su reti Fast e Giga ethernet;

- il ripristino della configurazione dopo la rilevazione di una violazione della sicurezza;

- monitoring delle modifiche sui diritti di gruppo dei file;

- monitoring dei permessi di esecuzione dei file;

- verifica delle credenziali dell'utente amministratore;

- la notifica di allarmi dovuti a intrusioni sui sistemi applicativi;

- piattaforma di Risk Management.

4.4 – SISTEMA ANTIVIRUS

Il sistema antivirus dovrà essere posizionato a livello di gateway, ovvero nel punto di confine tra la rete della Regione Campania e la rete esterna o Internet. Costituirà in tal modo la prima linea di difesa contro i virus impedendone l'ingresso nelle rete interna della Regione Campania.

La soluzione proposta dalla Ditta dovrà essere in grado di monitorare in tempo reale tutto il traffico SMTP, HTTP e FTP in transito sul gateway, sia in ingresso che in uscita, rilevando ed impedendo il transito di virus noti.

La scansione del traffico SMTP permetterà di verificare e rimuovere i virus da tutti i messaggi di posta elettronica, dai file allegati e dal relativo contenuto nel caso si tratti di archivi (file zip, tar, ecc.).

La scansione del traffico HTTP dovrà prevenire il download di file infetti nonché di codice Java o ActiveX maligno.

La scansione del traffico FTP dovrà prevenire il download di file infetti.

Il sistema dovrà consentire di scegliere se effettuare la scansione di tutti i file indipendentemente dalla tipologia oppure solamente i file appartenenti a determinate categorie. Analogamente dovrà essere possibile scegliere di bloccare determinati tipi di file indipendentemente dal fatto che siano infetti da virus.

Nel caso venga rilevato un virus il sistema dovrà permettere in maniera flessibile di stabilire l'azione da intraprendere sul file infetto e le modalità di notifica dell'evento.

Indipendentemente dal servizio all'interno del quale si è rilevata l'infezione le possibili azioni potranno essere le seguenti:

- Lasciare passare il file infetto senza alcuna modifica.

- Spostare il file infetto in un'area predefinita per una successiva analisi.

- Cancellare il file infetto.

- Rimuovere automaticamente il virus dal file infetto.

Nel caso in cui il virus venga rilevato all'interno di un messaggio di posta elettronica, il sistema dovrà permettere di notificare la presenza del virus ai destinatari tramite l'inserimento all'interno della stessa di un testo definibile dall'amministratore; dovrà inoltre permettere l'invio di una notifica al mittente e all'amministratore. Anche nel caso dei servizi ftp e web il sistema dovrà essere in grado di inviare mail di notifica all'amministratore.

Il sistema antivirus dovrà mantenere un registro di attività completo con i dettagli di tutti i file infetti e di tutti i tentativi di violazione della sicurezza: l'origine, il nome e la destinazione del file, la data di ricezione del file, l'identità del virus rilevato e l'azione intrapresa. Ciò per permettere agli amministratori di rintracciare con facilità la fonte del problema risolvendolo poi in maniera adeguata.

REQUISITI TECNICO/FUNZIONALI

Il sistema fornito dovrà prevedere almeno i seguenti requisiti Tecnico/Funzionali:

- rilevamento e rimozione in tempo reale dei virus per tutto il traffico SMTP, HTTP e FTP;

- scansione dei file allegati alla posta elettronica anche se compressi o all'interno di un file archivio (tar, zip, ecc.);

- possibilità di scegliere i tipi di file da verificare: tutti i file o solo determinate categorie;

- possibilità di scegliere i tipi di file da bloccare: tutti i file o solo determinate categorie;

- possibilità di bloccare codice maligno Java e ActiveX;

- scelta dell'azione da intraprendere nel caso venga rilevato un file infetto: nessuna azione, spostamento, cancellazione, rimozione automatica del virus;

- notifica via posta elettronica all'amministratore e nel caso di messaggi di posta elettronica ai destinatari e al mittente;

- mantenimento di un registro completo e dettagliato delle attività;

- aggiornamento automatico del file di definizione dei virus;

- configurazione remota tramite interfaccia web.

4.5 – SISTEMA DI STRONG AUTHENTICATION

La Ditta dovrà fornire una piattaforma di AAA (Authentication, Authorization e Accounting) Management per effettuare in modo centralizzato operazioni di controllo degli accessi dall'esterno e verso l'esterno, sulla base di profili e privilegi associati a singoli utenti e gruppi di utenze.

REQUISITI TECNICO/FUNZIONALI

Il Sistema di Strong Authentication richiesto dovrà almeno:

- disporre di un'interfaccia grafica Web facile da usare;

- permettere il controllo e la gestione centralizzata degli accessi degli utenti nell'ambito di reti locali (LAN) switched e wireless LAN secondo lo standard IEEE 802.1X;

- supportare servizi quali accesso remoto, VPN e firewall, banda larga, wireless e voce;

- supportare i protocolli RADIUS e TACACS+ e i diversi protocolli di password come ASCII/PAP, CHAP, MS-CHAP, LEAP, EAP-CHAP, EAP-TLS, ARAP;

- fornire alte prestazioni per poter distribuire i privilegi per l'accesso alla rete su grandi gruppi di utenti;

- supportare data store LDAP, NDS, ODBC, Windows NT/2000 User Database;

- presentare caratteristiche di scalabilità con servizi di data replication e ridondanza;

- disporre di funzionalità di accounting e reporting;

- consentire la restrizione degli accessi utente basata su Remote Address Calling Line Identification (CLID), Dial Number (DNIS), IP address, NAS e Port Disabling.

4.6 – SISTEMA DI CONFIGURATION MANAGEMENT

Il Sistema di Configuration Management dovrà permettere di controllare e semplificare la gestione del Software installato sui Client della Regione Campania. Con tale Sistema dovrà essere possibile verificare quanto installato sui Client ed eventualmente distribuire nuovo Software (Aggiornamenti SW di sistema e di base, antivirus locali, etc.).

REQUISITI TECNICO/FUNZIONALI

Il Sistema di Configuration Management richiesto dovrà almeno:

- consentire la distribuzione, installazione ed attivazione di software (di qualunque tipo) in un ambiente distribuito, a macchine eterogenee;

- consentire l'auto registrazione di nuovi elementi target di distribuzione che vengano aggiunti al dominio di distribuzione;

- consentire l'esecuzione di una distribuzione su richiesta dell'operatore;

- supportare l'esecuzione di una distribuzione in modo schedulato, consentendo all'operatore di impostare i tempi di distribuzione e installazione;

- centralizzare su una console di management il reporting delle operazioni di distribuzione;

- automatizzare, in caso di errore, i retries di distribuzione e consentire, in condizioni di errore irrecuperabile, di annullare le operazioni già effettuate, ritornando allo stato pre-distribuzione;

- gestire l'installazione di nuove versioni di software sugli elementi gestiti;

- disporre di un inventario, con riferimento ad ognuno dei sistemi gestiti, delle distribuzioni effettuate e del software installato (granularità software kit, patch, file....), sulla base del quale condizionare le distribuzioni successive.

4.7 – SISTEMA DI CONTENT FILTERING

La Ditta dovrà fornire un sistema in grado di monitorare in tempo reale tutti i tentativi di accesso effettuati dai computer della rete interna alla Regione Campania verso i siti web Internet al duplice scopo di tenere un registro dettagliato sull'utilizzo delle risorse Internet e di impedire l'accesso a tutti quei siti non ritenuti pertinenti all'attività della Regione Campania.

Il sistema dovrà avvalersi di un database contenente la classificazione del maggior numero possibile di siti web Internet e avere la possibilità di essere aggiornato dinamicamente per seguire l'evoluzione della rete Internet.

Dovrà inoltre essere possibile la personalizzazione da parte degli amministratori allo scopo di aggiungere eventuali siti web non censiti.

Il sistema dovrà consentire di specificare filtri in base alla fascia oraria, ovvero consentendo l'accesso a determinate categorie di siti web solo in determinati momenti della giornata.

Inoltre sarà possibile specificare regole in base agli utenti, gruppi di utenti e computer dai quali viene originata la richiesta di accesso al sito web.

Dovrà essere possibile impedire l'accesso a quelle categorie di siti web non direttamente coinvolti nell'attività della Regione Campania ottimizzando quindi l'utilizzo della banda di accesso a Internet e ottenendo maggiori prestazioni sull'accesso ai quei siti che sono invece ritenuti utili all'attività dell'Ente.

In base al registro delle attività dovrà essere possibile generare, anche in modalità automatica, report sull'attività di navigazione in Internet, quali per esempio il tempo speso per la navigazione e i siti web maggiormente acceduti.

REQUISITI TECNICO/FUNZIONALI

Il sistema fornito dovrà prevedere almeno i seguenti requisiti Tecnico/Funzionali:

- monitoraggio in tempo reale dell'accesso ai siti web Internet;
- database contenente la classificazione del più ampio numero di siti web;
- aggiornamento dinamico e automatico del database;
- possibilità di personalizzazione del database;
- filtraggio dei siti web in base alla classificazione del database;
- filtraggio dei siti web in base a parole chiave contenute all'interno dell'URL;
- filtraggio dei siti web in base alla fascia oraria;
- differenziazione dei filtri in base all'utente, gruppo o computer che ha originato la richiesta;
- mantenimento di un registro completo e dettagliato delle attività;
- possibilità di ottenere reportistica dettagliata sull'attività di navigazione web.

4.8 – SISTEMA DI AUTENTICAZIONE DI DOMINIO E FILE SERVER CENTRALIZZATO

La Ditta dovrà fornire un sistema in grado di autenticare l'accesso in rete intranet degli utenti della rete della Regione.

Il sistema di autenticazione dovrà essere basato sulla piattaforma di MicroSoft Windows 2000 server e dovrà interfacciarsi con il sistema di strong authentication.

Inoltre dovrà svolgere funzioni di File server centralizzato.

4.9 – LOAD BALANCING PER FIREWALL CISCO PIX525

La proposta tecnica dovrà prevedere una soluzione atta a migliorare l'utilizzo dei due firewall Cisco PIX 525 posti a protezione della LAN.

Si precisa che attualmente questi due apparati sono in configurazione fullstate failover in cui uno è attivo ed il secondo in stand-by.

Una soluzione di bilanciamento di carico tra i due firewall dovrà essere proposta in una configurazione ad alta affidabilità.

L'apparato proposto per la funzionalità di Load Balancing dovrà avere quantomeno i seguenti requisiti:

- active-active FireWall Load Balancing for High Avaliability;
- active-active Symmetric Load Balancing;
- almeno 100K connections setup per second;
- DoS mitigation integrated into device;
- L2/L3 integrato;
- Prodotto in formato stackable con scalabilità 16 e 24 porte 10/100 + 2 porte GE;
- Capacità di sessioni contemporanee per porta fino a 1.000.000;
- Capacità di effettuare contemporaneamente applicazioni di FWLB e SLB;
- Capacità di bilanciare fino a 32 Firewall contemporaneamente in applicazione FWLB;
- Capacità di bilanciare il traffico su base porta applicativa in applicazioni FWLB;
- Supporto della persistenza delle sessioni per: Cookie/SSL + Source IP, Source IP+VIP+port, Cookie, SSL;
- Port Tracking;
- Virtual Source;
- Funzionalità Always/Active, Active/StandBy e SuperZone/MultiZone per applicazioni FLWB;
- Protezione contro attacchi DoS su ogni porta;
- Supporto a livello di sicurezza di Packet Filternig con ACL base ed estese, NAT esteso;
- Supporto completo funzionalità L2 in particolar modo gli standard:
  - IEEE 802.1d;
  - IEEE 802.1P/Q;
  - Supporto funzionalità di routing a L3: Inter switch Routing fra Vlan, routing statico e dinamico (almeno RIP V1 e V2);
  - Supporto SSH V2;
  - Management SNMP V2, RMON gruppi (1,3,5,9).

5 – ADDESTRAMENTO DEL PERSONALE DELLA REGIONE CAMPANIA

Compito della Ditta aggiudicataria sarà anche quello di provvedere all'addestramento del personale che la Regione Campania renderà disponibile per far loro raggiungere un grado di autonomia sufficiente ad una autonoma gestione e conduzione di primo livello del sistema ed al suo utilizzo. Tale addestramento dovrà consistere in un pacchetto di almeno 500 (cinquecento) ore che dovranno essere destinate ad attività di training on the job.

6 – CARATTERISTICHE GENERALI DELLA FORNITURA

Il Sistema descritto nel presente documento dovrà essere fornito chiavi in mano, completo di tutto quanto necessario al suo corretto ed efficiente funzionamento.

Il software di base dei server utilizzati dovrà essere in grado di sostenere il carico dell'intero Sistema garantendo livelli di servizio adeguati alle caratteristiche funzionali delle applicazioni, in termini di tempi di risposta, scalabilità, affidabilità, continuità del servizio, sicurezza; dovrà inoltre essere conforme a standard de facto o de iure e dovrà essere in grado di interoperare sui sistemi di rete previsti in tale Disciplinare.

Il software applicativo di supporto ai sevizi forniti dovrà essere conforme alle norme di qualità ISO ed alla normativa emanata dall'AIPA in materia.

La piattaforma hardware ove verranno implementati le applicazioni e i servizi per la gestione avanzata della sicurezza e il controllo delle risorse in rete della Regione Campania necessita di caratteristiche minimali tali da garantire una gestione efficace del Sistema nel suo complesso e la scalabilità dello stesso in ragione della futura evoluzione dell'infrastruttura telematica in ordine allo sviluppo tecnologico e alle nuove forme di minaccia che verranno riscontrate.

L'infrastruttura Hardware dovrà avere almeno le seguenti caratteristiche:

processore: fino a due processori Pentium IV a 1,13 GHz, 1,26 GHz o 1.40 GHz con bus frontale (FSB) a 133 MHz;

Controller del sottosistema del disco: Controller SCSI Ultra3 integrato con velocità di trasferimento dati di 160 MB/sec;

Cache: 512 KB di cache on-die;

Porta I/O: 2 seriali; 1 parallela a 25 pin; 1 knock-out SCSI per i collegamenti esterni; 1 video a 15 pin; 2 Mini-DIN (porta per tastiera e porta per mouse); 1 opzionale per gestione seriale; 2 USB; 1 LAN;

Tipo di memoria: da 256 MB a 4 GB di SDRAM con controllo e correzione degli errori (ECC) PC-133 MHz;

Rack e scaffali: Memoria di massa di almeno 200GB in dischi SCSI da 160MB/sec; 12 vani totali: Un'unità disco flessibile da 3,5"; un'unità CD-ROM; due alloggiamenti per supporti rimovibili con vassoio comune aperto, adatto per un dispositivo a nastro per il backup oppure per le unità a disco con vassoio comune; sei alloggiamenti per memoria di massa aperti con opzione di duplexing per suddividere il backplane dell'unità hot-swap (2x6);

Slot di espansione: Sei slot PCI a 32 bit a lunghezza intera (quattro a 33MHz) e slot PCI a 64 bit (due a 66MHz);

CD-ROM/DVD: unità CD-ROM IDE 48X;

Unità disco flessibile: Unità disco flessibile da 3,5" da 1,44 MB

Tastiera: Tastiera localizzata

Mouse/dispositivo di puntamento: Mouse a due pulsanti

interfaccia di rete: adattatore LAN 10/100TX integrato con esecuzione pre-avvio (PXE) e funzione wake-on-LAN (WAN); supporta i NIC ridondanti

Si precisa che le caratteristiche dell'infrastruttura hardware e software, così come particolareggiate nel presente documento, sono solo indicative potendo le Ditte concorrenti, in ragione della natura stessa della gara, proporre una soluzione tecnica migliorativa e/o equivalente a quella rappresentata.

ALLEGATO "C"

Napoli, addì_____

Spett.Le_____

Oggetto: **Appalto-concorso per la fornitura di un Sistema di Sicurezza caratterizzato da una piattaforma di applicazioni e servizi per la gestione avanzata della sicurezza ed il controllo delle risorse in rete della Giunta Regionale della Campania.**

In riferimento alla nota del___, trasmessa da codesta Spettabile___ e protocollata agli atti di questa Amministrazione Regionale con protocollo n.___ del___ con la quale ha inteso partecipare al bando per l'appalto concorso di cui all'oggetto, si comunica che la predetta istanza, in sede di valutazione, è stata accolta favorevolmente, avendo verificato la sussistenza dei requisiti previsti nel bando.

Ai sensi, pertanto, di quanto espresso nell'art. 7 del Capitolato Speciale relativo al presente appalto, si invita la S.V. a far pervenire, nei termini e secondo le modalità indicate nello stesso articolo, l'offerta (tecnica ed economica) allo stesso indirizzo al quale è stata trasmessa la domanda di partecipazione.

Si rileva, in proposito, che le offerte, redatte in conformità del Capitolato Speciale, vanno racchiuse in un plico sigillato con ceralacca e firmato sui lembi di chiusura, con l'indicazione del mittente e la seguente scritta: "**Offerta per la Gara relativa all'appalto-concorso per la fornitura di un Sistema di Sicurezza caratterizzato da una piattaforma di applicazioni e servizi per la gestione avanzata della sicurezza ed il controllo delle risorse in rete della Giunta Regionale della Campania"** nella quale dovranno essere inseriti:

a) una busta contenente l'autocertificazione attestante il possesso dei requisiti di capacità finanziaria e tecnica prescritti nel presente Capitolato in conformità a quanto previsto dagli artt. 13 e 14 del D.Lgs 358/92, così come modificato dal D.Lgs 402/98. Tale documentazione non dovrà in alcun modo riportare indicazione sui costi, pena esclusione;

b) una busta, contenente l'offerta tecnica, sigillata con ceralacca e controfirmata sui lembi di chiusura, con l'indicazione del mittente e l'oggetto della gara. L'offerta tecnica, regolarmente sottoscritta in tutte le sue parti, deve contenere, pena esclusione:

• presentazione della Ditta e referenze generali e specifiche, con particolare riferimento a soluzioni analoghe a quelle previste dal presente Appalto;

• elenco in cui siano puntualmente identificati tutti gli oggetti componenti il Servizio;

• Progetto Tecnico, che deve includere appositi e specifici capitoli:

- la descrizione dettagliata delle caratteristiche tecniche delle apparecchiature offerte;

- la descrizione tecnica e funzionale del Sistema Intrusion Detection;

- la descrizione tecnica e funzionale del Sistema Antivirus Centralizzato;

- la descrizione tecnica e funzionale del Sistema di Strong Authentication;

- la descrizione tecnica e funzionale del Sistema di Configuration Management;

- la descrizione tecnica e funzionale del Sistema di Content Filtering;

- la descrizione tecnica e funzionale del Sistema di Autenticazione di Dominio;

- il Piano di implementazione del Load Balancing sui Firewall di Front-end;

- il Piano dettagliato delle modalità di integrazione dei nuovi apparati sull'infrastruttura intranet preesistente;

- il Piano di addestramento del personale della Regione Campania con le modalità di cui al presente Appalto;

- il Piano di installazione, messa in esercizio, configurazione, fornitura e posa in opera di ogni componente software e hardware dell'intera fornitura;

• la dichiarazione con la quale i concorrenti attestano:

- di aver esaminato gli elaborati di gara;

- di essersi recati sul luogo di esecuzione dei lavori;

- di aver preso conoscenza delle condizioni locali e delle eventuali preesistenze utilizzabili ai fini della implementazione del Sistema richiesto, nonché di tutte le circostanze generali e particolari

suscettibili di influire sulla determinazione dei prezzi, sulle condizioni contrattuali e sulla fornitura dell'appalto;

- di essere a conoscenza dell'infrastruttura Intranet della Giunta Regionale della Campania e che questa può essere messa in completa sicurezza grazie alla soluzione tecnica proposta;

- di aver giudicato il Servizio attuabile, gli elaborati di gara adeguati ed il prezzo a base della gara remunerativo e tale da indurre offerte in ribasso.

L'offerta tecnica dovrà essere corredata da tutta la documentazione tecnica ritenuta opportuna per la sua corretta valutazione. Per consentire una migliore consultazione, l'offerta tecnica dovrà essere fornita anche in formato elettronico PDF e non dovrà in alcun modo riportare indicazioni sui costi, pena esclusione;

c) una busta, contenente l'offerta economica, sigillata con ceralacca e controfirmata sui lembi di chiusura con l'indicazione del mittente e l'oggetto della gara. L'offerta economica, regolarmente sottoscritta, deve essere redatta in carta da bollo e in lingua italiana e, pena esclusione, deve contenere l'importo complessivo richiesto per la fornitura "chiavi in mano" dell'appalto, espresso in cifre e in lettere al netto di IVA, nonché la sua ripartizione nei singoli importi espressi in cifra ed in lettere, al netto di IVA, relativi ai singoli sottosistemi offerti. Nel caso di discordanza tra un importo in cifre ed il suo corrispondente in lettere farà fede quest'ultimo. In caso di discordanza tra l'importo complessivo e la sommatoria dei singoli importi farà fede l'importo più vantaggioso per l'Amministrazione. Tale plico dovrà pervenire, a pena di esclusione, all'A.G.C. Ricerca Scientifica, Statistica, Sistemi Informativi ed Informatica entro il 40° (quarantesimo) giorno successivo alla data di spedizione della lettera d'invito.

Fino a 10 (dieci) giorni prima del termine ultimo per la presentazione delle offerte sarà possibile richiedere chiarimenti e/o consultare documenti tecnici e/o amministrativi rispettivamente presso il CRED e l' A.G.C. Ricerca Scientifica, Statistica, Sistemi Informativi ed Informatica.

Alla gara possono partecipare società, Ditte individuali e raggruppamenti di imprese.

Saranno, comunque, escluse dalla gara le Ditte che produrranno dichiarazioni non conformi alle prescrizioni e norme tecniche dettate nel Capitolato Speciale di Appalto e relativo Disciplinare Tecnico allegato alla presente lettera d'invito.

Si richiama, da ultimo, l'attenzione dei concorrenti, che parteciperanno come raggruppamento temporaneo d'impresa, ad adempiere, nel formulare l'offerta, a tutto quanto previsto all'art. 7 del Capitolato Speciale d'Appalto.