Provincia di Pistoia

Servizio Informatico

CAPITOLATO SPECIALE D'APPALTO PER L'ACQUISIZIONE DI APPARATI HARDWARE, SOFTWARE E RELATIVI SERVIZI PER IL POTENZIAMENTO DEL SISTEMA INFORMATIVO DELLA PROVINCIA DI PISTOIA

Pistoia, lì 06.12.2007

Il Dirigente Responsabile
(*Dr. Vincenzo Evangelisti*)

1. Oggetto della gara

L'oggetto della gara è la fornitura, installazione e configurazione di sistemi hardware e software necessari alla realizzazione del progetto di adeguamento dell'architettura dei Sistemi Informativi della Provincia alle nuove e crescenti necessità di prestazioni, servizi e sicurezza.

Nella esecuzione del progetto la Provincia intende conservare il più possibile inalterate le scelte di architettura dei sistemi e dei software di base, descritti nel paragrafo successivo: saranno pertanto privilegiate in sede di valutazione le soluzioni che risulteranno più facilmente integrabili, nel rispetto della attuale architettura e del "know how" acquisito dagli operatori del Servizio Informatico.

Per il raggiungimento degli scopi progettuali sono state individuati una serie di interventi, raggruppati nelle quattro "Aree di intervento" di seguito indicate e meglio specificati nel successivo capitolo 3. "Interventi previsti", a cui si rimanda per più precisi riferimenti tecnici:

I. **Adeguamento della struttura esistente:**

1.1 Aggiornamento e allineamento dei sistemi software installati sui server esistenti con le nuove versioni disponibili;

1.2 adeguamento hardware e dimensionamento della SAN e dei server esistenti;

1.3 adeguamento dei dispositivi necessari alla gestione della sala macchine (armadi e console);

1.4 adeguamento dei sistemi di sicurezza perimetrale;

Per approfondimenti i riferimenti nel successivo capitolo 3. "Interventi previsti" sono all'interno della sezione 3.1.

II. **Adeguamento delle modalità di accesso alle applicazioni e ai dati:**

2.1 Remotizzazione degli accessi alle procedure client/server

2.2 Sicurezza degli accessi a procedure web: realizzazione di una soluzione di Access Management che consenta alle applicazioni di fruire delle funzionalità di Autenticazione ed Autorizzazione e di Single Sign On (SSO) ove richiesto,

2.3 Introduzione sperimentale e limitata di accessi tramite Smart Card

Per approfondimenti i riferimenti nel successivo capitolo 3. "Interventi previsti" sono sono all'interno della sezione 3.2.

III. **Adeguamento delle procedure di gestione delle utenze**

3.1 Implementazione di una soluzione di Gestione integrata delle identità che permetta l'automatizzazione del processo di *provisioning* delle utenze, integrato con i processi organizzativi dell'Ente, e che gestisca l'evoluzione delle identità (creazione, modifica, rimozione);

Per approfondimenti i riferimenti nel successivo capitolo 3. "Interventi previsti" sono all'interno della sezione 3.3.

IV. **Auditing e monitoraggio degli eventi legati alla sicurezza informatica**

4.1 Implementazione di un software di raccolta degli eventi in grado di tracciare e storicizzare le attività di accesso alla rete ed al file system.

4.2 Implementazione di un sistema di monitoraggio dei sistemi e servizi di rete, dotato di funzioni di messaggistica e alert.

Per approfondimenti i riferimenti nel successivo capitolo 3. “Interventi previsti” sono all’interno della sezione 3.4.

Ciascuna delle quattro aree di intervento precedenti, meglio descritte nel seguito, dovrà includere ogni necessità di hardware, software, attività sistemistica e formazione degli addetti e si concluderà con il relativo verbale di installazione e collaudo.

Per una migliore comprensione si premette una sintetica descrizione della attuale architettura della rete aziendale e dei sistemi software.

2. Architettura attuale dei sistemi e dei software di base

La rete informatica della Provincia collega fra loro 18 sedi di uffici, distribuite sul territorio provinciale, con una topologia a stella di cui la sede di Piazza S. Leone,1 a Pistoia costituisce il centro.

Nella rete aziendale sono presenti circa 400 stazioni di lavoro, a ciascuna delle quali vengono erogati tutti i servizi esistenti in rete .

In Piazza S. Leone, sede della Provincia di Pistoia e del Servizio Informatico, sono collocate le apparecchiature centrali per la gestione dei servizi di rete e per la comunicazione.

Le sedi periferiche urbane e quella della Protezione Civile dispongono di server locali, mentre le altre sono collegate alla rete via router ed ottengono i servizi da server remoti.

Per il dettaglio delle sedi si veda l’Allegato Tecnico A; per il dettaglio dei server attualmente installati l’Allegato Tecnico B.

La Provincia aderisce alla Rete Telematica della Regione Toscana (RTRT) ed usufruisce della infrastruttura di trasporto a banda larga a disposizione degli Enti aderenti, in base agli accordi ed ai progetti di RTRT, sia per il collegamento ad Internet che per le interconnessioni in modalità sicura con le altre Amministrazioni Locali della Regione.

Nella sede centrale si trova uno switch HP 9100 di backbone al quale sono connessi in fibra ottica, secondo lo standard IEEE 802.3z (Gigabit Ethernet), gli switch di distribuzione, mentre nelle sedi minori il cablaggio è realizzato con soli switch di distribuzione.

Gli switch di distribuzione raccolgono, in configurazione a stella, tutte le connessioni verso le stazioni di lavoro a 10/100 Mbps, secondo gli standard IEEE 802.3 e IEEE 802.3u (Ethernet e Fast Ethernet).

Ogni sede è collegata al nodo centrale della rete tramite circuiti diretti Telecom attestati su router Cisco ed Elsag.

Le comunicazioni fra i sistemi che fanno parte della rete aziendale avvengono tramite protocollo IP.

La rete è multipiattaforma ed i sistemi operativi utilizzati sono Novell NetWare, Microsoft Windows e varie distribuzioni Linux.

Il nucleo principale è costituito da server con sistemi Novell. I tre server che autorizzano l’accesso alla rete ed erogano i servizi di base hanno a bordo il sistema operativo NetWare 6.0 e sono collegati in un cluster fail-over per una maggior garanzia di continuità di servizio, anche in caso di malfunzionamento di uno di essi.

Nell'ottica di centralizzare ed ottimizzare lo spazio per la memorizzazione delle informazioni i tre server in cluster sono collegati ad una SAN Raidtec tramite appositi adattatori fibre-channel 2 Gb (HBA) e uno switch fibre-channel QLOGIC a 12 porte.

La SAN ha una capacità di 360 Gb (RAID 0) con possibilità di espansione fino ad alcuni Terabyte. La configurazione dei dischi prevede un disco spare globale per tutti i dischi logici definiti.

Oltre al sistema operativo NetWare nella rete sono utilizzati altri prodotti software NOVELL:

- "Novell GroupWise" è utilizzato come server di posta elettronica ed anche come client di posta sulle stazioni di lavoro;
- "Novell ZenWorks for Desktop" è usato per la gestione e diffusione delle risorse aziendali (gestione remota, policies, distribuzione delle procedure e accessi personalizzati per utente);
- "Novell eDirectory" costituisce il supporto per il servizio di gestione delle identità e l'accesso di sicurezza per gli impiegati, memorizzando e organizzando le informazioni relative a computer, utenti, condivisioni di rete, applicazioni;
- "ConsoleOne" è la console amministrativa con cui sono gestiti gli accessi degli utenti e le loro condivisioni e la distribuzione delle applicazioni;
- "Novell Border Manager" esplica funzioni di proxy e include un controllo sugli accessi internet integrando la soluzione di content filtering di *SurfControl* (vedi oltre);
- "Novell iChain" utilizza le informazioni di identità contenute nel directory server per fornire la gestione centralizzata degli accessi a procedure web, basata su norme e privilegi di autenticazione, nell'ambito di reti aziendali, extranet e Internet. "iChain" effettua il "reverse proxy", intercettando tutto il traffico diretto verso le risorse web da proteggere e, in base alla politica di accesso definita, è in grado di:
  - gestire l'autenticazione degli utenti;
  - gestire le autorizzazioni (su base URL) degli utenti;
  - fornire il servizio di web SingleSignOn;
  - effettuare il caching dei file statici;
  - rendere cifrato il canale di trasmissione con il browser lasciando sotto normale HTTP la comunicazione con le risorse web.

Per la protezione perimetrale della rete aziendale rispetto a possibili intrusioni, è installato un firewall hardware Cisco PIX 515, dotato di 6 interfacce ethernet, tramite le quali sono state impostate due DMZ.

In una delle DMZ sono collocati il server iChain e quello con il servizio antivirus, nell'altra il server NAL ("Nodo Applicativo Locale"), componente decentrata della infrastruttura per la cooperazione applicativa e finalizzato allo sviluppo di progetti di e-government che coinvolgono gli Enti appartenenti ad RTRT.

Per il controllo degli accessi a siti Internet è installato il prodotto di web-filtering di SurfControl, in grado di controllare e rilevare la violazione alle politiche aziendali di accesso ai siti web. Il prodotto di email-filtering sempre di SurfControl effettua un ulteriore filtraggio dei

messaggi postali, in grado di bloccare la maggior parte dello spamming generando solo un numero limitato di falsi positivi.

Nella rete aziendale non è presente un vero e proprio database server centralizzato, ma molte applicazioni utilizzano varie istanze di database relazionale ORACLE ed, in maniera minore, MS SQL e MySQL, distribuite su più server.

3. Interventi previsti

Per perseguire gli obiettivi del progetto sono stati individuati i seguenti interventi, per le quali la Ditta aggiudicataria dovrà eseguire le proprie attività e forniture all'interno delle quattro "Aree di intervento" sopra definite:

3.1 ADEGUAMENTO DELLA STRUTTURA ESISTENTE

3. 1.1 Aggiornamento dei sistemi software alle nuove versioni disponibili.

Quale attività preliminare e propedeutica alla realizzazione del progetto è stata individuata la necessità di procedere ad un aggiornamento generale delle versioni dei sistemi operativi e degli altri prodotti installati sui sistemi attualmente utilizzati, con le versioni aggiornate per effetto dei contratti di maintenance (upgrade protection, software assurance o quant'altro) stipulati con i relativi produttori.

Obiettivo di questa attività è quello di avere sistemi aggiornati per garantire al massimo l'interoperabilità con le nuove implementazioni che saranno realizzate nelle fasi seguenti.

Al contempo si avrà la disponibilità di tutte le nuove feature rilasciate, la correzione di eventuali difetti conosciuti ed il pieno supporto da parte del produttore.

In particolare in quest'area di intervento dovranno essere eseguite le seguenti attività:

- Migrazione delle piattaforme NetWare 6.x presenti, cluster e non, verso la nuova versione Open Enterprise Server 2 (OES 2) con kernel Linux, SUSE Linux Enterpise Server 10 (SLES 10), con eventuale riconfigurazione dei servizi erogati a seconda dei requisiti o delle dipendenze introdotte dalla nuova piattaforma.
- Aggiornamento di tutti i prodotti e delle piattaforme installate con le ultime versioni rese disponibili dai relativi produttori;
- Aggiornamento di tutti i prodotti e delle piattaforme installate con le ultime patch rilasciate dai rispettivi produttori;
- Eventuale bug-fixing e risoluzione di piccoli malfunzionamenti dei sistemi, conosciuti o evidenziati durante la fase di aggiornamento.

L'individuazione dei prodotti da aggiornare, l'ottenimento delle nuove versioni o patch dai rispettivi produttori e tutte le attività sistemistiche necessarie per realizzare detti aggiornamenti o migrazioni saranno a completo carico della Ditta aggiudicataria.

3.1.2 Adeguamento hardware e ridimensionamento dei server, della SAN e dei dispositivi per la gestione della sala macchine.

Contemporaneamente all'adeguamento dei sistemi software sarà eseguito, ove necessario, un adeguamento hardware (RAM e spazio disco) degli apparati server e delle memorie di massa (SAN) esistenti in funzione delle esigenze di utilizzo rilevate.

Per la sala macchine dovrà essere previsto l'acquisto di un ulteriore armadio (rack) da affiancare ai due esistenti, in modo da alloggiare tutti i server, sia quelli esistenti sia quelli necessari per la realizzazione del presente intervento. L'armadio dovrà essere corredato dei dispositivi necessari per la gestione: console (monitor, tastiera e mouse) e cavi di collegamento occorrenti.

Per le caratteristiche tecniche dei dispositivi vedere l'Allegato Tecnico E.

3.1.3 Adeguamento dei sistemi di sicurezza perimetrale.

Per aumentare il livello di sicurezza cosiddetto "perimetrale", cioè relativo agli accessi alla rete dall'esterno ed in generale per controllare tutto il traffico in ingresso ed in uscita, da e verso la rete pubblica ed RTRT, è prevista l'adozione di un sistema di firewall in affiancamento o in sostituzione dell'attuale Cisco PIX 515.

Oltre alla classica implementazione di logiche statefull per il controllo del traffico sulle interfacce, il nuovo dispositivo dovrà avere anche una tecnologia di ispezione dei pacchetti che consenta la *Intrusion Prevention (IPS)* cioè la prevenzione dagli attacchi conosciuti e non, effettuati sfruttando vulnerabilità dei sistemi o dei protocolli di comunicazione in essi implementati. Dovrà anche essere in grado di rilevare ed eventualmente impedire alcune tipologie di traffico indipendentemente dalle porte usate (es. pear-to-pear, ICQ, etc).

Tale apparato dovrà avere le caratteristiche descritte in dettaglio nell'Allegato Tecnico C.

3.2 ADEGUAMENTO DELLE MODALITÀ DI ACCESSO ALLE APPLICAZIONI ED AI DATI

3.2.1 Remotizzazione degli accessi alle procedure client-server

Nel sistema informativo della Provincia sono presenti molte applicazioni di tipo client-server, che hanno cioè un database centralizzato, installato su un server, acceduto da una componente applicativa Windows, installata singolarmente su ciascuna postazione di lavoro (client).

La sicurezza del sistema è data dalle credenziali necessarie per accedere alla postazione di lavoro, alla applicazione (solitamente profilata in una tabella applicativa all'interno del database stesso) e direttamente al database, da un qualsiasi computer connesso alla rete locale.

Questo intervento prevede la realizzazione di una server-farm, inizialmente dimensionata con cinque server, per la centralizzazione di tutte le applicazioni di tipo client-server (principalmente Protocollo, Contabilità, Personale e Paghe).

L'architettura prevede l'installazione nella server-farm, invece che sulle singole postazioni di lavoro, di tutte le applicazioni coinvolte e la remotizzazione dell'interfaccia grafica (desktop) delle applicazioni stesse direttamente dai server della server-farm.

Per aumentare ulteriormente il livello di sicurezza del sistema, il database server di ciascuna applicazione dovrà essere fisicamente connesso ad una nuova DMZ realizzata sul firewall, accessibile solo alla server-farm.

Le caratteristiche minime dell'architettura di remotizzazione saranno:

- Alta affidabilità, bilanciamento e distribuzione dinamica del carico di lavoro sui server della server-farm;
- Assegnazione, ottimizzazione e gestione dinamica delle risorse (CPU, RAM, banda);
- Garanzia di prestazioni adeguate, nonchè della necessaria scalabilità futura;
- Centralizzazione delle policy di distribuzione e di pubblicazione delle applicazioni sui client;
- Gestione di device locali (stampanti, usb, audio) dalle applicazioni remotizzate;
- Gestione integrata pass-throught della autenticazione locale verso le applicazioni remote;

- Integrazione con Novell eDirectory;
- Possibilità di SingleSignOn remoto con credenziali locali;
- Possibilità di Strong Authentication con device locali.

La gestione degli utenti e dei profili di accesso saranno integrate secondo quanto descritto nel paragrafo iniziale “Gestione delle utenze”.

Le applicazioni da remotizzare saranno:

- Protocollo
- Contabilità, Personale e Paghe

Per l’implementazione di questa architettura si stimano necessari cinque nuovi server in configurazione di tipo A di cui all’Allegato Tecnico D.

3.2.2 Sicurezza degli accessi a procedure web

Per rendere sicuri gli accessi alle applicazioni web sia dall’interno che dall’esterno è necessario estendere le funzionalità del reverse-proxy Novell iChain, già in uso presso la Provincia, a tutte le applicazioni critiche che hanno un’interfaccia web.

Oggetto della fornitura è quindi l’aggiornamento dell’attuale implementazione di iChain alla nuova versione denominata Novell Access Manager.

La fornitura dovrà prevedere l’adeguamento del numero di licenze dalle 50 attuali a 200, la re-installazione su un nuovo hardware in configurazione ridondata e bilanciata (attraverso apposito bilanciatore di carico hardware o software) per garantire la distribuzione del carico di lavoro e l’alta affidabilità.

La configurazione dovrà inoltre prevedere l’attivazione, ove possibile, delle funzionalità di web SingleSignOn e di gestione dei certificati X.509 per la crittografia SSL, previste dal prodotto.

La gestione degli utenti e dei profili di accesso saranno integrate secondo quanto descritto nel paragrafo iniziale “Gestione delle utenze”.

Le applicazioni da proteggere attraverso Access Manager saranno:

- IDOL (Incontro Domanda Offerta di Lavoro)
- Protocollo (visura web, procedura di consultazione)
- Paghe e Portale del personale
- Posta web (WebAccess)

Per l’implementazione di questa architettura si stimano necessari quattro nuovi server in configurazione di tipo B di cui all’Allegato Tecnico D.

3.2.3 Single sign on (SSO)

Per agevolare le procedure di login ai servizi resi disponibili in rete ed al contempo prevenire comportamenti a rischio da parte degli utenti, la Provincia ha deciso di avviare la sperimentazione, attraverso un progetto pilota su 50 postazioni di lavoro, di una soluzione completa di SingleSignOn.

La fornitura dovrà prevedere un sistema di automazione delle procedure di login alle applicazioni e piattaforme normalmente usate dagli utenti, da affiancare al web SSO già fornito da Novell Access Manager (vedi relativo paragrafo precedente).

Il sistema dovrà essere in grado di eseguire il SSO per qualunque applicazione Windows, java o web eseguita sul client.

Le caratteristiche minime della soluzione dovranno essere:

- Piena compatibilità con l'attuale configurazione delle postazioni di lavoro della Provincia ed in particolare con il client Novell NetWare;
- Piena compatibilità per il SSO remoto attraverso l'architettura di remotizzazione desktop fornita (vedi relativo paragrafo precedente);
- Piena compatibilità con il sistema di smartcard per la strong authentication (vedi relativo paragrafo successivo);
- Supporto di applicazioni Win32, java e web-based;
- Utilizzo di credenziali specifiche per ogni applicazione, anche diverse.

3.2.4 Strong Authentication tramite Smartcard

Fattore abilitante per una maggiore sicurezza delle postazioni di lavoro degli utenti ed elemento complementare di una soluzione di SSO è la Strong Authentication tramite dispositivo smartcard e certificato X.509.

Se da una parte il SSO aumenta la sicurezza delle credenziali sollevando l'utente dai processi di login ripetuti e quindi prevenendo password troppo semplici e comportamenti a rischio, dall'altra introduce come single point of failure di sicurezza le credenziali di accesso alla rete (il primo login) a cui seguono tutti quelli automatizzati dal SSO.

In caso di furto di quelle credenziali tutti i sistemi connessi al SSO sarebbero infatti conseguentemente accessibili.

Per evitare questo è possibile vincolare il procedimento di prima identificazione dell'utente basandolo su qualcosa che ha (la smartcard) invece che su qualcosa che sa (la password).

Analogamente a quanto descritto al punto precedente, la fornitura deve prevedere una implementazione pilota per 50 postazioni di lavoro, di una soluzione hardware e software per la lettura e conseguente verifica di un certificato X.509, generato internamente, contenuto in una smartcard.

La Ditta appaltante non dovrà comprendere nella fornitura le smartcard ed i relativi lettori che saranno invece approvvigionati direttamente dalla Provincia, per effetto di un contratto di fornitura in essere con Infocamere, tramite la Regione Toscana.

La tipologia di "certificato di autenticazione", la smartcard ed il relativo lettore che saranno a disposizione dell'Ente, corrispondono a quelli attualmente forniti dai Contratti Regionali Aperti "Area Reti Di Governance Del Sistema Regionale e Ingegneria dei Sistemi Informativi e della Comunicazione" nell'ambito degli Enti aderenti alla RTRT.

La fornitura deve avere le seguenti caratteristiche minime:

- Piena compatibilità con l'attuale configurazione delle postazioni di lavoro tipo della Provincia ed in particolare con il client Novell NetWare;
- Piena compatibilità per l'autenticazione web attraverso Novell Access Manager (vedi relativo paragrafo precedente);
- Piena compatibilità per l'autenticazione remota attraverso l'architettura di remotizzazione desktop fornita (vedi relativo paragrafo precedente);

- Blocco della postazione in caso di rimozione della smartcard dal lettore;
- Valutazione di quanto già disposto e suggerito in materia, sia dal CNIPA che dalla Regione Toscana, per assicurarsi la perfetta interoperabilità delle smartcard con altri eventuali progetti per le PA ai quali la Provincia potrebbe in futuro aderire.

3.3 ADEGUAMENTO DELLE PROCEDURE DI GESTIONE DELLE UTENZE

Quale elemento fondante per garantire un elevato grado di sicurezza degli accessi è stata individuata la necessità di attivare un processo di gestione integrata delle identità su tutte le principali applicazioni e piattaforme in uso presso la Provincia, relativamente alle tematiche di:

- Creazione, abilitazione, disabilitazione e cancellazione degli utenti, il ciclo di vita delle identità (normalmente detti processi di provisioning e de-provisioning);
- Profilazione iniziale e gestione dei ruoli, definizione delle autorizzazioni e gestione delle evoluzioni del ruolo aziendale;
- Autenticazione, la fase del riconoscimento dell'utente in base a qualcosa che sa (soft autentication, password) o a qualcosa che ha (strong authentication, smartcard).

Tale processo agevolerà inoltre l'adeguamento ed il rispetto di quanto previsto dalle normative di attuazione del Testo Unico sulla Privacy e delle norme interne di sicurezza descritte nel DPS.

Oggetto della fornitura sarà quindi un sistema di Identity Management (IDM) in grado di gestire la distribuzione delle utenze e degli attributi ad essi collegati, password compresa, all'interno di un insieme di sistemi connessi.

Il sistema di IDM implementato dovrà quindi avere le seguenti caratteristiche minime:

- Minimo impatto e massima integrazione possibile con i sistemi e le piattaforme attualmente utilizzato;
- Presenza di un directory service standard LDAP, come repository condiviso e centralizzato, contenente tutte le informazioni possibili su gli utenti e su ogni altro oggetto si volesse inserire nei processi di provisioning (es. Gruppi);
- La directory LDAP, come standard, dovrà avere lo schema modificabile, per consentire l'aggiunta di attributi e classi di aggetti anche non attualmente previsti;
- Capacità di sincronizzare bi-direzionalmente le informazioni tra il repository centrale e tutti i sistemi connessi, usando un set di policy configurabili che consentano una definizione flessibile per quanto riguarda:

  - i singoli attributi da sincronizzare per ogni oggetto e la direzione di sincronizzazione (dal repository ai sistemi connessi e/o viceversa)

  - la sorgente autoritativa del dato a livello di singolo attributo, con possibilità di ripristinare il valore originale in caso di modifica sui sistemi non autoritativi

  - la mappatura degli attributi tra i sistemi connessi e le eventuali regole di trasformazione;

  - la gestione degli eventi e le eventuali regole di trasformazione;

  - la possibilità di sincronizzare bidirezionalmente la password degli oggetti utenti, fatto salvo l'impossibilità oggettiva di sincronizzazione della password da un sistema connesso per il quale non sia noto l'algoritmo di crittazione;

- la possibilità di definire regole di riconciliazione di oggetti già esistenti per definire il popolamento iniziale del sistema;

- Possibilità di implementare policy nel repository centrale per il trattamento delle password (scadenza, complessità, unicità, etc), per renderle conformi a quanto previsto dal Testo Unico sulla Privacy e delle norme interne di sicurezza descritte nel DPS e di conseguenza forzare, attraverso la sincronizzazione, tali policy anche ai sistemi connessi;
- Logica di sincronizzazione near-real-time, preferibilmente event-driven;
- Log degli eventi completo e personalizzabile;
- Modalità di caching degli eventi tali da consentire il mantenimento delle informazioni da sincronizzare in caso di indisponibilità temporanea di uno o più sistemi connessi o delle relative linee di comunicazione;
- Comunicazione con i sistemi da sincronizzare con connessioni criptate o comunque sicure e per quanto possibile, agent-less cioè senza necessità di installare alcun componente sulle piattaforme da connettere;
- Nessuna necessità di modificare, in alcun modo, le applicazioni connesse;
- Strumenti visuali di sviluppo e di definizione delle policy "code-free" che non necessitano cioè di sviluppo e/o codifica di applicazioni specifiche;
- Possibilità di configurazione multipiattaforma (Windows o Linux) in alta affidabilità (cluster o similari);
- Disponibilità del maggior numero possibile di connettori verso sistemi eterogenei con la possibilità di connettere al minimo Novell eDirectory, Novell GroupWise, Microsoft Active Directory, database MS SQL, Oracle e MySQL

Le piattaforme da connettere, oggetto della fornitura, saranno indicativamente:

- Piattaforma Novell (eDirectory, GroupWise)
- Dotazione Organica;
- Contabilità, Personale e Paghe;
- Protocollo;
- IDOL (Incontro Domanda Offerta di Lavoro);
- Gestione opere pubbliche;
- Applicazioni proprietarie (Bacheca);

A titolo puramente esemplificativo, l'ipotesi progettuale potrebbe prevedere un flusso di informazioni del tipo:

- L'utente viene censito per la prima volta all'interno della procedura di gestione della dotazione organica. Le informazioni disponibili vengono raccolte e l'utente viene creato automaticamente nel repository centrale;
- L'utente viene creato dentro eDirectory di produzione con gli attributi necessari al login di rete e con la casella postale su GroupWise. L'utente può fare login alla rete e ricevere posta;
- Gli amministratori delle varie applicazioni, attraverso una apposita console web o con logiche automatizzate da definire, abilitano l'utente che ne ha diritto all'utilizzo delle

applicazioni per le quali hanno la responsabilità della gestione. Vengono creati gli account necessari nei database delle singole applicazioni e l'utente può iniziare ad usarle. Gli amministratori possono in un qualunque momento revocare l'abilitazione e gli account saranno disattivati o cancellati;

- Tutte le attività di provisioning e de-provisioning dovrebbero essere sottoposte ad un workflow approvativo multilivello e/o eventualmente basate su ruoli e profili applicativi;
- Ogni modifica effettuata agli attributi dell'utente sulle singole applicazioni viene riportata indietro nel repository centrale ed eventualmente aggiornata sulle altre applicazioni (sincronizzazione bidirezionale);
- Quando l'utente cessa il rapporto di lavoro e questo evento viene registrato all'interno della pianta organica, vengono cancellati o disattivati gli account dell'utente nel repository centrale e su tutte le applicazioni;
- Le applicazioni LDAP-ready potranno trovare le informazioni di cui necessitano direttamente dentro il repository centrale.

Per l'implementazione di questa architettura si stimano necessari due nuovi server in configurazione di tipo B di cui all'Allegato Tecnico D.

3.4 AUDITING DEGLI EVENTI LEGATI ALLA SICUREZZA INFORMATICA

Quale ulteriore elemento di completamento della architettura progettuale è stato identificata la necessità di disporre di un sistema di auditing centralizzato che consenta di avere, sia in real-time che su base storica, un log dei principali eventi accaduti nell'intero sistema di autenticazione descritto, per poter disporre di una base di analisi in caso di problemi o falle di sicurezza accertate.

Per quanto possibile tale sistema dovrà fornire strumenti in grado di segnalare proattivamente il verificarsi di tali condizioni.

3.4.1 LOG centralizzato

Implementazione di un software di raccolta degli eventi dal directory service di autenticazione e dal repository centrale delle utenze, con cui sia possibile tracciare in qualunque momento e storicizzare le attività di accesso alla rete e, possibilmente, di accesso al file system immagazzinandole in un database relazionale per future interrogazioni. A questo strumento potranno essere affiancati altri più specifici (tipo syslog) per monitorare gli accessi ad altri strumenti quali il firewall od il proxy.

Le informazioni minime da tracciare saranno:

- Flussi di provisioning e de-provisioning e relativi workflow;
- Attività di autenticazione e di accesso degli utenti;

Per l'implementazione di questa architettura si stima necessario un nuovo server in configurazione di tipo B di cui all'Allegato Tecnico D.

3.4.2 Monitoraggio di rete

La complessità della rete della Provincia, sia in termini di sistemi e servizi sia in termini di estensione geografica, suggerisce l'adozione di uno strumento di analisi e controllo del funzionamento e della fruibilità dei servizi erogati.

La soluzione realizzata dovrà costituire una rete di controllo dei parametri di funzionamento significativi dei principali apparati e i servizi da questi erogati, con lo scopo di realizzare:

- Gestione proattiva delle problematiche con segnalazione in tempo reale tramite e-mail e/o SMS ai sistemisti incaricati della manutenzione;
- Storicizzazione dei principali parametri di funzionamento a scopo statistico e di analisi dei trend di crescita.

Per l'implementazione di questa architettura si stima necessario un nuovo server in configurazione di tipo B di cui all'Allegato Tecnico D.

3.5 RIEPILOGO FORNITURE HARDWARE

In considerazione degli obiettivi del Progetto e delle aree di intervento sopra descritte, nella fornitura dovranno essere inclusi in totale i seguenti componenti hardware:

- 1 nuovo apparato IPS di cui all'Allegato Tecnico C (collegato al punto 3.1.3);
- 1 nuovo rack per server ed 1 switch KVM di cui all'Allegato Tecnico E (collegati al punto 3.1.2);
- 1 scheda FastEthernet 10/100baseT con 48 porte per lo switch HP 9100 di backbone (Codice HP J4881B) (collegato al punto 3.1.2);
- 2 schede GigaEthernet 1000baseT con 16 porte per lo switch HP 9100 di backbone (Codice HP J4895A) (collegato al punto 3.1.2);
- 6 dischi Fibre Channel da 146 GB / 10.000 rpm tipo Seagate ST3146707FC o similari, compatibili con la SAN Raidtec FibreArray 2104 (collegato al punto 3.1.2);
- 5 nuovi server in configurazione di tipo A di cui all'Allegato Tecnico D (collegati al punto 3.2.1);
- 8 nuovi server in configurazione di tipo B di cui all'Allegato Tecnico D di cui:

  - 2 collegati al punto 3.3
  - 4 collegati al punto 3.2.2
  - 1 collegato al punto 3.4.1
  - 1 collegato al punto 3.4.2

4. LICENZE ED ASSISTENZA SUI PRODOTTI

Tutti i prodotti hardware e software dovranno essere completi di ogni licenza d'uso o sottoscrizione necessaria al loro funzionamento, valida per minimo un anno e della relativa maintenance (upgrade protection, software assurance o quant'altro) che ne consenta il supporto e l'aggiornamento continuo delle caratteristiche o funzionalità (es. database IPS delle vulnerabilità), ove previsto, e di ogni nuova versione rilasciata dal produttore.

Tutte le forniture hardware dovranno essere conformi alle norme vigenti ed avere una garanzia del fornitore per almeno tre anni con modalità *on-site 8x5 NBD (Next Business Day)*

La copertura di licenza d'uso e d'installazione sui prodotti software/hardware, deve comprendere l'utilizzo da parte di almeno 200 utenti.

5. ANALISI PROGETTUALE ED ATTIVITÀ SISTEMISTICA

Tutte le forniture dovranno essere comprensive delle attività sistemistiche specializzate necessarie alla loro completa implementazione nell'ambiente operativo della Provincia, secondo le specifiche richieste funzionali.

Pertanto la Società fornitrice dovrà installare sui Server tutti i relativi sistemi operativi e predisporre tutte le configurazioni degli apparati e dei Software forniti in base alle specifiche di implementazione, già descritte nelle sezioni precedenti.

Le attività dovranno essere svolte da personale competente, con comprovata esperienza e munito delle certificazioni previste al successivo punto 8 del presente capitolato.

Inoltre dovranno essere rispettati i seguenti vincoli:

- ogni attività di analisi e le relative modalità operative dovranno essere concordate con il personale del Servizio Informatico dell'Ente
- tutte le attività di aggiornamento dovranno avvenire, con modalità preventivamente concordate con il personale del Servizio Informatico dell'Ente, riducendo al minimo il disservizio verso gli utenti interni ed esterni;
- le attività sistemistiche dovranno prevedere l'installazione, la configurazione dei sistemi forniti e la loro completa integrazione con i sistemi già in dotazione della Provincia; in particolare, ove necessario, dovranno essere realizzati tutti gli aggiornamenti dei sistemi preesistenti e la loro configurazione funzionale al progetto;
- tutte le attività sistemistiche dovranno essere svolte presso gli uffici della Provincia di Pistoia (Servizio Informatico);
- tutte le attività sistemistiche dovranno essere sempre svolte in affiancamento con il personale del Servizio Informatico;
- all'interno delle attività sistemistiche dovranno essere previste le necessarie azioni per erogare al personale del Servizio Informatico il know-how sufficiente alla gestione ed alla manutenzione di primo livello di tutti i sistemi forniti;
- dovrà essere consegnata al personale del Servizio Informatico idonea documentazione tecnica (sia in formato cartaceo che elettronico) in lingua italiana per la configurazione e la gestione di tutti i sistemi forniti oltre che la descrizione dettagliata di tutte le attività di configurazione e personalizzazione sui sistemi realizzate;
- gli interventi che saranno conteggiati sono quelli realizzati dal solo personale certificato così come descritto nel successivo punto 8 del presente capitolato.

6. DOCUMENTI DI PROGETTO

La soluzione richiesta non si compone di soli prodotti e della loro installazione e configurazione, ma deve comprendere elementi di analisi, proposte organizzative, aspetti gestionali e di coordinamento in fase di progetto e formativi. Le caratteristiche di complessità del progetto richiedono quindi la formalizzazione di una serie di documenti volti a condividere i contenuti del sistema, le sue modalità di realizzazione e le modalità di erogazione dei servizi richiesti, nonché il monitoraggio sullo stato di avanzamento del progetto

Dovranno dunque essere redatti i seguenti documenti:

- Piano di progetto, che rappresenta in dettaglio tempi e modi di realizzazione del sistema;

- Piano di test e collaudo;

- Piano di formazione.

Tutti i documenti, in bozza, devono essere contenuti nell'Offerta Tecnica, ed in versione definitiva dovranno essere consegnati secondo le scadenze stabilite nel Piano di Progetto e dovranno essere conformi a quanto richiesto nel presente Capitolato, nonché tenuti costantemente aggiornati.

La versione definitiva dovrà rispettare i contenuti della suddetta versione in bozza e tutti i Documenti di Progetto dovranno essere forniti sia su supporto cartaceo che elettronico

6.1 Piano di Progetto

Il Piano di Progetto, articolato su un arco temporale di 12 (dodici) mesi, è lo strumento essenziale in cui vengono identificate le attività da svolgere con le indicazione dei tempi previsti.

Il Piano di Progetto dovrà includere almeno le seguenti informazioni:

- una sintesi delle caratteristiche del progetto (requisiti e/o obiettivi che il progetto si prefigge di soddisfare);

- una descrizione dei prodotti e/o dei servizi che il progetto dovrà realizzare per soddisfare il contratto;

- la durata complessiva del progetto (inizio – fine);

- eventuali vincoli;

- indicazione del responsabile di progetto e dell'organizzazione;

- le risorse assegnate ed i relativi ruoli e profili professionali;

- la definizione della periodicità con cui verrà rilevato lo stato di avanzamento lavori e gli indicatori da utilizzare per misurare l'avanzamento;

- il piano di rilascio dell'infrastruttura tecnologica hw e sw;

- un coerente cronoprogramma (GANTT) delle macro-attività relative a ciascuna delle aree di intervento individuate dal progetto con contestuale definizione dei relativi "criteri di validazione".

Il Piano di Progetto dovrà prevedere una fornitura articolata in una serie di rilasci parziali successivi, in modo da rendere operativo il sistema (anche con un insieme parziale di funzionalità) il prima possibile.

Oltre alla completezza ed articolazione della soluzione proposta, che dovrà prevedere la descrizione dell'ambiente di sviluppo/test da attivare (a carico dell'Impresa aggiudicataria) per condurre i test architetturali e di integrazione con l'ambiente operativo di produzione, assumono particolare rilevanza nella valutazione del Piano di Progetto i tempi di esecuzione, laddove a parità di soluzione sarà premiato il progetto che presenterà tempi di esecuzioni minori.

6.2 Piano di test e collaudo

L'aggiudicatario dovrà descrivere metodologie e fornire gli strumenti atti a provare tutte le funzionalità del sistema e consentire di valutarne il corretto funzionamento.

Il Piano di test dovrà contenere le seguenti indicazioni:

- strategia del test: descrizione sintetica dell'approccio che si adotta per il test;

- elenco e descrizione dei test funzionali da effettuare;

- condizioni di partenza e valori attesi.

6.3 Piano di formazione

Il Piano di formazione dovrà contenere almeno i seguenti elementi:

- descrizione degli argomenti oggetto di formazione per le due tipologie di destinatari: amministratori (diretti e delegati) ed utenza finale (operatori degli uffici provinciali);
- descrizione del materiale didattico da distribuire ai partecipanti a ciascun modulo formativo;
- proposta di tempistica di svolgimento delle giornate di formazione.

A corredo del sistema è richiesta la documentazione relativa a personalizzazioni, parametrizzazioni e utilizzo delle funzioni. Tale documentazione dovrà avere e sarà valutata in base alle caratteristiche di comprensibilità, sinteticità, accuratezza, adeguatezza e aderenza all'oggetto.

In particolare la documentazione dovrà essere redatta in lingua italiana, dovrà comprendere la necessaria manualistica rivolta ad amministratori e utenza finale ed essere presentata in formato elettronico compatibile con Microsoft Office.

Tutta la documentazione deve essere consegnata in formato elettronico.

7. TEMPI E MODALITA' DELLA FORNITURA

Come meglio specificato all'art 1 "Oggetto della gara" del presente capitolato, la fornitura è articolata in quattro fasi denominate "Aree di intervento". Al termine di ciascuna fase, che comprende la consegna del materiale, la sua installazione e configurazione, tutte le attività connesse ed al termine di queste il collaudo, questa Amministrazione provvederà al pagamento di quanto dovuto che nello specifico sarà così determinato:

- Il costo dei prodotti hardware e software specificatamente necessari al completamento di ciascuna delle rispettive prime tre fasi di intervento, che dovrà essere specificato dall'aggiudicatario, più il 20% della parte rimanente, relativa al complesso delle attività da svolgere, così come indicato nella sezione relativa ai "Documenti di progetto"del presente capitolato.
- Al completamento della quarta ed ultima fase, ed a seguito di esito positivo del collaudo finale, sarà provveduto alla liquidazione dell'importo residuo della fornitura.

7.1 Materiale hardware

Il fornitore si obbliga ad effettuare la consegna del materiale hardware entro e non oltre 30 giorni dalla stipula del contratto o dall'ordine e, per le fasi successive alla prima, previo accordo con il Responsabile tecnico del Servizio Informatico.
La consegna dovrà essere effettuata presso gli uffici del Servizio Informatico – Piazza S. Leone, 1 Pistoia.
La consegna deve essere accompagnata da apposita distinta compilata dal fornitore contenente:

- la data di consegna;
- i riferimenti del contratto o dell'ordine;
- la specificazione della fornitura consegnata e, se del caso, la loro ripartizione in colli;

A seguito della consegna del materiale richiesto nella fase specifica, la sua installazione e configurazione e dopo le attività specificate per la fase suddetta, sarà effettuato, entro 30 giorni, il collaudo della fornitura consistente in un controllo sia qualitativo che quantitativo, di verifica della corrispondenza alle specifiche tecniche indicato nell'offerta e in un test di funzionalità dell'apparecchiatura, a cura del Responsabile del Servizio Informatico o suo delegato che

redigerà apposito verbale. Al collaudo potrà essere presente, se desiderato, un incaricato della Ditta aggiudicataria.
Al riguardo l'Amministrazione committente potrà:
- ordinare la rimozione dal luogo del collaudo, entro i termini specificati nell'aggiudicazione, delle forniture, non conformi al contratto;
- ordinare la sostituzione con forniture conformi ed appropriate entro 30 giorni. L'aggiudicatario deve provvedere a rimediare ai difetti indicati senza indugio e a sue spese. In caso di inadempimento da parte dell'aggiudicatario, il committente ha il diritto di assumere o retribuire altre persone per effettuare tali operazioni e di rivalersi sull'aggiudicatario stesso per tutte le spese ad esse conseguenti o inerenti ovvero di detrarre tali spese dalle somme a cui il fornitore ha o avrà diritto.
A seguito della sostituzione della merce non conforme, sarà redatto un ulteriore verbale di collaudo definitivo.

7.2 Materiale software, installazione e configurazione
Il fornitore si obbliga ad effettuare la consegna del materiale entro e non oltre 30 giorni dalla stipula del contratto o dall'ordine e, per le fasi successive alla prima, previo accordo con il Responsabile tecnico del Servizio Informatico.
La consegna del materiale software avverrà tramite la attribuzione alla Provincia delle relative certificazioni e licenze di uso, in formato cartaceo o elettronico.
Il software consegnato dovrà essere installato e configurato, sulle apparecchiature della Provincia previste dal presente capitolato e dovrà integrarsi con gli altri sistemi hardware e software della Provincia, così come descritti nel presente capitolato.
Al termine delle attività previste all'interno di ciascuna delle Aree di intervento specificate dal presente capitolato verrà effettuato da parte di personale tecnico del Servizio Informatico della Provincia ed entro 30 giorni, un collaudo della funzionalità del sistema e della sua corrispondenza alle specifiche richieste. Al collaudo potrà essere presente, se desiderato, un incaricato della Ditta appaltatrice.
Dell'avvenuto collaudo sarà redatto apposito verbale.

In caso di collaudo negativo l'Amministrazione committente potrà ordinare una nuova installazione e riconfigurazione sulle apparecchiature della Provincia di Pistoia più appropriata entro 30 giorni. L'aggiudicatario deve provvedere a rimediare ai difetti indicati senza indugio e a sue spese. In caso di inadempimento da parte dell'aggiudicatario, il committente ha il diritto di assumere o retribuire altre persone per effettuare tali operazioni e di rivalersi sull'aggiudicatario stesso per tutte le spese ad esse conseguenti o inerenti ovvero di detrarre tali spese dalle somme a cui il fornitore ha o avrà diritto.
A seguito della nuova configurazione sarà redatto un ulteriore verbale di collaudo definitivo.

8. ESPLETAMENTO DELLA GARA: REQUISITI DI PARTECIPAZIONE

Sono ammessi a partecipare alla presente procedura aperta tutti i soggetti di cui all'art. 34 del D.Lgs 163/2006 e s.m.i. che siano in possesso, oltre che di tutti i requisiti espressamente previsti dall'art. 38 lett. a-b-c-d-e-f-g-h-i-l-m-mis del D.Lgs 163/2006 e s.m.i., anche dei seguenti requisiti:

1. iscrizione alla C.C.I.A.A. per attività attinenti all'appalto in oggetto;
2. Certificazione aziendale ISO 9001;
3. Certificazione aziendale Novell Gold Solution Provider o superiore;

4. Aver effettuato con buon esito negli ultimi tre anni interventi analoghi a quelli descritti all'art. 1 ("Aree di intervento II e III) a favore di Pubbliche Amministrazioni o privati per un importo complessivo pari o superiore ad € 50.000,00;
5. Aver realizzato nei tre esercizi anteriori alla data di pubblicazione del bando (2004-2005-2006) un fatturato complessivo di almeno € 500.000,00.

Per i raggruppamenti temporanei di imprese i predetti requisiti dovranno essere ripartiti come segue:

- i requisiti di ordine generale ex art. 38 D.Lgs 163/2006 ed il requisito di cui al precedente punto 1) dovranno essere posseduti da ciascun soggetto facente parte del raggruppamento;
- il requisito di cui al precedente punto2) dovrà essere posseduto da almeno un soggetto associato;
- i requisiti di cui ai precedenti punti 3) e 4) dovranno essere posseduti dal soggetto che, nell'ambito del raggruppamento, effettuerà gli interventi di installazione, configurazione, assistenza e formazione;
- il requisito di cui al precedente punto 5) potrà essere cumulativamente posseduto dai soggetti associati

Per il controllo sul possesso dei predetti requisiti la stazione appaltante procederà ai sensi dell'art. 48 del D. Lgs 163/06.
Ogni concorrente, singolo o consorziato o raggruppato ai sensi dell'art. 34 D.Lgs 163/2006, potrà dimostrare il possesso dei requisiti economici, finanziari, tecnici e organizzativi avvalendosi dei requisiti di altro soggetto. A questo proposito si applica l'art. 49 D.Lgs 163/2006 con le seguenti precisazioni:
a) per quanto riguarda la documentazione prevista dal comma 2 lett. f) del predetto art. 49 il "contratto di avvalimento" dovrà indicare il titolo giuridico in base al quale l'impresa ausiliaria mette a disposizione le proprie risorse per tutta la durata del presente appalto;
b) il soggetto aggiudicatario ha l'obbligo di impiegare per l'espletamento dell'appalto esclusivamente il personale in possesso delle sopra dette certificazioni come indicato in fase di gara, pena l'applicazione dei successivi articoli 12 e 13.

9. IMPORTO DEL CONTRATTO DI APPALTO – PROCEDURA DI GARA E CRITERI DI VALUTAZIONE DELL'OFFERTA

L'importo complessivo del presente appalto ammonta ad € 220.833,32 oltre IVA di cui **€ 218.624,99** per importo **base di gara** ed **€ 2.208,33 per oneri per la sicurezza non soggetti a ribasso.** Il presente appalto verrà aggiudicato con il criterio dell'offerta economicamente più vantaggiosa per l'Amministrazione Provinciale, ai sensi dell'art. 83 D.Lgs 163/06 e s.m.i.
Ai fini della individuazione delle offerte anormalmente basse si applica l'art. 86 co. 2 D. Lgs. 163/06. Pertanto le offerte dovranno essere corredate, sin dalla loro presentazione, delle giustificazioni di cui all'art 87 co. 2 relative alle voci di prezzo che concorrono a formare il prezzo offerto. Nella valutazione dell'anomalia sarà tenuto conto che il valore economico dell'offerta sia adeguato e sufficiente rispetto al costo del lavoro ed al costo relativo alla sicurezza

L'offerta verrà giudicata da apposita Commissione Giudicatrice nominata dall'Amministrazione Provinciale secondo i disposti di cui all'Art. 84 del D.Lgs 163/2006. per la valutazione delle offerte la Commissione adotterà i seguenti criteri valutativi:

A. **Offerta economica**: massimo punti **60 su 100**
Ogni concorrente dovrà esprimere, in cifre ed in lettere, un prezzo complessivo inferiore rispetto ad € 218.624,99. Non sono ammesse offerte in aumento o condizionato o parziali.

I 60 punti, saranno attribuiti al soggetto che ha offerto il prezzo minore sulla base della seguente formula matematica:
Pi= (Minor prezzo offerto / prezzo offerto dal concorrente iesimo) x 60

B. **Valutazione tecnica**: massimo punti **24 su 100,** attribuiti secondo giudizio comparativo della commissione rispetto a:
   - Punti 15: soluzioni tecniche coerenti con la struttura sistemistica esistente e con il mantenimento delle conoscenze acquisite;
   - Punti 5: completezza e chiarezza del piano di lavoro e tempistica di esecuzione delle attività previste;
   - Punti 4: funzionalità aggiuntive offerte, coerenti con gli obiettivi del progetto;

C. **Presenza** all'interno dell'impresa o raggruppamento, dimostrabile con atti o documenti aventi data certa anteriore al bando, di personale professionalmente qualificato, operante come socio, dipendente o collaboratore continuativo: massimo punti **16 su 100** così determinati**:**
   - Presenza di personale munito di certificato M.C.P.: 2 punti per ogni soggetto fino a un massimo di 4 punti.
   - Presenza di personale munito di certificato Linux: 2 punti per ogni soggetto fino a un massimo di 4 punti.
   - Presenza di ulteriore personale munito di certificato C.N.E (Certified Novell Engineer), in aggiunta a quelli richiesti per la certificazione aziendale Novell Gold Solution Provider di cui al punto 3) dell'articolo precedente: 2 punti per ogni soggetto fino a un massimo di 4 punti.
   - Presenza di personale munito di certificazione OCP (Oracle Certified Professional), 2 punti.
   - Presenza di personale munito di altre certificazioni in ambito networking, purchè riconducibili alle tipologie di prodotti utilizzate nel presente progetto: massimo punti 2.

N.B.: Dovrà essere garantita la presenza di personale munito delle certificazioni dichiarate per tutta la durata del contratto pena l'applicazione dei successivi articolo 12 e 13.

Tra le offerte ammesse, l'aggiudicazione sarà affidata al concorrente che avrà totalizzato il punteggio complessivo più elevato, tenuto conto di tutti gli elementi di valutazione. Ad eventuale parità di punteggio complessivo, si procederà all'aggiudicazione al concorrente che ha offerto il prezzo più conveniente per l'Amministrazione.

10. OBBLIGHI DEL FORNITORE

Il fornitore provvede alla consegna del materiale richiesto nella singola area di intervento, alla sua installazione e configurazione con la debita cura e diligenza affinché la stazione appaltante consegua l'utilità perseguita con il presente affidamento; dovrà altresì contestualmente fornire manuali di istruzione d'uso e manuali necessari alla formazione del personale in lingua italiana.
Il fornitore non potrà effettuare cambiamenti di ordine quantitativo o qualitativo rispetto all'offerta presentata.
L'imballaggio, il trasporto (compresi eventuali permessi di importazione e sdoganamento), l'installazione, il collaudo e le istruzioni d'uso si intendono ricompresi nel prezzo offerto e pertanto sono eseguiti a cura e spese del fornitore.

11. ADEMPIMENTI PRELIMINARI IN MATERIA DI SICUREZZA SUI LUOGHI DI LAVORO. STIPULA DEL CONTRATTO

Trattandosi di fornitura comprensiva di posa in opera da effettuarsi presso gli uffici della stazione appaltante, la Provincia, prima della stipula del contratto, effettuerà un riunione di coordinamento

con il soggetto aggiudicatario al fine di fornire a quest'ultimo dettagliate informazioni sui rischi esistenti nell'ambiente in cui andrà ad operare e sulle misure di prevenzione ed di emergenza adottate in relazione all'attività ivi svolta. Al termine della riunione verrà redatto un apposito verbale con il quale concordemente la Provincia ed il soggetto aggiudicatario effettueranno una valutazione dei rischi esistenti e daranno atto delle misure adottate per eliminarli. Tale documento, ai sensi dell'art. 7 co. 3 D.Lgs 626/94 così come modificato dalla L. 123/2007, sarà allegato al contratto di appalto.
L'aggiudicatario è obbligato a comunicare alla stazione appaltante i rischi specifici derivanti dalla sua attività che verranno introdotti nell'ambiente in cui andrà ad operare.
La stipulazione del contratto, nella forma pubblico-amministrativa, con il soggetto aggiudicatario dovrà avvenire entro la data che verrà comunicata da parte dell'amministrazione appaltante nel rispetto dei termini di cui all'art. 11 co. 9 e 10 del D.Lgs. 163/2006.
Qualora l'aggiudicatario, previa diffida della stazione appaltante, non si presenti alla stipula del contratto di appalto si procederà alla revoca dell'aggiudicazione definitiva e all'incameramento della garanzia a corredo dell'offerta. È facoltà discrezionale della stazione appaltante procedere all'affidamento dell'appalto in favore del concorrente che segue in graduatoria ovvero all'affidamento dell'appalto mediante le procedure di cui al Codice Contratti Pubblici (D.Lgs 163/2006).
Tutte le spese ed imposte inerenti la stipulazione del contratto di appalto (bollo, registrazione del contratto, diritti di rogito, accessorie e conseguenti) sono a totale carico del soggetto aggiudicatario, senza alcun diritto di rivalsa. Il fornitore dovrà attenersi alle modalità di pagamento prescritte dalla Provincia, pena la revoca dell'aggiudicazione.

12. DISCIPLINA DELLE PENALI

Le penali sono applicabili per mancato rispetto delle condizioni di erogazione dei servizi. Le citate condizioni possono riferirsi a ritardo nello svolgimento delle attività e/o al mancato raggiungimento degli obiettivi di qualità.
Per mancato rispetto delle condizioni s'intende quello non giustificato e non sanato con sospensioni o proroghe accordate dall'Amministrazione ed esclusivamente imputabile a cause dovute al soggetto aggiudicatario o da esso provocate.
Le penali applicate per mancato rispetto delle condizioni di erogazione dei servizi, saranno detratte dalle fatture emesse e/o saranno incamerate dal deposito cauzionale definitivo prestato dalla ditta affidataria. In tale ultimo caso, l'applicazione della penale darà luogo all'incameramento della corrispondente quota dalla cauzione, con obbligo della ditta affidataria di provvedere alla sua reintegrazione entro 15 giorni.

Le modalità di applicazione delle penali ed i relativi importi sono di seguito riferiti:

Per ogni giorno di ritardo, anche nel caso dei collaudi, non imputabile alla Provincia, ovvero a forza maggiore o a caso fortuito, nella consegna, installazione, configurazione e tutte le altre attività previste e connesse di cui al presente capitolato, è applicata una penale pari al 2 per mille dell'importo di contratto, salvo il risarcimento dell'eventuale maggior danno.

Qualora fosse accertata l'assenza ingiustificata del personale della ditta aggiudicataria in servizio o si verifichino inadempimenti agli obblighi contrattuali, la Provincia contesterà per iscritto l'inadempienza ed applicherà una penale forfettaria di 200,00 Euro per ogni inadempimento accertato.

Nella nota di contestazione sarà prefissato un termine non inferiore a 15 giorni per la presentazione di eventuali osservazioni; decorso tale termine la Provincia, qualora non ritenga valide le giustificazioni addotte, applicherà le penali di cui al precedente comma.
Le penalità vengono detratte direttamente dal corrispettivo dovuto al fornitore.
Qualora le deduzioni raggiungano il 10% (o superiore) dell'importo di contratto, l'Amministrazione committente può risolvere il contratto, con escussione della garanzia prestata, salvo il risarcimento di maggiori danni.

13. RISOLUZIONE DEL CONTRATTO

La Provincia procederà alla risoluzione del contratto con preavviso di almeno 30 giorni solari, da comunicarsi mediante lettera raccomandata A.R., nei seguenti casi:

1. qualora taluno dei componenti l'organo di amministrazione o l'amministratore delegato o il direttore generale o il responsabile tecnico dell'aggiudicatario siano condannati, con sentenza passata in giudicato, per delitti di cui all'art. 135 D.Lgs 163/2006;
2. in caso di mancata sostituzione del personale certificato come dichiarato in sede di offerta previo avviso della stazione appaltante;
3. allorché il fornitore non esegua le forniture e i relativi servizi di installazione in modo strettamente conforme all'offerta e al presente capitolato e le penali applicate abbiano superato il 10% dell'importo contrattuale come previsto al precedente articolo 12;
4. qualora il fornitore ceda il contratto o lo dia in subappalto senza l'autorizzazione del stazione appaltante e fuori dai casi in cui ciò è consentito;
5. allorché il fornitore fallisca o divenga insolvente o formi oggetto di un provvedimento cautelare di sequestro o sia in fase di stipulazione di un concordato con i creditori o prosegua la propria attività sotto la direzione di un curatore, un fiduciario o un commissario che agisce per conto dei suoi creditori;
6. allorché il fornitore non ricostituisca la garanzia o l'assicurazione richiesta oppure una nuova garanzia o assicurazione, qualora, la cauzione prestata sia stata già escussa in tutto o in parte
7. per le aziende tenute all'applicazione dei commi 2 e 3 dell'art. 4 del D.Lgs 626/94 e.s.m.i., per mancata sostituzione del responsabile del servizio di prevenzione e protezione aziendale e del medico competente di cui all'art. 2 co. 1 lett. e) e d) D.Lgs 626/94 nel caso di venir meno degli stessi nel corso dell'esecuzione del contratto, previa diffida alla regolarizzazione;
8. per gravi e ripetute violazioni degli obblighi assicurativi, previdenziali e relativi al pagamento delle retribuzioni ai dipendenti impegnati nell'esecuzione dell'appalto accertate in contraddittorio col soggetto aggiudicatario, fatta salva l'applicazione dell'art. 1676 c.c.;
9. le gravi e ripetute violazioni delle misure attinenti alla sicurezza dei lavoratori accertate in contraddittorio fra la stazione appaltante e l'appaltatore;
10. l'impiego di personale non risultante dalle scritture o da altra documentazione obbligatoria qualora l'appaltatore non provveda alla immediata regolarizzazione su espressa diffida della stazione appaltante.
11. il mancato rispetto dell'obbligo di informare immediatamente la stazione appaltante di qualsiasi atto di intimidazione commesso nei suoi confronti nel corso dell'esecuzione del contatto con la finalità di condizionare la regolare e corretta esecuzione.

In caso di risoluzione per colpa del fornitore, l'Amministrazione committente è liberata da ogni obbligo sulla fornitura già erogata.

Nessuna parte può essere considerata inadempiente o colpevole di violazione degli obblighi contrattuali quando la mancata ottemperanza a tali obblighi sia dovuta a casi di forza maggiore

verificatisi dopo la data di stipula del contratto. Per “forza maggiore” si intendono calamità naturali o eventi imprevedibili che sfuggono al controllo delle parti e che non possono essere evitati neppure con la dovuta diligenza. In tali casi il fornitore non è passibile di ritenuta sui compensi dovuti, di penalità di mora o di risoluzione per inadempienza, se e nella misura in cui il ritardo nell’esecuzione o altre mancate ottemperanze agli obblighi contrattuali sono provocati da un caso di forza maggiore.
In conseguenza dell’avvenuta risoluzione del contratto, la Provincia escuterà la cauzione definitiva fermi restando l’applicazione delle penali, il risarcimento del danno, le segnalazioni all’Autorità di vigilanza sui Contratti Pubblici e le altre autorità competenti.

14. SUBAPPALTO

Il subappalto è consentito nei limiti ed alle condizioni di cui all’art. 118 del D.Lgs 163/2006 e s.m.i.
Qualora la ditta affidataria manifesti la volontà di avvalersi del subappalto, dovrà specificare in sede di offerta le parti della prestazione che intende subappaltare a terzi. Tale indicazione lascia impregiudicata la responsabilità del soggetto aggiudicatario.
L’affidatario del subappalto dovrà possedere tutti i requisiti di partecipazione richiesti per l’affidamento del presente appalto limitatamente alla prestazione effettuata, con particolare riferimento al possesso delle certificazioni richieste e/o dichiarate in sede di offerta.
I pagamenti all’aggiudicatario saranno effettuati solo previa effettuazione degli adempimenti di cui all’art. 35 co.32 del citato D.L. n° 223/2006.
La Provincia non provvede al pagamento diretto dei subappaltatori; pertanto ai sensi dell'articolo 118 co. 3 D.Lgs n° 163/2006, l’aggiudicatario dovrà trasmettere alla stazione appaltante, entro 20 giorni dalla data di ciascun pagamento effettuato nei confronti dei subappaltatori o cottimisti, le relative fatture quietanzate con indicazione delle ritenute di garanzia, pena la sospensione del pagamento in suo favore.
L’esecuzione delle prestazioni affidate in subappalto non potrà formare oggetto di ulteriore subappalto.
L'Aggiudicatario rimarrà comunque ugualmente responsabile, nei confronti della Stazione Appaltante, anche dei lavori subappaltati.

15. GARANZIE

Il fornitore garantisce che i beni forniti nell’ambito del contratto sono nuovi di fabbrica, dei modelli più recenti o comunque correntemente in uso e che essi contengono tutti i più recenti accorgimenti in termini tecnici e di antinfortunistica.
Ogni concorrente partecipante è tenuto a costituire apposita garanzia di esecuzione ai sensi dell’art. 75 del D. Lgs. n° 163/2006 come meglio specificato negli atti di gara.
Il concorrente aggiudicatario è tenuto a costituire la cauzione definitiva di cui all’art. 113 del D. Lgs. n° 163/2006 con le modalità che saranno specificate negli atti di gara.
L’esecutore del contratto è direttamente responsabile dei danni derivanti da cause a lui imputabili di qualunque natura che risultino arrecati dal proprio personale a persone o a cose, tanto dell’Amministrazione che di terzi, in dipendenza di omissioni o negligenze o, comunque, di un’esecuzione non corretta della prestazione.

16. PREZZO - PAGAMENTI

Il corrispettivo del presente appalto sarà rappresentato dal prezzo offerto dal concorrente aggiudicatario in sede di gara oltre € 2.208,33 per oneri per la sicurezza non soggetti a ribasso e oltre IVA.

I pagamenti saranno effettuati, nel rispetto della normativa vigente, entro 60gg dall'esito positivo del collaudo effettuato per ciascuna “Aree di intervento” dal dirigente o funzionario del Servizio Informatico dietro presentazione di regolare fattura.

17. RESPONSABILITA’ ED OBBLIGHI DEL CONTRAENTE

Il contraente è responsabile per infortuni o danni arrecati a persone o cose dell'Amministrazione o a terzi, per fatto proprio o dei suoi dipendenti e collaboratori, nell'esecuzione degli adempimenti assunti con il contratto, con conseguente esonero dell'Amministrazione da qualsiasi eventuale responsabilità a riguardo.

Il contraente è sottoposto a tutti gli obblighi verso i propri dipendenti e soci, risultanti da disposizioni legislative e regolamentari vigenti in materia di lavoro e di assicurazioni sociali ed assume a suo carico tutti gli oneri relativi.
Il contraente è obbligato ad attuare nei confronti dei propri dipendenti e soci se cooperative, occupati nelle prestazioni oggetto del contratto, condizioni previdenziali, normative e retributive non inferiori a quelle risultanti dai contratti collettivi di lavoro della categoria e degli accordi integrativi territoriali, e comunque nel rispetto della normativa in materia di sicurezza sui luoghi di lavoro.

18. DISPOSIZIONI GENERALI RELATIVE AI PREZZI

Il prezzo al netto dell’IVA si intende invariabile in modo assoluto in relazione a qualsiasi sfavorevole circostanza che potesse verificarsi dopo l’offerta. L’IVA fa carico all’Amministrazione come per legge.

19. OBBLIGHI DI RISERVATEZZA E DIRITTI DI PROPRIETA’

Il soggetto aggiudicatario ha l’obbligo di mantenere riservati i dati e le informazioni, ivi comprese quelle che transitano per le apparecchiature di elaborazione dati di cui venga in possesso e di non divulgarli in alcun modo e in qualsiasi forma e di non farne oggetto di utilizzazione a qualsiasi titolo per scopi diversi da quelli strettamente necessari all’esecuzione dell’appalto. L’obbligo di cui sopra sussiste, altresì, relativamente a tutto il materiale originario o predisposto in esecuzione delle attività affidate in appalto.
L’obbligo di cui sopra non concerne i dati che siano o divengano di pubblico dominio, nonché le idee, le metodologie e le esperienze tecniche che il soggetto aggiudicatario sviluppa o realizza in esecuzione delle prestazioni dovute.
Il soggetto aggiudicatario è responsabile per l’esatta osservanza da parte dei propri dipendenti, consulenti e collaboratori, nonché dei propri eventuali subappaltatori e dei dipendenti, consulenti e collaboratori di questi ultimi, degli obblighi di riservatezza anzidetti.
In caso di inosservanza degli obblighi di riservatezza, l’Amministrazione appaltatrice ha la facoltà di dichiarare risolto di diritto il contratto, fermo restando che l’aggiudicatario sarà tenuto a risarcire tutti i danni che dovessero derivare all’Amministrazione appaltatrice.
Il soggetto aggiudicatario potrà citare i termini essenziali del contratto laddove ciò fosse condizione necessaria per la partecipazione dell’impresa stessa a gare e appalti.
Il soggetto aggiudicatario si impegna, altresì, a rispettare quanto previsto dal D. Lgs. 30/06/2003 n. 196.
Tutto il software e la documentazione eventualmente prodotti durante l’attività contrattuale saranno di esclusiva proprietà della Provincia di Pistoia che, in base alle vigenti norme di legge, potrà avvalersi della facoltà di riutilizzare, completamente o in parte, durante il periodo di vigenza contrattuale e dopo il suo termine, quanto prodotto. Tutti i dati gestiti dal sistema sono e restano, in ogni caso, di esclusiva proprietà della Provincia di Pistoia.

20. CONTROVERSIE – FORO COMPETENTE

Per qualsiasi controversia sarà esclusivamente competente il Foro di Pistoia. E' escluso il ricorso all'arbitrato di cui agli artt. 806 e ss. C.p.c

21. CESSIONE DEL CREDITO – CESSIONE DEL CONTRATTO

La Provincia non aderirà a cessioni di credito relative alla presente fornitura. È vietata la cessione di tutto o di parte del contratto, pena la risoluzione di diritto del contratto, la perdita della cauzione definitiva, nonché il risarcimento di ogni danno conseguente.
I suddetti provvedimenti saranno adottati da questa Amministrazione con semplice atto amministrativo, senza bisogno di messa in mora, né di pronuncia giudiziale.

22. INFORMATIVA AI SENSI DEL D. LGS. 196/2003

In ottemperanza al D.Lgs. 30.06.2003 n. 196 "Codice in materia di protezione dei dati personali" i dati raccolti in occasione della gara d'appalto di cui al presente Capitolato, verranno utilizzati al solo fine dell'espletamento della stessa.
Il trattamento dei dati verrà effettuato con le modalità e le forme previste dall'art. 11 del D.Lgs. 196/2003.

23. NORME DI RINVIO

Per quanto non espressamente previsto nel presente capitolato, si richiamano il D.Lgs 163/2006 s.m.i., L.Reg. Tosc. 38/2007, le norme del Codice Civile e le eventuali normative in materia.

24. RESPONSABILITA' DEL PROCEDIMENTO

Ai fini della presente gara il responsabile del procedimento è il Dirigente Economo Provveditore Maurizio Bardini tel. 0573-374252.

ALLEGATI TECNICI

Allegato Tecnico A – Sedi della Provincia di Pistoia

	LOCALITA	INDIRIZZO	DESCRIZIONE_UFFICIO
01	Massa e Cozzile	Via 1 Maggio	Centro Operativo Strade Villa Anuri
02	Monsummano Terme	Piazza del Popolo, 97	Centro per l'Impiego di Monsummano Terme
03	Pescia	Via Dilezza, 2	Centro per l'Impiego di Pescia
04	Pistoia	Corso Gramsci, 110	Servizio Agricoltura e Patrimonio Naturale, Servizio Pianificazione Territoriale, Cartografia (SIT)
05	Pistoia	Piazza della Resistenza, 54	Servizio Tutela dell'Ambiente, Servizio Difesa del Suolo e Demanio Idrico, Polizia Provinciale
06	Pistoia	Piazza San Leone, 1	Sede Centrale, Servizio Informatica e Sala Macchine, Presidenza, Direzione Amministrativa, Direzione della Programmazione, Segreteria e URP, Personale, Bilancio, Ragioneria
07	Pistoia	Via Cavour, 37	Palazzo Baly
08	Pistoia	Via Mabellini, 9	Servizio Cultura
09	Pistoia	Via Mariotti, z.i. S.Agostino	Deposito Archivio, Magazzino Economato
10	Pistoia	Via Panconi, 14	Centro Operativo Fabbricati Auditorium
11	Pistoia	Via Petrini, 4	Servizio Lavoro e Politiche Sociali
12	Pistoia	Via Traversa della Vergine	Protezione Civile
13	Pistoia	Via Tripoli, 19	Servizio Istruzione, Formazione e Cultura Centro per l'Impiego di Pistoia
14	Pistoia	Via Vecchia Fiorentina, 71	Centro Operativo Strade Mariano
15	Pistoia	Viale Adua, 94	Centro Operativo Fabbricati Viale Adua
16	Quarrata	Via IV Novembre, 119 - Vignole	Sportello Territoriale di Quarrata
17	San Marcello P.se	Via Ximenes, 341 - Limestre	Sportello Territoriale di San Marcello P.se
18	San Marcello P.se	Zona Industriale Loc. Oppiaccio	Centro Operativo Strade San Marcello P.se

Allegato Tecnico B – Elenco dei server esistenti

	SEDE	MARCA	MODELLO	SISTEMA_OPERATIVO	CPU	RAM	NOTE
	SEDE CENTRALE						
1	PIAZZA SAN LEONE - PISTOIA	HP	DL 380	NETWARE 6.1	XEON	1 Gb (4x256) 6 slot totali	PTSEDECL01- NOVELL CLUSTER SERVICES 1.6 - CLUSTER NODO 01 (NDPS - FILESYSTEM - DNS - DHCP - POST OFFICE - DOMINIO POSTA - PROXY - WEBACCESS) COLLEGATO CON GLI ALTRI DUE CLUSTER CON FIBRE CHANNEL 2Gbps
2	PIAZZA SAN LEONE - PISTOIA	HP	DL 380	NETWARE 6.1	XEON	1 Gb (4 x256) 6 slot totali	PTSEDECL02 - NOVELL CLUSTER SERVICES 1.6 - CLUSTER NODO 02 (NDPS - FILESYSTEM - DNS - DHCP - POST OFFICE - DOMINIO POSTA - PROXY - WEBACCESS) COLLEGATO CON GLI ALTRI DUE CLUSTER CON FIBRE CHANNEL 2Gbps
03	PIAZZA SAN LEONE - PISTOIA	HP	DL 380	NETWARE 6.1	XEON	1,5 Gb (6x256Mb) 6 slot totali	PTSEDECL03 - NOVELL CLUSTER SERVICES 1.6 - CLUSTER NODO 03 (NDPS - FILESYSTEM - DNS - DHCP - POST OFFICE - DOMINIO POSTA - PROXY) COLLEGATO CON GLI ALTRI DUE CLUSTER CON FIBRE CHANNEL 2Gbps
04	PIAZZA SAN LEONE - PISTOIA	COMPAQ	PROLIANT ML530T	WINDOWS NT 4.0	PENTIUM III	768 Mb	APPLICATIVI STR LINEA32 PER OPERE PUBBLICHE – DB ORACLE
05	PIAZZA SAN LEONE - PISTOIA	HP	DL 380	WINDOWS 2000 SERVER	XEON	1 Gb (4x256) 6 slot totali	PTSEDESRV01 CONSOLE ANTIVIRUS - BACHECA - SCHEDULATORE
06	PIAZZA SAN LEONE - PISTOIA	HP	DL 360	WINDOWS 2003 SERVER	XEON	2 Gb (2x256+512) 4 slot totali	PTSEDESRV02 - DNS PUBBLICO E ANTIVIRUS PER E-MAIL - INTERSCAN
07	PIAZZA SAN LEONE - PISTOIA	HP	DL 380	LINUX RED HAT 7.3	XEON	1 Gb (2x512) 6 slot totali	PTSEDEIDOL01 - RAID 5 - PROCEDURA IDOL - TOMCAT 4.0.3 - SERVER APACHE 1.3.27
08	PIAZZA SAN LEONE - PISTOIA	COMPAQ	PROLIANT ML 530T G2	LINUX RED HAT 7.2	XEON	2 Gb (1024+2x512)	PTSEDEIDOLDB01 - DATABASE IDOL ORACLE 8.1.7

09	PIAZZA SAN LEONE - PISTOIA	HP	DL 380	ICS	XEON	512 Mb (2x256)	PTSEDEICS01- I-CHAIN REVERSE PROXY	
10	PIAZZA SAN LEONE - PISTOIA	HP	DL 380	WINDOWS 2000 SERVER	XEON	1.5 Gb (2x256+512) 6 slot totali	PTSEDEBKP01 – CONSOLE AMMINISTRAZIONE BACKUP EXEC	
11	PIAZZA SAN LEONE - PISTOIA	HP	DL 380	NETWARE 6.1	XEON	512 Mb (2x256) 6 slot totali	PTSEDENPS01 - PORTALE NOVELL	
12	PIAZZA SAN LEONE - PISTOIA	HP	DL 380	WINDOWS 2003 SERVER	XEON	3 Gb (2x1Gb+2x512) 6 slot totali	PTSEDEWEB01 – WEB SERVER X SITO INTERNET	
13	PIAZZA SAN LEONE - PISTOIA	HP	DL 380	LINUX SUSE VER. 9	XEON	1 Gb ( ) 6 slot totali	PTSEDEWEB03 - APPLICATIVI URP E PORTALE TURISMO – DB ORACLE	
14	PIAZZA SAN LEONE - PISTOIA	HP	DL 380	WINDOWS 2000 SERVER	XEON	2 Gb (4x512) 6 slot totali	PTSEDEAPP01 - APPLICATIVI ADS CONTABILITA' E PERSONALE- DATABASE ORACLE	
15	PIAZZA SAN LEONE - PISTOIA	HP	PROLIANT DL385	WINDOWS 2003 SERVER	AMD OPTERON 270	2 Gb (2x1Gb) 6 slot totali	PTSEDEAPP02 - APPLICATIVO PROTOCOLLO - DB ORACLE	
16	PIAZZA SAN LEONE - PISTOIA – SEDE	HP	DL 380	NETWARE 6.1	XEON	512 Mb (2x256) 6 slot totali	PTSEDEFAX01 - FAX SERVER	
17	PIAZZA SAN LEONE - PISTOIA	HP	ML 370	PETRA NAL	2xXEON	4 Gb	IN DMZ2 - UTILIZZATO PER IL NODO APPLICATIVO LOCALE DIELLA RETE REGIONALE	
18	PIAZZA SAN LEONE - PISTOIA	FUJITSU COMPUTERS - SIEMENS	PRIMERGY TX200 S2	LINUX ENTERPRISE SERVER 9	2 x XEON	2.5 Gb	APPLICATIVI PROGETTO GENESI	
	SEDI PERIFERICHE							
19	VIA PETRINI - PISTOIA - CENTRO DIREZIONALE LAVORO		HP	PROLIANT ML350T	NETWARE 6.1	XEON 3.0	1 Gb	SERVER DI SEDE LOCALE
20	CORSO GRAMSCI - PISTOIA - AGRICOLTURA E PIANIFICAZIONE		HP	ML350 G4	NETWARE 6.5	XEON	1 Gb	SERVER LOCALE X CARTOGRAFIA
21	CORSO GRAMSCI - PISTOIA - AGRICOLTURA E PIANIFICAZIONE		HP	PROLIANT ML350T	NETWARE 6.1	XEON 3.0	1 Gb	SERVER DI SEDE LOCALE
22	VIA TRIPOLI - PISTOIA - I.F.P. E CENTRI IMPIEGO		HP	NETSERVER LH3	NETWARE 6.1	PENTIUM II	896 Mb	SERVER DI SEDE LOCALE
23	PIAZZA RESISTENZA - PISTOIA - TUTELA AMBIENTE		COMPAQ	PROLIANT ML 350	NETWARE 6.1	PENTIUM III	1 Gb	SERVER DI SEDE LOCALE
24	VIA MABELLINI - PISTOIA - CULTURA		BULL	EXPRESS 5800 MH4500	NETWARE 6.1	PENTIUM III	768 Mb	SERVER DI SEDE LOCALE
25	VIA TRAVERSA DELLA VERGINE - PISTOIA - PROTEZIONE CIVILE		IBM	P96DGIT X225	NETWARE 6.0 SP5	XEON	512	SERVER DI SEDE LOCALE

	Caratteristiche Funzionali
Network and Filtering	• Routed, translated, bridged e hybrid mode • Routing by interface • Dynamic routing (RIP, BGP, OSPF) • Supporto per almeno 128 VLANs • Built-in Dialup router (PPTP, PPPoE, PPP) • Address Translation (NAT, 1 to 1, PAT e Split) • Time Scheduling • Policy rule (NAT, filter, URL) compliance checker • xDSL High Availability HA e Load Balancing • Supporto per almeno 12 xDSL o Dialup modems • Dynamic bandwidth management • Quality of Service management (Stateful QoS) • Alias IP support (multiple IP addresses per interface)
Intrusion Prevention System	• Real Time Intrusion Prevention • Protocolli supportati: IP, TCP, UDP, HTTP, FTP, DNS, RIP, H323, Edonkey, SSL, SSH, Telnet, SMTP, POP3, IMAP4, NNTP • Multi-layer analysis (protocol and application layers) • rilevazione e blocco di attacchi (codificati e non) • Flooding protection (ICMP, UDP e TCP) • Blocks data evasion • Protezione da Trojan horses/backdoors • Protezione da Session hijack • Aggiornamento automatico dei “Contextual Signatures” • Quarantena permanente e temporanea • Applicazione di filtri P2P e Instant Messaging • Protezione Antispyware • Protezione da “vulnerability scanners”
IPSEC	• Protocolli VPN supportati: IPSec e PPTP • Supporto di almeno 64 PPTP VPN clients • Supporto crittografia a 256 bit per DES, 3DES, AES, CAST128 e Blowfish • autenticazione SHA-1 & MD5 • autenticazione attraverso pre-shared keys, certificati X509 o statica • Hub & Spoke VPN • Gateway – Gateway VPN tunnels • Client - Gateway VPN tunnels • VPN Keep-alive • Dead Peer Detection • NAT-Traversal (UDP 500 e 4500)
SSL VPN	• Clientless SSL VPN access supported • WEB Mode: access to web servers • Full Mode: access to applications via JAVA applets • User profile management
High Availability	• Attiva / Passiva • Sincronizzazione della configurazione

	• Session replication • Detection di “technical failures”
Antispam	• DNS Blacklisting • Combined heuristic analyses
Autenticazione	• Supporto per Single-Sign-On • LDAP Authentication (Interna ed Esterna) • Windows Authentication (NT4 – NTLM e WIN2K Kerberos) • Radius • Internal PKI CA & CRL • External PKI compatibility • Web enrolment (creazione di utenti e certificati)
Servizi	• HTTP Proxy - URL filtering • Supporto ICAP per URL filtering • SMTP Proxy • POP3 Proxy • DynDNS • DNS Cache Proxy • SNMP v1, v2 e v3 • Supporto NTP • DHCP Server interno • Aggiornamento Automatico del firmware e del software di amministrazione
Logging / Monitoring	• Notifica tramite E-mail • SNMP v1, v2 e v3 • Real Time Monitor • Syslogging • Internal Log Storage • Historical Reporting • Packet Dumping
Management	• Firewall Manager (Windows GUI) • Firewall Monitor (Windows GUI) • Firewall Reporter PRO (Windows GUI) • Global Administration for 5 appliances • Syslog, SSHv2, Console
Certificazioni	• Common Criteria EAL 2+ • ICSA Labs v4.0

	Caratteristiche Prestazionali
IPS-Firewall performance (**con IPS attivo**)	1,6 Gbps
AES VPN performance	210 Mbps
1000 Base T Interface	10 porte
Connessioni simultanee	600.000
Numero di regole di filtering supportate	16.384
Numero di IPSec VPN tunnels	3.750
Client-Gateway IPSec VPN Tunnels	Sì
SSL VPN Tunnels	Sì
Massimo numero di utenti	Illimitato
	Caratteristiche Hardware
Numero di porte Gigabit:	10
Storage	74 GB
Dimensioni	1U / 19’’
Control connection	RS-232C serial port, VT100 emulation, Mini-din keyboard, VGA screen

Configurazione Tipo A

Processore, sistema operativo e memoria

Processore	Processore Intel Xeon DualCore (od equivalente) a 3 GHz o superiore Numero di processori installati: 2 processori
Cache interna	4 MB (1 x 4 MB) di cache livello 2
Slot per memoria	8 slot DIMM
Memoria RAM	memoria installata: 4 GB. Possibilità di espansione a 32 GB
Tipo di memoria	DIMM Fully Buffered PC2-5300 (DDR2-667) con disponibilità interlacciamento 4:1 e 2:1 (l'interlacciamento richiede DIMM identici)

Unità interne

Memoria di massa interna	Controller del disco rigido: Controller per RAID 0/1/1+0/5/6. Alloggiamenti unità interne: 6 alloggiamenti per unità small form factor (SFF) hot plug per il supporto di unità disco Serial-attached SCSI (SAS) Memoria di massa installata: 2 dischi da 146GB (o superiore) a 10k RPM SAS drive hot plug
Unità dischi ottici	Unità combo DVD-ROM/CD-RW IDE

Caratteristiche del sistema

Chassis	Rack 1U
Montaggio in rack	deve essere dotato di un sistema di guide a rapida installazione per essere montato senza la necessità di attrezzi su rack con fori di montaggio quadrati o tondi con un intervallo di regolazione di 24" - 36". Il braccio di gestione dei cavi ambidestro può essere montato sia sulla sinistra che sulla destra per una migliore gestione dei cavi.
Porta I/O	Seriale - 1; Dispositivo di puntamento (Mouse) - 1; Tastiera - 1; VGA - 1; Rete RJ-45 - 2; porta gestione remota - 1; porte USB 2.0 - 5 (1 fronte, 2 retro, 1 interna)
Interfaccia di rete	Adattatore di rete integrato con porta doppia PCI-X 10/100/1000T Gigabit
Slot di espansione	Due (2) slot PCI-Express disponibili
Sistemi operativi compatibili	Microsoft® Windows® Server 2000; Microsoft®

	Windows® Server 2003; Novell NetWare; LINUX (Red Hat, SuSE); SCO UnixWare, OpenServer.
Tipo di alimentazione	Alimentatore ridondante hot plug CA 700 watt conforme al marchio CE
Requisiti di alimentazione	da 100 a 132 V CA, da 200 a 240 V CA; 50/60 Hz
Dimensioni	(L x P x A) 42,62 x 70,49 x 4,32 cm
Standard di settore per la conformità	Conformità ACPI 2.0; conformità PCI 2.2; supporto per WOL; certificazioni Logo Microsoft®; supporto per USB 2.0
Gestione della sicurezza	Password di avvio; Password per tastiera, Controllo floppy disk; Controllo dell'avvio da floppy; QuickLock, Modalità server di rete; Controllo interfaccia parallela e seriale; Password amministratore; Blocco di configurazione del disco
Facilità di manutenzione	Il sistema di guide a rapida installazione include guide scorrevoli universali, un braccio di gestione dei cavi ambidestro e leve a rilascio rapido per manutenzione rapida e semplice; Accesso senza attrezzi a tutti i componenti di sistema per manutenzione semplice in rack
Garanzia standard	3 anni sulle parti, 3 anni sulla manodopera e 3 anni di assistenza on-site

Configurazione Tipo B

Come configurazione di tipo A ma con un solo processore installato e 2 GB di memoria RAM.

- Rack: Caratteristiche Tecniche

Caratteristiche	
Tipo prodotto	Rack
Materiale prodotto	Metallo
Dimensioni rack	19"
Altezza (unità rack)	42U
Larghezza	80 cm
Profondità	100.8 cm
Altezza	200 cm
Peso	inferiore ai 150 kg
Miscellanea	
Limite di peso	non inferiore ai 450 kg
Caratteristiche	Porta frontale bloccabile, porta posteriore bloccabile Accoppiabile con gli armadi rack esistenti
Garanzia del produttore	
Servizi e supporto	3 anni di garanzia
Dettagli servizi e supporto	Garanzia limitata - parti - 3 anni

- Switch KVM (Keyboard-Video-Mouse) a 16 porte per montaggio in Rack

Caratteristiche:

Switch console server KVM a 16 porte, dotato di interfaccia OSD (On-Screen Display) per l’accesso ai dispositivi collegati.

Tutti i cavi di collegamento inclusi.