UFFICIO SPECIALE

PER LA CRESCITA E LA TRANSIZIONE DIGITALE

ALLEGATO 3 - CAPITOLATO TECNICO

AFFIDAMENTO DI “SERVIZI DI SYSTEM MANAGEMENT PER LA GIUNTA REGIONALE DELLA CAMPANIA” MEDIANTE APPALTO SPECIFICO NELL’AMBITO DELL’ACCORDO QUADRO PER LA PRESTAZIONE DI SERVIZI DI SYSTEM MANAGEMENT PER LE PUBBLICHE AMMINISTRAZIONI STIPULATO DA CONSIP

Indice

1 PREMESSA

Il presente Appalto Specifico rientra nell'ambito dell'Accordo Quadro stipulato da Consip con più operatori economici per la prestazione di servizi di System Management per le Pubbliche Amministrazioni.

Le indicazioni contenute nel presente Capitolato Tecnico rappresentano i requisiti minimi dell'Appalto Specifico (i quali, salvo diversa indicazione, debbono intendersi come aggiuntivi ai requisiti già espressi nel Capitolato Tecnico dell'Accordo Quadro) che devono essere soddisfatti per l'affidamento dei servizi.

In allegato al presente Capitolato Tecnico vengono riportate le seguenti Appendici:

- Appendice 1: "Indicatori di qualità generali";
- Appendice 2: "Descrizione contesto tecnologico".

Nel corpo del presente Capitolato Tecnico, con il termine:

- "AQ" si intende l'Accordo Quadro stipulato da Consip;
- "AS" si intende il presente Appalto Specifico;
- "Amministrazione", indica nel complesso le strutture organizzative facenti capo alla Giunta Regionale della Campania;
- "Fornitore/i AQ" si intende l'Impresa/le Imprese Fornitrice/i selezionate nell'ambito dell'Accordo Quadro;
- "Fornitore AS" si intende l'Impresa Fornitrice aggiudicataria dell'Appalto Specifico;
- "CRED" si intente il Centro Elaborazione Dati della Regione Campania;
- "NOC" (Network & Security Operation Center) si intende una struttura altamente specializzata nel campo delle reti e della sicurezza;
- "SOC" si intende una struttura altamente specializzata sulla sicurezza informatica;
- "SIS" si intende una struttura altamente specializzata nella nell'installazione, configurazione ed amministrazione di Sistemi Operativi, Sistemi di virtualizzazione, Infrastrutture di Iperconvergenza, Storage/Backup, DBMS e infrastrutture Cloud
- "PDL" si intendono personal computer fissi e portatili nonché le periferiche ad essi associate (monitor, scanner, webcam e stampanti personali):

2 CONTESTO ORGANIZZATIVO

La regione Campania si struttura per livelli gerarchici le cui macrostrutture si distinguono per il riferimento apicale e per i temi trattati.

Le seguenti strutture riferiscono al presidente di giunta e si occupano di temi trasversali riguardanti l'ente:

- Uffici Speciali: 6
- Autorità di Audit

- Strutture di Missione: 2

Le direzioni generali riferiscono agli assessori di giunta e sono responsabili di specifici temi amministravi per un totale di 17 unità organizzative.

L'Ufficio Speciale per la Crescita e la Transizione Digitale, attraverso il suo Servizio "Infrastrutture digitali", detiene la titolarità e la competenza per la progettazione, lo sviluppo e la gestione dei sistemi server e delle postazioni client, la gestione dei Data Center Regionali e per la progettazione e definizione delle politiche e dei piani di sicurezza delle infrastrutture digitali regionali.

Per maggiori dettagli sul contesto organizzativo, si faccia riferimento al sito della Regione Campania:

Uffici e contatti - Regione Campania

3 CONTESTO TECNICO

Il datacenter di Regione Campania ospita diversi cluster di server fisici che, tipicamente, vengono virtualizzati con Hypervisor VMware Esxi per l'erogazione dei servizi IT.

L' infrastruttura più recente è stata realizzata con cluster di 29 server (DELL POWEREDGE R7425) virtualizzati utilizzano la soluzione VMware (vCenter 7, vSphere con vSAN). Attualmente, ospita la maggior parte dei servizi erogati dal datacenter ed è in corso la migrazione delle restanti VM dalla precedente infrastruttura.

All'interno di questa infrastruttura sono ospitati anche 4 ambienti di containerizzazione basati su Kubernetes e Rancher.

La precedente infrastruttura è composta da 64 server blade (Dell M610 e Hitachi 520H) connessi ad una storage area network per accedere a uno storage di 250 Tb (Hitachi G1000). Questa infrastruttura è in corso di dismissione, soprattutto per quanto riguarda la SAN, potendo I server connettersi via NFS ad altri storage di rete. Pertanto, verranno mantenuti attivi 4 chassis Dell e 3 chassis Hitachi che continueranno ad essere virtualizzati e gestiti con il vCenter 6 (no vSan).

Lo storage utilizzato dal datacenter sia per le machine virtuali che per i dati viene erogato da tre diversi sistemi:

- storage prestazionale per una capacità totale di circa 700 Tb è ottenuto dai dischi ssd dell'infrastruttura VMware vSan
- storage capacitivo per un totale di circa 1.200 Tb è ottenuto da un apparato NAS di tipo scale-out (Dell EMC Isilon A2000/H500).
- storage per l'archiviazione a lungo termine (313 Tb) che utilizza l'apparato Dell EMC ECS EX3000 che esporta object storage (S3, Swift).

È presente un'infrastruttura iperconvergente (Nutanix) che ospita la Virtual Desktop Infrastructure Citrix in uso presso la Regione Campania in grado di erogare fino a 2100 desktop virtuali. I server sono distribuiti sui due siti (6 nodi a Via Don Bosco e 4 nodi al Centro Direzionale Is. A6) interconnessi in fibra a 10 Gb.

Il datacenter è dotato anche di una infrastruttura hardware non virtualizzata dedicata all'ambiente SAP, in particolare al database SAP HANA, costituita da 8 server HPE Proliant DL560 Gen10 con sistema operativo Red Hat Enterprise Linux for SAP Solutions ed una capacità di storage utile di circa 48 Tb ssd e 48 Tb hdd.

L'infrastruttura di rete del datacenter della Giunta Regionale della Campania è realizzata in tecnologia Brocade VCS. In particolare:

- Il blocco di accesso è realizzato con switch Brocade VDX 6740 in configurazione Spine/Leaf ed installati in modalità Top-of-Rack (ToR). Questi, garantiscono il collegamento a 10Gbps verso tutti i server (blade) grazie al protocollo FCoE.
- Per il blocco Core è installata una coppia di switch L3 Brocade ICX 7740, collegati tra loro con un doppio collegamento 40 GbE, a formare uno stack a elevata capacità con 160 Gbps.
- Il blocco applicativo include anche gli apparati di bilanciamento di carico L4-L7 mediante un Application Delivery Controller (ADC) Brocade ADX 1000.
- L'infrastruttura di server VMware vSan utilizza per ogni armadio una coppia di switch Dell S5224F-ON con porte a 25Gbit ed è interconnesso al core con link a 10Gb.
- L'infrastruttura iperconvergente Nutanix utilizza per il networking una coppia di switch Huawei 6720 con porte a 10Gbit e uplink a 10Gb verso gli switch di core.

L'architettura di sicurezza prevede l'utilizzo di 3 coppie di Firewall FortiGate, in cluster attivo-passivo:

- Cluster FortiGate 900D: a protezione della porzione di Front-End del Data Center. Nello specifico, l'apparato si occupa di gestire tutte le connessioni verso Internet e di mettere in sicurezza le DMZ che ospitano servizi pubblicati all'esterno.
- Cluster FortiGate 900D: quale punto di accesso per le VPN.
- Cluster FortiGate 1500D: protegge le subnet di Back-End del Data Center e, in linea generale, tutte quelle porzioni di rete che ospitano sistemi che richiedono un più elevato grado di sicurezza e che non sono esposte su Internet.

La soluzione di backup è la Dell EMC Data Protection Suite che utilizza il software Networker abbinato a due Data Domain Virtuali che, a loro volta, utilizzano lo storage Hitachi HUS110 con 200TB utili per il salvataggio dei dati deduplicati.

La Giunta Regionale della Campania ha circa 135 sedi periferiche, di cui 60 con funzioni di Centri per l'Impiego, distribuite su tutto il territorio regionale ed una sede a Roma, collegate in MPLS al nodo di centro stella del data center di Don Bosco. Le sedi del Centro Direzionale di Napoli (A6, C3, C5) sono collegate in fibra ottica dedicata tra di loro, la sede A6 è collegata in fibra ottica dedicata al datacenter. È in corso di realizzazione anche il collegamento in fibra dedicata per altre 4 sedi presenti nella città di Napoli (Via S. Lucia, Via Marina, Via Metastasio, Via De Gasperi).

All’interno di ogni sede sono presenti reti locali con cablaggi strutturati in fibra ottica e/o in rame, eventualmente articolate in più sottoreti sulle quali sono attestate circa 5000 postazioni client in dotazione al personale dell’Amministrazione.

Nelle sedi più importanti è presente anche la connessione WiFi mentre l'infrastruttura VoIP è distribuita in tutte le sedi connesse.

Per ulteriori dettagli si faccia riferimento all’Appendice 2 “Descrizione contesto tecnologico”.

4 OGGETTO DELLA FORNITURA

L'oggetto della fornitura è l'erogazione del Servizio di Gestione e manutenzione della infrastruttura di rete, dei beni hardware, dei sistemi per i servizi ICT e delle postazioni client in uso presso la Giunta Regionale della Campania, per i servizi ICT offerti dall’Ente stesso e di un Contact center unificato.

Al Fornitore in particolare si richiedono i servizi di seguito elencati e dettagliati nei capitoli successivi:

a) servizi base
    i. conduzione operativa sistemi open in modalità remota orario base
b) servizi opzionali
    i. monitoraggio notturno/festivo sistemi open in modalità remota
    ii. supporto specialistico
    iii. reperibilità
    iv. interventi fuori orario
c) servizi accessori
    i. ulteriori ambienti elaborativi
    ii. sicurezza fisica
    iii. manutenzione hardware
    iv. supporto ambienti client

5 DURATA DEL CONTRATTO

La durata del contratto è di 36 mesi. I servizi dovranno essere erogati a partire dalla data di scadenza dell’attuale contratto di System Management e a far data dal 01 luglio 2022. Alla scadenza dei 36 mesi, l’Amministrazione si riserva di estendere il contratto per ulteriori 24 mesi, con un preavviso di 60 giorni. In tale circostanza, il fornitore sarà tenuto alla fornitura dei servizi agli stessi prezzi, patti e condizioni del contratto originario, o a condizioni migliorative per l’Amministrazione.

6 DESCRIZIONE DEI SERVIZI

La finalità del servizio è garantire la piena operatività delle infrastrutture tecnologiche dei Centri Elaborazione Dati, mantenerne la perfetta efficienza, garantire agli utenti la disponibilità e le prestazioni delle applicazioni su di esse installate e l'integrità dei relativi dati nonché a fornire il supporto necessario per garantirne il costante allineamento con l'evoluzione tecnologica del mercato ICT.

I servizi sono stati articolati in:

- servizi base;
- servizi opzionali;
- servizi accessori

come descritti nel seguito.

6.1 Servizi base

Il servizio base richiesto dall'Amministrazione riguarda la conduzione operativa dei sistemi open equipaggiati con Windows, Linux.

La conduzione deve essere effettuata in modalità remota tramite un collegamento telematico tra il centro servizi del Fornitore e il CED dell'Amministrazione. Si richiede la fascia oraria base di 50 ore settimanali da lunedì a venerdì, dalle ore 8:00 alle ore 18:00.

6.1.1 Servizio Conduzione Operativa Sistemi Open

Le successive attività sono da intendersi integrative, ove non previste, rispetto a quelle espressamente indicate nel capitolo 5.1, del Capitolato Tecnico dell'AQ. Alcune attività potrebbero richiedere competenze specialistiche non rientranti nella conduzione operativa. Tali attività saranno erogate tramite supporto specialistico continuativo, come descritto nei successivi paragrafi.

Nella descrizione delle attività, tra parantesi viene riportata la struttura specializzata a gestirla (NOC, SIS, SOC, etc.)

6.1.1.1 IMPLEMENTAZIONE, INTEGRAZIONE, GESTIONE E MANUTENZIONE DEI SISTEMI SERVER E INFRASTRUTTURE (SIS)

Questa voce include tutte quelle attività necessarie per implementare, prendere in carico, condurre e mantenere sempre aggiornata e funzionante una infrastruttura hardware e software utilizzata per l'erogazione di più servizi informatici nel rispetto degli SLA contrattuali, ossia:

- Implementazione di infrastrutture informatiche a supporto dell'erogazione di un servizio (dimensionamento dei server, S.O., database, configurazione, interconnessioni, etc.);

- Integrazione di sistemi e di infrastrutture provenienti da altre Amministrazioni/Fornitori;
- Installazioni di hardware, software di base e middleware, loro configurazione e personalizzazione;
- Conduzione operativa dei sistemi;
- Monitoraggio dei sistemi, del livello di utilizzo delle risorse e dei livelli di prestazione dei servizi applicativi. Interventi di ripristino;
- Analisi dei guasti hardware ed attivazione dei fornitori/garanzia per la sostituzione delle parti difettose. Ripristino delle funzionalità;
- Gestione e monitoraggio Infrastrutture di virtualizzazione (VMware vCenter, Oracle VM), comprese le attività di: installazione, configurazione, modifica ed eliminazione di nuovi sottosistemi (host, cluster, datastore, networking, ecc.);
- Installazione, configurazione e gestione ambienti virtualizzati tramite container (Docker, Kubernetes)
- Installazione, gestione ed evoluzione dei servizi infrastrutturali (Active Directory, Exchange, DNS, File Server, etc);
- Installazione e gestione dei software di sicurezza (antivirus, antispam, etc.)
- Gestione e aggiornamento di procedure, script o meccanismi automatici per allineamento dati tra diverse piattaforme.
- Gestione e verifica periodica di tutti gli accessi amministrativi secondo normativa vigente;
- Gestione dei contratti di manutenzione dei sistemi;
- Approvazione e distribuzione degli aggiornamenti critici e delle configurazioni per la protezione dei sistemi;
- Migrazione, anche massiva, di server Linux con versione del S.O. non più aggiornata e supportata verso nuove distribuzioni Linux condivise con l'Amministrazione;
- Verifica ed attuazione di tutte le misure di sicurezza ICT per le PA emanate dall'AGID
- Consultazione della piattaforma Infosec per la rilevazione delle vulnerabilità (CVE) degli asset dell'Amministrazione;
- Consultazione del documento tecnico Cipher Suite protocolli TLS minimi per gestire la comunicazione tra le PA e verso i cittadini
- Gestione ed analisi dei LOG dei sistemi con strumenti automatici in conformità con quanto indicato dal Garante per la privacy
- Gestione degli incidenti di sicurezza;
- Effettuazione degli interventi hw e sw periodici programmati per garantire il buon funzionamento dei sistemi, dall'upgrade del firmware dei server alla pulizia integrale degli stessi (p.e., rimozione della polvere all'interno degli enclosure e/o dei server) e manutenzione dei server e degli armadi rack;
- Verifica delle funzionalità degli impianti logistici (elettrico, condizionamento, etc.) ed attivazione dei fornitori in caso di anomalie;
- Gestione documentazione tecnica e delle licenze software. Mantenimento del DB degli interventi;
- Monitoraggio della scadenza delle licenze dei prodotti software installati sull'Infrastruttura ICT e dei certificati server e applicativi;
- Gestione delle utenze e dei relativi livelli di autorizzazione.

6.1.1.2 CONFIGURAZIONE, GESTIONE E CONTROLLO DEI SOTTOSISTEMI DI STORAGE E BACKUP (SIS)

Obiettivo di queste attività è mantenere l'integrità e la disponibilità delle informazioni e delle strutture di elaborazione delle informazioni:

- Gestione e Monitoraggio dei sottosistemi SAN/NAS e configurazione degli apparati di collegamento (LUN zoning e LUN mapping, etc.);
- Installazione, configurazione e manutenzione ambienti di backup;
- Definizione e configurazione policy di Backup di dati, log e sistemi in accordo a esigenze, normative vigenti e alle misure di sicurezza ICT dell'AGID;
- Configurazione laboratorio Backup/Recovery e prove periodiche di ripristino;
- Monitoraggio degli esiti dei backup, delle risorse ed interventi di ripristino. Definizione di report periodici;
- Archiviazione, catalogazione, conservazione, riutilizzo e smaltimento dei supporti magnetici in accordo con le norme di sicurezza.

6.1.1.3 GESTIONE APPLICATIVI E BASI DI DATI (SIS)

La gestione applicativi e basi dati comprende l'insieme di attività per la presa in carico e gestione di applicativi e delle loro relative basi dati:

- Presa in carico e dismissione piattaforme applicative e relative basi di dati;
- Gestione sistemistica di piattaforme applicative (software di base/middleware, etc.) e dei relativi Database;
- Attività propedeutiche all'installazione di un DB Server e all'installazione di un'istanza. Determinazione dei requisiti e delle risorse;
- Installazione e/o aggiornamenti di versioni;
- Controllo, gestione e conservazione dei log generati dai servizi erogati in base alle policy definite dall'Amministrazione;
- Backup dati e dei log;
- Migrazione tra le diverse piattaforme di virtualizzazione;
- Migrazione da soluzioni on premises in cloud e viceversa;
- Attività di start up e shutdown di un'istanza e/o di un database;
- Gestione degli utenti, profili e ruoli e dei livelli di autorizzazione;
- Configurazione e gestione dei database in Alta Affidabilità/Disponibilità utilizzando tecnologie standard (DataGuard per Oracle, DataReplication per MySql, etc.);
- Pianificazione, con i responsabili di backup, delle attività di backup/restore;
- Monitoraggio e ottimizzazione delle prestazioni;
- Gestione documentazione e licenze;

6.1.1.4 SVILUPPO, GESTIONE E MANUTENZIONE RETI (NOC)

La gestione reti ha la finalità di garantire il corretto funzionamento dell'infrastruttura di rete LAN attraverso il suo continuo monitoraggio e l'interazione con i fornitori titolari dei contratti di manutenzione delle apparecchiature di rete. Tra le attività richieste:

- Gestione e controllo del regolare funzionamento del servizio;
- Configurazione e gestione di tutti gli elementi che costituiscono l'infrastruttura di rete (LAN, WIFI, MAN e WAN, apparati attivi e passivi, armadi reti, patch panel);
- Gestione dei servizi per la trasmissione dati, in ambito geografico e/o locale, con vari protocolli di comunicazione (IP, Frame Relay, ATM, MPLS, VPN, IEEE 802.X, SD-WAN, etc.) e/o tecnologie trasmissive (ADSL, HDSL, SDH) e/o portanti trasmissive (rame, fibre ottiche, wireless, ponti radio, link satellitari) interazione con i carrier e gli upstream providers;
- Ripristino delle funzionalità del servizio di rete e di tutti gli apparati TLC attivi e passivi;
- Sopralluogo, installazione e configurazione apparati e cablaggio per attivazione nuove sedi;
- Analisi e troubleshooting sugli incidenti rilevati;
- Gestione allarmi, attivazione del servizio di manutenzione hardware in caso di riparazione di sistemi/componenti difettosi;
- Monitoraggio costante dei parametri significativi della qualità e delle prestazioni della rete;
- Trouble ticketing per la gestione dei guasti di rete;
- Funzioni di Routing Registration Authority per la rete in coordinamento con le Registration Authority internazionali;
- Politiche di sicurezza informatica, blocco dei tentativi di accesso non autorizzati;
- Back-up dei dati;
- Test prestazionali periodici e/o di nuovi servizi applicativi e di infrastruttura da attivare;
- Abilitazione del traffico SNMP per l'invio delle TRAP sul sistema desktop;
- Configurazione routing BGP, gestione del peering tra AS e gestione dei rapporti con upstream providers e RIPE NCC;
- Gestione access-list per limitazioni del traffico;
- Gestione configurazione e implementazione dei firewall;
- Gestione e configurazione bilanciatori di carico;
- Supporto alla configurazione degli apparati di sede per variazione/inserimento parametri;
- Predisposizione di test di varia natura (carico della CPU, traffico delle interfacce);
- Manutenzione reti;
- Interventi hw e sw periodici programmati, a garanzia del buon funzionamento degli apparati e della sicurezza, dall'upgrade del firmware degli apparati attivi di rete (switch, router) alla pulizia, bonifica periodica e manutenzione degli armadi reti e patch panel;
- Sicurezza reti;
- Gestione dei log degli apparati di rete conforme alle normative vigenti;

- Produzione di report con cadenza mensile sulla fruizione in percentuale della rete. Il report deve contenere anche i riferimenti dell'eventuale interruzione del servizio (per interruzione si intende anche il singolo apparato).

6.1.1.5 GESTIONE DELLA SICUREZZA LOGICA (SOC)

La gestione della sicurezza logica realizza e gestisce le contromisure di tipo tecnologico volte alla difesa perimetrale e di contenuto del sistema informativo. Sono incluse le seguenti attività:

- Valutazione periodica dei rischi, minacce e vulnerabilità;
- Supporto per la definizione e verifica delle politiche di sicurezza in accordo con le normative;
- Gestione sicurezza perimetrale (firewall, accessi remoti, etc.) e sicurezza della Intranet (IPS, Url Filtering, etc.);
- Gestione della tracciabilità delle connessioni da/verso internet (tenuta dei file di log) e supporto all'Amministrazione per la gestione degli incidenti informatici;
- Profilazione degli utenti, Autenticazione ed Autorizzazioni, Strong authentication, controllo traffico internet;
- Gestione degli accessi esterni alla rete (VPN);
- Conduzione operativa dei Sistemi di Sicurezza logica della Rete Telematica.

6.1.1.6 TROUBLE TICKETING

La Regione Campania dispone, per la gestione di "Richieste", "Incident", "Asset", "FAQ", etc, di uno strumento web di Touble Ticketing ottenuto dall'integrazione di diversi software open source (GLPI + OCS Inventory).

Con questo strumento (GLPI), utilizzato da tutti gli utenti e consulenti regionali, oltre alle richieste di supporto per reti, sistemi, PDL, etc., sono stati definiti processi operativi interni per usufruire dei servizi offerti dall'amministrazione. Alcuni processi prevedono una fase autorizzativa, es.:

1. un utente di un settore specifico apre un ticket;
2. il dirigente di quel settore, identificato automaticamente dal sistema in base al profilo, approva il ticket;
3. il ticket viene lavorato.

Gli utenti e i profili, poiché cambiano continuamente, vengono aggiornati ogni notte con una fonte ufficiale (Active Directory). Lo strumento gestisce anche deleghe e dirigenti ad interim.

Di contro, però, GLPI non permette una completa analisi degli andamenti dei livelli di servizio.

Pertanto, gli strumenti del fornitore devono poter integrare i processi così come già definiti dall'Amministrazione.

I requisiti degli strumenti richiesti sono dettagliati nel paragrafo 8.5 “Strumenti del centro servizi”.

6.2 Servizi opzionali

I servizi opzionali, descritti nei paragrafi successivi, completano i servizi base,

6.2.1 Servizio “Supporto Specialistico”

Questo servizio è finalizzato a coprire esigenze di supporto tecnico, estemporanee o continuative, aggiuntive rispetto al servizio di conduzione operativa:

Il servizio di supporto specialistico è generalmente riferito ad attività ad elevato contenuto tecnologico che comportino un effort non riconducibile nell’ambito dei normali servizi di conduzione operativa e può comprendere sia attività di supporto tecnico alle strutture operative del fornitore, sia attività di supporto tecnico all’Amministrazione o altri operatori indicati dall’Amministrazione.

6.2.1.1 SUPPORTO SPECIALISTICO ALLA CONDUZIONE OPERATIVA

L’Amministrazione richiede un supporto specialistico, in tutti gli ambiti tecnologici (sistemi, apparati di rete/sicurezza, storage, DBMS e applicativi, ecc.) decritti nel par.6.1.1, per quelle attività che necessitano di competenze specialistiche non presenti nella conduzione operativa.

Tra le attività afferenti a tale servizio è possibile riscontrare, a titolo esemplificativo:

- supporto specialistico negli ambiti tecnologici previsti, quali sistemi, apparati di rete/sicurezza, storage, DBMS e applicativi, ecc;
- supporto specialistico per la definizione e la verifica delle politiche di sicurezza;
- disegno, dimensionamento ed implementazione dei sistemi;
- supporto alla definizione di piani di disponibilità e continuità operativa delle infrastrutture;

Resta intesto che il servizio di supporto specialistico si estende anche a tutte le altre attività descritte nel paragrafo 6.1.1.

Nel caso in cui alcune delle attività fossero eseguite da terzi, il supporto specialistico deve garantire l’affiancamento, il supporto e la cooperazione nella conduzione dell’attività. Il fornitore è responsabile del rispetto degli standard in uso e della consegna della documentazione completa ed aggiornata.

Inoltre, il supporto specialistico deve garantire:

- il supporto all’Amministrazione nella definizione e miglioramento dei processi di service management o dei processi operativi in generale;
- il supporto all’Amministrazione per il tracciamento e la verifica dei livelli di servizio dell’attività di conduzione operativa;

- il supporto ai progetti applicativi (verifica documentazione architetturale, matrice compatibilità, configurazione servizi in cloud, etc,);
- **la conduzione degli ambienti non critici** (SIS) come ad esempio ambienti di test/sviluppo, per i quali non sono definiti particolari livelli di servizio e dove su tali ambienti possono operare con privilegi elevati anche altri fornitori;
- **la conduzione degli access point** distribuiti su tutte le sedi periferiche (NOC), inclusi nei servizi base solo come monitoraggio. Nel caso di attività non eseguibili da remoto o su richiesta dell'Amministrazione, si dovranno recare a proprie spese sulle sedi oggetto di intervento, portando con sé gli apparati necessari per l'intervento, ove previsti. In tale attività è possibile avvalersi anche dell'Assistenza On Site (AOS).

Il "Supporto specialistico conduzione operativa" si configura come un presidio onsite composto da quattro risorse, due nell'ambito dei sistemi (SIS) e due nell'ambito reti e sicurezza (NOC e SOC), con profilo di "Sistemista senior". Tra queste risorse ne devono essere individuate 2 con le seguenti responsabilità:

- un "Responsabile SIS", tra i cui compiti quello del coordinamento delle attività, gestione e controllo del regolare funzionamento del servizio SIS, interfacciandosi con l'Amministrazione (es. Struttura di controllo, Unità di Monitoraggio) per garantire il regolare funzionamento del servizio;
- un "Responsabile NOC", tra i cui compiti quello del coordinamento delle attività, gestione e controllo del regolare funzionamento dei servizi NOC e SOC, interfacciandosi con l'Amministrazione (es. Struttura di controllo, Unità di Monitoraggio) per garantire il regolare funzionamento del servizio.

Le risorse impiegate opereranno principalmente nel CED di Napoli. Per esigenze dell'Amministrazione, si dovranno recare a proprie spese su altre sedi regionali.

Nell'appendice 2 "Descrizione Contesto Tecnico" sono riportati tutte le sedi periferiche regionali collegate al Datacenter

L'orario del servizio è dalle ore 7.30 alle ore 19.30, dal lunedì al venerdì escluso i giorni festivi. L'orario indicato, per esigenze amministrative, può essere anticipato o posticipato. Le risorse impegnate dovranno coprire l'intero orario di servizio attraverso la turnazione. Pertanto, le risorse dello stesso ambito dovranno sfalsare l'orario di ingresso.

6.2.1.2 SUPPORTO SPECIALISTICO- ASSISTENZA ON SITE (AOS)

L'Amministrazione intende realizzare un servizio di assistenza OnSite (AOS), attraverso l'acquisizione di un supporto specialistico continuativo, per tutte le problematiche degli utenti e sull'infrastruttura ICT di supporto non risolvibili da remoto.

Le problematiche potranno riguardare, quindi:

- gli apparati attivi e passivi della rete regionale;
- le risorse informatiche distribuite (hardware e software) in uso presso la Giunta Regionale della Campania;

- le postazioni di Lavoro Regionali (comprese di: stampante, Monitor, Scanner, Webcam, Lettore Card, etc.).

L'Assistenza On Site sarà dislocata sulle sedi periferiche più importanti (in base al numero degli utenti e/o ai servizi che offrono), ma in caso di necessità dovranno spostarsi nelle sedi non presidiate.

I tecnici dell'AOS opereranno in stretta collaborazione con l'HD remoto e saranno, per la sedi assegnate, il supporto per tutte le problematiche non risolvibili da remoto.

Inoltre, l'AOS è il punto di riferimento per le strutture SIS, NOC ed i referenti informatici del CRED per le problematiche indicate all'inizio del paragrafo inerenti le sedi loro assegnate.

Tra gli operatori dello AOS deve essere individuato un "Responsabile Help Desk", con il compito di coordinare sia le attività dell'Help Desk remoto che quelle dell'Assistenza On Site.

Gli operatori AOS, in base alle esigenze dell'Amministrazione, potrebbero temporaneamente essere incaricati ad effettuare attività specifiche.

Il responsabile HD insieme alla struttura regionale competente decidono:

- L'assegnazione delle sedi regionali non presidiate agli operatori AOS (in base alla distanza dalla sede assegnata, al numero di utenti da gestire, etc);
- Lo spostamento, in base alle esigenze, di un operatore AOS da una sede ad un'altra;
- In caso di richieste multiple allo stesso operatore, un piano di lavoro indicando priorità e tempi da rispettare ed eventuale ridistribuzione delle attività su operatori più liberi.

In caso di attività particolarmente impegnative, l'Amministrazione potrebbe richiedere temporaneamente ulteriori tecnici AOS.

Gli operatori AOS dovranno spostarsi tra le varie sedi, in tutte le circostanze, a proprie spese.

Inoltre, gli operatori AOS, su richiesta dell'Amministrazione, dovranno attivare, a proprie spese, un servizio di trasporto tra le sedi assegnate e la sede di Don Bosco. Tale circostanza si verifica soprattutto durante la sostituzione delle apparecchiature obsolete, da riportare a Don Bosco, con apparecchiature nuove, da prelevare da Don Bosco. La periodicità delle richieste di trasporto non supera le 2 volte al mese.

L'Assistenza On Site sarà costituita inizialmente da 15 Sistemisti Junior distribuiti sulle varie sedi e un Sistemista con il ruolo di Responsabile HD che opererà principalmente nella sede del CED di Napoli. L'Amministrazione si riserva la possibilità di individuare, nel corso della fornitura, soluzioni alternative all'AOS e quindi di rivedere in diminuzione il numero di sistemisti richiesti, nel rispetto delle previsioni dell'art.106 del D.lgs.50/2016.

L'orario del servizio è dalle ore 8.00 alle ore 17.00, dal lunedì al venerdì escluso i giorni festivi.

6.2.1.3 SUPPORTO SPECIALISTICO PER PROGETTI DI INNOVAZIONE

L'Amministrazione sta avviando diversi progetti per l'innovazione tecnologia (impianti, infrastruttura, etc.). A tal fine potrebbe essere richiesto, di volta in volta il supporto in specifici ambiti tecnologici, tra cui:

- Definizione di piani di disponibilità e continuità operativa delle infrastrutture;
- Progettazione, disegno e integrazione di nuove componenti dell'infrastruttura ICT, sia in ambito sistemi che reti;
- Sperimentazione ed integrazione di nuove tecnologie;
- Migrazione di servizi complessi tra piattaforme differenti;
- Infrastrutture VDI;
- Sistema monitoraggio impianti;
- Progetti per la sicurezza fisica e logica ed evoluzione dell'infrastruttura tecnologica;
- Etc.

6.2.2 Servizio "Monitoraggio notturno/festivo dei sistemi open"

Il servizio di monitoraggio notturno/festivo dei sistemi open comprende un sottoinsieme delle attività di conduzione operativa, effettuate al di fuori del normale orario di lavoro per garantire l'operatività dei sistemi di notte e nei giorni festivi. Il servizio include attività di gestione e controllo della schedulazione di procedure codificate, monitoraggio dei sistemi per la rilevazione di malfunzionamenti hardware e/o software, interventi per la risoluzione dei malfunzionamenti, ecc.

Il servizio deve essere erogato in modalità remota, dal Centro Servizi del Fornitore (vedi par. 4.3 del Capitolato Tecnico dell'AQ) mediante collegamento telematico alla rete dell'Amministrazione. In questa modalità, sono incluse nel servizio anche le eventuali attività di escalation e gli eventuali interventi onsite che si rendessero necessari a fronte di malfunzionamenti non risolvibili remotamente.

Il Fornitore deve effettuare il monitoraggio e controllo di tutti i servizi indicati dall'Amministrazione e i Componenti ICT ospitati dall'Infrastruttura ICT, anche nel caso in cui tali servizi o componenti siano riferiti a infrastrutture gestite da terze parti (es. provider esterni) ed in tale caso le procedure devono prevedere l'escalation verso i gruppi esterni al fornitore individuati dall'Amministrazione.

Nel servizio di monitoraggio è incluso anche la videosorveglianza della sala CED di Don Bosco, tramite gli apparati già installati. Le modalità operative saranno condivise nella fase iniziale del contratto.

E', inoltre, incluso nel servizio anche la gestione delle segnalazioni di malfunzionamento provenienti da personale dell'Amministrazione o da fornitori terzi da essa individuati.

Per la segnalazione di malfunzionamenti il fornitore deve mettere a disposizione dell'Amministrazione, oltre ai normali strumenti (web ed e-mail), un numero telefonico unico da contattare.

Dovranno essere garantiti i seguenti livelli minimi di servizio, riportati anche nel paragrafo 8.1 "Organizzazione del Service Desk":

- risposta entro 30", per il 90% delle chiamate ricevute. Sarà misurato il tempo che intercorre tra l'inizio della chiamata e la risposta da parte dell'Operatore. In caso di chiamata perduta, va misurato il tempo complessivo della chiamata. La percentuale delle chiamate perdute non può essere superiore al 4% delle chiamate totali. Si definisce chiamata perduta quella telefonata che:
  a. non ottiene risposta da un operatore entro 90 secondi;
  b. a cui segue il segnale di occupato;
  c. a cui segue risposta immediata tramite messaggio preregistrato;
  d. è messa in diretto contatto con la segreteria telefonica.

Il fornitore, inoltre, deve produrre un report con cadenza mensile, relativo all'espletamento del servizio ed al rispetto dei livelli di servizio previsti, "Tempo di Attesa" (**IQTA**) e "Chiamate Perse" (**IQCP**), con almeno i seguenti dati:

a. Identificativo Utente;
b. Tempo inizio chiamata dell'utente;
c. Tempo risposta dell'operatore;
d. Problema segnalato;
e. Tempo risoluzione problema, se risolto dall'operatore;
f. Tempo di segnalazione e gruppo di intervento, in caso di escalation.

Il formato dei dati deve essere compatibile con le comuni Suite applicative per l'ufficio, per un successivo eventuale trattamento.

Gli interventi devono essere registrati (aperti e chiusi) sul sistema di Service Desk per poter verificare la problematica, la soluzione, le tempistiche, etc.

Per la risoluzione dei malfunzionamenti i livelli di servizio da rispettare sono dati dall'indicatore "Tempestività di risoluzione degli incident" (**IQ12**)

Eventuali interventi onsite necessari per il ripristino delle funzionalità, a seguito di malfunzionamenti rilevati o segnalati non possono essere ricondotti al servizio "Intervento fuori orario".

L'elenco dei sistemi critici afferenti al servizio "Monitoraggio notturno/festivo dei sistemi open" sarà condiviso nella fase iniziale della fornitura, fermo restando la facoltà per l'Amministrazione di rivedere tale elenco nel corso della durata contrattuale.

6.2.3 Servizio "Reperibilità"

Il servizio Reperibilità è finalizzato a garantire un supporto tecnico, al di fuori del normale orario di servizio diurno, da parte del personale impiegato nel supporto specialistico, per attività programmate o a fronte di malfunzionamenti. Il servizio è attivato su richiesta dell'Amministrazione ed include il supporto telefonico o l'eventuale intervento attraverso connessione remota.

6.2.4 Servizio "Intervento fuori orario"

Il servizio Interventi fuori orario è finalizzato a garantire l'intervento sui sistemi, al di fuori del normale orario di servizio diurno, da parte del personale impiegato nel supporto specialistico. Il servizio è attivato dall'Amministrazione nelle seguenti situazioni:

- necessità di intervento on-site notturno/festivo, a fronte di malfunzionamenti, da parte delle risorse professionali in reperibilità;
- necessità di lavoro straordinario pianificato on-site per attività che non possono essere effettuate durante il normale orario di disponibilità dei sistemi.

6.3 Servizi accessori

I servizi accessori richiesti, a completamento dei servizi base e opzionali, sulla base delle esigenze operative/organizzative dell'Amministrazione vengono descritti nei successivi paragrafi.

6.3.1 Servizio "Gestione Infrastrutture non standard" – Ulteriori ambienti elaborativi

Il servizio è volto alla conduzione di ulteriori ambienti elaborativi su infrastrutture tecnologiche non rientranti negli schemi standard dei servizi base. Tale servizio comprende:

- la gestione della **Virtual Desktop Infrastracture (VDI**), basata sulla soluzione VDI di Citrix e ospitata su un'infrastruttura iperconvergente Nutanix descritta nel paragrafo 3 contesto tecnico. Attualmente tale infrastruttura gestisce circa 200 VDI tra statiche e shared. Per la conduzione di questo ambiente sono necessarie delle competenze evolute sui sistemi Citrix

La gestione delle infrastrutture non standard rientra comunque nell'ambito delle modalità operative (tempistiche per gli interventi, presidio, orari di servizio, etc.) descritte nei paragrafi precedenti.

6.3.2 Servizio "Gestione Infrastrutture non standard" – Sicurezza fisica

Il servizio di gestione della sicurezza fisica comprende le misure necessarie per proteggere il sistema informativo dal punto di vista della sicurezza delle apparecchiature, in termini di sicurezza di area e di continuità operativa, ovvero è finalizzato alla gestione dei sistemi di controllo accessi e degli impianti di alimentazione, condizionamento ed antincendio delle sale CED.

In particolare, è richiesta la fornitura di un servizio di manutenzione e monitoraggio di tutti gli impianti esistenti a servizio del CED Regionale così come descritti nei paragrafi 2 "Impianti" dell'appendice 2 "Descrizione contesto tecnologico".

6.3.2.1 MANUTENZIONE IMPIANTI

Il servizio di manutenzione impianti riguarda le attività necessarie per ripristinare il funzionamento degli impianti a fronte di guasti e comprende la responsabilità completa del ripristino dell'impianto, inclusa la fornitura dei componenti da sostituire a quelli guasti/difettosi.

Nell'appendice 2 sono riportate le caratteristiche specifiche degli impianti e le relative scadenze di manutenzione.

Per gli impianti ancora in garanzia/manutenzione è compito della Ditta Aggiudicataria analizzare i guasti, attivare i fornitori/garanzia per il ripristino delle funzionalità e verificare il rispetto dei tempi e delle modalità in essa previsti.

Per gli impianti per i quali verrà offerto il rinnovo contrattuale del supporto e della manutenzione, i contratti dovranno essere stipulati direttamente con la casa produttrice degli impianti o, in mancanza, con partner accreditati dalla casa produttrice. Eventuali contratti stipulati con soggetti che non rispettano i suddetti requisiti verranno considerati nulli ai fini dell'erogazione del servizio. Tali contratti dovranno essere stipulati almeno 15 giorni prima della scadenza e comunicati immediatamente all'Amministrazione. Per eventuali ritardi si applicheranno le penali previste dall'indicatore di qualità "Slittamento delle scadenze" (**IQ06**).

Il rinnovo contrattuale deve essere offerto per tutto il periodo contrattuale residuo ossia dalla scadenza della manutenzione alla scadenza prevista del contratto di System Management, indicando, nell'offerta economica, sia i mesi contrattuali offerti, che dovranno obbligatoriamente corrispondere ai mesi residui, sia il costo annuo per ogni tipologia di apparato.

È richiesta sia la manutenzione preventiva che la manutenzione correttiva.

6.3.2.2 MANUTENZIONE PREVENTIVA

La manutenzione preventiva è finalizzata alla prevenzione dei guasti o malfunzionamenti, prevedendo la sostituzione di componenti che al momento del controllo presentano delle problematiche.

Entro il primo mese di contratto, il Fornitore dovrà comunicare il piano degli interventi periodici di manutenzione preventiva e una checklist delle verifiche da effettuare. Dovranno essere eseguiti almeno due interventi annuali. Ad ogni controllo il fornitore deve inviare all'Amministrazione, entro 3 giorni lavorativi, la checklist completa, controfirmata da un Responsabile Tecnico della Regione Campania, di tutte le verifiche effettuate e le eventuali anomalie riscontrate.

6.3.2.3 MANUTENZIONE CORRETTIVA

La manutenzione correttiva è finalizzata a ripristinare il corretto funzionamento degli impianti a seguito di malfunzionamenti o guasti.

L'intervento di manutenzione può essere attivato:

- direttamente dai tecnici del CRED, compreso SIS e NOC, tramite uno dei canali di comunicazione previsti e indicati nel capitolo 8, informandone l'Unità di monitoraggio;
- dal sistema automatico di monitoraggio adottato dall'Amministrazione e/o in caso di manutenzione preventiva.

Il servizio dovrà essere erogato H24x365 giorni all'anno con le seguenti tempistiche:

- intervento entro 60 minuti dall'inizio del disservizio per situazioni critiche dovute sia a situazioni di pericolo che a indisponibilità dei sistemi critici (eccessivo aumento della temperatura, problemi sull'impianto antincendio, indisponibilità di servizi critici per mancanza di alimentazione elettrica, etc.);
- risoluzione del guasto entro il giorno lavorativo successivo alla chiamata ("servizio NBD") durante l'orario lavorativo base per situazioni non critiche.

6.3.2.4 MONITORAGGIO IMPIANTI

Il datacenter utilizza la soluzione Vertiv Environet Alert per monitorare i seguenti impianti a servizio del CED di Napoli:

- n. 2 Gruppi Elettrogeni
- n. 2 Gruppi di Continuità
- n. 18 Multimetri presenti nei Quadri Elettrici
- n. 40 PDU che alimentano gli apparati in n. 30 armadi rack
- n. 18 Condizionatori
- controllo accessi
- impianto antincendio
- impianto antintrusione.

Il fornitore dovrà acquisire in tempo reale, H24x365 giorni, gli alert generati dal sistema di monitoraggio, tramite il proprio Centro Servizi, ed attivare il servizio manutenzione, se necessario, nel rispetto delle tempistiche indicate nel paragrafo precedente. I tempi di attivazione si andranno a sommare ai tempi di risoluzione per gli impianti il cui contratto di manutenzione sia stato già attivato con l'aggiudicataria del AS.

6.3.3 Servizio "Manutenzione hardware" – Cred, Reti Periferiche e PDL

Il servizio di manutenzione hardware riguarda le attività necessarie per ripristinare il funzionamento dei sistemi a fronte di guasti e comprende la responsabilità completa del ripristino dei sistemi, inclusa la fornitura dei componenti da sostituire a quelli guasti/difettosi. Gli apparati/componenti sostitutivi dovranno essere della stessa marca, modello e tipo, e dovranno garantite le medesime

prestazioni e funzionalità. In caso di indisponibilità delle parti di ricambio il Fornitore avrà la facoltà di sostituire, interamente e a proprie spese, il dispositivo guasto con uno sostitutivo di prestazioni e costi di gestione equivalenti.

In caso di riparazione, il servizio deve comprendere la **sostituzione** dell'apparecchiatura con un'altra, di caratteristiche uguali o equivalenti, per tutto il periodo necessario all'intervento di riparazione.

Il servizio di manutenzione hardware comprende anche le attività necessarie per mantenere continuamente allineati i Sistemi HW e SW alle più recenti innovazioni tecnologiche, rilasciate dai fornitori HW e utili per la corretta erogazione del servizio, e tutte le attività necessarie per ripristinare il funzionamento dei dispositivi a fronte di errori o guasti.

Il servizio di manutenzione hardware è composto da:

- Manutenzione Preventiva: controlli periodici finalizzati alla prevenzione dei guasti o malfunzionamenti, prevedendo la sostituzione di componenti che al momento del controllo presentano delle problematiche.
- Manutenzione Correttiva: interventi di manutenzione a seguito di malfunzioni o guasti.

Qualora l'intervento di manutenzione da effettuare dovesse rendere necessarie operazioni di backup e successiva reinstallazione dei software di base e/o applicativo e/o dei dati utente tale operazione sarà anch'essa a carico del Fornitore e senza costi aggiuntivi.

Di seguito le specifiche per la manutenzione degli apparati del CRED, delle Reti Periferiche e delle PDL.

6.3.3.1 MANUTENZIONE HARDWARE CRED

Per gli apparati Server, Storage, Rete e Sicurezza, elencati nel paragrafo 3.1 "Apparati installati al CRED e date di scadenze del supporto" dell'appendice 2 "Descrizione contesto tecnologico", si chiede il servizio di manutenzione hardware per tutta la durata contrattuale, da attivare alla scadenza dell'attuale supporto. Tale scadenza è riportata a fianco di ogni tipologia di apparato nel paragrafo suddetto.

Sono inclusi nel servizio anche gli interventi e gli oneri dovuti a guasti o malfunzionamenti causati da: sovratensione, sovracorrente, esaurimento batterie/accumulatori e sovratemperatura (anche dei locali).

Per le apparecchiature ancora in garanzia/manutenzione è compito della Ditta Aggiudicataria analizzare i guasti hardware, attivare i fornitori/garanzia per la sostituzione delle parti difettose, verificare il rispetto dei tempi e delle modalità in essa previsti e ripristinare le funzionalità.

Per le apparecchiature per le quali verrà offerto il rinnovo contrattuale del supporto e della manutenzione, i contratti dovranno essere stipulati direttamente con la casa produttrice degli apparati o, in mancanza, con partner accreditati dalla casa produttrice. Eventuali contratti stipulati con soggetti che non rispettano i suddetti requisiti verranno considerati nulli ai fini dell'erogazione del servizio. Tali contratti dovranno essere stipulati almeno 15 giorni prima della scadenza e comunicati immediatamente

all'Amministrazione. Per eventuali ritardi si applicheranno le penali previste dall'indicatore di qualità "Slittamento delle scadenze" (**IQ06**).

Il rinnovo contrattuale deve essere offerto per tutto il periodo contrattuale residuo ossia dalla scadenza della manutenzione alla scadenza prevista del contratto di System Management, indicando, nell'offerta economica, sia i mesi contrattuali offerti, che dovranno obbligatoriamente corrispondere ai mesi residui, sia il costo annuo per ogni tipologia di apparato.

Per la manutenzione preventiva, entro il primo mese di contratto, il Fornitore dovrà comunicare il piano degli interventi periodici e una checklist delle verifiche da effettuare. Dovranno essere eseguiti almeno due interventi annuali. Ad ogni controllo il fornitore deve inviare all'Amministrazione, entro tre giorni lavorativi, la checklist completa, controfirmata da un Responsabile Tecnico della Regione Campania, di tutte le verifiche effettuate e le eventuali anomalie riscontrate.

Qualora durante le attività di manutenzione preventiva venissero riscontrati malfunzionamenti, il Fornitore provvederà alla riparazione o sostituzione delle componenti guaste ed alle attività, eventualmente necessarie, per il ripristino delle normali funzionalità.

Il servizio di manutenzione correttiva dovrà garantire per le attività di sostituzione/riparazione i seguenti livelli di servizio:

- risoluzione del guasto H24x365 giorni entro 60 minuti dall'inizio del disservizio per apparecchiature definite critiche (apparecchiature il cui disservizio comporti l'immediata indisponibilità dei servizi critici o il blocco o il rallentamento del lavoro di più utenti. Es: router, switch, server, armadi reti, etc.);
- risoluzione del guasto entro il giorno lavorativo successivo alla chiamata ("servizio NBD") durante l'orario lavorativo base per situazioni non critiche.

L'intervento di manutenzione può essere attivato:

- da qualunque utente del servizio o direttamente dai tecnici del CRED, compreso SIS e NOC, tramite uno dei canali di comunicazione previsti e indicati nel capitolo 8, informandone l'Unità di monitoraggio;
- dal sistema automatico di monitoraggio e/o in caso di manutenzione preventiva.

6.3.3.2 MANUTENZIONE HARDWARE RETI PERIFERICHE

Per gli apparati di rete sulle sedi periferiche e gli apparati utilizzati per la connettività utente (reti client, switch, access point, UPS, etc.), descritti nel paragrafo 4.1 "Apparati rete sulle sedi periferiche e scadenze del supporto" dell'appendice 2 "Descrizione contesto tecnologico, si chiede, un servizio di manutenzione per tutto il periodo contrattuale, a partire dalla scadenza dell'attuale contratto, con le modalità indicate di seguito.

Sempre nell'appendice 2, nel paragrafo 5 "Elenco sedi regionali", sono riportate tutte le sedi regionali dove sono installati gli apparati e la criticità di ogni sede in termini di tempi di intervento.

Entro il primo mese di contratto, il fornitore dovrà comunicare il piano degli interventi periodici di manutenzione preventiva, per tutte le sedi, e una checklist delle verifiche da effettuare. Dovrà essere eseguito almeno un intervento all'anno. Ad ogni controllo il fornitore deve inviare all'Amministrazione, entro tre giorni lavorativi, la checklist completa, controfirmata da un Responsabile Tecnico della Regione Campania, di tutte le verifiche effettuate e le eventuali anomalie riscontrate.

Qualora, durante le attività di manutenzione preventiva, venissero riscontrati malfunzionamenti, il Fornitore deve provvedere alla riparazione o sostituzione delle componenti guaste ed alle attività eventualmente necessarie per il ripristino delle normali funzionalità.

Il servizio di manutenzione correttiva deve garantire per le attività di sostituzione/riparazione i seguenti livelli di servizio:

- Risoluzione del guasto H24x365 giorni, entro 60 minuti dall'inizio del disservizio per apparecchiature definite critiche (apparecchiature il cui disservizio comporti l'immediata indisponibilità dei servizi critici o il blocco o il rallentamento del lavoro di più utenti, es: router, switch, server, armadi reti, etc.) dislocate nelle sedi con "**criticità alta**" (identificate nell'appendice 2 con la lettera "A");
- risoluzione del guasto, in orario lavorativo, entro 120 minuti dall'inizio del disservizio per apparecchiature definite critiche (apparecchiature il cui disservizio comporti l'immediata indisponibilità dei servizi critici o il blocco o il rallentamento del lavoro di più utenti, es: router, switch, server, armadi reti, etc.) dislocate nelle sedi con "**criticità media**" (identificate nell'appendice 2 con la lettera "M");
- risoluzione del guasto entro il giorno lavorativo successivo alla chiamata ("servizio NBD") durante l'orario lavorativo base per situazioni non critiche e per tutte le apparecchiature dislocate nelle sedi con "**criticità bassa**" (identificate nell'appendice 2 con la lettera "B").

Sono incluse, in questo servizio, attività di attivazione, gestione e ripristino dei punti rete presenti presso tutte le sedi periferiche. Devono essere garantite la realizzazione di almeno 100 (cento) nuovi punti rete per ogni anno di contratto. I punti rete non utilizzati in un anno si cumulano con quelli degli anni successivi. Ogni nuovo punto realizzato deve essere doppio e comprensivo di certificazione.

Le risorse impiegate dovranno recarsi a proprie spese sulle sedi oggetto di intervento, portando con sé gli apparati necessari per l'intervento, ove previsti, e riportando gli apparati guasti alla sede di Don Bosco.

L'intervento di manutenzione può essere attivato:

- da qualunque utente del servizio o direttamente dai tecnici del CRED, compreso SIS e NOC, tramite uno dei canali di comunicazione previsti e indicati nel capitolo 8, informandone l'Unità di monitoraggio;
- dal sistema automatico di monitoraggio e/o in caso di manutenzione preventiva.

6.3.3.3 MANUTENZIONE HARDWARE PDL

Per le apparecchiature elencate nel sottoparagrafo 4.2 “Infrastruttura ambienti client”, dell’appendice 2 “Descrizione contesto tecnologico”, si richiede un servizio di manutenzione hardware per tutto il periodo di vigenza contrattuale e per tutte le apparecchiature non più coperte da garanzia.

Il numero delle apparecchiature da manutenere potrebbe cambiare in base alle possibili variazioni del numero del personale della Regione Campania. Il servizio dovrà essere erogato sulla dimensione attuale delle risorse preesistenti con un incremento massimo del 20% (venti %).

Tutte le attività onsite necessarie per la manutenzione/sostituzione PDL saranno effettuate dal Supporto Specialistico “Assistenza On Site” secondo le priorità ed i tempi indicati nel paragrafo “Supporto ambiente client”. Tali risorse dovranno recarsi a proprie spese sulle sedi oggetto di intervento, portando con sé gli apparati necessari per l’intervento, ove previsti, e riportando gli apparati guasti alla sede di Don Bosco.

L’orario di intervento potrebbe essere condizionato dalla presenza dell’utente. In tal caso la sola pianificazione dell’intervento deve essere effettuata entro i tempi indicati.

6.3.4 Supporto ambiente client

Il servizio di supporto degli ambienti client riguarda la gestione delle infrastrutture elaborative degli utenti, complementari rispetto alle infrastrutture server primarie, allo scopo di gestire le funzionalità dei sistemi elaborativi in modalità integrata tra i diversi livelli.

Possono essere considerate oggetto del servizio sia le infrastrutture fisiche (apparati elaborativi) a disposizione degli utenti, sia quelle logiche (quali ad esempio sistemi client virtualizzati gestiti centralmente), e possono essere incluse, a titolo esemplificativo e non esaustivo, attività di service desk per le problematiche utente, assistenza remota e/o locale per la risoluzione dei malfunzionamenti, servizi centralizzati di software distribution, monitoraggio, ecc.

In tale contesto, l’Amministrazione chiede un servizio remoto di Service Desk che comprende tutte le attività di gestione delle problematiche degli utenti e delle postazioni di lavoro (PDL) con esclusione della manutenzione HW, inclusa nei servizi accessori “Servizio Manutenzione hardware”. Sono considerate oggetto del servizio le postazioni fisiche (PC, Thin Client, video, stampanti, scanner, fax, etichettatrici, etc) a disposizione degli utenti, le postazioni virtuali (VDI), i programmi e le procedure installati.

Il servizio deve essere erogato in modalità remota, dalle ore 8:00 alle ore 20:00 dal lunedì al venerdì, dal Centro Servizi del fornitore.

L’Help Desk deve essere coordinato da un “Responsabile gestione HD” onsite, con il compito di coordinamento delle attività, gestione e controllo del regolare funzionamento del servizio, interfacciandosi con l’Amministrazione (p.e., Struttura di controllo, Unità di monitoraggio) per garantire il regolare funzionamento dello stesso.

Per le sole attività necessariamente onsite, che non possono essere, quindi, espletate da remoto, il servizio si avvarrà di una "Assistenza On Site", composta di 15 tecnici, con competenze specialistiche, dislocati sulle sedi periferiche più importanti.

Tali figure, "Responsabile gestione HD" e "Assistenza On Site", rientrano nel supporto specialistico descritto nel paragrafo "Supporto Specialistico – Assistenza On Site".

In linea di massima, le attività previste in questo servizio sono le seguenti:

1. Monitoraggio software di base, patching, aggiornamenti critici e di sicurezza Windows e Office;
2. Monitoraggio e controllo sul rispetto delle misure di sicurezza ICT emanate dall'AGID e le policy indicate dall'Amministrazione;
3. Monitoraggio e controllo sui software installati con aggiornamento del DB degli asset;
4. Monitoraggio periodico delle prestazioni delle PdL al fine di individuare ed anticipare potenziali problemi;
5. Installazione ed aggiornamento del software di base, di software di produttività, di software antivirus (S.O., suite Office, java, firma elettronica, lettori PDF, etc.) attraverso distribuzione elettronica degli aggiornamenti (da remoto e, in caso di impossibilità, con interventi on-site). Il servizio comprende anche l'upgrade dei Sistemi Operativi che comporta il passaggio da una major release ad un'altra;
6. IMAC: Installazione e configurazione nuove PDL o riassegnazione con eliminazione dati e tracce d'uso ai fini della privacy. Installazione periferiche esterne e client di posta elettronica. Ripristino backup dati utente. Installazione e configurazione stampanti, smart card e scanner di rete. Consegna dell'apparecchiatura all'utente finale, collegamento alla rete e test funzionalità. Disinstallazione e trasporto PDL nelle sedi indicate dall'Amministrazione. Aggiornamento del DB degli asset;
7. Installazione e configurazione strumenti e software per Smart Working e supporto all'utente;
8. Attivazione/disattivazione delle prese LAN negli armadi di piano e borchie utente;
9. Manutenzione preventiva e correttiva della PDL;
10. Gestione Licenze Stand Alone e Gestione Office 365: Assegnazione licenze, Siti Share Point e aggiornamento utenti esterni;
11. Gestione utenze Active Directory: Creazione e Rinnovo utenze esterne, reset password Ad, console MMC e Gruppi di AD;
12. Gestione cartelle condivise Sharepoint e Share Isilon;
13. Configurazione stampanti di piano;
14. Supporto all'utilizzo degli applicativi in uso in Regione Campania, tra cui (l'elenco è solo indicativo):
    a. Delibere, Determine e Decreti (DDD)
    b. Protocollo
    c. Gestione del personale (SIGARU)
    d. Contabilità (SAP)
    e. Firme Digitali
    f. Etc.

15. Attività di supporto all'Amministrazione per il potenziamento delle postazioni (Verifica HW, cancellazione dati, Upgrade SW e HW, Installazione SSD e RAM, reinstallazione SO, etc.) e dismissione di quelle obsolete;
16. Gestione Contratti ditte terze per assistenza tecnica per gli apparati in garanzia;
17. Interfaccia con i referenti Informatici degli uffici regionali;
18. Gestione dei supporti tecnologici
    a. postazioni di lavoro e attrezzature nelle aule informatizzate;
    b. sistemi di video e audio conferenza;
    c. sistemi multimediali e di videoproiezione.

Le suddette attività possono essere riviste ed integrate dall'Amministrazione durante tutta la fase contrattuale.

Il servizio interagisce con altri servizi richiesti dall'Amministrazione. In particolare, interagisce con l'Assistenza On Site, per le attività legate ad interventi onsite, con il servizio manutenzione, per attività legate alla manutenzione hardware (esempio: sostituzione di un hard disk), e con lo SPOC, per le quali si vedano i paragrafi specifici.

Il servizio può essere attivato da tutti i dipendenti e consulenti interni della Regione Campania tramite uno dei canali di comunicazione previsti e indicati nel capitolo 8;

Il servizio deve essere dimensionato sul numero delle postazioni di lavoro tenendo conto di un possibile incremento del 20%.

Per una classificazione dei disservizi (incident), relativamente al supporto ambienti client, la scala di riferimento, con i tempi massimi di risoluzione, è la seguente, con grado di gravità decrescente:

- **Priorità 1 - Bloccante e critico – 2 h lavorativa:** l'Utente non è in grado di usufruire del servizio per indisponibilità dello stesso o perché le sue prestazioni risultano decisamente degradate in alcune sue componenti ritenute critiche dall'Amministrazione.
- **Priorità 2 - Bloccante – 4 h lavorative:** l'Utente non è in grado di usufruire del servizio per indisponibilità dello stesso o perché le sue prestazioni risultano decisamente degradate.
- **Priorità 3 - Non bloccante critico – 6 h lavorative**: l'Utente è in grado di usufruire del servizio anche se le prestazioni dello stesso risultano degradate in alcune sue componenti ritenute critiche dall'Amministrazione.
- **Priorità 4 - Non bloccante non critico – 8 h lavorative**: l'Utente è in grado di usufruire del servizio anche se le prestazioni dello stesso risultano degradate in alcune sue componenti ritenute non critiche dall'Amministrazione.

La classificazione degli incident va concordata nella fase di segnalazione e prima diagnosi. In caso di mancato accordo con l'utente, la classificazione sarà quella indicata dall'Amministrazione.

L'Amministrazione può, durante la fase del contratto, rivedere la scala di classificazione.

L'indicatore di qualità di riferimento è **IQA3** – "Tempestività di risoluzione degli incident ambiente client". I tempi massimi di riferimento si riferiscono alla soluzione del problema, se risolvibile da remoto. In caso di trasferimento della chiamata al supporto specialistico i tempi massimi si riferiscono ai tempi di intervento. Il trasferimento della richiesta ad uno specifico supporto (del fornitore stesso o fornitori terzi) deve sempre essere immediato e tracciato sul sistema di service desk.

Per i change standard, l'indicatore di qualità di riferimento è **IQA4** "Tempestività di esecuzione dei change standard/predefiniti ambiente client". L'associazione Attività-Classe sarà condivisa con il fornitore in fase di avvio del contratto. In caso di mancato accordo, l'associazione sarà indicata dall'Amministrazione.

L'Amministrazione, durante la fase di gestione del contratto, può chiedere di fornire report specifici su attività effettuate in remoto e/o onsite con i relativi tempi.

Gli strumenti principali utilizzati dall'Amministrazione per la gestione delle PDL sono i seguenti:

1. Connessione Desktop remoto per l'assistenza:
    a. Per collegamento a PDL fisiche: CA ITCM Remote Host
    b. Per collegamento a VDA e VDI: Citrix Director
2. OCS Inventory e GLPI per Asset management PDL e software
3. GLPI per Trouble Ticketing e per la gestione di licenze varie
4. Console Microsoft Office 365 per le licenze Office 365
5. Console Sophos per la gestione dell'antivirus e policy di sicurezza
6. WSUS: Patching dei software di base e Aggiornamenti Critici e di Sicurezza Windows e Office

Lo strumento CA ITCM Remote Host non è più in manutenzione.

Gli strumenti minimi richiesti al fornitore, per la gestione remota in sicurezza dei PC (connessione remota, installazione software, strumenti automatici di discovery PDL e configurazioni, etc.) sono riportati nel paragrafo 8.6. L'eventuale costo di tali strumenti, con relative licenze per utente, è a completo carico del fornitore.

7 DIMENSIONAMENTO DEI SERVIZI

In questo paragrafo è riportato il dimensionamento massimo stimato per i servizi oggetto della fornitura, al meglio delle conoscenze iniziali. Il dimensionamento è riferito alla durata contrattuale di 36 mesi con la possibilità per l'Amministrazione di estenderlo per ulteriori 24 mesi.

Tale dimensionamento si intende pertanto non vincolante, riservandosi la Committente di attivare i servizi in misura maggiore o minore rispetto a quanto di seguito riportato, sulla base di quanto specificato nel paragrafo 8.2 del Capitolato Tecnico dell'Accordo Quadro. Per i servizi accessori, eventuali parametri di dimensionamento vengono indicati tra le parentesi.

7.1 Servizi base

CONDUZIONE OPERATIVA SISTEMI OPEN REMOTO ORARIO BASE							
Descrizione		**Tipologia**	**N° elem. I Anno**	**N° elem. II Anno**	**N° elem. III Anno**	**N° elem. IV Anno OPZIONALE**	**N° elem. V Anno OPZIONALE**
Presidio remoto orario base server logici Unix/Linux	U1	Server logico Unix/Linux semplice	**750**	**750**	**750**	**750**	**750**
	U3	Server logico Unix/Linux complesso	**20**	**20**	**20**	**20**	**20**
Presidio remoto orario base server logici Windows	W1	Server logico Windows semplice e	**200**	**200**	**200**	**200**	**200**
	W3	Server logico Windows complesso	**20**	**20**	**20**	**20**	**20**
Presidio remoto orario base apparati rete/sicurezza	R1	Apparato rete/sicurezza semplice	**500**	**500**	**500**	**500**	**500**
	R2	Apparato rete/sicurezza complesso	**81**	**81**	**81**	**81**	**81**
Presidio remoto orario base sottosistemi DBMS	D1	Sottosistema DBMS semplice	**95**	**95**	**95**	**95**	**95**
	D2	Sottosistema DBMS complesso	**5**	**5**	**5**	**5**	**5**
Quantità complessiva di storage installato (TeraByte)			**2000**	**2000**	**2000**	**2000**	**2000**
Livello di complessità infrastruttura storage (0, 1, 2, 3, 4)			**2**	**2**	**2**	**2**	**2**

7.2 Servizi opzionali

MONITORAGGIO NOTTURNO/FESTIVO							
Descrizione		**Tipologia**	**N° elem. I Anno**	**N° elem. II Anno**	**N° elem. III Anno**	**N° elem. IV Anno OPZIONALE**	**N° elem. V Anno OPZIONALE**
Presidio remoto orario notturno e festivo	S1	Server logico semplice	**500**	**500**	**500**	**500**	**500**
	S2	Server logico complesso	**40**	**40**	**40**	**40**	**40**

SUPPORTO SPECIALISTCO						
Descrizione	**N° giorni I Anno**	**N° giorni II Anno**	**N° giorni III Anno**	**N° giorni IV Anno OPZIONAE**	**N° giorni V Anno OPZIONALE**
Supporto specialistico a richiesta specialista di tecnologia	**300**	**300**	**300**	**300**	**300**
Supporto specialistico sistemista senior	**1080**	**1080**	**1080**	**1080**	**1080**
Supporto specialistico sistemista	**270**	**270**	**270**	**270**	**270**
Supporto specialistico sistemista junior	**4050**	**4050**	**4050**	**4050**	**4050**

REPERIBILITA'					
Descrizione	**N° ore I Anno**	**N° ore II Anno**	**N° ore III Anno**	**N° ore IV Anno OPZIONALE**	**N° ore V Anno OPZIONALE**
Reperibilità specialista di tecnologia					
Reperibilità sistemista senior	**2000**	**2000**	**2000**	**2000**	**2000**
Reperibilità sistemista	**1000**	**1000**	**1000**	**1000**	**1000**
Reperibilità sistemista junior	**1000**	**1000**	**1000**	**1000**	**1000**

INTERVENTI FUORI ORARIO					
Descrizione	**N° ore I Anno**	**N° ore II Anno**	**N° ore III Anno**	**N° ore IV Anno OPZIONALE**	**N° ore V Anno OPZIONALE**
Interventi fuori orario coordinatore/capo progetto					
Interventi fuori orario specialista di tecnologia					
Interventi fuori orario sistemista senior	**500**	**500**	**500**	**500**	**500**
Interventi fuori orario sistemista	**100**	**100**	**100**	**100**	**100**
Interventi fuori orario sistemista junior	**500**	**500**	**500**	**500**	**500**

7.3 Servizi accessori

SERVIZI ACCESSORI						
Descrizione	**Tipologia (dimensionamento)**	**N° elem. I Anno**	**N° elem. II Anno**	**N° elem. III Anno**	**N° elem. IV Anno OPZIONALE**	**N° elem. V Anno OPZIONALE**
Gestione Infrastrutture non standard	Ulteriori Ambienti Elaborativi – VDI (n.200 VDI)	**1**	**1**	**1**	**1**	**1**
	Sicurezza fisica	**1**	**1**	**1**	**1**	**1**
Manutenzione Hardware	Hardware CRED	**1**	**1**	**1**	**1**	**1**
	Reti Periferiche	**1**	**1**	**1**	**1**	**1**
	Postazioni di Lavoro (n.5.000 PDL)	**1**	**1**	**1**	**1**	**1**
Supporto Ambiente Client	(N.5.000 Pdl)	**1**	**1**	**1**	**1**	**1**

8 MODALITA' DI ESECUZIONE DELLA FORNITURA

In questo paragrafo vengono descritte le specifiche modalità di esecuzione della fornitura.

8.1 Organizzazione del Service Desk

I servizi richiesti di Conduzione Operativa, Monitoraggio, Supporto ambiente client, etc, devono essere erogati in modalità remota, dal Centro Servizi del Fornitore (vedi par. 4.3 del Capitolato Tecnico dell'AQ) mediante collegamento telematico alla rete dell'Amministrazione.

In questa modalità il fornitore deve disporre di un Service Desk disponibile H24 che funzioni da Single Point of Contact (SPoC), in grado di far fronte a:

- In orario base da lunedì a venerdì, tutte le esigenze degli utenti regionali;
- H24 x 365 giorni/anno, tutte le segnalazioni di malfunzionamento provenienti dagli utenti e a tutti gli eventi impattanti sull'infrastruttura generati dai sistemi di monitoraggio, se non inoltrati direttamente alle strutture specializzate;
- H24 x 365 giorni/anno, segnalazioni di malfunzionamenti provenienti da fornitori terzi o utenti esterni indicati dall'Amministrazione.

L'estensione dall'orario da base ad H24x365, per la segnalazione dei malfunzionamenti, avviene tramite il servizio di "Monitoraggio notturno/festivo" per i sistemi contrattualizzati in tale servizio.

L'obiettivo dello SPoC è quello di provvedere a identificare le necessità dell'utente chiamante, eventualmente fornire un primo livello di supporto sulla base di FAQ consolidate, documentazione o indicazioni specifiche fornite dall'Amministrazione (sull'uso di particolari strumenti o servizi applicativi), e/o instradare allo specifico supporto i casi non risolti.

L'accesso allo SPOC dovrà prevedere almeno i seguenti canali:

- E-mail;
- Numero telefonico unico con possibile IVR;
- Web, tramite sistema Trouble Ticketing del fornitore (TT) o GLPI dell'Amministrazione.

Si deve garantire la continuità con il servizio Service Desk attuale, assicurando l'utilizzo del numero telefonico unico e dedicato a tale scopo, fornito dall'Amministrazione;

Lo SPOC deve provvedere a:

- Assicurare la comunicazione tempestiva ed efficace con l'utenza;
- Registrare tutte le chiamate e classificarle in base alla criticità;
- Risolvere i problemi più ricorrenti di non elevata complessità;
- Smistare la richiesta di assistenza di livello specialistico alle strutture specifiche (NOC, SIS, Supporto Client, Servizio Manutenzione Hardware, etc.);
- Smistare la richiesta alla struttura competente per le applicazioni software;
- Smistare la richiesta ad una determinata Struttura regionale competente;
- Qualora la risoluzione dei problemi sia di competenza di una Ditta terza (supporto manutenzione di un software, fornitore di connettività, etc.), smistare la richiesta a quest'ultima entro gli stessi tempi

previsti per lo smistamento delle richieste alle proprie strutture di competenza dedicate e supportare la Stazione Appaltante nel monitoraggio delle susseguenti attività;

- Controllare i processi di risoluzione attivati e verificarne gli esiti;
- Gestire le richieste di intervento in modo da rendere disponibili in tempo reale informazioni sullo stato di avanzamento delle richieste;
- Provvedere alla predisposizione ed al continuo aggiornamento di un inventario informatico (da rendere disponibile sul Service desk);
- Aggiornare la Knowledge base sulla base delle richieste più frequenti.

Per le richieste telefoniche devono essere garantiti i livelli minimi di servizio nel seguito elencati:

- risposta entro 30", per il 90% delle chiamate ricevute. Sarà misurato il tempo che intercorre tra l'inizio della chiamata e la risposta da parte dell'Operatore. In caso di chiamata perduta, va misurato il tempo complessivo della chiamata. Percentuale di chiamate perdute non superiore al 4%. Si definisce chiamata perduta quella telefonata che:
  a. non ottiene risposta da un operatore entro 90 secondi;
  b. a cui segue il segnale di occupato;
  c. a cui segue risposta immediata tramite messaggio preregistrato;
  d. è messa in diretto contatto con la segreteria telefonica.

Il fornitore, inoltre, deve produrre un report con cadenza mensile, relativo all'espletamento del servizio ed al rispetto dei livelli di servizio previsti, "Tempo di Attesa" (**IQTA**) e "Chiamate Perse" (**IQCP**), con almeno i seguenti dati:

a. Identificativo Utente;
b. Tempo inizio chiamata dell'utente;
c. Tempo risposta dell'operatore;
d. Problema segnalato;
e. Tempo risoluzione problema, se risolto dall'operatore;
f. Tempo di segnalazione e gruppo di intervento, in caso di escalation.

Il formato dei dati deve essere compatibile con le comuni Suite applicative per l'ufficio, per un successivo eventuale trattamento.

Per le richieste via web o e-mail, di competenza dello SPOC, devono essere garantiti i seguenti livelli minimi di servizio:

- risposta all'utente entro 15 minuti, per il 90% delle richieste ricevute. Sarà misurato il tempo che intercorre tra la richiesta e la risposta dell'Operatore.

Per le richieste di competenza di altri gruppi di supporto del fornitore, nei tempi di soluzione finale si tiene conto anche dei tempi di smistamento.

Per le richieste di competenza di strutture di ditte terze, devono essere garantiti i seguenti livelli minimi di servizio:

- smistamento della richiesta a strutture di ditte terze entro 5 minuti, per il 90% delle richieste ricevute. Sarà misurato il tempo che intercorre tra la richiesta dell'utente e lo smistamento dell'Operatore.

In orario base, per gli eventuali interventi onsite necessari per il ripristino delle funzionalità, il fornitore può avvalersi del supporto specialistico di presidio soltanto per gli apparati installati presso il CRED di via Don Bosco.

Gli interventi onsite fuori orario base, notturni e festivi sono inclusi nel servizio di "Monitoraggio notturno/festivo" e non possono essere ricondotti al supporto specialistico di presidio o al servizio "Intervento fuori orario".

Gli utenti del servizio sono tutti i dipendenti ed i consulenti interni della Regione Campania. Per la sola segnalazione di malfunzionamenti, possono essere autorizzati strutture pubbliche critiche (es. Protezione Civile) o ditte terze (es. supporto applicativi).

Il Fornitore deve effettuare il monitoraggio e controllo di tutti i servizi indicati dall'Amministrazione e i Componenti ICT ospitati dall'Infrastruttura ICT anche nel caso in cui tali servizi o componenti siano riferiti a infrastrutture gestite da terze parti (es. provider esterni) ed in tale caso le procedure devono prevedere l'escalation verso strutture specifiche, esterne all'organizzazione del fornitore, individuati dall'Amministrazione.

L'organizzazione proposta, nell'offerta tecnica, per l'erogazione dei servizi di Service Desk, inclusa la modalità di interazione tra i diversi gruppi tecnici di supporto, indipendentemente se appartenenti tutti al fornitore aggiudicatario o meno, sarà oggetto di valutazione tra i criteri discrezionali.

Le specifiche di tutti i gruppi tecnici di supporto e delle relative competenze verranno fornite ad inizio contratto dall'Amministrazione, fermo restando che tali gruppi possono cambiare durante il periodo contrattuale.

8.1.1 Attività di apertura e registrazione

Le richieste di intervento esplicitate attraverso i diversi mezzi disponibili dovranno essere convogliate nel Service desk e rese immediatamente disponibili alla consultazione via web al personale dell'Amministrazione autorizzato. In caso di chiamata telefonica il sistema dovrà creare automaticamente un ticket con almeno le informazioni essenziali (numero di telefono del chiamante, tipologia della richiesta, timestamp). Il ticket aperto dovrà subito dopo essere integrato, anche manualmente dall'operatore, con le informazioni descritte di seguito. Analoga procedura devono seguire le richieste pervenute via e-mail e via web.

Ogni registrazione dovrà obbligatoriamente contenere almeno le seguenti informazioni:

1. nominativo dell'utente richiedente;
2. identificativo dell'operatore dello SPOC;
3. data con l'indicazione dell'ora, minuti e secondi in cui è stata ricevuta la richiesta;
4. canale di comunicazione utilizzato per l'inoltro della richiesta di intervento;

5. tipologia della richiesta di intervento;
6. descrizione della richiesta di intervento;
7. procedure avviate per la risoluzione del problema.

Nel caso di smistamento della richiesta ad unità operative dedicate, la registrazione deve altresì prevedere almeno i seguenti dati:

a. gruppo o struttura interessata e nome dei tecnici intervenuti,
b. descrizione dell'anomalia o del guasto riscontrato,
c. descrizione dettagliata dell'intervento risolutivo (p.e., configurazioni, riparazioni, ripristini, parti di ricambio),
d. tempi di intervento e di ripristino,
e. note per eventuali comunicazioni,
f. nel caso di smistamento della chiamata a Ditte terze, lo stato della richiesta e il controllo del rispetto dei tempi di intervento delle Ditte terze,
g. chiusura formale dell'intervento con l'indicazione dell'ora, minuti e secondi in cui è stata soddisfatta la richiesta, del nome, cognome e identificativo dell'operatore che effettua la chiusura e nome, cognome e matricola dell'utente che ha confermato la chiusura del ticket.

Si rileva che in caso di operazioni che richiedano necessariamente la presenza dell'utente, l'operatore dovrà inserire la data di inizio intervento concordata con l'utente

8.1.2 Attività di chiusura

La chiusura formale della richiesta di intervento è a cura della struttura dello SPOC.

Lo SPOC, prima di chiudere il ticket, deve **assicurarsi** che la richiesta di assistenza o manutenzione, da parte dell'utente, sia stata correttamente soddisfatta. L'utente dovrà, comunque, avere la possibilità di confermare la chiusura del ticket o, nel caso la soluzione non lo soddisfi, riaprirlo.

I ticker riaperti sono conteggiati ai fini dell'indicatore di qualità "Attività eseguite correttamente" (**IQ16**).

Per le ipotesi di smistamento della chiamata a Ditta terza, la chiusura formale della richiesta è sempre a cura dello SPOC a valle della comunicazione dell'esito da parte della Ditta terza, fatto salvo il monitoraggio della richiesta per conto dell'Amministrazione.

8.2 Organizzazione dei gruppi di lavoro onsite/remoto

Il supporto specialistico alla conduzione operativa (SIS e NOC/SOC) e all'Assistenza OnSite (AOS) deve essere erogato in modalità continuativa a canone senza soluzione di continuità, a partire dalla data di avvio del contratto e fino al termine della fornitura, salvo diverse indicazioni dell'Amministrazione.

Le risorse del supporto specialistico onsite (SIS e NOC/SOC), per il loro ruolo e per le loro competenze, devono acquisire, durante la fase di affiancamento, la completa conoscenza:

- di tutti i servizi gestiti, indipendentemente da dove sono ospitati (CRED; Cloud, etc.) e della loro architettura (bilanciatori, proxy, frontend, backend, DB, SAN/NAS associate, etc., con i relativi IP) e le policy di backup applicate;
- dell'infrastruttura hardware e della sua configurazione;
- di tutti gli apparati di rete e sicurezza e la loro architettura;
- della configurazione della rete/vlan e delle politiche di routing;
- della configurazione degli apparati di sicurezza e le policy applicate;
- di tutte le procedure operative e dell'attività in corso.

Nella fascia oraria 8:00-20:00, dal lunedì al venerdì, è obbligatoria la presenza, nel CED di Don Bosco, di almeno una risorsa del supporto onsite per ogni struttura (NOC/SOC, SIS, PDL). In caso di ferie o malattia la risorsa onsite deve essere immediatamente sostituita con un'altra con lo stesso profilo e le stesse competenze. Nel caso in cui tale risorsa non sarà immediatamente sostituita o sostituta con una risorsa che l'Amministrazione riterrà, a suo insindacabile giudizio, non adeguata, verranno applicate le penali previste.

Per il servizio remoto di conduzione Operativa Sistemi Open viene chiesto l'erogazione in orario base di 10 ore al giorno, dal lunedì al venerdì e dalle ore 8:00 alle ore 18:00. È previsto un criterio tecnico premiante per le offerte in AS che prevedono un orario giornaliero che vada oltre le 10 ore giornaliere.

Per i servizi a consumo (Reperibilità, Interventi fuori orario, etc.), le procedure per l'attivazione verranno concordate durante la fase iniziale del contratto.

.

8.3 Fasi operative della fornitura

L'affidamento dei servizi di system management è inserito in un quadro organico di discontinuità della fornitura, dal momento che il fornitore aggiudicatario dell'Appalto Specifico dovrà subentrare al fornitore uscente e, a fine contratto, dovrà cedere i servizi ad un fornitore subentrante. Il progetto di fornitura deve pertanto prevedere inizialmente un inserimento graduale ed efficace nella realtà organizzativa dell'Amministrazione richiedente, nonché una fuoriuscita controllata e progressiva dalla stessa, a fine contratto.

8.3.1 Affiancamento iniziale

La fase di affiancamento iniziale si pone l'obiettivo di permettere il passaggio di consegne tra la struttura di servizio precedente alla stipula dell'Appalto specifico e la nuova. La durata è di due mesi e si articola nelle seguenti principali sottofasi:

- Affiancamento e gestione transitoria iniziale: affiancamento ai gestori dei servizi oggetto dell'Appalto specifico (Strutture organizzative dell'Amministrazione e ai fornitori in scadenza di contratto).

- Esame di tutta la documentazione esistente su tutti i servizi gestiti, gli asset informatici, i processi, le procedure operative, documenti di progetto, mappe di rete, etc, procedendo inoltre al popolamento della Knowledge Management. L'esito dell'esame della documentazione (documentazione incompleta, non aggiornata, etc.) deve essere sottoscritta da entrambi le parti (fornitore entrante e forniture uscente) e inviata all'Amministrazione.
- Predisposizione del piano generale della fornitura: realizzazione e sviluppo del piano generale della fornitura, in linea con le linee guida definite dall'Amministrazione in AS. Tale piano deve essere approvato dall'Amministrazione.
- Completamento del collegamento telematico con il Centro Servizi.
- Installazione e/o avvio operativo degli strumenti a supporto della fornitura richiesti o messi a disposizione dall'Amministrazione.

Le risorse del fornitore che parteciperanno all'affiancamento dovranno essere almeno due per ogni ambito (reti, sistemi e PDL) tra cui i responsabili dei vari ambiti e dovranno essere le stesse che prenderanno in carico i servizi.

Durante il periodo di affiancamento (startup) la responsabilità dei servizi rimane in capo al fornitore uscente ed il fornitore aggiudicatario dell'AS non percepirà alcun corrispettivo.

8.3.2 Trasferimento del know-how a fine fornitura

In prossimità della conclusione del contratto, il Fornitore deve garantire un periodo di supporto alla transizione verso un nuovo eventuale fornitore, o alla presa in carico dei servizi da parte dell'Amministrazione. In tale periodo, il Fornitore si impegna a collaborare all'ordinata migrazione di infrastrutture tecnologiche, comprensive dei DBMS utilizzati per il governo della fornitura e l'erogazione dei servizi, e competenze verso l'Amministrazione o ad un terzo designato dall'Amministrazione.

Dovrà esser definito un Piano di Trasferimento per attuare la migrazione di cui sopra. Tale piano, che dovrà essere formalizzato nei tempi richiesti dall'Amministrazione, sarà mantenuto aggiornato per tutto il periodo di vigenza contrattuale.

Il Piano di Trasferimento consisterà nella redazione di un piano di massima di tipo esecutivo, articolato in attività con l'indicazione di scadenze di inizio e fine, di responsabilità, di contenuti e risultati tali da attivare il "Trasferimento" e da renderne controllabile la sua effettiva attuazione.

I costi del supporto alla transizione sono inclusi nei costi dei servizi base.

Il periodo di supporto potrà durare fino a tre mesi dove dovranno essere previste sessioni di addestramento.

Se richiesto, il fornitore deve trasferire all'Amministrazione anche le soluzioni e gli strumenti utilizzati nel corso della fornitura. Gli strumenti dovranno essere installati presso un datacenter regionale senza costi aggiuntivi. Saranno a carico dell'Amministrazione solo i costi relativi ad eventuali licenze.

8.3.3 Fase esecuzione contratto di fornitura

Le figura professionali del supporto specialistico offerte dal fornitore dovranno essere adeguate a coprire gli ambiti tecnologici e le attività indicate dall'Amministrazione nel paragrafo 6. Tale adeguamento potrà essere richiesto dall'Amministrazione anche nel corso di esecuzione del contratto ed anche a seguito dell'introduzione di variazioni nell'ambito tecnologico. Il fornitore si impegna a adeguare le conoscenze del personale impiegato nell'erogazione dei servizi o ad inserire nei gruppi di lavoro risorse con skill adeguato, senza alcun onere aggiuntivo per l'Amministrazione.

L'Amministrazione si riserva il diritto di richiedere la sostituzione del personale afferente ad un servizio qualora, a suo insindacabile giudizio, risulti non adeguato all'attività svolta.

Il personale onsite opererà principalmente nei locali delle sedi Regionali messi a disposizione dell'Amministrazione, secondo le direttive impartite dalla stessa in merito alle politiche di sicurezza e di accesso.

La documentazione acquisita durante la fase di affiancamento dovrà servire ad alimentare la Knowledge Base (KB) del fornitore. Durante tutto il periodo contrattuale il fornitore dovrà gestire e mantenere sempre aggiornata tutta la documentazione utile per l'erogazione dei servizi di propria competenza, procedendo, inoltre, al popolamento della KB. Entro i primi quattro mesi, il fornitore dovrà aggiornare/completare tutta la documentazione che durante la fase di affiancamento risulta non aggiornata/non completa o inesistente, in particolare:

- Architettura di tutti i servizi gestiti (bilanciatori, proxy, frontend, backend, DB, SAN/NAS associate, VM con i relativi IP, interazione con altri servizi, policy di backup applicate, descrizione sintetica del servizio, etc.);
- Disegno degli schemi dettagliati delle reti del Datacenter e di tutte le reti periferiche con descrizione e configurazione degli apparati.

La qualità della documentazione prodotta, nel rispetto degli standard documentali, sarà verificata dall'Amministrazione.

Per il rispetto dei tempi e della qualità della documentazione, gli indicatori di riferimento sono "Slittamento delle scadenze" (**IQ06**) e "Qualità della documentazione prodotta" (**IQ07**).

Inoltre, l'AOS deve effettuare, nei primi quattro mesi dell'avvio del contratto, il censimento di tutte le postazioni fisse e portatili, distribuite in tutte le sedi regionali, utilizzando, per identificare gli item, soluzioni innovative (Rfid, Qrcode, NFC, etc.). La soluzione individuata dal fornitore sarà oggetto di valutazione tecnica e dovrà essere fornita senza costi aggiuntivi per l'Amministrazione. Il censimento va ripetuto con cadenza annuale da programmare con i referenti dell'Amministrazione.

Anche questi censimenti dovranno servire ad alimentare e mantenere sempre aggiornata la base dati integrata negli strumenti forniti all'Amministrazione. L'obiettivo è quello di avere le informazioni il più possibile corrispondenti alle situazioni reali.

8.4 Service Management

Tali indicazioni sono state inserite nei paragrafi opportuni.

8.5 Strumenti del centro servizi

Il Fornitore dovrà disporre degli opportuni strumenti operativi da utilizzare nell'esecuzione delle attività di system management e in particolare:

- una piattaforma di Service Management;
- una piattaforma di monitoraggio sistemi;
- una piattaforma di reportistica e SLA management.

Queste piattaforme devono essere completamente integrate tra di loro.

L'utilizzo degli strumenti suddetti è incluso nei costi dei servizi richiesti e pertanto non comportano alcun onere aggiuntivo per l'Amministrazione. In particolare, sono inclusi nei costi dei servizi, sia eventuali licenze necessarie, sia eventuali installazioni di componenti client (agent) o server. Nel seguito sono evidenziate le principali funzionalità che tali strumenti devono possedere.

8.5.1 Piattaforma di Service Management

Come indicato nel paragrafo 6, l'Amministrazione utilizza GLPI come strumento di Service Desk.

Con tale strumento sono stati strutturati diversi processi: per servizi di system management, per servizi offerti dalla stessa Amministrazione (es. richiesta PEC) e per servizi offerti da fornitori terzi (es. servizi di supporto applicativo). Alcuni processi prevedono l'approvazione di utenti con profilo specifico (es. dirigente) o in gruppi particolari (gruppo NOC).

Inoltre, in GLPI:

- tramite collegamento con OCS inventory, viene gestito l'inventario dei Computer, Schermi, Stampanti, Software, etc.;
- sono state definite tutte le categorie delle richieste e degli incident;
- vengono gestite le licenze software, gruppi, entità, etc.

Pertanto, il fornitore deve mettere a disposizione dell'Amministrazione, senza oneri aggiuntivi, una piattaforma di Service Management che, oltre a soddisfare i requisiti previsti nel capitolato tecnico relativo all'AQ, tenga conto ed integri quanto già realizzato dall'Amministrazione in GLPI. Di seguito vengono indicate solo alcune delle funzionalità che deve prevedere la piattaforma:

- La rilevazione di tutti i parametri di dimensionamento dei servizi richiesti (server, DBMS, apparati rete, storage, postazioni, utenti, etc.).
- La rilevazione dei tempi di risposta e delle chiamate telefoniche perse.

- La rilevazione degli indicatori di qualità della fornitura.
- Recepire tutti i requisiti descritti nei paragrafi precedenti (priorità degli incident, approvazione della soluzione, definizione dei change standard, etc.).
- La possibilità che l'Amministrazione possa definire e modificare flussi di lavoro (workflow di processo).
- La possibilità che gruppi tecnici dell'Amministrazione, o da essa indicati, possano partecipare alla lavorazione dei ticket.
- Rilevare i tempi di lavoro dei vari gruppi (interni o esteri al fornitore).
- La possibilità che l'Amministrazione possa approvare/monitorare la lavorazione dei ticket.
- La possibilità che l'Amministrazione possa accedere a tutte le informazioni contenute nel CMDB, di effettuare ricerche e produrre report.

La rilevazione dei parametri di dimensionamento deve essere automatizzata tramite strumenti di autodiscovery, script che importano periodicamente i dati da altre fonti. Gli oggetti relativi ad ogni parametro devono poter essere identificati tramite una chiave univoca (IP, Matricola, Codice inventario, etc).

L'Amministrazione si riserva di chiedere, durante il corso della fornitura e senza oneri aggiuntivi, nuove funzionalità o la gestione di nuovi item.

8.5.2 Piattaforma di Monitoraggio

Relativamente al monitoraggio dei sistemi e delle reti l'Amministrazione utilizza:

- Zabbix per gli apparati (Server, Storage, Switch, Router, SAN) e per i servizi (database e applicazioni)
- CA Spectrum, la suite di prodotti per le attività di network management
- CA E-Health per l'analisi delle performance della rete

La maggior parte dei server ha un agent installato per comunicare con il server Zabbix.

Il fornitore può riusare gli strumenti già utilizzati dall'Amministrazione o altri strumenti con caratteristiche uguali o superiori.

Nel caso decida di utilizzare alcuni degli strumenti preesistenti, il fornitore ne assume la completa conduzione, la responsabilità del corretto funzionamento e di eventuali licenze necessarie e, se necessario, dovrà rivederne le configurazioni.

Per gli strumenti forniti, invece, l'installazione di tutto quanto necessario per la loro configurazione, compreso l'installazione di eventuali agent, è a completo carico del fornitore.

Inoltre, tutti gli strumenti devono essere accessibili e configurati per il monitoraggio anche dalla Control Room del CED di Regione Campania.

Le piattaforme di monitoraggio devono consentire di tenere sotto controllo lo stato operativo dei sistemi e delle relative componenti e degli apparati di rete, rilevando automaticamente informazioni quali a titolo esemplificativo, ma non esaustivo, le seguenti:

- Allocazioni di spazio disco,
- Utilizzo della memoria,
- Utilizzo della CPU,
- Utilizzo delle interfacce di rete,
- Utilizzo della banda,
- Modifiche delle configurazioni.

Oltre a monitorare la disponibilità dei servizi applicativi e ad essere di supporto nella risoluzione dei problemi, le soluzioni adottate dovranno consentire di controllare le performance dei servizi erogati per verificarne l'aderenza ai livelli di servizio attesi.

Tali strumenti devono essere resi accessibili, in tutte le sue funzioni, anche all'Amministrazione.

Il sistema, inoltre, deve essere integrato con:

- la piattaforma di Service Management per l'apertura/chiusura automatica dei ticket di incident
- altri sistemi di monitoraggio per es. il sistema di monitoraggio impianti

A fine contratto, qualunque siano stati gli strumenti di monitoraggio utilizzati, tali strumenti, se richiesto, devono essere passati in gestione, senza oneri aggiuntivi, all'Amministrazione o terzi parti indicate dall'Amministrazione.

8.5.3 Piattaforma di reportistica e SLA management

Il Fornitore dovrà rendere disponibile alle Amministrazioni un sistema per l'analisi degli andamenti dei livelli di servizio, allo scopo di:

- verificare la conformità dei servizi rispetto a quanto richiesto;
- verificare l'effettivo andamento dei servizi e anticipare la gestione degli scostamenti;
- consuntivare i servizi e le attività;
- verificare l'andamento degli Indicatori di qualità;
- ottimizzare le attività di monitoraggio dei servizi.

Il sistema dovrà avere tutte le specifiche indicate nel Capitolato Tecnico relativo all'AQ, riportate anche nei paragrafi successivi.

Il sistema dovrà raccogliere i dati elementari e calcolare gli indicatori di qualità della fornitura e, sulla base di essi, predisporre delle rappresentazioni dell'andamento della stessa. Nel caso in cui parte dei dati elementari siano gestiti da sistemi dell'Amministrazione, il Fornitore dovrà predisporre ed assicurare tutto

quanto necessario per il caricamento dei dati, nel formato e con la periodicità stabilita congiuntamente all'Amministrazione, e la successiva elaborazione e pubblicazione secondo le stesse modalità applicate ai dati elementari direttamente gestiti.

Inoltre, il fornitore si impegna a fornire la base dati di dettaglio contenente tutti i dati rilevati, utilizzata per la valorizzazione degli indicatori di qualità.

Il sistema dovrà prevedere la possibilità di esportare i report in formati dati e grafici di comune utilizzo e visualizzabili nelle comuni Suite applicative per l'ufficio, per un successivo ed eventuale trattamento (modifica, manipolazione, esportazione, ecc.).

Inoltre, è richiesta la fornitura di strumenti idonei, cui verrà dato accesso all'Amministrazione, per effettuare interrogazioni e query delle basi dati sopra definite.

Dovranno, inoltre, essere rese disponibili tutte le informazioni inerenti al personale impegnato nel servizio onsite AOS, in termini grado di utilizzo.

8.6 Strumenti per la gestione e la configurazione delle PDL

Come indicato nel paragrafo 6.3.4, il fornitore deve mettere a disposizione dell'Amministrazione, senza oneri aggiuntivi, tutti gli strumenti necessari alla gestione in remoto ed integrata delle postazioni di lavoro sia fisse che mobili.

Di seguito, gli strumenti principali richiesti:

- Gestione degli asset (HW e SW) e delle configurazioni: oltre alla gestione degli asset, devono permettere lo scanning ad intervalli stabiliti delle PDL, dell'HW e del SW, creando statistiche di funzionamento (spazi disco, memoria utilizzata, etc.) e rilevando eventuali modifiche nelle configurazioni.
- Controllo remoto: devono permettere il collegamento remoto degli operatori HD sulle postazioni degli utenti con qualunque S.O. Microsoft installato sul client.
- Distribuzione degli applicativi: devono permettere l'installazione o il ripristino, individuale o massivo, dei pacchetti software.
- Upgrade Sistema Operativo: strumenti e procedure per l'aggiornamento di S.O. Microsoft Windows da una major release ad un'altra.

Gli strumenti individuati dal fornitore saranno oggetto di valutazione tecnica.

9 MODALITA' DI REMUNERAZIONE E VARIAZIONE DEI CORRISPETTIVI

La seguente tabelle riepiloga le modalità di remunerazione per il presente AS.

Servizio	Tipologia	Parametri di dimensionamento	Modalità di remunerazione

Conduzione operativa sistemi open (windows, linux, unix)	Base	1. Modalità di presidio (on-site, **remoto**) 2. Orario di servizio (**base**, esteso) 3. Infrastruttura gestita (**server, rete, DBMS, storage**)	Canone
Monitoraggio notturno/festivo sistemi open	Opzionale	1. Modalità di presidio (on-site, **remoto**) 2. Orario di servizio (notturno, **notturno/festivo**) 3. Infrastruttura gestita (**server**)	Canone
Supporto specialistico	Opzionale	1. Risorse professionali	Tempo/spesa o a corpo (giorni/persona)
Reperibilità	Opzionale	1. Risorse professionali	Tempo/spesa (ore/persona)
Intervento fuori orario	Opzionale	1. Risorse professionali	Tempo/spesa (ore/persona)
Gestione Infrastruttura non standard - Ulteriori ambienti operativi	Accessorio	1. Dimensionamento VM	Canone
Gestione Infrastruttura non standard - Sicurezza fisica	Accessorio	1. Dimensionamento infrastruttura fisica	Canone
Manutenzione Hardware	Accessorio	1. Dimensionamento infrastruttura rete, sicurezza, server e PdL	Canone
Supporto Ambienti Client	Accessorio	1. Dimensionamento PdL	Canone

Per i servizi per i quali è prevista la remunerazione “Tempo/spesa” o “a corpo”, l’Amministrazione potrà rivedere annualmente la quantità definita inizialmente sulla base di consuntivi di attività e di effort stimati per attività progettuali.

Per i servizi per i quali è prevista una remunerazione di tipo “a canone” l’Amministrazione potrà rivedere, con cadenza annuale, le quantità definite inizialmente, effettuando una verifica degli asset hardware/software oggetto del servizio, e di conseguenza adeguerà gli importi da corrispondere al fornitore alla effettiva configurazione gestita, aumentandoli o diminuendoli proporzionalmente, nel rispetto dell’art. 106 del D.Lgs. 50/2016 e comunque della normativa vigente.

10 GOVERNO DELLA FORNITURA

Nell’ambito del contratto stipulato dall’Amministrazione, il fornitore dovrà indicare un Responsabile della fornitura che dovrà essere il responsabile dell’intera struttura organizzativa proposta, avere una visione unica ed integrata dello stato dell’arte dell’intera fornitura, delle attività e dei progetti in corso, verificare e riportare all’Amministrazione i rendiconti periodici. Pertanto, il Responsabile della fornitura dovrà garantire la qualità complessiva dei servizi erogati, operare quale interfaccia unica amministrativa verso l’Amministrazione e risolvere le potenziali criticità durante tutta la durata del contratto.

Nell’ambito della governance della fornitura, il Responsabile dovrà, in particolare, fornire all’Amministrazione la reportistica periodica, con cadenza uguale a quella della fatturazione, relativa agli asset degli apparati gestiti (come risultanti dal DB della configurazione), ai ticket elaborati nel periodo di

riferimento, ai livelli di servizio conseguiti con l'eventuale calcolo delle penali applicabili, alla rendicontazione delle risorse professionali utilizzate a consumo, agli stati di avanzamento (SAL) delle attività remunerate a corpo.

Il Responsabile della fornitura potrà avvalersi di una struttura di supporto. Il Responsabile della fornitura e la struttura di supporto non faranno parte di alcuno dei gruppi di lavoro operativi e non comporteranno alcun onere aggiuntivo per l'Amministrazione.

Il Fornitore dovrà effettuare la rilevazione della soddisfazione degli utenti, con una periodicità semestrale e per l'intera durata del contratto, sull'utenza di riferimento indicata dall'Amministrazione.

I risultati della rilevazione dovranno essere consegnati insieme alla reportistica periodica al fine di poter verifica l'indicatore "**IQ09**" relativo al grado di soddisfazione dei referenti.

La rilevazione è a carico del Fornitore, senza alcun onere aggiuntivo per l'Amministrazione.

10.1 Pianificazione

A valle della stipula del contratto, durante la fase di affiancamento, il fornitore deve redigere un piano di lavoro di tutte le attività iniziali (configurazione ed attivazione dei servizi, configurazione degli strumenti, etc.). per la presa in carico dei servizi. Un piano analogo va presentato per tutte le attività che prevedono una fase progettuale anche durante il periodo contrattuale. Tutta la documentazione di pianificazione deve essere approvata dall'Amministrazione.

10.2 Consuntivazione dei servizi svolti

L'Amministrazione sulla base della documentazione specifica (piano di lavoro, consuntivo attività, rendiconto risorse utilizzate, etc.) effettuerà la verifica di conformità delle prestazioni rese dal fornitore. Gli esiti di tali verifiche saranno comunicati tramite mail o altra comunicazione scritta nonché attraverso lettere di rilievo.

10.3 Assicurazione qualità

I servizi di system management dovranno essere svolti dal Fornitore in regime di qualità, secondo gli standard ISO 9001:2015.

Inoltre, i servizi che richiedono operatività remota dovranno essere svolti dal Fornitore garantendo le Amministrazioni richiedenti sul rispetto delle prassi e delle norme sulla sicurezza per tali modalità operative.

10.3.1 Piano della qualità

Il Fornitore, in sede di Appalto Specifico, dovrà predisporre e fornire all'Amministrazione, entro 10 (dieci) giorni lavorativi dalla data di stipula del contratto, il Piano della Qualità del progetto di fornitura. Il Piano della Qualità dovrà:

- fornire lo strumento per collegare i requisiti specifici dei servizi contrattualmente richiesti, con le procedure generali del sistema qualità del Fornitore già esistenti;
- esplicitare le disposizioni organizzative e metodologiche adottate dal fornitore, allo scopo di raggiungere gli obiettivi tecnici e di qualità contrattualmente definiti;
- dettagliare i metodi di lavoro messi in atto dal fornitore, facendo riferimento o a procedure relative al proprio sistema, e perciò descritte nel manuale qualità, o a procedure sviluppate per lo specifico contratto, a supporto delle attività in esso descritte, in questo caso da allegare al piano;
- garantire il corretto e razionale evolversi delle attività contrattualmente previste, nonché la trasparenza e la tracciabilità di tutte le azioni messe in atto dalle parti in causa, il Fornitore e la Amministrazione contraente.

Il Piano della Qualità sarà valutato dalla Amministrazione e dovrà essere esplicitamente approvato o emendato e gli eventuali emendamenti dovranno essere recepiti dal Fornitore.

Il Fornitore, nello svolgimento delle attività contrattualmente previste, dovrà attenersi e dovrà essere conforme a quanto previsto dal piano della qualità approvato.

Il Fornitore dovrà accettare le eventuali verifiche ispettive (verifiche mirate o verifiche di seconda parte), effettuate dall'organismo di ispezione designato dalla Amministrazione e svolte nel rispetto di quanto prescritto dalla serie di norme EN ISO 19011, allo scopo di verificare il rispetto di quanto stabilito nel Piano di Qualità.

10.3.2 Indicatori della qualità

Il Fornitore è tenuto, per l'intera durata dei servizi, a rendicontare gli Indicatori di qualità richiesti dall'Amministrazione. Tutti gli Indicatori di qualità dovranno essere indicati nel Piano della Qualità generale da sottoporre all'approvazione dell'Amministrazione.

Durante l'intero periodo contrattuale ciascun indicatore di qualità potrà essere riesaminato su richiesta dell'Amministrazione; il riesame potrà derivare da nuovi strumenti di misurazione non disponibili alla data di stipula del contratto e/o dall'adeguamento delle metodiche atte alla rilevazione dei singoli indicatori di qualità che sono risultate non efficaci.

Nella stesura del Piano della Qualità, sottoposto all'approvazione dell'Amministrazione, il Fornitore per ciascun Indicatore di qualità dovrà dettagliare le fonti dati utilizzate per la raccolta dei dati elementari nonché gli strumenti per l'elaborazione delle informazioni di dettaglio.

L'Amministrazione ed il Fornitore, in caso di necessità, concorderanno eventuali modifiche ai metodi di calcolo successivamente riportati e tracciati nel Piano della Qualità generale.

Il Fornitore si impegna a erogare i servizi tenendo conto delle modifiche richieste e a recepirle nel Piano della Qualità generale, da sottoporre all'approvazione dell'Amministrazione.

Gli Indicatori di Qualità scelti dall'Amministrazione nell'ambito dell'AS tengono conto delle tipologie e dei modelli di remunerazione dei servizi richiesti.

Per i servizi di conduzione operativa remunerati a canone secondo i modelli descritti nel paragrafo 9, per i quali viene fortemente delegata al Fornitore la responsabilità di strutturare i servizi con le risorse e le modalità organizzative da lui ritenute ottimali, l'Amministrazione ha scelto gli Indicatori di Qualità relativi al funzionamento del Sistema Informativo, quali ad esempio disponibilità dei servizi e dei sistemi, tempestività e correttezza nell'esecuzione delle attività, ecc.

Per i servizi di supporto specialistico e per tutte le risorse impegnate, per i quali il Fornitore è tenuto a dimensionare i gruppi di lavoro in base alle specifiche fornite dall'Amministrazione, si è dato maggiore enfasi agli Indicatori di Qualità relativi alla gestione delle risorse, quali ad esempio adeguatezza del personale, sostituzione di risorse, ecc.

Di seguito si riepilogano gli indicatori di Qualità generali richiesti. Per la loro definizione si rimanda al capitolo 2 "Indicatori di qualità generali" dell'Appendice 1 "Indicatori di qualità". Per ogni indicatore vengono riportati i valori soglia, i periodi di riferimento e le penali definiti dall'Amministrazione

Indicatore di Qualità generali	Valore Soglia	Periodo di riferimento	Penale applicata al superamento del valore soglia
IQ01 - Personale della fornitura inadeguato	1	Trimestrale	0,5‰ del valore complessivo del Contratto di Fornitura per ogni risorsa sostituita oltre soglia
IQ02 - Turn over del personale	1	Trimestrale	0,5‰ del valore complessivo del Contratto di Fornitura per ogni risorsa sostituita oltre soglia
IQ03 - Inadeguatezza del personale proposto	2	Trimestrale	0,5‰ del valore complessivo del Contratto di Fornitura per ogni curriculum non accettato oltre soglia
IQ04 - Inserimento/sostituzione del personale	0	Trimestrale	0,3‰ del valore complessivo del Contratto di Fornitura per ogni giorno di ritardo oltre soglia

IQ05 - Attivazione degli interventi	2	Trimestrale	0,3‰ del valore complessivo del Contratto di Fornitura per ogni giorno di ritardo oltre soglia
IQ06 - Slittamento delle scadenze	5	Trimestrale	0,3‰ del valore complessivo del Contratto di Fornitura per ogni giorno di ritardo oltre soglia
IQ07 - Qualità della documentazione prodotta	10%	Trimestrale	0,3‰ del valore complessivo del Contratto di Fornitura per ogni punto percentuale oltre soglia
IQ08 – Rilievi sulla fornitura	3	Trimestrale	0,3‰ del valore complessivo del Contratto di Fornitura per ogni rilievo oltre soglia
IQ09 – Grado di soddisfazione dei referenti	80%	Semestrale	0,2‰ del valore complessivo del Contratto di Fornitura per ogni cinque punti percentuali di scostamento in diminuzione rispetto al valore di soglia

Di seguito si riepilogano gli indicatori di Qualità Operativi richiesti per l'intera fornitura. Per la loro definizione si rimanda al capitolo 3 "Indicatori di qualità operativi" dell'Appendice 1. Per ogni indicatore vengono riportati i valori soglia, i periodi di riferimento e le penali definiti dall'Amministrazione

Indicatore di Qualità Operativi	Valore Soglia	Periodo di riferimento	Penale applicata per mancato rispetto del valore soglia
IQ10a – Disponibilità in H24x365 dei servizi con monitoraggio notturno/festivo	99.90%	Mensile	0,3‰ del valore complessivo del Contratto di Fornitura per ogni 0.1% di disponibilità in meno rispetto al valore di soglia
IQ10b – Disponibilità in orario base dei servizi senza	99.50%	Mensile	0,3‰ del valore complessivo del Contratto di Fornitura per ogni 0.1% di disponibilità in meno rispetto al valore di soglia

monitoraggio notturno/festivo			
IQ11 – Disponibilità dei Sistemi	99.80%	Mensile	0,3‰ del valore complessivo del Contratto di Fornitura per ogni 0.1% di disponibilità in meno rispetto al valore di soglia
IQ12 - Tempestività di risoluzione degli incident	95%	Mensile	0,3‰ del valore complessivo del Contratto di Fornitura per ogni 1% sotto al valore di soglia
IQ13 - Tempestività di esecuzione dei change standard/predefiniti	95%	Mensile	0,3‰ del valore complessivo del Contratto di Fornitura per ogni 1% sotto al valore di soglia
IQ14 - Tempestività di esecuzione dei change non standard	95%	Trimestrale	0,3‰ del valore complessivo del Contratto di Fornitura per ogni 1% sotto al valore di soglia
IQ15 – Ticket oggetto di ripianificazione	10%	Trimestrale	0,3‰ del valore complessivo del Contratto di Fornitura per ogni 1% sopra al valore di soglia
IQ16 - Attività eseguite correttamente	5%	Trimestrale	0,3‰ del valore complessivo del Contratto di Fornitura per ogni 1% sopra al valore di soglia
IQ17 – Aggiornamento del CMS	5%	Mensile	0,3‰ del valore complessivo del Contratto di Fornitura per ogni 1% sopra al valore di soglia

Sono stati introdotti, inoltre, alcuni livelli di servizio specifici per i servizi accessori non previsti nell'AQ. Per la loro definizione si rimanda al capitolo 4 "Indicatori di qualità aggiuntivi per l'AS" dell'Appendice 1:

Indicatore di Qualità Operativi	Valore Soglia	Riferimento	Penale applicata per mancato rispetto del valore soglia
IQA1a – Servizi Accessori critici: Sicurezza Fisica par.6.3.2 Manutenzione HW Cred par.6.3.3.1 Manutenzione HW Reti Periferiche par.6.3.3.2 – sedi con “criticità alta” Risoluzione guasto H24x365	1 ora	Singolo intervento	0,3‰ del valore complessivo del Contratto per ogni ora di ritardo nella risoluzione del guasto
IQA1b – Servizi Accessori medio critici: Manutenzione HW Reti Periferiche par.6.3.3.2 - sedi con “criticità media” Risoluzione guasto in orario lavorativo	2 ore	Singolo intervento	0,3‰ del valore complessivo del Contratto per ogni ora di ritardo nella risoluzione del guasto
IQA2– Servizi Accessori non critici: Sicurezza Fisica par.6.3.2 Manutenzione HW Cred par.6.3.3.1 Manutenzione HW Reti Periferiche par.6.3.3.2 - sedi con “criticità bassa” Risoluzione guasto in orario lavorativo	NBD	Singolo intervento	0,3‰ del valore complessivo del Contratto per ogni giorno lavorativo di ritardo nella risoluzione del guasto
IQA3 - Tempestività di risoluzione degli incident ambienti client	95%	Mensile	0,1‰ del valore complessivo del Contratto per ogni 1% sotto al valore di soglia
IQA4 - Tempestività di esecuzione dei change standard/predefiniti ambienti client	95%	Mensile	0,1‰ del valore complessivo del Contratto per ogni 1% sotto al valore di soglia
IQTA – Tempo Attesa: Tempo che intercorre tra l’inizio della chiamata e la risposta da parte dell’operatore,	Entro 30’’ nel 90% delle chiamate telefoniche;	Mensile	0,1‰ del valore complessivo del Contratto per ogni 1% sotto al valore di soglia

come indicato nei paragrafi 6.2.2 e 8.1	entro 15' nel 90% dei casi per richieste inoltrate a mezzo web o e-Mail		
IQCP –Chiamate Perse: Percentuale numero chiamate perse dallo SPOC/ Centro Servizi, sul totale ricevute, come indicato nei paragrafi 6.2.2 e 8.1	Entro il 4% delle chiamate telefoniche	Mensile	0,1‰ del valore complessivo del Contratto per ogni 1% sopra al valore di soglia
IQTS – Tempo Smistamento: Tempo che intercorre tra la richiesta e lo smistamento a strutture di ditte terze	Entro 5’ nel 90% delle richieste	Mensile	0,1‰ del valore complessivo del Contratto per ogni 1% sotto al valore di soglia

10.4 Profili professionali e schema per la presentazione dei CV

Le figure professionali onsite richieste per lo svolgimento dei servizi indicati nei paragrafi precedenti dovranno rispettare i profili di seguito descritti. Si precisa che la cultura equivalente può corrispondere, indicativamente, a 4 anni di esperienza lavorativa addizionale in ambito informatico.

L’Amministrazione potrà richiedere, anche in corso di esecuzione del contratto, competenze specifiche in relazione ad ulteriori tematiche, prodotti, sistemi e metodologie.

I curricula vitae del personale da impiegare nei vari servizi dovranno essere resi disponibili alla Committente secondo quanto previsto dal capitolato e dal contratto, rispettando il template riportato alla fine del paragrafo.

10.4.1 Sistemista senior

I profili professionali indicati nella tabella seguente devono essere presenti nel complesso delle risorse professionali richieste al fornitore per il supporto specialistico alla conduzione operativa.

Titolo di studio	Laurea in discipline tecniche o cultura equivalente
Anzianità lavorativa	Minimo 7 anni di cui almeno 4 nella funzione

Esperienze consolidate	• Interazione e relazione con gli utenti • Gestione delle interazioni, riguardo alle competenze ed alle responsabilità del settore di competenza nei confronti degli ambiti applicativi, di rete e sistemistici • Problem determination e problem solving • Redazione e controllo di procedure, di specifiche tecniche, di manuali operativi e di rapporti statistici sui servizi • Stima delle risorse per l'erogazione dei servizi e per la realizzazione di attività progettuali • Tecniche di gestione progetti • Elaborazione e redazione di specifiche di progetto e di studi di fattibilità • Conoscenze di best practices ITIL • Tecniche di progettazione e dimensionamento di architetture hardware/software • Tecniche di pianificazione • Tecniche e strumenti di monitoraggio • Tecniche di analisi del rischio • Controllo della qualità del servizio • Controllo dello stato di avanzamento delle attività • Progettazione test integrati
Ambiti	
Conoscenze in ambito system architecture	• Disegno di architetture tecnologiche complesse (multivendor); • Attività di dimensionamento sistemi e capacity planning; • Conoscenza delle principali tendenze evolutive delle architetture tecnologiche per sistemi enterprise; • Conoscenze approfondita e integrata degli elementi tecnologici che costituiscono un sistema complesso; • Metodologia per l'analisi, il disegno e la revisione dell'IT Service Management; • Analisi delle necessità di impianto delle applicazioni in ambienti complessi.
Conoscenze approfondite in ambito System Administration	• Amministrazione e gestione Sistemi Operativi, installazione, configurazione, personalizzazione/tuning e gestione dei principali sistemi operativi di tipo Open Source (distribuzioni di **Linux** quali Centos, Oracle Linux, SUSE, Red Hat, Mandrake, Debian, ecc) e **Microsoft**, anche in configurazione cluster; • Amministrazione e gestione dell'infrastruttura Active Directory e DNS • Personalizzazione di file di sistema (es. password, group, hosts)

	• Gestione delle procedure di startup e shutdown; • Attività di tuning applicativo e ottimizzazione con l'uso di strumenti per il test di carico.
Conoscenze in ambito Database	• Database administration (Oracle Db, Sql server, mysql, postgress sql, ecc.) • Configurazioni dei database in Alta Affidabilità/Disponibilità utilizzando tecnologie standard (DataGuard per Oracle, DataReplication per MySql, etc.); • Ottimizzazione delle strutture dati.
Conoscenze in ambito prodotti middleware	• Application Server administration (Apache Tomcat, RedHat Jboss,Microsoft IIS, ecc..); • Amministrazione dei prodotti per portali applicativi (Zend, OpenCMS, WordPressr, Drupal, Joomla, ecc.) • Applicazioni enterprise conformi agli standard Java 2 Platform Enterprise Edition ed in particolare dei componenti Enterprise JavaBeans, servlet e JavaServer Pages.
Conoscenze approfondite nell'ambito delle tecnologie di virtualizzazione	• Installazione, configurazione, personalizzazione/tuning e gestione delle tecnologie di virtualizzazione (**VMWare**, Oracle VM Server) in ambienti complessi con storage su SAN e vSAN • Installazione e gestione di ambienti virtualizzati tramite container (Docker, Kubernetes) • Disegno e implementazione di server, storage e modalità di backup e restore • Supporto di ambienti enterprise.
Conoscenze approfondite in ambito networking	• Amministrazione Sistemi operativi degli apparati di rete con particolare riferimento a tecnologia **Brocade**. • Tecniche di bilanciamento del traffico con particolare riferimento ai Brocade ADX • Tecniche di ridondanza ed alta affidabilità • Disegno e progettazione di reti TCP/IP complesse • Implementazione di infrastrutture gestionali per reti complesse • Protocolli di rete (Ethernet, FCoE, FDDI, ATM, ecc.) • Protocolli di routing (IGRP, OSPF, ecc.) • Standard per cablaggio strutturato (ISO/IEC 11801, EN 50173) • Apparati di rete (switch, bridge, router, ecc.) • Sistemi di network management • Sicurezza delle reti.
Conoscenze approfondite in	• Amministrazione sistemi operativi degli apparati di sicurezza quali Firewall, terminatori VPN, sistemi di autenticazione forte, ecc., con

ambito sicurezza	particolare riferimento a tecnologia **Fortinet**. • Protocolli applicativi di base quali HTTP, HTTPS, SMTP, POP3, IMAP, SSH, telnet, ecc. • Principali vulnerabilità/tipi di attacchi di rete e dei sistemi • Tecniche di ridondanza ed alta affidabilità • Amministrazione ISS Intrusion Detection/Prevention, SSL Gateways • Amministrazione sistemi Antivirus; • Analisi di problematiche complesse ed individuazione del componente in errore • Comprovata esperienza nella definizione e progettazione di architetture di sicurezza • Approfondita conoscenza dei principali standard di sicurezza (ITSEC, BS7799) • Conduzione di assessment di sicurezza logica, fisica e organizzativa.
Conoscenze in ambito Operation Management	• Installazione, configurazione, customizzazione, tuning e troubleshooting degli strumenti di system monitoring, application performance monitoring, workload automation, prodotti di analisi log
Conoscenze in ambito Service Management	• Installazione, configurazione, customizzazione, tuning e troubleshooting dei prodotti di IT Service Management • Controllo dei Processi IT e delle relative procedure operative

Le risorse specialistiche “Sistemisti Senior” devono essere dotate, non solo delle competenze tecnologiche ed organizzative adeguate alle attività da svolgere, ma possedere anche un’approfondita conoscenza ed esperienza del contesto organizzativo e dei prodotti tecnologici in uso presso l’Ente.

Devono possedere globalmente le certificazioni attinenti alle tecnologie utilizzate dall’Amministrazione (VMware, Linux, Fortinet e Brocade) ed all’interno del relativo percorso di certificazione.

Costituirà elemento preferenziale le esperienze lavorative documentate in contesti simili a quello di Regione Campania.

Nel caso in cui, in corso di esecuzione, il Fornitore debba provvedere alla sostituzione di una risorsa certificata, detta sostituzione dovrà avvenire per il tramite di una nuova risorsa che possegga le medesime certificazioni ed esperienze possedute dalla risorsa da sostituire.

10.4.2 Sistemista

Nell'ambito del supporto specialistico – assistenza onsite (AOS), il responsabile dell'Help Desk deve avere il profilo professionale indicato nella seguente tabella:

Titolo di studio	Laurea in discipline tecniche o diploma di perito informatico o cultura equivalente
Anzianità lavorativa	Minimo 4 anni nella funzione
Esperienze consolidate	• Interazione e relazione con gli utenti • Gestione delle interazioni, riguardo alle competenze ed alle responsabilità del settore di competenza nei confronti degli ambiti applicativi, di rete e sistemistici • Problem determination e problem solving • Supporto alla redazione e controllo di procedure, di specifiche tecniche, di manuali operativi e di rapporti statistici sui servizi; • Supporto all'elaborazione ed alla redazione di specifiche di progetto e di studi di fattibilità; • Metodologie di project management e di best practices ITIL; • Tecniche di progettazione e dimensionamento di architetture hardware/software; • Tecniche di pianificazione; • Tecniche e strumenti di monitoraggio; • Tecniche di analisi del rischio; • Controllo della qualità del servizio; • Controllo dello stato di avanzamento della attività; • Progettazione test integrati;
Conoscenze in ambito System Administration e Mail Server per S.O. Microsoft	• Amministrazione e gestione Sistemi Operativi, installazione, configurazione, personalizzazione/tuning e gestione dei sistemi operativi Microsoft • Amministrazione e gestione dei server Microsoft Exchange, dell'infrastruttura Active Directory e DNS • Gestione delle procedure di startup e shutdown; • Attività di tuning applicativo e ottimizzazione con l'uso di strumenti per il test di carico.
Conoscenze base nell'ambito delle tecnologie di virtualizzazione	• Installazione, configurazione, personalizzazione/tuning e gestione delle tecnologie di virtualizzazione (VMWare, Oracle VM Server) in ambienti complessi con storage su SAN • Supporto di ambienti enterprise.

Conoscenze base in ambito sicurezza	• Protocolli applicativi di base quali HTTP, HTTPS, SMTP, POP3, IMAP, SSH, telnet, ecc. • Principali vulnerabilità/tipi di attacchi di rete e dei sistemi • Tecniche di ridondanza ed alta affidabilità • Amministrazione sistemi Antivirus; • Analisi di problematiche complesse ed individuazione del componente in errore • Approfondita conoscenza dei principali standard di sicurezza (ITSEC, BS7799) • Conduzione di assessment di sicurezza logica, fisica e organizzativa.
Conoscenze base in ambito Operation Management	• Installazione, configurazione, customizzazione, tuning e troubleshooting degli strumenti di system monitoring, application performance monitoring, workload automation, prodotti di analisi log
Conoscenze in approfondite in ambito Service Management	• Installazione, configurazione, customizzazione, tuning e troubleshooting dei prodotti di IT Service Management • Controllo dei Processi IT e delle relative procedure operative

Conoscenze approfondite in ambito Client	• Architetture dei sistemi client Microsoft e Linux
	• principali prodotti di software distribution e di remote desktop control
	• sistemi operativi client e dispositivi mobili (es. Windows, Apple, Android)
	• principali prodotti software di informatica individuale, ad es.:
	  ○ suite MS Office, MS SharePoint, ecc.
	  ○ web browser (es. Internet Explorer, Firefox, Chrome, Safari)
	  ○ antivirus (es. sophos, ecc.)
	  ○ Sistemi di virtualizzazione (es. Citrix)

La risorsa specialistica “Sistemista” deve essere dotata, non solo delle competenze tecnologiche ed organizzative adeguate alle attività da svolgere, ma possedere anche un’approfondita conoscenza ed esperienza del contesto organizzativo e dei prodotti tecnologici in uso presso l’Ente.

Deve essere in possesso di certificazioni in ambito dei processi di Service Management (ITIL, etc.) ed all’interno del relativo percorso di certificazioni.

Costituirà elemento preferenziale le esperienze lavorative documentate in contesti simili a quello di Regione Campania.

Nel caso in cui, in corso di esecuzione, il Fornitore debba provvedere alla sua sostituzione detta sostituzione dovrà avvenire per il tramite di una nuova risorsa che possegga le medesime certificazioni ed esperienze possedute dalla risorsa da sostituire.

10.4.3 Sistemista junior

Nell'ambito del supporto specialistico – assistenza onsite (AOS), ogni risorsa deve avere il profilo professionale indicato nella seguente tabella:

Titolo di studio	Diploma in perito informatico o cultura equivalente
Anzianità lavorativa	Minimo 2 anni nella funzione
Esperienze consolidate	• Interazione e relazione con gli utenti • Gestione delle interazioni, riguardo alle competenze ed alle responsabilità del settore di competenza nei confronti degli ambiti applicativi, di rete e sistemistici • Problem determination e problem solving • Supporto alla redazione e controllo di procedure, di specifiche tecniche, di manuali operativi e di rapporti statistici sui servizi;
Conoscenze base in ambito network e sicurezza	Competenza ed esperienza di base in gestione (es. installazione, upgrading, applicazione di patch, configurazione, back-up, test, tuning, monitoraggio) e analisi e risoluzione malfunzionamenti relativamente a: • reti locali Ethernet • architettura di rete TCP/IP • standard per cablaggio strutturato • apparati (hardware e software di base) relativi ai sistemi tecnologici semplici installati presso le sedi periferiche (UPS, Access Point, Patch Panel, Patch Cord, etc. • architettura client/server e web • Protocolli applicativi di base quali HTTP, HTTPS, SMTP, POP3, IMAP, SSH, telnet, ecc. • Principali vulnerabilità/tipi di attacchi di rete e dei sistemi • sistemi antimalware, antispam, intrusion prevention/detection, url filtering
Conoscenze approfondite in ambito Client	Competenza ed esperienza approfondita in gestione (es. installazione, upgrading, applicazioni di patch, configurazione, back-up, test, tuning, monitoraggio) e analisi e risoluzione malfunzionamenti relativamente a:

	• Architetture dei sistemi client Microsoft e Linux
	• Utilities (es. gestione batteria, power management, processore, display e camera)
	• hardware di personal computer e periferiche
	• principali prodotti di software distribution, di remote desktop control e service desk
	• sistemi operativi client e dispositivi mobili (es. Windows, Apple, Android)
	• Software per la gestione degli asset (es. OCS Inventory)
	• principali prodotti software di informatica individuale, ad es.:
	  ○ suite MS Office, MS Teams, MS SharePoint, ecc.
	  ○ web browser (es. Internet Explorer, Firefox, Chrome, Safari)
	  ○ antivirus (es. sophos, ecc.)
	  ○ Sistemi di virtualizzazione desktop (es. XenApp, XenDesktop)

10.4.4 Schema per la presentazione dei curricula

Di seguito viene presentato lo schema che il fornitore dovrà utilizzare per la compilazione dei curricula vitae.

Si sottolinea che nella redazione dei contenuti dovranno essere privilegiati gli aspetti di interesse per la fornitura e che, orientativamente, il documento non dovrà superare le 3 pagine.

<table>
<tr><td>Nominativo</td><td colspan="4">(Inserire il Cognome e il Nome della risorsa)</td></tr>
<tr><td>Ruolo</td><td colspan="4">(Inserire il Ruolo attualmente ricoperto dalla risorsa)</td></tr>
<tr><td>Figura professionale</td><td colspan="4">(Indicazione del ruolo assegnato alla risorsa in funzione delle figure professionali richieste nel capitolato tecnico - nonché eventuali specifici ruoli aggiuntivi indicati in Offerta)</td></tr>
<tr><td>Servizio/attività</td><td colspan="4">(Fornire l'indicazione del servizio/attività per cui viene proposta la risorsa in relazione agli ambiti definiti nel Capitolato o ad eventuali aspetti caratterizzanti l'Offerta tecnica)</td></tr>
<tr><td>Conoscenze</td><td colspan="4">(Fornire una breve descrizione del profilo professionale in termini di conoscenze/competenze e di aree chiave in cui la risorsa ha maturato esperienze significative)</td></tr>
<tr><td rowspan="11">Principali Esperienze Lavorative</td><td colspan="4">(Indicare le esperienze più significative per la gara in oggetto e comprovanti le competenze richieste nel Capitolato Tecnico, a partire dalla più recente, fornendo una breve descrizione delle attività svolte, del ruolo ricoperto, della durata del progetto. E' necessario suddividere le esperienze per anno e per settore (Es: Pubblica Amministrazione, Bancario, Telecomunicazioni)</td></tr>
<tr><td>Settore</td><td colspan="2">Data inizio-Data fine</td><td>Esperienze</td></tr>
<tr><td rowspan="3"></td><td colspan="2"></td><td></td></tr>
<tr><td colspan="2"></td><td></td></tr>
<tr><td colspan="2"></td><td></td></tr>
<tr><td rowspan="3"></td><td colspan="2"></td><td></td></tr>
<tr><td colspan="2"></td><td></td></tr>
<tr><td colspan="2"></td><td></td></tr>
<tr><td rowspan="3"></td><td colspan="2"></td><td></td></tr>
<tr><td colspan="2"></td><td></td></tr>
<tr><td colspan="2"></td><td></td></tr>
<tr><td>Competenze Tecniche</td><td colspan="4">(Indicare le competenze specifiche di cui si è in possesso)</td></tr>
<tr><td></td><td colspan="4"></td></tr>
<tr><td rowspan="4">Specializzazioni</td><td colspan="4">(Indicare eventuali specializzazioni, master, ecc.)</td></tr>
<tr><td>Anno</td><td colspan="2">Titolo</td><td>Descrizione</td></tr>
<tr><td></td><td colspan="2"></td><td></td></tr>
<tr><td></td><td colspan="2"></td><td></td></tr>
<tr><td>Certificazioni</td><td colspan="4">(Indicare eventuali certificazioni)</td></tr>
</table>

	Anno	Titolo	Descrizione
Istruzione	*(indicare i titoli di studio)*		
Lingue	*Per ogni lingua straniera, indicare il grado di conoscenza, dove:* *1 -in grado di leggere* *2 - in grado di leggere e scrivere* *3 - in grado di leggere, parlare e scrivere in maniera più che comprensibile* *4 - fluente sia nello scritto che nell'orale* *5 - madrelingua - (native language)*		
	Lingue		Grado di conoscenza
Principali pubblicazioni	*(indicare le principali pubblicazioni)*		