DIREZIONE GENERALE PER L'UNIVERSITA',

LA RICERCA E L'INNOVAZIONE

APPALTO SPECIFICO

RELATIVO ALL'ACCORDO QUADRO PER LA PRESTAZIONE DI SERVIZI DI SYSTEM MANAGEMENT PER LE PUBBLICHE AMMINISTRAZIONI

CAPITOLATO TECNICO

Indice generale

1. Premessa

Il presente Capitolato Tecnico disciplina gli aspetti tecnici dell'Appalto Specifico relativo all'Accordo Quadro relativo per la fornitura di servizi di System Management per le Pubbliche Amministrazioni.

Nel corpo del presente Capitolato Tecnico, con il termine:

"AQ" si intende l'Accordo Quadro a cui il Capitolato tecnico si riferisce;

"AS" si intende l'Appalto Specifico basato sull'Accordo Quadro a cui il Capitolato tecnico si riferisce;

"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;

"Amministrazione" si intende la Giunta Regionale della Campania;

"Servizi base" si intende l'insieme dei servizi, analiticamente descritti nel Capitolo 5 dell'AQ;

"Servizi accessori": si intende l'insieme dei servizi, analiticamente descritti nel Capitolo 6 dell'AQ;

2. Contesto

La Giunta Regionale della Campania ha la necessità di gestire e mantenere in perfetta efficienza tutta l'infrastruttura di rete, gli impianti, i beni hardware ed i sistemi (fisici e virtuali) per i servizi ICT in uso presso le strutture della Regione stessa o offerti dall'Ente, nonché, di implementare tutti quegli interventi di aggiornamento dell'infrastruttura ritenuti necessari sia per aspetti di sicurezza che di evoluzione tecnologica

Il presente paragrafo, quindi, ha lo scopo di definire le attività, l'ambito tecnologico, le sedi e le risorse hardware, per le quali l'Amministrazione chiede la fornitura di Servizi di gestione, Manutenzione e Supporto Specialistico Continuo, così come previsti nel AQ.

2.1. Infrastruttura tecnologica oggetto dei servizi richiesti

L'infrastruttura IT della Giunta Regionale della Campania è configurata per offrire servizi in alta disponibilità. E' articolata su tre siti, due che hanno la potenzialità di essere interscambiabili nell'erogazione dei servizi e un terzo, detto di quorum, utile al funzionamento dei meccanismi di replica

I due siti principali (Napoli e Salerno) sono collegati attraverso due circuiti a 10 Gbps, mentre il Quorum (Benevento) è collegato ai due precedenti attraverso link geografici in tecnologia MPLS.

La soluzione adottata per la Continuità Operativa e per il Disaster Recovery consiste nell'utilizzo di tecnologie abilitanti alla configurazione di un "cluster geografico".

In sintesi la soluzione di alta disponibilità adotta questi componenti:

- Meccanismi di HA, Vmotion, DRS per le macchine virtuali ;
- Meccanismi di virtualizzazione in ambiente Oracle (OVM);
- Meccanismi di bilianciamento (ADX Brocade);
- Funzioni storage attivo-attivo (GAD Hitachi);
- Servizi di backup;
- Resilienza di rete (networking);
- Sistemi di monitoraggio;
- Protezioni specifiche a livello database (Dataguard per piattaforma Oracle e Active-Standby per Mysql e Postgres e SQL Server);
- Cluster per Exchange;

Solitamente le VM sono ospitate nel Nodo Principale (Napoli) e, secondo le policy implementate a livello vSphere-vCenter, sono candidate a migrare sul Nodo Secondario attraverso i meccanismi di HA, DRS e vMotion.

L'infrastruttura di rete per entrambi i Data Center 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, presso entrambi i siti 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 tutti gli apparati di bilanciamento di carico L4-L7. In particolare, in ogni sede è installato un Application Delivery Controller (ADC) Brocade ADX 1000, a realizzare una soluzione di clusterizzazione/HA geografica.

L'architettura di Sicurezza prevede l'utilizzo di due coppie di Firewall FortiGate, all'interno dei quali sono stati creati dei VDOM, ossia dei Firewall virtuali, in tutto e per tutto assimilabili alle loro controparti reali. La soluzione si basa su un'architettura in cui è presente un doppio livello di Firewall così organizzato:

- Cluster FortiGate 1000C: 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 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.

Ogni coppia rappresenta, di fatto, un singolo Firewall configurato in modalità Active-Standby. Il nodo attivo è responsabile della gestione di tutto il traffico, mentre quello passivo è situato geograficamente in un sito diverso ed è pronto ad attivarsi in caso di malfunzionamento dell'altro nodo. Il meccanismo di Alta Affidabilità è implementato tramite il protocollo VRRP

Completano l'infrastruttura di sicurezza due appliance McAfee Network Security NS 7200, specializzate per l'analisi del traffico, e tecnologia Sophos come soluzione antivirus ed antispam.

La SAN è implementata tramite storage Hitachi VSPG1000 con Globale-Active-Device (GAD) in configurazione VMware vSphere Metro Storage Cluster. La soluzione cluster dei sistemi Hitachi è basata su replica sincrona tra i siti, creando così un unico volume logico presente e accessibile da siti geograficamente distribuiti. Questo design permette un'elevata disponibilità dei servizi, consentendo la migrazione delle macchine virtuali tra i siti senza tempi di inattività. In ogni nodo sono inoltre installati 2 swtich Brocade 7840 per la conversione tra protocollo FC e IP

La soluzione di Backup, ASG Time Navigator, sul sito primario è composta da:

- n.1 macchina "Time Navigator", per la gestione dei backup tramite l'utilizzo di un DB proprietario;
- n.1 macchina con la funzione di deduplica (HSS) per il salvataggio delle macchine virtuale;
- n.1 macchina con la funzione di deduplica (HSS) per il salvataggio, tramite agent, degli applicativi specifici (Ms-Sql, Exchange, Oracle, MySql, PostgreSQL, Filesystem, etc…);
- n.1 Storage Hitachi HUS110 con 100TB utili per il backup.

Analogamente, ulteriori 3 macchine e un HUS110 sono installati anche nel sito secondario, al fine di poter replicare i dati salvati (repliche tra i due HSS via LAN) ed avere una console di riserva in caso di disastro.

La Giunta Regionale della Campania ha circa 100 sedi, distribuite su tutto il territorio regionale ed una sede a Roma, collegate in MPLS ad entrambi i nodi (Napoli e Salerno). All'interno di ciascuna sede sono presenti reti locali con cablaggi strutturati in fibra ottica e/o in rame, eventualmente articolate in più sottoreti sulle quali sono attestate le circa 5000 postazioni client del personale dell'Amministrazione. Nelle sedi più importanti è presente anche un'infrastruttura WiFi e una rete VOIP parallela.

Di seguito si riporta un elenco dettagliato degli apparati installati presso ogni sito/sede.

Sito Napoli

- n.2 switch di core Brocade ICX7750;
- n.2 firewall Fortinet 1000C
- n.2 firewall Fortinet 1500D
- n.1 IPS McAfee Network Security Platform
- n.1 appliance Sophos Anti spam
- n.1 bilanciatore Brocade ADX1216;
- n.8 switch Brocade VDX6740;
- n.4 switch ICX6430, per il monitoraggio out-of-band della rete;
- n.2 switch FC Brocade 6510;
- n.1 extension switch Brocade 7840;
- n.1 storage Hitachi Virtual Storage Platform G1000 (VSP G1000) con 350 TB utili
- n.82 blade server Dell PowerEdge M610 per jun totale di 660 processori
- n.1 server rackmount Hitachi CR220H
- n.1 Storage Array HUS110 (Backup) con circa 100 TB utili
- n.1 NAS DellEMC Isilon X210 con 200 TB utili

Sito Salerno

- n.2 switch di core Brocade ICX7750;
- n.1 firewall Fortinet 1000C
- n.1 firewall Fortinet 1500D
- n.1 IPS McAfee Network Security Platform
- n.1 appliance Sophos Anti spam
- n.1 bilanciatore Brocade ADX1216;
- n.2 switch Brocade VDX6740;
- n.1 extension switch Brocade 7840;
- n.3 switch ICX6430, per il monitoraggio out-of-band della rete;
- n.2 switch FC Brocade 6510;
- n.1 storage Hitachi Virtual Storage Platform G1000 (VSP G1000) con 350 TB utili
- n.24 blade server Hitachi 500, per un totale di 500 processori.
- n.1 server rackmount Hitachi CR220H
- n.1 Storage Array HUS110 (Backup)
- n.1 NAS DellEMC Isilon X210 con 200 TB utili

Le apparecchiature sopra elencate sono installate all'interno del container presso l'Università di Salerno a Fisciano.

Sito Benevento.

- n.2 Switch Brocade 6505: switch Fibre Channel per l'accesso allo storage
- n 1. extension Brocade 7840: apparato che esegue la conversione tra protocollo FC e IP
- n 1. Switch Brocade 6430: switch di Management
- n.1 server rackmount Hitachi CR220H
- n.1 Storage Array HUS110 (Quorum)

Questo sito svolge le funzioni di "Quorum" ed ospita anche alcune macchine virtuali realizzate con tecnologia Oracle VM

Tutte le Sedi

- n.350 Apparati CISCO (switch / access point)
- n.5300 (PDL Regione + PDL CPI + notebook)

Mentre, le principali tecnologie software utilizzate in ambiente di produzione, senza considerare ambienti di test, collaudo o sperimentazione, sono:

Sistemi Operativi Server

- n.160 Microsoft Windows Server nelle varie release

- n.300 Sistemi Linux (95% CentOs nelle varie release)

Software di virtualizzazione

- n.1 VMware vCenter Server 6.5
- n.89 lame VMware ESXI 6.0
- n.4 lame Oracle VM Server

Database Management Systems

- n.20 Oracle
- n.25 PostgreSQL
- n.80 Mysql/MariaDB
- n.20 MS SQL Server

Storage Management

- n.2 Hitachi Storage Command Suite
- n.2 DellEMC Isilon X210

Backup & recovery

- n.2 ASG Time Navigator

Application, Integration, Middleware Software, Web Server e CMS

- Microsoft IIS
- Apache Http Server
- Microsoft.NET
- Apache Tomcat
- RedHat Jboss
- WSO2
- WordPress
- Drupal
- OpenCMS
- Joomla

Sistemi di monitoraggio e analisi delle performance

- SiteScan (DCIM) per gli impianti
- Zabbix per gli apparati (Storage, Switch, Router, SAN) e per i servizi (macchine virtuali database, applicazioni),
- CA E-Health per l'analisi delle performance della rete

Strumenti di gestione

- CA Spectrum, la suite di prodotti per le attività di network management
- CA Service Desk Manager (CA SDM), suite di prodotti per la gestione degli asset, trouble ticket (preesistente)
- GLPI versione open per la gestione degli asset, trouble ticket (candidati a subentrare a CA SDM)

Le tecnologie sopra riportate possono cambiare in numero e tipologia a fronte di specifiche esigenze dell'Amministrazione stesse o per le naturali evoluzioni dei sistemi ICT.

2.2. Elenco sedi regionali collegate ed oggetto dei servizi richiesti

Di seguito l'elenco delle sedi regionali, principali e secondarie, collegate in MPLS ai due nodi ed il numero orientativo di PDL in ogni sede.

Solo per le sedi principali è previsto un presidio locale come indicato in tabella.

Sedi principali	Num. PDL	Presenza in sede
NAPOLI - SANTA LUCIA	589	2
NAPOLI - DON BOSCO	157	5
NAPOLI - ISOLA A6	691	2
NAPOLI - ISOLA C3	492	1
NAPOLI - ISOLA C5	237	
NAPOLI - DE GASPERI 28	261	1
NAPOLI - VIA MARINA	252	
NAPOLI - METASTASIO	187	1
CASERTA - SAN NICOLA LA STRADA	215	1
CASERTA - VIA CESARE BATTISTI	73	
SALERNO VIA CLARK	212	2
SALERNO VIA PORTO	200	
AVELLINO - COLLINA LIGUORINI	256	2
AVELLINO - VIA ROMA	78	
BENEVENTO - PZZA SANTA COLOMBA	165	1
BENEVENTO - ARCO TRAIANO	89	
TOTALE	**4154**	**16**

Sedi secondarie	Num. PDL	Presenza in sede
AVELLINO - SANT'ANGELO DEI LOMBARDI	35	
AVELLINO - ARIANO IRPINO	28	
AVELLINO - CALITRI	8	
AVELLINO - MERCOGLIANO	15	
AVELLINO - MIRABELLA ECLANO	11	
AVELLINO - MONTELLA	7	

SALERNO - BATTIPAGLIA VIA ADRIATICO	7	
BENEVENTO - AIROLA	5	
BENEVENTO - COLLE SANNITA	1	
BENEVENTO - S. BARTOLOMEO IN GALDO	1	
BENEVENTO - SAN MARCO DEI CAVOTI	3	
BENEVENTO - TELESE TERME	12	
BENEVENTO - VIA MELLUSI	7	
BENEVENTO - VIA NICOLA DA MONTEFORTE	4	
BENEVENTO - VIA TORRETTA	12	
CASERTA - ALIFE	18	
CASERTA - AVERSA	7	
CASERTA - CARINOLA	21	
CASERTA - CASALUCE	7	
CASERTA - CELLOLE	2	
CASERTA - DRAGONI	8	
CASERTA - SMCV VIA CASERTA	19	
CASERTA - SMCV VIA NAZIONALE APPIA	3	
CASERTA - VAIRANO PATENORA	13	
CASERTA - VIALE ELLITTICO	2	
SALERNO CAVA DEI TIRRENI GiovanniXXIII	6	
SALERNO CONTURSI TERME	9	
NAPOLI - COMOLA RICCI	10	
NAPOLI - VARCO S.ERASMO	1	
NAPOLI - VIA ARENELLA	26	
NAPOLI - VIA BRACCO	19	
NAPOLI - VIA PIGNA	9	
SALERNO - NOCERA INFERIORE VIA SOLIMENA	12	
NAPOLI - NOLA	13	
SALERNO - PADULA	3	
NAPOLI - POZZUOLI	2	
SALERNO - ROCCADASPIDE - VIA GIULIANI	8	
ROMA - VIA POLI	15	
SALERNO SALA CONSILINA - BARCA	11	
SALERNO VIA ABELLA SALERNITANA	25	
SALERNO VIA DEI CARRARI	8	
SALERNO VIA NIZZA	16	
SALERNO - SANTA MARINA - POLICASTRO	9	
SALERNO - SAPRI	1	
SALERNO - TEGGIANO	5	
NAPOLI - TORRE DEL GRECO - BATTISTI	5	
NAPOLI - TORRE DEL GRECO - GIOVANNI XXIII	12	
SALERNO - VALLO DELLA LUCANIA - MAINENTE	5	

SALERNO - VALLO DELLA LUCANIA - NICODEMO	5	
SALERNO - VALLO DELLA LUCANIA - RUBINO	9	
TOTALE	**500**	**0**

Infine, nella seguente tabella sono elencate le sedi relative ai centri per l'impiego passati dalla Provincia alla Regione che contano circa 500 PDL.

n.	Provincia	CPI/RECAPITO/Provincia	Indirizzo Sede
1	Avellino	AVELLINO	Via Salvatore Pescatori 91/93
2	Avellino	ARIANO IRPINO	Via Serra,5
3	Avellino	CALITRI	Contrada Sanbuco,snc
4	Avellino	GROTTAMINARDA	Via Bellini,snc
5	Avellino	S. ANGELO DEI LOMBARDI	Via Boschetto,1
6	Benevento	BENEVENTO	VIA XXV LUGLIO, 14
7	Benevento	SANT'AGATA DE GOTI	VIA STARZA-PANORAMICA, 3 - SANT'AGATA DE'GOTI
8	Benevento	SAN BARTOLOMEO IN GALDO	VIA PER CASTELVETERE DI VALFORTORE
9	Benevento	TELESE TERME	VIA ELSA MORANTE,5
10	Caserta	AVERSA	Via Pommella, 28/30/32
11	Caserta	CAPUA	Piazza De Renzis, 8 (Angolo via E. Fieramosca)
12	Caserta	CASAL DI PRINCIPE	Via P.P.Pasolini, 8/10
13	Caserta	CASERTA	Via Santa Chiara, 42 - Complesso Regency (1° e 2° piano)
14	Caserta	MADDALONI	Via Matilde Serao, 245
15	Caserta	PIEDIMONTE MATESE	Via sannitica
16	Caserta	SESSA AURUNCA	Via Sant'Agata, 10
17	Caserta	TEANO	Via Orto Saetta
18	Napoli	NAPOLI - RAIMONDI	VIA PIETRO RAIMONDI, 16/18
19	Napoli	NAPOLI - FUORIGROTTA	Via Diocleziano 330, Napoli
20	Napoli	NAPOLI - SCAMPIA	Viale della Resistenza
21	Napoli	AFRAGOLA	VIA PO N°10 - CASORIA
22	Napoli	CASTELLAMMARE	Via Regina Margherita n° 72 Castellammare di Stabia

23	Napoli	FRATTAMAGGIORE	VIA GENOINO 69
24	Napoli	GIUGLIANO IN CAMPANIA	VIA DEGLI INNAMORATI 113 - GIUGLIANO
25	Napoli	ISCHIA	VIA PRINCIPESSA MARGHERITA N. 33 CASAMICCIOLA
26	Napoli	MARIGLIANO	Via Pontecitra n. 56 Marigliano
27	Napoli	NOLA	VIA DELLA REPUBBLICA 24
28	Napoli	OTTAVIANO	VIA GABRIELE D'ANNUNZIO 131
29	Napoli	POMIGLIANO D'ARCO	VIA PASSARIELLO, 109 - P.co REA - POMIGLIANO D'ARCO
30	Napoli	POMPEI	Viale Mazzini. 104
31	Napoli	PORTICI	VIA SALUTE, 45 - PORTICI -
32	Napoli	POZZUOLI	VIA VIRGILIO, 8 POZZUOLI
33	Napoli	SORRENTO	via S. Francesco, 8 - Sorrento
34	Napoli	TORRE DEL GRECO	VIA CUPA SAN PIETRO 11
35	Salerno	AGROPOLI	viale Lazio snc - Agropoli
36	Salerno	BATTIPAGLIA	VIA MONCHARMONT
37	Salerno	MAIORI	Via Reginna, 71
38	Salerno	MERCATO SAN SEVERINO	VIA DEI DUE PRINCIPATI, 49/1 Mercato San Severino
39	Salerno	NOCERA INFERIORE	Via Cucci, 24 Nocera Inferiore
40	Salerno	OLIVETO CITRA	Via Alcide de Gasperi, 31 - OLIVETO CITRA (SA)
41	Salerno	ROCCADASPIDE	Piazzetta Mercato snc - Roccadaspide
42	Salerno	SALA CONSILINA	Via Matteotti 100, SALA CONSILINA SA)
43	Salerno	SALERNO	VIA PRINCIPESSA SIGHELGAITA 76/B
44	Salerno	SAPRI	Via Flavio Gioia, snc
45	Salerno	SCAFATI	Via Terze, Parco Giugliano
46	Salerno	VALLO DELLA LUCANIA	Via Stefano Passero, 2 Vallo della Lucania

Tutte le sedi sopra elencate possono variare in numero e località in base alle esigenze dell'Ente.

2.3. Attività minime necessarie per la gestione e manutenzione dei sistemi, reti e sicurezza logica

La gestione dell'infrastruttura tecnologica di Giunta Regionale della Campania comprende attività di:

2.3.1. Sviluppo, Integrazione, Gestione e Manutenzione dei sistemi server e infrastrutture

- Disegno e 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;
- Presa in carico e dismissione dei server/piattaforme applicative;
- Gestione sistemistica di piattaforme applicative (aggiornamento software di base/middleware, backup dati e log, monitoraggio, etc.) e dei relativi Database;
- 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.);
- Gestione servizi infrastrutturali (Active Directory, Exchange, DNS, File Server, etc);
- Gestione accessi amministrativi secondo normativa vigente e gestione dei contratti di manutenzione dei sistemi;
- Approvazione e distribuzione degli aggiornamenti critici e delle configurazioni per la protezione dei sistemi;
- Gestione delle misure di sicurezza sui server in accordo con le norme contenute nel DPS/GDPR/ AGID, compresa la creazione di policy di logging e la raccolta, archiviazione e analisi del log;
- 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 giornale degli interventi;

2.3.2. Configurazione, Gestione e Controllo dei sottosistemi di Storage e Backup

- Gestione e Monitoraggio dei sottosistemi SAN/NAS e configurazione degli apparati di collegamento (LUN zoning e LUN mapping, etc.);
- Configurazione e manutenzione ambienti di backup;
- Definizione e configurazione policy di Backup di dati, log e sistemi in accordo a esigenze e normative vigenti;

- Laboratorio per il Backup/Recovery;
- 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;

2.3.3. Configurazione, Gestione e Manutenzione Servizio di Continuità Operativa

- Verifica e aggiornamento del Piano di Continuità;
- Test periodico della soluzione di continuità;
- Attività finalizzate a garantire la continua erogazione dei servizi tramite allineamento delle configurazioni tra i due siti;
- Attività finalizzate a garantire l'alta disponibilità dei dati (mirroring sincrono/asincrono, immagine logica, immagine fisica);
- Configurazione di sistemi nuovi/esistenti in continuità;
- Adeguamento delle soluzioni di continuità ai cambiamenti ed aggiornamento documentazione;
- Gestione straordinaria in casi di eventi disastrosi/incidenti;
- Rientro nelle condizioni di normalità;

2.3.4. Configurazione e Gestione delle Base di dati in Alta Disponibilità

- 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;
- Migrazione tra le diverse piattaforme di virtualizzazione;
- Attività di start up e shut down di un’istanza e/o di un database;
- Gestione degli utenti, profili e ruoli;
- 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 le attività di backup/restore;
- Monitoraggio e ottimizzazione delle prestazioni;
- Gestione documentazione e licenze;

2.3.5. Sviluppo, Gestione e Manutenzione Reti

- Gestione e controllo del regolare funzionamento del servizio;
- Configurazione e gestione di tutti gli elementi che costituiscono l'infrastruttura di rete (LAN, 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, 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;
- 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 e manutenzione degli armadi reti e patch panel;
- Sicurezza reti;
- Gestione dei log degli apparati di rete conforme alle normative vigenti.

2.3.6. Configurazione, gestione e manutenzione della Sicurezza Informatica

- Valutazione dei rischi, minacce e vulnerabilità (CERT, patching,…);
- Sicurezza perimetrale (firewall, accessi remoti, etc.) e Sicurezza della Intranet (IPS, Url Filtering);
- Gestione delle misure di sicurezza in accordo con le normative;
- Tracciabilità delle connessioni da/verso internet (tenuta dei file di log) e relativa gestione degli incidenti informatici;

- Profilo utente, Autenticazione ed Autorizzazioni, Strong autentication, controllo traffico internet;
- Gestione degli accessi esterni alla rete (VPN);
- Conduzione operativa dei Sistemi di Sicurezza logica della Rete Telematica;
- Verifica delle attività di supporto alla gestione dei sistemi di sicurezza;

2.3.7. Gestione PDL e Supporto Tecnico per gli Utenti Interni

- Servizio di Help Desk;
- Customer Satisfaction Servizi PDL e HD;
- Gestione e IMAC delle PDL;
- Gestione della Sicurezza delle PDL;
- Assistenza HW e SW da remoto PDL;
- Assistenza HW e SW on-site PDL;
- Distribuzione software PDL;
- Richieste di informazioni;
- Interfaccia con i referenti Informatici degli uffici regionali;
- Gestione licenze SW installato sulle PDL;
- Gestione Servizio di Directory delle Risorse in Rete (Active Directory);
- Gestione dei Servizi per l'Utenza regionale (Share, Cloud, Inventario Asset, ecc.);

2.4. Attività di gestione/manutenzione/monitoraggio piattaforma SOA

La piattaforma SOA è l'infrastruttura abilitante per:

- garantire l'interoperabilità dei sistemi informativi (regionali e non);
- l'inoltro delle informazioni alle PP.AA. abilitate alla ricezione automatica dei dati di interesse;
- la cooperazione applicativa in sicurezza orientata ai servizi per garantire lo scambio di informazioni anagrafiche certificate;

ed è composta da circa 70 virtual machine tra test e produzione.

Le attività sono classificate tra azioni di Monitoraggio, Conduzione e manutenzione correttiva.

Di seguito le attività sono riportate in termini skills, input e output atteso attraverso una rappresentazione tabellare.

Tutte le attività insisteranno sull'insieme dei prodotti/semi-lavorati che compongono la piattaforma SOA nella sua interezza, ovvero:

- **Enterprise Service BUS (ESB)**: è un prodotto software sviluppato completamente open source, utilizzando framework OSGI supporta i principali tipi di enterprise integration patterns (EIPs) quali: Filtering di messaggi, Transforming di messaggi da un formato ad un altro, Routing SOAP,

Supporto per code JMS, Supporto per proxy pass through (in HTTP, HTTPS), Iterazioni con basi, di dati, Supporto alla transazionalità

- **Data Service Server (DSS)**: è un prodotto open source che ha come scopo il disaccoppiamento dell'infrastruttura di memorizzazione (data base, file di testo, CVS, Excel, etc) dai dati, rendendone trasparente l'accesso e/o la manipolazione a chi ne fa richiesta esponendo le operazioni come se fossero dei servizi web della SOA
- **Application Server (AS)**: è un prodotto software open source che permette di condividere facilmente logica, dati e processi aziendali nell'intero ecosistema IT. Fornisce una solida base per l'hosting di applicazioni SaaS condivise, multi-tenant e scalabili
- **Business Process Server (BPS)**: è il modulo di WSO2 atto a gestire e realizzare business process, Human Task e Process Modeling
- **Business Rules Server (BRS)**: è un modulo realizzato da WSO2 che permette di definire, implementare, monitorare e gestire regole di business. Tali regole vengono esposte tramite servizi web affidabili e sicuri in modo che esso possa essere integrato all'interno dell'architettura SOA
- **Message Broker (MB)**: è un prodotto open source di WSO2 sviluppato per la gestione della messaggistica implementando una comunicazione asincrona e il paradigma "publish/subscribe"(Topic), code distribuite (Queue)
- **Business Process Management (JBPM)**: è un prodotto open source per la progettazione ed esecuzione di workflow BPMN2, caratterizzato da una forte community e implementato sui principali standard di workflow.
- **Porta di dominio (PDD)**: è un prodotto software certificato DIGIT PA che implementa le specifiche SPCoop per la cooperazione applicativa tra enti pubblici di Regione Campania.
- **Identity Server (IdS)**: è un prodotto software open source che risolve il problema della gestione delle identità in termini di autenticazione, autorizzazione e accounting.
- **Componente Business Activity Monitor (BAM)**: è una componente open source che permette: il monitoraggio, l'aggregazione, analisi e presentazione di dati relative alle attività di business. Garantendo lo storage e trasferimento di grandi moli di dati con alte prestazioni e in modo totalmente affidabile
- **Componente Governance (GR)**: è un prodotto sviluppato per l'archiviazione, la catalogazione, indicizzazione, gestione dei metadati del proprio sistema in relazione al qualsiasi tipo di attività, fornendo un sistema molto semplice per l'accesso a tali informazioni anche in un contesto distribuito. Implementando il concetto di SOA Governance (l'insieme delle operazioni di progettazione sviluppo ed esecuzione della governance ossia del ciclo di vita dei processi)
- **Componente API Manager (APIM)**: è un prodotto della suite che permette di esporre i propri processi chiave, dati e servizi come API per il pubblico, così facendo altri sviluppatori possono utilizzare le API messe disposizione per creare i propri servizi in modo semplice

2.4.1. Attività di Monitoraggio

Gli skill richiesti per effettuare queste attività sono:

- Competenze basilari sistemi linux per la verifica dello stato di un processo in memoria.
- Capacità di avviare e interrompere l'esecuzione di un processo/servizio (daemon).
- Capacità di navigare attraverso un file system linux per visualizzare file di testo ed estrarre informazioni dagli stessi
- Capacità di sviluppare ed eseguire semplici script shell (bash)

- Capacità di redigere documentazione per report che riportano lo stato del sistema ed eventuali azioni da intraprendere.

Attività di monitoraggio dei vari moduli applicativi da effettuare per la verifica del corretto funzionamento degli software in questione.

Modulo	Input richiesti	Output attesi
ESB	N/A	Report bi-settimanale che riporta lo stato del servizio con l'analisi dei principali log di sistema, errori riportati e relativa valutazione sulla gravità degli stessi. Evidenza del carico medio di lavoro e proposte di eventuali azioni migliorative da effettuare
DSS	N/A	Report mensile che riporta lo stato del servizio con l'analisi dei principali log di sistema, errori riportati e relativa valutazione sulla gravità degli stessi.
AS	N/A	Report mensile che riporta lo stato del servizio con l'analisi dei principali log di sistema, errori riportati e relativa valutazione sulla gravità degli stessi.
BPS	N/A	Report mensile che riporta lo stato del servizio con l'analisi dei principali log di sistema, errori riportati e relativa valutazione sulla gravità degli stessi.
BRS	N/A	Report mensile che riporta lo stato del servizio con l'analisi dei principali log di sistema, errori riportati e relativa valutazione sulla gravità degli stessi.
MB	N/A	Report mensile che riporta lo stato del servizio con l'analisi dei principali log di sistema, errori riportati e relativa valutazione sulla gravità degli stessi.
JBPM	N/A	Report bi-settimanale che riporta lo stato del servizio con l'analisi dei principali log di sistema, errori riportati e relativa valutazione sulla gravità degli stessi.
PDD	N/A	Report settimanale che riporta lo stato del servizio con l'analisi dei principali log di sistema, errori riportati e relativa valutazione sulla gravità degli stessi.
IDS	N/A	Report settimanale che riporta lo stato del servizio con l'analisi dei principali log di sistema, errori riportati e relativa valutazione sulla gravità degli stessi. Nel report sarà presentato a cadenza mensile un security assessment con la

Modulo	Input richiesti	Output attesi
		segnalazione di eventuali criticità di sicurezza. Evidenza del carico medio di lavoro e proposte di eventuali azioni migliorative da effettuare
DA	N/A	Report mensile che riporta lo stato del servizio con l'analisi dei principali log di sistema, errori riportati e relativa valutazione sulla gravità degli stessi.
GR	N/A	Report mensile che riporta lo stato del servizio con l'analisi dei principali log di sistema, errori riportati e relativa valutazione sulla gravità degli stessi.
APIM	N/A	Report mensile che riporta lo stato del servizio con l'analisi dei principali log di sistema, errori riportati e relativa valutazione sulla gravità degli stessi.

2.4.2. Attività di conduzione

Gli skill richiesti per effettuare queste attività sono quanto descritto precedentemente per le competenze necessarie per le attività di Monitoraggio, e in più:

Modulo	Skill richiesti per la conduzione
ESB	Conoscenza base della console WSO2 per la gestione dei servizi dell'ESB. In particolare capacità di utilizzare i principali enterprise integration patterns (EIP) quali ad esempio: Filtering di messaggi, Transforming di messaggi da un formato ad un altro, Routing SOAP, integrazione code JMS, …
DSS	Conoscenza base della console WSO2 per la gestione dei servizi dell'DSS. Capacità di aggiungere/modificare/cancellare data source e servizi.
AS	Conoscenza base della console WSO2 di gestione dell'AS, con particolare riferimento all'hosting e gestione delle web application, hosting e gestione di web services, monitoraggio delle applicazioni pubblicate.
BPS	Conoscenza base della console WSO2. Conoscenza base WS-BPEL e BPMN2. Capacità di pubblicare nuovi processi.

Modulo	Skill richiesti per la conduzione
BRS	Conoscenza base dei profili Rule Service Deployer e Rule Service Invoker. Capacità di Creare Servizi che implementano le regole definite. Conoscenza base Drools.
MB	Capacità di creare ed eliminare le code di messaggi, creare ed eliminare topic, creare e gestire sottoscrizioni, visualizzare le statistiche dei messaggi, vavigare il registro
JBPM	Conoscenza base workbench KIE. Conoscenza BPMN2. Capacità di definire nuovi repository. Capacità di pubblicare nuovi processi.
PDD	Conoscenza specifiche SPCoop per la cooperazione applicativa. Conoscenza base Web Services SOAP. Conoscenza base standard per la firma e verifica della firma digitale.
IDS	Conoscenza base console di gestione WSO2. Conoscenza base dello standard SAML2. Capacità di gestire il ciclo di vita di User Store, Gruppi e profili utente. Capacità di gestire Claim.
BAM	Conoscenza base console WSO2. Conoscenza base struttura di un Agent. Capacità di realizzare script di analisi
GR	Conoscenza base console WSO2. Capacità di gestire le risorse (qualsiasi manufatto da file WSDL per XML, documenti Word / Excel, immagini JPEG, ecc) e le collezioni.
APIM	Capacità di creare e pubblicare nuove API (anche distribuite) Gestione dei tenant e degli utenti Importazione ed esportazione API Gestione del gateway in termini di sicurezza e caching Definire modelli di billing per la monetizzazione delle API Gestire la scalabilità del server in termini di cluster e balancer Gestire le estensioni, personalizzazioni e sequenze personalizzate Gestire e configurare l'integrazione con la componenente WSO2 Identity Server

Tutte le attività saranno gestite tramite apposita piattaforma software il cui manuale di gestione sarà condiviso in fase di inizio lavori.

La tabella seguente riporta le colonne “Input richiesti” e “Output attesi”. La prima identifica la tipologia di richiesta che sarà gestita tramite apposito “tracker” sulla piattaforma di gestione dei ticket. La seconda colonna rappresenta il risultato atteso. Sempre nel manuale di gestione, saranno riportati tutte le informazioni che dovranno essere fornite al termine dell’attività stessa.

Di seguito è riportata una lista indicativa e non esaustiva delle possibili attività di conduzione da gestire:

Modulo	Input richiesti	Output attesi
TUTTI	Riavvio servizi	Processi/Servizi arrestati, ripartiti e funzionanti
	Applicazione patch di sistema	Condivisione eventuale disservizio, Backup files impattati Applicazione patch, riattivazione sistemi e verifiche
	Applicazione patch applicativa	Condivisione eventuale disservizio, Backup files impattati Applicazione patch applicativa, riattivazione sistemi e verifiche
	Estrazione logs	Estrazione logs in file compresso da allegare alla chiusura del relativo ticket o path da dove recuperare il file se troppo grande
ESB	CRUD EIP	Aggiunta, Modifica, Cancellazione EIP
DSS	CRUD data source	Creazione, Cancellazione, Modifica e aggiornamento data source DSS.
AS	Pubblicazione applicazione	Applicazione WEB pubblicata e disponibile sulla console.
BPS	CRUD processi	Aggiunta, modifica, cancellazione di un processo.
BRS	CRUD Rules	Aggiunta, modifica, cancellazione di regole.

MB		
JBPM	CRUD workflow	Aggiunta, modifica, cancellazione di un workflow.
	CRUD utenti	Aggiunta, modifica, cancellazione di utenti.
	CRUD repository	Aggiunta, modifica, cancellazione di un repository
PDD	CRUD Porta Applicativa	Aggiunta, modifica, cancellazione di una porta applicativa
	CRUD Porta Delegata	Aggiunta, modifica, cancellazione di una porta delegata
IDS	CRUD Gruppi	Aggiunta, Modifica, Cancellazione Gruppi di utenti (roles)
	CRUD Utenti	Aggiunta, Modifica, Cancellazione Utente
	CRUD User Store	Aggiunta, Modifica, Cancellazione User store
BAM	Reports	Produzione reports analisi dati.
GR	Reports	Produzione reports per estrazione assets.
APIM	Aggiunta, Modifica, Cancellazione API	API aggiunta, modificata o cancellata.

2.4.3. Attività di manutenzione correttiva

La manutenzione correttiva sarà potenzialmente applicabile a tutti i moduli applicativi oggetto di monitoraggio e gestione. In particolare, possiamo considerare le attività di manutenzione correttiva, nell'ambito dei moduli applicativi afferenti:

- Personalizzazioni realizzate nell'ambito dello stack applicativo WSO2
- Porta di dominio della Regione Campania

Entrambi gli ambiti applicativi, richiedono i seguenti skill trasversali:

- Approfondita conoscenza di Java/J2EE (JDK >=1.5)
- Conoscenza dell'ambiente di sviluppo Eclipse e Eclipse based (WSO2 Developer Studio, JBPM Designer)
- Capacità di comprendere e modificare web services SOAP/REST
- Capacità di utilizzo di SCM quali ad esempio Subversion e/o GIT

L'ambito applicativo PDD, richiede i seguenti specifici:

- Approfondita conoscenza delle specifiche SPcoop per la definizione della busta eGov.
- Approfondita conoscenza di Axis 1.4. In particolar modo nella sua componente API Core.
- Conoscenza delle specifiche di interfacce java definite in OpenPDD L2.
- Capacità di modificare semplici applicazioni web basate su tecnologia Java/Servlets/JSP/JDBC.

L'ambito applicativo WSO2 richiede i seguenti skill specifici di piattaforma:

- Capacità di interpretare e modificare custom authenticator realizzati per l'Identity Server
- Capacità di interpretare e modificare i principali EAI per la componente Enterprise Service Bus.
- Conoscenza dello standard BPEL

Il ciclo di vita dell'anomalia software afferente la manutenzione correttiva sarà definito nel relativo manuale di gestione condiviso in fase di inizio attività.

In termini puramente indicativi e non esaustivi:

- Le azioni di manutenzione correttiva (MCC) saranno guidate dall'utilizzo di una piattaforma software per la gestione dei ticket di MCC.
- La piattaforma in questione sarà l'unito strumento di condivisione delle informazioni il cui ciclo di vita sarà, come detto, presente nel manuale di gestione.
- Il ticket creato da operatori specifici, conterranno almeno le seguenti informazioni che verranno fornite in input a chi prenderà in carico la MCC
    - Nome applicativo (tra quelli soggetti a correttiva, sottoinsieme dei moduli oggetti di monitoraggio e gestione)
    - Classificazione della priorità
    - Descrizione dettagliata della problematica
    - Eventuali screenshot dell'errore
- Il responsabile della MCC, a valle della presa in carico e della risoluzione della MCC, chiuderà il ticket con almeno le seguenti informazioni:
    - Descrizione della soluzione
    - Documento di rilascio in allegato al ticket con i test cases per la verifica del corretto funzionamento dell'applicativo oggetto della MCC
    - Eventuale documentazione aggiornata qualora la MCC impatti sulla stessa.
    - Il ticket sarà assegnato all'operatore atto alla verifica funzionale
- L'operatore, a valle della verifica positiva, autorizza il rilascio in produzione che sarà eseguita da specifici operatori.
- Il responsabile della MCC, dovrà sempre mantenere aggiornato il registro di configurazione definito nel manuale di gestione, con tutti i sorgenti e quanto necessario

2.5. Elenco hardware oggetto di manutenzione

2.5.1. Elenco hardware con scadenza manutenzione 2019

Di seguito l'elenco hardware con scadenza di manutenzione 28/02/2019:

MARCA	PRODOTTO	Q.TA'	DESCRIZIONE
Dell	Dell PowerEdge M1000e	8	Blade Chassis
Dell	Dell PowerEdge M610	80	Blade Server - 2 CPU intel Xeon 2,53GHz 4 core, 96 GB RAM - 2 Ports CNA 10Gbs
Dell	Dell PowerEdge M620	2	Blade Server - 2 CPU intel Xeon E5-2695 2,40 GHz 12 core, 96 GB RAM
Dell	Dell MD PowerVault 3860f	1	L'Encloure ospita 60 HD Seagate SAS da 3.5 TB per una capacità totale (al lordo della configurazione RAID) pari a 210 TB.

2.5.2. Elenco hardware con scadenza manutenzione 2020

Di seguito l'elenco hardware con scadenza di manutenzione 01/04/2020:

MARCA	PRODOTTO	Q.TA'	DESCRIZIONE
Hitachi	Chassis Compute Blade 500	3	2 LANpass-through 16x10Gbs ports internal – 16x10Gbs ports external
Hitachi	Blade server Hitachi 520H B2	24	2 CPU Xeon E5-2697v2 2.7GHz 12Core 384GB RAM 2 HDD SAS 300GB 15KRPM RAID 1 2 Ports CNA 10Gbs
Fortinet	Firewall Fortinet 1000C	3	
Fortinet	Firewall Fortinet 1500D	3	
McAfee	IPS McAfee Network Security Platform NS 7200	2	
Hitachi	Server rackmount Hitachi CR220H	3	
Hitachi	Storage Array HUS110 (Backup) con circa 100 TB utili	2	2 controller 8 porte FC 8Gbps 8 GB di cache per controller 30 HDD SAS 4TB 2 SSD 400GB
Hitachi	Storage Array HUS110 (Quorum)	1	n.9 HDD SAS 300GB 10KRpm
Hitachi	Storage Hitachi Virtual	2	350TB utili ognuno con dischi:

	Storage Platform G1000		18 FMD 1.6TB 258 HDD SAS 600GB 10KRpm 162 HDD SAS 4TB 7.2 KRpm
Brocade	Bilanciatore Brocade ADX1216;	2	
Brocade	Extension Brocade 7840: apparato che esegue la conversione tra protocollo FC e IP	3	
Brocade	Switch Brocade 6505: switch Fibre Channel per l'accesso allo storage	2	
Brocade	Switch Brocade VDX6740;	10	
Brocade	Switch di core Brocade ICX7750;	4	
Brocade	Switch FC Brocade 6510;	4	
Brocade	Switch ICX6430, per il monitoraggio out-of-band della rete;	7	

2.5.3. PDL, Scanner ed etichettatrici

Presso tutte le diverse sedi della Regione Campania sono presenti circa:

- N. 5200 Postazioni di lavoro (PDL), ossia PC completi di monitor, tastiera e mouse ;
- N. 100 Notebook;
- N. 250 Scanner;
- N. 75 Etichettatrici.

I PC coperti da garanzia sono circa il 10%, mentre gli altri, avendo un'età compresa tra i tre e i dieci anni, non sono coperti da garanzia..

In alcune sedi sono inoltre presenti anche dei server (15 in tutto) con funzione di distribuzione software e condivisione file.

2.6. Impianti

Di seguito gli impianti presenti nei due datacenter principali.

2.6.1. Napoli

Il datacenter primario è ospitato in un locale di circa 250 mq al cui interno è vi è una zona compartimentata in cui si trova l'UPS. Gli impianti presenti sono:

Impianto elettrico

Il datacenter primario è alimentato da una doppia linea trifase, ciascuna proveniente da due cabine di trasformazione di media tensione, la seconda cabina dotata di trasformatore di 400kVA, interruttori, sezionatori e protezioni dovrà essere presa in carico. Le due linee trifasi a BT seguono percorsi diversi per terminare nei quadri elettrici generali per le linee A e B. Ciascuna linea è protetta da un gruppo elettrogeno e si divide in due rami, uno protetto da ups che alimenta i server e gli apparati IT ed un altro ramo che alimenta i condizionatori. Ciascun ramo di entrambe le linee è dotato di quadro elettrico con sezionatori per ogni armadio rack o sottosezione elettrica.

Impianto continuità elettrica (UPS e Gruppi Elettrogeni)

La continuità elettrica è garantita da due gruppi elettrogeni VISA GALAXY - F 400 GX da 320kW (400kVA) e due gruppi di continuità Liebert Hipulse E 300 kVA con armadio batterie al piombo ermetico (una per ogni UPS), in grado di garantire un'autonomia di 10' con un carico di 300 KVA a cosfi 0,8.

Impianto condizionamento

L'impianto raffreddamento della sala utilizza sia unità infrarack Liebert CRV 20, ad espansione diretta, che unità ad armadio della Liebert (n.2 HPM 17 e n. 2 HPM 25) per una una potenza totale pari a 188 kW frigoriferi. Tutte le unità di raffreddamento sono dotate di un quadro di alimentazione a scambio automatico con doppia alimentazione trifase.

Il locale esterno alla sala che ospita l'UPS della Line A viene raffredato da n.2 Liebert WM13MD.

Impianto di illuminazione

L'illuminazione della sala è stata realizzata con n. 78 pannelli led 60x60 da 36W (Nobile Italia LPS66/4K)

Impianto antincendio

La sala ed il locale UPS sono protetti da un impianto di rivelazione e segnalazione incendio, cosi costituito:

- Centrale di allarme a microprocessore per sistemi ad indirizzamento mod Notifire AM 2000.
- Rivelatori ottici di fumo installati rispettivamente a protezione del controsoffitto, ambiente e sottopavimento.
- Segnalatori luminosi per rivelatori posti nel controsoffitto o sottopavimento;
- Pulsanti di allarme posti lungo le vie di esodo.
- Segnalatori ottico-acustici di allarme.

I locali di cui sopra, sala calcolo e locale ups, sono protetti con un impianto di spegnimento ad Aerosol a base di carbonato di potassio comandato dalla stessa centrale di rivelazione incendio mediante la sua unità USD-3N. Le unità sono realizzare in acciaio verniciato e dimensionate sia per zona che per copertura volumetrica.

Sono stati installati generatori di aerosol sotto il pavimento flottante, in ambiente e nel controsoffitto del nodo primario.

Impianto antiallagamento

E' presente sotto tutte le unità di condizionamento ed i rack posti in fila, un sistema di rilevazione perdite acqua con tipologia a nastro, connesso ad un apposito quadro di controllo mod. Liebert Emerson AC4 che ha sua volta comunica con il sistema di monitoraggio DCIM.

Impianto antintrusione e controllo accessi

L'accesso alla sala Nodo Primario ed al locale UPS è dotato di un impianto di controllo accessi costituito da n° 6 Lettori della serie MINITIME-SI con tecnologia di lettura a prossimità. Le singole teste di lettura sono collegate tramite Bus RS485 al concentratore SATURT-N

Le gerarchie di accesso ai singoli varchi sono gestite e regolate dall'apposito software di controllo accessi WINGAEP-5 installato su un PC locale.

La sala Nodo Primario e del locale UPS è protetta da un impianto antintrusione costituito da;

- Centrale antintrusione ATS1000 8-32 zone 4 aree serie Advisor Advanced
- Contatti magnetici installati sulle porte di accesso.
- Rivelatori a vibrazione installati sulle vetrate.
- Sirena interna.
- Sirena esterna autoalimenta con batteria tampone.

Tutti i dispositivi facenti parte dell'impianto antintrusione sono conformi alla normativa CEI 79-2.

Impianto TVCC

Il sistema di videosorveglianza realizzato a protezione della sala Nodo Primario e del locale UPS è costituito da:

- Nr. 2 Telecamere tipo Bullet Avigilon 2.0W-H3-B01-IR con IR integrato poste in esterno ad angolo del corpo di fabbrica.
- Nr. 3 Telecamere tipo Bullet Avigilon 2.0W-H3-B01-IR con IR integrato poste all'interno del data center per il controllo degli accessi principali.
- Nr. 3 Telecamere Mini Dome Avigilon 1.0-H3-D1 per il monitoraggio dell'area Green.
- Sistema NVR di registrazione e visualizzazione delle immagini relative alle telecamere sopra descritte dotato di HD da 1TB.

2.6.2. Fisciano (SA)

Il **datacenter secondario** è ospitato in un container installato presso l'Università di Saleno, sede di Fisciano.

Impianto elettrico, gruppo elettrogeno, ups

Analogamente agli altri impianti di base del container, l'impianto elettrico è stato installato in fabbrica ed essenzialmente composto da QE ridondanti che alimentano gli apparati mediante linee dedicate verso ogni singolo rack. Dagli stessi QE, ovviamente mediante linee dedicate, sono alimentati anche tutti gli altri impianti di servizio ed in particolare l'impianto di condizionamento,

quello FM di servizio ed illuminazione oltre tutti gli impianti speciali ed a correnti deboli presenti nel sito. Gli interruttori primari sono da 250A regolabili con soglia minima a 200.

Posizionato all'esterno del container si trova un gruppo elettrogeno da 160 KVA completo di quadro di commutazione LTS, con commutazione di potenza rete/gruppo quadripolare. L' autonomia a pieno carico è prevista per 10 ore; la potenza nominale LTP è di 164 KVA = 131,2 kW mentre la potenza PRP è di 158 KVA = 126,4 kW

All'interno del container si trova il gruppo statico di continuità di produzione EMERSON Modello APM con moduli in Rack, scalabile con moduli aggiuntivi inseribili a caldo, la configurazione attuale N+1 (60 KVA + 30 KVA) con n° 3 moduli UPS da 30 KVA cad. (2 in funzione ed uno in ridondanza) con 10 minuti primi di autonomia a pieno carico mediante moduli batteria tampone sostituibili a caldo ed installati in Rack attiguo.

Impianto condizionamento

All'esterno del container si trovano due gruppi refrigeratori ad acqua sono di marca EMERSON Network Power modello HPC-S FG006, completi di batterie freecooling montate direttamente sul gruppo e sono forniti di serbatoio inerziale, di doppia pompa (una in stand-by) e di sistema Soft Start.

All'interno del container in linea con gli armadi rack vi sono n° 6 condizionatori in the row con potenza di 22 kW frigoriferi di marca Emerson Knurr CRV- Mod. CR030RC

Impianto antincendio

L'impianto di estinzione è il Novec 1230, gas "clean agent" in conformità con EN 15004 tipo; NFPA 2001, NPB 88-2001.

La centrale di gestione impianto di spegnimento mod. Smart Line è equipaggiata di scheda estinzione ad 1 canale certificata secondo norma EN 54 parte 2 e 4 e EN12094

2.6.3. Scadenze manutenzione

Sede	Tipo	Marca e Modello	Qta	Scadenza manutenzione
NA	Condizionatori	Emerson CRV 020	10	28/2/2019
NA	Condizionatori	Emerson HPM D17	2	28/2/2019
NA	Condizionatori	Emerson HPM D25	2	28/2/2019
NA	Condizionatori	Emerson WM13MD	2	28/2/2019
NA	UPS	Liebert - Hipulse E 300	2	28/2/2019
NA	Gruppo Elettrogeno	VISA 400kW	1	28/2/2019

NA	Gruppo Elettrogeno	VISA 400kW	1	01/04/2020
NA	Cabina MT	400kVA	1	28/2/2019
NA	Impianto Elettrico	Quadri e linee	1	28/2/2019
NA	Cablaggio e Rack	Panduit, Emerson	1	28/2/2019
NA	Impianti Speciali	Antincendio, Video sorv., Accessi, anti allagamento	1	01/04/2020
NA	DCIM	Analizzatori di rete	17	01/04/2020
NA	DCIM	Centrale di misura	2	01/04/2020
NA	DCIM	PDU monitorabili	40	01/04/2020
NA	DCIM	Site Scan	1	01/04/2020
NA	DCIM	Analizzatori di rete	5	01/04/2020
SA	DCIM	PDU monitorabili	20	01/04/2020
SA	Chiller	Emerson HPC	2	01/04/2020
SA	Condizionatori	CRV- Mod. CR030RC	6	01/04/2020
SA	UPS	30kW modulari	3	01/04/2020
SA	Gruppo Elettrogeno	160kW	1	01/04/2020
SA	Impianto Elettrico	Quadri e linee	1	01/04/2020
SA	Impianti Speciali	Antincendio, Video sorv., Accessi, anti allagamento	1	01/04/2020

3. Definizione della fornitura

L'oggetto della fornitura è l'erogazione di Servizi di Gestione, Manutenzione ed Evoluzione della infrastruttura di rete, degli impianti, dei beni hardware e dei sistemi per i servizi ICT in uso presso la Giunta Regionale della Campania. L'oggetto della fornitura comprende anche un supporto specialistico continuativo con funzione di Assistenza On-Site ed Help Desk (di seguito indicato con AOS-HD).

I suddetti servizi nei capitoli 5,6 e 7 dell'AQ vengono divisi in due macro-categorie:

3.1. Servizi Base

Tutte le attività richieste nei Cap.2.3 e Cap.2.4 del presente AS trovano applicazione nei servizi base indicati nel capitolo 5 dell'AQ:

- gestione sistemi;
- manutenzione sistemi;
- gestione reti;
- gestione applicativi e base dati;
- gestione della sicurezza logica;
- sviluppo e integrazione sistemi;
- service management;

I servizi dovranno essere erogati H24x365 giorni all'anno con le modalità previste nel capitolo 7 dell'AQ:

- Conduzione operativa – presidio on site
- Reperibilità "standard"
- Interventi fuori orario
- Supporto specialistico – continuativo
- Supporto specialistico – a richiesta

Per i dettagli e per il dimensionamento si rimanda al capitolo successivo.

3.2. Servizi Accessori

Le attività di manutenzione dell'hardware e degli impianti indicati rispettivamente nei Cap. 2.5 e Cap.2.6. trovano, invece, applicazione nei servizi accessori del capitolo 6 dell'AQ:

- Manutenzione Hardware;
- Gestione della sicurezza fisica

3.3. Durata del contratto

Il contratto avrà durata **30 mesi** e non comprende la fase iniziale del passaggio consegne.

4. Descrizione e dimensionamento della fornitura

I servizi, richiesti e descritti nei paragrafi precedenti, in questo capitolo vengono schematizzati e dimensionati secondo il modello di erogazione dei servizi riportato al capitolo 7 dell'AQ.

4.1.Servizi Base: Gestione, Manutenzione, Sviluppo e Integrazione Sistemi

Ad integrazione di quanto espressamente previsto ai capitoli 5.1, 5.5 e 5.6 del Capitolato Tecnico dell'AQ, sono richiesti all'interno dei Servizi Base di gestione, manutenzione, sviluppo ed integrazione sistemi le attività dettagliate nei paragrafi:

2.3.1. "Sviluppo, Integrazione, Gestione e Manutenzione dei sistemi server e infrastrutture"

2.3.3. "Configurazione, Gestione e Manutenzione Servizio di Continuità Operativa"

2.3.6. "Configurazione, gestione e manutenzione della Sicurezza Informatica", per le competenze sui sistemi

2.4"Attività di gestione/manutenzione/monitoraggio piattaforma SOA"

I servizi devono essere erogati H24x365 giorni l'anno con le seguenti modaliltà:

1. Presidio onsite orario esteso per i seguenti sistemi:
    - Servizi Infrastrutturali: Active Directory, DNS, Mail Server, Proxy, etc.
    - Servizi Documentali: Delibere Decreti Determine, Protocollo, Burc;
    - Servizi per il personale: Sigrep, Sigaru;
    - Piattaforma SOA;
    - Portali Istituzionali
2. Presidio onsite orario base per tutti sistemi per i quali non è previsto l'orario esteso:
3. Reperibilità standard, per tutti i sistemi, nelle ore non presidiate e nei giorni del sabato e festivi
4. Interventi on site fuori orario di presidio, per tutti i sistemi, in caso di necessità.

I punti 3 e 4 saranno descritti più avanti in questo capitolo.

Nella modalità presidio i servizi devono essere erogati da personale del Fornitore collocato fisicamente nella sede dell'Amministrazione.

Al fine del dimensionamento dei servizi si sono considerati il numero dei server, la complessità e la tipologia di sistemi operativi in accordo al cap.7.1.1.3 del AQ.

Quindi, il fabbisogno di blocchi elementari di remunerazione previsti per ciascun anno per i Servizi Base di gestione, manutenzione, sviluppo ed integrazione sistemi applicando le indicazioni dell'AQ sono riepilogati nella seguente tabella:

Codice	CONDUZIONE OPERATIVA	Q.tà Server logico	N. Blocchi /Anno
P1O1U1	Presidio onsite orario base Server logico Unix/Linux semplice e non critico	209	3
P1O1W1	Presidio onsite orario base server logici Windows semplice e non critico	80	1
P1O2U1	Presidio onsite orario esteso Server logico Unix/Linux semplice e non critico	89	1

P1O2W1	Presidio onsite orario esteso server logici Windows semplice e non critico	80	1

Le risorse impegnate, per ogni singolo servizio, devono avere l'esperienza e le competenze specifiche prescritte nel paragrafo 9.1 *Profili professionali - Sistemista Esperto*.

Relativamente alla piattaforma SOA, gli skill richiesti sono stati indicati nel paragrafo *2.4. "Attività di gestione/manutenzione/monitoraggio piattaforma SOA"* nei sottoparagrafi:

2.4.1. "Attività di Monitoraggio"

2.4.2. "Attività di conduzione"

2.4.3. "Attività di manutenzione correttiva"

Il personale impiegato opererà principalmente nel CED di Napoli. Nel caso di disservizi o esigenze dell'Amministrazione sugli altri due nodi (Salerno o Benevento) non risolvibili da remoto, si dovrà recare a proprie spese sulle sedi oggetto di intervento, portando con sé gli apparati necessari per l'intervento ove previsti e provvedendo allo smaltimento RAEE degli apparati dismessi.

L'orario base del servizio è dalle ore 9.00 alle ore 18.00, dal lunedì al venerdì escluso i giorni festivi.

L'orario esteso del servizio è dalle ore 7.30 alle ore 19.30, dal lunedì al venerdì escluso i giorni festivi.

Gli orari indicati, per esigenze amministrative, possono essere anticipati o posticipati.

Le risorse impegnate in ogni fascia oraria, dalle 7.30 alle 19.30, non dovranno mai essere inferiori a due.

4.2.Servizi Base: Sottosistemi storage/backup

Ad integrazione di quanto espressamente previsto al capitolo 5 del Capitolato Tecnico dell'AQ, sono richiesti all'interno dei Servizi Base di conduzione sottosistemi storage/backup le attività dettagliate nel paragrafo:

2.3.2. "*Configurazione, Gestione e Controllo dei sottosistemi di Storage e Backup"*

Questi servizi devono essere erogati da personale del Fornitore collocato fisicamente nella sede dell'Amministrazione.

Al fine del dimensionamento, si è individuata nel capitolo 7.1.1.3 dell'AQ la categoria T3 - "Sottosistemi di storage complessi e con modalità di backup articolate".

Il fabbisogno di blocchi elementari di remunerazione previsti per ciascun anno sono riepilogati nella seguente tabella

Codice	CONDUZIONE OPERATIVA	Q.tà Sotto-sistemi	N. Blocchi /Anno
P1O1T3	Presidio onsite orario base Sottosistema storage complesso backup articolato	10	1

Le risorse impegnate, per ogni singolo servizio, devono avere l'esperienza e le competenze specifiche prescritte nel paragrafo 9.1 *Profili professionali - Sistemista Esperto*.

L'orario base del servizio è dalle ore 9.00 alle ore 18.00, dal lunedì al venerdì escluso i giorni festivi. L'orario indicato, per esigenze amministrative, può essere anticipato o posticipato.

4.3.Servizi Base: Sottosistemi DBMS

Ad integrazione di quanto espressamente previsto al capitolo 5.4 del Capitolato Tecnico dell'AQ, sono richiesti all'interno dei Servizi Base di conduzione sottosistemi DBMS le attività dettagliate nel paragrafo:

2.3.4. "*Configurazione e Gestione delle Base di dati in Alta Disponibilità*"

Questi servizi devono essere erogati da personale del Fornitore collocato fisicamente nella sede dell'Amministrazione.

Al fine del dimensionamento, si sono individuate nel capitolo 7.1.1.3 dell'AQ le seguenti categorie:

- D1 – "Sottosistema DBMS semplice e non critico";
- D2 – "Sottosistema DBMS semplice e critico oppure complesso e non critico";
- D3 – "Sottosistema DBMS complesso e critico".

Il fabbisogno di blocchi elementari di remunerazione previsti per ciascun anno sono riepilogati nella seguente tabella

Codice	CONDUZIONE OPERATIVA	Q.tà Sotto-sistemi	N. Blocchi /Anno
P1O1D1	Presidio onsite orario base Sottosistema DBMS semplice e non critico	25	1
P1O1D2	Presidio onsite orario base Sottosistema DBMS complesso e non critico o viceversa	17	
P1O1D3	Presidio onsite orario base Sottosistema DBMS complesso e critico	10	

Le risorse impegnate, per ogni singolo servizio, devono avere l'esperienza e le competenze specifiche prescritte nel paragrafo 9.1 *Profili professionali - Sistemista Esperto*.

L'orario base del servizio è dalle ore 9.00 alle ore 18.00, dal lunedì al venerdì escluso i giorni festivi. L'orario indicato, per esigenze amministrative, può essere anticipato o posticipato.

4.4.Servizi Base: Apparati Rete e Sicurezza

Ad integrazione di quanto espressamente previsto ai capitoli 5.3 e 5.5 del Capitolato Tecnico dell'AQ, sono richiesti all'interno dei Servizi Base di conduzione apparati di rete e di sicurezza le attività dettagliate nei paragrafi:

2.3.5. "*Sviluppo, Gestione e Manutenzione Reti*"

2.3.6. "*Configurazione, gestione e manutenzione della Sicurezza Informatica*" per le competenze sulle reti

Questi servizi sono richiesti solo per gli apparati installati nei 3 nodi principali (Napoli, Fisciano, Benevento), ma non per gli apparati installati nelle altre sedi periferiche.

Per gli apparati periferici è previsto un intervento di sostituzione che ne comprende anche la gestione.

I servizi devono essere erogati H24x365 giorni l'anno con le seguenti modaliltà:

1 Presidio onsite orario esteso:

2 Reperibilità standard, nelle ore non presidiate e nei giorni del sabato e festivi

3 Interventi on site fuori orario di presidio, in caso di necessità.

I punti 2 e 3 saranno descritti più avanti in questo capitolo.

Nella modalità presidio i servizi devono essere erogati da personale del Fornitore collocato fisicamente nella sede dell'Amministrazione.

Al fine del dimensionamento, si è individuata nel capitolo 7.1.1.3 dell'AQ la categoria R2 - "Apparato rete/sicurezza complesso".

Il fabbisogno di blocchi elementari di remunerazione previsti per ciascun anno sono riepilogati nella seguente tabella

Codice	CONDUZIONE OPERATIVA	Q.tà Sotto-sistemi	N. Blocchi /Anno
P1O2R2	Presidio onsite orario esteso Apparato rete/sicurezza complesso	70	1

Le risorse impegnate, per ogni singolo servizio, devono avere l'esperienza e le competenze specifiche prescritte nel paragrafo 9.1 *Profili professionali - Sistemista Esperto*.

Il personale impiegato opererà principalmente nel CED di Napoli. Nel caso di disservizi o esigenze dell'Amministrazione sugli altri due nodi (Salerno o Benevento) non risolvibili da remoto, si dovrà recare a proprie spese sulle sedi oggetto di intervento, portando con sé gli apparati necessari per l'intervento ove previsti e provvedendo allo smaltimento RAEE degli apparati dismessi.

L'orario esteso 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 essere almeno tre divise nelle seguenti fasce orarie:

- n.1 risorsa dalle 7.30 alle 16.30;
- n.1 risorsa dalle 9.00 alle 18.00;
- n.1 risorsa dalle 10.30 alle 19.30.

Eventuali ulteriori risorse previste dal fornitore vanno inserite nella fascia centrale.

4.5.Servizi Base: Service Management

Il Fornitore, ove richiesto anche durante la vigenza del contratto, deve assicurare a costo zero sia l'organizzazione dei servizi, in accordo con le best practices ITIL, che gli strumenti di gestione. Eventuali sistemi forniti dovranno avere tecnologia open source e modalità on-premises.

4.5.1. Sistema di monitoraggio

L'Amministrazione già dispone sia di strumenti di monitoraggio che di una struttura dedicata (Unità di Monitoraggio).

Gli strumenti, come riportati nelle pre-esistenze sono:

- Zabbix per gli apparati (Server, Storage, Switch, Router, SAN) e per i servizi (macchine virtuali database, applicazioni),
- SiteScan (DCIM) per gli impianti
- CA E-Health per l'analisi delle performance della rete

Zabbix è un software open source per la rilevazione degli alert e dei parametri di funzionamento dei sistemi stessi. Ad oggi, alcuni dispositivi non vengono monitorati. Il fornitore dovrà mantenere il sistema sempre in piena efficienza, upgradare il software all'ultima release e fare in modo che vengano monitorati sempre tutti i dispositivi installati presso i 3 nodi principali.

L'Unità di Monitoraggio dell'Amministrazione è ubicata nella sala di controllo adiacente alla sala server. Oltre agli strumenti indicati sopra, dispone di una serie di allarmi audio/visivi e la possibilità di ispezionare "de visu" la sala server.

4.5.2. Sistema di Service Management

L'Amministrazione dispone di un strumento di "Service Desk" (GLPI) per:

- la Gestione dei Change Order, Incident, etc..
- l'inventario di tutti gli asset con storicizzazione delle configurazioni;
- la gestione delle licenze;
- la Knoweledge Base (FAQ);
- la gestione dei report su hardware, rete, interventi.

Questo strumento è ottenuto dall'integrazione di diversi software open source (GLPI + OCS Inventory).

Il fornitore dovrà mantenere il sistema sempre in piena efficienza, upgradare il software all'ultima release e su richiesta dell'Amministrazione integrarlo con strumenti specifici per arricchirne le funzionalità.

I presidi on site sia dei SIstemi (SIS) che delle Reti (NOC) possono essere attivati o mediante lo strumento di Service Desk o con un sistema automatico di alert, da:

- Unità di Monitoraggio;
- Strumenti di monitoraggio;
- Referenti informatici o del CRED;
- Responsabili degli applicativi autorizzati dal CRED
- Assistenza tecnica On-Site e Help Desk (AOS-HD, servizio descritto nei paragrafi successivi)

All'Aggiudicataria è fatto obbligo di comunicare all'Unità di Monitoraggio della Stazione appaltante, in tempo reale e mediante Service desk, ogni guasto, anomalia o disservizio che pregiudichi il funzionamento della rete, dei sistemi e delle applicazioni in uso.

Il Fornitore, in ogni caso, dovrà, in accordo con l'Amministrazione, proporre e adottare un'adeguata strutturazione dei processi di gestione secondo le best practices ITIL, attraverso una fase iniziale di

implementazione da ricondurre nell'ambito del servizio di sviluppo e integrazione sistemi. Questa strutturazione può essere rivista periodicamente durante la vigenza del contratto.

4.5.3. Sistema di Reportistica e SLA Management

Il Fornitore dovrà rendere disponibile all'Amministrazione 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 serviz;

in accordo alle specifiche indicate al capitolo 4.2.2 dell'AQ.

Il sistema come indicato all'inizio del paragrafo dovrà essere fornito con tecnologia open source e in modalità on-premises.

4.6.Servizi Base: Reperibilità standard

Al fine di garantire la continuità dei servizi H24x365, si chiede la disponibilità di risorse professionali da ingaggiare al di fuori del normale orario di lavoro per la risoluzione di eventuali malfunzionamenti. Tali risorse potranno essere attivate dai referenti dell'Amministrazione o in automatico da sistemi di allarmi.

Il servizio di reperibilità standard non include gli interventi onsite. Gli interventi dovranno essere erogati in remoto dal Centro Servizi del Fornitore, pertanto, il servizio di reperibilità dovrà includere, senza ulteriori oneri, anche:

- La disponibilità di un numero telefonico unico da contattare dedicato all'Amministrazione
- La connessione telematica tra il Centro Servizi e la sede dell'Amministrazione.

La connessione deve garantire adeguate prestazioni e affidabilità. Le modalità di attestazione di tale collegamento dovranno essere concordate con l'Amministrazione in fase di avvio della fornitura.

Il fornitore deve garantire la sicurezza dei collegamenti e la riservatezza dei sistemi e delle informazioni attraverso la formalizzazione e l'applicazione di procedure e politiche di sicurezza da adottare al proprio interno (Sistema di Gestione delle Sicurezza delle Informazioni – SGSI), adeguate ai requisiti stabiliti dall'Amministrazione.

Inoltre, il fornitore deve mettere a disposizione dell'Amministrazione un sistema di monitoraggio dove si evincono almeno i seguenti elementi:

- Tempo inizio chiamata dell'utente;
- Tempo risposta dell'utente;
- Problema segnalato;
- Tempo risoluzione problema o di richiesta intervento on-site

Il servizio di reperibilità standard deve essere erogato con le seguenti tempistiche:

- risposta entro 30 secondi per l'90% delle chiamate ricevute. Verrà 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.

Eventuali malfunzionamenti non risolvibili da remoto, con impatto sui sistemi critici, devono essere immediatamente segnalati all'Amministrazione. Successivamente l'operatore remoto, su autorizzazione dell'Amministrazione, dovrà attivare il supporto per l'intervento on-site.

I fabbisogni previsti per ciascun anno sono riepilogati nella seguente tabella:

Codice	REPERIBILITA' STANDARD	N° elem Anno
RSTS	Server logico a disponibilità continuativa	150
RSTR	Apparato rete/sicurezza a disponibilità continuativa	70
RSTD	Istanza DBMS a disponibilità continuativa	30

L'orario del servizio è dalle 19.30 alle 7.30 dal lunedì al venerdì; dalle 0.00 alle 24.00 sabato, domenica e festivi.

Per particolari periodi dell'anno, l'Amministrazione potrà richiedere che Il servizio di reperibilità venga esteso anche ad altri sistemi.

4.7.Servizi Base: Interventi fuori orario

Per particolari esigenze o a seguito di malfunzionamenti, l'Amministrazione può richiedere **interventi onsite al di fuori dell'orario di lavoro** per risorse professionali già operanti presso l'Amministrazione.

Sono richieste 480 ore di interventi on site fuori dell'orario di lavoro così ripartiti:

- 240 ore annue per Sistemista Senior con competenze sull'infrastruttura server
- 240 ore annue per Sistemista Senior con competenze sull'infrastruttura di rete

Il fabbisogno in ore previsti per ciascun anno sono riepilogati nella seguente tabella

Codice	FUORI ORARIO	N° ore Anno
FOSS	Interventi fuori orario sistemista senior	480

Tale servizio può essere attivato, a seguito di malfunzionamenti non risolvibili da remoto, dal Centro Servi avendo preventivamente segnalato il disservizio all'Amministrazione e deve essere eseguito entro un'ora dalla richiesta. Può essere, inoltre, attivato su richiesta dell'Amministrazione per estensioni temporanee dell'orario di servizio per esigenze contingenti di durata limitata nel tempo che richiedano la piena disponibilità del personale di conduzione e/o di supporto oltre l'orario standard.

Al termine di ciascun intervento, dovrà essere redatta un'apposita nota, sottoscritta da un incaricato dell'Amministrazione e da un incaricato del Fornitore, nella quale saranno registrati:

- l'orario ed il numero identificativo della richiesta di intervento effettuata dal servizio di Reperibilità Standard;
- il luogo, l'ora ed il giorno di intervento;
- l'ora ed il giorno dell'avvenuto ripristino (o di chiusura dell'intervento);
- descrizione dell'intervento.

Il servizio sarà remunerato, nel corso di validità del contratto, sulla base delle attività periodicamente consuntivate.

4.8. Servizi Base: Supporto specialistico continuo "AOS-HD"

L'Amministrazione intende realizzare un servizio di AOS-HD attraverso l'acquisizione di supporto specialistico continuo. L'AOS-HD rappresenterà, per tutti gli utenti regionali, il punto di contatto centralizzato per il servizio di supporto ed assistenza su tutte le problematiche inerenti sia l'infrastruttura ICT che i servizi offerti.

Le problematiche potranno riguardare, quindi:

1. gli apparati attivi e passivi della rete regionale
2. le risorse informatiche centralizzate o distribuite (hardware e software) in uso presso la Giunta Regionale della Campania
3. le postazioni di Lavoro Regionali (comprese di: stampante, Monitor, Scanner, Webcam, Lettore Card, etc.))
4. I servizi applicativi offerti dalla Giunta Regionale della Campania (Protocollo, Workflow documentale, Posta Elettronica, etc.)

Relativamente all'ultimo punto, gli operatori dell'AOS-HD saranno opportunamente formati. Le altre attività di competenza dell'AOS-HD sono dettagliate nel paragrafo:

2.3.7 "*Gestione PDL e Supporto Tecnico per gli Utenti Interni*"

L'AOS-HD sarà organizzato su due livelli: periferico e centrale.

Sulle sedi periferiche più importanti (in base al numero degli utenti o ai servizi che offrono) saranno dislocati una parte degli operatori del supporto specialistico richiesto. Questi saranno il punto di riferimento per le problematiche indicate all'inizio del paragrafo, per gli utenti di quella sede. Inoltre, potranno essere di supporto ai gruppi SIS, NOC ed ai referenti informatici del CRED per attività inerenti quella sede.

Periodicamente, con cadenza almeno mensile, dovranno attivare un servizio di trasporto delle apparecchiature tra le sedi periferiche e quella di Don Bosco.

L' AOS-HD centrale, invece opererà in stretta collaborazione con i gruppi di presidio SIS e NOC. All' AOS-HD centrale arriveranno, tramite Service Desk, numero verde o posta elettronica, tutte le richieste degli utenti.

L' AOS-HD centrale potrà in base alla richiesta ed alle proprie competenze:

- risolvere il problema
- smistare la richiesta ali gruppi di presidio opportuni (SIS e NOC)
- smistare la richiesta ai referenti applicativi, per problematiche applicative;

- inoltrare la richiesta all' AOS-HD periferico per interventi onsite sulle postazioni.

L'elenco di cui sopra non è esaustivo. Gli operatori dell' AOS-HD saranno gestiti direttamente dalla struttura regionale di competenza, la quale, impartirà istruzioni dettagliate sul servizio da rendere e sull'organizzazione.

Tra gli operatori dello AOS-HD centrale deve essere individuato un "Responsabile Help Desk" con il compito di coordinamento delle attività, della tenuta, 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 dell' AOS-HD.

Gli strumenti a disposizione dello AOS-HD sono:

1. Service Desk e Trouble Ticketing impelementati dall'integrazione dei prodotti GLPI e OCS Inventory;
2. Client CA DSM per l'assistenza remota all'utenza;
3. Microsoft WSUS per la distribuzione degli Upgrade dei Sistemi Operativi Microsoft;
4. CA per la Software Distribution;
5. CA Software Delivery;
6. Sophos Endpoint Protection Advanced and Mail;
7. Microsoft KMS per la gestione delle licenze Microsoft.

Per il dimensionamento si sono considerati gli interventi effettuati negli ultimi anni, il numero di sedi ed infine il numero complessivo di utenti.

Il fabbisogno in risorse previste per ciascun anno sono riepilogati nella seguente tabella

Codice	SUPPORTO SPECIALISTCO CONTINUATIVO	N° risorse Anno
SCSJ1	Supporto specialistico continuativo orario base sistemista junior	1
SCOP1	Supporto specialistico continuativo orario base operator	17

L' AOS-HD centrale sarà costituito da 4 operatori e da un sistemista junior con il ruolo di "Responsabile dell'Hel Desk" ed opereranno principalmente nel CED di Napoli.

L' AOS-HD periferico sarà costituito da 13 persone e opereranno nelle sedi periferiche più importanti. Ogni risorsa potrebbe operare contemporaneamente in più sedi attigue.

La suddetta distribuzione nonché le sedi interessate potranno cambiare, anche temporaneamente, per esigenze dell'Amministrazione.

L'Amministrazione ha anche avviato un progetto di migrazione delle PDL fisiche alle VDI. Pertanto, il numero di risorse necessarie sulle sedi periferiche potrebbe, nel corso del tempo, diminuire. Quindi, l'Amministrazione si riserva di attivare nei successivi periodi del contratto un numero inferiore di risorse. E' facoltà dell'Amministrazione utilizzare le economie sulle risorse non attivate per nuovi servizi.

La risorsa impegnata come "responsabile dell'AOS-HD", deve avere l'esperienza e le competenze specifiche prescritte nel paragrafo 9.2 *Profili professionali - Sistemista junior*.

Le risorse impegnate come "operatore dell' AOS-HD", devono avere l'esperienza e le competenze specifiche prescritte nel paragrafo 9.3 *Profili professionali - Operatore*.

Gli orari sono riportati nella tabella seguente. I giorni vanno dal lunedì al venerdì escluso i giorni festivi. L'orario indicato, per esigenze amministrative, può essere anticipato o posticipato.

Gruppi	SEDE	N. Operatori	Distribuzione oraria	Orario
HD Periferico	Sedi principali	**13**		8.00-17.00
HD Centrale	Don Bosco	**5**	3	7.30 - 16.30
			1	9.00 - 18.00
			1	10.30 - 19.30

4.9.Servizi Base: Supporto specialistico a richiesta

L'Amministrazione ha avviato diversi progetti di innovazione tecnologica e di sicurezza informatica.

Pertanto, per la corretta evoluzione dell'infrastruttura tecnologica sono richieste n.80 giorni annui del **servizio Supporto specialistico a richiesta** specialista di tecnologia principalmente in ambito Sicurezza, Cloud Ibrido, Architetture distribuite e VDI.

Tale servizio si attiverà a richiesta dell'Amministrazione e saranno preventivamente definiti programmi, tempi e obiettivi.

Il servizio sarà remunerato, nel corso di validità del contratto, sulla base delle attività periodicamente consuntivate.

Il fabbisogno in risorse previste per ciascun anno sono riepilogati nella seguente tabella:

Codice	SUPPORTO SPECIALISTCO A RICHIESTA	N° giorni Anno
SRCT	Supporto specialistico a richiesta specialista di tecnologia	80

4.10.Servizi Accessori: Manutenzione Hardware

Il servizio di manutenzione hardware consiste nell'individuazione delle cause del guasto, nonché nella riparazione delle parti mal funzionanti e nella sostituzione dei componenti guasti con componenti uguali e/ o di livello superiore.

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.

Per gli apparati elencati nel sottoparagrafo 2.5.1. *"Elenco hardware con scadenza manutenzione 2019"* si richiede il servizio di **manutenzione hardware per 2 anni da attivare il 1/03/2019**

Per gli apparati elencati nel sottoparagrafo 2.5.2. *"Elenco hardware con scadenza manutenzione 2020"* si richiede il servizio di **manutenzione hardware per 1 anno da attivare il 1/04/2020**

Per le apparecchiature elencate nel sottoparagrafo 2.5.3. *"PDL, Scanner ed etichettatrici"* si richiede il 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, relative al sottoparagrafo 2.5.3, potrebbe nel corso del tempo diminuire per cambiamento di tecnologia. Quindi, l'Amministrazione si riserva di rideterminare nei successivi periodi del contratto un servizio di manutenzione per un numero inferiore di apparecchiature.

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

L'intervento di manutenzione può essere attivato:

- direttamente dai tecnici del CRED, compreso SIS e NOC, tramite il sistema di trouble ticketing integrato per i servizi ICT in dotazione all'Amministrazione, informandone l'Unità di monitoraggio;
- da un qualunque utente del servizio tramite chiamata all'AOS-HD, che provvederà immediatamente ad aprire un ticket nel Service desk e a inoltrarlo alla struttura di competenza;
- dal sistema automatico di monitoraggio adottato dall'Amministrazione e/o in caso di manutenzione preventiva.

Il servizio dovrà essere erogato entro il giorno lavorativo successivo alla chiamata ("servizio NBD", Next Business Day On-site Service).

L'orario di intervento relativo alla sola manutenzione delle PDL va dalle ore 8.00 alle ore 16.00

4.11. Servizi Accessori: Gestione della 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 e di condizionamento delle sale CED.

In particolare è richiesta la fornitura di un servizio di manutenzione e monitoraggio di tutti gli impianti esistenti a servizio dei due nodi regionali (Napoli e Salerno) così come descritti nei paragrafi 2.6. "*Impianti".*

4.11.1. Manutenzione Impianti

Come evidenziato nel sottoparagrafo 2.6.3. *"Scadenza manutenzione*", gli impianti si possono dividere in due gruppi in base alla scadenza dell'esistente contratto di manutenzione

In particolare:

- Per gli impianti con scadenza manutenzione nel 2019 è richiesto un servizio di **manutenzione di 2 anni da attivare il 01/03/2019;**
- Per gli impianti con scadenza manutenzione nel 2020 è richiesto un servizio di **manutenzione di 1 anno da attivare il 1/04/2020**

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

L'intervento di manutenzione può essere attivato:

- direttamente dai tecnici del CRED, compreso SIS e NOC, tramite il sistema di trouble ticketing integrato per i servizi ICT in dotazione all'Amministrazione, 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 30 minuti dall'inizio del disservizio per situazioni critiche (eccessivo aumento della temperatura, problemi sull'impianto antincendio, etc.);
- risoluzione del guasto entro il giorno lavorativo successivo alla chiamata ("servizio NBD") durante l'orario lavorativo base per situazioni non critiche.

4.11.2. Monitoraggio Impianti

Mediante il software il software DCIM SiteScan Web della Emerson ed i relativi misuratori vengono monitorati i seguenti impianti a servizio di entrambi i nodi, primario e secondario:

- n. 3 Gruppi Elettrogeni
- n. 3 Gruppi di Continuità
- n. 22 Multimetri presenti nei Quadri Elettrici
- n. 60 PDU che alimentano gli apparati in n. 30 armadi rack
- n. 18 Condizionatori
- rilevamento accessi
- antincendio
- antintrusione.

Il fornitore dovrà acquisire in tempo reale, H24x365 giorni, gli alert generati dal sistema di monitoraggio, anche 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.

5. Strumenti a supporto della fornitura

Gli strumenti di supporto già in uso all'Amministrazione sono stati descritti nel paragrafo 4.5 del presente AS.

6. Riepilogo della fornitura

La seguente Tabella riepiloga l'insieme dei servizi richiesti per il presente appalto

Codice	Descrizione	Q.tà	Unità Misura
P1O1U	Conduzione Operativa - Presidio onsite orario base server logici Unix/Linux	3	blocchi/anno
P1O2U	Conduzione Operativa - Presidio onsite orario esteso server logici Unix/Linux	1	blocchi/anno
P1O1W	Conduzione Operativa - Presidio onsite orario base server logici Windows	1	blocchi/anno
P1O2W	Conduzione Operativa - Presidio onsite orario esteso server logici Windows	1	blocchi/anno
P1O2R	Conduzione Operativa - Presidio onsite orario esteso apparati rete/sicurezza	1	blocchi/anno
P1O1T	Conduzione Operativa - Presidio onsite orario base sottosistemi storage/backup	1	blocchi/anno
P1O1D	Conduzione Operativa - Presidio onsite orario base sottosistemi DBMS	1	blocchi/anno
RSTS	Reperibilità standard - Server logico a disponibilità continuativa	150	elem/anno
RSTR	Reperibilità standard - Apparato rete/sicurezza a disponibilità continuativa	70	elem/anno
RSTD	Reperibilità standard - Istanza DBMS a disponibilità continuativa	30	elem/anno
FOSS	Interventi fuori orario sistemista senior	480	ore/anno
SCSJ1	Supporto specialistico continuativo orario base sistemista junior	1	risorse/anno
SCOP1	Supporto specialistico continuativo orario base operatore	17	risorse/anno
SRCT	Supporto specialistico a richiesta specialista di tecnologia	80	giorni/anno
	Servizi accessori – Manutenzione Hardware		
	Servizi accessori – Gestione della Sicurezza Fisica		

I canoni periodici (calcolati in base al numero iniziale di componenti infrastrutturali) e il numero di risorse per il supporto specialistico continuo (calcolato in base alla tecnologia e l'organizzazione attuale) potranno essere oggetto di revisione periodica, in aumento o in diminuzione, in base al ricalcolo del numero di componenti infrastrutturali presenti al momento ed al supporto necessario per la nuova tecnologia.

I servizi di manutenzione richiesti per le apparecchiature informatiche e per gli impianti descritti nei paragrafi 2.5 e 2.6 saranno attivati solo a scadenza dei contratti di manutenzione vigenti.

7. Fasi operative della fornitura

L'affidamento dei servizi di system management è inserito in un quadro organico di discontinuità della fornitura, dal momento che in 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.

7.1. Fase di startup delle Fornitura

La fase di startup 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 3 mesi e si articola nelle seguenti principali sotto-fasi:

- 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).
- 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.
- 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 e sistemi) 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.

7.2. Fase finale

In prossimità della conclusione del contratto, il Fornitore dovrà 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.

Il periodo di supporto potrà durare fino a 3 mesi dove dovranno essere previste sessioni di addestramento ed il trasferimento all'Amministrazione delle soluzioni e strumenti utilizzati nel corso della fornitura.

7.3. Fase esecuzione contratto di fornitura

Le figura professionali offerte dal fornitore dovranno essere adeguate a coprire tutti gli ambiti tecnologici e tutte le attività indicate dall'Amministrazione nel paragrafo 2. 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 ad 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 adeguate all'attività svolta.

Il personale impiegato opererà principalmente nel CED di Napoli nei locali messi a disposizione dell'Amministrazione e secondo le direttive impartite dalla stessa, relativamente alle politiche di sicurezza e di accesso.

8. Piano della 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 Concorrente garantendo le Amministrazioni richiedenti sul rispetto delle prassi e delle norme sulla sicurezza per tali modalità operative.

Il Fornitore, in sede di Appalto Specifico, dovrà predisporre e fornire all'Amministrazione 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 per ciò 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.

8.1. 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.

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 secondo i modelli descritti nel paragrafo 7.1, 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 al Capitolato Tecnico dell'AQ. 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	1‰ del valore complessivo del Contratto di Fornitura per ogni risorsa sostituita oltre soglia
IQ02 - Turn over del personale	1	Trimestrale	1‰ 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	0.2‰ del valore complessivo del Contratto di Fornitura per ogni giorno di ritardo oltre soglia
IQ06 - Slittamento delle scadenze	5	Trimestrale	0.2‰ del valore complessivo del Contratto di Fornitura per ogni giorno di ritardo oltre soglia
IQ07 - Qualità della documentazione prodotta	10%	Trimestrale	0.2‰ del valore complessivo del Contratto di Fornitura per ogni punto percentuale oltre soglia
IQ08 – Rilievi sulla fornitura	3	Trimestrale	0.2‰ 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 al Capitolato Tecnico dell'AQ. 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
IQ10 – Disponibilità dei Servizi con presidio on site orario esteso indicati nel par.4.1	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
IQ10 – Disponibilità dei Servizi con presidio on site orario base indicati nel par.4.1	99.50%	Mensile	0.1‰ del valore complessivo del Contratto di Fornitura per ogni 0.1% di disponibilità in meno rispetto al valore di soglia
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, inoltre, introdotti alcuni livelli di servizio specifici per i servizi accessori non previsti nell'AQ:

Indicatore di Qualità Operativi	Valore Soglia	Riferimento	Penale applicata per mancato rispetto del valore soglia
IQA1 – Servizi Accessori: Manutenzione Hardware/Impianti- Servizio richiesto come indicato nei paragrafi 4.10 e 4.11.	NBD	Singolo intervento	1000 Euro per ogni giorno lavorativo di ritardo nella risoluzione del guasto
IQA2 – Servizi Accessori: Manutenzione Hardware/Impianti- Servizio richiesto come indicato nei paragrafi 4.10 e relativo alle sole apparecchiature elencate nel sottoparagrafo 2.5.3. *"PDL, Scanner ed etichettatrici"*.	NBD	Singolo intervento	100 Euro per ogni giorno lavorativo di ritardo nella risoluzione del guasto
IQTA – Tempo Attesa: Tempo che intercorre tra l'inizio della chiamata e la risposta da parte dell'operatore, come indicato nel paragrafo 4.6	Entro 30'' nel 90% delle chiamate telefoniche	Trimestrale	1000 Euro per ogni punto percentuale di scostamento in diminuzione.

9. Profili professionali e Schema per la presentazione dei CV

Le figure professionali proposte per lo svolgimento dei servizi oggetto della fornitura 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.

Pertanto, le competenze e conoscenze tecniche delle figure che seguono non sono da considerarsi esaustivi delle esigenze della fornitura, in quanto 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.

9.1.Sistemista Esperto

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 • Certificazioni nei diversi ambiti tecnologici
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 per	• Amministrazione e gestione Sistemi Operativi, installazione, configurazione, personalizzazione/tuning e gestione dei sistemi operativi UNIX e dei principali sistemi operativi di tipo Open Source (distribuzioni di

S.O. Linux e relative Certificazioni	Linux quali Centos, Oracle Linux, SUSE, Red Hat, Mandrake, Debian, ecc); • 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 approfondite in ambito System Administration ed Mail Server per S.O. Microsoft e relative Certificazioni	• Amministrazione e gestione Sistemi Operativi, installazione, configurazione, personalizzazione/tuning e gestione dei sistemi operativi Microsoft, anche in configurazione cluster; • Amministrazione e gestione dei server Microsoft Exchange, 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 approfondite in ambito Database e relative Certificazioni	• Database administration (Oracle Db, Sql server, mysql, postgress slq, ecc.) • Configurazioni dei database in Alta Affidabilità/Disponibilità utilizzando tecnologie standard (DataGuard per Oracle, DataReplication per MySql, etc.); • Ottimizzazione delle strutture dati.
Conoscenze approfondite 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. • Prodotti che compongono la piattaforma **SOA** come descritti nel paragrafo 2.4 "Attività di gestione/manutenzione/monitoraggio piattaforma SOA"
Conoscenze approfondite in ambito SAN e Backup e relative Certificazioni	• Tipologie di Raid • Tecnologie e best practice di integrazione tra host e apparati di storage • Mobilità dei dati • SCSI e FCS – LUN e associazione con File System • Zoning e LUN Masking • Multipathing • Data center in modalità active-active con Global Active Device • Disaster Recovery e funzioni di alta affidabilità degli storage • Remote Mirroring e aggiornamento Sincrono-Asincrono • Orchestrazione del backup con ASG Time Navigator • Data loss prevention • Data retention e deduplica
Conoscenze	• Installazione, configurazione, personalizzazione/tuning e gestione delle

approfondite nell'ambito delle tecnologie di virtualizzazione e relative Certificazioni	tecnologie di virtualizzazione (VMWare, Oracle VM Server) in ambienti complessi con storage su SAN • Disegno e implementazione di server, storage e modalità di backup e restore • Supporto di ambienti enterprise.
Conoscenze approfondite in ambito networking e relative Certificazioni	• 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 ambito sicurezza	• Amministrazione sistemi operativi degli apparati di sicurezza quali Firewall, terminatori VPN, sistemi di autenticazione forte, ecc., con 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 approfondite 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 approfondite in	• Installazione, configurazione, customizzazione, tuning e troubleshooting dei prodotti di IT Service Management

ambito ServiceManagement	• 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. XenApp, XenDesktop)

Ogni risorsa deve avere almeno una certificazione in un ambito indicato. Le certificazioni richieste in ogni ambito devono essere possedute da almeno una risorsa. Saranno considerate ai fini della valutazione solo le certificazioni attinenti la tecnologia utilizzata dall'Amministrazione ed all'interno del relativo percorso di certificazioni. Tutti i sistemisti richiesti devono coprire l'insieme degli ambiti sopra descritti fermo restando che le esperienze consolidate devono essere possedute da tutti.

9.2.Sistemista junior

La figura professionale, deve rispettare i requisiti indicati nella successiva tabella

Titolo di studio	Laurea in discipline tecniche o diploma di 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; • Supporto all'elaborazione ed alla redazione di specifiche di progetto e di studi di fattibilità; • Metodologie di project management e di best practices ITIL; • Certificazioni nei diversi ambiti tecnologici
Conoscenze base 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 dei sistemi operativi

	Microsoft; • 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 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 base in ambito ServiceManagement	• 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. XenApp, XenDesktop)

9.3. Operatore

La figura professionale, deve rispettare i requisiti indicati nella successiva tabella

Titolo di studio	Diploma di maturità 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 System Administration	• Esecuzione procedure su Sistemi Operativi Open Source e Microsoft, anche in configurazione cluster; • Personalizzazione di file di sistema (es. password, group, hosts) • Gestione delle procedure di startup e shutdown;
Conoscenze base nell'ambito delle tecnologie di virtualizzazione	• Tecnologie di virtualizzazione (VMWare, Citrix, Microsoft) in ambienti complessi con storage su SAN • -Supporto di ambienti enterprise (esecuzione di procedure).
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 • Principali standard di sicurezza (ITSEC, BS7799)
Conoscenze base in ambito Operation Management	• strumenti di system monitoring, application performance monitoring, workload automation, prodotti di analisi log (esecuzione comandi e procedure)

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. XenApp, XenDesktop)

9.4.Schema per la presentazione dei CV

Di seguito viene presentato lo schema che il fornitore dovrà utilizzare per la compilazione dei curriculum 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="3">(Inserire il Cognome e il Nome della risorsa)</td></tr>
<tr><td>Ruolo</td><td colspan="3">(Inserire il Ruolo attualmente ricoperto dalla risorsa)</td></tr>
<tr><td>Figura professionale</td><td colspan="3">(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="3">(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="3">(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="3">(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>Data inizio-Data fine</td><td>Esperienze</td></tr>
<tr><td rowspan="3"></td><td></td><td></td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
<tr><td rowspan="3"></td><td></td><td></td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
<tr><td rowspan="3"></td><td></td><td></td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
<tr><td rowspan="2">Competenze Tecniche</td><td colspan="3">(Indicare le competenze specifiche di cui si è in possesso)</td></tr>
<tr><td colspan="3"></td></tr>
<tr><td rowspan="2">Specializzazioni</td><td colspan="3">(Indicare eventuali specializzazioni, master, ecc.)</td></tr>
<tr><td>Anno</td><td>Titolo</td><td>Descrizione</td></tr>
</table>

<table>
<tr><td rowspan="2"></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td>Certificazioni</td><td colspan="3">(Indicare eventuali certificazioni)</td></tr>
<tr><td rowspan="3"></td><td>Anno</td><td>Titolo</td><td>Descrizione</td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td rowspan="4">Istruzione</td><td colspan="3">(indicare i titoli di studio)</td></tr>
<tr><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></td><td colspan="3">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</td></tr>
<tr><td rowspan="4">Lingue</td><td colspan="3">5 - madrelingua - (native language)</td></tr>
<tr><td colspan="2">Lingue</td><td>Grado di conoscenza</td></tr>
<tr><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>Principali pubblicazioni</td><td colspan="3">(indicare le principali pubblicazioni)</td></tr>
</table>