



CAPITOLATO TECNICO SPECIALE

OGGETTO: RICHIESTA DI OFFERTA (RDO) SULLA PIATTAFORMA MEPA, EX ART. 36, C.2, LETT. B DEL D.LGS 50/2016 E S.M.I., PER L’AFFIDAMENTO DI SERVIZI INFORMATICI DI ASSISTENZA TECNICA CON CONSULENZA SPECIALISTICA EVOLUTA NECESSARI PER LA GESTIONE E IL MANTENIMENTO DELL’INFRASTRUTTURA IT DEL CIP DAL 01/01/2021 AL 31/12/2023

CIG 8419035776

1. PREMESSA

Il presente capitolato tecnico disciplina l'affidamento di servizi informatici con consulenza specialistica evoluta necessari per la gestione e il mantenimento dell'infrastruttura IT del CIP fino al 31/12/2023.

Nell'esecuzione delle proprie attività il fornitore dovrà attenersi alle indicazioni riportate nel presente documento.

Missione, statuto, regolamenti, normative di riferimento, organi e struttura del Comitato Italiano Paralimpico (di seguito anche Comitato o CIP) sono pubblicati sul sito web istituzionale: www.comitatoparalimpico.it.

2. ANALISI DELL’INFRASTRUTTURA IT DEL CIP

All'interno dell'infrastruttura IT del CIP sono definite le sedi così distinte:

- a) CIP HQ (con sede in Via Flaminia Nuova 830 – 00191 Roma)
- b) CIP Circuito Tre Fontane (con sede in Via delle Tre Fontane 25/27/29 – 00144 Roma)
- c) CIP Palazzo dell'Archivio (con sede in P.le degli Archivi 41 – 00144 Roma)
- d) CIP Strutture Territoriali (con sedi su tutto il territorio nazionale di cui al link <http://www.comitatoparalimpico.it/territorio.html>)

2.1 WAN e sicurezza di accessi

L'infrastruttura informatica del Comitato è protetta attraverso dei firewall della famiglia Cisco Meraki (19 appliances totali) configurati a valle dei servizi di connettività.

Gli accessi dall'esterno sono disponibili solo unicamente attraverso l'instaurazione di un collegamento VPN, preventivamente abilitato dai network admins, su protocollo L2TP-IPSEC.

All'interno del Comitato non ci sono servizi che richiedono una esposizione esterna.

Ad oggi è attivo un processo di centralizzazione che prevede il collegamento di tutte le strutture territoriali con la sede principale in modo tale da garantire la fruizione di servizi messi a disposizione dal Comitato; tale collegamento è attivo per tutte le strutture territoriali dislocate a livello nazionale.

2.2 Piattaforma server e servizi

L'infrastruttura server del Comitato prevede appliances basati su piattaforma virtuale gestita dal sistema operativo Vmware ESXi 6.x.

All'interno della piattaforma sono configurate distinte macchine virtuali per l'erogazione di servizi interni basati sulle funzionalità Microsoft Active Directory:

- a) CIP HQ: N° 2 x Dell PowerEdge R440
- b) CIP Circuito Tre Fontane: N° 1 HPE Microserver GEN8
- c) CIP Palazzo dell'Archivio: N° 1 HPE Microserver GEN8
- d) CIP Strutture Territoriali: Nessuna piattaforma server

L'organizzazione Active Directory prevede quindi 6 nodi locali con procedure di sincronizzazione ad anello fra i vari domain controllers in esercizio (DC01, DC02, DC03, DC04, DC05, DC06).

Ulteriori 3 virtual machines con sistema operativo Windows Server, dislocate nei nodi server fisici, sono in esercizio per la gestione delle procedure di backup e delle condivisioni interne (SRV01, SRV02, SRV03).

Di seguito un riepilogo delle VM in esercizio in termini di risorse:

CIP HQ

Nome	CPU	RAM	Storage	Sistema operativo
DC01	2 vCPU	8 GB	180 GB	WS 2016
DC02	2 vCPU	8 GB	180 GB	WS 2016
SRV01	2 vCPU	8 GB	2000 GB	WS 2016

CIP Circuito Tre Fontane

Nome	CPU	RAM	Storage	Sistema operativo
DC03	2 vCPU	8 GB	180 GB	WS 2016
DC04	2 vCPU	8 GB	180 GB	WS 2016
SRV02	2 vCPU	8 GB	180 GB	WS 2016

CIP Palazzo dell'Archivio

Nome	CPU	RAM	Storage	Sistema operativo
DC05	2 vCPU	8 GB	180 GB	WS 2016
DC06	2 vCPU	8 GB	180 GB	WS 2016
SRV03	2 vCPU	8 GB	130 GB	WS 2016

2.3 Infrastruttura Wi-Fi

CIP HQ

4 x Cisco Meraki MR18
1 x Cisco Meraki MR26
1 x Cisco Meraki MR33

CIP Circuito Tre Fontane

20 x Cisco Meraki MR33
4 x Cisco Meraki MR42
4 x Cisco Meraki MR74

CIP Palazzo dell'Archivio

5 x Open Mesh A42

L'infrastruttura wireless per le sedi sopra indicate gestisce la propagazione di diversi SSIDs:

- 1) Bridge-to-lan per la fruizione dei servizi interni attraverso connettività wireless;
- 2) Guest access su network DMZ per l'utilizzo del servizio internet con policy di bandwidth steering dedicata.

CIP Strutture Territoriali

Cisco WAP150

Per ogni Comitato Regionale è stata configurata una singola SSID accessibile tramite password statica WPA2.

2.4 Client e utenze di accesso

La gestione dei client assegnati agli utenti e relative utenze di accesso viene realizzata attraverso le funzionalità Microsoft Active Directory.

Le utenze abilitate sono quindi definite su una piattaforma centralizzata che gestisce gli accessi ai client, alle cartelle condivise ed alle stampanti in base al ruolo definito all'interno dell'organigramma aziendale.

Tutti i client abilitati all'accesso presentano sistemi operativi Microsoft PRO per i quali è attivo il rilascio diretto da parte della casa madre di aggiornamenti di sicurezza e di versione. Sono inoltre predisposti per l'accesso in rete anche alcuni client con sistemi Operativi MacOSX.

Software standard utilizzati:

- Suite Microsoft Office;
- Adobe Acrobat Reader;
- Eset Antivirus 7.0

Di seguito il numero dei client suddivisi per singole sedi:

CIP HQ: 52 client

CIP Circuito Tre Fontane: 22 client

CIP Palazzo dell'Archivio: 13 client

CIP Strutture Territoriali: 27 client

2.5 Posta elettronica

Tali servizi sono ospitati su piattaforma cloud Office 365.

Ogni utente dispone di una casella nominale e di privilegi personalizzati su caselle condivise in base al ruolo rivestito e dichiarato all'interno dell'organigramma aziendale.

Il totale delle caselle di posta elettronica attualmente attive è uguale a 292.

2.6 Gestione domini

Di seguito l'elenco dei domini registrati ed attivi per conto del Comitato:

- **comitatoparalimpico.it**
- comitatoparalimpico.com
- paralimpico.it
- festivalculturaparalimpica.com
- **festivalculturaparalimpica.it**
- festivaldellaculturaparalimpica.com
- festivaldellaculturaparalimpica.it

2.7 Backup

Ad oggi sono implementate due forme di backup:

- Versioning dei files: tali procedure garantiscono un ripristino immediato dei files oggetto di azioni involontarie da parte del personale interno;
- Backup di infrastruttura: tali operazioni eseguono il backup di tutta l'infrastruttura server a cadenza giornaliera su network storage locale attraverso applicativo dedicato.

3. OGGETTO DELL'APPALTO

Nell'ottica di un continuo miglioramento e aggiornamento tecnologico del Sistema Informativo, il Comitato si propone di:

- Ottimizzare le procedure di assistenza tecnica garantendo una copertura totalitaria;
- Rafforzare la sicurezza dei sistemi informativi interni.

Il Fornitore dovrà pertanto erogare i servizi informatici con consulenza specialistica evoluta necessari per la gestione e il mantenimento dell'infrastruttura IT del CIP per 36 mensilità di seguito elencati:

- Assistenza e manutenzione per l'intera infrastruttura IT (on-premises e cloud);
- Attività di IT Management e consulenza ICT ad ampio spettro;
- Disaster Recovery e Business Continuity;
- Backup as a Service;
- Upgrade sistemi operativi;
- Servizio di supporto telefonico dedicato alla Presidenza e alla Segreteria Generale
- Servizio di help desk remoto 24/7 per tutte le sedi;
- Servizio di help desk on site per le seguenti sedi:

- SEDE CENTRALE
Via Flaminia Nuova 830 - 00191 Roma
- CENTRO DI PREPARAZIONE PARALIMPICA
Via delle Tre Fontane 25/27/29 - 00144 Roma
- SEDE INAIL / PALAZZO DELL'ARCHIVIO CENTRALE DI STATO
P.le degli Archivi 41 – 00144 Roma

4. INFRASTRUTTURA CLOUD

Il fornitore nell'erogazione dei servizi in modalità “as a service” dovrà descrivere dettagliatamente nell'offerta progettuale le soluzioni adottate, che devono obbligatoriamente rispondere a quanto di seguito indicato:

- L'erogazione dei servizi di cui al presente Capitolato dovranno essere obbligatoriamente dislocati su sedi ubicate sul territorio comunitario ed ottemperare la Direttiva 95/46/CE del Parlamento Europeo e del Consiglio (*Tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati*). È fatto obbligo inoltre al Fornitore di trattare, trasferire e conservare le eventuali repliche dei dati conservati dai suddetti Centri Servizi sempre all'interno del territorio comunitario;
- Si richiede che il Fornitore indichi l'ubicazione dei Centri Servizi e le principali caratteristiche in termini di logistica e condizioni ambientali (es. almeno: infrastrutture di collegamento, impianto elettrico, dislocazione apparecchiature di rete e server, illuminazione, sicurezza, insonorizzazione, aerazione e impianto di climatizzazione artificiale);
- L'infrastruttura tecnologica dovrà garantire elevati livelli di integrazione, scalabilità, performance e resilienza, dovranno inoltre garantire la continuità di servizio: in caso di eventi di disastro che rendono indisponibile l'intero sito preposto all'erogazione dei servizi remoti, il Fornitore dovrà garantire la ripartenza di tutti i servizi, anche su un diverso sito;
- I Centri Servizi del Fornitore, dai quali vengono erogati i servizi del presente capitolato, devono essere interconnessi alla rete Internet attraverso connessioni ridondanti;
- Il Fornitore dovrà garantire la sicurezza delle strutture, 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. In particolare, è responsabilità del Fornitore assicurare che i Centri Servizi, le infrastrutture in esso ospitate, le informazioni gestite e le transazioni siano protette mediante l'adozione di adeguati sistemi e metodologie, nel rispetto di quanto stabilito dallo standard ISO/IEC 27001, oltre che gestite in piena conformità con la normativa cogente;
- Devono essere adottate tutte le necessarie misure volte a limitare il rischio di attacchi informatici ed eliminare eventuali vulnerabilità della rete, causate dalla violazione e utilizzo illecito di sistemi o infrastrutture del Fornitore.

- Deve essere resa disponibile un'area, accessibile via web, attraverso la quale visualizzare l'intera infrastruttura, le VM utilizzate e le relative risorse, l'utilizzo dello storage e delle risorse di rete.
- L'infrastruttura proposta deve essere dotata degli strumenti e apparati utili a garantire la sicurezza perimetrale, la prevenzione e la protezione da attacchi informatici o attacchi causati da virus. I servizi devono essere svolti nel rispetto del REGOLAMENTO (UE) 2016/679 e delle eventuali normative o regolamenti nazionali che dovessero essere emanati in materia di privacy e protezione dei dati.

5. SERVIZI DI ASSISTENZA E MANUTENZIONE

I servizi richiesti di gestione dell'infrastruttura consistono nella gestione ordinaria, manutenzione programmata, manutenzione straordinaria ed evolutiva e tutte le attività necessarie a supportare nuovi progetti applicativi e infrastrutturali. Il Fornitore dovrà eseguire tutti i controlli periodici per verificare a titolo preventivo l'alta affidabilità della infrastruttura, i livelli di performance e possibili criticità di carico.

Dovrà inoltre eseguire tutti gli aggiornamenti software (minor e major release) delle diverse componenti architetture (sistemi operativi, web server, application server, componenti network, ecc.).

Sono inoltre comprese nella gestione ordinaria le attività di patching e di migrazione alle nuove release dei prodotti, comprensive delle attività di test, degli aggiornamenti delle configurazioni applicative e degli adeguamenti dei programmi di interfaccia con gli altri sistemi. In caso di disservizio il Fornitore dovrà porre in essere tutti gli interventi correttivi sia a livello architetture, sia a livello di configurazione sistemistica ed applicativa.

Il Fornitore dovrà inoltre attivare processi di presa in carico e rilascio dei nuovi servizi per verificarne il corretto funzionamento, i livelli di performance, la sicurezza e la compatibilità con l'architettura.

A titolo indicativo e non esaustivo si segnalano le seguenti attività:

- garantire la disponibilità ed il funzionamento dell'ambiente;
- analisi dei Log dell'ambiente al fine di individuare eventuali anomalie determinate da errori e/o accessi non autorizzati.

Il Fornitore dovrà, senza alcun aggravio di costi, garantire al Comitato il rispetto dei medesimi livelli di protezione dei dati da parte dei soggetti coinvolti nell'erogazione dei servizi e in particolare dovrà:

- assicurare la riservatezza dei dati personali di cui il Comitato è titolare e il loro trattamento nel rispetto delle normative in materia di protezione dei dati personali applicabili relativamente a ogni territorio nel quale vengano localizzati i servizi;
- garantire il rispetto di adeguate misure di sicurezza volte alla protezione dei dati personali, nel rispetto della normativa di riferimento (Reg. UE 2016/679 – GDPR in primis) prestando in particolar modo adeguate garanzie in merito alla distruzione, alla perdita e alla prevenzione di accessi non autorizzati ai dati del Comitato da parte di terzi, prevedendo idonee procedure di notificazione al Committente da parte dei soggetti coinvolti nell'erogazione dei servizi in caso di accesso abusivo, sottrazione e perdita dei dati, così come per qualsiasi richiesta giuridicamente vincolante presentata da autorità giudiziarie o di polizia ai fini della comunicazione di dati personali;
- garantire che i soggetti coinvolti nell'erogazione dei servizi accettino la nomina a "responsabile esterno del trattamento", ottemperino alle istruzioni ivi previste dal

Committente e rispondano prontamente e adeguatamente a tutte le richieste del Committente relative al trattamento dei dati personali;

- garantire l'adempimento delle disposizioni in materia di amministrazione di sistema da parte dei soggetti coinvolti nell'erogazione dei servizi, ove applicabili;
- garantire al Committente la possibilità di effettuare adeguate procedure di audit e svolgere per conto del Committente le medesime procedure di controllo nei confronti dei soggetti coinvolti nell'erogazione dei servizi;
- assicurare un livello adeguato di formazione del personale chiamato ad interagire o comunque coinvolto nei processi di erogazione dei servizi;

5.1. Monitoraggio

È richiesto un servizio di monitoraggio e assistenza, 24 ore su 24 per 7 giorni su 7 dei servizi in produzione. Esso dovrà comprendere la gestione sistemistica e il monitoraggio hardware e software di tutti i server e apparati networking. Eventuali guasti hardware o la mancata raggiungibilità dei server comporteranno l'intervento proattivo del personale tecnico.

Il sistema di monitoraggio proposto dovrà effettuare il controllo di disponibilità dell'infrastruttura, la verifica puntuale e tracciata della disponibilità dei servizi e delle performance delle principali applicazioni indicate dal Comitato, attraverso simulazioni di accesso e di effettivo utilizzo lato utente. È inoltre richiesto il monitoraggio del sistema di firewalling atto a rilevare eventi di intrusione e la conseguente tempestiva gestione degli eventuali incidenti di sicurezza.

E' richiesta inoltre l'interfaccia diretta del Fornitore con i provider del servizio di connettività Internet e centralino telefonico VoIP affidatari per le diverse sedi o altri gestori di servizi informatici attivati dal Comitato che comportino interazione con l'infrastruttura IT e i relativi utenti, nonché la configurazione e gestione delle apparecchiature di stampa (stampanti, multifunzioni, plotter, fotocopiatrici, etc...) presso tutte le sedi del Comitato.

5.2. Servizi gestione infrastruttura e Cloud

Di seguito un elenco dei servizi minimi richiesti per la gestione dell'infrastruttura:

- Gestione sistemistica comprensiva delle operazioni di ottimizzazione delle risorse e di configurazione della sicurezza nonché del monitoraggio delle prestazioni generali dei sistemi;
- Gestione sistemistica e amministrativa dei profili utente su posta, documentali e DC;
- Gestione degli ambienti virtualizzati;
- Gestione dei domini attivi e dei servizi ad essi correlati;
- Gestione policy per l'accesso alle risorse;
- Gestione dei backup ridondato;
- Gestione completa dei sistemi antivirus, antispamming in linea con le politiche di sicurezza e di controllo definite dal Comitato;
- Gestione completa del patch management;
- Gestione completa e monitoraggio delle Infrastrutture e Sistemi interni;
- Monitoraggio delle prestazioni generali dei sistemi;
- Risoluzione di tutti i problemi di funzionalità e disponibilità degli ambienti server e networking, ivi comprese le azioni correttive finalizzate a prevenire malfunzionamenti o disservizi;
- Garantire l'adozione delle adeguate misure di sicurezza logica ovvero sicurezza dei dati, programmi e procedure dal rischio di perdita, alterazione o distruzione o dall'accesso non autorizzato da parte di terzi ai dati di proprietà del Comitato;

- Aggiornamenti periodici delle release del software in uso e dei sottosistemi, anche nel caso di prodotti software di proprietà del Comitato;

5.3. Servizi di manutenzione e gestione ordinaria dell'ambiente applicativo

5.3.1. Posta elettronica/antispamming

Il Fornitore dovrà garantire l'esecuzione di tutte le attività di normale gestione legate alla creazione e manutenzione delle caselle di posta (ad es: attività di creazione, eliminazione, modifica delle cassette postali, gestione delle liste di distribuzione, ecc.); inoltre, in accordo con il Comitato, il Fornitore dovrà gestire le policy relative all'ambiente antispamming. In carico al Fornitore saranno inoltre tutte le configurazioni prettamente sistemistiche sulla piattaforma Exchange Online.

5.3.2. Gestione Domini

Di seguito un elenco di attività non esaustivo inerente la gestione dei domini:

- Controllo completo delle impostazioni DNS;
- i domini dovranno essere trasferiti e diventare di completa gestione del fornitore;
- il trasferimento deve garantire l'assenza di disservizio per tutti i servizi pubblici basati su servizio DNS, come siti web, posta elettronica e posta elettronica certificata;
- i dati di registrazione del dominio (REGISTRANT/ADMIN/TECH) dovranno essere aggiornati in base alle istruzioni ricevute dal Comitato Italiano Paralimpico.

5.3.3. Microsoft Active Directory

Il Fornitore, attraverso la gestione delle infrastrutture descritte nei precedenti articoli, dovrà garantire la corretta configurazione e ottimizzazione dell'intera architettura applicativa, la diagnostica delle performance e la verifica delle componenti applicative; dovrà garantire il funzionamento del servizio di autenticazione e di provisioning delle identità anche attraverso le politiche di Business Continuity e Disaster Recovery.

5.3.4. Servizio Antivirus

Nell'esecuzione di tutti i Servizi descritti nel presente documento, il Fornitore dovrà porre la massima attenzione alle problematiche di sicurezza degli ambienti e degli utenti. In particolare, dovrà farsi carico, per tutta la durata del contratto, di installare e gestire un sistema antivirus per garantire la protezione dei server e delle postazioni di lavoro. A titolo esemplificativo ma non esaustivo, si segnalano le seguenti attività:

- garantire la disponibilità dell'ambiente antivirus;
- garantire l'aggiornamento delle impronte virali, motori di scansione e programmi come da specifiche del Fornitore del prodotto (anche per i singoli client);
- intervenire tempestivamente in caso di diffusione di virus con lo scopo di ripristinare la normale funzionalità di tutto l'ambiente;
- eseguire l'aggiornamento delle release di prodotto.

6. BACKUP AS A SERVICE

Il Fornitore dovrà implementare un Servizio *BaaS* con le seguenti caratteristiche:

- La piattaforma dovrà rispettare i requisiti di riservatezza, integrità, disponibilità e resilienza dei sistemi;
- La conservazione dei dati dovrà avvenire all'interno dei confini geografici della UE oppure in paesi convenzionati con il Decreto UE 679/2016;

- Il servizio dovrà essere completamente indipendente rispetto alle soluzioni di backup ad oggi in esercizio;
- Il sistema sarà configurato per garantire l'esecuzione delle attività di backup a cadenza giornaliera con una *retention policy* utile alla conservazione delle ultime 3 copie;
- La configurazione del servizio prevederà un salvataggio dei dati di tipo full, ossia backup basati su immagini remotizzate.
- Il sistema dovrà essere sottoposto a costante monitoraggio per garantire il corretto espletamento delle attività;
- Le schedulazioni dovranno avvenire in maniera trasparente, senza impatto sulle quotidiane attività del Comitato.

7. DISASTER RECOVERY E BUSINESS CONTINUITY

Il Fornitore si occuperà dell'erogazione al Comitato del servizio DR che, utilizzando un'apposita infrastruttura realizzata e gestita dallo stesso a suo carico, totalmente esterna ai nodi fisici dell'infrastruttura del Committente, assicuri il ripristino della disponibilità e funzionalità del sistema informativo, inteso come complesso di strutture hardware, software, applicazioni e servizi ICT, nel caso in cui tali funzionalità diventassero inutilizzabili a causa di eventi disastrosi o calamitosi, in caso di switch-over ovvero in occasione di lavori di manutenzione ordinaria e straordinaria dello stabile o degli impianti tecnologici che richiedano lo spegnimento dei sistemi di esercizio. Il servizio DR deve inoltre garantire una adeguata procedura di fail-back, cioè di rientro dalla situazione di emergenza, in modo che sia nulla la perdita di dati nel processo e sia minimizzato il tempo di fermo dei sistemi necessario per il rientro.

Il Fornitore potrà integrare quanto richiesto nel presente Capitolato offrendo servizi aggiuntivi, prodotti e/o risorse, non esplicitamente previsti, che consentano di migliorare l'erogazione e/o la qualità del servizio DR.

8. SERVIZIO DI HELP-DESK REMOTO E ON-SITE

È richiesto un servizio di Help Desk (remoto e on site) e di assistenza sistemistica su tutto il sistema strutturato su due livelli:

- Help Desk di primo livello;
- Help Desk di secondo livello.

Il servizio dovrà essere disponibile H24, 7 giorni su 7.

Il Fornitore dovrà implementare un sistema di Trouble Ticketing destinato a ricevere le richieste di assistenza e le segnalazioni di eventuali problematiche inerenti ai servizi offerti.

Il Fornitore dovrà garantire al committente l'attività di Help Desk on-site a cadenza settimanale con interventi quattro ore continuative (dalle 9:00 alle 13:00 ovvero dalle 14:00 alle 18:00) così suddivisa:

- CIP HQ: 12 ore settimanali;
- CIP Circuito Tre Fontane: 4 ore settimanali;
- CIP Palazzo dell'Archivio: 4 ore settimanali.

L'organizzazione del supporto on-site sarà concordata direttamente con il committente in base alle effettive necessità operative del Comitato.

Attualmente si ipotizza la seguente ripartizione degli interventi:

LUNEDI'	MARTEDI'	MERCOLEDI'	GIOVEDI'	VENERDI'
9:00/13:00	9:00/13:00	9:00/13:00	9:00/13:00	9:00/13:00
HQ	TRE FONTANE	HQ	PALAZZO DELL'ARCHIVIO	HQ

Le attività di assistenza on-site saranno da considerarsi nel riquadro completo del servizio di Help Desk che invece non avrà limiti temporali in termini di ore settimanali.

Per quanto concerne il servizio di Help Desk per i Comitati Regionali, l'Aggiudicatario garantirà il livello di supporto FULL attraverso assistenza remota mentre, per interventi on-site di tipo "specialist" sarà aggiunta una franchigia di € 100 per il trasporto e € 50/giorno per l'alloggio.

Esclusivamente per la Presidenza e la Segreteria Generale del CIP (max 8 utenti) dovrà essere predisposto un servizio di supporto telefonico, attivo nei giorni lavorativi dalle ore 08.15 alle ore 18.00.

8.1. Help-Desk di primo livello

L'HD di primo livello è responsabile della ricezione della segnalazione - che oltre al suddetto sistema di Trouble Ticketing, potrà essere inoltrata anche via mail o telefono - della registrazione, classificazione e inoltro delle richieste di intervento provenienti dal Comitato o dalle segnalazioni dai sistemi di monitoraggio; svolgerà, nell'arco temporale di un'ora dalla segnalazione, con le opportune competenze, le seguenti funzioni (a titolo indicativo e non esaustivo):

- Risposta ad eventuali richieste di informazioni tecniche di base sul servizio;
- Prima analisi e risoluzione delle problematiche più semplici;
- Controllo dello stato di avanzamento dei ticket, la relativa chiusura e la comunicazione al Comitato.

Il personale dell'HD di primo livello gestirà i contatti, fornirà le informazioni richieste, prenderà in carico segnalazioni di problematiche e deciderà l'eventuale inoltro all' HD di secondo livello qualora non possa intervenire direttamente. Nel caso di risoluzione delle problematiche direttamente da parte del primo livello di assistenza, questo provvederà ad aggiornare il ticket con le informazioni sul contatto e a chiuderlo.

Le funzioni richieste all' HD di primo livello sono:

- Creazione e Presa in carico delle richieste;
- Analisi della richiesta;
- Gestione di Incident e Request;
- Eventuale riclassificazione delle richieste (in caso di erronea classificazione);
- Eventuali approfondimenti con l'utente Finale che ha generato la richiesta;
- Individuazione della soluzione definitiva o di un workaround;
- Innesco delle procedure di escalation (nel caso di impossibilità a chiudere la richiesta);
- Tracciatura della richiesta;
- Inoltro della Risposta/Soluzione per la chiusura del Ticket (Resolved).

8.2. Help desk di secondo livello

L'HD di secondo livello viene erogato dagli specialisti ai quali il l'HD di primo livello inoltra gli Incident ed i Problem che non hanno trovato una soluzione.

Le funzioni e garanzie richieste all' Help Desk di secondo livello sono:

- Garantire il livello di servizio concordato;
- Gestire i processi di Incident e Problem Management sino alla definitiva soluzione;
- Gestire le attività di ripristino dell'infrastruttura del Comitato;
- Analizzare, pianificare e realizzare i Change autorizzati;

- Disporre di risorse con skill specialistici per ambito tecnologico;
- Esercire l'infrastruttura del Fornitore (in perimetro);
- Effettuare la revisione periodica del Capacity Planning per le varie risorse infrastrutturali e, in caso di necessità gestire il deploy delle migliorie d'applicare;
- Garantire la System Administration degli apparati di rete e dei sistemi;
- Garantire il Servizio di Reperibilità;
- Effettuare le attività di Change dopo averle pianificate e concordate con il Comitato.

9. UPGRADE SISTEMI OPERATIVI

Il Fornitore si occuperà di upgrade dei sistemi operativi client per i quali non è ulteriormente previsto il rilascio di *Security patches* dalla casa madre, oggetto di tale attività sono attualmente 40 client ca. dislocati fra tutte le sedi a livello nazionale.

Resta inteso quanto segue:

- I costi inerenti licenze ed eventuale hardware aggiuntivo saranno a carico del Comitato;
- E' onere del Fornitore effettuare un'analisi mirata sullo stato dei client notificando al committente la quantità di client oggetto di upgrade e relativi costi in termini di hardware e licenze da sostenere;
- Il Fornitore proporrà al Comitato una schedulazione utile al completamento delle attività, la stessa sarà validata dal Fornitore in base alle disponibilità ed al carico di lavoro degli utenti;
- Il Fornitore si occuperà in autonomia delle procedure di backup e di ripristino delle configurazioni utili a garantire il corretto flusso lavorativo degli utenti finali.

10. ATTIVITÀ DI IT MANAGEMENT E CONSULENZA ICT

Il Fornitore supporterà il Comitato nel processo di eventuale aggiornamento ed evoluzione informatica, con particolare riferimento, a titolo esemplificativo, alle tematiche di seguito indicate, anche attraverso la produzione di studi di fattibilità economica e tecnica che consentiranno al CIP di individuare le migliori soluzioni offerte dal mercato nel rispetto delle norme di legge vigenti in materia:

- **Cyber Security:** consulenza per aumentare il livello di protezione della rete interna implementando soluzioni ad-hoc per il monitoraggio, prevenzione e blocco;
- **Infrastruttura server:** aggiornamento Hardware e Software con ottimizzazione delle risorse;
- **Infrastruttura backup:** ottimizzazione delle procedure di backup as a service e implementazione di infrastruttura di Disaster Recovery;
- **Piattaforma E-procurement:** supporto nella gestione dei procedimenti di utilizzo delle piattaforme E-procurement con particolare riferimento alla piattaforma CONSIP acquistinretepa.it per affidamenti di Convenzioni, Accordi quadro, MEPA e SDAPA, ai sensi delle normative vigenti;
- **Digitalizzazione PA:** consulenza sui processi di digitalizzazione della pubblica amministrazione ai sensi delle normative vigenti;
- **Portale Fornitori:** consulenza nella realizzazione di un sito web (miniportale) dedicato all'iscrizione all'Albo Fornitori CIP ed alle procedure di gara da proporre ai propri fornitori qualificati, ai sensi della normativa vigente;
- **Centralizzazione Informatica:** consulenza per la centralizzazione informatica delle strutture CIP, con particolare riferimento agli Organi Territoriali ed ai servizi informatici loro offerti.

L'affidamento di eventuali servizi discendenti dall'attività di IT Management e Consulenza ICT sono esclusi dal presente appalto e saranno oggetto di apposite procedure, secondo le norme di legge vigenti in materia.

11. INTERVENTI DI MANUTENZIONE STRAORDINARIA

Qualora si rendessero necessari interventi in esubero rispetto a quelli indicati nel presente Capitolato che, per cause non imputabili al Fornitore, non potranno essere sostenuti nell'ambito del Contratto sottoscritto tra le parti, gli stessi saranno considerati interventi di manutenzione straordinaria e potranno essere oggetto di eventuale offerta da parte del Fornitore in base alle necessità specifiche rilevate in corso d'opera e dovranno essere accordati dal CIP attraverso specifica lettera d'ordine, a titolo esemplificativo e non esaustivo, riferiti alle tipologie di seguito indicate:

a) acquisto o riparazione di materiale informatico hardware, fornitura o abbonamento a software e licenze, registrazione e gestione di licenze e domini web, laddove non sia obbligatorio il ricorso alle convezioni CONSIP o al Mercato Elettronico della Pubblica Amministrazione;

b) interventi straordinari on site presso la Sede centrale del CIP, il Centro di Preparazione Paralimpica, il Palazzo dell'Archivio Centrale di Stato, le strutture territoriali del CIP o in occasione di eventi e manifestazioni su tutto il territorio nazionale.

Si specifica che il Comitato si riserva di affidare gli interventi di manutenzione straordinaria di cui al presente articolo ad altro Fornitore.

Le suddette ulteriori attività che potranno essere remunerate utilizzando le eventuali somme a disposizione derivanti dal ribasso offerto in sede di RDO dall'aggiudicatario, ovvero, previo ulteriore stanziamento da parte del CIP secondo le previsioni di legge.

12. FIGURE PROFESSIONALI

12.1 Il Fornitore dovrà nominare un proprio Responsabile di Progetto al quale saranno affidate le mansioni di supervisione e coordinamento delle attività svolte dal Fornitore stesso nell'esecuzione del contratto, coordinandosi con il Direttore dell'esecuzione nominato dal Comitato e con il DPO dello stesso.

Il Responsabile di Progetto del Fornitore (Capo Progetto) rappresenterà il referente unico del Direttore dell'esecuzione nominato dal Comitato ed assicurerà, tra l'altro, la necessaria assistenza consulenziale al Comitato, anche al fine di definire le interazioni con sistemi di organizzazioni sociali, enti ed istituzioni.

12.2 Profili professionali richiesti

Per le attività previste nell'erogazione dei servizi dovranno essere impiegate figure professionali adeguate in termini di competenze e numerosità per la realizzazione delle attività progettuali.

Le figure professionali proposte dovranno fare riferimento ai profili descritti, fermo restando l'obbligo per il Fornitore ad erogare i servizi richiesti anche a fronte di significative variazioni del contesto tecnologico di inizio fornitura, adeguando le conoscenze del personale impiegato nell'erogazione dei servizi o inserendo nei gruppi di lavoro risorse con skill adeguato, senza alcun onere aggiuntivo per il Comitato.

Il team sarà composto da figure professionali altamente specializzate e competenti proprio negli ambiti dei servizi richiesti ed in possesso di un'approfondita conoscenza degli ambienti tecnologici, così come delle possibili problematiche relative alla erogazione dei servizi oggetto di gara.

12.2.1 – Requisiti generali

Di seguito si riporta un elenco non esaustivo delle competenze tecniche e le principali competenze trasversali e normative

TECNOLOGIE E STRUMENTI:

- Tecnologie di virtualizzazione;
- Sistemi di cloud computing;
- Infrastrutture complesse ed eterogenee, basate su VMware, GNU/Linux e Windows;
- Gestione domini Windows Server, Active Directory
- Sistemi Documentali;
- Web server e Application server;
- Prodotti di grafica e grafica Web;
- Sistemi di Identity and Access Management;
- Strumenti di crittografia, firma digitale, firma digitale remota, firma elettronica, firma elettronica avanzata, marche temporali, e sicurezza.

12.2.2 - Piano di impiego delle figure professionali

Il Fornitore dovrà garantire l'impiego di figure professionali adeguate in termini di competenze e numerosità. Il gruppo di lavoro dovrà comprendere necessariamente almeno una figura per ognuno dei seguenti profili professionali:

- Capo progetto
- Specialista di Tecnologia/Prodotto
- Sistemista senior

Le conoscenze indicate nei prospetti delle diverse figure professionali devono essere presenti nel complesso delle risorse professionali richieste dal Committente sulle diverse attività e/o servizi e non in un'unica persona.

13. LIVELLI DI SERVIZIO RICHIESTI E PENALI

13.1 Uptime dell'infrastruttura cloud

Aspetto da valutare: Disponibilità Infrastruttura (risorse hw, servizi virtuali creati ed allocati e disponibilità dei nodi fisici (server) che ospitano l'infrastruttura virtuale)

Unità di misura: Minuti

Soglia $\geq 99,95\%$ per anno

Penale: L'indisponibilità della infrastruttura a supporto della erogazione dei servizi per un tempo complessivo superiore o uguale al valore soglia di Uptime richiesto, costituisce disservizio e comporta l'emissione di una penale pari allo 0,5% (zero virgola cinque) dell'importo complessivo del servizio di riferimento nel contratto esecutivo di fornitura per ogni 0,01% (zero virgola zero uno per cento) in diminuzione rispetto al valore soglia.

13.2 Rispetto dell'RTO (Recovery Time Objective) per DC

Aspetto da valutare: Rispetto del RTO nel caso di evento di disastro che rende indisponibile il Centro Servizi, per cause non imputabili al Fornitore.

Unità di misura: Ore

Soglia ≤ 48

Penale: Il superamento del valore di soglia comporta l'applicazione della penale pari allo 0,5% (zero virgola cinque) dell'importo complessivo del contratto esecutivo di fornitura per ogni 24 hh di ritardo.

13.3 Rispetto dell'RTO (Recovery Time Objective)

Aspetto da valutare: Rispetto del RTO nel caso di evento di disastro gestito dal servizio di Disaster Recovery.

Unità di misura: Minuti

Soglia <= 10

Penale: Il superamento del valore di soglia comporta l'applicazione della penale pari allo 0,2% (zero virgola due) dell'importo complessivo del contratto esecutivo di fornitura.

13.4 HELP DESK

1 - Intervento tramite assistenza remota per CIP HQ e sedi remote:

1.1	Tempo massimo di attesa per la presa in carico delle segnalazioni	Max 30 min
1.2	Tempo Massimo per la gestione della segnalazione STANDARD	4 (quattro) ore lavorative
1.3	Tempo Massimo per la gestione della segnalazione URGENTE	2 (due) ore lavorative

2 - Intervento tramite assistenza on-site per CIP HQ, CIP Circuito Tre Fontane e CIP Palazzo dell'Archivio:

2.1	Tempo massimo di attesa per la presa in carico delle segnalazioni	Max 30 min
2.2	Tempo Massimo per la gestione della segnalazione STANDARD	8 (otto) ore lavorative
2.3	Tempo Massimo per la gestione della segnalazione URGENTE	4 (quattro) ore lavorative

3 - Intervento tramite assistenza on-site per le Strutture Territoriali:

3.1	Tempo massimo di attesa per la presa in carico delle segnalazioni	Max 30 min
3.2	Tempo Massimo per la gestione della segnalazione STANDARD	2 gg. lavorativi
2.3	Tempo Massimo per la gestione della segnalazione URGENTE	1 gg. lavorativo

Il superamento delle soglie comporta l'applicazione della penale pari allo 0,1% (zero virgola uno per cento) dell'importo complessivo del contratto esecutivo di fornitura.

Se il ritardo dovesse superare il decimo giorno senza che il fornitore abbia provveduto alle attività richieste, il CIP, oltre al diritto di applicare le penalità maturate, si riserva la facoltà insindacabile di risolvere il Contratto ai sensi dell'art. 1456 del Codice civile, fermo restando il diritto al risarcimento di ogni danno subito.

14. DICHIARAZIONE DI CONFORMITA' AL GDPR

Il Fornitore si impegna a rilasciare entro trenta giorni dall'avvio dell'erogazione dei servizi di cui al presente Capitolato al DPO nominato dal Comitato una dichiarazione di conformità al REGOLAMENTO (UE) 2016/679 (noto come GDPR) dell'infrastruttura IT secondo il facsimile di seguito riportato, ovvero indicare le eventuali misure da implementare:

1. Il sottoscritto _____ nella qualità di legale rappresentante della _____, con riferimento allo stipulando contratto con il CIP, Comitato Italiano Paralimpico, avente ad oggetto l'attività di assistenza e consulenza informatica specialistica evoluta per il quadriennio 2021/2023 dichiara che, in esecuzione delle prestazioni di cui al citato contratto ed in relazione ai servizi ivi disciplinati, con riferimento alle operazioni di trattamento di dati personali poste in essere dal CIP, quale Titolare del trattamento, *verranno implementate*, tutte le misure tecniche e organizzative adeguate ai fini dell'assolvimento da parte del CIP degli obblighi di cui all'articolo 32 del GDPR.
2. Dichiara inoltre:
 - che le suddette misure tengono conto dello stato dell'arte, dei costi di implementazione e natura, scopo, contesto e finalità di trattamento dei dati personali nonché della probabilità e gravità di violazioni ai diritti e alle libertà di persone fisiche e sono atte a garantire un livello adeguato di sicurezza rispetto al rischio;
 - che nella valutazione del livello di sicurezza sono stati presi in considerazione i rischi derivanti dalle operazioni di trattamento che, accidentalmente o in modo illecito, possano comportare la distruzione, la perdita, la modifica, la comunicazione non autorizzata o l'accesso a dati personali trasmessi, memorizzati o altrimenti trattati.
3. Stante quanto sopra, dichiara altresì che:
 - le seguenti misure vengono implementate per garantire la pseudonimizzazione dei dati personali

 - le seguenti misure vengono implementate per attuare la cifratura dei dati personali

 - le seguenti misure vengono implementate per garantire la riservatezza dei sistemi di trattamento e dei servizi;

 - le seguenti misure vengono implementate per garantire l'integrità dei sistemi di trattamento e dei servizi;

 - le seguenti misure vengono implementate per garantire la disponibilità dei sistemi di trattamento e dei servizi;

 - le seguenti misure vengono implementate per garantire la resilienza dei sistemi di trattamento e dei servizi;

 - verranno applicate procedure volte a testare l'efficacia delle misure adottate.

Roma 01/09/2020

Il Responsabile Unico del Procedimento
Flavio Caprarelli
(originale sottoscritto)