Capitolato Tecnico per la fornitura del servizio di gestione del Network Operation Center

NOC

Sommario

1. OGGETTO DELL'APPALTO 4
2. CONTESTO ORGANIZZATIVO 5
3. RISORSE MESSE A DISPOSIZIONE DALL'ENTE 6
4. MODELLO GENERALE DI ORGANIZZAZIONE DEI SERVIZI IN USO PRESSO L'ENTE 7
5. COMPONENTI DELLA FORNITURA 9
5.1 COMPONENTI TRASVERSALI A TUTTI I LOTTI 9
5.2 LOTTO-1 – Infrastruttura di Rete e Fonia 9
5.3 LOTTO-2 – Infrastruttura Tecnologica e Posta Elettronica 10
5.4 LOTTO-3 – Sicurezza 10
5.5 Coordinamento operativo tra i Lotti 11
6. RUOLI E COMPETENZE DELLE RISORSE PROFESSIONALI RICHIESTE 12
6.1 FIGURE TRASVERSALI A TUTTI I LOTTI 12
6.1.1 Responsabile del Contratto (Account Manager) 12
6.1.2 Responsabile di Progetto (Project Manager) 12
6.1.3 Coordinatore del servizio (Service Manager) 13
6.2 LOTTO-1 – Infrastruttura di Rete e Fonia 13
6.2.1 Sistemista di Rete 13
6.2.2 Sistemista di Fonia 14
6.3 LOTTO-2 – Infrastruttura Tecnologica e Posta Elettronica 15
6.3.1 Sistemista Server 15
6.3.2 Sistemista Sistemi di Infrastruttura 16
6.3.3 Sistemista di Posta 17
6.4 LOTTO-3 – Sicurezza 18
6.4.1 Specialista di Cyber Security 18
6.5 Composizione del Presidio dedicato 19
6.6 Aggiornamento Professionale e Corsi di Formazione 19
6.7 Comitato di Controllo (CC) 19
7 DESCRIZIONE DEI SERVIZI IN FORNITURA 21
7.1 LOTTO 1 e 2 – Infrastruttura di Rete e Fonia e Infrastruttura Tecnologica e Posta Elettronica 21
7.1.1 Servizio di gestione dei sistemi e delle infrastrutture 21
7.1.2 Strutturazione dei Servizi richiesti in Fornitura 22
7.1.2.1 Monitoring Management 22
7.1.2.2 Local Monitoring 23
7.1.2.3 Remote Monitoring 23
7.1.2.4 Service Transition Management 24
Responsabilità chiave 24
Competenze richieste 24
7.1.2.5 Change Management 24
7.1.2.6 Configuration Management 26
7.1.2.7 Release and Deployment Management 27
7.1.2.8 Attività straordinarie 28
7.1.2.9 Transition Planning and Support 29
7.1.2.10 Service Validation and Testing Management 29
7.1.2.11 Knowledge Management 31
7.1.2.12 Incident Management e Problem Management 31
7.1.2.13 Backup Management 34
7.1.2.14 Gestione Logistica 34
7.1.2.15 Licensing Management 35
7.1.2.16 Performance Management 35

Piazza Ospedale Maggiore, 3 20162 Milano – Tel. 02 6444.1 – Fax 02 6420901- C.F. e P.I. 11390840152 - www.ospedaleniguarda.it

7.1.2.17 Reporting 36
7.1.2.18 Presidio locali tecnici 36
7.1.2.19 Apparati gestiti 37
7.1.2.20 Consulenza 37
7.1.3 Servizio di gestione degli asset 37
7.1.4 Servizio di provisioning 38
7.2 LOTTO-3 – SICUREZZA 39
7.2.1 Servizio di gestione della sicurezza 39
7.2.2. Test violazione sicurezza 40
7.2.3 Controllo degli accessi di rete 41

8 LIVELLI DI SERVIZIO 43
8.1 Livelli di servizio SLA 43

8 PIANO DI COMUNICAZIONE 45
9.1 Matrice di Coordinamento 45
9.2 Riunioni di coordinamento 45
9.2.1 Modalità 45
9.2.2 Scopo 46
9.2.3 Report sullo Stato di Avanzamento Lavori (SAL) 46
9.2.4 Diagrammi di GANTT e pianificazione risorse 46
9.2.5 Report di Eccezione 47
9.2.6 Interfaccia con l'Ente ed "Escalation Path" 47

10 PROCEDURE E STANDARD DI QUALITÀ 48
10.1 Procedure generali tra il Fornitore e l'Ente 48
10.1.1 Tipologia delle segnalazioni 48
10.1.2 "Follow up" delle azioni 48
10.2 Standard per la produzione di documentazione 48
10.2.1 Formato di un documento 48
10.2.2 Linguaggio dei Documenti 49

11 PIANO DI IMPLEMENTAZIONE 50
11.1 System Audit 50
11.2 Installazione 51
11.3 Avviamento 51

12 EXIT MANAGEMENT 52

13 ALLEGATI 55
13.1 Indicazioni di lettura del documento 55

Piazza Ospedale Maggiore, 3 20162 Milano – Tel. 02 6444.1 – Fax 02 6420901- C.F. e P.I. 11390840152 - www.ospedaleniguarda.it

1. OGGETTO DELL'APPALTO

Oggetto del presente capitolato è la fornitura in outsourcing per **cinque (5) anni** delle **Piattaforme e dei Servizi** come di seguito indicato:

LOTTO	DESCRIZIONE	
1	Servizio di gestione Infrastruttura di Rete	Piattaforma di Monitoraggio e Piattaforma di Trouble Ticketing
	Servizio di gestione Infrastruttura di Fonia	
2	Servizio di gestione Infrastruttura di Server Farm	Piattaforma di Monitoraggio e Piattaforma di Trouble Ticketing
	Servizio di gestione Sistema di Infrastruttura	
	Servizio di gestione Sistema di Posta	
3	Servizio di Cyber Security	Piattaforma di Monitoraggio e Piattaforma di Trouble Ticketing

per i seguenti Enti:

a) ASST Niguarda (**NIG);**
b) ASST Gaetano Pini (**IOGP**);
c) Fondazione IRCCS Istituto Nazionale dei Tumori (**INT**);
d) Fondazione IRCCS Istituto Neurologico Carlo Besta (**BESTA**).

Nel prosieguo con la parola **Ente** si indicherà complessivamente NIG, INT, IOGP e BESTA, laddove non diversamente specificato.
Con il termine **Sistema** si indicherà l'insieme delle Piattaforme e dei Servizi indicati dal **punto 1) al punto 9).**

La fornitura delle singole componenti (Piattaforme e Servizi) del **Sistema** possono essere **opzionale** (OPZ) o meno in base a quanto indicato da ciascun Ente nel proprio allegato tecnico di dettaglio.

Il Fornitore potrà **candidarsi** per la gestione **di uno o più LOTTI** e dovrà prevedere la gestione di tutte le componenti del **Sistema** presenti nello specifico LOTTO. Il Fornitore dovrà inoltre dotarsi di un sistema di archiviazione dei dati ed informazioni relative agli asset inclusi nel relativo LOTTO, mediante un Data Base relazionali modello CMDB (Configuration Management Data Base).
Tale strumento con accesso WEB dovrà essere conforme a quanto richiesto dalla direttiva NIS2.

Gli strumenti necessari ad implementare tali servizi devono essere preferibilmente virtualizzati e forniti unitamente alla piattaforma utilizzata (Hw e SW a carico del Fornitore), tali strumenti devono essere gestiti in completa autonomia dal Fornitore stesso.

Piazza Ospedale Maggiore, 3 20162 Milano – Tel. 02 6444.1 – Fax 02 6420901- C.F. e P.I. 11390840152 - www.ospedaleniguarda.it

2. CONTESTO ORGANIZZATIVO

La sede principale dell'ASST Niguarda è situata a Milano in Piazza Ospedale Maggiore 3. L'elenco delle sedi esterne è dettagliato nell'Allegato Tecnico 1.
La sede principale della Fondazione IRCCS "Istituto Nazionale dei Tumori" è situata a Milano in via Venezian 1, i distaccamenti sono situati in largo Murani (Cascina Rosa), via Amadeo 42, via Ponzio 44.
La sede principale dell'ASST Gaetano Pini è situata a Milano in Piazza A. C. Ferrari, 1 con il polo Riabilitativo ubicato in via Isocrate 19.
La sede principale della Fondazione IRCCS Istituto Neurologico Carlo Besta è situata a Milano in via Giovanni Celoria 11.

Maggiori informazioni sono disponibili in:

- **Allegato Tecnico 1 – ASST Grande Ospedale Metropolitano Niguarda;**
- **Allegato Tecnico 2 – ASST Gaetano Pini;**
- **Allegato Tecnico 3 – IRCCS Istituto Nazionale dei Tumori;**
- **Allegato Tecnico 4 – IRCCS Istituto Neurologico Carlo Besta.**

Le informazioni fornite negli Allegati dei vari Enti sono da intendersi come indicative al fine di mettere il Fornitore in condizione di formulare una proposta correttamente dimensionata.

Piazza Ospedale Maggiore, 3 20162 Milano – Tel. 02 6444.1 – Fax 02 6420901- C.F. e P.I. 11390840152 - www.ospedaleniguarda.it

3. RISORSE MESSE A DISPOSIZIONE DALL'ENTE

Per perseguire le finalità del progetto **l'Ente** mette a disposizione del Fornitore le seguenti risorse:

- Infrastruttura di rete e fonia, infrastruttura di server farm, sistema d'infrastruttura e sistema di posta elettronica dettagliatamente descritti negli allegati tecnici di dettaglio.
- Documentazione tecnica relativa al NOC.
- Locali arredati ad uso del Presidio on-site, le **PDL** (Postazioni di Lavoro) si intendono a carico del Fornitore.
- Locali magazzino che dovranno essere gestiti in completa autonomia dal Fornitore.
- Referente dell'Ente per il servizio in oggetto.
- Collegamento Internet non dedicato.

L'Ente si riserva di acquistare in autonomia sul mercato componenti aggiuntivi e/o sostitutivi relative ai **Servizi** oggetto del capitolato (apparati/server di rete, apparati/server di fonia, terminali telefonici, software, etc.) concordando preventivamente con il Fornitore le caratteristiche generali.
Sarà responsabilità del Fornitore prendere in carico tali componenti aggiuntivi e/o sostitutivi, procedere all'installazione, configurazione ed alla successiva assistenza secondo il modello dei servizi in fornitura, successivamente al collaudo positivo e congiunto (Fornitore Ente).
Tutti i componenti aggiuntivi acquisiti dall'Ente durante il periodo contrattuale e presi in carico dal Fornitore comporteranno la rivalutazione dei relativi canoni alle condizioni del § 13 – Estensione o riduzione del contratto.

Piazza Ospedale Maggiore, 3 20162 Milano – Tel. 02 6444.1 – Fax 02 6420901- C.F. e P.I. 11390840152 - www.ospedaleniguarda.it

4. MODELLO GENERALE DI ORGANIZZAZIONE DEI SERVIZI IN USO PRESSO L'ENTE

I servizi richiesti in fornitura si inquadrano ed interagiscono nel modello generale di organizzazione già in uso presso l'**Ente**. Tale modello è di seguito descritto.
Le modalità di integrazione dei servizi in fornitura con gli altri servizi già in uso presso l'Ente sono indicate al § 7 – Descrizione dei servizi in fornitura.
Il modello è uno schema classico di supporto a più livelli. Prevede che un Service Desk (**SD**) di primo livello riceva le chiamate di assistenza e le richieste da parte degli utenti. Il SD qualifica la chiamata/richiesta di servizio, eroga un primo livello di supporto e se necessario inoltra la chiamata alle code di competenza per un secondo livello di supporto più specifico.

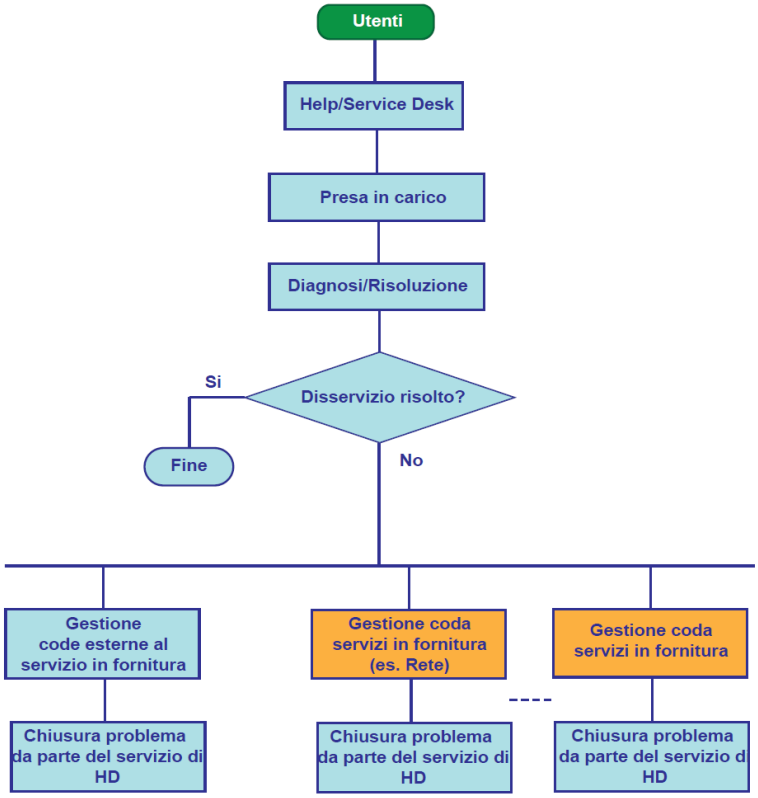

Figura 1

Le **code** relative ai servizi in fornitura sono:

- Rete
- Fonia
- Server Farm
- Infrastruttura
- Posta Elettronica
- Cyber Security
- Provisioning

Piazza Ospedale Maggiore, 3 20162 Milano – Tel. 02 6444.1 – Fax 02 6420901- C.F. e P.I. 11390840152 - www.ospedaleniguarda.it

Nel modello sopra esposto il SD è una struttura già operante e non deve essere inclusa nella fornitura.

Il SD rappresenta l'unico punto di contatto (**SPOC** – **S**ingle **P**oint **O**f **C**ontact) per ogni tipo di richiesta di supporto o di informazione da parte degli utenti.

Le chiamate possono riguardare:

1. Richieste di Supporto per problemi Hw
2. Richieste di Supporto per problemi Sw
3. Richieste di nuove Installazioni
4. Richieste di nuovi servizi/prodotti
5. Richieste di servizio per Inslall, Move, Add, Change (**IMAC**)
6. Richieste di informazioni
7. Solleciti su chiamate già aperte
8. etc.

Il SD è una funzione comune "propedeutica" alle altre funzioni e deve perciò essere attivata per prima.
In particolare, una volta recepita la richiesta di supporto, effettua una diagnosi on-line e, quando possibile, ripristina la corretta fruizione del prodotto/servizio da parte dell'utenza.
Nel caso in cui la soluzione non possa essere fornita direttamente on-line, il SD ha comunque la responsabilità di individuare la natura del malfunzionamento e dispacciare correttamente la chiamata alla/le linea/e operativa/e cui compete la soluzione del problema. Ciò ricorrendo al suo interno a sistemisti di secondo livello o, se necessario, facendosi aiutare dalle linee operative. Fino però al dispacciamento del problema il SD ne rimane l'unico responsabile.
Compito del SD è anche l'apertura, il monitoraggio ed, a conclusione del processo di problem solution, la chiusura del Trouble Ticket, da effettuare solo dopo verifica con il cliente del servizio fornito (call-back).
Per ogni chiamata, ad esclusione dei solleciti, viene aperto un ticket all'interno del sistema di trouble ticketing del SD. Il ticket rimane aperto fino alla soluzione dell'anomalia o alla conclusione della richiesta di servizio.

Nel caso in cui sia necessario l'inoltro ad una delle Linee Operative, il personale di Service Desk provvede a:

- assegnare un appropriato status al ticket,
- assegnare il ticket alla coda di competenza,
- eseguire il monitoring del ticket,
- verificare la risoluzione del problema con call back sull'utente che ha aperto la chiamata,
- chiudere il ticket sullo strumento di trouble ticketing.

Tutte le attività vengono registrate nello storico del ticket, il quale costituisce quindi una traccia dettagliata di tutti i servizi forniti, del personale coinvolto (Ente, Fornitore, Fornitori terzi) e delle azioni compiute per arrivare alla soluzione.

Il Fornitore dovrà dotarsi di un sistema di Trouble Ticketing perfettamente integrabile con il sistema di Trouble Ticketing Regionale in modo che possano scambiarsi tramite opportuni canali (mail, web services, ecc.) indicazioni circa i ticket di competenza del NOC. In alternativa il Fornitore, in accordo con l'ente, può utilizzare il servizio Trouble Ticketing fornito nell'ambito del contratto di Fleet Management regionale, assumendosi gli eventuali oneri economici.
Il sistema dovrà essere in grado di gestire e tracciare i cambi stato dei vari ticket (presa in carico, pending, risoluzione, ecc.) e comunicarli di conseguenza al sistema di **Trouble Ticketing Regionale.**

Piazza Ospedale Maggiore, 3 20162 Milano – Tel. 02 6444.1 – Fax 02 6420901- C.F. e P.I. 11390840152 - www.ospedaleniguarda.it

5. COMPONENTI DELLA FORNITURA

In questo paragrafo vengono elencati sinteticamente le componenti della fornitura successivamente descritti in maniera dettagliata al § 7 - Descrizione dei servizi in fornitura.

Il Fornitore dovrà seguire le best practice del framework Information Technology Infrastructure Library (ITIL)
Il Fornitore dovrà includere, nell'offerta tecnica una **prima versione delle procedure operative** (che saranno oggetto di particolare valutazione da parte della commissione tecnica, in particolare dovrà essere definita la procedura di start-up per la conduzione dei servizi di seguito indicati, riprendendo l'articolazione dei servizi nelle aree funzionali come indicate nel §7 Descrizione dei servizi in fornitura.

5.1 COMPONENTI TRASVERSALI A TUTTI I LOTTI

- **Piattaforma di monitoraggio:** Il Fornitore dovrà rendere disponibile (con oneri a proprio carico) una piattaforma di monitoraggio e controllo di tutti i **Servizi** in propria gestione e la corretta e continua evoluzione del sistema di monitoring e di controllo stesso (Hardware e Software).

- **Piattaforma di Trouble Ticketing:** Il Fornitore dovrà rendere disponibile una Piattaforma di Trouble Ticketing (con oneri a proprio carico) la quale dovrà integrarsi perfettamente con la Piattaforma di **Trouble Ticketing Regionale**, questo allo scopo di poter scambiare con quest'ultima i ticket indirizzati alle code del NOC.

5.2 LOTTO-1 – INFRASTRUTTURA DI RETE E FONIA

- **Servizio di gestione dell'Infrastruttura di Rete:** Il Fornitore dovrà garantire un servizio di gestione, manutenzione ed evoluzione dell'Infrastruttura di Rete dell'Ente, completa di tutti i componenti passivi (compreso cablaggio strutturato), attivi ed UPS dedicati, già operativi presso l'Ente.

- **Servizio di gestione Infrastruttura di Fonia:** Il Fornitore dovrà garantire un servizio di gestione, manutenzione ed evoluzione dell'Infrastruttura di Fonia, incluse le centrali telefoniche, i satelliti, gli UPS dedicati, i componenti passivi (compreso cablaggio strutturato) ed i terminali telefonici già operativi presso l'Ente.

- **Provisioning** Il servizio comprende tutto quanto necessario (apparati, materiali e opere) alla predisposizione di nuove terminazioni utente. Tutte le nuove terminazioni utente dovranno essere collaudate e certificate come meglio indicato nell'**Allegato Tecnico 5 – Listino Provisioning** Tutte le attività di provisioning verranno preventivamente concordate e pianificate con l'Ente e il costo verrà valutato in base ai singoli prezzi di aggiudicazione dei componenti come meglio descritto al § 7.1.4 "Servizio di provisioning".

Piazza Ospedale Maggiore, 3 20162 Milano – Tel. 02 6444.1 – Fax 02 6420901- C.F. e P.I. 11390840152 - www.ospedaleniguarda.it

5.3 LOTTO-2 – INFRASTRUTTURA TECNOLOGICA E POSTA ELETTRONICA

- **Servizio di gestione Infrastruttura di Server Farm:** Il Fornitore dovrà garantire un servizio di gestione, manutenzione ed evoluzione dell'Infrastruttura di Server Farm comprensiva di tutti le componenti sia esse fisiche che virtuali (Hardware, Sistema di virtualizzazione, Sistema Operativo).

- **Servizio di gestione Sistema di Infrastruttura:** Il Fornitore dovrà garantire un servizio di gestione, manutenzione ed evoluzione dei Sistemi di Infrastruttura. In generale con Sistemi d'Infrastruttura si intendono i sistemi server non destinati all'esecuzione di applicativi aziendali clinico amministrativo. Il servizio garantisce il corretto funzionamento ed evoluzione dei sistemi d'infrastruttura quali il Servizio di Web Filtering, Dominio Windows, Proxy, Firewall server, DNS, DHCP, log management, ecc. già operativi presso l'Ente.

- **Servizio di gestione Sistema di Posta Elettronica:** Il Fornitore dovrà garantire un servizio di gestione, manutenzione ed evoluzione del Sistema di Posta Elettronica Aziendale, come previsto all'interno degli allegati tecnici di ciascun Ente.

5.4 LOTTO-3 – SICUREZZA

- **Servizio di Cyber Security:** Il Fornitore dovrà garantire un servizio di gestione, verifica di corretto funzionamento ed evoluzione in ottica di **Cyber Security** dei **Servizi** dell'Ente come previsto all'interno degli allegati tecnici di ciascun **Ente** e come meglio esplicitato nel proseguo nella sezione specifica.
  Il servizio ha una funzione prettamente operativa e deve prevedere il monitoraggio dello stato e patching dei sistemi in gestione, rendendosi proattivo nell'applicazione delle patch su tali sistemi, nel rispetto delle normative vigenti e concordando l'applicazione e le eventuali implicazioni sui servizi con l'Ente. Deve inoltre farsi carico di predisporre le misure necessarie a fronte di alert o bollettini emanati dal SOC regionale. La funzione decisionale è comunque sempre in carico all'Ente.

Fatto salvo quanto messo a disposizione dall'Ente, è responsabilità del Fornitore dotarsi degli opportuni strumenti di gestione (hardware e software) per garantire la perfetta conduzione dei servizi richiesti in fornitura, nel rispetto degli SLA (Service Level Agreement) di capitolato.
Strumenti di particolare importanza sono ad esempio quelli per il monitoraggio e controllo dei **Servizi** e gli strumenti di gestione inventariale di tutti gli asset oggetto di fornitura.
Il servizio deve garantire, anche attraverso l'utilizzo di uno strumento dedicato, (Hardware e Software a carico del Fornitore) la gestione del parco apparati, garantendo l'archiviazione e la disponibilità delle informazioni di base dell'asset, tra le quali, etichetta identificativa (assegnata dall'Ente), data di acquisto, data di installazione, localizzazione, caratteristiche tecniche di base, ecc.
Il Fornitore dovrà inoltre mantenere aggiornata **tutta la documentazione operativa** relativa ai **Servizi** dell'Ente, le **mappe di rete e tutta la documentazione indicata dall'Ente stesso**.

Tale documentazione, di proprietà dell'Ente, dovrà essere memorizzata sul sistema di archiviazione (CMDB) richiesto in fornitura. L'accesso web a tale strumento di gestione deve essere garantito ai referenti dell'Ente.
Il servizio deve prevedere inoltre la gestione del magazzino con **oneri e responsabilità** totalmente a carico del Fornitore.

Piazza Ospedale Maggiore, 3 20162 Milano – Tel. 02 6444.1 – Fax 02 6420901- C.F. e P.I. 11390840152 - www.ospedaleniguarda.it

Si precisa che i Sistemi sopra indicati sono differenti in numero e tipologia per i vari Enti, come meglio precisato nei rispettivi Allegati tecnici di dettaglio.

5.5 COORDINAMENTO OPERATIVO TRA I LOTTI

In caso di aggiudicazione dei Lotti a operatori economici differenti, ciascun Fornitore è tenuto a cooperare con gli aggiudicatari degli altri Lotti e con i referenti dell'Ente, assicurando la continuità operativa e la tempestiva gestione delle attività che coinvolgano più ambiti tecnologici.

Ogni attività inter-lotto dovrà essere tracciata mediante il sistema di Trouble Ticketing, con indicazione almeno del soggetto richiedente, del Lotto competente per l'esecuzione, della priorità, dei tempi di assegnazione, presa in carico, esecuzione, verifica e chiusura.

La responsabilità dell'esecuzione tecnica e del rispetto dei relativi livelli di servizio resta in capo al Fornitore del Lotto competente per tecnologia. La responsabilità dell'analisi, della definizione delle indicazioni di sicurezza e della verifica degli interventi di remediation resta in capo al Fornitore del Lotto 3, ferma restando in ogni caso la funzione decisionale e autorizzativa dell'Ente.

I Fornitori non potranno opporre all'Ente eventuali carenze informative o ritardi imputabili agli aggiudicatari degli altri Lotti senza averli tempestivamente segnalati e formalmente tracciati mediante gli strumenti contrattuali.

Piazza Ospedale Maggiore, 3 20162 Milano – Tel. 02 6444.1 – Fax 02 6420901- C.F. e P.I. 11390840152 - www.ospedaleniguarda.it

6. RUOLI E COMPETENZE DELLE RISORSE PROFESSIONALI RICHIESTE

In questo paragrafo vengono brevemente illustrati i profili professionali e le competenze **minime** delle risorse ritenute indispensabili per l'erogazione dei servizi.
Sarà responsabilità del Fornitore adeguare in termini qualitativi e quantitativi, per tutta la durata del contratto, le risorse utilizzate in modo tale da garantire gli SLA di capitolato.

L'Ente si riserva di valutare e segnalare incompatibilità del personale predisposto dal Fornitore (elencato in seguito nelle figure principali) per l'erogazione dei **Servizi** e richiederne la sostituzione.
Qualora l'Ente richieda la sostituzione di personale di presidio, il Fornitore aggiudicatario dovrà #**entro 30 gg solari** sostituire il personale indicato, in caso contrario verrà applicata una penale, si veda art. 16 del Capitolato Speciale d'Appalto. "Livelli di servizio e Penali".

6.1 FIGURE TRASVERSALI A TUTTI I LOTTI

6.1.1 RESPONSABILE DEL CONTRATTO (ACCOUNT MANAGER)

È una figura professionale di alto livello ed elevato profilo gerarchico, con forti doti di leadership e capacità manageriali, il cui ruolo è caratterizzato dalle seguenti responsabilità:

- essere l'interfaccia del Fornitore;
- garantire la congruità tra quanto riportato nel contratto con quanto erogato;
- proporre e giustificare, in termini di costi, benefici, tempi e rischi, le soluzioni per il miglioramento continuo;
- farsi parte diligente e cooperare nella risoluzione dei conflitti o problemi che potrebbero sorgere durante lo svolgimento del contratto;
- attivarsi per le approvazioni e seguire il raggiungimento degli scopi/obiettivi;
- fornire informazioni accurate e tempestive per la gestione amministrativa e contabile del contratto.

È richiesta una figura con almeno 5 anni di esperienza in questo ruolo.

6.1.2 RESPONSABILE DI PROGETTO (PROJECT MANAGER)

Il Project Manager è una figura professionale di alto livello è responsabile del Team di Lavoro per il periodo di Transizione (implementazione) durante il quale vengono implementati i servizi oggetto del capitolato. Il suo ruolo è caratterizzato dalle seguenti responsabilità:

- realizzare il progetto di implementazione, rispettando le specifiche tecniche, i tempi, ed avvalendosi delle risorse previste;
- predisporre ed eseguire tutte le attività previste per raggiungere nei tempi stabiliti i livelli di SLA contrattuali;
- integrare gli apporti di tutti i partecipanti al progetto, in ottica di team;
- verificare lo stato di sviluppo delle singole attività, intervenendo con gli opportuni correttivi sugli scostamenti temporali e realizzativi;
- definire per ogni processo di erogazione, le procedure operative;
- ricercare l'ottimizzazione dei singoli processi, attraverso la loro integrazione;

Piazza Ospedale Maggiore, 3 20162 Milano – Tel. 02 6444.1 – Fax 02 6420901- C.F. e P.I. 11390840152 - www.ospedaleniguarda.it

- verificare ed eventualmente attuare le modifiche e le integrazioni richieste dall'Ente.

Il suo ruolo inizia dall'aggiudicazione della gara e termina con la chiusura del progetto di implementazione (progetto esecutivo, si veda §11 fase P2), in modo da poter assicurare una gestione unitaria ed una condivisione degli obiettivi tra Ente e Fornitore.

Il Project Manager al completamento della sua attività di predisposizione dei servizi dovrà fornire all'Ente il manuale delle **procedure operative definitivo.**

Ai fini della valutazione dell'offerta tecnica saranno attribuiti specifici punteggi alle certificazioni professionali possedute dalle risorse nominativamente indicate dal concorrente e destinate all'esecuzione del servizio, purché pertinenti al ruolo ricoperto, alle attività assegnate e alle tecnologie comprese nel relativo Lotto.

Le certificazioni dovranno essere in corso di validità alla data di presentazione dell'offerta o, qualora non sia prevista una scadenza, riferite a tecnologie e competenze ancora attuali e pertinenti. Saranno ammesse certificazioni equivalenti, purché il concorrente ne documenti l'organismo emittente, il livello, il programma d'esame e la coerenza con le competenze richieste.

In caso di sostituzione, la nuova risorsa dovrà possedere esperienza, competenze e certificazioni almeno equivalenti a quelle della risorsa sostituita che hanno concorso all'attribuzione del punteggio tecnico.

6.1.3 COORDINATORE DEL SERVIZIO (SERVICE MANAGER)

Il Service Manager è il Responsabile dei servizi ed è la risorsa di riferimento per quanto attiene l'erogazione e la gestione dei servizi richiesti, ed è quindi l'interfaccia verso l'Ente per la gestione dei rapporti e delle relazioni operative. Ha le seguenti responsabilità:

- verificare lo stato dell'erogazione dei servizi, si relaziona con i referenti dell'l'Ente ed organizzare gli incontri di Sato Avanzamento Lavori (**SAL**) previsti;
- organizzazione complessiva dei servizi, in riferimento al dimensionamento dei presidi, alle modalità operative (turnazione dei tecnici o degli operatori), al mantenimento degli skill professionali delle risorse;
- coordinamento delle strutture tecniche periferiche, dirette o dei partner di riferimento;
- analisi delle criticità e relative proposte di intervento;
- controllo costante dei livelli di servizio garantiti;
- predisposizione della documentazione e dei report periodici;
- elaborazione dei piani per la realizzazione di singoli progetti/eventi.

È richiesta una figura con almeno 5 anni di esperienza in questo ruolo.

6.2 LOTTO-1 – INFRASTRUTTURA DI RETE E FONIA

6.2.1 SISTEMISTA DI RETE

È una figura professionale, componente del presidio presso l'Ente, caratterizzata dai seguenti skill:

Piazza Ospedale Maggiore, 3 20162 Milano – Tel. 02 6444.1 – Fax 02 6420901- C.F. e P.I. 11390840152 - www.ospedaleniguarda.it

- conoscenza approfondita dei principali protocolli di routing di switching, relative alle apparecchiature descritte negli **Allegati specifici**;
- conoscenza dei sistemi operativi di rete (router, switch, Access Point, ecc.)
- conoscenza dei sistemi operativi Firewall (IPSec, VPN Client, etc.)
- conoscenza sistemi Wireless e sistemi Voip,
- capacità di analisi dei requisiti e progettazione di soluzioni;
- esperienza nella realizzazione e nel supporto di reti locali e geografiche, in particolare per quanto riguarda le problematiche di troubleshooting negli ambienti Lan/Wan.
- esperienza nell'operare e configurare con strumenti complessi quali analizzatori di protocollo e tool di controllo rete al fine del monitoraggio e dell'analisi dei problemi;
- conoscenza approfondita dei problemi di Networking IP;
- competenze specifiche per l'integrazione dei prodotti con l'ambiente di internetworking.

Attività' principali (elenco indicativo e non esaustivo):

- risoluzione guasti e gestione/configurazione degli apparati di rete;
- gestione operativa, manutenzione, aggiornamento e configurazione tecnica degli apparati firewall, comprese l'implementazione delle regole e delle policy preventivamente autorizzate dall'Ente, la configurazione delle VPN, il backup e il ripristino delle configurazioni e il troubleshooting di rete, nel rispetto delle procedure di Change Management e delle indicazioni di sicurezza formulate nell'ambito del Lotto 3.
- utilizzo del software per il monitoraggio della rete;
- interfacciamento con i secondi livelli o con i competence center di Fornitori terzi;
- apertura di ticket per richieste pervenute via mail da parte dei referenti dell'Ente.

È richiesta una figura con almeno 3 anni di esperienza in questo ruolo.

Ai fini della valutazione dell'offerta tecnica saranno attribuiti specifici punteggi alle certificazioni professionali possedute dalle risorse nominativamente indicate dal concorrente e destinate all'esecuzione del servizio, purché pertinenti al ruolo ricoperto, alle attività assegnate e alle tecnologie comprese nel relativo Lotto.

Le certificazioni dovranno essere in corso di validità alla data di presentazione dell'offerta o, qualora non sia prevista una scadenza, riferite a tecnologie e competenze ancora attuali e pertinenti. Saranno ammesse certificazioni equivalenti, purché il concorrente ne documenti l'organismo emittente, il livello, il programma d'esame e la coerenza con le competenze richieste.

In caso di sostituzione, la nuova risorsa dovrà possedere esperienza, competenze e certificazioni almeno equivalenti a quelle della risorsa sostituita che hanno concorso all'attribuzione del punteggio tecnico.

6.2.2 SISTEMISTA DI FONIA

È una figura professionale, componente del presidio presso l'Ente, caratterizzata dai seguenti skill:

- conoscenza approfondita delle centrali telefoniche indicate negli **Allegati specifici**;
- capacità di analisi dei requisiti e progettazione di soluzioni;
- esperienza nella configurazione e nel supporto delle centrali telefoniche oggetto della fornitura.
- competenze specifiche per l'integrazione dei prodotti con l'ambiente di fonia.

Piazza Ospedale Maggiore, 3 20162 Milano – Tel. 02 6444.1 – Fax 02 6420901- C.F. e P.I. 11390840152 - www.ospedaleniguarda.it

Attività principali (elenco indicativo e non esaustivo):
- risoluzione guasti su infrastruttura di fonia;
- gestione/configurazione degli apparati di fonia;
- gestione/configurazione degli apparati Voip;
- utilizzo del software per il monitoraggio della infrastruttura di fonia;
- interfacciamento con i secondi livelli o con i competence center di Fornitori terzi;
- apertura di ticket per richieste pervenute via mail da parte dei referenti dell'Ente.

È richiesta una figura con almeno 3 anni di esperienza in questo ruolo.

Ai fini della valutazione dell'offerta tecnica saranno attribuiti specifici punteggi alle certificazioni professionali possedute dalle risorse nominativamente indicate dal concorrente e destinate all'esecuzione del servizio, purché pertinenti al ruolo ricoperto, alle attività assegnate e alle tecnologie comprese nel relativo Lotto.

Le certificazioni dovranno essere in corso di validità alla data di presentazione dell'offerta o, qualora non sia prevista una scadenza, riferite a tecnologie e competenze ancora attuali e pertinenti. Saranno ammesse certificazioni equivalenti, purché il concorrente ne documenti l'organismo emittente, il livello, il programma d'esame e la coerenza con le competenze richieste.

In caso di sostituzione, la nuova risorsa dovrà possedere esperienza, competenze e certificazioni almeno equivalenti a quelle della risorsa sostituita che hanno concorso all'attribuzione del punteggio tecnico.

6.3 LOTTO-2 – INFRASTRUTTURA TECNOLOGICA E POSTA ELETTRONICA

6.3.1 SISTEMISTA SERVER

È una figura professionale, componente del presidio presso l'Ente, caratterizzata dai seguenti skill:

- conoscenza approfondita dei sistemi e delle infrastrutture operativi presso l'Ente, descritti negli **Allegati specifici**;
- capacità di operare in ambienti con server virtualizzati (es. VMware);
- capacità di operare in ambienti basati si Sistemi Operativi Windows e Linux;
- capacità di operare su ambienti Data Base (Oracle, Mysql Server);
- capacità di analisi dei requisiti e progettazione di soluzioni;
- esperienza nella gestione e progettazione di sistemi server;
- competenze specifiche per l'integrazione dei sistemi server;

Attività' principali (elenco indicativo e non esaustivo):
- risoluzione guasti sui sistemi server;
- gestione/configurazione dei sistemi server;
- utilizzo del software per il monitoraggio dei sistemi server;
- interfacciamento con i secondi livelli o con i competence center di Fornitori terzi;
- gestione/configurazione del dominio dell'Ente;
- gestione configurazione del DNS;
- gestione configurazione Antispam/Antivirus;

Piazza Ospedale Maggiore, 3 20162 Milano – Tel. 02 6444.1 – Fax 02 6420901- C.F. e P.I. 11390840152 - www.ospedaleniguarda.it

- gestione configurazione LDAP per autenticazione applicativi aziendali;
- gestione e configurazione della piattaforma di Backup di proprietà dell'**Ente**;
- apertura di ticket per richieste pervenute via mail da parte dei referenti dell'Ente.

E' richiesta una figura con almeno 5 anni di esperienza in questo ruolo.

Ai fini della valutazione dell'offerta tecnica saranno attribuiti specifici punteggi alle certificazioni professionali possedute dalle risorse nominativamente indicate dal concorrente e destinate all'esecuzione del servizio, purché pertinenti al ruolo ricoperto, alle attività assegnate e alle tecnologie comprese nel relativo Lotto.

Le certificazioni dovranno essere in corso di validità alla data di presentazione dell'offerta o, qualora non sia prevista una scadenza, riferite a tecnologie e competenze ancora attuali e pertinenti. Saranno ammesse certificazioni equivalenti, purché il concorrente ne documenti l'organismo emittente, il livello, il programma d'esame e la coerenza con le competenze richieste.

In caso di sostituzione, la nuova risorsa dovrà possedere esperienza, competenze e certificazioni almeno equivalenti a quelle della risorsa sostituita che hanno concorso all'attribuzione del punteggio tecnico.

6.3.2 SISTEMISTA SISTEMI DI INFRASTRUTTURA

È una figura professionale, componente del presidio presso l'Ente, caratterizzata dai seguenti skill:

- conoscenza approfondita dei sistemi di infrastruttura operativi presso l'Ente, descritti negli **Allegati specifici**;
- capacità di operare in ambienti con server virtualizzati (es. VMware);
- capacità di analisi dei requisiti e progettazione di soluzioni;
- esperienza nella gestione e progettazione sistemi di infrastruttura;
- competenze specifiche per l'integrazione dei sistemi di infrastruttura;
- capacità di operare in ambienti con server virtualizzati (es. VMware).

Attività' principali (elenco indicativo e non esaustivo):

- risoluzione guasti sui sistemi di infrastruttura;
- gestione/configurazione dei sistemi di infrastruttura;
- utilizzo del software per il monitoraggio dei sistemi di infrastruttura;
- interfacciamento con i secondi livelli o con i competence center di Fornitori terzi;
- apertura di ticket per richieste pervenute via mail da parte dei referenti dell'Ente.

È richiesta una figura con almeno 5 anni di esperienza in questo ruolo.

Ai fini della valutazione dell'offerta tecnica saranno attribuiti specifici punteggi alle certificazioni professionali possedute dalle risorse nominativamente indicate dal concorrente e destinate all'esecuzione del servizio, purché pertinenti al ruolo ricoperto, alle attività assegnate e alle tecnologie comprese nel relativo Lotto.

Le certificazioni dovranno essere in corso di validità alla data di presentazione dell'offerta o, qualora non sia prevista una scadenza, riferite a tecnologie e competenze ancora attuali e pertinenti. Saranno ammesse certificazioni equivalenti, purché il concorrente ne documenti l'organismo emittente, il livello, il programma d'esame e la coerenza con le competenze richieste.

Piazza Ospedale Maggiore, 3 20162 Milano – Tel. 02 6444.1 – Fax 02 6420901- C.F. e P.I. 11390840152 - www.ospedaleniguarda.it

In caso di sostituzione, la nuova risorsa dovrà possedere esperienza, competenze e certificazioni almeno equivalenti a quelle della risorsa sostituita che hanno concorso all'attribuzione del punteggio tecnico.

6.3.3 SISTEMISTA DI POSTA

È una figura professionale, componente del presidio presso l'Ente, caratterizzata dai seguenti skill:

- capacità di pianificare ed eseguire l'installazione e la configurazione degli ambienti operativi esperienza nella gestione di server;
- capacità di operare in ambienti server critici dal punto di vista dell'affidabilità e del numero di utenti supportati;
- conoscenze tecniche d'analisi e risoluzione problemi complessi negli ambienti MS e Linux;
- capacità di operare in ambienti con server virtualizzati (es. VMware).
- Conoscenza dell'ecosistema Microsoft 365: Exchange Online, SharePoint Online, OneDrive for Business, Teams, Intune, Defender for Office 365, e Azure Active Directory (Entra ID)
- Gestione utenti, gruppi e ruoli in Azure AD (Entra ID).
- Configurazione di autenticazione multifattore (MFA), Single Sign-On (SSO) e Conditional Access Policies.
- Integrazione con Active Directory locale (AD) tramite Azure AD Connect / Entra Connect.
- Gestione di ruoli amministrativi e principi di least privilege.
- Exchange Online e posta elettronica
- Creazione e gestione di caselle di posta, alias, gruppi di distribuzione e regole di trasporto.
- Configurazione di antispam, antiphishing, quarantena e sicurezza della posta (Defender for Office 365).
- Gestione di record DNS per la posta (MX, SPF, DKIM, DMARC).
- Pianificazione di migrazioni da Exchange on-premise o da altri provider (IMAP, Gmail, ecc.).
- Gestione dei siti SharePoint Online, permessi e librerie documentali.
- Configurazione e sicurezza di OneDrive for Business
- Amministrazione di Microsoft Teams: creazione di team, policy, meeting, telefoni, e integrazioni con app.
- Gestione delle retention policies e data loss prevention (DLP)
- Configurazione e gestione dei dispositivi tramite Microsoft Intune / Endpoint Manager.
- Applicazione di policy di sicurezza, aggiornamenti, compliance, e controllo remoto.
- Gestione di BitLocker, Windows Update for Business, e configurazioni MDM/MAM.
- Comprensione delle funzionalità di audit e compliance (Microsoft Purview, eDiscovery, Data Governance).

Attività' principali (elenco indicativo e non esaustivo):

- gestione/configurazione architettura di posta;
- interfacciamento con i secondi livelli o con i competence center di Fornitori terzi;
- apertura di ticket per richieste pervenute via mail da parte dei referenti dell'Ente.

È richiesta una figura con almeno 5 anni di esperienza in questo ruolo.

Ai fini della valutazione dell'offerta tecnica saranno attribuiti specifici punteggi alle certificazioni professionali possedute dalle risorse nominativamente indicate dal concorrente e destinate all'esecuzione del servizio, purché pertinenti al ruolo ricoperto, alle attività assegnate e alle tecnologie comprese nel relativo Lotto.

Le certificazioni dovranno essere in corso di validità alla data di presentazione dell'offerta o, qualora non sia prevista una scadenza, riferite a tecnologie e competenze ancora attuali e pertinenti. Saranno ammesse

Piazza Ospedale Maggiore, 3 20162 Milano – Tel. 02 6444.1 – Fax 02 6420901- C.F. e P.I. 11390840152 - www.ospedaleniguarda.it

certificazioni equivalenti, purché il concorrente ne documenti l'organismo emittente, il livello, il programma d'esame e la coerenza con le competenze richieste.

In caso di sostituzione, la nuova risorsa dovrà possedere esperienza, competenze e certificazioni almeno equivalenti a quelle della risorsa sostituita che hanno concorso all'attribuzione del punteggio tecnico.

6.4 LOTTO-3 – SICUREZZA

6.4.1 SPECIALISTA DI CYBER SECURITY

È una figura professionale, componente del presidio presso l'Ente, il suo compito è quello di espletare attività quali information security auditing e analysis, definizione di policy di sicurezza, consulenza proattiva in termini di identificazione delle aree di rischio ed individuazione delle soluzioni di miglioramento anche in termini di pianificazione acquisti, applicazione degli interventi correttivi sui **Servizi** già operativi presso l'Ente coordinandosi con l'Ente stessi.
Egli dovrà inoltre:

- effettuare verifiche, proporre eventuali adeguamenti ed implementare tali adeguamenti (se richiesto dall'Ente) in linea con le varie direttive e/o normative sia a livello regionale che nazionale in vigore (**NIS2 Legge 90. Ecc.)**,
- completare verificare e/o integrare la documentazione a corredo del servizio stesso e di proprietà dell'**Ente**, ivi comprese documentazioni richieste da: **AGID, ARIA, Garante della Privacy, ecc.;**
- collaborare con eventuali **Servizi di Cyber Security in capo a Fornitori terzi** allo scopo di gestire in maniera più proattiva eventuali problematiche di sicurezza componendo un TEAM multi-fornitore dedicato alla tematica (es. CSIRT Nazionale, Soc regionale, Team di cybersecurity aziendale).
- effettuare, con riferimento agli apparati firewall, l'analisi dei requisiti di sicurezza, la valutazione e revisione delle policy, la verifica delle regole configurate, l'analisi dei log e degli eventi, la proposta delle modifiche e la verifica dell'efficacia degli interventi eseguiti. Le attività operative di configurazione, manutenzione e aggiornamento degli apparati restano in capo al personale del Lotto 1, salvo diversa e motivata indicazione dell'Ente.

Avrà anche il compito, previa verifica e successivamente all'approvazione dei referti dell'Ente, di supervisionare le attività di aggiornamento dei sistemi per criticità legate alla sicurezza

È richiesta una figura con almeno 5 anni di esperienza professionale in attività di cybersecurity, maturata in contesti organizzativi complessi. L'esperienza dovrà comprendere attività operative o di coordinamento in almeno due dei seguenti ambiti: vulnerability management, incident response, gestione di apparati di sicurezza, gestione e analisi degli eventi di sicurezza, hardening dei sistemi, penetration testing, gestione delle identità e degli accessi, coordinamento con SOC o CSIRT.

Ai fini della valutazione dell'offerta tecnica saranno attribuiti specifici punteggi alle certificazioni professionali possedute dalle risorse nominativamente indicate dal concorrente e destinate all'esecuzione del servizio, purché pertinenti al ruolo ricoperto, alle attività assegnate e alle tecnologie comprese nel relativo Lotto

Le certificazioni dovranno essere in corso di validità alla data di presentazione dell'offerta o, qualora non sia prevista una scadenza, riferite a tecnologie e competenze ancora attuali e pertinenti. Saranno ammesse

Piazza Ospedale Maggiore, 3 20162 Milano – Tel. 02 6444.1 – Fax 02 6420901- C.F. e P.I. 11390840152 - www.ospedaleniguarda.it

certificazioni equivalenti, purché il concorrente ne documenti l'organismo emittente, il livello, il programma d'esame e la coerenza con le competenze richieste.

In caso di sostituzione, la nuova risorsa dovrà possedere esperienza, competenze e certificazioni almeno equivalenti a quelle della risorsa sostituita che hanno concorso all'attribuzione del punteggio tecnico.

6.5 COMPOSIZIONE DEL PRESIDIO DEDICATO

Il Fornitore dovrà indicare in modo esplicito in offerta, la composizione del presidio presente presso l'Ente.
Nell'allegato tecnico ogni Ente ha esplicitato nel dettaglio la presenza minima e contemporanea giornaliera in termini di persone presenti per la copertura delle varie fasce orarie del presidio.

Nel caso, nel corso del contratto, ci sia la necessità di inserimento di nuovo personale, ogni singola risorsa dovrà avere un affiancamento di almeno **10 gg. lavorativi** prima di poter essere inserito nel presidio.
Il Fornitore deve poter disporre di una struttura disponibile H24 x 365gg, composta da sistemisti di secondo livello, necessaria a supportare problematiche complesse non risolvibili dal personale di presidio, tutto questo nel rispetto degli SLA di capitolato.

Il presidio composto dalle persone, come richiesto nei singoli allegati tecnici di dettaglio, deve essere obbligatoriamente presente presso le sedi dell'Ente e non può operare assolutamente da sedi remote del Fornitore, salvo esplicita richiesta dell'Ente stesso.

Il personale presente in presidio verrà munito di Badge aziendale, il Badge strettamente personale avrà la duplice valenza, da un lato permettere l'accesso ai locali riservati (Server Farm e uffici in cui viene effettuato il presidio) dall'altro monitorare la copertura del servizio come da contratto.

Il mancato rispetto di tale obbligo è motivo di esclusione in sede di valutazione dell'offerta di gara ed è causa di recesso se rilevato nel corso dell'esecuzione del contratto.

6.6 AGGIORNAMENTO PROFESSIONALE E CORSI DI FORMAZIONE

Il Fornitore dovrà prevedere lo sviluppo e l'aggiornamento degli skill del personale impiegato nell'erogazione dei servizi; tale aggiornamento dovrà essere documentato con cadenza #semestrale all'Ente.

6.7 COMITATO DI CONTROLLO (CC)

Il Comitato di Controllo è un organismo paritetico tra Ente e Fornitore preposto al controllo dei livelli di servizio e alla gestione del contratto nel tempo.
Il comitato si riunisce a scadenze periodiche, tipicamente #mensili in occasione dei SAL, per tutta la durata del contratto.
In particolare, al **CC** sono attribuite le seguenti funzioni:

- analisi delle richieste di modifica dei processi di erogazione dei servizi e dell'organizzazione, in termini quantitativi e qualitativi;
- definizione, revisione e controllo della qualità dei servizi erogati e delle tecnologie fornite;
- valutazione delle azioni da intraprendere per risolvere eventuali problemi operativi;
- risoluzione di conflitti tra le parti.

Deve essere data indicazione puntuale della composizione della **CC** come segue:

Piazza Ospedale Maggiore, 3 20162 Milano – Tel. 02 6444.1 – Fax 02 6420901- C.F. e P.I. 11390840152 - www.ospedaleniguarda.it

Fornitore		Ente	
Ruolo	Nome	Ruolo	Nome
Account Manager		Responsabile ICT	
Project manager		Responsabile Service Operations	
Service Manager		Coordinatore NOC	

Piazza Ospedale Maggiore, 3 20162 Milano – Tel. 02 6444.1 – Fax 02 6420901- C.F. e P.I. 11390840152 - www.ospedaleniguarda.it

7 DESCRIZIONE DEI SERVIZI IN FORNITURA

7.1 LOTTO 1 E 2 – INFRASTRUTTURA DI RETE E FONIA E INFRASTRUTTURA TECNOLOGICA E POSTA ELETTRONICA

7.1.1 SERVIZIO DI GESTIONE DEI SISTEMI E DELLE INFRASTRUTTURE

Il servizio prevede un presidio operativo presso il Network Operation Centre (**NOC**) **ubicato presso l'Ente**, dove saranno centralizzate le funzioni di esercizio del **Sistema** oggetto di fornitura. Il Service Desk effettua le attività di 1° livello, inoltrando al NOC le richieste di competenza in accordo con le attività di pertinenza.
In aggiunta al personale dedicato al presidio, la struttura tecnica del Fornitore deve essere organizzata e disponibile per interventi on-site **con parti di scorta proprie** e per intervento sistemistico con copertura oraria 7 giorni su 7, 24 ore su 24, 365 gg. (7x7 h24 365 gg). Il modello di attivazione potrà essere diretto o su reperibilità e sempre con gli SLA concordati.

Il Fornitore deve prendere in carico problematiche e richieste relative a:

- Tutte le componenti hardware e software incluse nel **Sistema** oggetto della fornitura;
- la rete di distribuzione passiva;
- le linee di fonia e dati interne;
- le linee di fonia e dati esterne (secondo le modalità indicate dal Provider del servizio pubblico di connettività);
- tutti le periferiche collegate agli impianti principali;
- telefoni completi di tutte le loro componenti
- pc dedicati al controllo delle componenti del **Sistema**;
- sistemi UPS di centrale (compresa la fornitura e la sostituzione delle batterie di centrale senza oneri aggiuntivi per l'Ente).

Il **Sistema** oggetto della fornitura è dettagliato negli **Allegati tecnici degli Enti.**
Il servizio richiesto dovrà essere svolto utilizzando un'organizzazione così articolata:

- **presidio tecnico specialistico on-site** secondo gli orari richiesti nel § 8 - Livelli di servizio e composto secondo il § 6-Ruoli e competenze delle risorse professionali richieste;
- **reperibilità** con intervento on-site 7x7 h24 x 365 gg. sui sistemi e sulle infrastrutture categorizzate dall'Ente ad alta e media criticità.

  Si precisa che l'intervento effettuato sia dal presidio on site, sia in reperibilità è da considerarsi obbligo contrattuale indipendentemente dalla natura che ha causato la criticità o il guasto, ad es. eventi avversi quali allagamenti, blackout, danneggiamenti sabotaggi, ecc.

- **monitoraggio locale e da remoto** dei sistemi e delle infrastrutture 7x7 h24 x 365 gg.
- **escalation** ai Competence Center propri e/o di Fornitori terzi (Allied Telesyn, Cisco, Microsoft, Extreme Network, Stonesoft ecc.) per le problematiche che ne richiedano l'intervento.

Il Fornitore dovrà inoltre produrre le procedure operative necessarie, rispettando il framework ITIL, al fine di garantire i servizi richiesti con gli SLA di capitolato, definire le aree di responsabilità del processo stesso, nonché creare il manuale di tali procedure.

Piazza Ospedale Maggiore, 3 20162 Milano – Tel. 02 6444.1 – Fax 02 6420901- C.F. e P.I. 11390840152 - www.ospedaleniguarda.it

L'Ente dovrà approvare il manuale delle procedure.

7.1.2 STRUTTURAZIONE DEI SERVIZI RICHIESTI IN FORNITURA

Il Fornitore dovrà attivare, per la gestione delle Infrastrutture e dei Sistemi inclusi nei **Servizi** richiesti in fornitura, una organizzazione come di seguito indicato:

- **Monitoring Management**
  - Local Monitoring
  - Remote Monitoring

- **Service Transition Management**
  - Change Management
  - Configuration Management
  - Release Management and Deployment Management
  - Attività straordinarie
  - Transition Planning and Support
  - Service Validation and Testing Management
  - Knowledge Management

- **Service Operations Management**
  - Incident Management e Problem Management
  - Backup Management
  - Gestione Logistica

- **Licensing Management**

- **Performance Management**

- **Reporting**

- **Presidio locali tecnici**

- **Apparati Gestiti**

- **Consulenza**

7.1.2.1 Monitoring Management

Le attività di monitoring comprendono la verifica e il controllo costante del buon funzionamento dei **Servizi** oggetto di fornitura (apparati di rete e fonia, centrali telefoniche, satelliti di fonia, terminali telefonici, server, memoria, cpu, occupazione disco, ecc.) indicati negli **Allegati specifici**, sia dal punto di vista fisico, sia dal punto di vista logico utilizzando, oltre al controllo puntuale on-site, anche strumenti di monitoraggio (a carico del Fornitore sia a livello Hardware che Software) che diano una visione globale della situazione.
Durate la durata contrattuale potrà essere richiesto al Fornitore anche l'**estensione (H24)** del monitoraggio di **applicativi, server o servizi**, non in sua diretta gestione. In tal caso a fronte di una segnalazione il Fornitore dovrà contattare il Fornitore terzo per notificargli l'alert.
L'estensione richiesta non determinerà un incremento dei **Servizi** monitorati superiore al 20% dei **Servizi** contrattualizzati.

Piazza Ospedale Maggiore, 3 20162 Milano – Tel. 02 6444.1 – Fax 02 6420901- C.F. e P.I. 11390840152 - www.ospedaleniguarda.it

Ai referenti dell'Ente deve essere garantito l'accesso via Web ai sistemi di monitoring.

Il Fornitore deve inoltre mettere a disposizione uno strumento web di sintesi (dashboard) che, in una unica videata, da concordare con l'Ente, riassuma lo stato dei differenti alert dell'intero impianto. La fornitura (HW e SW) del sistema dovrà essere con oneri a carico del Fornitore.

Dovrà essere previsto, senza alcun onere per gli Enti, un sistema di messaggistica via mail per ogni alert che si presenterà sulla dashboard di monitoraggio.
Dovrà essere predisposto un report mensile che conterrà le statistiche delle segnalazioni dei sistemi, per meglio affrontare sistemicamente i problemi che si presentano.

7.1.2.2 Local Monitoring

Attività a carico del Fornitore:
Servizio di monitoring dei **Servizi** oggetto della fornitura, attuato localmente dal sistema di monitoring, gestito dal presidio situato presso l'Ente:

- installazione hw dei sistemi di monitoring;
- installazione sw dei sistemi di monitoring;
- configurazione sw dei sistemi di monitoring;
- garantisce l'operatività e l'aggiornamento (patch, upgrade) dei sistemi di monitoring;
- installazione di sistemi di monitoring ridondati;
- fornisce ed abilita le tecnologie di controllo remoto delle infrastrutture e dei sistemi identificati dall'Ente;
- impostazione discovery automatica o manuale apparati/servizi attivi;
- definizione ed impostazione delle soglie per allarmi e performance;
- controllo continuo degli allarmi usando la tecnologia di monitoring scelta, segnalando tempestivamente eventuali disservizi (fault);
- controllo del corretto funzionamento delle linee di comunicazione esterne ed interne, anche se non in sua diretta gestione (es. linee Telecom, Fastweb, Garr,Provider SISS ecc);
- controllo del corretto funzionamento delle centrali telefoniche e dei servizi IVR (Interactive Voice Response);
- monitoring dei sistemi UPS di proprietà dell'Ente;
- apertura/chiusura ticket interfacciandosi automaticamente con il sistema di Trouble Ticketing in uso presso l'Ente;
- invio di SMS e o mail ai referenti dell'Ente a fronte di allarmi e/o superamento soglie prestabilite;
- effettua escalation al proprio secondo livello, se necessario, a fronte di un fault;
- notifica al responsabile dell'Ente a fronte di ricezione allarmi;
- segnalazione non automatica di presa in carico dell'allarme da parte del reperibile mediante invio di sms ai referenti dell'Ente.
- propone contenuto e fornisce report riassuntivo fault;
- fornitura di un accesso web al sistema di monitoring per i referenti dell'Ente.
- test periodici (#mensili) sul sistema di monitoring, con simulazioni di fault per verificare il corretto funzionamento del sistema.

7.1.2.3 Remote Monitoring

Attività a carico del Fornitore:

Piazza Ospedale Maggiore, 3 20162 Milano – Tel. 02 6444.1 – Fax 02 6420901- C.F. e P.I. 11390840152 - www.ospedaleniguarda.it

Servizio di monitoring dei **Servizi** oggetto della fornitura, attuato remotamente nella sede del Fornitore dal sistema di monitoring (7x7 h24 x 365 gg.):
Il Servizio deve prevedere una infrastruttura di monitoraggio presso la sede del Fornitore, in modo tale da garantire la continuità del servizio anche in caso di indisponibilità dell'infrastruttura di **monitoraggio locale**.
I tempi di intervento e/o di ripristino sono definiti in base agli SLA di capitolato.

Attività a carico dell'Ente:

- approvare le tecnologie di monitoring;
- approvare soglie di allarmi e performance sui sistemi di management;
- approvare modello report riassuntivo;
- approvare le procedure operative proposte dal Fornitore.

7.1.2.4 Service Transition Management

- Assicurare che i servizi nuovi o modificati vengano rilasciati in produzione senza impatti negativi.
- Pianificare e coordinare tutte le attività di transizione (rilascio, deployment, test, formazione, change management).
- Garantire che i servizi soddisfino gli standard di qualità richiesti dall'organizzazione.
- Minimizzare rischi e interruzioni durante il passaggio dalla fase di sviluppo a quella operativa.

RESPONSABILITÀ CHIAVE

- **Pianificazione della transizione:** sviluppo dei piani di Service Transition, inclusi tempi, risorse, dipendenze e criteri di accettazione.
- **Coordinamento dei rilasci:** gestione delle attività di Release & Deployment Management.
- **Gestione dei cambiamenti:** collaborazione con il Change Manager per valutare impatti, rischi e prerequisiti.
- **Controllo della configurazione:** assicurare che gli elementi di configurazione (CI) siano registrati e aggiornati nel CMDB.
- **Gestione dei test:** coordinamento dei test tecnici, funzionali e di accettazione (UAT).
- **Consegna all'Operations:** garantire che i team operativi ricevano documentazione, formazione e strumenti necessari.
- **Monitoraggio e reporting:** verifica delle metriche di transizione, qualità e rispetto dei Service Level.
- **Gestione dei rischi:** identificazione, valutazione e mitigazione dei rischi di progetto e di release.

COMPETENZE RICHIESTE

- Conoscenza approfondita delle pratiche **ITIL v3 / ITIL 4**, in particolare Service Transition.
- Capacità di gestione progetti (anche metodologie Agile/Waterfall).
- Ottime competenze di comunicazione e coordinamento tra team tecnici e business.
- Capacità di analisi dei rischi e problem solving.
- Familiarità con processi di test, configurazione, release e change management.
- Attitudine a lavorare in ambienti complessi e multi-team.

7.1.2.5 Change Management

Il processo di **IMAC** (Install, Move, Add & Change) è focalizzato sulla gestione relativa alle richieste di spostamento, ampliamento, installazione, cambiamento relativamente al parco Hardware e al parco Software dei sistemi e delle infrastrutture dell'Ente e loro integrazione con l'ambiente preesistente presso l'Ente stesso.

Piazza Ospedale Maggiore, 3 20162 Milano – Tel. 02 6444.1 – Fax 02 6420901- C.F. e P.I. 11390840152 - www.ospedaleniguarda.it

Attività a carico del Fornitore:

- eseguire attività on-site o da remoto sugli apparati (centrali e/o periferici) o sui permutatori nel caso di modifica o ampliamento del cablaggio;
- eseguire attività on-site o da remoto di configurazione sugli apparati (centrali e/o periferici) a fronte di modifica o ampliamento dell'infrastruttura;
- eseguire attività on-site o da remoto di configurazione sugli apparati (centrali e/o periferici) a fronte di attivazione/spostamento nuovi utenti e/o servizi;
- eseguire l'upgrade dei sistemi e delle infrastrutture per attivazione di nuovi servizi o funzioni;
- eseguire attività on-site per richieste di movimentazione delle PDL occupandosi di attivare la connessione fisica sia sull'apparato centrale sia sul punto rete utente;
- rimuovere fisicamente le attivazioni sia lato apparato, sia lato utente non più utilizzate in caso di traslochi o spostamenti;
- verifica periodica (#trimestrale) dell'effettivo utilizzo dei punti rete e fonia al fine di bonificare lato armadio il cablaggio inutilizzato;
- eseguire configurazione o riconfigurazione delle utenze su tutti i **Servizi** oggetto di fornitura;
- eseguire attività di configurazione sugli apparati in modo tale da permettere la connessione alla rete sia wired che wireless di utenti esterni (pazienti, ospiti, etc.), occupandosi di rendere attiva la connessione del terminale utente sulla rete. Si richiede inoltre un minimo di controllo/modifica configurazione sul pc dell'utente per permette la connessione dell'apparato stesso alla rete dell'Ente se richiesto.
- installazione di nuovi apparati e/o di loro parti;
- configurazione dei dispositivi mobili **aziendali** (per accesso alla posta elettronica aziendale, configurazione di APP aziendali, configurazione servizi aziendali, ecc).;
- configurazione dei dispositivi mobili **personali** per accesso alla posta elettronica aziendale;
- consegna e sostituzione di apparecchiature presso gli utenti;
- coordinare attività on-site di eventuali fornitori terzi;
- aggiornare la base dati relativa all'asset inventory;
- aggiornare la documentazione dei sistemi e delle infrastrutture;
- tenere traccia delle attività svolte e dei tempi necessari alla evasione delle richieste;
- documentare l'attività se richiesto
- creazione/aggiornamento delle anagrafiche utenze con cognome, nome, numero interno, unità operativa/struttura, centro di costo, eventuale numero mobile di riferimento, eventuale indirizzo email;
- creazione/aggiornamento delle utenze con i dati di riferimento necessari alle centrali utilizzando gli standard previsti dall'Ente;
- creazione/aggiornamento della documentazione tecnica di gestione degli attacchi utente sia lato centrale che lato permutazione;
- gestione delle informazioni relative alle abilitazioni degli interni, ai gruppi di utenti, alla gestione della messaggistica;
- configurazione/modifica degli alberi dell'IVR, questa attività deve essere effettuata sia nella fascia oraria del presidio, sia in fascia oraria non coperta dal presidio se richiesto dall'Ente;
- reportistica e statistiche su IVR e documentazione addebiti;
- produzione della documentazione di centrale riportante le principali configurazioni in linea (es. gestione delle chiamate, gestione dei trabocchi, classi di abilitazione, esclusione di numeri o servizi, etc.);
- disabilitazione dei servizi di sistema operativo non usati, rimuovere dall'esecuzione i servizi non necessari è un'attività che comprende un'analisi del sistema e delle risorse utilizzate. Tale attività è particolarmente utile per ottimizzare le performance del sistema. Contestualmente aumenta la sicurezza del sistema;

Piazza Ospedale Maggiore, 3 20162 Milano – Tel. 02 6444.1 – Fax 02 6420901- C.F. e P.I. 11390840152 - www.ospedaleniguarda.it

- amministrazione account utente, consiste nel proteggere il sistema dagli accessi indesiderati. Il sistema diventa sempre più importante quante più informazioni confidenziali conserva;
- amministrazione utenti: consiste nella creazione/rimozione account, secondo le policy definite dall'Ente e reset delle password;
- gestione delle risorse condivise: consiste nell'abilitare o negare l'accesso alle risorse condivise ai singoli utenti in funzione delle policy definite dall'Ente;
- assistenza sistemistica relativa ad ambienti correlati, come ad esempio i servizi accessori (gestione mailing list, gestione o modifica del disclaimer aziendale) relativi alla posta elettronica, di cui il Fornitore sia stato preventivamente informato dal punto di vista delle funzionalità e degli aspetti tecnici rilevanti.
- fornire consulenza e supporto alle altre linee operative.

I tempi di intervento e di ripristino sono definiti in base agli SLA di capitolato.

Attività a carico dell'Ente:

- assicurare l'accesso ai locali dove necessita eseguire l'intervento;
- trasmettere informazioni relative ai traslochi;
- approvare le procedure presentate dal Fornitore;
- approvare richiesta dell'attività.

L'Ente potrà richiedere delle attività IMAC con carattere d'urgenza, come indicato nel § 8 - livelli di servizio, non superiori alle **20 attività #mensili**.

7.1.2.6 Configuration Management

Il Configuration Management verifica se i Configuration Item (configurazioni e sistemi operativi dei routers, firewall, switch, server, documentazione attinente agli apparati), siano correttamente aggiornati ed allineati secondo le procedure concordate e che siano state create le copie di back-up mantenendo la storicità delle configurazioni precedenti.
Il Configuration Management mira a garantire il massimo dell'efficienza, minimizzando i tempi di Incident, nel caso di ripristino di situazioni pregresse, garantendo la possibilità di recuperare situazioni antecedenti la comparsa di eventuali problemi. Valuta, inoltre, l'impatto delle richieste di cambiamento sulle release software e sui servizi erogati.
Per la finalità di questo servizio il Fornitore si dovrà dotare, con oneri a suo carico, (Hardware e Software) di un data base modello CMDB (Configuration Management Data Base) secondo le linee guida ITIL.

Attività a carico del Fornitore:

- fornire (hardware e software) sistema di raccolta/gestione di tutte le informazioni, configurazioni, immagini di pc, immagini dei server, apparati di rete/fonia/posta, relative al parco macchine dell'Ente;
- installazione hw dei sistemi di raccolta e gestione dati;
- installazione sw dei sistemi di raccolta e gestione dati;
- configurazione sw dei sistemi di gestione dati;
- garantire l'operatività e l'aggiornamento (patch, upgrade) dei sistemi di gestione dati;
- raccogliere tutte le informazioni, configurazioni, immagini di pc, immagini dei server, apparati di rete/fonia/posta, relative al parco macchine dell'Ente;
- migrare la base dati esistente presente presso l'Ente sul sistema di gestione richiesto in fornitura;
- eseguire attività di allineamento tra la base dati migrata e la situazione attuale dell'Ente;
- aggiornare o produrre, se mancanti, gli schemi di rete e più in generale gli schemi rappresentativi dei **Servizi** componenti la fornitura;

Piazza Ospedale Maggiore, 3 20162 Milano – Tel. 02 6444.1 – Fax 02 6420901- C.F. e P.I. 11390840152 - www.ospedaleniguarda.it

- mantenere e controllare l'efficienza dei sistemi atti alla raccolta in automatico delle configurazioni dei sistemi operativi del parco apparati, installazione patch e upgrade dei sistemi di gestione;
- mantenere in modo affidabile le informazioni e le immagini dei software specifici per ogni apparato operativo. Proporre il modello per la registrazione di tutti i componenti attivi o in store, le relazioni fra loro e le informazioni sul produttore, lo status e la documentazione disponibile;
- allineare in modalità manuale gli archivi sopra descritti nel caso non risulti possibile agire in modalità automatica;
- eseguire tramite controlli scadenzati (#semestrale) la verifica sulla congruità dell'intero parco, controllando l'allineamento e l'obsolescenza delle release hardware e software dei diversi apparati, archiviando le configurazioni e garantendone sempre la disponibilità;
- prendere in carico la documentazione sulla dislocazione di tutto il parco apparati;
- mantenere aggiornate le documentazioni relative agli apparati oggetto di fornitura del servizio;
- mantenere aggiornati gli schemi relativi alle infrastrutture e sistemi in fornitura;
- fornire accurate informazioni e documentazione per supportare le altre linee operative e l'Help/Service Desk, fornire dettagliate informazioni sull'allineamento, sullo stato degli archivi e sulle componenti in esso contenute;
- creare ed aggiornare la documentazione tecnica di gestione degli attacchi utente sia lato centrale che lato permutazione.

Attività a carico dell'Ente:

- fornire il software e le licenze necessarie ai sistemi e alle infrastrutture oggetto della Fornitura, se non diversamente indicato;
- approvare gli aggiornamenti sw;
- approvare le procedure operative proposte dal Fornitore.

7.1.2.7 Release and Deployment Management

Il release management effettua la gestione e la messa in produzione dei cambiamenti inerenti il software dell'infrastruttura e dei sistemi (anche l'eventuale sistema operativo degli apparati).

Attività a carico del Fornitore:

- valutazione dell'impatto e delle varie fasi da implementare per cambiamenti sulle release software/sistemi operativi o sui servizi erogati;
- configurare i sistemi e gli apparati delle infrastrutture sia centrali che periferici per l'erogazione di nuovi servizi o per il miglioramento di quelli attualmente in produzione;
- installare le nuove release sw e/o patch su le componenti dei **Servizi se** richiesto;
- eseguire e gestire l'aggiornamento Hw e Sw di tutte le componenti dei **Servizi**, facendo eventuale escalation verso il proprio competence centre;
- eseguire e gestire l'aggiornamento Hw e Sw di tutte le componenti dei **Servizi**, facendo eventuale escalation verso competence centre di fornitori terzi;
- proporre gli aggiornamenti Hw e Sw;
- installazione e configurazione dell'antivirus, consiste nella gestione della configurazione dei prodotti antivirus installati sugli apparati, mantenendoli aggiornati nel tempo;
- fornire consulenza e supporto alle altre linee operative;
- gestione delle patch dei **Sistemi Operativi** (**SO**), sarà cura del personale di presidio mantenere la storia delle patch rilasciate da Microsoft o altri fornitori di sistema operativo per permetterne l'eventuale recupero o per ripercorrere in direzione inversa il processo di upgrade;

Piazza Ospedale Maggiore, 3 20162 Milano – Tel. 02 6444.1 – Fax 02 6420901- C.F. e P.I. 11390840152 - www.ospedaleniguarda.it

- gestione delle patch dei **sistemi di virtualizzazione**, sarà cura del personale di presidio mantenere la storia delle patch rilasciate dai vari vendor (es. vmware) o altri fornitori di sistema di virtualizzazione per permetterne l'eventuale recupero o per ripercorrere in direzione inversa il processo di upgrade

I tempi di intervento e di ripristino sono definiti in base agli SLA di capitolato.

Tali attività dovranno essere costantemente verificate e programmate anche con il supporto della figura di cyber security che avrà anche il compito di supervisionare l'aggiornamento di ogni parte dei sistemi di infrastruttura eventualmente soggetti a criticità di sicurezza.
Mensilmente dovrà essere predisposto un report che descriva in modo sintetico la situazione degli aggiornamenti dei sistemi, indicando la release attualmente installata e l'eventuale release (major o minor) successiva.

Attività a carico dell'Ente:

- fornire le licenze software;
- assicurare l'accesso ai locali dove necessita eseguire l'intervento;
- approvare le procedure operative presentate dal Fornitore;
- approvare gli aggiornamenti proposti.
- mettere a disposizione le componenti Hw e Sw per gli aggiornamenti tecnologici.

7.1.2.8 Attività straordinarie

Tra le attività di Release Management, inerenti la gestione dei **Servizi**, che necessitano un'attenta pianificazione e coordinamento vi sono:

- eventuale cambio di Internet Service Provider (**ISP**) con conseguente **cambio d'indirizzamento** IP, configurazione DNS, configurazione apparati di rete, aggiornamento schemi e configurazioni, comunicazione del nuovo indirizzamento a Fornitori terzi per l'aggiornamento dei siti/domini presenti presso l'Ente. Si prevedono al massimo **tre attività** del genere nell'arco della durata contrattuale;
- eventuale **cambio Provider di Fonia** di linee esterne (flussi principali) con conseguente configurazione lato centrale del sistema telefonico, aggiornamento schemi e configurazioni. Si prevedono al massimo **tre attività** del genere nell'arco della durata contrattuale;
- configurazione dei sistemi e delle infrastrutture su **nuovi ambienti** (branch office) con conseguente collegamento/integrazione con i sistemi e le infrastrutture esistenti. Si prevedono al massimo **tre attività** del genere nell'arco della durata contrattuale e per strutture periferiche che non superino i **50 dipendenti**. Su indicazione dell'Ente verrà richiesta la stesura di un report riassuntivo;
- attività di test e verifica #**annuale** sulla tenuta del sistema di **batterie della centrale telefonica**, con eventuale sostituzione del sistema batterie in caso di necessità.
- attività di test e verifica annuale sulla tenuta del sistema di **batterie collegate ad apparati di rete**, con eventuale sostituzione del sistema batterie in caso di necessità.
- nel caso, durante la durata contrattuale, debbano essere apportare modifiche e/o aggiornamenti che si rendessero necessari a seguito di **variazioni legislative e/o normative** a livello regionale, nazionale, il Fornitore dovrà farsi carico delle attività necessarie ad allineare i **Servizi** secondo la normativa vigente e questo senza oneri aggiuntivi a carico dell'Ente. In presenza di norme suscettibili di più interpretazioni, gli interventi di manutenzione e/o aggiornamento rifletteranno l'interpretazione dell'Ente.
- Con cadenza #**annuale**, il Fornitore dovrà effettuare **prove di disaster recovery** così come indicato dall'Ente, sui **Servizi** in sua gestione.

Piazza Ospedale Maggiore, 3 20162 Milano – Tel. 02 6444.1 – Fax 02 6420901- C.F. e P.I. 11390840152 - www.ospedaleniguarda.it

- Tutte le attività di **IMAC** straordinarie su apparati ad **Alta e Media Criticità** (Apparati di Rete, Centrali telefoniche, IVR, Server, ecc.) che impattano sul servizio dovranno essere svolte, salvo diverse indicazioni dell'Ente **al di fuori dell'orario di presidio**;
- **#50 giornate all'anno per il LOTTO1 e #25 giornate all'anno per il LOTTO2** ad opera di **strutture di progettazione** (del Fornitore aggiudicatario) da dedicare ad attività di progettazione complessa definite durante le riunioni mensili (SAL). Qualora le giornate non dovessero essere erogate nell'anno solare corrispondente, **potranno essere utilizzate negli anni a seguire**.
- **10 giornate all'anno di un DBA** (Data Base Amministrator). Qualora le giornate non dovessero essere erogate nell'anno solare corrispondente, **potranno essere utilizzate negli anni a seguire.**
- **Pulizia accurata** dei locali tecnici dell'**Ente** con cadenza #annuale.

Tali attività straordinarie ai punti sopra esposti dovranno essere effettuate senza oneri aggiuntivi a carico dell'Ente, sia in termini di progettazione sia in termini di implementazione.

7.1.2.9 Transition Planning and Support

Il Fornitore dovrà produrre periodicamente, con cadenza almeno annuale, un piano operativo di aggiornamento tecnologico del parco apparati installati da proporre all'Ente.
L'installazione e il trasloco degli apparati dovrà essere previsto come attività ordinaria compresa nella fornitura.
Il Fornitore dovrà pianificare ed eseguire l'intero ciclo necessario per il rinnovo tecnologico oggetto della fornitura e comprensivo di:

- ricevimento merce vedi § 7.1.2.14
- installazione software di base sul nuovo apparato;
- trasferimento dati e caricamento di eventuali applicativi presenti sul vecchio apparato;
- installazione del nuovo apparato;
- rimozione e stoccaggio del vecchio apparato nei magazzini dell'Ente;
- smaltimento del vecchio apparato § 7.1.2.14

7.1.2.10 Service Validation and Testing Management

Obiettivo principale di questo servizio è quello di definire una o più configurazioni hardware e software standard, che saranno utilizzate dall'Ente.
Il Fornitore è tenuto inoltre a segnalare all'Ente la disponibilità di nuove versioni software dei sistemi operativi degli apparati e dei driver utilizzati qualora si verifichino i seguenti eventi:

- disponibilità di versioni significativamente più aggiornate rispetto a quelle in esercizio;
- individuazione di malfunzionamenti delle versioni in esercizio **per cui vengano rese disponibili patch o rilasci di versioni che risolvano tali problemi**.

In seguito a tali segnalazioni dovranno essere concordate le operazioni di aggiornamento delle corrispondenti immagini e il Fornitore dovrà rendere operativa ogni variazione.
Nel caso in cui tali variazioni implicassero operazioni di aggiornamento di apparati in esercizio, dovranno essere concordati tempi e modi.

In sintesi:

- il Fornitore terrà sotto controllo il mercato per individuare tempestivamente la disponibilità di versioni aggiornate o patch per la risoluzione di eventuali problemi, segnalando all'Ente il risultato di tali osservazioni in un rapporto che dovrà essere valutato dall'Ente per l'impatto sull'organizzazione e per

Piazza Ospedale Maggiore, 3 20162 Milano – Tel. 02 6444.1 – Fax 02 6420901- C.F. e P.I. 11390840152 - www.ospedaleniguarda.it

una valutazione dei benefici attesi, dei rischi e degli eventuali disservizi. ***#Attività da schedulare annualmente***

- il Fornitore manterrà l'amministrazione delle immagini, costituendo con ciò i riferimenti di standard per le componenti di base applicative per la produttività degli apparati.

Dovrà garantire inoltre processi di aggiornamento anche parziale del software installato sugli apparati oggetto di questa fornitura.

Il Fornitore dovrà gestire l'elenco del Sw applicativo già testato e la documentazione a corredo utilizzando risorse proprie comprese nella fornitura.
Al fine di garantire un corretto ciclo di validazione dell'apparato, il Fornitore deve costituire a proprio carico un laboratorio attrezzato (**Validation Lab**) con tutte le componenti Hw, Sw e di infrastruttura atte a replicare quanto più possibile la situazione reale di funzionamento delle apparecchiature; a questo scopo l'Ente metterà a disposizione del Fornitore i locali da adibire per il laboratorio.

Il processo di validazione dovrà seguire le seguenti fasi operative:

- Rilevazione esigenze di Validation
- Preparazione del *Test Plan* unitamente con l'Ente
- Preparazione dell'ambiente di laboratorio per replicare il contesto operativo degli apparati
- Esecuzione del *Test Plan*

Rilevazione esigenze di Validation

Gli scenari operativi tipici che portano a rilevare una esigenza di validazione possono essere:

- **Change Management**
  È il caso di richiesta di installazione di applicativi/servizi nell'ambito del servizio di change management. La richiesta di installazione, dopo approvazione dell'operazione da parte dell'Ente, sarà passata via trouble ticketing al Presidio che avrà il compito di controllare che l'applicativo/servizio sia già stato validato nella configurazione target e, qualora ciò non fosse già avvenuto, attiverà la fase di Validation for Delivery.
- **Rinnovo Tecnologico**
  Il rinnovo tecnologico degli apparati può introdurre delle esigenze di test e validazione qualora la nuova apparecchiatura richieda una configurazione Sw diversa da quella in cui i servizi e/o le applicazioni erano state certificate.
  Rientrano in questa tipologia, ad esempio, il rinnovo degli apparati di rete, l'aggiornamento dei sistemi operativi dei server, l'aggiornamento dei software, l'aggiornamento di firmware relativi a parti degli apparati oggetto della fornitura, ecc.

Preparazione del Test Plan

Sulla base delle esigenze di validazione, il Presidio redige il Test Plan, in cui sono specificati l'ambiente di test, la Check List per il Test ed i deliverables da fornire al termine dell'attività; l'Ente approverà la check list per la validazione.

Preparazione del Laboratorio

Il Test Plan può prevedere la sola attività di laboratorio oppure, nei casi più complessi, anche una attività pilota su isole di utenti predefiniti.

È a carico del Fornitore installare le apparecchiature fornite dall'Ente e fare il set-up dell'ambiente di test.

Nel caso di test pilota, l'attività prevede:

- Individuazione degli utenti Pilota
- Installazione delle nuove componenti

Piazza Ospedale Maggiore, 3 20162 Milano – Tel. 02 6444.1 – Fax 02 6420901- C.F. e P.I. 11390840152 - www.ospedaleniguarda.it

- Monitoring delle applicazioni per il tempo previsto
- Analisi degli errori e rimozione delle incompatibilità
- Reporting verso l'Ente

Esecuzione Test Plan

Sulla base della Check List approvata dall'Ente, vengono eseguiti i test di validazione degli applicativi sulla nuova configurazione. Qualora il test evidenzi errori o non conformità rispetto alla check list, il Fornitore coinvolgerà l'Ente per l'analisi della incompatibilità.

L'attività di Validation si chiude con i seguenti deliverables:

- **Report di Validazione**
  Riporta gli obiettivi dell'attività, la Check List eseguita e i risultati ottenuti. Il documento è inviato dal Fornitore all'Ente.
- **Note Operative di Installazione**
  È il documento che riporta le informazioni tecniche di supporto per il componente testato: procedura di installazione, configurazione e, laddove possibile, troubleshooting guide.
- **Sw Media**
  Si tratta di archiviare sul CMDB il Sw che è stato validato.
  Il Sw può essere anche ripacchettizzato qualora tra gli obiettivi della validazione era inclusa la costruzione di un kit di installazione.

7.1.2.11 Knowledge Management

Il Fornitore dovrà produrre e mantenere aggiornate tutte le procedure operative atte alla creazione e conservazione della documentazione, nonché la documentazione stessa per tutte le attività in fornitura.
Tutta la documentazione prodotta sarà di proprietà dell'Ente.

7.1.2.12 Incident Management e Problem Management

Come definizione, il processo di Incident Management aiuta a risolvere l'anomalia o l'errore che si può verificare e a ripristinare velocemente l'erogazione del servizio.
Nell'ambito del Problem Management invece, se si sospetta di un problema ricorsivo all'interno dell'infrastruttura IT, l'analisi proattiva del problema aiuta ad identificarne la causa in anticipo rispetto all'insorgenza del problema.
Una volta che le cause sono state identificate, viene presa una decisione per fare in modo che siano implementati i miglioramenti all'infrastruttura necessari a prevenire l'insorgere di nuovi incidenti.
L'attività è svolta principalmente dai sistemisti di presidio NOC, esperti dei sistemi e delle infrastrutture oggetto della fornitura che, sulla base dei problemi individuati, apportano le modifiche necessarie alle configurazioni dei **Servizi** salvaguardando al massimo l'operatività dell'impianto e, comunque, prevedendo piani di ripristino in caso di malfunzionamenti.
I sistemisti di presidio si avvarranno del Competence Center sito presso il Fornitore per problematiche di tipo specialistico, ovvero in tutti quei casi ove sia necessario eseguire on-site o da remoto un'analisi di livello superiore. Potranno in prima persona o delegando al supporto di livello superiore aprire un "case" sul problema "irrisolto" direttamente al Technical Assistance Center del fornitore della tecnologia in uso.

Attività a carico del Fornitore:

Fase di rimozione del guasto:

Piazza Ospedale Maggiore, 3 20162 Milano – Tel. 02 6444.1 – Fax 02 6420901- C.F. e P.I. 11390840152 - www.ospedaleniguarda.it

- Utilizzare lo strumento di Trouble Ticketing (TT) per la gestione dei ticket sulle code di propria competenza;
- supportare il Service Desk nell'individuazione del problema, utilizzando gli strumenti idonei ed effettuando le operazioni necessarie per determinare il problema ed individuare la causa del disservizio;
- supportare da remoto o on-site le altre linee operative presenti presso l'Ente durante la fase di "trouble shooting" ad esempio organizzando interventi congiunti;
- **raccogliere le richieste che provengono in genere dal Service Desk, dai tecnici che si trovano sul campo o dai referenti dell'Ente. In questo caso deve essere comunque aperto il trouble ticket dal sistemista di presidio;**
- prendere in carico, analizzare e risolvere temporaneamente o definitivamente i disservizi dovuti a malfunzionamenti del cablaggio, dei sistemi e delle infrastrutture sia a livello centrale che di utenza finale;
- eseguire attività on-site per il controllo delle connessioni fisiche a fronte di un fault dei sistemi e delle infrastrutture, con strumentazione adeguata (tester specifici);
- operare remotamente sugli apparati e sulle componenti del sistema per realizzare le soluzioni individuate;
- dove necessario provvedere personalmente alle attività on-site o richiedere l'intervento per supporto (hw replacement o supporto tecnico on-site);
- gestire i processi di escalation al proprio interno o verso fornitori terzi;
- provvedere e supportare la riconfigurazione e riattivazione dei servizi;
- ripristinare la configurazione esistente in termini di utenze e servizi;
- upgrade dei software o dei sistemi operativi degli apparati oggetto di fornitura qualora si dovessero evidenziare bachi che ne compromettano le normali attività;
- fornire il supporto sistemistico per il ripristino funzionale degli apparati oggetto della fornitura;
- eliminazione dei virus sui **Servizi** oggetto di fornitura;
- informare l'Ente sullo status dell'intervento e se la soluzione richiede l'emissione di una patch software da parte del fornitore (Allied Telesyn, Cisco, Microsoft, etc.), comunicare tempestivamente la prevista data di disponibilità della patch certificata;
- pianificare l'eventuale ulteriore intervento di installazione della patch per la rimozione definitiva del problema;
- riparare o sostituire integralmente le apparecchiature o le parti risultate difettose;
- reinstallare i sistemi operativi e software a fronte di problematiche;
- nel caso il componente sostituito contenga la configurazione, immagine software, il tecnico provvede al ripristino attingendo autonomamente dal CMDB;
- controlli ed interventi di ripristino sui siti Internet e Intranet;
- operazioni di shutdown e restart dei sistemi e degli apparati delle infrastrutture;
- eseguire riallineamento delle antenne wireless in caso di spostamento dei supporti;
- definire ed attivare quando necessario le procedure d'emergenza per garantire il collegamento telefonico dell'Ente al massimo livello consentito dai sistemi di emergenza stessi (es. linee telefoniche dirette esterne, linee di emergenza, commutatori, etc.) anche fuori orario del servizio di presidio;
- assistenza sull'uso di messaggistica, segreterie, creazione di gruppi e tutte le funzioni previste dal sistema telefonico;
- collegarsi, se richiesto, al sistema di gestione remota delle PDL (fornito dell'Ente) in caso di necessità per avere una visione più dettagliata e proattiva della problematica rilevata dal personale dell'Ente **in modo tale da fornire supporto direttamente al personale dell'Ente che ha aperto il ticket**.
- Tra le attività richieste nell'ambito del servizio possono esserci anche lo **spostamento fisico dei server** da un rack ad un altro, **spostamento delle mattonelle del pavimento flottante per il**

Piazza Ospedale Maggiore, 3 20162 Milano – Tel. 02 6444.1 – Fax 02 6420901- C.F. e P.I. 11390840152 - www.ospedaleniguarda.it

passaggio di cavi.

- Gestione delle suite **Office 365** in particolar modo della componente **Posta, Share point, One Drive, Teams** a livello **amministrativo** di sistema

Fase di chiusura guasto e gestione della documentazione:

- tenere traccia di ogni fault assegnato, dei tempi delle varie fasi di risoluzione;
- eseguire le prove di funzionalità dell'impianto ai fini della certificazione di intervento eseguito positivamente dopo la sostituzione di parte o dell'intero apparato;
- mantenere un database con le soluzioni dei problemi risolti;
- chiusura del trouble ticket assegnato alla propria coda di competenza dall'Help Desk;
- fornire report riassuntivo fault, se richiesto.
- fornire una reportistica #mensile sugli interventi di manutenzione straordinaria o a seguito di malfunzioni, indicando il tipo di intervento, la causa del malfunzionamento, l'ora di intervento;

I tempi di intervento e/o di ripristino sono definiti in base agli SLA di capitolato.

Attività a carico dell'Ente:

- approvare la soluzione a fronte di un fault;
- assicurare l'accesso ai locali dove necessita l'intervento;
- approvare le procedure operative presentate dal Fornitore;
- approvare modello dei report riassuntivi.

Per quel che riguarda la gestione **delle apparecchiature definite ad alta e media criticità** il Fornitore si farà carico dei servizi di manutenzione e assistenza tecnica alle condizioni sopra descritte. La finestra d'intervento sarà però estesa h24 7X7 365 gg. con intervento di un tecnico on site munito di scorta per la riparazione del guasto, anche attingendo al magazzino parti e muletti sostitutivi in caso di guato non riparabile.

In generale per ciascun apparato oggetto del servizio in fornitura (apparati ad alta, media e bassa criticità) sia centrale che periferico (telefoni, tastierini, Access Point, ecc.) comprensivo di ogni sua parte, qualora si verificasse un guasto che comportasse la sostituzione di una parte o dell'intero apparato, il Fornitore dovrà garantire, con oneri esclusivamente a proprio carico, la sostituzione mediante fornitura, installazione e configurazione dell'intero apparato o della parte guasta.

Nel caso in cui l'apparato centrale e/o periferico o sua componente, non fosse più reperibile, si dovrà procedere alla sostituzione con un apparato equivalente e questo con oneri completamente a carico del Fornitore. L'obbligo di riparazione o sostituzione a carico del Fornitore si applica esclusivamente agli apparati e alle componenti espressamente identificati negli Allegati tecnici come inclusi nel servizio di manutenzione full risk.

Per ciascun apparato incluso dovranno essere indicati almeno la classificazione come centrale o periferico, il produttore, il modello, la consistenza, lo stato di supporto del produttore e, ove disponibile, l'anno di installazione.

In caso di irreperibilità della parte o dell'apparato originario, il Fornitore dovrà proporre un componente tecnicamente equivalente o migliorativo, compatibile con l'infrastruttura esistente e preventivamente approvato dall'Ente. La sostituzione dovrà comprendere fornitura, installazione, configurazione, migrazione delle configurazioni, collaudo e aggiornamento della documentazione.

Piazza Ospedale Maggiore, 3 20162 Milano – Tel. 02 6444.1 – Fax 02 6420901- C.F. e P.I. 11390840152 - www.ospedaleniguarda.it

Sono esclusi dall'obbligo di sostituzione full risk gli apparati espressamente indicati negli Allegati tecnici come esclusi, nonché le sostituzioni derivanti da ampliamenti, rinnovi tecnologici programmati o esigenze non riconducibili a guasto, salvo diversa previsione contrattuale.

I tempi di intervento e di ripristino sono definiti in base agli SLA di capitolato.

7.1.2.13 Backup Management

Il servizio si occupa di garantire, pianificare, sviluppare e verificare le procedure, atte al salvataggio e all'eventuale ripristino dei dati e del sistema operativo, dei **Servizi** dell'Ente.

Attività a carico del Fornitore (elenco indicativo e non esaustivo):

- creare le immagini delle configurazioni sw;
- eseguire le procedure di backup e recovery con frequenza concordata tra Ente e Fornitore;
- eseguire le procedure di backup secondo le modalità previste;
- garantire la capacità di ripristino dei dati necessari al funzionamento del servizio;
- garantire l'integrità e la disponibilità dei dati necessari al funzionamento del servizio in caso di eventi che comportino perdite di dati statici e variabili;
- controllare che tutte le attività di salvataggio siano congruenti allo status di esercizio ed abbiano avuto buon esito;
- proporre contenuto report riassuntivi backup/restore;
- fornire report riassuntivi backup/restore;
- fornire indicazioni sulle soluzioni per migliorare le capacità di ripristino dati.

Attività a carico dell'Ente:

- fornire il software e le licenze necessarie ai sistemi e agli apparati;
- approvare il modello riassuntivo dei report backup/restore;
- approvare le procedure operative presentate dal Fornitore.

7.1.2.14 Gestione Logistica

Ha il compito di organizzare e pianificare la conduzione delle attività a supporto del processo di approvvigionamento, mantenimento e dismissione del bene.

Le attività a carico del Fornitore**,** sia all'inizio che durante tutta la durata contrattuale sono le seguenti:

- gestione della consegna di tutte le apparecchiature provenienti dal Fornitore aggiudicatario o da Fornitori Terzi di HW e sistemazione presso i locali adibiti a magazzino indicati dall'Ente, **con totale carico di responsabilità e competenza**;
- verifica fisica della conformità dei prodotti ricevuti in base all'ordine (accettazione);
- consegna, disimballaggio e configurazione dell'apparecchiatura presso il laboratorio di test (**Validation Lab**) per il caricamento del sw necessario;
- disinstallazione, imballaggio, stoccaggio in magazzino delle apparecchiature da sostituire.
- smaltimento delle apparecchiature dismesse dall'Ente e/o dei loro imballaggi.

Lo smaltimento delle apparecchiature ormai obsolete è a carico del Fornitore, anche nel caso in cui queste non siano incluse nell'elenco indicato nell'allegato tecnico, ma della stessa tipologia, garantendo la distruzione **senza possibilità di ripristino dei dati in essi contenuti nel rispetto della normativa vigente**.

Piazza Ospedale Maggiore, 3 20162 Milano – Tel. 02 6444.1 – Fax 02 6420901- C.F. e P.I. 11390840152 - www.ospedaleniguarda.it

Le modalità operative per la sostituzione dovranno essere concordate con l'Ente, e dovranno comunque rendere disponibili contestualmente le vecchie e le nuove apparecchiature per un periodo di tempo sufficiente a garantire la migrazione di quanto presente nella vecchia apparecchiatura (dati e programmi).
Tale attività di migrazione sarà a carico del Fornitore.
Il Fornitore dovrà concordare il programma dei lavori con i diretti interessati, interni o esterni alla sua struttura, e con l'Ente, per le eventuali azioni di competenza e per assicurare la necessaria condivisione da parte della struttura interne all'Ente, destinataria finale dei servizi e dei beni acquisiti.
Agirà in qualità di project manager nella pianificazione e nell'esecuzione delle attività previste avvalendosi di un referente interno all'Ente.
Il Fornitore pertanto sarà l'unico responsabile dell'esecuzione nei tempi programmati di tutte le attività necessarie alla consegna e allo smaltimento delle apparecchiature informatiche.
Dovrà inoltre farsi carico di tutte le operazioni di registrazione, nel sistema informativo aziendale, dei dati relativi alla movimentazione dei beni, in modo conforme alle policy aziendali, consentendo l'esatta tracciatura del posizionamento del bene in ogni istante, come definito nel § 7.4 Servizio di gestione degli asset.

Tutte le operazioni effettuate dovranno trovare riscontro su documentazione cartacea controfirmata dalle parti coinvolte nel processo.

7.1.2.15 Licensing Management

Il servizio prevede che il Fornitore metta a disposizione dell'Ente dei report sulla situazione complessiva e dettagliata del parco licenze, così come riportato nei seguenti punti:

Attività a carico del Fornitore:

- report riportanti indicazioni sulla tipologia e sul numero complessivo delle licenze;
- monitoring del loro utilizzo;
- controllo e segnalazione con congruo preavviso della scadenza licenze;
- controllo che le licenze acquisite dall'Ente siano adeguate all'ambiente di lavoro in cui si opera;
- eventuale disallineamento sul numero di licenze in possesso dell'Ente ed effettivo numero di software utilizzato.

Attività a carico dell'Ente:

- acquisto delle licenze software.

7.1.2.16 Performance Management

Il processo di Performance Management ha lo scopo di anticipare le necessità di performance e workload per i sistemi e per le infrastrutture. Ha inoltre lo scopo di assicurare la disponibilità di risorse per la corretta erogazione dei relativi servizi applicativi.

Attività a carico del Fornitore (elenco indicativo e non esaustivo):

- fornire sistema (Hardware e Software) per il controllo delle **Servizi** oggetto di fornitura;
- installare sistema (Hardware e Software) per il controllo delle Performance sui **Servizi** oggetto di fornitura;
- configurare sistema (Hardware e Software) per il controllo delle Performance sui **Servizi** oggetto di fornitura;
- identificare ed eseguire in prima istanza un assesment sulle prestazioni dei sistemi e delle infrastrutture;
- pianificare ed assicurare l'utilizzo efficace ed efficiente delle risorse sui **Servizi in** fornitura;
- identificare in modo proattivo le necessità di ulteriori risorse per anticipare o risolvere problemi di performance applicativa;

Piazza Ospedale Maggiore, 3 20162 Milano – Tel. 02 6444.1 – Fax 02 6420901- C.F. e P.I. 11390840152 - www.ospedaleniguarda.it

- identificare potenziali impatti sui **Servizi**, in termini di performance, dovuti all'inserimento di nuove applicazioni o funzionalità;
- proporre azioni correttive in presenza di performance anomale dei **Servizi**;
- collaborare alla progettazione delle evoluzioni dei **Servizi**;
- proporre quali componenti dei **Servizi** debbano essere monitorati, quali tool saranno utilizzati e dove le misure saranno effettuate;
- proporre i dati che devono essere collezionati ed implementare il meccanismo di raccolta;
- raccogliere ed analizzare i dati sulle prestazioni dei **Servizi** allo scopo di identificare eventuali problemi di dimensionamento;
- proporre il modello dei report delle performance con evidenza del superamento delle soglie di controllo stabilite;
- mettere a disposizione periodicamente i report, evidenziando il superamento delle soglie di controllo stabilite;
- verificare la congruenza dei dati raccolti con i parametri di dimensionamento e di soglie stabiliti come obiettivo progettuale;
- collaborare con gli eventuali fornitori esterni per il controllo e la pianificazione del traffico soggetto a canoni o al pagamento del traffico gestito;
- gestire log di sistema, ossia verificare le eventuali anomalie riscontrate e riportate nell'event log dei **Servizi** e l'adozione della conseguente procedura concordata.

Attività a carico dell'Ente:

- approvare il sistema di monitoring;
- valutare ed approvare le modifiche proposte dal Fornitore;
- approvare modello dei report delle performance;
- approvare le procedure operative presentate dal Fornitore.

7.1.2.17 Reporting

Il Fornitore dovrà produrre con cadenza periodica, specificata al § 8 – Livello di servizio tutti i report richiesti.
Il contenuto dei report dovrà presentare informazioni chiare ed esaustive e potrà essere modificato o integrato dal Fornitore su indicazione dell'Ente che dovrà autorizzarlo.
Nell'arco della durata contrattuale, potranno essere richiesti dall'Ente dei Report Custom per tali richieste il Fornitore avrà 5 giorni lavorativi per produrre tali report.
Nell'arco della durata contrattuale, potranno essere richiesti dall'Ente ulteriori Report Ricorsivi, giornalieri, settimanali, mensili, annuali o con frequenza definita dall'Ente stesso. Il primo di tali report dovrà essere disponibile entro 5 giorni lavorativi dalla richiesta dell'Ente. Le modalità sono quelle indicate nel § 8 – Livello di servizio.

7.1.2.18 Presidio locali tecnici

Il Fornitore presente presso il presidio dell'Ente, garantisce che sia assicurato un ordine congruo alle attività che vi si svolgono, attraverso il:

- controllo dell'accesso fisico ai locali tecnici;
- supporto al personale di assistenza/manutenzione per l'accesso al locale ed il ripristino delle funzionalità;
- mantenimento dell'ordine funzionale del locale tecnico e della sua agibilità;
- compilazione di appositi moduli che tengono traccia della durata degli interventi tecnici in Server Farm "rapporto tecnico" per il personale di Fornitori terzi;
- controllo ambientale sia diretto che attraverso gli strumenti messi a disposizione dell'Ente.

Piazza Ospedale Maggiore, 3 20162 Milano – Tel. 02 6444.1 – Fax 02 6420901- C.F. e P.I. 11390840152 - www.ospedaleniguarda.it

7.1.2.19 Apparati gestiti

Il servizio gestisce tutti gli apparati appartenenti ai **Servizi** oggetto del capitolato indicati negli **Allegati tecnici specifici.**

7.1.2.20 Consulenza

Potrà essere necessaria una consulenza sistemistica al personale dell'Ente, il supporto potrà riguardare:

- supporto per lo studio e la definizione di nuovi servizi;
- supporto allo sviluppo di progetti per l'ampliamento dei sistemi e delle Infrastrutture;
- supporto ai servizi di connettività Dati e Fonia; il personale del Fornitore lavorerà in collaborazione con il personale tecnico dell'Ente per la messa a punto delle modalità operative in termini di attività necessarie per la riconfigurazione dei sistemi e per quanto riguarda gli aspetti connessi alle infrastrutture ed all'interfacciamento con i Provider;
- supporto sistemistico – ove necessario – alla problem resolution relativa ad applicazioni su **Servizi** correlati ai servizi erogati, anche nel caso in cui l'eventuale problema possa essere fatto risalire ad applicativi non standard o non in sua diretta gestione.
- definizione dei profili relativi alle active directory di dominio.

7.1.3 SERVIZIO DI GESTIONE DEGLI ASSET

Il servizio di gestione degli asset prevede la raccolta ed il mantenimento dei dati di inventario relativamente a tutti i software e a tutti gli apparati centrali e periferici appartenenti ai **Servizi** ed alle infrastrutture oggetto del servizio in fornitura.
Il Fornitore dovrà mettere a disposizione (Hardware e Software) uno strumento adibito alla corretta gestione degli asset

Attività a carico del Fornitore:

- fornire implementare e gestire un sistema Hw e Sw per la raccolta e gestione inventariale di tutti gli asset componenti della fornitura.
- mantenere aggiornato tale strumento (hardware e software) in relazione alle necessarie compatibilità con nuovi ambienti operativi, anche mediante l'upgrade ad una major release superiore.
- effettuare l'inventario iniziale di tutti gli apparati della tipologia oggetto del contratto presenti presso l'Ente;
- procedere all'etichettatura dell'asset in base alle indicazioni fornite dall'Ente;
- mantenere e controllare l'efficienza dei sistemi atti alla raccolta in automatico delle informazioni hardware di sistemi, apparati, terminali telefonici, etc.;
- mantenere e controllare le configurazioni hardware degli apparati attivi e in magazzino, ovvero tutti i dettagli hardware come: il modello dello chassis, le interfacce installate, la dimensione della memoria, gli identificativi o codice prodotto;
- eseguire l'inserimento dei nuovi dati relativi agli aggiornamenti o upgrade degli apparati in esercizio; ove la tecnologia lo consente, esegue la "discovery on-line" in automatico per aggiornare o semplicemente verificare la coerenza delle informazioni gestite;
- eseguire controlli periodici di consistenza di contenuto inventario;
- allineare in modalità manuale gli archivi sopra descritti nel caso non risulti possibile agire in modalità automatica;
- raccogliere i dati logistici degli apparati come l'ubicazione, la matricola di inventariazione dell'Ente, il responsabile o utente assegnatario;

Piazza Ospedale Maggiore, 3 20162 Milano – Tel. 02 6444.1 – Fax 02 6420901- C.F. e P.I. 11390840152 - www.ospedaleniguarda.it

- proporre contenuto report riassuntivo;
- fornire report riassuntivo;
- fornire report mirati alle varie esigenze, se richiesto;
- provvedere allo smaltimento delle apparecchiature dismesse secondo le normative vigenti, man mano che verranno sostituite, garantendone la distruzione senza possibilità di ripristino dei dati contenuti;
- controllare l'aggiornamento hw e sw di tutti i componenti, in modo tale da garantire la sopportabilità in base alle indicazioni del produttore;
- prevedere un piano di aggiornamento indicando per tempo le date di fine supporto del software e dell'hardware in modo tale da consentire all'Ente l'approvvigionamento per tempo dei componenti sostitutivi;
- mantenere e controllare le configurazioni hardware delle centrali telefoniche e apparati di rete in termini di schede presenti ed attacchi utente disponibili;
- concordare le modalità di accesso/consultazione alle strutture tecniche dell'Ente.

Attività a carico dell'Ente:

- mettere a disposizione locali adibiti a magazzino;
- approvare contenuto report riassuntivi;
- approvare le procedure presentate dal Fornitore.

7.1.4 SERVIZIO DI PROVISIONING

Il servizio comprende tutto quanto necessario (apparati, materiali e opere) alla predisposizione di nuove terminazioni utente. Tutte le nuove terminazioni utente dovranno essere collaudate e certificate.
L'ampliamento potrà riguardare anche le componenti di dorsale della rete fonia-dati e l'aggiunta degli apparati di rete, espansione delle centrali telefoniche, terminali telefonici.
Le attività in oggetto saranno preventivate dal Fornitore, approvate dall'Ente e consuntivate sulla base del listino prezzi dell'offerta aggiudicata.
Tale listino sarà costituito dalla tabella provisioning il cui formato è riportato in **Allegato Tecnico 5 – Listino Provisioning**. La tabella deve essere compilata in ogni sua parte dal Fornitore e inserita nell'offerta economica per il calcolo dell'importo annuo stimato per il servizio di provisioning.

Le voci di listino indicate nell'**Allegato Tecnico 5 – Listino Provisioning** vengono utilizzate ai soli fini dell'aggiudicazione e non costituiscono vincolo di fornitura. L'Ente si riserva di acquistare in autonomia sul mercato componenti aggiuntive relative ai **Servizi** oggetto del capitolato (Apparati/server di rete, apparati/server di fonia, terminali telefonici, software) concordando preventivamente con il Fornitore le caratteristiche generali.

Attività a carico del Fornitore:

- per ogni ampliamento, spostamento, modifica del cablaggio strutturato esistente si richiede di aggiornare le relative planimetrie in formato Visio, AutoCAD, ecc.;
- registrazione delle richieste di provisioning in un sistema consultabile dall'Ente riportante l'attività, la data della richiesta, la data pianificata, la data di esecuzione, il numero di punti eseguiti o l'attività svolta;
- registrazione giornaliera dello stato di avanzamento e di tutti gli impedimenti incontrati nella realizzazione lavori che ne determinano la sospensione o necessitano di azioni da parte dell'Ente;
- esecuzione di sopralluoghi per la preparazione dei lavori e pianificazione delle attività con gestione delle relative risorse;
- essere in grado di operare in completa autonomia con attrezzature necessarie (scale, trabattelli ecc.), nel rispetto delle norme di sicurezza, delimitazione di aree di cantiere ecc. per la realizzazione di opere

Piazza Ospedale Maggiore, 3 20162 Milano – Tel. 02 6444.1 – Fax 02 6420901- C.F. e P.I. 11390840152 - www.ospedaleniguarda.it

murarie sia per attraversamenti di pareti che per fissaggio canaline in plastica o metalliche sia di dorsale che di distribuzione in tutti gli ambienti dell'Ente (interni, sotterranei, esterni);
- provvedere alla rimozione e al ripristino nelle condizioni originarie di infrastrutture quali pannelli, controsoffitti e altro;
- operare nei cavidotti dedicati alle distribuzioni delle dorsali fonia e fibra ottica sia interni, propri o concessi da fornitori terzi, che attraversanti suolo pubblico; in caso di necessità il Fornitore dovrà farsi carico di richiedere le necessarie autorizzazioni;
- realizzazione di nuovi punti rete con componenti esterne (canalizzazione, cassetta, etc.) comprese le opere di fissaggio e gli eventuali fori di entrata nei locali;
- infilaggio cavi e realizzazione punti rete in canalizzazioni predisposte (canali di dorsale e di distribuzione, discese, scatole 503); certificazioni;
- completamento di punti rete già infilati: fornitura frutti e componenti tranne i fili, attestazione lato armadio e lato utente, certificazione;
- fornitura e configurazione di nuovi apparecchi telefonici come individuati dal listino in **Allegato Tecnico 5 – Listino Provisioning**;
- fornitura e configurazione di schede di espansione delle centrali telefoniche;
- fornitura e configurazione di nuovi apparati di rete (switch) e aggiunta di componenti agli apparati di backbone;

Attività a carico dell'Ente:
- esecuzione di lavori murari per allargamento cavedi esistenti, realizzazione di nuovi cavedi, attraversamento solette, rimozione impedimenti particolari segnalati dal Fornitore;
- fornire le documentazioni di progetto quando disponibili e indicazione delle attività legate a traslochi, ristrutturazioni, ecc.
- approvazione delle pianificazioni e controllo delle priorità.

La richiesta standard di predisposizione per nuovi punti rete e/o lo spostamento di punti rete preesistenti, non supererà le 50 unità mensili, quantitativi superiori seguiranno una tempistica pianificata congiuntamente tra l'Ente e il Fornitore
Le richieste urgenti di predisposizione per nuovi punti rete e/o lo spostamento di punti rete preesistenti, non supererà le 12 unità mensili.

7.2 LOTTO-3 – SICUREZZA

7.2.1 SERVIZIO DI GESTIONE DELLA SICUREZZA

Il servizio di gestione della sicurezza deve considerare il **perimetro totale dell'Ente**, deve quindi rivolgersi anche a tutti i sistemi ed infrastrutture in esso contenute **anche se non sotto la diretta gestione del Fornitore** (es. strumentazione di Ingegneria Clinica, Apparati dei Servizi Tecnici, ecc.)
Questo allo scopo di effettuare una valutazione completa ed esaustiva della tematica "sicurezza" a 360°.

Il **Servizio di Gestione della Sicurezza** deve essere articolato nel seguente modo:

1. **Gruppo dedicato esclusivamente alla Cyber Security** presso la sede del Fornitore, le figure all'interno di questo gruppo dovranno essere in grado di gestire tematiche e problematiche tecniche in tema cyber e dovranno fornire un valido supporto alla figura dello **Specialista Cyber Security;**
2. **Specialista Cyber Security** presente presso la sede dell'**Ente,** con il compito di interfacciarsi con il proprio Gruppo di Cyber Security per la gestione di tematiche e problematiche cyber, interfacciarsi con

Piazza Ospedale Maggiore, 3 20162 Milano – Tel. 02 6444.1 – Fax 02 6420901- C.F. e P.I. 11390840152 - www.ospedaleniguarda.it

i referenti dell'**Ente,** interfacciarsi con i servizi di **Cyber Security Regionali** allo scopo di gestire in maniera più proattiva e congiunta eventuali problematiche in tema di sicurezza
Lo specialista cyber sarà, inoltre, **parte integrante nel gruppo di gestione della crisi** e dovrà cooperare con il resto del gruppo allo scopo di notificare incidenti, coordinamento interno, ricezione allerte.
Lo specialista cyber dovrà pianificare, coordinare e verificare le attività in tema cyber security definite con i referenti dell'**Ente.** Tali attività saranno svolte operativamente dal personale **di presidio degli altri lotti (se non diversamente indicato),** la figura dello specialista cyber è infatti considerata una figura di coordinamento verso i sistemisti rete, fonia infrastruttura e server farm sulle tematiche di sicurezza informatica.

3. **Lo Specialista Cyber Security,** verrà incaricato formalmente come **referente CSIRT** dovrà quindi espletare tali compiti:
    a. Riceve e invia le notifiche di incidente verso il CSIRT o ACN (**entro le 24h previste**);
    b. Coordina internamente la risposta agli incidenti di sicurezza (con il CISO e i team IT);
    c. Gestisce il flusso informativo verso l'esterno (solo le informazioni necessarie, evitando divulgazioni non autorizzate);
    d. Mantiene i contatti continuativi con il CSIRT nazionale per aggiornamenti, allerte, indicatori di compromissione, ecc.;
    e. Collabora nella predisposizione di procedure interne di incident response conformi ai requisiti NIS2;
    f. E' incluso nell'Incident Response Team richiesto dalle normative vigenti, data la particolare delicatezza delle tematiche trattate all'interno di questo gruppo, l'ingaggio può avvenire H24

Il **Servizio di Gestione della Sicurezza** deve garantisce in ottica di **Cyber Security la conformità, il corretto funzionamento e l'evoluzione** dei **Servizi** dell'Ente espletando in particolare i seguenti punti **sull'intero perimetro aziendale dell'Ente**:

a. **Information Security Auditing e Analysis**, definizione di policies, consulenza proattiva in termini di identificazione delle aree di rischio ed individuazione delle soluzioni di miglioramento anche in termini di pianificazione acquisti ed applicazione degli interventi correttivi sui **Servizi** già operativi presso l'Ente e su rilascio di nuove funzionalità e/o Servizi;
b. La verifica della conformità alle varie direttive e/o normative sia a livello regionale che nazionale in vigore (**NIS2, Legge 90. ecc**.);
c. verifica della compilazione e/o l'eventuale integrazione della documentazione a corredo del servizio stesso e di proprietà dell'**Ente**, ivi comprese documentazioni richieste da: **AGID, ARIA, Garante della Privacy, ecc.;**
d. interfacciamento diretto, se necessario, con il **Servizio di Sicurezza Regionale e/o Servizi di Cyber Security in capo a Fornitori terzi** allo scopo di gestire in maniera più proattiva eventuali problematiche di sicurezza componendo un TEAM multi-fornitore dedicato alla tematica;
e. **Vulnerability Assessment and Penetration Testing, (VAPT)** con programmazione periodica così come definita dall'**Ente**.

In relazione ai servizi che verranno di seguito elencati, si precisa che tutti gli strumenti che il Fornitore riterrà opportuno utilizzare, non già presenti presso l'Ente, dovranno essere forniti, installati ed attivati dal Fornitore stesso con oneri a proprio carico.

7.2.2. Test violazione sicurezza

Piazza Ospedale Maggiore, 3 20162 Milano – Tel. 02 6444.1 – Fax 02 6420901- C.F. e P.I. 11390840152 - www.ospedaleniguarda.it

Per analizzare gli impatti di eventuali attacchi interni, esterni ed adottare le necessarie azioni correttive (preventive e/o di contrasto) dovranno essere svolte delle simulazioni di attacco, sia dall'esterno della rete dell'Ente (internet, ecc.) che dall'interno (singola postazione, ecc.), rivolte alla scoperta e definizione di tutte le vulnerabilità più note al momento, a livello di network, di database, di applicativo, oltre che essere rivolti anche all'evidenziazione di impostazioni non adeguate del sistema IDS e del sistema di gestione aziendale antivirus e antispam, ecc.
Il Fornitore dovrà condurre i test di violazione della sicurezza **sulla totalità degli asset dell'Ente** o dovrà dare supporto a servizi esterni (ad es. Servizi di Sicurezza Regionali) nell'espletamento dei test stessi.
Detti test dovranno essere condotti sia a livello generale, simulando un potenziale attaccante che non abbia già raccolto notizie relative all'architettura del sistema, sia mirate sul singolo sistema.

Tutte le suddette attività di test dovranno essere svolte senza che vi possa essere alcun degrado significativo dell'operatività quotidiana degli utenti aziendali; laddove i test potessero comportare un degrado o un blocco del sistema oggetto di test, questo dovrà essere preventivamente e opportunamente evidenziato all'Ente per esplicita approvazione.

Attività a carico del Fornitore:

- assessment iniziale sulla situazione di vulnerabilità dei sistemi e delle infrastrutture dell'Ente;
- produzione di un piano analitico di test di simulazione di attacco, soggetto a revisione #trimestrale, concordato, da sottoporre all'Ente per approvazione;
- effettuazione di test # trimestrali di violazione delle politiche di sicurezza. Detti test dovranno essere congiuntamente pianificati;
- produzione di report #trimestrali di dettaglio con gli esiti dei test effettuati e indicazione delle possibili azioni correttive, relative sia agli apparati gestiti dal Fornitore (azioni correttive da effettuarsi direttamente dal Fornitore stesso), sia ai sistemi/server testati in carico all'Ente o fornitori terzi. In particolare, ogni test svolto dovrà essere catalogato in base al livello di gravità del problema riscontrato e fornita una precisa indicazione per la correzione;
- su richiesta dell'Ente dovranno essere effettuati successivi test di approfondimento rispetto alle singole anomalie riportate, per meglio evidenziare il comportamento del sistema e le conseguenti azioni correttive.
- Supporto a servizi di gestione della sicurezza esterni (ad es. Sistema della Sicurezza a livello Regionale)

Attività a carico dell'Ente:

- approvazione del documento relativo al piano di test;
- pianificazione dei test;
- validazione delle azioni correttive proposte dal Fornitore.

7.2.3 Controllo degli accessi di rete

In una realtà aziendale come quella dell'Ente, in termini di numerosità dei nodi di rete, risulta di primaria importanza effettuare un controllo puntuale sugli accessi alla rete informatica. In questo ambito l'Ente si è già dotata di una serie di politiche di sicurezza, rispetto ai vari livelli di accesso; tuttavia, **viene richiesto al Fornitore di gestire il sistema NAC (se presente) o attivare un controllo dell'accesso alla rete informatica da parte di apparati non autorizzati e/o non appartenenti alla dotazione aziendale.**

Attività a carico del Fornitore (elenco indicativo e non esaustivo):

- **gestione** del sistema di supervisione degli accessi di rete (**NAC**) a livello di singolo nodo, con monitoraggio continuo della presenza in rete e con l'individuazione puntuale dell'armadio e/o apparato, porta di connessione;

Piazza Ospedale Maggiore, 3 20162 Milano – Tel. 02 6444.1 – Fax 02 6420901- C.F. e P.I. 11390840152 - www.ospedaleniguarda.it

- redazione di un documento, soggetto a revisione #trimestrale, contenente le azioni da intraprendere in caso di scoperta della presenza in rete di un nodo non autorizzato e i relativi tempi di intervento, da inoltrare all'Ente per approvazione;
- attivazione di un sistema automatico per la disconnessione e/o tracciamento (tramite e-mail) dalla rete dei nodi non autorizzati, con relativa segnalazione puntuale ed immediata all'Ente;
- generazione di report periodici relativi agli interventi effettuati;
- messa a disposizione dell'Ente di una console in grado di effettuare ricerche immediate di posizionamento dei nodi informatici, con evidenziazione dell'armadio, apparato, porta di rete.

Attività a carico dell'Ente:

- Approvazione del documento relativo alle azioni di disconnessione.

Le richieste di modifica delle configurazioni degli apparati firewall formulate dal Lotto 3 dovranno essere preventivamente approvate dall'Ente e successivamente eseguite dal Fornitore del Lotto 1. Ogni richiesta dovrà essere tracciata mediante Trouble Ticket e contenere almeno la motivazione, la valutazione del rischio, gli asset interessati, la configurazione richiesta, il piano di verifica e, ove necessario, il piano di ripristino della configurazione precedente.

Si precisa che tutte le attività operative relative ai Servizi descritti nei paragrafi precedenti sono da intendersi come attività ad opera del presidio, attività quali (a mero titolo esemplificativo) configurazioni di nuove LAN, servizi fonia basici, regole firewall, configurazioni access list, attivazione di protocolli di routing creazione di nuovi server virtuali o fisici, ecc. ecc. non sono considerate attività di secondo livello, nonostante ciò il Fornitore deve essere munito di un servizio di secondo livello, nonché di terzo livello (escalation verso il vendor delle varie tecnologie) per supportare e risolvere tematiche che il presidio non riesce o non è in grado di gestire.
Tali attività non vengono in alcun modo considerate come giornate di progettazione e/o ingegneria.

Piazza Ospedale Maggiore, 3 20162 Milano – Tel. 02 6444.1 – Fax 02 6420901- C.F. e P.I. 11390840152 - www.ospedaleniguarda.it

8 LIVELLI DI SERVIZIO

8.1 LIVELLI DI SERVIZIO SLA

Ai fini della misurazione dei livelli di servizio si intendono per:

1. **Tempo di presa in carico:** intervallo intercorrente tra l'assegnazione del ticket alla coda di competenza del Fornitore e la registrazione, nel sistema di Trouble Ticketing, dell'effettiva presa in carico da parte di una risorsa tecnica.
2. **Tempo di intervento:** intervallo intercorrente tra l'assegnazione del ticket e l'avvio documentato delle attività tecniche da remoto o on-site.
3. **Tempo di ripristino:** intervallo intercorrente tra l'assegnazione del ticket e il ripristino, anche mediante soluzione temporanea o workaround approvato dall'Ente, delle funzionalità essenziali del servizio.
4. **Tempo di risoluzione:** intervallo intercorrente tra l'assegnazione del ticket e la rimozione definitiva della causa del malfunzionamento, comprensiva delle verifiche tecniche e dell'aggiornamento della relativa documentazione.
5. Tutti gli eventi utilizzati per la misurazione dovranno essere registrati e verificabili sul sistema di Trouble Ticketing. Eventuali sospensioni dei tempi saranno ammesse esclusivamente per cause preventivamente definite nel contratto, documentate nel ticket e validate dall'Ente.

L'Ente richiede i seguenti orari di servizio:

Servizio	Ente		
Orari	Lun - Ven	Sabato	Festivi
Presidio	7:30 - 18:00	8:00 – 12:00	no
Reperibilità	24h		
Monitoraggio remoto	24h		

Tabella 3

Il capitolo riporta gli SLA (Service Level Agreement) che saranno contrattualizzati nell'ambito dei servizi richiesti.
Gli indicatori degli SLA sottoindicati verranno **valutati #mensilmente**.
Tutti i report dovranno essere prodotti su base **#mensile** (dove non diversamente specificato) e inviati **entro la #prima decade del mese successivo**.
Gli indicatori che costituiscono gli SLA sono descritti nella tabella che segue:

Indicatore	Descrizione
Tempo di presa in carico	Definisce il tempo che intercorre tra il rilascio di una chiamata sulla coda di propria competenza e la presa in carico del problema da parte del personale di presidio, tramite strumento di Trouble Ticketing.
Tempo di risoluzione chiamata	Definisce il tempo che intercorre tra il rilascio di una chiamata sulla coda di propria competenza e la risoluzione della stessa.
Tempo di esecuzione richiesta IMAC	Definisce il tempo che intercorre tra il rilascio di una chiamata IMAC sulla coda di propria competenza e la chiusura della chiamata di richiesta servizio.

Piazza Ospedale Maggiore, 3 20162 Milano – Tel. 02 6444.1 – Fax 02 6420901- C.F. e P.I. 11390840152 - www.ospedaleniguarda.it

Tempo di esecuzione richiesta IMAC urgenti	Definisce il tempo che intercorre tra il rilascio di una chiamata IMAC urgente sulla coda di propria competenza e la chiusura della chiamata di richiesta servizio.
Tempo di delivery procedura	Definisce il tempo che intercorre tra l'individuazione della necessità di una nuova procedura (formalizzata con mail) ed il rilascio della stessa
Tempo di disponibilità del report di guasto se richiesto	Definisce il tempo che intercorre tra la richiesta di report (formalizzata con mail) da parte dell'Ente al Fornitore, e il rilascio del report richiesto.
Tempo di messa in produzione nuovi report concordati	Definisce il tempo che intercorre tra la richiesta di report mediante(formalizzata con mail) da parte dell'Ente al Fornitore, e la messa in produzione del report richiesto e concordato.

Tabella 4

Le chiamate vengono classificate a seconda delle seguenti priorità:

- **Alta criticità**:
  - almeno una prestazione del Servizio è fuori uso a livello centrale o di reparto critico (ad esempio blocco centrale telefonica, blocco nodo di edificio, nodi di piano critici, blocco di un sistema d'infrastruttura, blocco sistema web E-mail, blocco di un Server);
  - problematiche su apparati **catalogati** come apparati ad **alta criticità**.

- **Media Criticità**:
  - almeno una prestazione del Servizio è fuori uso a livello periferico, oppure si presenta un degrado del servizio in un nodo centrale o di reparto critico ma che può essere aggirato con un workaround (es. blocco di un nodo di piano o di sue componenti, blocco di componenti delle centrali telefoniche, blocco di componenti di sistemi ridondati);
  - problematiche su apparati **catalogati** come apparati a **media criticità**;

- **Bassa Criticità**:
  - almeno una prestazione del Servizio è fuori uso a livello di gruppo utenti non critici, oppure si presenta un degrado del servizio a livello di Blocco ma che può essere aggirato con un workaround;
  - richieste IMAC;
  - problematiche su apparati **catalogati** come apparati a **bassa criticità**.

Per guasti ad Alta e Media Criticità i tempi indicati sono relativi alle 24h, per guasti a Bassa Criticità il tempo indicato è relativo all'orario di presidio.

Piazza Ospedale Maggiore, 3 20162 Milano – Tel. 02 6444.1 – Fax 02 6420901- C.F. e P.I. 11390840152 - www.ospedaleniguarda.it

8 PIANO DI COMUNICAZIONE

Questa sezione del documento descrive le modalità adottate per gestire le comunicazioni tra Ente e Fornitore, include quindi la **Matrice di Coordinamento** di tutti i partecipanti, una descrizione sulle modalità da seguire nelle **Riunioni di Coordinamento** ed i documenti che verranno prodotti e/o discussi in tali riunioni.

9.1 MATRICE DI COORDINAMENTO

L'elenco delle persone di riferimento dell'Ente sarà comunicato successivamente all'aggiudicazione della gara.

NOME	FUNZIONE	TELEFONO	E-MAIL

I nominativi delle figure professionali del Fornitore coinvolte nel progetto saranno specificati nella riunione di avviamento:

NOME	FUNZIONE	TELEFONO	E-MAIL

9.2 RIUNIONI DI COORDINAMENTO

9.2.1 Modalità

Le riunioni formali saranno un momento di incontro e discussione dei partecipanti al progetto, e quindi saranno organizzate e gestite secondo quanto qui di seguito riportato, fatte salve modalità specifiche descritte nei paragrafi successivi.

Convocazione

La convocazione della riunione potrà essere effettuata, in funzione dell'oggetto della riunione stessa, da un Project Manager (PM), da un Service Manager (SA) o da un altro dei referenti identificati nei Gruppi di Lavoro del Fornitore o dell'Ente.

Verbalizzazione

In sede di riunione (o subito dopo) sarà redatto dal Fornitore un verbale, che sarà inviato per revisione a tutti i partecipanti alla riunione stessa, per posta elettronica entro 5 #giorni lavorativi.
Le revisioni, per poter essere incorporate, dovranno pervenire entro 5 #giorni lavorativi dalla data di invio della bozza del verbale, trascorsi i quali il documento sarà consolidato, inviato a tutti i partecipanti ed archiviato.

Piazza Ospedale Maggiore, 3 20162 Milano – Tel. 02 6444.1 – Fax 02 6420901- C.F. e P.I. 11390840152 - www.ospedaleniguarda.it

9.2.2 Scopo

Le riunioni di coordinamento effettuate periodicamente con cadenza #mensile, hanno lo scopo di definire, pianificare ed approvare i progetti e valutare le problematiche che si possono di volta in volta presentare durante la durata contrattuale.
Durante tali riunioni verrà redatto dal Fornitore ed approvato dall'Ente il documento di Stato Avanzamento Lavori (**SAL**), tale documento sarà esaminato, valutato e confrontato con la pianificazione corrente ed infine approvato.
Cadenze diverse potranno essere concordate con l'Ente a seconda dell'opportunità e del periodo di progetto (report più frequenti, ad esempio settimanali, nei periodi di maggiore criticità ad es. in fase di transizione).
Due volte l'anno dovranno essere organizzati **SAL congiunti** tra il Fornitore e gli Enti allo scopo di valutare nel complesso il servizio e mettere le esperienze maturate a fattor comune.
Qui di seguito sono brevemente descritte le modalità di svolgimento delle riunioni periodiche di avanzamento lavori ed i vari tipi di report e documenti associati.

9.2.3 Report sullo Stato di Avanzamento Lavori (SAL)

Il **Report dello Stato di Avanzamento Lavori** (**SAL**), preparato direttamente dal Project Manager e/o Service Manager del Fornitore, o da qualche altro collaboratore sotto la sua supervisione, riporta le seguenti informazioni:

- **Attività svolte secondo i piani**
  Viene riportata una breve descrizione delle attività previste nel periodo ed i risultati ottenuti.
  Commenti alle attività svolte vengono aggiunti se ritenuti interessanti.

- **Attività pianificate ma non eseguite**
  Vengono elencate le attività previste e non eseguite, unitamente alle motivazioni che hanno reso impossibile l'esecuzione (ritardi di esecuzione, ripianificazione, cancellazione dell'attività, etc.). Se ci sono date di ripianificazione, esse vengono riportate.

- **Attività svolte ma non pianificate**
  Si tratta di attività che non erano state pianificate ma che sono state eseguite a seguito di necessità contingenti (anticipazione di attività, nuove attività richieste con procedure di change management, etc.)

- **Obiettivi di prossimo periodo**
  Vengono elencati i principali obiettivi del prossimo periodo.

- **Problemi e Warnings**
  Questa sezione serve ad illustrare i principali problemi incontrati, o solo previsti, che possono influenzare negativamente la riuscita del progetto e sui quali il team di progetto è chiamato alla massima collaborazione ed attenzione, al fine di rimuoverli o di aggirarli.

9.2.4 Diagrammi di GANTT e pianificazione risorse

Nella fase di predisposizione del servizio e affiancamento con il Fornitore Uscente deve essere presentato, a cura del Project Manager del Fornitore, un documento contenente il **GANTT** di attivazione e gestione dei servizi in fornitura. Inoltre, con cadenza da #mensile (e se richiesto dall'Ente) tipicamente unitamente ai SAL, dovranno essere emessi dal Fornitore diagrammi di GANTT aggiornati in modo da fornire un maggior dettaglio sullo stato dei progetti e sulla loro pianificazione, tali diagrammi rappresentano la pianificazione di base rispetto alla quale viene verificato l'avanzamento lavori.

Piazza Ospedale Maggiore, 3 20162 Milano – Tel. 02 6444.1 – Fax 02 6420901- C.F. e P.I. 11390840152 - www.ospedaleniguarda.it

La scheda con il GANTT contiene:

- identificativo della attività;
- nome attività;
- la percentuale del risultato stimato dal project manager;
- le date di inizio e fine delle attività previste;
- le date di inizio e fine effettive.

9.2.5 Report di Eccezione

Il “report di eccezione” (Exception Report) è un segnale che il Project Manager manda al Comitato di Controllo e Revisione, per avvisarlo che una o più fasi del progetto devieranno al di fuori dei margini di tolleranza.
Il “report di eccezione” descrive la deviazione prevista rispetto ai piani, fornisce una analisi sia della eccezione sia delle scelte disponibili per il prosieguo, e suggerisce la scelta più opportuna.
Il Report di eccezione contiene:

- una descrizione della causa di deviazione del piano
- conseguenze della deviazione
- le scelte disponibili
- l'effetto di ogni scelta sul progetto
- i suggerimenti del Project Manager

Un report di eccezione di solito conduce ad una riunione per l’approfondimento della materia e per stabilire la decisione finale.

9.2.6 Interfaccia con l’Ente ed “Escalation Path”

Durante il progetto, il Project Manager e/o Service Manager deve essere allertato di ogni situazione causante inefficienza e perdita di tempo. È sua responsabilità identificare queste situazioni e correggerle. Egli deve predisporre i “sensori” appropriati ed essere pronto a rispondere con rapidità quando insorgono problemi.
I problemi che non possono essere risolti internamente al progetto devono essere scalati al Comitato di Controllo.

Piazza Ospedale Maggiore, 3 20162 Milano – Tel. 02 6444.1 – Fax 02 6420901- C.F. e P.I. 11390840152 - www.ospedaleniguarda.it

10 PROCEDURE E STANDARD DI QUALITÀ

Sono riportate qui di seguito le informazioni più importanti per il mantenimento degli standard qualitativi delle attività di gestione e controllo del progetto, per quanto attiene ai contenuti del presente documento.

10.1 PROCEDURE GENERALI TRA IL FORNITORE E L'ENTE

Lo scopo di queste procedure è facilitare il Project Management nel formalizzare e mantenere un archivio storico di tutte le relazioni importanti fra il Fornitore ed il corrispondente Project Manager dell'Ente.
La procedura di gestione delle segnalazioni registra e gestisce tutte quelle che nascono durante il ciclo di vita del progetto; fornisce le informazioni sul loro stato, controlla tutto il loro processo e fornisce il riscontro a chi ha emesso la segnalazione circa le azioni che sono state intraprese di conseguenza.
Questo capitolo spiega il modo in cui vengono sollevati problemi e suggerimenti, ed il meccanismo all'interno del metodo per gestire i vari tipi di segnalazioni.

10.1.1 Tipologia delle segnalazioni

Il processo delle segnalazioni viene innescato al nascere di una criticità sul progetto, per documentare un cambiamento all'interno del progetto stesso oppure un errore riscontrato in uno delle sue parti.
Una segnalazione, che ogni membro del gruppo di progetto (Ente o Fornitore) può originare, è in generale un problema riscontrato, una differenza di opinioni, un suggerimento o una questione in sospeso, che richiede per la sua chiusura lo svolgimento di una serie di attività.
Se la segnalazione non può essere analizzata e risolta immediatamente, dovrà essere documentata e tracciata attraverso questa procedura, che gestirà pertanto solo le più significative.
Si richiede quindi al Fornitore la creazione della procedura necessaria a gestire e regolare quanto sopra esposto.

10.1.2 "Follow up" delle azioni

Durante il ciclo di vita del progetto viene richiesto al Project Manager di mantenere una lista delle azioni che sono state intraprese a seguito di una segnalazione; ovviamente una o più azioni possono essere necessarie per dar seguito ad una segnalazione, a seconda della sua tipologia e complessità.

Ogni azione deve essere assegnata ad una risorsa ben identificata, e la lista viene riesaminata durante le riunioni di avanzamento.

10.2 STANDARD PER LA PRODUZIONE DI DOCUMENTAZIONE

Di seguito indicazioni su come dovrebbe essere organizzato un documento:

10.2.1 Formato di un documento

Tutta la documentazione prodotta deve essere sottoposta a controllo di revisione, indicando la storia delle modifiche:

- Autore
- Versione
- Data
- Stato del documento
- Etc.

Piazza Ospedale Maggiore, 3 20162 Milano – Tel. 02 6444.1 – Fax 02 6420901- C.F. e P.I. 11390840152 - www.ospedaleniguarda.it

10.2.2 Linguaggio dei Documenti

Salvo quando diversamente concordato tra le parti, tutti i documenti sviluppati per il progetto saranno redatti e consegnati in lingua italiana.

Piazza Ospedale Maggiore, 3 20162 Milano – Tel. 02 6444.1 – Fax 02 6420901- C.F. e P.I. 11390840152 - www.ospedaleniguarda.it

11 PIANO DI IMPLEMENTAZIONE

Il Fornitore dovrà produrre #**entro 15 giorni** dalla comunicazione dell'avvenuta aggiudicazione un **Progetto Esecutivo** che esplichi in maniera esaustiva le modalità di attuazione della fornitura presso l'Ente dettagliando attività, tempi, risorse e procedure operative.

Il progetto esecutivo presenta la pianificazione di massima che consente di individuare i "major deliverables" e le date con i principali milestones di progetto.
Il piano deve essere suddiviso in più fasi, come di seguito riportate:

- **P1** → Fase di adempimento contrattuale, dalla comunicazione dell'avvenuta aggiudicazione alla firma del contratto
- **P2** → Fase di affiancamento con il Fornitore uscente e di predisposizione dei servizi (periodo in cui il Fornitore si prepara ad erogare i servizi in fornitura e predispone il progetto esecutivo); in tale arco temporale il numero di persone che costituisce il presidio dovrà coincidere con quanto dichiarato in offerta, mentre gli SLA e le Penali saranno a carico del Fornitore uscente. **Durata 2 mesi dalla firma del contratto all'Avviamento e consegna del servizio**
- **P3** → Fase di regime operativo. **Durata 60 mesi dall'Avviamento e consegna del servizio**

La fase di Predisposizione dei servizi (P2) prevede la formazione del personale di presidio, a carico del Fornitore, sulla base delle procedure in essere e tramite modalità "on the job". Il servizio di Remote Monitoring si inserisce in questo quadro, attivando le strutture tecnologiche necessarie e definendo le procedure opportune, secondo quanto descritto nei successivi paragrafi. Le fasi sono articolate in:

- System Audit
- Installazione
- Avviamento

La fase di Predisposizione (P2) si sviluppa su un arco temporale di **due mesi** e si conclude con una valutazione congiunta attestante l'effettiva capacità di erogazione dei servizi.

11.1 SYSTEM AUDIT

Comprende l'analisi della configurazione di tutte le infrastrutture e sistemi oggetto del capitolato, con l'obiettivo di:

- effettuare l'inventario degli apparati (HW e SW) oggetto del servizio;
- redigere gli schemi logici e fisici del cablaggio strutturato (fibra e multi coppia) su planimetrie fornite dall'Ente in formato elettronico;
- redigere gli schemi logici e fisici della rete fonia dati, in formato Visio o equivalente;
- etichettatura dei punti rete;
- mappatura dei permutatori;
- determinare il livello corrente di gestibilità remota;
- determinare e proporre le modifiche raccomandate e gli eventuali componenti addizionali necessari per assicurare il livello desiderato di servizio. Questo potrebbe comprendere, ad esempio, un "agente" software da installare sul sistema oggetto del servizio, un'apparecchiatura di misurazione, ecc.;
- definire la tabella di responsabilità operativa, sulla base di quanto proposto nel presente capitolato;
- redigere la **versione finale** delle procedure operative.

Piazza Ospedale Maggiore, 3 20162 Milano – Tel. 02 6444.1 – Fax 02 6420901- C.F. e P.I. 11390840152 - www.ospedaleniguarda.it

11.2 INSTALLAZIONE

Comprende l'installazione, l'attivazione e la configurazione dei "componenti" necessari per la gestione delle Infrastrutture e sistemi oggetto del capitolato.

1) Livello centrale e periferico
   Questa classe di attività è relativa all'installazione e avviamento dell'ambiente di gestione, e include:
   a) installazione della Management station centrale e degli applicativi per la gestione delle Infrastrutture e dei sistemi oggetto del capitolato;
   b) mappatura delle Infrastrutture e dei sistemi oggetto del capitolato;
   c) definizione dei contenuti delle soglie di performance;
   d) definizione del formato dei report periodici;
   e) attivazione dell'ambiente di gestione;
   f) documentazione delle mappe.

2) Livello distribuito:
   a) configurazione degli agenti di management;
   b) configurazione e definizione iniziale delle soglie di anomalia;
   c) test delle linee di comunicazione.

11.3 AVVIAMENTO

Nel primo periodo, l'obiettivo principale sarà determinare il "profilo ottimale" dell'ambiente sotto controllo, e quindi si procederà tramite:

- Definizione delle soglie di anomalia;
- Tuning delle prestazioni;
- Aggiustamento delle soglie di anomalia;
- Verifica procedure operative.

Piazza Ospedale Maggiore, 3 20162 Milano – Tel. 02 6444.1 – Fax 02 6420901- C.F. e P.I. 11390840152 - www.ospedaleniguarda.it

12 EXIT MANAGEMENT

Nel presente paragrafo vengono descritte le attività e le procedure, incluse nel contratto, che saranno richieste al Fornitore nella fase **finale del rapporto o qualora il singolo Ente decida il passaggio verso un servizio regionale e/o previsto da una centrale di committenza (ARIA, CONSIP, Ecc.).**

Il Fornitore dovrà effettuare nei confronti del subentrante designato (Fornitore Entrante) il passaggio delle consegne e di tutte le conoscenze necessarie a garantire la fluida transizione nella erogazione del servizio, garantendo la continuità operativa all'Ente.
Alla scadenza del contratto il Fornitore presterà l'assistenza necessaria a trasferire la gestione dei servizi all'Ente o al nuovo Fornitore per un periodo pari #**agli ultimi due mesi** contrattuali.

La fase di Exit management, oltre a quanto detto, contempla i seguenti aspetti:

- fornitura del servizio e delle modalità di garanzia di continuità nella fase di trasferimento;
- gestione del processo di trasferimento: ruoli, responsabilità, autorizzazioni e risorse da assegnare;
- diritti di proprietà intellettuale: accordi necessari, licenze, ecc.;
- due diligence: definizione della documentazione e dei contenuti da trasferire al Fornitore che subentra, nonché la definizione delle altre obbligazioni e penalità previste;
- contratti e licenze;
- sicurezza;
- piano di comunicazione.

Di seguito si riporta una traccia dei contenuti e delle caratteristiche qualificanti dell'attività di Exit, che saranno gestite in ambito Comitato di Governance dei servizi, relativamente a:

- oggetto della transizione, attività e relative modalità di esecuzione
- compiti e responsabilità di ciascuna delle parti

Le caratteristiche qualificanti si riconoscono nei seguenti aspetti:

- **Piano di Transizione**:
  le attività di affiancamento e rilascio sono specificate e governate da uno specifico Piano di Transizione, in cui saranno riportate tutte le attività previste in termini di tempi, risorse impiegate, punti di verifica e controllo dei risultati attesi, criteri di accettazione, i rischi, la cadenza degli incontri per la verifica dello stato di avanzamento delle attività;

- **Responsabilità**:
  durante il periodo di affiancamento e migrazione al termine del Contratto, la responsabilità dei Servizi viene mantenuta dal Fornitore fino al termine previsto contrattualmente;

- **Governo del processo**:
  Il Fornitore assicura tutte le attività finalizzate a coordinare e verificare la corretta ed efficace esecuzione delle attività di Affiancamento e Rilascio nel rispetto dei termini concordati nonché la coerenza con i requisiti, i vincoli ed i termini stabiliti nei documenti contrattuali; a tale scopo viene individuata una figura unica per il Fornitore (Service Manager) che coordinerà tutte le attività e che interfaccerà l'Ente ovvero l'eventuale Fornitore terzo subentrante;

- **Continuità dei servizi**:

Piazza Ospedale Maggiore, 3 20162 Milano – Tel. 02 6444.1 – Fax 02 6420901- C.F. e P.I. 11390840152 - www.ospedaleniguarda.it

al fine di garantire all'Ente il mantenimento dei richiesti livelli di servizio da parte del subentrante, nel Piano di Transizione sono previste fasi di verifica e validazione sia del trasferimento di know-how che del rilascio della documentazione; altresì, contestualmente al trasferimento delle conoscenze, si prevede un adeguato periodo di affiancamento delle risorse del subentrante nella operatività corrente del Fornitore uscente;

- **Risorse professionali**:

un gruppo di risorse del Fornitore appositamente designato affiancherà le risorse dell'Ente e/o del Fornitore subentrante per il trasferimento delle conoscenze sui servizi e sulle relative attività di gestione; il team (minimo 2 persone) sarà composto da personale già impegnato nell'erogazione dei servizi;

In particolare, il Fornitore si deve impegnare a soddisfare i seguenti requisiti generali:

- durante la fase finale, fino al termine del periodo contrattuale, non vi saranno impatti o interruzioni del servizio causate specificamente dalle attività di passaggio di consegne;
- analogamente, in tale periodo, non vi saranno decadimenti dei livelli di servizio, specificamente imputabili al passaggio delle consegne e all'affiancamento del personale del Fornitore con quello subentrante;
- nel medesimo periodo, dal punto di vista dell'utente finale, non vi saranno significativi cambiamenti, specificamente imputabili al passaggio delle consegne, che possano inficiare le attività operative.

Per quanto riguarda la presa in carico del servizio da parte del subentrante, il Fornitore si impegna a mettere a disposizione, nelle modalità di seguito indicate, tutto il proprio personale responsabile e preposto ai servizi contrattualmente previsti, ad attività quali le seguenti:

- addestramento del personale subentrante, prevalentemente con affiancamento e in modalità on the job, finalizzato alla rapida acquisizione da parte di quest'ultimo delle conoscenze specifiche dei **Servizi** oggetto del contratto;
- illustrazione della gestione del servizio e delle relative procedure di servizio in essere alla data e messa a disposizione di tutta la relativa documentazione.

La fase finale del periodo contrattuale sarà finalizzata, da una parte, alla prosecuzione dei servizi contrattualmente previsti, con il mantenimento dei livelli di servizio consolidati, dall'altra, a mettere in grado il personale tecnico indicato dall'Ente ad un efficace subentro nei servizi in questione. Per tale ragione, il Fornitore si deve impegnare nei confronti del subentrante ad un completo passaggio delle consegne ed alla fornitura di tutta la documentazione e il supporto necessari a consentire un agevole avvio del nuovo ciclo di servizio.

Gli obiettivi di cui sopra saranno raggiunti organizzando le attività nelle seguenti fasi:

- **fase di programmazione del passaggio di consegne**:
  - predisposizione e raccolta della documentazione per il passaggio di consegne (procedure, report, strumenti, …);
  - riunione preparatoria con l'Ente;
  - pianificazione incontri di passaggio delle consegne;

- **fase di affiancamento**:

  - consegna della documentazione per il passaggio di consegne;
  - effettuazione degli incontri finalizzati al passaggio delle consegne;

Piazza Ospedale Maggiore, 3 20162 Milano – Tel. 02 6444.1 – Fax 02 6420901- C.F. e P.I. 11390840152 - www.ospedaleniguarda.it

- training on the job (affiancamento) del personale subentrante per consentire la prosecuzione dei servizi senza significativi decadimenti di qualità.

Piazza Ospedale Maggiore, 3 20162 Milano – Tel. 02 6444.1 – Fax 02 6420901- C.F. e P.I. 11390840152 - www.ospedaleniguarda.it

13 ALLEGATI

- **Allegato Tecnico 1 – ASST Grande Ospedale Metropolitano Niguarda;**
- **Allegato Tecnico 2 – ASST Gaetano Pini;**
- **Allegato Tecnico 3 – IRCCS Istituto Nazionale dei Tumori;**
- **Allegato Tecnico 4 – IRCCS Istituto Neurologico Carlo Besta;**
- **Allegato Tecnico 5 - Listino Provisioning.**

13.1 INDICAZIONI DI LETTURA DEL DOCUMENTO

Per meglio dare una visione chiara ed unitaria all'interno del documento sono riportati dei codici chiave:

- # fa riferimento a scadenze e attività ricorsive da tenere sotto controllo;

ROBERTO
VILLA
24.09.2026
10:43:40
GMT+01:00

Piazza Ospedale Maggiore, 3 20162 Milano – Tel. 02 6444.1 – Fax 02 6420901- C.F. e P.I. 11390840152 - www.ospedaleniguarda.it