Azienda Ospedaliera

Istituti Clinici di Perfezionamento

Ospedale di rilievo nazionale e di alta specializzazione convenzionato con l'Università degli Studi di Milano

Servizi di outsourcing per la gestione delle apparecchiature informatiche dell'A.O. Istituti Clinici di Perfezionamento

Lotto 1 (cig n. 33821026DB): **Servizio di Help Desk, gestione PdL e apparati di rete**

Lotto 2 (cig. n. 3382108BCD): **Progettazione, fornitura e gestione dei server**

CAPITOLATO SPECIALE

Sistema Sanitario Regione Lombardia

1 Premessa 9
1.1 Legenda e terminologia 9
2 Il Contesto 11
2.1 Istituti Clinici di Perfezionamento 12
2.2 I servizi di ICT di ICP 12
3 PARTE I - PRESTAZIONI OGGETTO DELL'APPALTO E SUDDIVISIONE IN LOTTI 13
4 Lotto 1: Servizio di Help Desk, gestione PdL e apparati di rete 14
4.1 Servizi Richiesti 14
4.2 Durata del contratto 14
4.3 Modalità organizzative e luogo di fornitura dei servizi 15
4.4 Orari di copertura dei servizi 16
4.5 Servizio di reperibilità 16
4.6 Livelli di Servizio e misura della qualità del servizio 17
4.7 Variazioni del servizio 18
4.8 Variazioni di priorità nelle attività di fornitura dei servizi 18
4.9 Servizio di Help Desk 18
4.9.1 Requisiti 20
4.9.1.1 Conduzione operativa del servizio 20
4.9.1.2 Struttura a due livelli dell'help desk e relazione tra i livelli 21
4.9.1.3 Help desk 1° livello 22
4.9.1.4 Help desk 2° livello 23
4.9.1.5 Servizi informativi e supporto ad operazioni specifiche 23
4.9.1.6 Software di gestione 24
4.9.1.7 Sistema di misurazione SLA 26
4.9.1.8 Standard e norme di riferimento 26
4.9.1.9 Supporto alla gestione dei ticket originati dalla gestione dei sistemi server 26
4.10 Servizio di Gestione delle Postazioni di Lavoro (PdL) 26
4.10.1 Requisiti 27
4.10.1.1 Censimento iniziale 27
4.10.1.2 IMAC 27
4.10.1.3 Approvvigionamento 29
4.10.1.4 Installazione 29
4.10.1.5 Disinstallazione 30

4.10.1.6 Sostituzione 30
4.10.1.7 Dismissione 31
4.10.1.8 Servizi IMAC associati a cambi di sede e traslochi 31
4.10.1.9 Documentazione ciclo di vita delle PdL 32
4.11 Servizio di Gestione della rete Aziendale 32
4.11.1 Requisiti 34
4.11.1.1 Censimento iniziale 34
4.11.1.2 Gestione operativa del servizio 34
4.11.1.3 Monitoraggio automatico dell'infrastruttura di rete 34
4.11.1.4 Network management 34
4.11.1.5 Gestione dei problemi, assistenza tecnica e manutenzione correttiva 35
4.11.1.6 Manutenzione preventiva 36
4.11.1.7 Analisi dei problemi ripetitivi 37
4.11.1.8 Rendicontazione 38
4.12 Servizio di gestione del Software di base, ambiente e rete (incluso CRS-SISS) 38
4.12.1 Requisiti 39
4.12.1.1 Censimento iniziale 39
4.12.1.2 Supporto alle configurazioni SW 39
4.12.1.3 Distribuzione del Software 40
4.12.1.4 Gestione del software relativo al progetto CRS-SISS su PdL 41
4.12.1.5 Gestione operativa delle applicazioni 42
4.12.1.6 Esecuzione di interventi di aggiornamento collettivo 42
4.13 Servizio di manutenzione hardware 42
4.13.1 Requisiti 43
4.13.1.1 Manutenzione PdL ed apparati connessi 43
4.13.1.2 Manutenzione apparati di rete 44
4.13.1.3 Rendicontazione 44
4.14 Servizio di Configuration Management 44
4.14.1 Requisiti 45
4.14.1.1 Accesso del personale ICP al CMDB 45
4.14.1.2 Asset Management 45
4.14.1.3 Supporto all'asset management dei sistemi server 47
4.15 Servizio di gestione della sicurezza 47
4.15.1 Requisiti 48
4.15.1.1 Censimento iniziale 48
4.15.1.2 Responsabile della sicurezza informatica 48

4.15.1.3 Strategia di gestione ... 49
4.15.1.4 Controllo del codice malevolo ... 49
4.15.1.5 Monitoraggio di sicurezza ... 50
4.15.1.6 Configuration management per la sicurezza ... 51
4.15.1.7 Aggiornamenti ... 52
4.15.1.8 Verifica della conformità ... 52
4.15.1.9 Gestione degli incidenti di sicurezza informatica ... 53
4.15.1.10 Identificazione del personale ... 53
4.15.1.11 Supporto alle operazioni ... 53
4.15.1.12 Accesso ai dati circolanti in rete ... 53
4.15.1.13 Conformità a norme e standard ... 54
4.16 Rilascio di rapporti di servizio ... 54
4.17 Strumenti di gestione ... 54
4.18 Specifica dei livelli di servizio minimi richiesti ... 55
4.18.1 Modello di valutazione della continuità del servizio ... 56
4.18.2 SLA ... 59
4.18.3 Verifiche ispettive ... 60
4.18.4 Strumenti di misura dei livelli di servizio minimi richiesti ... 61
4.18.5 Report periodico per la misura dei livelli di servizio minimi richiesti ... 61
4.19 Penali ... 62
4.20 Struttura organizzativa ... 63
4.20.1 Struttura e responsabilità ... 63
4.20.2 Dimensione e caratteristiche del gruppo di lavoro ... 64
4.20.3 Sostituzione del personale ... 64
4.21 Modalità di esecuzione della fornitura ... 64
4.21.1 Fase di trasferimento ... 65
4.21.2 Fase di avvio ... 65
4.21.3 Fase di esercizio ... 66
4.21.4 Fase di transizione finale ... 66
4.22 Accreditamento SISS ... 66
5 Lotto 2: Progettazione, fornitura e gestione dei server ... 68
5.1 Servizi Richiesti ... 68
5.2 Durata del contratto ... 68
5.3 Modalità organizzative e luogo di fornitura del servizio ... 69
5.4 Caratteristiche del personale ... 69

5.5 Orari di copertura dei servizi 70
5.6 Servizio di reperibilità 70
5.7 Livelli di Servizio e misura della qualità del servizio 71
5.8 Variazioni del servizio 72
5.9 Variazioni di priorità nelle attività di fornitura dei servizi 72
5.10 Sala server 72
5.11 Progettazione e fornitura dell'infrastruttura server inclusa l'infrastruttura di rete della sala server. 73
5.11.1 Requisiti 73
5.12 Accesso e proprietà delle infrastrutture della sala server 74
5.13 Servizio di gestione dei Server 74
5.13.1 Requisiti 76
5.13.1.1 Censimento iniziale 76
5.13.1.2 Conduzione operativa dei server 76
5.13.1.3 Monitoraggio automatico dei sistemi e dei servizi applicativi 77
5.13.1.4 Analisi del carico dei Sistemi e monitoraggio delle prestazioni 77
5.13.1.5 Gestione degli incidenti, assistenza tecnica e manutenzione correttiva 77
5.13.1.6 Dominio e Domain Controllers 78
5.13.1.7 Gestione degli utenti 78
5.13.1.8 DHCP Server 79
5.13.1.9 DNS Server 79
5.13.1.10 Servizio NAT 80
5.13.1.11 Servizio FTP 80
5.13.1.12 File Servers 81
5.13.1.13 Print Servers 81
5.13.1.14 Server Applicativi 81
5.13.1.15 Web Server 82
5.13.1.16 Gestione sistemistica RDBMS 82
5.13.1.17 Gestione dell'Asset 83
5.13.1.18 Installazione 83
5.13.1.19 Supporto specialistico 83
5.13.1.20 Qualità del servizio 84
5.14 Servizio di gestione del Software di base, d'ambiente e di rete 84
5.14.1 Requisiti 85
5.14.1.1 Censimento iniziale 85
5.14.1.2 Supporto alle configurazioni SW 85

5.15 Servizio di manutenzione hardware 85
5.15.1 Requisiti 86
5.15.1.1 Manutenzione sistemi 86
5.15.1.2 Gestione degli interventi 86
5.16 Servizio di Gestione del Backup 86
5.16.1 Requisiti 88
5.16.1.1 Censimento iniziale 88
5.16.1.2 Gestione Ambienti del “Sistema di Backup” 88
5.16.1.3 Aggiunta di un server e sostituzione di un server esistente 89
5.16.1.4 Controllo delle operazioni di backup 89
5.16.1.5 Risoluzione failure 89
5.16.1.6 Tuning 89
5.16.1.7 Gestione delle operazioni di restore 90
5.16.1.8 Gestione delle archiviazioni 90
5.16.1.9 Definizione e implementazione di un piano di Disaster Recovery 90
5.16.1.10 Gestione delle operazioni per recovery del servizio di backup/restore 91
5.16.1.11 Gestione supporti magnetici (Tape) 91
5.17 Servizio di gestione della sicurezza 92
5.17.1 Requisiti 93
5.17.1.1 Censimento iniziale 93
5.17.1.2 Responsabile della sicurezza informatica 93
5.17.1.3 Strategia di gestione 93
5.17.1.4 Sottosistemi di sicurezza perimetrale e modalità operative 94
5.17.1.5 Controllo del codice malevolo 96
5.17.1.6 Monitoraggio di sicurezza 96
5.17.1.7 Scansione della rete 98
5.17.1.8 Configuration management per la sicurezza 98
5.17.1.9 Aggiornamenti 99
5.17.1.10 Verifica della conformità 100
5.17.1.11 Gestione degli incidenti di sicurezza informatica 100
5.17.1.12 Backup 102
5.17.1.13 Rendicontazione 102
5.17.1.14 Gestione delle utenze 103
5.17.1.15 Verifiche di sicurezza 104
5.17.1.16 Servizi di sicurezza fisica 104
5.17.1.17 Identificazione del personale 104

5.17.1.18 Supporto alle operazioni 104
5.17.1.19 Accesso ai dati circolanti in rete 104
5.17.1.20 Supporto al rispetto della normativa sulla privacy 105
5.17.1.21 Certificazioni di sicurezza informatica 106
5.17.1.22 Conformità a norme e standard 106
5.18 Servizio di Gestione della Posta Elettronica 106
5.18.1 Requisiti 108
5.18.1.1 Censimento iniziale 108
5.18.1.2 Vincoli 108
5.18.1.3 Attività di gestione e modalità operative 109
5.18.1.4 Risoluzione failure 109
5.19 Servizio di Configuration Management 110
5.19.1 Requisiti 111
5.19.1.1 Accesso del personale ICP al CMDB 111
5.19.1.2 Asset Management 111
5.20 Formazione in affiancamento 112
5.21 Rilascio di rapporti di servizio 112
5.22 Supporto al progetto CRS-SISS 112
5.23 Strumenti di gestione 113
5.24 Specifica dei livelli di servizio minimi richiesti 113
5.24.1 Modello di valutazione della continuità del servizio 114
5.24.2 SLA 117
5.24.3 Verifiche ispettive 117
5.24.4 Strumenti di misura dei livelli di servizio minimi richiesti 118
5.24.5 Report periodico per la misura dei livelli di servizio minimi richiesti 119
5.25 Penali 119
5.26 Struttura organizzativa 120
5.26.1 Struttura e responsabilità 120
5.26.2 Dimensione e caratteristiche del gruppo di lavoro 120
5.26.3 Sostituzione del personale 120
5.27 Modalità di esecuzione della fornitura 121
5.27.1 Fase di installazione e trasferimento 121
5.27.2 Fase di avvio 122
5.27.3 Fase di esercizio 123
5.27.4 Fase di transizione finale 123

6 PARTE II – CONDIZIONI GENERALI DEL CONTRATTO 124
6.1.1 Clausola di salvaguardia 124
6.1.2 Responsabilità civile, copertura assicurativa 124
6.1.3 Deposito cauzionale 125
6.1.4 Cessione del contratto, del credito e subappalto 126
6.1.5 Scioperi e cause di forza maggiore 127
6.1.6 Risoluzione del contratto e disdetta del contratto 128
6.1.7 Codice etico aziendale e Codice etico regionale degli appalti 130
6.1.8 Tracciabilità dei flussi finanziari 130
6.1.9 Fatturazione e pagamenti 131
6.1.10 Revisione prezzi 132
6.1.11 Obblighi dell'Impresa aggiudicataria 132
6.1.12 Norme di comportamento 133
6.1.13 Brevetti industriali e diritti d'autore 134
6.1.14 Obblighi connessi alla sicurezza ai sensi dell'art. 26 del D.Lgs. 81/08 134
6.1.15 Controversie 134
6.1.16 Spese contrattuali 135
6.1.17 Rinvio ad altre norme 135
7 Allegati per il lotto 1 136
8 Allegati per il lotto 2 136

1 Premessa

Gli Istituti Clinici di Perfezionamento (ICP) sono un'Azienda Ospedaliera di rilievo nazionale ad alta specializzazione, convenzionata con l'Università degli Studi di Milano. Gli ICP erogano attività sanitarie d'elevata specializzazione, prestazioni di base e di media complessità mediante l'utilizzo di tecnologie avanzate e di metodologie innovative.

L'attività di diagnosi, terapia e riabilitazione vuole rispondere alla necessità degli utenti a livello cittadino, regionale ed extra regionale.

L'Amministrazione degli Istituti Clinici di Perfezionamento riconosce l'importanza di mantenere elevati livelli di qualità ed efficienza nella gestione dell'infrastruttura informatica.

Per garantirne l'efficacia e l'efficienza, ICP ha deciso di procedere ad una gara d'appalto al fine di stipulare contratti di servizi in outsourcing per le proprie apparecchiature informatiche.

All'interno di questo documento sono state adottate le seguenti convenzioni:

L'amministrazione appaltante (Istituti Clinici di Perfezionamento), sarà indicata come ICP;

L'aggiudicatario sarà indicato come il Fornitore;

I partecipanti alla gara saranno indicati come i Concorrenti.

1.1 Legenda e terminologia

Service Level Agreement (SLA):

Definizione ed associato criterio di misura / valutazione della qualità dei Servizi che saranno erogati dal Fornitore.

Fornitore:

Il Fornitore che sarà prescelto per erogare i Servizi coperti dal Contratto

Cliente:

Il Cliente, Ente appaltante di questo Contratto è ICP.

Concorrente

Qualsiasi Partecipante alla Gara di Appalto di questo Contratto

Information Technology Infrastructure Library (ITIL®):

Un insieme di Best Practices per la conduzione e lo svolgimento dei Servizi IT, originariamente emessa dall'Office of Government Commerce del Governo britannico.

ISO 20000:

Standard internazionale per l'"IT Service Management" che riflettere le linee guida delle best practice contenute nel framework ITIL.

Calendario di lavoro:

Da Lunedì a Venerdì incluso e Sabato mattina, eccetto le Festività infrasettimanali del Calendario italiano, ed il 7 Dicembre, festività patronale.

Orario di lavoro amministrativo:

Dalle 7.30 alle 19.00, dal Lunedì al Venerdì

Orario di lavoro sanitario:

Dalle 7.00 alle 19.00, dal Lunedì al Venerdì

Dalle 7 alle 13 il Sabato

Orario di lavoro esteso:

H24*7

Incidente:

Si definisce Incidente un malfunzionamento, misurabile o percepito dall'utente, rispetto al normale comportamento atteso di un sistema o di un servizio.

Risoluzione di un Incidente:

La Risoluzione di un Incidente è definita come il ripristino dell'operatività normale dal punto di vista dell'utente. Tale ripristino può essere ottenuto attraverso la rimozione delle cause dell'incidente, o fornendo all'utente un "workaround" (soluzione provvisoria che "aggira" la difficoltà che ha causato l'incidente, senza provocare controindicazioni) per lui/lei accettabile.

Problema:

Si definisce Problema la causa "ultima" che origina un Incidente. Gli incidenti che non possono essere risolti per mancanza di soluzione disponibile al relativo problema saranno comunicati al processo di Problem Management, così come gli incidenti ripetuti relativi ad un problema noto ("known problem/error")

Software di base

Si intende per Software di base l'insieme dei programmi che consentono ad un utente di eseguire operazioni base come costruire e mandare in esecuzione un programma o gestire una base dati. Tipici esempi di software di base sono il sistema operativo, gli editors, i compilatori e i sistemi di gestione di basi di dati;

Software d'ambiente

Il Software d'ambiente rappresenta l'insieme di programmi specializzati che facilitano la scrittura / gestione di applicazioni. Tipici esempi di software d'ambiente sono gli application server.

Software di rete

Il Software di rete è inteso come l'insieme di programmi specialistici per la gestione delle comunicazioni. Tipici esempi di software di rete sono i gestori di posta ed i prodotti di gestione e condivisione di risorse distribuite.

Software applicativo

Programma che utilizza il software di base, d'ambiente e di rete per realizzare una funzione specifica legata agli scopi dell'organizzazione che lo utilizza.

Software di produttività individuale

Software utilizzato per elaborazioni individuali standard (es. WinZip, Adobe, MS Office, MS Project, …)

PdL

Postazione di Lavoro normalmente costituita da un Personal Computer dotato di adeguato Software e apparati connessi (ad esempio stampanti individuali, di gruppo e dipartimentali, scanner).

Guasto bloccante

Una o più funzioni sostanziali del sistema (Pdl o server / apparato connesso o apparato di rete) sono compromesse.

Per una PdL significa l'impossibilità di essere utilizzata per fornire uno o più dei servizi per i quali è prevista

Per un server, un apparato connesso al server o un apparato di rete significa l'impossibilità di fornire uno o più servizi per i quali è stato previsto

Guasto non bloccante

Il Sistema "malfunziona", ma il funzionamento sostanziale del Sistema non è compromesso; i servizi per i quali il sistema è utilizzato possono comunque essere forniti.

2 Il Contesto

Questa Sezione descrive il contesto in cui dovrà operare il Fornitore.

Queste sintetiche informazioni sono solo a scopo informativo, e pertanto non riflettono necessariamente ed *in toto* la presente e futura situazione di ICP.

2.1 Istituti Clinici di Perfezionamento

L'Azienda Ospedaliera "Istituti Clinici di Perfezionamento" è composta da 4 presidi ospedalieri, 23 poliambulatori (di cui 21 nel comune di Milano) e da delle sedi minori, principalmente appartenenti al Dipartimento di Salute Mentale, sparse sul territorio dei comuni di Sesto San Giovanni, Cinisello Balsamo, Cormano, Cusano Milanino e Cologno Monzese.

Per una descrizione più dettagliata dell'attività degli ICP si rimanda al sito www.icp.mi.it

2.2 I servizi di ICT di ICP

Attualmente è attivo un servizio di outsourcing globale, affidato ad una RTI composta da Dedalus (mandataria), Sysline (mandante) e Beta80 (mandante), che include:

- Gestione e manutenzione degli applicativi e delle loro integrazioni (LIS, ADT, CUP, AMB, REP, Blocco operatorio, Gestione completa delle Risorse Umane, Ordini e magazzini economali, ordini e magazzini farmaceutici, contabilità generale ed analitica, protocollo e gestione documentale, Datawarehouse ed analisi scenari, posta elettronica, siti internet ed intranet);
- Hosting dei server principali in server farm;
- Gestione e manutenzione dei server e degli storage ovunque disposti;
- Gestione e manutenzione delle postazioni di lavoro;
- Gestione e manutenzione delle reti locali;
- Gestione della rete geografica, interagendo con il fornitore della stessa (attualmente Fastweb) per la gestione delle configurazioni e la risoluzione dei guasti;
- Helpdesk di primo e secondo livello.

La gestione dei server relativi al RIS/PACS e delle workstation di refertazione è stata affidata ad un RTI composto da Agfa e Emmeesse.

La gestione delle centrali telefoniche è stata affidata, tramite adesione alla convenzione CONSIP "Centrali telefoniche 4" alla società Vitrociset.

Le risorse facenti capo all'unità Sistemi Informativi di ICP gestiscono l'infrastruttura informatica delle sedi elencate in **Allegato A**.

Presso la sala server saranno installate le componenti hardware e software di supporto a ICP. L'attuale configurazione è elencata nell'Allegato B. L'allegato B è da considerare, dal punto di vista contrattuale, indicativo della complessità dell'infrastruttura ma non esaustivo.

Gli utenti coinvolti nell'erogazione dei servizi oggetto di questo Capitolato sono circa 3800 per un totale di circa:

- 2300 Postazioni di Lavoro (PdL) (di cui circa 1000 postazioni SISS);
- 1600 periferiche di tipo diverso (stampanti ed altri apparati);
- 60 server di cui 30 fisici;

- Infrastruttura di rete.

I servizi informativi di ICP sono attualmente gestiti sia con personale interno che tramite l'utilizzo di Terze Parti.

I servizi delle Terze Parti sono erogati tramite contratti stipulati da ICP secondo la normativa vigente (Dlgs. 163/2006 e regolamenti aziendali).

I dati forniti, ivi compresi quelli inclusi negli allegati, sono di riferimento. Sarà compito del Fornitore sviluppare un'accurata attività di censimento iniziale.

3 PARTE I - PRESTAZIONI OGGETTO DELL'APPALTO E SUDDIVISIONE IN LOTTI

L'appalto riguarda l'espletamento, per conto di ICP, di tutte le attività operative e specialistiche necessarie a realizzare:

1. La fornitura dei servizi di gestione infrastruttura e supporto utenti necessari a garantire il funzionamento dell'infrastruttura informatica di ICP (e quindi delle dette apparecchiature), operando per rimuovere o superare qualsiasi impedimento operativo si presenti all'utenza, garantendo la gestione efficace della sicurezza informatica, della manutenzione hardware e software, ed in generale il supporto specialistico on-site;
2. Il monitoraggio costante e puntuale dei processi di erogazione dei servizi secondo le normali prassi contrattuali, utilizzando le opportune misurazioni/rilevazioni che si rendano necessarie per supportare ICP nella gestione dei servizi e dell'evoluzione dell'infrastruttura informatica;
3. La garanzia di un costante supporto tecnologico all'evoluzione dei processi informativi richiesti dalle normative nazionali e regionali in ambito sanitario e socio-sanitario.

L'appalto è suddiviso in due lotti distinti:

Lotto 1: Servizio di Help Desk, gestione PdL e apparati di rete;

Lotto 2: Progettazione, fornitura e gestione dei Server.

Questo documento descrive in dettaglio i requisiti sui quali il Concorrente baserà la propria offerta, ed i corrispondenti Servizi che il Fornitore dovrà fornire a ICP per ognuno dei lotti.

4 Lotto 1: Servizio di Help Desk, gestione PdL e apparati di rete

4.1 Servizi Richiesti

Il lotto include i seguenti servizi:

- **Servizio di Help Desk:** il Fornitore dovrà garantire un servizio di assistenza, comprensivo di Call Center generico, Helpdesk per le parti di competenza e interazione con gli Helpdesk di secondo livello gestiti da terze parti.
- **Servizio di gestione delle Postazioni di Lavoro (PdL):** gestione del ciclo di vita, e quindi di tutti i cambiamenti del ciclo di vita delle PdL, dall'installazione al ritiro e dismissione**.**
- **Servizio di gestione della Rete aziendale:** gestione complessiva delle apparecchiature di infrastruttura di rete locale responsabili della fornitura dei servizi informatici e della connettività agli utenti.
- **Servizio di gestione del software di base,di ambiente e di rete con inclusione del software SISS:** gestione complessiva dei componenti software di base e di infrastruttura relativi alle PdL ed alla rete aziendale sui quali si basa la fornitura di servizi applicativi. Il fornitore dovrà garantire idoneo supporto al processo di gestione delle PdL che operano come postazioni SISS con particolare riferimento al rispetto delle specifiche tecniche di progetto previste da Lombardia Informatica/Regione Lombardia.
- **Servizio di Manutenzione hardware:** riparazione / sostituzione di apparecchiature relative alle PdL ed alla rete aziendale a seguito di guasti che perturbano l'operatività del sistema messo a disposizione.
- **Servizio di gestione della sicurezza:** Il Fornitore dovrà adeguarsi alle direttive in materia di sicurezza adottate da ICP, garantendo allo stesso tempo un adeguato supporto in caso di incidenti e nella risoluzione di eventuali problemi di sicurezza informatica.
- **Servizio di Configuration Management:** gestione degli asset relativi alle PdL ed alla rete aziendale e di tutti i cambiamenti attraverso un Configuration Management Data Base.

4.2 Durata del contratto

La durata del contratto è di 5 (cinque) anni a decorrere dalla data che sarà indicata nella comunicazione di aggiudicazione definitiva, con facoltà di recesso per l'A.O. ICP dopo 3 (tre) anni.
Sarà facoltà dell'Azienda Appaltante prorogare il rapporto contrattuale – dopo la naturale scadenza dello stesso – per ulteriori **6** mesi o per il periodo strettamente necessario per l'espletamento delle procedure concorsuali di individuazione del nuovo aggiudicatario – alle medesime condizioni contrattuali in essere – senza che l'Appaltatore possa pretendere compensi ulteriori. L'aggiudicatario si obbliga, pertanto, a proseguire la fornitura del servizio dietro semplice richiesta scritta dell'A.O. con un preavviso di 30 giorni rispetto la scadenza naturale del contratto.

4.3 Modalità organizzative e luogo di fornitura dei servizi

Il servizio sarà fornito presso una sede ICP di Milano di seguito denominata "Sede centrale del servizio", che sarà comunicata all'aggiudicazione dell'appalto, attraverso la presenza di un gruppo di lavoro del Fornitore che opererà durante l'orario di copertura del servizio di seguito definito.

Il gruppo di lavoro sarà costituito da personale di competenza adeguata alla fornitura dei servizi di seguito elencati.

ICP metterà a disposizione i locali adeguati arredati e le linee telefoniche per la sede centrale del servizio. Ogni altro mezzo e strumento (ad esempio: tool software per la gestione del servizio e relativa infrastruttura server e di comunicazione di rete; mezzi di trasporto) sarà a carico del Fornitore.

Il Fornitore garantirà la presenza di parte del gruppo di lavoro, di seguito identificato come "Servizio di presidio", presso alcune sedi ICP.

Sono di seguito definite le sedi da presidiare e il relativo numero minimo di personale:

- Ospedale Buzzi. 2
- Ospedale Bassini: 2
- Ospedale Sesto S. Giovanni: 1
- CTO: 1

Per il servizio di presidio, ICP metterà a disposizioni i locali adeguati.

Il personale di presidio potrà operare solo nella specifica sede di riferimento, salvo autorizzazione da parte di ICP.

Il servizio di presidio sarà fornito da personale di competenza adeguata alla fornitura dei servizi di seguito elencati.

Si precisa che la lingua abituale di lavoro per questo servizio dovrà essere l'italiano.

Il servizio di reperibilità di seguito definito dovrà essere fornito, durante gli orari che eccedono l'orario di copertura del servizio definito in "Orari di copertura dei servizi" attraverso personale, locali, mezzi e strumenti totalmente a carico del Fornitore, al di fuori dei locali messi a disposizione da ICP.

Il gruppo di lavoro che opererà presso la sede centrale del servizio, il personale del servizio di presidio e del servizio di reperibilità saranno coordinati e dipenderanno da un Responsabile Operativo nominato dal Fornitore.

Il Responsabile Operativo, di competenza adeguata al ruolo di coordinatore e referente tecnico / organizzativo, opererà come interfaccia tra il Responsabile ICP ed il gruppo di lavoro.

Il Responsabile Operativo opererà presso la sede centrale del servizio in ICP, coprendo l'orario del servizio di presidio.

Il gruppo di lavoro che opera presso la sede centrale del servizio (compreso il Responsabile Operativo) sarà fornito in aggiunta al personale del servizio di presidio.

Tutto il personale del Fornitore che opererà presso ICP sarà soggetto a registrazione delle presenze.

Il Fornitore è tenuto ad intervenire presso tutte le sedi indicate da ICP.

Eventuali future variazioni (aperture o chiusure di sedi) saranno comunicate tempestivamente al Fornitore; tali variazioni non daranno luogo di per sè ad alcun incremento dei compensi dovuti, in ogni scenario in cui non avvenga una rilevante variazione dell'organizzazione complessiva di ICP (incremento di più del 20 (venti)% delle attuali sedi).

Sono da considerare obbligazioni contrattuali tassative:

- La presenza del gruppo di lavoro (compreso il Responsabile Operativo) presso la Sede centrale del servizio;
- La presenza del "Servizio di presidio" presso le sedi ICP sopra definite e la relativa numerosità minima del personale.

4.4 Orari di copertura dei servizi

Il servizio dovrà essere disponibile durante gli orari di seguito elencati (orario di lavoro sanitario):

- Dalle 7.00 alle 19.00, dal Lunedì al Venerdì
- Dalle 7 alle 13 il Sabato

Il servizio di presidio dovrà essere disponibile durante gli orari di seguito elencati:

- Dalle 8.00 alle 17.00, dal Lunedì al Venerdì

Ogni attività contrattuale ordinaria e straordinaria, ad eccezione delle attività connesse al servizio di reperibilià, dovrà essere in generale svolta all'interno degli orari indicati, a meno del verificarsi di condizioni particolari e in ogni caso a seguito di autorizzazione scritta del Responsabile ICP.

4.5 Servizio di reperibilità

Il fornitore renderà disponibile un servizio di help desk con funzione di Single Point of Contact (SPOC) H24 *7.

Durante gli orari che eccedono l'orario di copertura del servizio definito in "Orari di copertura dei servizi", lo SPOC gestirà:

- I guasti bloccanti (su tutti i sistemi oggetto del servizio) relativi ai servizi ICP aperti in orario esteso;
- I guasti bloccanti relativi agli apparati di rete.

I guasti saranno risolti direttamente da remoto o attivando il proprio personale reperibile del servizio di help desk di 2° Livello eventualmente on-site. Ove necessario il servizio attiverà il

personale reperibile di terza parte (ad esempio per la gestione server e per la connettività geografica).

ICP comunicherà al Fornitore, in fase di avvio del contratto, l'elenco dei servizi aperti in orario esteso.

4.6 Livelli di Servizio e misura della qualità del servizio

Il Fornitore si impegna a garantire i livelli di servizio contrattuali che dovranno essere corrispondenti o migliorativi rispetto ai livelli minimi di seguito specificati per ogni servizio.

Il Fornitore registrerà e documenterà nel sistema informatico di monitoraggio dell'esecuzione del contratto ciascun evento accaduto durante l'intero iter di gestione degli incidenti, dei problemi o degli interventi, al fine non solo di gestire accuratamente il servizio, ma anche di permettere a ICP di valutare la qualità del servizio prestato.

A tal fine ogni evento o richiesta (ad esempio richiesta da utente Pdl, evento di malfunzionamento di un componente di infrastruttura di rete, richiesta di installazione/configurazione di un componente hardware o software) dovrà comportare l'apertura di un ticket nel ticketing system di seguito descritto e l'esecuzione del conseguente processo di tracciatura fino alla chiusura del ticket.

Il Fornitore è tenuto ad informare il Responsabile ICP:

- Nel caso occorrano situazioni o eventi, di natura tecnica ovvero organizzativa, non gestibili in completa autonomia da parte del proprio personale, o per i quali risultino necessarie autorizzazioni da parte di ICP prima di procedere
- Quando eventi rilevanti, ben giustificati da motivi di natura tecnica o organizzativa, pregiudichino sostanzialmente il conseguimento dei Livelli di Servizio stabiliti; il responsabile tecnico di ICP provvederà a valutare le motivazioni addotte, e di volta in volta determinerà sia le azioni da prendere, che le ripercussioni in termini di reportistica ed eventuali penali.

Tutte le procedure legate ai servizi oggetto del presente appalto dovranno essere opportunamente documentate a cura del Fornitore e concordate con ICP ed eventuali terze parti qualora fossero coinvolte nel processo.

I livelli di servizio saranno oggetto di monitoraggio con rendicontazione sulla base di periodi specificati.

Relativamente al servizio di presidio, il Fornitore dovrà:

- Garantire la presenza minima richiesta di personale;

- In ogni caso soddisfare i livelli minimi di seguito specificati per ogni servizio (con il personale necessario, eventualmente eccedente la presenza minima).

Gli utenti e le apparecchiature sono classificati in fasce diverse dipendenti dalla loro criticità, con riferimento al Livello di Servizio che sarà loro associato, come segue:

- Livello 1 H24*7: priorità elevata ed appartenenza a servizi aperti in orario esteso;
- Livello 1: priorità elevata;
- Livello 2: priorità normale.

Il numero di PdL a "Livello 1 H24*7: priorità elevata ed appartenenza a servizi aperti in orario esteso" è orientativamente pari al 10 % del totale delle PdL installate.

Il numero di PdL a "Livello 1: priorità elevata" è orientativamente pari al 40 % del totale delle PdL installate.

Il numero di PdL A "Livello 2: priorità normale" è pari al rimanente 50%.

4.7 Variazioni del servizio

Tutti i servizi di seguito esplicitati dovranno essere forniti, senza oneri aggiuntivi e senza alcun vincolo, rispettando gli SLA contrattuali, relativamente a tutti gli interventi che ICP riterrà necessari ed alle configurazioni ed ai volumi che potranno risultare dalle evoluzioni che ICP deciderà, nel corso del periodo contrattuale, per il proprio Sistema Informativo (ad esempio modifiche dell'infrastruttura di rete).

Unica eccezione al criterio generale sopra esposto è la numerosità delle PdL installate. Sarà incluso nel contratto un incremento massimo delle Pdl installate (verificato a seguito del censimento in fase di avvio) pari al 20 (venti)%.

4.8 Variazioni di priorità nelle attività di fornitura dei servizi

Sulla base di specifiche esigenze, il responsabile dell'unità Sistemi Informativi di ICP potrà richiedere al Fornitore di gestire con priorità maggiore specifiche attività all'interno dell' elenco delle attività aperte (corrispondenti a ticket aperti) ed il Fornitore dovrà ottemperare alla richiesta.

4.9 Servizio di Help Desk

Il Fornitore dovrà organizzare e gestire una struttura di Call Center che riceverà le segnalazioni dagli utenti e/o dai responsabili ICP ed avrà la funzione di Helpdesk.

Tale struttura, ed i processi da essa gestiti, saranno ispirati dalle Best Practices ITIL (e alla norma ISO 20000), alle quali facciamo riferimento; sarà oggetto di valutazione la coerenza e completezza della proposta fornita, nei termini di integrazione dell'insieme dei servizi proposti in tal senso.

In sintesi, il Servizio di Assistenza richiesto dovrà erogare tramite una struttura dedicata i seguenti servizi:

- Ricezione e smistamento di tutte le problematiche di informatica;
- Gestione degli Incidenti;
- Gestione dei Problemi;
- Servizi informativi e supporto a operazioni specifiche.

Si richiede che il fornitore, per la gestione di tutti gli interventi ordinari e straordinari e per la gestione delle richieste, dei problemi e degli incidenti si doti degli adeguati strumenti al fine di registrare e monitorare nel tempo tutti gli eventi legati ad essi e di supportare efficacemente ed efficientemente la loro risoluzione. I Concorrenti dovranno fornire la descrizione dettagliata di come intendano fornire il servizio, nel rispetto dei requisiti di seguito dettagliati, includendo le caratteristiche degli strumenti di gestione e di monitoraggio del contratto.

Il Fornitore dovrà utilizzare uno strumento software di Trouble Ticketing che dovrà supportare il servizio di Help Desk qui definito ed integrarsi con lo strumento di Configuration Management Data Base (CMDB) e con le funzionalità dello strumento di controllo remoto e distribuzione software.

Gli strumenti di trouble ticketing, Configuration Management Data Base, controllo remoto e distribuzione software saranno a carico del Fornitore.

Il sistema utilizzato dovrà essere compatibile con le Best Practices ITIL.

L'assistenza tecnica dovrà essere garantita attraverso un Call Center con funzione di Single Point Of Contact (SPOC) Help Desk che sarà organizzato secondo i criteri esposti in "Modalità organizzative e luogo di fornitura dei servizi" ed opererà in accordo con le specifiche riportate nel seguito del presente documento.

Il database dei ticket ed il CMDB saranno dedicati a ICP.

Il servizio di assistenza dovrà essere realizzato da una struttura a due livelli, a seconda della tipologia, della complessità e della gravità degli inconvenienti da gestire, di seguito descritti.

Al fine di garantire un costante monitoraggio dei servizi e degli interventi effettuati dall'Help Desk, dovrà essere possibile produrre rapporti visibili in tempo reale riguardanti l'attività erogata contenenti i dati significativi ed un insieme di indicatori che evidenziano le performance di servizio.

Tali informazioni saranno anche registrate in un report periodico.

In particolare il Servizio prevederà:

- La gestione completa dei Trouble Ticket (dall'apertura alla chiusura della chiamata);
- La risoluzione delle chiamate di primo livello ed in particolare per:
  - La diagnosi e l'eventuale risoluzione delle disfunzioni relative a PdL e infrastrutture di rete.
  - Il supporto agli utenti per l'utilizzo delle applicazioni più comuni in ambito Office Automation e sistemi operativi Microsoft.
- La registrazione e lo smistamento e la gestione fino alla chiusura delle chiamate riguardanti il supporto di attività di responsabilità di terze parti quali ad esempio i sistemi server e gli applicativi software, compresa la verifica con l'utente finale dell'avvenuta risoluzione del problema a cura del fornitore terzo.
- Lo smistamento delle chiamate di secondo livello agli specialisti delle varie Classi di Servizio.

- Il coordinamento delle operazioni quando la problematica prevede più livelli d'intervento e competenze coinvolte: assegnazione di un nuovo posto di lavoro, spostamento fisico di apparecchiature come prerequisito ad installazioni SW, etc.
- La gestione degli interventi di manutenzione hardware e software a cura del Fornitore o con la collaborazione di terze parti.
- L'inventario dei dati significativi di tutte le PdL e infrastrutture di rete di ICP con inclusione di configurazione hardware e software, contratti d'acquisto, contratti di manutenzione, garanzie dei prodotti, allocazione, etc.
- L'elenco delle anagrafiche necessarie alla gestione degli asset (utenti finali, addetti al supporto)
- La gestione delle relazioni tra asset e utenti finali
- I report sulle attività di Help Desk e sulle dotazioni inventariate (asset).
- L'archiviazione della documentazione prodotta nelle varie Classi di Servizio.
- La gestione del SW di gestione del Servizio, compresa la personalizzazione delle interfacce e le procedure di backup/recovery.

Il Fornitore dovrà garantire il rispetto dei livelli di servizio indicati al paragrafo relativo.

4.9.1 Requisiti

4.9.1.1 Conduzione operativa del servizio

Il Fornitore dovrà garantire per tutto l'orario di lavoro, la presenza di un numero adeguato di risorse (operatori di Call Center) cui saranno inviate le richieste di supporto tramite telefono, e-mail, web, segreteria telefonica. Ogni richiesta di supporto darà luogo a un trouble ticket.

I trouble ticket dovranno essere generati anche automaticamente da tool di monitoraggio.

La gestione dei ticket sarà la base per l'operatività di tutti i servizi e per la misurazione degli SLA. Di conseguenza i ticket saranno accuratamente classificati per Classi di Servizio. La classificazione dei ticket sarà concordata con ICP nella fase di avvio dell'esecuzione della fornitura.

L'operatore di Call Center dovrà:

- Tracciare l'intera vita delle richieste di supporto, dall'apertura del Trouble Ticket alla chiusura dello stesso, dovrà gestirne la priorità, l'escalation e la gravità e sarà responsabile della verifica dei tempi di risoluzione dei problemi e degli SLA.
- Essere in grado di dare supporto di primo livello a tutte le richieste risolvibili telefonicamente e/o mediante opportuni tools di supporto remoto.
- Gestire i contatti con l'assistenza di II livello; sarà sua cura smistare le richieste ai responsabili delle Classi di Servizio.
- Fornire informazioni sullo stato di avanzamento del ticket qualora venga richiesto dagli utenti finali o dal Responsabile ICP.

- Chiudere il Trouble Ticket; effettuare le registrazioni relative all' intervento per la verifica degli SLA ed avere cura dell'archivio dei rapporti d'intervento.

All'interno del Gruppo di Gestione sarà individuato un responsabile per ciascuna Classe di Servizio.

Lo smistamento delle chiamate al secondo livello dovrà essere effettuato dall'operatore tenendo conto delle aree specialistiche definite dalle Classi di Servizio: l'operatore trasferirà le richieste non risolte al Responsabile incaricato della Classe di Servizio relativa, il quale prenderà in carico la richiesta, eventualmente coinvolgendo altri specialisti. L'incaricato della Classe di Servizio autonomamente dovrà chiudere la richiesta, una volta terminata l'attività di supporto, indicando all'operatore eventuali cambiamenti alle configurazioni degli asset.

Il Fornitore dovrà quindi:

- Istituire un unico punto di raccolta per tutte le possibili problematiche dell'utente (numero telefonico unico);
- Predisporre un adeguato numero di operatori adibiti alla ricezione dei contatti e tarare dinamicamente il volume del servizio erogato sulla base delle reali necessità legate al momento, e comunque sempre nel pieno rispetto dei livelli di servizio richiesti;
- Disporre di un sistema informativo affidabile relativo all'insieme complessivo delle richieste e segnalazioni pervenute, al loro ciclo di vita ed ai livelli di servizio erogati;

4.9.1.2 Struttura a due livelli dell'help desk e relazione tra i livelli

L'Help desk sarà organizzato in due livelli.

Il primo livello sarà unico e riceverà tutte le chiamate degli utenti ICP relative a incidenti o richieste di assistenza per apparecchiature informatiche (PdL, infrastruttura di rete e sistemi server) e applicazioni software.

Il primo livello opererà per risolvere la chiamata limitando al meglio possibile l'escalation al secondo livello. Ove necessario il primo livello individuerà il tipo di help desk di secondo livello da coinvolgere e passerà la chiamata (il ticket aperto) al secondo livello.

Il secondo livello sarà costituito da diversi help desk:

- Help desk di 2° livello per le apparecchiature informatiche, gestito direttamente dal Fornitore che sarà responsabile di tutti gli aspetti di seguito definiti nel presente documento;
- Help desk di 2° livello gestiti da terze parti per:
  - Sistemi server;
  - Applicazioni software.

Tutti gli eventi di servizio (sia originati da un utente ICP che da qualsivoglia incidente o richiesta di servizio) causeranno l'apertura di un ticket nel ticketing system ed il loro ciclo di vita sarà tracciato.

Il Fornitore si assumerà l'onere non solo di fornire e mettere in servizio il ticketing system per il proprio servizio di help desk di primo e secondo livello, ma anche di fornire e mettere in servizio le adeguate interfacce con gli help desk di secondo livello gestiti da terze parti.

Le interfacce dovranno essere definite in modo che, per ogni ticket (sia gestito totalmente dal Fornitore che in collaborazione con terze parti) sia possibile tracciare tutti gli eventi significativi, dall'apertura del ticket alla sua chiusura.

4.9.1.3 Help desk 1° livello

Il servizio di Helpdesk di 1° livello, utilizzando la struttura di call center interno garantirà il servizio di assistenza con risposta diretta di un operatore durante l'orario di servizio.

Il servizio di Help Desk di 1° livello sarà disponibile per tutti gli utenti di ICP, e dovrà essere dimensionato conseguentemente.

Il servizio dovrà assistere gli utenti per risolvere incidenti nell'utilizzo delle PdL e/o richieste e/o domande su sistemi operativi, software di ambiente, software di connettività, browser ed applicativi di produttività individuale installati nelle PdL, garantendo la seguente operatività:

- Accogliere e registrare le richieste di assistenza, registrando i dati principali della chiamata e classificando la problematica;
- Qualificare l'incidente facendone una prima diagnosi, deducendo la priorità di servizio sulla base delle caratteristiche dell'utente e della gravità dell'incidente e individuando le successive azioni sulla base delle procedure stabilite;
- Tenere traccia (tracking) delle chiamate e degli incidenti in tutte le fasi: apertura, qualifica ed assegnazione di priorità, risoluzione, escalation e chiusura;
- Risolvere definitivamente (o cercare di aggirare temporaneamente) gli incidenti di non elevata complessità;
- Effettuare l'escalation delle chiamate di competenza non risolte alle organizzazioni competenti del proprio HelpDesk di 2° Livello (più avanti definito);
- Indirizzare, come Help Desk unico, le chiamate non di competenza (Sistemi server, SW applicativo, attrezzature di fonia, ecc.) alle organizzazioni responsabili indicate da ICP;
- Gestire le chiamate dall'apertura fino alla chiusura, attuando un monitoring per garantire il raggiungimento della soluzione, inclusi eventuali solleciti, gestendo e coordinando gli interventi presso gli utenti;
- Aggiornare gli Utenti circa lo stato di ciascuna chiamata e attività fino alla sua soluzione e chiusura del Ticket, anche in caso di ricorso al secondo livello.

L'Help Desk di 1° Livello, per il suo ruolo e collocazione nei flussi informativi, è inoltre responsabile di:

- Evidenziare gli incidenti ricorrenti agli specialisti interni/esterni al servizio in modo da attuare soluzioni preventive;

- Popolare ed alimentare una Knowledge Database al fine di documentare e migliorare le conoscenze e capacità di risoluzione degli operatori dedicati al servizio;
- Verificare a campione la soddisfazione degli utenti con produzione di rapporti periodici;
- Produrre periodicamente delle statistiche sullo svolgimento del servizio e generare i report standard periodici concordati con ICP relativi sia ai volumi contrattuali che ai Livelli di Servizio (SLA) raggiunti con statistiche raggruppate ad es. per tipo di richiesta, tempi di risoluzione, reparto, etc..;
- Elaborare le informazioni provenienti dalle statistiche degli incidenti e del servizio, fornendo indicazioni e suggerimenti per ovviare a problemi e criticità, evidenziate da correlazioni tra numerosità/tipologia delle chiamate e tipologia degli utenti, argomenti/problemi affrontati, fasce orarie, tempi di servizio ecc.

Oltre al supporto all'utente il servizio di Help Desk di 1° Livello rappresenta un momento organizzativo di coordinamento fra le attività che gli sono proprie (supporto all'utente da postazione remota) e quelle assicurate da altri servizi presso l'utente (ad esempio manutenzione hardware) o da altri servizi di natura specialistica (Help desk di 2° Livello).

L'elenco di interventi attivabili direttamente dal servizio di Helpdesk di 1° livello è sottoposto ad approvazione da parte di ICP, che si riserva di decidere quali interventi possano essere richiesti senza autorizzazione e quali necessitino di una richiesta esplicita da parte dell'Help desk ai responsabili di ICP.

Il Fornitore potrà utilizzare strumenti di controllo remoto, in questo o nei successivi passi del flusso di supporto, al fine di guidare l'utente nella verifica e nella soluzione di problemi segnalati. L'attivazione di tali strumenti sarà possibile solo con l'esplicita autorizzazione dell'utente.

4.9.1.4 Help desk 2° livello

L'Help Desk dovrà essere completato con una funzione di Help Desk di 2° livello. Le attività a carico dell'Help desk di 2° livello sono in particolare:

- Valutazione di dettaglio
- Individuazione, assegnazione ed attivazione delle risorse tecniche idonee disponibili;
- Gestione e controllo di interventi On Site;
- Coordinamento e integrazione dei diversi attori per completare il ciclo di risoluzione;
- Consulenza all'Help Desk di primo livello riguardo ad incidenti di particolare gravità, e fornitura di soluzioni e workaround di problemi
- Gestione dei contatti operativi con eventuali altre terze parti per la gestione di problematiche ben definite (server, applicazioni, etc.);
- Analisi delle statistiche sugli interventi al fine di identificare i fabbisogni e definire azioni di prevenzione dei problemi.

4.9.1.5 Servizi informativi e supporto ad operazioni specifiche

Il sistema di Help Desk dovrà essere predisposto per fornire informazioni agli utenti in merito agli aspetti più rilevanti del servizi quali ad esempio:

- Funzionamento di beni e servizi informatici;
- Problematiche comuni;
- Come svolgere specifiche operazioni.

Tale servizio sarà erogato sia tramite il personale operativo, sia attraverso la costituzione di un portale Web in cui raccogliere le principali informazioni ad esempio sotto forma di Frequently Asked Question (FAQ) o di raccolta di documentazione o manualistica.

4.9.1.6 Software di gestione

Il Fornitore dovrà proporre il SW di gestione dell'Help Desk ed il CMDB, provvedendo a suo carico alla fornitura sia del SW che dell' HW necessario. Il SW selezionato dovrà garantire tutte le funzionalità necessarie alla conduzione operativa del Servizio, tra cui:

1. Consentire la gestione degli inventari di tutto l'HW ed il SW di ICP ed in particolare:
    - Per tutte le famiglie di prodotti almeno le seguenti informazioni:
        1. Nome (se applicabile)
        2. Codice Inventario ICP
        3. Famiglia (PC, Stampante, Server, etc.)
        4. Classe (Stampante locale, dipartimentale, etc.)
        5. Marca / Modello / Numero Seriale / Fornitore
        6. Date di installazione / accettazione / inizio garanzia / fine garanzia / dismissione
        7. Tipo acquisizione (locazione, acquisto, ecc)
        8. Stato (Attivo, scorta, riparazione,etc.)
        9. Tipo di manutenzione (On-site, scambio parti, SLA, ecc.)
        10. Manutentore
        11. Ordine di manutenzione
        12. Gruppo di gestione
        13. Dislocazione
        14. Centro di costo
        15. Referente Primario (utente o sistemista)
        16. Relazione con altri asset connessi (monitor, basi per portatili e device varie);
    - Per la famiglia di prodotti "Personal Computer" e "Server" informazioni come: CPU (Numero processori, modello, frequenza) / Memoria fisica / Spazio totale disco / Composizione dei dischi / Tipo di Unità ottica (CD-ROM/CD-RW) / Scheda video / Scheda di rete / Sistema Operativo / Unità di backup;

- Per la famiglia di prodotti “Apparati di rete” informazioni come: CPU (Numero processori, modello, frequenza) / O.S. / Firmware / RAM (MB) / Flash memory / Interfacce/tipo (q.tà/protocollo/connettore) / Troughput (bits/sec. E/o packets/sec.)
- Per la famiglia di prodotti “Software” informazioni come: Tipo licenza / Totale licenze / Totale installazioni / Media Type / Memoria richiesta / Prerequisiti di O.S. / Piattaforma / Versione/Release / Upgrade info.

2. Consentire la gestione delle liste degli utenti, dei fornitori, dei manutentori e la relazione tra questi e gli asset inventariati;
3. Consentire la tracciabilità dell’intero ciclo di vita dei trouble tickets. Per questi dovrà essere possibile gestire almeno le seguenti informazioni:
   - Codice chiamata / Descrizione / Codice inventario ICP (asset coinvolto) / Sistemista / Criticità-Gravità / Priorità;
   - Data e ora di eventuale inoltro della segnalazione del problema ai preposti alla risoluzione (o manutentore esterno);
   - Status (aperta, chiusa, sospesa, annullata, in attesa (autorizz., fornitura, ecc.).ecc.);
   - Tipo di richiesta (o famiglia, per individuare e schematizzare il tipo di attività).
   - Date significative (apertura, chiusura, cambi di status);
   - Utente finale;
   - Solleciti;
   - Note

   e la possibilità di trasferire la richiesta di supporto da un sistemista ad un altro senza che venga modificato il codice del trouble ticket.
4. Consentire il reporting sintetico ed analitico, sia periodico sia on-line su necessità, delle informazioni gestite (inventari; trouble tickets classificati anche per Classi di Servizio, stato e fuori SLA; ordini di servizio).
5. Consentire l’accesso all’applicazione via Web in modo che sia utilizzabile, da tutte le sedi ICP, dai sistemisti e dai Referenti del Servizio di ICP ed eventualmente dai fornitori esterni. Tramite l’applicazione ciascun addetto ai lavori dovrà poter:
   - Modificare lo stato delle richieste di propria competenza;
   - Trasferire la richiesta ad altro Addetto;
   - Inserire eventuali commenti.
6. Consentire l’accesso via Web agli utenti in modo che possano aprire e tracciare le proprie richieste di supporto, prevedendo diritti di accesso differenziati tra Addetti ai lavori ed Utenti finali.
7. Prevedere le procedure di ripristino (backup/restore) del DataBase dell’applicazione per eventuale recovery della stessa.

4.9.1.7 Sistema di misurazione SLA

Il Fornitore dovrà provvedere a raccogliere le misure caratteristiche del servizio tramite il sistema di Trouble Ticketing integrato con l'infrastruttura tecnologica di Call Center.

Le misure relative all'andamento del servizio dovranno essere archiviate e conservate a cura del Fornitore, che dovrà utilizzare a tal fine un adeguato sistema di gestione automatizzato dei problemi e della reportistica.

Il sistema dovrà anche permettere l'estrapolazione dei report relativi agli SLA associati ai servizi previsti dal presente Contratto.

Per ogni servizio erogato il Fornitore si impegna a rilevare e ad elaborare i dati elementari e le statistiche indicativi dell'andamento del servizio ed a trasmettere ad ICP i rapporti necessari alla sua valutazione in termini di rispetto dei livelli di servizio, per quantificare l'accettabilità contrattuale dei servizi e l'occorrenza o meno di condizioni di penale.

I rapporti e le misure/indicatori statistici in essi contenuti dovranno consentire di meglio conoscere le performance e quindi studiare ed attuare percorsi di miglioramento continuo, nonché di poter procedere ad una valutazione tecnico/economica dei servizi stessi.

4.9.1.8 Standard e norme di riferimento

Nell'implementazione del Service Desk si dovrà fare riferimento alle norme europee e nazionali indirizzate ai servizi di outsourcing: in particolare quelle relative alla privacy (ex legge 675/1996, ora 196/2003), alla sicurezza (legge 626) e all'ergonomia (direttiva CEE 90/270 recepita dalla legislazione italiana con la legge 142) del posto di lavoro.

Il processo proposto per la gestione del servizio dovrà essere compatibile con le Best Practices ITIL.

4.9.1.9 Supporto alla gestione dei ticket originati dalla gestione dei sistemi server

Il fornitore dovrà rendere disponibile a ICP e/o Fornitori nominati da ICP il sistema di gestione dei ticket, in modo che ICP e/o Fornitori nominati da ICP possano gestire i ticket originati dalla gestione dei sistemi server.

4.10 Servizio di Gestione delle Postazioni di Lavoro (PdL)

Nei seguenti punti sono descritte in dettaglio le operazioni che si richiedono per ciascuna fase del ciclo di vita della PdL.

Nella categoria "Postazioni di Lavoro" rientrano tutti i PC desktop e portatili e gli apparati connessi. Esempi di apparati sono le periferiche di stampa (individuali, di gruppo e dipartimentali) e le apparecchiature scanner di ICP che sono utilizzate per la fruizione delle applicazioni Office, dei servizi applicativi centralizzati e dei sistemi informativi locali .

In particolare il Servizio prevederà:

- La salvaguardia dei dati degli utenti (backup e restore in caso di sostituzione HW, installazione e gestione prodotti antivirus e di supporto alla gestione centralizzata);

- La gestione delle configurazioni delle apparecchiature degli utenti con particolare attenzione alle performance ed ai tempi di ripristino;
- L'installazione di hardware e software, gestione delle modifiche e degli aggiornamenti;
- La gestione delle risorse critiche, predisposizione rapporti periodici di consuntivazione dei problemi;
- L'analisi della qualità del servizio.

Il servizio di gestione delle postazioni di lavoro dovrà comprendere l'esecuzione di tutte le fasi connesse al ciclo di vita delle postazioni. In particolare al Fornitore sono richiesti i seguenti servizi:

1. Presa in carico e risoluzione dei malfunzionamenti HW e SW direttamente o con eventuale attivazione e controllo delle società con le quali è attivo un servizio di manutenzione;
2. Conduzione operativa e monitoraggio (Installazione, Movimentazione, Aggiunte, Cambiamenti). Configurazione ed Amministrazione delle PDL, stampanti e scanner. Monitoring e fault management delle apparecchiature hardware. Change Management. Software distribution. User/resource management).

Tutte le attività elencate prevedono l'aggiornamento delle configurazioni e dei dati inventariali nel data-base degli asset (parte del CMDB).

Il Fornitore dovrà garantire il rispetto dei livelli di servizio indicati al paragrafo relativo.

4.10.1 Requisiti

4.10.1.1 Censimento iniziale

Il Fornitore dovrà rilevare, mediante opportuna attività di censimento iniziale, tutto il parco PdL e apparecchiature connesse di ogni genere e tipo (ad esempio stampanti e scanner) a disposizione di ICP, alimentando il CMDB.

4.10.1.2 IMAC

Il servizio in questione comprende tutte le attività inerenti Installazioni, Movimentazioni, Aggiunte, Cambiamenti (IMAC), con riferimento a qualsiasi apparecchiatura rientrante nell'ambito contrattuale definito, che si rendessero necessari a seguito di qualsiasi evento che interessi l'utente, le condizioni di impiego delle apparecchiature, la loro sicurezza informatica e/o la loro configurazione hardware o software.

Per le aggiunte ed i cambiamenti, il Fornitore dovrà quindi assicurare i processi necessari per gestire ed attuare aggiunte, rimpiazzi e disinstallazioni:

- Di componenti hardware e relative modifiche software da essi indotte;
- Di moduli software per l'attivazione o aggiornamento di pacchetti non normalmente distribuiti via rete.

Il servizio è erogato a seguito di:

- Richieste singole dell'utente ("richiesta a Service Desk");
- Richieste di responsabili di ICP, sulla base di un piano da concordare preventivamente.

Tali richieste porteranno sempre all'apertura di un Ticket di intervento di tipo IMAC che dovrà essere inserito nel sistema di registrazione dei Ticket che il Fornitore dovrà gestire.

Il Fornitore sarà responsabile dell'esecuzione delle seguenti attività, nel rispetto delle condizioni di generale garanzia di sicurezza e riservatezza:

- Pianificazione dell'intervento;
- Interazione con il servizio di manutenzione hardware;
- Distribuzione ed aggiornamento software: nuovi pacchetti, versioni, patch;
- Installazione e configurazione di PdL, dispositivi aggiuntivi e relativo software;
- Esecuzione delle modifiche;
- Riconfigurazione delle PdL/Periferiche, se necessario;
- Collaudo presso l'utente e rilascio in esercizio dell'apparecchiatura modificata, assicurando, nel caso di sostituzione, la migrazione di dati e programmi di uso locale dell'utente.
- A chiusura dell'intervento (approvvigionamento/ installazione/ disinstallazione/ sostituzione / dismissione), aggiornamento delle necessarie posizioni di inventario, registrando l'intervento e il suo esito sul CMDB.

La conclusione di qualsiasi intervento IMAC si avrà, quando l'utente finale potrà riprendere il proprio lavoro senza problemi e senza perdita di alcuna informazione o programma. Ove ciò fosse impossibile a causa di reali impedimenti di ordine tecnico/pratico il Fornitore agirà per limitare al massimo grado perdite e disallineamenti, e riporterà sul CMDB – e secondo necessità ai responsabili di ICP - le ragioni relative.

La migrazione dei dati e di eventuali programmi applicativi oltre quelli di produttività individuale da un ambiente ad un altro (macchine diverse in caso di sostituzione, stessa macchina, in caso di modifica, ecc.) è parte integrante dei processi di servizio attivati nell'intervento stesso e la loro corretta esecuzione deve essere verificata nel collaudo di accettazione.

Nei casi in cui le operazioni IMAC comportassero:

- Dismissione della PdL;
- Reinstallazione completa del sistema operativo e SW applicativo di pertinenza del profilo utente;
- Ed in tutti quei casi in cui le operazioni sulla PdL potrebbero comportare rischio di perdita dei dati,

il Fornitore dovrà fornire un opportuno servizio di backup dei dati residenti sulla Pdl e sulla home directory dello stesso utente garantendone la conservazione fino ad un massimo di 30 giorni solari su appositi supporti di memorizzazione o backup server.

Sarà cura del Fornitore installare software applicativi forniti da terze parti ad ICP. Il fornitore sarà tenuto anche ad effettuare i relativi aggiornamenti e le istallazioni di eventuali patch correttive o migliorative del software in questione in base a quanto indicato dal fornitore del software e da ICP. Il fornitore opererà sulla base di definite e documentate procedure rilasciate dal fornitore del software e da ICP.

Le operazioni di aggiunta, cambiamento, modifica e Installazione di software, dovranno essere di norma effettuabili tramite lo strumento di Software Distribution.

Operazioni con elevati volumi non attuabili remotamente mediante strumenti di distribuzione SW automatica, dovranno essere concordate nei modi e nei tempi con ICP, tramite presentazione di un opportuno piano di progetto e con una idonea valutazione dell'impatto sull'organizzazione di ICP.

4.10.1.3 Approvvigionamento

Nel caso di sostituzione integrale di apparati (ad esempio PC, stampanti o scanner) dichiarati non riparabili o nel caso di aggiunta / sostituzione su richiesta ICP, l'approvvigionamento delle apparecchiature sarà a carico di ICP che le renderà disponibili in generale presso il magazzino economale principale, attualmente collocato c/o il Presidio Ospedaliero "Vittore Buzzi" di via Castelvetro a Milano.

Per quanto riguarda l'approvvigionamento di parti di ricambio ci si riferisca a quanto specificato al capitolo "Servizio di manutenzione hardware".

La numerosità delle apparecchiature richiede un'attività di tracciamento e di monitoraggio molto dettagliata; ICP comunicherà al fornitore le regole utilizzate al proprio interno per la numerazione degli assets (cespiti), il tipo di etichettatura da utilizzare e tutti i dettagli di identificazione degli apparati da consegnare agli utenti finali.

Come parte del servizio di approvvigionamento il Fornitore registra nell'inventario del CMDB tutti i dati di gestione, incluso il carico/scarico del bene dal magazzino.

Il fornitore, ove il componente da installare sia disponibile presso una qualunque sede ICP, provvederà al trasporto presso la sede di installazione.

4.10.1.4 Installazione

L'installazione comprende almeno le seguenti fasi a titolo esemplificativo ma non esaustivo:

- Ricezione configurazione (consegna presso l'utente, disimballaggio e rimozione cartoni, controllo formale dei colli secondo la normativa di ICP e registrazione degli stessi nel database di gestione, smaltimento imballaggi);
- Posizionamento e collegamento (collocazione nelle posizioni previste dall'arredamento d'ufficio - secondo la normativa ICP, collegamento dei singoli componenti con le prese elettriche e di rete, eventuale attivazione della presa di rete presente ma priva di patch lato armadio verso l'apparato attivo);
- Installazione vera e propria (installazione hardware, configurazione in rete locale utilizzando indirizzi IP e indirizzi di posta elettronica indicati da ICP, installazione dei moduli SW della configurazione utente non ancora preinstallati);

- Personalizzazione (configurazione e personalizzazione dei moduli SW della configurazione utente, ripristino tramite passaggio sulle nuove apparecchiature di eventuale software o di archivi specificati dall'utente qualora si trattasse di sostituzione di Personal Computer preesistente o di disco rigido);
- Test delle macchine;
- Formazione - istruzione del personale circa le principali nozioni di utilizzo;
- Consegna (della PdL e della relativa documentazione dei prodotti – eventualmente con indicazione dei siti Intranet e/o on-line dove reperirla, rilascio all'utente o a chi indicato da ICP di apposita documentazione di test delle apparecchiature installate, tramite benestare dell'avvenuta funzionalità firmata dall'utente);
- Accettazione: la consegna del Posto di Lavoro correttamente funzionante sarà comprovata dalla firma dell'utente su un Verbale di Consegna, che includerà l'elenco delle componenti hardware e delle applicazioni software installate. Il verbale documenterà inoltre la chiusura della richiesta d'installazione del Posto di Lavoro;
- Ritiro contestuale (entro la medesima giornata) delle eventuali apparecchiature precedenti e preesistenti;
- Registrazione su apposito applicativo dell'operazione conclusa entro la medesima giornata.

L'attività di installazione, principalmente nel caso di nuova installazione, dovrà essere preceduta da quella di "site preparation", a carico di ICP, che comprende varie azioni tra cui, per esempio, la corretta predisposizione dell'impianto elettrico.

Se l'installazione avviene in sostituzione di un sistema preesistente, dovrà essere preceduta dalla disinstallazione dello stesso.

4.10.1.5 Disinstallazione

Le attività di disinstallazione potranno essere effettuate, sia contestualmente alle attività di installazione, che separatamente. Normalmente sono incluse le attività di:

- Disattivazione delle funzionalità HW e SW del sistema da disinstallare;
- Eventuale disconnessione dalla rete, anche lato armadio;
- Disassemblaggio delle apparecchiature;
- "bonifica del sito": raccolta ordinata dei cavi delle apparecchiature disinstallate e posizionamento degli stessi all'interno dell'unità da trasferire a magazzino;
- Predisposizione al trasporto ed esecuzione del trasporto.

4.10.1.6 Sostituzione

L'esecuzione di programmi di sostituzione degli apparati installati sarà pianificata con ICP nei tempi e nelle quantità, coinvolgendo le strutture della stessa unicamente per quanto necessario al governo delle finalità e al controllo dei risultati.

La consegna dei prodotti dovrà avvenire secondo le quantità e le tipologie stabilite di volta in volta da ICP mediante piani di consegna articolati per strutture, uffici, piano e stanza di ogni sede di ICP.

Il Fornitore agisce in qualità di project manager per l'esecuzione delle attività previste nella pianificazione, avvalendosi, per eventuali attività in carico a ICP, della collaborazione del responsabile di ICP e, per suo tramite, delle strutture competenti, eventualmente da attivare.

Il Fornitore quindi sarà l'unico responsabile nei confronti di ICP per l'esecuzione nei tempi programmati di tutte le attività necessarie a consegnare le apparecchiature agli utenti finali.

Nei casi di sostituzione della PdL dovrà comunque essere garantito:

- Il ripristino della configurazione base della stessa (reinstallazione di sw di base, di sw di produttività personale e della posta elettronica);
- Il ripristino dei dati e dei documenti elettronici presenti nella PdL da sostituire nonché la reinstallazione degli applicativi associati a quel profilo utente.

4.10.1.7 Dismissione

Il Fornitore s'impegna a ritirare ed a smaltire a suo carico e sulla base delle leggi vigenti, i personal computer, le periferiche, gli accessori, e i terminali, man mano che vengono dismessi.

La sede prescelta dal Fornitore per lo stoccaggio delle apparecchiature dovrà essere al di fuori delle sedi di ICP.

Le modalità operative per la dismissione delle PdL o di altra attrezzatura dovranno essere concordate con il responsabile di ICP. Inoltre le attività di recupero e dismissione dovranno riguardare:

- Il trasferimento di dati e programmi dalla vecchia alla nuova PdL;
- La rimozione del contenuto dalle unità di memoria di massa;
- Lo smaltimento del materiale conformemente alle norme delle leggi vigenti e rilascio a ICP di idonea documentazione.

ICP potrà suggerire al Fornitore la devoluzione gratuita delle PdL dismesse ad associazioni ONLUS. Il Fornitore stesso dovrà farsi carico anche del trasporto e della consegna delle PdL dismesse presso le ONLUS designate da ICP, nei casi in cui le ONLUS scelte siano localizzate sul territorio di ICP o nelle immediate adiacenze.

ICP potrà chiedere al Fornitore di recuperare dalle PdL dismesse alcuni componenti (es: alimentatori, RAM, Hard Disk, Lettori CD) ancora funzionanti da utilizzare come componenti di ricambio per gestire guasti su apparecchiature fuori garanzia del produttore.

4.10.1.8 Servizi IMAC associati a cambi di sede e traslochi

Nei casi di cambio di sede o trasloco di intere unità, la richiesta per servizi di tipo IMAC verrà normalmente avanzata dai responsabili ICP nei confronti del Fornitore, con il quale sarà concordato un piano di trasloco opportuno.

Il Fornitore dovrà fornire il proprio contributo, anche in fase di pianificazione, per l'esecuzione delle operazioni richieste cercando di garantire la massima soddisfazione degli utenti finali e minimizzando i tempi di inattività di questi ultimi.

Il Fornitore dovrà attivare il processo di servizio per la movimentazione di apparecchiature fra uffici nella stessa sede o in sedi diverse, sempre su richiesta del Referente informatico di ICP.

In caso di trasloco il Fornitore assicura:

- Pianificazione delle attività, concordandole con il Referente designato da ICP;
- Disinstallazione delle apparecchiature da movimentare;
- Messa in sicurezza delle connessioni e configurazione delle reti e degli apparati di comunicazione connessi;
- Imballaggio per il trasporto;
- Disimballaggio dopo il trasporto;
- Reinstallazione delle apparecchiature movimentate e riconfigurazione reti ed apparati di rete;
- Riconfigurazione PdL/ Periferiche;
- Collaudo presso l'utente e rilascio in esercizio dell'apparecchiatura movimentata;
- Aggiornamento base dati contenente le informazioni di configurazione e di dislocazione fisica e dell'utente.

Il trasporto dei colli imballati è a carico di ICP.

4.10.1.9 Documentazione ciclo di vita delle PdL

Al fine di mantenere un costante controllo sulla funzionalità dei beni installati, ICP richiede che il Fornitore documenti tutte le operazioni riguardanti il ciclo di vita di ciascuna PdL (identificazione PdL, identificazione utente, identificazione temporale e descrizione degli eventi del ciclo di vita) nel database contenuto nel CMDB.

4.11 Servizio di Gestione della rete Aziendale

La rete ICP è costituita da un'infrastruttura di comunicazione presente nelle sedi.

L'infrastruttura delle sedi è interconnessa da un sistema di comunicazione gestito da un fornitore terzo di connettività (con inclusione dei router che interfacciano le sedi).

Il Servizio di Gestione di seguito specificato riguarderà:

- L'infrastruttura presente nelle sedi;

- L’attivazione del fornitore terzo di connettività in caso di malfunzionamenti e la collaborazione con il fornitore terzo al fine di risolvere i malfunzionamenti o in ogni caso far fronte ad esigenze ICP relative all’ infrastruttura di comunicazione.

Il Servizio di Gestione di seguito specificato non riguarderà l’infrastruttura di rete della sala server (firewall e apparati di rete della sala server).

Il servizio di gestione e manutenzione delle reti costituisce l’insieme delle attività effettuate al fine di garantire costantemente la corretta funzionalità dei servizi di connettività e trasporto dati delle reti di comunicazione, nonché la misura ed il rispetto degli SLA contrattuali.

In particolare esso:

- Consente la gestione operativa di tutti gli elementi che costituiscono l’infrastruttura di rete dell’ICP (reti locali, apparati attivi, VPN IP, ecc.);
- Coordina ed assicura gli interventi volti al ripristino delle funzionalità del servizio di rete e/o apparati TLC dati;
- Provvede agli interventi di riparazione di sistemi/componenti difettosi o, nel caso, ad interagire con la società che eroga il servizio di garanzia / manutenzione;
- Prevede la disponibilità on-line di mappe di rete aggiornate in grado di rendere visibile in ogni istante la situazione infrastrutturale delle sedi;
- Effettua il monitoraggio costante dei parametri significativi della qualità della rete e delle prestazioni;
- Prevede un sistema di trouble ticketing automatico per la gestione dei guasti;
- Assicura l’effettuazione degli interventi di manutenzione preventiva per garantire il buon funzionamento dei sistemi di trasmissione dati;
- Fornisce un sistema di rendicontazione dei livelli di servizio;
- Prevede opportuni sistemi di back-up dei dati delle configurazioni dei sistemi TLC e di rete dati.

Il Fornitore, con mezzi, strumenti e risorse umane, garantirà l’esercizio operativo della rete ed il reporting sulle qualità del servizio e sulle prestazioni.

L’architettura tecnica ed applicativa dell’infrastruttura ICT di ICP è descritta in Allegato C. I contenuti dell’Allegato C sono da considerare, dal punto di vista contrattuale, indicativi della complessità dell’infrastruttura ma non esaustivi.

Il servizio dovrà essere fornito, senza oneri aggiuntivi e senza alcun vincolo, rispettando gli SLA contrattuali, relativamente alle configurazioni ed ai volumi che potranno risultare dalle evoluzioni che ICP deciderà, nel corso del periodo contrattuale, per il proprio Sistema Informativo (ad esempio modifiche ed incremento dell’infrastruttura di rete).

Il Fornitore dovrà garantire il rispetto dei livelli di servizio indicati al paragrafo relativo.

4.11.1 Requisiti

4.11.1.1 Censimento iniziale

Il Fornitore dovrà rilevare, mediante opportuna attività di censimento iniziale, la configurazione della rete e degli apparati connessi a disposizione di ICP, alimentando il CMDB.

4.11.1.2 Gestione operativa del servizio

Il sistema di gestione predisposto e impiegato dal Fornitore dovrà essere basato su architetture e tecnologie standard di tipo SNMP.

Il servizio di gestione delle infrastrutture e servizi TLC dovrà comprendere l'esecuzione di tutte le fasi connesse al ciclo di vita del servizio, ed in particolare al Fornitore sono richiesti le seguenti attività:

- Gestione operativa dei malfunzionamenti HW e SW;
- Conduzione operativa;
- Configurazione ed amministrazione degli apparati di rete;
- Monitoraggio;
- Gestione delle configurazioni degli apparati attivi;
- Effettuazione di misure prestazionali e statistiche relative all'utilizzo della rete.

4.11.1.3 Monitoraggio automatico dell'infrastruttura di rete

Il fornitore dovrà mettere in atto un sistema di monitoraggio anche automatico degli apparati di rete installati presso ICP.

Il monitoraggio dovrà operare da remoto ed essere in grado di chiamare un servizio di reperibilità su urgenza del Fornitore con una disponibilità h24*7.

Il monitoraggio, a fronte di situazioni critiche dovrà essere in grado di avvisare (via sms, chiamata telefonica su cellulare e mail) il responsabile del Sistema Informativo ICP.

Il monitoraggio terrà sotto controllo i principali parametri operativi degli apparati.

Il monitoraggio innescherà l'emissione e la gestione di allarmi:

- Derivanti dalla rilevazione di anomalie;
- Derivanti dal superamento di soglie di indicatori rappresentativi del servizio (monitoraggio delle prestazioni).

4.11.1.4 Network management

Le attività di configurazione e gestione della soluzione di rete sono condotte secondo requisiti di efficienza e sicurezza volti ad assicurare:

- La gestione della consistenza della rete ed il salvataggio delle configurazioni degli apparati attivi;
- Il supporto "on line" ad ICP;
- L'attivazione della procedura di gestione malfunzionamenti ogni qualvolta non sia possibile raggiungere la terminazione di rete nella sede di ICP a livello fisico, di protocollo o di routing;
- La predisposizione e configurazione dei sistemi di gestione e degli apparati, nella sede di ICP, prevedendo criteri di autenticazione di base (per es. protezione da accessi LAN indesiderati attraverso password riservate);

Nell'ambito delle funzioni svolte, assume particolare rilevanza l'attività di Gestione della Configurazione, intesa come predisposizione della configurazione iniziale e adeguamento successivo della soluzione di rete adottata.

Alcuni esempi di eventi e relativi aggiornamenti dei dati di configurazione possono essere i seguenti:

- Qualsiasi modifica, sia su richiesta del Cliente sia su proposta del Fornitore per ottimizzare il sistema, di configurazione sugli apparati dati: indirizzi IP, VLAN, ACL, abilitazioni, funzioni, tabelle di routing, parametri di accesso, security, ecc. che non richiedono modifiche od aggiunte di hardware;
- Modifiche legate alla necessità di modificare/rivedere in parte o per intero il piano di indirizzamento IP, in toto oppure in parte. Queste attività possono essere svolte tramite il Management di rete o presso gli apparati stessi;
- Abilitazione del traffico SNMP per l'invio delle TRAP anche su un sistema del Cliente oltre che su quello del fornitore stesso;
- Configurazione route statiche per la visibilità di server o router di proprietà del cliente;
- Inserimento di access-list per limitazioni di traffico;
- Configurazione degli apparati di sede per variazione/inserimento parametri;
- Predisposizione di test notturni di varia natura (carico della CPU, traffico delle interfacce, ecc.);
- Verifica dell'effettiva attività sulle singole prese, in modo da bonificare quelle non utilizzate.

4.11.1.5 Gestione dei problemi, assistenza tecnica e manutenzione correttiva

L'obiettivo delle attività di Assistenza tecnica e manutenzione correttiva è di assicurare la corretta funzionalità dei servizi di trasmissione dati sulla rete LAN, garantendone il miglior funzionamento continuativo e riducendo i tempi di fermo delle apparecchiature e dei sistemi, a fronte di guasti o malfunzionamenti.

Le attività comprendono gli interventi su tutti i componenti hardware e software degli apparati LAN e relativi accessori che per qualsivoglia ragione si dovessero guastare o presentare anomalie di funzionamento.

A seguito dell'escalation di un ticket di Help Desk al gruppo di supporto specialistico della rete o di un allarme generato da un sistema di diagnosi, viene prodotto e gestito un ticket di supporto.

Verificato a seguito di opportuna diagnosi che il ticket sia di competenza del gruppo di supporto rete, il gruppo contatta ICP per fornire le prime indicazioni circa la natura dei disservizi e le previsioni temporali per il ritorno alla normalità, e procede con le attività che portano al ripristino del servizio.

Più in dettaglio le attività possono riassumersi in:

- Risoluzione del problema tramite indicazione telefonica all'Utente o intervento in telediagnosi;
- Risoluzione della causa del guasto tramite:
  - Intervento presso la sede dell'apparato per il quale è stato richiesto l'intervento;
  - Sostituzione di parti sulla base dello scambio e/o tarature elettroniche, meccaniche o software finalizzate al recupero delle prestazioni iniziali dell'apparecchiatura.
  - Ripristino del servizio sui livelli preesistenti al guasto/anomalia;
  - Collaudo dell'apparato e della rete ad esso attinente in tutte le sue funzionalità per verificare l'avvenuta eliminazione della causa del guasto/anomalia;
  - Ripristino della funzionalità degli apparati attraverso sostituzione, in caso di impossibilità a garantire la riparazione/manutenzione (ad esempio per indisponibilità delle parti di ricambio).
  - Eventuale attivazione del fornitore terzo di connettività e collaborazione con lo stesso al fine di correttamente diagnosticare il problema e risolverlo.

L'attività sarà espletata tramite adeguati strumenti di controllo, allarmistica e troubleshooting quali ad esempio: TDR, Analizzatori LAN, Management SNMP, ecc.

Il Fornitore si dovrà far carico delle chiamate ad esso dirette per malfunzionamenti sulla rete dati anche quando i malfunzionamenti dichiarati dovessero essere poi imputabili ad altre cause.

Il Rapporto di malfunzionamento documenterà l'evasione della segnalazione e il ripristino del corretto funzionamento nell'ambito della procedura di trouble ticketing.

4.11.1.6 Manutenzione preventiva

Per ridurre il numero di richieste d'intervento a fronte di anomalie e criticità evidenziate, e quindi massimizzare l'operatività degli apparati e la produttività dell'utenza, saranno effettuati interventi preventivi sui prodotti oggetto del servizio; essi saranno pianificati in accordo con ICP laddove comportino una momentanea interruzione del servizio.

L'obiettivo fondamentale dell'attività di manutenzione preventiva è la riduzione dell'incidenza delle malfunzioni (sia hardware che software).

Questa attività comprende anche:

- L’analisi del contesto di evoluzione tecnologica e l’individuazione tempestiva delle azioni da intraprendere in merito a nuovi servizi offerti, nuove componenti tecnologiche o quant’altro possa migliorare il servizio offerto in termini di capacità e qualità;
- Gli interventi volti al miglioramento o arricchimento funzionale, a seguito di migliorie decise e introdotte dalla casa costruttrice degli apparati, che non comportano oneri contrattuali (aspetto evolutivo della manutenzione preventiva).

La manutenzione preventiva viene eseguita anche per assicurarsi del regolare funzionamento di ogni singola componente degli apparati LAN o, in caso di potenziali problemi di sicurezza, effettuando tutti gli interventi raccomandati dal produttore, per assicurare gli adeguati standard di sicurezza.

Nel dettaglio le attività previste sono:

- Controlli di regolare funzionamento tramite la postazione di management locale, effettuando test generali sia riguardo gli apparati che i link. La supervisione prenderà in considerazione non solo eventuali anomalie dovute a guasti hardware o software, ma anche situazioni di degrado dovute a congestione sui link (interni, privati e/o pubblici), sui nodi di switching/routing o sui carichi di CPU degli apparati principali, al fine di verificare l'efficienza degli apparati e di consentirne un adeguato dimensionamento;
- Misurazioni ed analisi sui componenti più significativi della rete per verificarne efficienza e prestazioni;
- Rilevamento di eventuali altri dati statistici importanti per valutare il corretto funzionamento della rete e dei suoi componenti;
- Effettuazione di backup dei dati di configurazione;
- Verifica e mantenimento dei requisiti di sicurezza funzionale, associati agli apparati e ai sistemi oggetto del servizio;
- Controllo periodico delle batterie degli UPS accertandone l’autonomia di funzionamento;
- Qualsiasi altra attività preventiva e/o periodica necessaria o utile per garantire un regolare funzionamento dei sistemi e delle reti LAN/WAN.

Queste verifiche andranno svolte periodicamente, salvo diverse necessità e urgenze, e genereranno apposito verbale.

4.11.1.7 Analisi dei problemi ripetitivi

Sulla base di variabili ricavate da serie storiche e sulla base di segnalazioni pervenute dai sistemi di gestione e di monitoraggio, nonché di valori stabiliti da norme tecniche, sono definite le soglie oltre le quali è necessario intervenire.

In questa fase è analizzato il verificarsi di problemi ripetitivi (oltre una soglia di attenzione). I risultati dell’analisi sono inseriti in un data-base e sugli elementi interessati sono eseguiti controlli approfonditi atti ad individuare e risolvere problemi di tipo strutturale.

Di questa attività va data visibilità ad ICP.

4.11.1.8 Rendicontazione

L'attività comprende il reporting della qualità del servizio ed il reporting sulle prestazioni.

Il reporting della qualità del servizio potrà includere:

- Informazioni riassuntive sui livelli di servizio globali, in termini di disponibilità della rete e tempi di ripristino;
- Informazioni (numero di trouble ticket, data di accettazione, data di chiusura, causa del disservizio, durata, tipo) relative a singoli disservizi;
- Trend storici dei valori di sintesi.

IL reporting sulle prestazioni genererà rapporti (sia di sintesi, che di dettaglio) su base periodica (per es. periodi di osservazione settimanali e giornalieri), analizzando, per esempio:

- L'interfaccia fisica per la connessione geografica (link);
- Gli apparati di networking (per es. router, switch,…);
- I tempi di attraversamento della rete.

I parametri analizzati saranno ad esempio:

- Volume totale di traffico (per i link): traffico totale (in e out) che ha interessato tutti gli elementi omogenei nel periodo di osservazione;
- Livello di occupazione di banda (per i link): misura, per specifico elemento, in termini percentuali del traffico generato rispetto alla velocità fisica (link);
- Utilizzo risorse HW (per i router): misura, per specifico elemento, del livello di sovraccarico del router (per es. % occupazione CPU,...).

4.12 Servizio di gestione del Software di base, ambiente e rete (incluso CRS-SISS)

Il servizio di gestione riguarda il software di base, d'ambiente e di rete installato su PdL e infrastruttura di rete.

Il servizio include anche tutte le attività su PdL necessarie per l'operatività SISS.

Il servizio include anche il software applicativo installato su PdL, come meglio precisato di seguito.

Al fine di tenere sotto controllo le configurazioni installate in esercizio, il Fornitore, organizzerà la gestione del SW di base, d'ambiente e di rete rilasciato in ottica di Release Management secondo ITIL: si chiede a tale proposito al Fornitore, a fini di valutazione dei processi proposti, di descrivere le strategie di gestione raccomandate, per i principali ambienti HW e SW supportati.

Questo comporterà la configurazione delle apparecchiature secondo "immagini" concordate, in modo da garantire configurazioni "controllate" sul parco e quindi ridurre le possibilità di incidenti, svolgendo le seguenti principali attività:

- Il Fornitore definisce delle “immagini”, cioè delle configurazioni di riferimento hardware e software di base e di produttività individuale;
- Il Fornitore amministra le configurazioni hardware e software, di base e di produttività individuale, delle PdL, sulla base degli indirizzi ricevuti da ICP, e definisce di conseguenza le “immagini” che costituiscono il riferimento per le PdL, in ogni condizione operativa di interventi dall’installazione, alla normale manutenzione, al backup e ripristino, ecc.
- Il Fornitore assicura l’installazione e l’aggiornamento del software compreso nelle “immagini”, facendo uso, per le PdL connesse alla rete, del Sistema di controllo remoto e di distribuzione del software, secondo piani concordati con l’utenza in caso di intervento singolo o con il Responsabile ICP, per interventi più ampi e generalizzati;
- Il Fornitore è tenuto a segnalare ad ICP la disponibilità di nuove versioni dei sistemi operativi, dei pacchetti di produttività e dei driver utilizzati in corrispondenza di eventi quali:
  - Disponibilità di versioni significativamente più aggiornate rispetto a quelle in esercizio;
  - Scoperta di malfunzionamenti nelle versioni in esercizio, per cui siano disponibili soluzioni “tampone” (patch) o rilasci di versioni che risolvano tali problemi;
- In seguito a tale segnalazione sarà facoltà di ICP autorizzare o meno l’aggiornamento delle corrispondenti “immagini” e rendere quindi operativa ogni variazione. Nel caso che tale variazione implichi operazioni di aggiornamento che interessino unità in esercizio, PdL o server, il Fornitore è tenuto a concordarne tempi e modi con il Responsabile di ICP.

È responsabilità del Fornitore:

- Proporre eventuali variazioni o migliorie del SW di base, sia in funzione delle norme contrattuali, che dell’evoluzione del mercato e della tecnologia hardware e software;
- Installare il software presso l’utente:
  - A fronte di aggiornamenti collettivi quali ad esempio l’aggiornamento di versione di applicazioni standard o la distribuzione di file per prodotti antivirus;
  - Per richieste individuali rivolte all’Help Desk ed approvate.
- Produrre una Relazione periodica relativa alle operazioni svolte.

Il Fornitore dovrà garantire il rispetto dei livelli di servizio indicati al paragrafo relativo.

4.12.1 Requisiti

4.12.1.1 Censimento iniziale

Il Fornitore dovrà rilevare, mediante opportuna attività di censimento iniziale, la configurazione del software di base, d’ambiente e di rete a disposizione di ICP, alimentando il CMDB.

4.12.1.2 Supporto alle configurazioni SW

Il supporto per le configurazioni SW copre:

- Incident, problem, change and release management per tutti gli aspetti che riguardano le configurazioni software di base, d'ambiente e di rete;
- La distribuzione di configurazioni SW utilizzando lo strumento di SW distribution;
- La manutenzione ed il supporto delle configurazioni ottimizzate;
- La gestione delle "major upgrades" (distribuzione in volume di una nuova configurazione di riferimento ad ogni PdL);
- La gestione delle "minor upgrades" che contengono:
  - Cambiamenti della configurazione;
  - Aggiornamento del middleware, dei driver, etc …
  - Installazione di patches di vulnerabilità;
- Amministrazione del server di SW distribution.

4.12.1.3 Distribuzione del Software

Il sistema di gestione messo a disposizione del fornitore deve essere in grado di installare in maniera automatica sulle PdL sia software di base e produttività individuale sia software applicativi sviluppati da ICP di Milano e da terze parti.

La distribuzione deve anche poter essere pianificata al di fuori degli orari di lavoro, senza intervento in locale di un operatore.

Il sistema deve assicurare la creazione e la gestione delle "Immagini", e comunque deve poter gestire anche "immagini" generate con altri tools, già in uso presso ICP.

In caso di migrazione del sistema operativo, il sistema deve anche essere in grado di migrare il profilo utente.

L'attività di distribuzione automatica del SW a cui si fa riferimento nel presente documento comprende:

- Aggiornamenti del SW di base installato sulle PdL;
- Installazione ed aggiornamento degli applicativi forniti da terze parti ad ICP, inclusi i prodotti di Office Automation;
- Installazione ed aggiornamento di qualsiasi programma di utilità od applicativo commerciale richiesto da ICP.

Tutte le attività suddette dovranno essere implementate mediante procedure di diffusione elettronica operando remotamente.

Tali procedure di aggiornamento dovranno essere utilizzabili dal Fornitore per l'aggiornamento di tutto il SW in dotazione delle PdL.

Eventuali applicativi sviluppati da terze parti per i quali viene richiesta la distribuzione su tutte oppure solo alcune PdL, devono essere opportunamente pacchettizzati e documentati

(a cura della terza parte che li ha forniti) al fine di essere resi installabili in automatico e da remoto.

Il Fornitore, qualora non fosse in grado di predisporre il SW per l'installazione da remoto autonomamente, dovrà concordare con ICP una pianificazione degli interventi di installazione on site.

4.12.1.4 Gestione del software relativo al progetto CRS-SISS su PdL

Come tutte le aziende sanitarie pubbliche della Regione Lombardia, anche ICP aderisce al progetto CRS SISS. All'avvio del progetto, nel 2006, Lombardia Informatica, in nome e per conto di Regione Lombardia, ha fornito le componenti di integrazione al progetto. Nel caso specifico di ICP, tali componenti sono commercialmente noti come PRI (Piattaforma Standard di Integrazione) prodotti da Santer-Reply.

Questo comporta la presenza in azienda di:

- Alcune componenti hardware e software "centrali" relative ai servizi di:
  - Porta Applicativa
  - Repository Referti
  - Banca Anagrafica Centralizzata
  - Middleware di integrazione
- Alcune componenti software installati sulle PdL:
  - Software di ambiente SISS
  - Software d'integrazione SISSway

In particolare per questi due ultimi componenti, il Fornitore si impegna ad eseguire tutte le operazioni connesse con la corretta gestione dell'impianto SISS aziendale. In particolare sono incluse le operazioni di:

- Nuova installazione dei software SISS e SISSway su nuove PdL;
- Aggiornamento di installazioni SISS e SISSway preesistenti;
- Verifica/correzione/re-installazione di SISS e SISSway su PdL che evidenzino malfunzionamenti;
- Presenza e supporto durante i test di non regressione eseguiti con le nuove release dei prodotti SISS e SISSway e le applicazioni sanitarie aziendali;
- Registrazione sul CMDB delle versioni sw presenti su ogni PdL e conseguenti operazioni di aggiornamento.

Attualmente questo servizio viene gestito tramite i "Service Provider" regionali accreditati a livello centrale con una procedura di gara, ma a fine 2011 tali accreditamenti scadranno. Lombardia Informatica si è impegnata a gestire le procedure di accreditamento per consentire ad altri fornitori di operare liberamente questo tipo di servizio. A tal proposito si veda il paragrafo "Accreditamento SISS".

Il Fornitore si impegna a fornire a ICP annualmente un report di consuntivo dei costi relativi alla gestione del software per il progetto CRS-SISS su PdL.

4.12.1.5 Gestione operativa delle applicazioni

Il Fornitore, relativamente al software applicativo installato su PdL avrà le seguenti responsabilità:

- Installazione dell'applicazione e suo avviamento;
- Preparazione delle utenze;
- Gestione dei problemi secondo il ciclo consueto di Help Desk;
- Risoluzione di incidenti attribuibili all'ambiente hardware e software di base, d'ambiente e di rete;
- Escalation, se necessaria, nei confronti di ICP e della terza parte fornitrice del software applicativo.

4.12.1.6 Esecuzione di interventi di aggiornamento collettivo

Nel caso di Esecuzione di interventi di aggiornamento collettivo, la richiesta sarà normalmente avanzata dai responsabili ICP nei confronti del Fornitore, con il quale sarà concordato un piano di aggiornamento opportuno.

Il Fornitore dovrà fornire il proprio contributo, anche in fase di pianificazione, per l'esecuzione delle operazioni richieste cercando di garantire la massima soddisfazione degli utenti finali e minimizzando i tempi di inattività di questi ultimi.

4.13 Servizio di manutenzione hardware

Il Fornitore dovrà mettere in opera una struttura organizzativa e tecnologica adeguata a far fronte alle richieste di interventi di manutenzione hardware che dovessero rendersi necessari per l'intera durata della fornitura.

Sono identificate le seguenti possibili categorie di interventi di manutenzione, a seconda del tipo di attività effettuata:

Manutenzione preventiva: l'insieme delle attività che si effettuano, secondo un Piano di manutenzione preventiva, al fine di garantire la disponibilità dei sistemi e degli apparati, anticipando, per quanto possibile, malfunzioni di natura Hardware e Software. Rientrano in questa categoria, per esempio, la verifica generale delle apparecchiature; la pulizia delle ventole e dei filtri; la pulizia e lubrificazione delle parti soggette a movimento, ecc.

Manutenzione correttiva: l'insieme delle attività intraprese in occasione delle segnalazioni di malfunzione parziale o totale delle apparecchiature, ivi comprendendo la diagnosi, la sostituzione di componenti, la sostituzione temporanea dell'apparecchiatura difettosa con altra equivalente, la riparazione dell'apparecchiatura, la sostituzione del componente o dell'apparecchiatura, l'attivazione dell'intervento della società che fornisce garanzia / supporto.

Il servizio di manutenzione contribuirà al soddisfacimento dei livelli di servizio indicati per gli altri servizi.

4.13.1 Requisiti

4.13.1.1 Manutenzione PdL ed apparati connessi

Relativamente alle Pdl ed a tutti gli apparati connessi (ad esempio stampanti e scanner) il Fornitore dovrà garantire un servizio di riparazione / sostituzione / modifica di componenti hardware coprendo tutti gli aspetti di servizio necessari. Saranno incluse eventuali attrezzature derivanti da contratti ad hoc o forniture estemporanee o di terze parti.

La fornitura dei pezzi di ricambio delle Pdl e degli apparati connessi (RAM, Hard Disk, ventole, alimentatore, mouse, tastiera, …) sarà inclusa nel servizio senza oneri aggiuntivi.

Saranno invece esclusi dalla fornitura: Batterie dei portatili, Batterie cache, Toner e Fusori delle stampanti.

Non è inclusa nel servizio la sostituzione integrale di apparati (PC, stampanti, scanner,…) dichiarati non riparabili. I materiali necessari in questo caso saranno prelevati dal Fornitore, su autorizzazione ICP, dal magazzino ICP.

ICP si riserva, attraverso visite ispettive, di verificare la corretta dichiarazione di riparabilità (sostituzione di componenti il cui valore è significativamente minore rispetto al valore dell'apparato).

Il Fornitore rilascerà ad ICP un rapporto mensile a consuntivo con il dettaglio delle operazioni di riparazione eseguite e le richieste di sostituzione evase.

Il Concorrente dovrà inserire nella busta contenente l'offerta economica per il lotto 1, un listino prezzi per la fornitura di pezzi HW per eventuale upgrade dei PC (RAM, Hard Disk). Il Fornitore dovrà aggiornare annualmente il listino; si precisa che tale eventuale fornitura non è vincolante per l'Azienda ICP che si riserva, comunque, la facoltà di procedere all'acquisto di detto materiale sul libero mercato.

In particolare il Fornitore dovrà:

- Riparare o sostituire integralmente ogni parte o componente (o l'intera apparecchiatura) risultata difettosa, danneggiata o inutilizzabile.
- Qualora il Fornitore ritenga che una riparazione non possa essere eseguita entro i limiti definiti nei Livelli di Servizio, sostituirà, per il periodo di riparazione, l'apparecchiatura guasta con una equivalente al fine di mantenere i livelli di servizio concordati. In tale circostanza il Fornitore dovrà garantire il caricamento dei dati utente e della configurazione della macchina standard ove possibile.

L'intervento del tecnico di manutenzione del Fornitore presso le sedi in cui sono installate le apparecchiature dovrà avvenire in modalità reattiva, sulla base di una programmazione giornaliera/oraria che dovrà tener conto della data ed ora di apertura della richiesta di intervento, della gravità del problema e della priorità assegnata, in relazione ai livelli di servizio previsti.

Sarà a carico del Fornitore recarsi con propri mezzi sul posto dell'intervento, così come l'eventuale trasporto delle apparecchiature, pezzi di ricambio e strumentazione; pertanto il Fornitore sarà responsabile di ogni danno conseguente e/o derivante dal trasporto delle stesse.

Il servizio di manutenzione sarà effettuato su tutte le apparecchiature, siano esse in garanzia o no; per le apparecchiature in garanzia, ICP comunicherà al Fornitore i contratti e le interfacce, ed il Fornitore sarà responsabile della gestione della garanzia.

4.13.1.2 Manutenzione apparati di rete

Gli apparati di rete saranno gestiti con le stesse modalità di cui alla voce "Manutenzione PdL ed apparati connessi", ad eccezione del criterio di seguito espresso.

Qualora sia necessario sostituire integralmente un apparato, il Fornitore lo sostituirà momentaneamente con un proprio apparato equivalente, al fine di ripristinare il servizio. L'apparato sarà reso disponibile ad ICP, senza oneri aggiuntivi, per la durata massima di giorni 30 (trenta) lavorativi, al fine di garantire il servizio durante il periodo di approvvigionamento del nuovo apparato da parte di ICP.

Nel caso di apparati con contratti di garanzia / supporto in essere, il Fornitore farà riferimento alle terze parti referenti di contratto.

ICP comunicherà al Fornitore l'elenco degli apparati sotto contratto di garanzia / supporto con terze parti.

ICP comunicherà al Fornitore i contratti e le interfacce, ed il Fornitore sarà responsabile della gestione della garanzia.

4.13.1.3 Rendicontazione

Tutti gli interventi di manutenzione dovranno essere tracciati attraverso l'apertura di un Ticket di intervento che dovrà essere inserito nel sistema di registrazione dei Ticket che il Fornitore dovrà gestire

4.14 Servizio di Configuration Management

Il servizio ha lo scopo di rilevare le variazioni nella composizione del parco a seguito dell'introduzione di nuove apparecchiature o di variazioni dell'infrastruttura ICT di ICP ed il mantenimento delle informazioni inventariali da comunicare secondo necessità ad altri uffici di ICP.
Obiettivo di ICP è il mantenimento delle informazioni relative al parco ICT non solo in termini di volumi (tipologie e quantità di hardware e software) ma anche in termini di attribuzione ai singoli centri di costo dell'Amministrazione e di assegnazione ai singoli Utenti (cambio di ubicazione, cambio di utenza, spostamento organizzativo).

Si chiede al Fornitore di supportare l'intero Servizio con strumenti informatici integrati, in grado di tenere sotto controllo il volume di apparecchiature in evoluzione continua che sarà oggetto del servizio stesso. Tutte le informazioni dovranno essere conservate in unico database sul quale dovranno essere registrati tutti i dati di configurazione, secondo il modello del CMDB suggerito da ITIL.

Dovranno essere gestiti fra gli altri (elenco non esaustivo):

- Rapporti di Service Desk ("tickets"), e relative statistiche;
- Rapporti sugli interventi di manutenzione - programmata e non;
- Livelli di servizio, di modo che ICP e Fornitore siano in grado di intervenire in tempo reale in caso di scostamenti rispetto agli obiettivi;
- Configurazioni di tutte le apparecchiature supportate e loro modifiche nel tempo, nonchè relazioni fra i componenti (Configuration Items – CI) che le costituiscono, più una serie di attributi che ne permettano la gestione non solo tecnica ma anche amministrativa e finanziaria ("Asset management");
- Specifiche, manuali etc. dei prodotti supportati;
- Rapporti contenenti le statistiche provenienti da sistemi di monitoraggio automatico (es. di sistemi o di reti);
- Rapporti relativi ai test periodici per la verifica di parametri degli SLA. I rapporti dovranno esplicitare con chiarezza i valori di misura da cui si evidenzi il soddisfacimento o meno degli SLA con possibilità di visualizzare nel dettaglio i ticket fuori SLA;
- Database di FAQ, Known-errors etc …
- Ogni altra documentazione prodotta dal personale di ICP o del Fornitore per qualsiasi tipo di motivo inerente al controllo della fornitura;
- In generale tutta la documentazione o i dati che, a vario titolo, sono connessi alla gestione tecnica ed amministrativa del contratto, nel corso del suo svolgimento.

Il Fornitore dovrà garantire il rispetto dei livelli di servizio indicati al paragrafo relativo.

4.14.1 Requisiti

4.14.1.1 Accesso del personale ICP al CMDB

Il personale di ICP dovrà essere reso autonomo nell'accesso e nell'elaborazione delle informazioni gestite dal CMDB e dovrà poter disporre di tutti gli strumenti di reporting.

Di conseguenza, indipendentemente dalle attività di reporting periodico richieste al Fornitore, ICP potrà utilizzare ed elaborare tutti i dati memorizzati, in ogni momento senza vincoli da parte del Fornitore.

Tutti i dati caricati ed i report prodotti dovranno essere esportabili in formati standard (ad esempio csv).

Il Fornitore garantirà la possibilità di accesso a 15 (quindici) utenti ICP di cui 5 (cinque) contemporanei.

4.14.1.2 Asset Management

La componente più strettamente di Configuration Management del CMDB costituisce una piattaforma per lo svolgimento del servizio normalmente definito come Asset Management, e di cui un componente essenziale ma parziale è l'inventario.

Il fornitore si dovrà dotare di un sistema specifico in grado di registrare tutti gli asset gestiti da contratto e in grado di aggiornare in maniera automatica tutti i dati relativi agli asset che lo consentono. Questo sistema dovrà essere integrato con il sistema di Helpdesk e farà riferimento allo stesso database contenuto nel CMDB.

Le principali operazioni da supportare saranno:

- Raccogliere, mantenere e distribuire informazioni accurate e aggiornate sulle apparecchiature supportate per poterne gestire le dotazioni;
- Controllare lo stato di operatività dei beni, per poter pianificare con efficienza gli upgrade in relazione alle richieste e necessità degli obiettivi del Cliente;
- Generare i report necessari alla valutazione dell'inventario per un'eventuale pianificazione di rinnovo tecnologico.

Il servizio dovrà essere svolto implementando e manutenendo un database iniziale di gestione del ciclo di vita completo del parco delle attrezzature informatiche, telematiche e del software installato.

Il sistema dovrà essere integrato con quello di Help Desk, per permettere agli operatori di aprire e chiudere i ticket. Nel caso la richiesta sia passata a terze parti, dovranno essere predisposte delle modalità che garantiscano la registrazione della chiusura della richiesta sullo strumento di supporto.

Il servizio è attivato come conseguenza dell'erogazione di altri servizi (di norma IMAC) che causano la necessità di aggiornamento della base dati inventariale, e si chiude successivamente alla variazione inventariale.

L'aggiornamento deve essere tempestivamente assicurato per ogni variazione, quali, ad esempio:

- Nuova installazione di PC e/o periferiche locali;
- Installazione di nuova periferica di rete (stampanti, periferiche multifunzione,ecc.);
- Movimentazione utente e/o postazione;
- Aggiunte hardware/software su PC/periferiche;
- Dismissione di PC/periferiche.

Il sistema dovrà poter rilevare, in automatico:

- Il serial number della CPU delle PdL e le caratteristiche dei principali componenti della stessa RAM, capacità dell'hard disk, tipo di monitor ecc.
- Il software installato in termini di sistema operativo, software di ambiente, software di produttività individuale e standard, software di connettività, browser web, software applicativo. Si segnala che è fatto divieto all'utente finale installare sulla PdL software personale che non sia stato autorizzato dal SIA.

- L'elenco degli utenti di ogni PdL ed i relativi privilegi.

Il sistema deve riversare i dati inventariali hardware e software in un DataBase SQL o Oracle; ai dati inventariali rilevati automaticamente devono poter essere aggiunti dati richiesti all'utente.

Il sistema deve essere in grado di inventariare apparecchiature con ogni famiglia di sistema operativo principale (Windows, Mac, Linux, Unix) e di tutti i principali produttori.

In generale il Fornitore avrà la responsabilità di effettuare il controllo della configurazione completa di ogni sistema in gestione, con l'esclusione di eventuali parametri variabili in modo dinamico e non controllabile ed il controllo degli addetti preposti alla manutenzione di quel determinato sistema o classe di sistemi. Per "configurazione" si intende non solo i parametri di installazione dell'apparato, ma anche tipo e versione del sistema operativo e software applicativo installati e tutti gli eventuali aggiornamenti. Le attività richieste sono:

- Identificazione e controllo della configurazione;
- Registrazione dello stato di configurazione;
- Audit sulla configurazione.

Ogni tipologia di richiesta che comporti il cambiamento alla configurazione effettuata dal Fornitore su sistemi dovrà comunque essere sempre documentata e nel caso comporti un potenziale pericolo ai sistemi informativi di ICP, il Fornitore dovrà produrre un'analisi delle motivazioni e dell'impatto da sottoporre ai corrispettivi riferimenti di ICP che decideranno in merito all'attuazione dello stesso ("change management").

4.14.1.3 Supporto all'asset management dei sistemi server

Il fornitore dovrà rendere disponibile a ICP e/o Fornitori nominati da ICP il sistema di asset management (CMDB) integrato con il ticketing system, in modo che ICP e/o Fornitori nominati da ICP possano caricare e gestire tutti i dati riguardanti i sistemi server nel CMDB.

4.15 Servizio di gestione della sicurezza

Al fine di consentire un'efficace ed efficiente gestione della sicurezza informatica sotto tutti gli aspetti, il Fornitore si impegna a rispettare le prescrizioni in materia di sicurezza informatica che saranno emanate da ICP e si impegna a fornire tutto il supporto necessario per la risoluzione di eventuali incidenti o situazioni di crisi per la sicurezza delle informazioni.

La gestione della sicurezza informatica implica l'esecuzione di compiti, fra i quali:

- Effettuare un costante monitoraggio di tutte le risorse, per intercettare e documentare tentativi di violazione di qualsiasi origine;
- Gestire gli incidenti di sicurezza, e le eventuali emergenze ad essi connesse, assicurando la formazione di task force, operanti nell' ambito di unità di crisi, finalizzate al superamento/soluzione in caso di eventi che compromettono le normali condizioni di operatività di funzionalità critiche per dimensione, durata ed estensione;
- Approntare e trasmettere con periodicità almeno mensile un rapporto sugli aspetti della sicurezza;

- Predisporre costantemente tutte le misure preventive, che possano ridurre i rischi (es. aggiornamenti per sistemi operativi, database firme antivirus, system hardening, etc…);
- Amministrare il sistema di diritti e profili d'utente secondo opportune policy di sicurezza;
- Raccomandare ad ICP nuovi approcci, che possano aumentare la sicurezza complessiva del servizio, ed in generale del Cliente.

Il Concorrente descriverà caratteristiche e modalità di erogazione dei servizi richiesti e documenterà nella apposita sezione dell'Offerta Tecnica un modello organico e articolato per la gestione della sicurezza informatica per le attività di competenza, a partire da tutto quanto richiesto nei successivi paragrafi.

Il servizio deve provvedere a:

- Garantire un adeguato livello di sicurezza per le risorse informatiche;
- Applicare e garantire le policy stabilite da ICP relativamente alle risorse e ai servizi informatici;
- Reagire prontamente ed efficacemente agli eventi di sicurezza segnalati dai canali stabiliti (monitoraggio, help desk, enti e organismi specializzati);
- Attivare tempestivamente i processi di escalation per il supporto decisionale;
- Fornire le statistiche sugli eventi registrati al fine di identificare carenze di sicurezza e definire le azioni necessarie alla riduzione del rischio;
- Mettere tempestivamente in atto gli aggiornamenti necessari per l'efficace funzionamento delle componenti fornite;
- Migliorare l'efficacia e l'efficienza nelle modifiche alle configurazioni richieste;
- Controllare ed analizzare i log dei sistemi e gli allarmi di tipo automatico;
- Effettuare una analisi periodica dello stato della sicurezza (sistemi e servizi) con emissione di relativo report.

I servizi erogati e le modalità di gestione dovranno essere conformi sia alle politiche per la sicurezza stabilite da ICP, sia quanto più possibile in linea con le norme ISO 17799.

Il Fornitore dovrà garantire il rispetto dei livelli di servizio indicati al paragrafo relativo.

4.15.1 Requisiti

4.15.1.1 Censimento iniziale

Il Fornitore dovrà rilevare, mediante opportuna attività di censimento iniziale, la configurazione di tutti gli aspetti relativi alla gestione della sicurezza in essere relativi alle PdL ed all'infrastruttura di rete, alimentando il CMDB.

4.15.1.2 Responsabile della sicurezza informatica

Il Fornitore dovrà identificare un'apposita figura di responsabile della sicurezza informatica per il presente contratto, di cui fornirà riferimenti completi, che assumerà pieni poteri e responsabilità dalla data di inizio del contratto.

Il responsabile della sicurezza:

- Sarà il riferimento diretto ed unico per il comitato di sicurezza di ICP per ogni tipo di problema di sicurezza informatica relativo al contratto oggetto di questo appalto, alle cui riunioni dovrà partecipare se richiesto;
- Sarà poi responsabile del coordinamento, supervisione ed attuazione di tutti gli interventi tecnici relativi alla sicurezza informatica che saranno richiesti da ICP per quanto di competenza del Fornitore;
- E' considerato garante del rispetto delle disposizioni di sicurezza qui indicate e di tutte quelle emanate dal comitato di sicurezza;
- In caso di sua assenza temporanea o prolungata, dovrà essere tempestivamente identificato un sostituto avente delega completa, i cui riferimenti dovranno essere immediatamente comunicati ad ICP.

4.15.1.3 Strategia di gestione

Il servizio di Gestione della Sicurezza realizza e gestisce le contromisure di tipo tecnologico e procedurale volte alla difesa del sistema informativo di ICP: difesa perimetrale, controllo codice malevolo, analisi periodica dei sistemi/servizi, procedure di ripristino in seguito ad incidenti informatici, reportistica e rendicontazione.

Tutto ciò si realizza attraverso la gestione di idonei sistemi specializzati (firewall, antivirus, proxy etc.), verifica e rimozione di collegamenti esterni non controllati (es. modem), attività di monitoring e correzione di anomalie hardware/software, definizione ed applicazione di policy che regolano l'utilizzo delle risorse e dei servizi informatici erogati.

Un altro aspetto altrettanto importante è l'osservazione "a freddo" dei fenomeni e degli eventi relativi alla sicurezza delle risorse informatiche, al fine di poter adattare le contromisure e le policy alle nuove minacce e ai rischi ad essi associati; ciò viene realizzato sulla base di un rapporto periodico sullo stato delle risorse informatiche e degli eventi/incidenti occorsi, per la composizione del quale concorrono tutte le attività descritte in questo capitolo.

La sicurezza informatica è gestita attraverso le procedure qui descritte ed è prevalentemente di pertinenza delle figure professionali che se ne occupano; ma tutto il personale informatico impegnato nella gestione dell'infrastruttura informatica concorre nel mantenere un adeguato livello di sicurezza (informatica), poiché questa è intrinsecamente correlata a sistemi, procedure e applicazioni che compongono l'infrastruttura informatica nel suo insieme.

Il processo proposto per la gestione della sicurezza delle informazioni dovrà essere compatibile con le Best Practices for Security Management – ITIL.

4.15.1.4 Controllo del codice malevolo

Le licenze dei prodotti antivirus sono a carico di ICP.

Il sistema di controllo del codice malevolo (virus, spyware etc.) deve essere installato su tutte le PDL. Il Centro dispone di un sistema antivirus centralizzato che è costantemente mantenuto aggiornato in particolare riferimento alle signature dei virus.

Gli aggiornamenti (automatici) devono essere distribuiti su tutte le PDL, le Workstation e i sistemi che offrono servizi informatici.

L'attività di controllo deve verificare che gli aggiornamenti siano distribuiti sulle PDL e su tutti i sistemi su cui è previsto.

Eventuali anomalie nella procedura di aggiornamento, in tutte le sue fasi, devono essere prontamente rilevate e risolte.

Il Rapporto mensile conterrà le seguenti informazioni:

- Variazioni della configurazione del sistema,
- Anomalie riscontrate
- Virus o altro codice rilevato

4.15.1.5 Monitoraggio di sicurezza

Il monitoraggio consiste di un insieme di attività il cui scopo principale è la rapida ed efficace risoluzione delle anomalie riscontrate e il ripristino del corretto funzionamento dell'infrastruttura:

- Una costante attività di analisi dei sistemi di sicurezza e dei sistemi critici dell'infrastruttura;
- Rilevazione tempestiva di eventi ed allarmi critici per la sicurezza informatica;

È quindi necessaria una continua e consapevole osservazione dell'infrastruttura gestita al fine di:

- Prevenire i rischi;
- Verificare la corretta attuazione delle politiche di sicurezza e la loro efficacia;
- Individuare tempestivamente situazioni di allarme;
- Fornire un report periodico emesso mensilmente;
- Concorrere a dare una visione globale sull'attività svolta e lo stato di funzionamento dei sistemi di sicurezza;
- Supportare ICP nell'individuazione di strategie di miglioramento che possano simulare e contenere attacchi al sistema informatico con l'obiettivo di ottimizzazione delle risorse investite.

In particolare:

- La Rilevazione tempestiva di eventi ed allarmi critici per la sicurezza informatica è un elemento essenziale per poter fronteggiare nel più breve tempo possibile gli incidenti informatici di qualsiasi natura, al fine di evitare il propagarsi e l'aggravarsi del problema.

- Dove possibile devono essere attivati i servizi di notifica a mezzo e-mail (o in altro modo altrettanto efficace) verso il Security Manager/amministratore di sistemi/postazione di monitoraggio, sempre controllato durante l'orario stabilito di presidio.
- Ogni allarme o evento ed eventuali richieste da parte dell'Help Desk innescano il processo di gestione delle emergenze.

Si richiede un monitoraggio costante delle informazioni e delle componenti dell'infrastruttura definiti dalla politica per la sicurezza di ICP che permetta di:

- Prevenire i rischi;
- Verificare la corretta attuazione delle politiche di sicurezza e la loro efficacia;
- Individuare tempestivamente situazioni di allarme.

Gli allarmi generati avvieranno l'attività di gestione delle emergenze (escalation) che dovrà elaborare tali allarmi al fine di ripristinare:

- La disponibilità delle risorse (es. Dati, Software) rispettando i medesimi SLA previsti a seguito di guasti;
- La robustezza/consistenza originaria delle misure di sicurezza.

4.15.1.6 Configuration management per la sicurezza

Il servizio provvede alla definizione, manutenzione e controllo delle politiche di configurazione e di aggiornamento dei sistemi rilevanti per ICP, in termini di sistema operativo e applicazioni di base.

Tutte le configurazioni e le release del SW delle apparecchiature dovranno essere ottimizzate avendo in primo luogo attenzione al miglioramento della loro protezione e sicurezza; di conseguenza quanto qui espresso dovrà informare le attività del Fornitore in tutte le attività di Configuration e Release Management.

In relazione alle componenti SW presenti sulle apparecchiature che dovranno essere gestite dal Fornitore comprensive di SW di Base, SW di Rete, SW di produttività individuale, il Fornitore avrà la responsabilità di:

1. Effettuare il security hardening delle apparecchiature, per limitare il livello di vulnerabilità delle risorse ICT del sistema operativo e delle applicazioni di base:
    - Producendo ed implementando direttive di configurazione che eliminano le funzionalità non necessarie e personalizzano i sistemi operativi per i soli servizi che essi debbono offrire, seguendo le indicazioni fornite da ICP;
    - Monitorando e segnalando la disponibilità degli aggiornamenti, con relativo livello di criticità, ed indicazione del tempo massimo di applicazione, ed implementandoli di conseguenza; qualora non applicabili a causa di incompatibilità con software istallati, attuazione di correttivi o contromisure finalizzate a ridurre il rischio.
2. Effettuare l'installazione pianificata di aggiornamenti collettivi del software (nuove versioni di applicazioni standard o la distribuzione di file di definizioni antivirus aggiornati) presso gli utenti, con modalità concordate con ICP;

3. Effettuare l'installazione di aggiornamenti per la correzione mirata di vulnerabilità critiche nel caso possano mettere in serio pericolo la sicurezza del Sistema Informativo di ICP;
4. Configurare e (far) utilizzare ogni apparecchiatura al livello minore ("più sicuro") di accesso utilizzatore necessario per l'uso corrispondente (es. "tutte" le PdL in modalità "user"; accesso ed operatività in modalità "administrator" anche sui server per lo stretto necessario);
5. Produrre una relazione semestrale comprensiva sia di nuove release che di patch o correzione di bug, o per integrazione di nuove funzioni, rilasciate ufficialmente dai produttori di software specifici installati, anche di proprietà di ICP.

4.15.1.7 Aggiornamenti

Ci si riferisce qui all'aggiornamento dei sistemi di sicurezza, attività avviata solitamente a seguito della disponibilità di nuovi rilasci da parte dei fornitori dei prodotti, finalizzati a proteggere da minacce note e/o prevenirne di nuove; ad esempio:

- Database delle *signature* degli antivirus;
- *Aggiornamenti critici* per i sistemi operativi e le applicazioni di base;
- Black list per sistemi di content filtering;
- Database dei *pattern* di attacco degli IDS.

La rapidità nella distribuzione degli aggiornamenti varia in base al tipo di servizio ed in funzione dell'entità del rischio derivante dalla mancata od intempestiva esecuzione dell'attività.

In ottica di Change Management (e di conseguenza tenendo conto dei rischi derivanti dai ripetuti cambi di configurazione), si richiede al Concorrente di formulare una proposta relativa alla tempestività degli aggiornamenti, da perfezionare in sede di contratto in accordo con la politica per la sicurezza stabilita di ICP.

4.15.1.8 Verifica della conformità

È necessario verificare l'allineamento dell'insieme della configurazione installata sul parco alle direttive stabilite in materia di sicurezza delle configurazioni (risultato delle scelte concordate del Fornitore e di ICP, mettendo in pratica direttamente le indicazioni dei produttori dei sistemi operativi o delle applicazioni stesse, e/o personalizzando le configurazioni in base alle specifiche dell'infrastruttura in cui i sistemi si trovano ad operare).

È opportuno che la verifica esamini cambiamenti importanti della configurazione:

- Su base periodica, per l'intero parco macchine al quale il servizio è rivolto;
- Prima del rilascio in esercizio delle applicazioni;
- A seguito di modifiche importanti ai servizi erogati.

È necessaria inoltre una verifica periodica:

- Sia delle direttive definite per eventuali miglioramenti e adeguamenti a fronte di nuove vulnerabilità;
- Sia della conformità delle configurazioni dei sistemi alle direttive approvate.

A tale proposito si chiede al Fornitore, un'autocertificazione periodica dell'attuazione delle regole e delle policy decise da ICP e la cui implementazione è stata richiesta al Fornitore stesso mediante le opportune procedure.

In particolare tale documentazione deve includere:

- La descrizione delle regole implementate;
- Il risultato dei test effettuati atti a garantire l'effettivo rispetto di tali regole.

4.15.1.9 Gestione degli incidenti di sicurezza informatica

L'attività di gestione degli incidenti di sicurezza informatica (gestione delle emergenze) ha l'obiettivo di fornire rapide ed efficaci risoluzioni delle anomalie riscontrate in termini di sicurezza informatica, fino al ripristino del corretto funzionamento dell'infrastruttura nel rispetto degli SLA indicati.

La gestione degli incidenti informatici deve assumere una più alta priorità di intervento rispetto ad altri eventi in relazione alla entità degli stessi; più è elevata la gravità dell'evento più alta sarà la priorità assegnata.

Il processo è attivato a seguito di una segnalazione od evento potenzialmente critico. La segnalazione può essere notificata da:

- Un allarme generato dal processo di monitoraggio di sicurezza;
- Una richiesta o una segnalazione del Help Desk (primo o secondo livello).

La segnalazione determinerà l'intervento di un gruppo specialistico di gestione della sicurezza informatica messo a disposizione dal servizio di gestione dei server.

Il fornitore collaborerà con il gruppo specialistico al fine di gestire al meglio l'incidente.

4.15.1.10 Identificazione del personale

Il personale che opera per la fornitura dei servizi deve essere chiaramente identificabile. L'elenco completo del personale addetto e dei relativi recapiti, compiti e permessi amministrativi dovrà essere mantenuto aggiornato e accessibile dal CMDB. Ogni variazione a questo elenco dovrà essere segnalata preventivamente a ICP; nessun addetto all'infuori di quelli elencati ed approvati avrà autorizzazione ad accedere alle sedi di ICP.

4.15.1.11 Supporto alle operazioni

Il Fornitore si impegna a fornire, tramite la supervisione del proprio responsabile della sicurezza, tutto il supporto tecnico necessario nel caso ICP decidesse di implementare nuove funzionalità di sicurezza sulla propria infrastruttura.

Il Fornitore si impegna altresì a fornire tutto il supporto tecnico necessario, e per tutto il tempo entro il quale questo sarà richiesto, in caso di risoluzione di incidenti relativi alla sicurezza delle informazioni ed in caso di disastro che porti all'interruzione del servizio di parti dell'infrastruttura di rete.

4.15.1.12 Accesso ai dati circolanti in rete

Il Fornitore non potrà mai, salvo esplicita autorizzazione di ICP, accedere ai dati trasportati sulla rete di ICP, con l'esclusione della parte necessaria alla corretta erogazione del servizi richiesti.

Ogni abuso in questo senso verrà sottoposto agli organi competenti per la valutazione di potenziali ripercussioni anche di tipo legale.

4.15.1.13 Conformità a norme e standard

L'erogazione dei servizi di sicurezza sarà in linea con le regole d'arte correnti nell'industria (best practices) ed almeno in linea con le seguenti normative:

ISO/IEC 17799:2005: Information Security Management – Code of practice for information security management, 2005;

ISO/IEC 27001:2005: Information security management systems – Requirements, 2005;

Ministero per l'Innovazione Tecnologica – La sicurezza Informatica e delle Telecomunicazioni (ICT Security) – Allegato 2, Gennaio 2002;

Dlgs 196/2003 e suoi aggiornamenti– Codice in materia di protezione dei dati personali, Allegato B. Disciplinare tecnico in materia di misure minime di sicurezza;

Provvedimenti del Garante della Privacy

DigitPA – Linee guida per la sicurezza ICT delle Pubbliche Amministrazioni.

4.16 Rilascio di rapporti di servizio

Il Fornitore dovrà produrre, nell'ambito dello svolgimento dei servizi previsti, un insieme di rapporti periodici.

La rendicontazione ha sia l'obiettivo di verificare l'andamento del servizio che di fornire informazioni utili all'evoluzione delle forme contrattuali.

La descrizione dei servizi previsti precedentemente fornita include alcune specifiche relative ai rapporti da emettere.

In generale si prevede l'emissione di rapporti che contengono i dati fondamentali relativi ad ogni servizio fornito ed ICP concorderà con il Fornitore, nella fase di avvio del contratto, gli specifici contenuti, la periodicità ed i formati con cui i rapporti saranno prodotti.

4.17 Strumenti di gestione

Il fornitore dovrà rendere disponibile un sistema hardware e software che includa, al minimo, gli strumenti software adeguati a svolgere le seguenti funzioni:

- Gestione ticket;
- Gestione CMDB;
- Monitoraggio e controllo remoto PdL;
- Monitoraggio infrastruttura di rete;

- Monitoraggio server e applicazioni software installate sui sistemi server;
- Distribuzione software di base e applicativo.

La funzione di monitoraggio dovrà riguardare le caratteristiche di affidabilità, prestazioni e sicurezza.

Il sistema dovrà essere indipendente dai sistemi ICP e dovrà possedere elevati requisiti di disponibilità.

Tutti gli strumenti software (funzionalità e dati gestiti) dovranno essere accessibili da remoto attraverso interfacce web.

Tutti i dati caricati dovranno essere esportabili in formati standard (ad esempio csv).

La relativa proposta tecnica sarà oggetto di specifica valutazione.

Sarà cura del fornitore:

- Installare e rendere operativo il sistema presso la sala server ICP in modo che possa essere utilizzato anche dal personale ICP o da personale nominato da ICP;
- Mettere a disposizione il contratto di manutenzione hardware del sistema, per tutta la durata del contratto e con livelli di servizio adeguati al rispetto degli SLA contrattuali.

Il sistema sarà utilizzato sia dal fornitore del lotto 1 che dal fornitore del lotto 2 (ad esempio per gestione ticket, gestione CMDB e monitoraggio server e rete sala server).

Il sistema hardware e software di base sarà gestito dal fornitore del lotto 2.

Gli strumenti software installati sul sistema saranno gestiti dal fornitore del lotto 1.

Al termine del contratto, in caso di recesso dopo i tre anni e in caso di risoluzione anticipata del contratto, il Fornitore rilascerà senza oneri aggiuntivi a ICP la proprietà del sistema e la licenza illimitata, se esistente o alternativamente per sette anni, di tutti gli strumenti software, incluso il CMDB caricato e la base dati completa dei ticket fino ad allora registrati.

Tutti i dati caricati resteranno di esclusiva proprietà ICP.

4.18 Specifica dei livelli di servizio minimi richiesti

Il modello di specifica dei livelli di servizio è teso a garantire il mantenimento dell'alto livello di affidabilità che caratterizza i sistemi informativi ICP, con livelli di continuità del servizio superiori al 99,9%.

Il Fornitore responsabile del I^{o} lotto avrà la piena responsabilità di garantire il mantenimento dell'alto livello di servizio. Egli risponderà per ogni interruzione osservata. Il mancato raggiungimento degli obiettivi di continuità comporta il pagamento di penali che sono dimensionate in base all'impatto rispetto all'erogazione del servizio.

Il Fornitore potrà presentare evidenze che trasferiscano la responsabilità del disservizio ad altri fornitori di ICP (ad es., Fornitore responsabile del II^{o} lotto, fornitori delle applicazioni, fornitori della connettività di rete). Solo nel caso in cui le evidenze consentano effettivamente il trasferimento della responsabilità in capo ad altri, il Fornitore sarà esentato

dal pagamento delle penali. Nel caso non sia raggiunto un accordo sull'assunzione di responsabilità, ICP assume il ruolo di arbitro con parere vincolante.

Il modello che valuta il livello di servizio ha una struttura con tre componenti principali.

1. Il primo componente è rappresentato da un modello quantitativo che ha come obiettivo la stima della continuità del servizio erogato. Diversi servizi sono caratterizzati da diversi livelli di importanza.
2. Il secondo componente è costituito da un insieme di indicatori di livello di servizio (SLA), i quali hanno come obiettivo quello di imporre vincoli relativi alla capacità da parte del sistema di fornire una risposta pronta alle richieste di intervento e di verificare il soddisfacimento delle richieste di ICP per quanto riguarda tutte le attività che non comportino un impatto immediato sulla continuità di erogazione del servizio. Si prevedono SLA relativi ai tempi di gestione delle chiamate telefoniche verso il servizio HelpDesk, tempi per la gestione di richieste IMAC, tempi per la gestione dei traslochi. Per ogni servizio sono di seguito identificati i corrispondenti SLA minimi.
3. Il terzo componente è rappresentato dalla esecuzione di verifiche ispettive. La visita ispettiva verificherà che le modalità di attuazione del servizio soddisfino i vincoli del presente capitolato e tutti gli altri vincoli derivanti dal contratto con il Fornitore. L'obiettivo di questa attività di verifica è di tenere sotto controllo sia gli aspetti quantitativi sia quelli qualitativi.

4.18.1 Modello di valutazione della continuità del servizio

Come già attualmente in essere, la continuità del servizio sarà misurata attraverso un modello che valuta la disponibilità dei sistemi agli utenti. Il modello considera attentamente la variabilità del livello di criticità nelle diverse applicazioni e il grado di necessità di un pronto intervento nella risoluzione dei problemi. Il parametro "Peso" rappresenta la criticità di ogni attività. E' da notare che il parametro "Peso" è cumulabile e qualora un guasto pregiudichi sulla stessa PdL la esecuzione di una varietà di servizi, il valore di "Peso" da applicare sarà dato dalla somma dei diversi valori. Per quanto riguarda la prontezza di intervento, il modello specifica una "franchigia" per le attività in cui un breve periodo di non disponibilità del servizio produce un impatto limitato sull'effettivo servizio erogato. La franchigia rappresenta un valore soglia di minuti che non comporta un contributo del guasto alla misura del livello di servizio, applicabile una sola volta per data e un massimo di 15 volte per periodo mensile di valutazione mensile. Se la risoluzione del problema avviene oltre la durata della franchigia, l'intero ammontare di minuti di non disponibilità contribuirà alla misura del livello di servizio. Le attività di manutenzione che sono svolte seguendo un piano approvato da ICP non contribuiscono alla misura, purché l'esecuzione avvenga rispettando il piano concordato.

Nella tabella seguente, sono elencate le componenti del servizio, con il corrispondente peso relativo e l'eventuale franchigia. I coefficienti devono essere intesi come misurati su ciascuna PdL.

DOMINIO APPLICATIVO	PESO	TEMPO DI FRANCHIGIA (MIN)
Servizi base di infrastruttura	**114**	
Impossibilità di accesso al sistema di ticketing e ritardo nella registrazione dell'istante di inizio dei guasti/disservizi	100	
Accessibilità utenti a Internet	6	30
Posta elettronica	6	30
Antivirus	2	240
Servizi Area Sanitaria	**70**	
LIS	7	
CUP	7	
ADT	7	
Reparto	7	
Ambulatoriale	7	
PS	7	
Blocco operatorio	7	
Interfaccia HOpera-LIS	7	
Interfaccia HOpera- RIS	7	
Interfaccia HOpera-BDA/RS-SISS	7	
Servizi Area Amministrativa	**45**	
Protocollo	3	15
Portale WEB	3	15
Intranet	3	15
Gestione Contabile-Amministrativa (NFS)	4	
Gestione personale (giuridico-economico – 25/10)	2,5	
Gestione personale (giuridico-economico – 11/24)	5	
Gestione personale (gestione presenze WEB)	4	
Gestione Determine	4	15
Gestione Delibere	4	15
Data Warehouse	2,5	15

DOMINIO APPLICATIVO	PESO	TEMPO DI FRANCHIGIA (MIN)
Khalix	4	15
Produttività individuale	3	15
File server	3	10

Sulla base di questi domini applicativi la seguente formula stabilisce il disservizio totale sommando i disservizi dei singoli sistemi applicativi:

$$Serv = 1 - \frac{\sum_{j=1}^{n} Peso_j \left(\sum_{i=1}^{m} \beta_i \sigma_i \quad t_i \, d_i \quad \right)}{\sum_{j=1}^{n} T_j \, D_j}$$

Dove:

j = 1,n	applicativi gestiti
Peso$_j$	peso attribuito all'applicativo j
i = 1,m	eventi negativi registrati (disservizi)
β_i	Indicatore sul superamento della franchigia (0, 1)
σ_i	criticità del disservizio: 0,5 = degrado delle prestazioni (efficienza diminuita) 1 = blocco totale (non si possono completare le transazioni)
t_i	tempo di non disponibilità registrato (durata del disservizio)
d_i	numero di postazioni bloccate
T_j	Tempo complessivo di disponibilità del servizio
D_j	Numero di postazioni che erogano il servizio

A titolo d'esempio, si supponga che vi siano solo due servizi con peso 5 con franchigia di 5 minuti erogati da 1000 postazioni che sono attive 24/7. Si assuma poi che in un mese di 30 giorni si siano verificati: un guasto g1 non bloccante di 4 minuti sul primo servizio che ha coinvolto 10 postazioni, un guasto g2 non bloccante di 10 minuti sul primo servizio che ha coinvolto 100 postazioni, e un guasto g3 bloccante di 30 minuti sul secondo servizio che ha coinvolto 20 postazioni. Il livello di servizio *Serv* sarà pari a:

1-(5 *peso* * ((0 * 0,5 σ * 4 *min* * 10 *PdL*)$_{g1}$ + (1 * 0,5 σ * 10 *min* * 100 *PdL*)$_{g2}$) + 5 *peso* * (1 * 1 σ * 30 *min* * 20 *PdL*)$_{g3}$) / (30*24*60*1000+30*24*60*1000)

= 1 – ((0 + 2500) + 3000)/86400000

= 0,9999363

E’ da notare che la presenza del fattore “Peso” rende il risultato dell’applicazione della formula diverso da quello convenzionalmente adottato in ambito tecnico per valutare l’affidabilità dei sistemi.

Si osservi che per "numero di postazioni" s'intende il numero di PdL da cui uno specifico servizio può essere invocato. Ad esempio l'accesso al sistema di ticketing riguarda tutte le PdL da cui è possibile aprire un ticket via web.

4.18.2 SLA

Per ogni servizio sono di seguito identificati i corrispondenti SLA minimi.

Ogni SLA è identificato da una o più misure o da modalità di verifica. Ove non altrimenti specificato, per “ore / giorni” si intende “ore / giorni lavorativi”.

Servizio di Assistenza

- Percentuale di chiamate telefoniche entranti in cui il tempo di risposta da parte dell’operatore è inferiore a 30 secondi:

  70 %

- Esito positivo delle verifiche ispettive.

Servizio di Gestione delle Postazioni di Lavoro (PdL)

- Tempo massimo di esecuzione (dall’apertura alla chiusura di ticket) di una richiesta di attività (movimentazione, aggiunta, cambiamento, installazione, disinstallazione, sostituzione, dismissione) per singola PdL per utenti di livello 1-priorità elevata o livello 1-priorità elevata h24/7:

  giorni 1

- Tempo massimo di esecuzione (dall’apertura alla chiusura di ticket) di una richiesta di attività (movimentazione, aggiunta, cambiamento, installazione, disinstallazione, sostituzione, dismissione) per singola PdL per utenti di livello 2-priorità normale:

  giorni 2

- Rispetto del piano di esecuzione concordato con ICP per interventi di manutenzione programmata, sostituzione, trasloco:

  100% nei tempi pianificati

- Esito positivo delle verifiche ispettive.

Servizio di gestione della rete aziendale

- Esito positivo delle verifiche ispettive.

Servizio di gestione del Software di base, d’ambiente e di rete

- Tempo massimo di esecuzione (dall'apertura alla chiusura di ticket) di una richiesta di attività per singola PdL per utenti di livello 1-priorità elevata o livello 1-priorità elevata h24/7:

  giorni 1

- Tempo massimo di esecuzione (dall'apertura alla chiusura di ticket) di una richiesta di attività per singola PdL per utenti di livello 2-priorità normale:

  giorni 2

- Tempo massimo di esecuzione di interventi di aggiornamento collettivo la cui pianificazione è stata concordata con ICP:

  100 % nei tempi pianificati

- Esito positivo delle verifiche ispettive.

Servizio di manutenzione hardware

Il servizio di manutenzione contribuirà al soddisfacimento dei livelli di servizio indicati per gli altri servizi.

- Esito positivo delle verifiche ispettive.

Servizio di Configuration Management

- Esito positivo delle verifiche ispettive.

Servizio di gestione della sicurezza, lato PdL

- Esito positivo delle verifiche ispettive.

4.18.3 Verifiche ispettive

Nella fase di esecuzione del servizio, ICP eseguirà periodicamente e/o in specifiche occasioni un'attività di verifica ispettiva. ICP prevede di attivare una Commissione di valutazione, di norma costituita da personale ICP e da esperti esterni di terza parte. La verifica valuterà la corretta esecuzione del servizio raccogliendo tutte le necessarie evidenze dall'operatività e dalle informazioni gestite.

La verifica produrrà un rapporto nel quale potranno essere evidenziate:

- Carenze minori,
- Non conformità,

che saranno notificate al Fornitore.

Si intende per non conformità un comportamento o uno stato del sistema di informazioni gestito che potrebbe, se non corretto, compromettere in maniera sostanziale l'efficacia e l'efficienza dei servizi forniti.

Possibili esempi di non conformità sono:

- L'evidenza che le procedure definite per la gestione delle PdL non sono state applicate;

- La presenza di un disallineamento significativo nel CMDB rispetto allo stato di fatto delle PdL installate;
- La ripetuta non corretta registrazione dei ticket rispetto alle evidenze raccolte presso gli utenti del servizio (come ad esempio la chiusura di ticket anche se il problema non è stato risolto e quindi la ripetuta apertura di ticket a fronte dello stesso problema);
- La ripetuta dichiarazione di "non riparabilità" di apparati, ove risulti che gli apparati stessi potevano essere riparati con sostituzione di componenti il cui valore era significativamente minore rispetto al valore dell'apparato.

La visita ispettiva avrà esito positivo se:

- Il Fornitore risolverà tutte le non conformità entro 10 giorni lavorativi o ripristinando le condizioni di conformità o ponendo in atto azioni che impediscano il ripetersi della non conformità. Al termine di questo periodo sarà eseguita un'ulteriore verifica che produrrà un rapporto sullo stato di risoluzione dei problemi evidenziati.
- Il Fornitore risolverà tutte le carenze minori entro la successiva visita ispettiva.

Altrimenti la visita ispettiva avrà esito negativo.

La presenza della stessa non conformità in due successive visite ispettive determinerà l'esito negativo, anche nel caso in cui il Fornitore risolva la non conformità entro 10 giorni lavorativi.

4.18.4 Strumenti di misura dei livelli di servizio minimi richiesti

Il Fornitore metterà a disposizione uno strumento software per la raccolta dei dati, il calcolo dei livelli di servizio (modello di valutazione della continuità di servizio e SLA) e la generazione del report mensile relativo.

Lo strumento dovrà garantire la tracciabilità dei dati (provenienti dal ticketing system) in modo che i livelli di servizio calcolati siano chiaramente riconducibili ai singoli dati che li hanno originati.

Lo strumento dovrà coprire anche la misura dei livelli di servizio riguardanti l'infrastruttura server e l'infrastruttura di rete della sala server.

Lo strumento dovrà essere integrato con gli strumenti software di gestione ticket e di monitoraggio.

4.18.5 Report periodico per la misura dei livelli di servizio minimi richiesti

Il Fornitore consegnarà mensilmente a ICP il report sulla base del quale sarà possibile verificare la corrispondenza del servizio con il livello di servizio minimo richiesto (modello di valutazione della continuità del servizio) e gli SLA attesi.

Il report dovrà essere comprensivo sia delle attività del lotto 1 che del lotto 2.

4.19 Penali

Per ogni giorno solare di ritardo relativo al termine della fase di trasferimento (vedi paragrafo "Modalità di esecuzione della fornitura") è applicata una penale di:

1.500 (Millecinquecento) euro.

Per quanto riguarda la valutazione del livello di servizio, la tolleranza è data dal livello di servizio pari al 99,96%, così come calcolato in base alla formula sopra descritta.

Per ogni 0,1% o frazione di scostamento da tale valore per il periodo di osservazione (mensile), è applicata una penale pari allo 0,3% del canone mensile.

Per quanto riguarda il rispetto degli SLA e l'esecuzione delle verifiche ispettive, si riportano di seguito le penali che saranno applicate al Fornitore, distinte per le varie tipologie di servizi.

Servizio di Assistenza.

Superamento dello SLA relativo alla percentuale di chiamate gestite entro 30 secondi in un periodo di un mese di calendario:

10.000 (Diecimila) euro

Esito negativo di una visita ispettiva:

10.000 (Diecimila) euro

Servizio di Gestione delle Postazioni di Lavoro (PdL).

Superamento dello SLA relativo al tempo massimo di soluzione di un ticket per tre volte in un mese di calendario:

10.000 (Diecimila) euro

Mancato rispetto della pianificazione delle attività di esecuzione di interventi di manutenzione/sostituzione programmata o delle attività pianificate per trasloco:

10.000 (Diecimila) euro

Esito negativo di una visita ispettiva:

10.000 (Diecimila) euro

Servizio di Gestione della rete Aziendale.

Esito negativo di una visita ispettiva:

10.000 (Diecimila) euro

Servizio di gestione del Software di base, d'ambiente e di rete.

Superamento dello SLA relativo al tempo massimo di soluzione di un ticket per tre volte in un mese di calendario:

10.000 (Diecimila) euro

Mancato rispetto della pianificazione degli interventi di aggiornamento collettivo la cui pianificazione è stata concordata con ICP:

10.000 (Diecimila) euro

Esito negativo di una visita ispettiva:

10.000 (Diecimila) euro

Servizio di manutenzione hardware.

Esito negativo di una visita ispettiva:

10.000 (Diecimila) euro

Nel caso di perdite di dati causate da negligenza del fornitore, ICP potrà rivalersi nei confronti del Fornitore per i danni subiti.

Servizio di Configuration Management.

Esito negativo di una visita ispettiva:

10.000 (Diecimila) euro

Servizio di gestione della sicurezza.

Esito negativo di una visita ispettiva:

10.000 (Diecimila) euro

Nel caso di danni derivanti da problemi di sicurezza causati da negligenza del fornitore, ICP potrà rivalersi nei confronti del Fornitore per i danni subiti.

ICP potrà condurre una visita ispettiva relativa ad uno o più servizi. Nel caso in cui una singola visita ispettiva generi un esito negativo relativo a più servizi, la penale sarà applicata una sola volta.

ICP si riserva il diritto di dichiarare non compatibile il servizio e di procedere alla risoluzione del contratto dopo l'applicazione di 3 (tre) penalità derivanti dal mancato rispetto degli SLA o da esito negativo delle visite ispettive.

4.20 Struttura organizzativa

Sono di seguito definite la struttura organizzativa, i ruoli e le responsabilità del personale del Fornitore e le modalità di interazione con ICP.

4.20.1 Struttura e responsabilità

Il servizio sarà fornito attraverso un gruppo di lavoro che opererà durante l'orario di copertura del servizio.

Il gruppo di lavoro sarà costituito da personale di competenza adeguata alla fornitura dei vari servizi.

Il gruppo di lavoro sarà coordinato e dipenderà da un Responsabile Operativo nominato dal Fornitore.

Il Responsabile Operativo farà parte del gruppo di lavoro del Fornitore ed opererà durante l'orario di copertura del servizio.

ICP nominerà un Responsabile ICP che opererà come unico referente ICP del Responsabile Operativo. Il Responsabile Operativo del Fornitore costituirà l'unico referente del gruppo di lavoro nei confronti del Responsabile ICP.

Relativamente ad attività di verifica degli SLA contrattuali ed in generale della qualità e del buon andamento dei servizi, ICP potrà avvalersi di terze parti che opereranno per conto di ICP.

Il Fornitore nominerà un Responsabile di contratto che opererà come referente degli aspetti contrattuali complessivi (valutazione complessiva dell'esecuzione del contratto, aspetti amministrativi e legali) nei confronti del corrispondente Responsabile di contratto ICP o suo delegato.

4.20.2 Dimensione e caratteristiche del gruppo di lavoro

Il gruppo di lavoro sarà costituito da un insieme di figure professionali adeguate a coprire i vari ruoli necessari per svolgere i servizi inclusi nel contratto.

Sarà cura del Concorrente offrire il dimensionamento del gruppo di lavoro e descrivere i ruoli coperti.

Per ogni partecipante al gruppo di lavoro il Concorrente dovrà indicare il profilo professionale e presentare il curriculum corrispondente.

Certificazioni attinenti ai servizi che costituiscono il contratto, relativi sia all'azienda concorrente che al personale proposto, saranno considerati durante la valutazione.

4.20.3 Sostituzione del personale

E' responsabilità del Fornitore sostituire il personale assente dal servizio per qualsivoglia motivo (ad esempio per malattia) con personale di equivalente profilo professionale.

ICP si riserva, a suo insindacabile giudizio e senza giustificazione, di richiedere per scritto ed ottenere la sostituzione di personale del gruppo di lavoro (incluso il Responsabile Operativo) con personale equivalente per ruolo, profilo professionale e curriculum.

4.21 Modalità di esecuzione della fornitura

L'esecuzione della fornitura si svilupperà attraverso le seguenti fasi:

- Fase di trasferimento.

  Durata: 20 gg lavorativi decorrenti dalla scadenza del termine dilatorio previsto all'art. 11 comma 10 del D. Lgs. 163/2006 e ss.mm.ii. (pari a 35 giorni solari dall'invio dell'ultima delle comunicazioni del provvedimento di aggiudicazione definitiva);

- Fase di avvio.

  Durata: 40 gg lavorativi dal termine della fase di trasferimento.

- Fase di esercizio.

  Durata: dal termine della fase di avvio al termine del periodo contrattuale.

- Fase di transizione finale.

  Durata: gli ultimi 60 gg lavorativi prima della scadenza del periodo contrattuale o comunque del termine del rapporto contrattuale (qualunque ne sia la causa).

4.21.1 Fase di trasferimento

La fase di trasferimento include tutte le attività svolte dal Fornitore al fine di prendere carico dei servizi affiancando il personale ICP e gli attuali fornitori.

ICP provvederà, durante tale fase, ad affiancare il personale tecnico del Fornitore, con l'obiettivo di una progressiva autonomia operativa da parte del Fornitore.

In questa fase il fornitore provvederà ad installare e rendere operativo il sistema di gestione (vedi capitolo "Strumenti di gestione") presso la sala server ICP.

4.21.2 Fase di avvio

Al termine della fase di trasferimento il gruppo di lavoro del Fornitore sarà in grado di prendersi carico dei servizi ed il Fornitore assumerà piena ed esclusiva responsabilità della gestione dei servizi.

Il Fornitore, per il solo fatto di partecipare alla presente gara, si obbliga ad accettare di garantire il servizio per tutte le componenti dell'infrastruttura ICT, così come identificate nelle loro caratteristiche essenziali (ma non esaustive) negli Allegati per tutta la durata contrattuale, nello stato in cui si trovano all'atto dell'affidamento del servizio, senza opporre alcuna riserva in merito allo stato degli impianti, degli apparati, dei sistemi e dei terminali, sulle versioni hardware e/o software, sui modelli e/o versioni degli stessi, nonché sul livello di aggiornamento della documentazione associata.

Il Fornitore è consapevole che quanto specificato nel presente documento (inclusi gli Allegati) identifica il dimensionamento dell'infrastruttura e non il dettaglio dello stato di fatto.

Con la presa in consegna degli impianti, il Fornitore assume le responsabilità previste dalle vigenti normative e dal presente Contratto ed è responsabile della buona e diligente conservazione del materiale ricevuto, rispondendo nei confronti dell'Amministrazione e di terzi per l'eventuale incuria o negligenza sulla gestione e conduzione degli impianti, nell'uso della documentazione e delle modalità di accesso fisico e logico agli apparati.

Nella fase di avvio, successiva alla fase di trasferimento, il Fornitore fornirà i servizi previsti contrattualmente in accordo con il livello di servizio minimo richiesto (modello di valutazione della continuità del servizio) e gli SLA definiti che saranno misurati / valutati.

Il Fornitore eseguirà tutte le operazioni di censimento ed il caricamento del CMDB.

Il Fornitore concorderà con ICP l'insieme delle procedure operative che dovranno descrivere le modalità di esecuzione dei servizi e le regole connesse (ad esempio le procedure di incident management, change management, security management). L'insieme di tali procedure sarà utilizzato come riferimento operativo durante l'erogazione dei servizi e riferimento di controllo durante le verifiche ispettive.

Il fornitore scriverà le procedure concordate che saranno sottoposte ad approvazione da parte di ICP.

Il fornitore metterà in esercizio tutte le procedure operative.

In questa fase le visite ispettive non valuteranno gli aspetti relativi al caricamento del CMDB ed alle procedure operative.

4.21.3 Fase di esercizio

Il Fornitore opererà sulla base del livello di servizio minimo richiesto (modello di valutazione della continuità del servizio) e degli SLA definiti che saranno misurati / valutati.

Le visite ispettive valuteranno tutti gli aspetti.

4.21.4 Fase di transizione finale

In questa fase il Fornitore si impegna, oltre che a fornire il servizio contrattualmente dovuto, ad affiancare ICP o un nuovo Fornitore indicato da ICP, che subentrerà nella gestione, trasferendo tutta l'informazione e le procedure di gestione in essere in modo da permettere un ordinato ed efficiente passaggio di consegne.

Alla scadenza del contratto, ICP ed il Fornitore procederanno alla visita degli impianti per accertare la buona conservazione degli stessi, nonché per accertare l'adempimento da parte del Fornitore degli obblighi contrattuali.

Qualora il Fornitore non dovesse intervenire alle operazioni di riconsegna entro dieci giorni dalla data di comunicazione dell'inizio delle operazioni di riconsegna, si procederà comunque alle operazioni alla presenza di un testimone.

Le operazioni di verifica saranno avviate almeno 30 (trenta) giorni prima del termine fissato per l'ultimazione del servizio e saranno ultimate entro la data di scadenza dello stesso.

Il Fornitore si renderà disponibile ad intervenire su richiesta per piccoli interventi per un periodo di ulteriori 2 (due) mesi dopo la scadenza del contratto.

Il Fornitore cederà in proprietà ad ICP tutte le parti di ricambio installate nel corso del periodo contrattuale.

4.22 Accreditamento SISS

Ai fini dell'ammissione alla procedura di gara, il concorrente deve essere accreditato SISS.

Qualora il soggetto concorrente non fosse accretitato SISS, potrà soddisfare detto requisito di ammissione con le modalità espressamente specificate nel Disciplinare di gara (paragrafo *B "termini e modalità di presentazione dell'offerta)*, ossia:

- mediante ricorso all'istituto dell'**Avvalimento** di cui all'art. 49 del D.Lgs. 163/2006 e ss.mm.ii. (in tal caso dovrà essere fornita in sede di gara tutta la documentazione elencata nel par. C "Avvalimento" del Disciplinare di gara), fatta salva la facoltà di conclusione anticipata del contratto di avvalimento, nel caso di ottenimento - da parte della società concorrente - dell'accreditamento SISS entro tre mesi dall'apertura della procedura di accreditamento;

- mediante ricorso all'istituto del **Subappalto** nel rispetto dei limiti e disposizioni contenute all'art. 118 del D. Lgs. 163/2006 e ss.mm.ii., fatta salva la facoltà di conclusione anticipata del contratto di subappalto, nel caso di ottenimento - da parte della società concorrente - dell'accreditamento SISS entro tre mesi dall'apertura della procedura di accreditamento.

5 Lotto 2: Progettazione, fornitura e gestione dei server

5.1 Servizi Richiesti

Il lotto include i seguenti servizi:

1. **Progettazione e fornitura dell'infrastruttura server inclusa l'infrastruttura di rete della sala server.**
2. **Gestione dei server:**
    - **Servizio di gestione dei Server:** gestione complessiva dei server inclusa l'infrastruttura di rete della sala server.
    - **Servizio di gestione del software di base, di ambiente e di rete:** gestione complessiva dei componenti software di base e di infrastruttura sui quali si basa la fornitura di servizi applicativi.
    - **Servizio di Manutenzione hardware:** riparazione / sostituzione di apparecchiature a seguito di guasti che perturbano l'operatività del sistema messo a disposizione
    - **Servizio di Gestione del Backup:** organizzazione e realizzazione di un servizio di backup del software e dei dati che garantisca la continuità del servizio a fronte di malfunzionamenti ed eventi eccezionali.
    - **Servizio di gestione della sicurezza:** Il Fornitore dovrà adeguarsi alle direttive in materia di sicurezza adottate da ICP, garantendo allo stesso tempo un adeguato supporto in caso di incidenti e nella risoluzione di eventuali problemi di sicurezza informatica.
    - **Servizio di gestione della posta elettronica:** gestione dell'operatività necessaria a garantire agli utenti il servizio di posta elettronica.
    - **Servizio di Configuration Management:** gestione degli asset relativi ai sistemi server e di tutti i cambiamenti attraverso un Configuration Management Data Base.
    - **Formazione in affiancamento:** Il Fornitore dovrà garantire un opportuno trasferimento di conoscenze sistemistiche/informatiche al fine di garantire una corretta gestione delle risorse.

5.2 Durata del contratto

La durata del contratto è di 5 (cinque) anni a decorrere dalla data che sarà indicata nella comunicazione di aggiudicazione definitiva, con facoltà di recesso per l'A.O. ICP dopo 3 (tre) anni.
Sarà facoltà dell'Azienda Appaltante prorogare il rapporto contrattuale – dopo la naturale scadenza dello stesso – per ulteriori **6** mesi o per il periodo strettamente necessario per l'espletamento delle procedure concorsuali di individuazione del nuovo aggiudicatario – alle

medesime condizioni contrattuali in essere – senza che l'Appaltatore possa pretendere compensi ulteriori. L'aggiudicatario si obbliga, pertanto, a proseguire la fornitura del servizio dietro semplice richiesta scritta dell'A.O. con un preavviso di 30 giorni rispetto la scadenza naturale del contratto.

5.3 Modalità organizzative e luogo di fornitura del servizio

Il servizio sarà fornito presso la sede dell'Ospedale Bassini a Cinisello Balsamo di seguito denominata "Sala server", attraverso la presenza di un gruppo di lavoro del Fornitore che opererà durante l'orario di copertura del servizio di seguito definito.

ICP metterà a disposizione i locali come meglio precisato al capitolo " Sala server".

Il servizio di reperibilità di seguito definito dovrà essere fornito, durante gli orari che eccedono l'orario di copertura del servizio definito in "Orari di copertura dei servizi" attraverso personale, mezzi e strumenti totalmente a carico del Fornitore.

Il gruppo di lavoro che opererà presso la sala server dipenderà da un Responsabile Operativo nominato dal Fornitore.

Il Responsabile Operativo, di competenza adeguata al ruolo di coordinatore e referente tecnico / organizzativo, opererà presso la sala server come interfaccia tra il Responsabile ICP ed il gruppo di lavoro.

Tutto il personale del Fornitore che opererà presso ICP (gruppo di lavoro e Responsabile Operativo) sarà soggetto a registrazione delle presenze.

Il Fornitore è tenuto ad intervenire presso tutte le sedi indicate da ICP ove sono presenti infrastrutture server.

Eventuali future variazioni (aperture o chiusure di sedi) saranno comunicate tempestivamente al Fornitore; tali variazioni non daranno luogo di per sè ad alcun incremento dei compensi dovuti, in ogni scenario in cui non avvenga una rilevante variazione dell'organizzazione complessiva di ICP (incremento o trasferimento di più del 20 (venti)% delle attuali sedi).

E' da considerare obbligazione contrattuale tassativa la presenza del gruppo di lavoro (compreso il Responsabile Operativo) presso la sala server.

5.4 Caratteristiche del personale

Il personale del gruppo di lavoro ed il responsabile operativo dovranno possedere competenze tali da coprire la fornitura dei servizi di seguito elencati sulla base dei sistemi e delle tecnologie hardware e software presenti.

Il personale dovrà essere indicato nominativamente.

La competenza del personale dovrà essere certificata e sarà valutata sulla base di certificazioni professionali di mercato specificatamente relative ai sistemi gestiti ed in particolare almeno a: sistemi server Microsoft, Linux, Oracle, apparati di rete e protezione della sicurezza forniti e ambiente di virtualizzazione fornito. Il curriculum professionale sarà ulteriore elemento di valutazione.

Sarà oggetto di valutazione il profilo complessivo di competenze certificate fornito e la sua distribuzione nel personale. Il proponente dovrà presentare in fase di offerta uno schema da cui emerga con chiarezza la matrice che descrive il numero di persone fornite per ogni competenza certificata.

Ove il personale impiegato sostituisca il personale indicato nominativamente, la sostituzione dovrà essere effettuata a parità di schema (numerosità di persone per ogni competenza certificata).

ICP si riserva di richiedere i documenti di certificazione.

Si precisa che la lingua abituale di lavoro per questo servizio dovrà essere l'italiano.

ICP potrà rifiutare per scritto, a suo insindacabile giudizio e senza ulteriore giustificazione, ogni sostituzione che non rispetti il criterio sopra detto.

5.5 Orari di copertura dei servizi

Il servizio dovrà essere disponibile durante gli orari di seguito elencati (orario di lavoro amministrativo):

- Dalle 7.30 alle 19.00, dal Lunedì al Venerdì

Il Responsabile Operativo opererà coprendo l'orario:

- Dalle 8.00 alle 17.00, dal Lunedì al Venerdì

Ogni attività contrattuale ordinaria e straordinaria (purchè non comprometta i livelli di servizio richiesti), ad eccezione delle attività connesse al servizio di reperibilià, dovrà essere in generale svolta all'interno dei periodi indicati, a meno del verificarsi di condizioni particolari e in ogni caso a seguito di autorizzazione scritta del Responsabile ICP.

Il Fornitore dovrà essere disponibile a fornire, su richiesta specifica di ICP, per attività che compromettono i livelli di servizio e richiedono interventi fuori dall'orario precedente, incluso i sabati, festivi e orari notturni di qualunque giorno della settimana, periodi determinati e preventivamente pianificati, per un ammontare globale massimo di 220*8 ore in 5 anni in lotti minimi di ore quattro.

Per richieste che superino tale ammontare massimo di giornate, il fornitore dovrà indicare il costo di un tecnico per ogni ulteriore giornata di assistenza di h8.

Sono esclusi dall'ammontare globale:

- Ogni attività (compresa o non compresa nell'orario di lavoro) derivante da interventi richiesti al fine di adempiere alla fornitura dei servizi previsti contrattualmente rispettando gli SLA contrattuali;
- Ogni attività derivante dal servizio di reperibilità;
- Ogni attività richiesta durante le fasi precedenti alla fase di esercizio.

5.6 Servizio di reperibilità

Il fornitore renderà disponibile un servizio di reperibilità H24*7 che potrà essere attivato da:

- Sistema di monitoraggio automatico dei sistemi server e dei servizi applicativi installati sui sistemi server;
- Servizio di Help Desk fornito da ICP (lotto 1 del presente capitolato).

Durante gli orari che eccedono l'orario di copertura del servizio definito in "Orari di copertura dei servizi", il servizio gestirà:

- I guasti bloccanti (su tutti i sistemi oggetto del servizio) relativi alla sala server;
- I guasti bloccanti (su tutti i sistemi oggetto del servizio) relativi ai servizi ICP aperti in orario esteso;

I guasti saranno risolti direttamente da remoto o attivando il proprio personale reperibile del servizio di help desk di 2° Livello.

ICP comunicherà al Fornitore, in fase di avvio del contratto, l'elenco dei servizi aperti in orario esteso.

5.7 Livelli di Servizio e misura della qualità del servizio

Il Fornitore si impegna a garantire i livelli di servizio contrattuali che dovranno essere corrispondenti o migliorativi rispetto ai livelli minimi di seguito specificati per ogni servizio.

Il Fornitore registrerà e documenterà nel sistema informatico di monitoraggio dell'esecuzione del contratto ciascun evento accaduto durante l'intero iter di gestione degli incidenti, dei problemi o degli interventi, al fine non solo di gestire accuratamente il servizio, ma anche di permettere a ICP di valutare la qualità del servizio prestato.

A tal fine ogni evento o richiesta (ad esempio evento di malfunzionamento di un server o di un componente di infrastruttura di rete, richiesta di installazione/configurazione di un componente hardware o software) dovrà comportare l'apertura di un ticket nel ticketing system di seguito descritto e l'esecuzione del conseguente processo di tracciatura fino alla chiusura del ticket.

Il Fornitore è tenuto ad informare il Responsabile ICP:

- Nel caso occorrano situazioni o eventi, di natura tecnica ovvero organizzativa, non gestibili in completa autonomia da parte del proprio personale, o per i quali siano necessarie autorizzazioni da parte di ICP prima di procedere.
- Quando eventi rilevanti, ben giustificati da motivi di natura tecnica o organizzativa, pregiudichino sostanzialmente il conseguimento dei Livelli di Servizio stabiliti; il responsabile tecnico di ICP provvederà a valutare le motivazioni addotte, e di volta in volta determinerà sia le azioni da prendere, che le ripercussioni in termini di reportistica – ed eventuali penali.

Tutte le procedure legate ai servizi oggetto di questa fornitura dovranno essere opportunamente documentate a cura del Fornitore e concordate con ICP ed eventuali terze parti qualora fossero coinvolte nel processo.

I livelli di servizio saranno oggetto di monitoraggio con rendicontazione sulla base di periodi specificati.

5.8 Variazioni del servizio

Tutti i servizi di seguito esplicitati dovranno essere forniti, senza oneri aggiuntivi e senza alcun vincolo, rispettando gli SLA contrattuali, relativamente alle configurazioni ed ai volumi che potranno risultare dalle evoluzioni che ICP deciderà, nel corso del periodo contrattuale, per il proprio Sistema Informativo (ad esempio modifiche ed incremento dei server e dell'infrastruttura di rete).

E' cura del Concorrente, sulla base della propria esperienza in analoghe situazioni, stimare il carico di lavoro connesso.

5.9 Variazioni di priorità nelle attività di fornitura dei servizi

Sulla base di specifiche esigenze, il responsabile dell'unità Sistemi Informativi di ICP potrà richiedere al Fornitore di gestire con priorità maggiore specifiche attività all'interno dell' elenco delle attività aperte (corrispondenti a ticket aperti) ed il Fornitore dovrà ottemperare alla richiesta.

5.10 Sala server

ICP metterà a disposizione i locali allestiti della sala server. La planimetria dei locali è fornita in Allegato D.

La sala server includerà:

- Locale sala server e locali per ufficio;
- Installazione nella sala server di pavimento flottante di portata elevata;
- Arredamento;
- Climatizzazione ridondata della sala server e climatizzazione dell'ufficio;
- Sistemi per il controllo degli accessi;
- Alimentazione elettrica primaria ridondata a partire dall'alimentazione primaria disponibile;
- UPS ridondato;
- Distribuzione secondaria dell'alimentazione elettrica;
- Accesso ridondato alla rete dati a partire dalla rete di comunicazione dati ICP.

Sarà a carico di ICP gestione e la manutenzione di tutte le attrezzature per la durata contrattuale.

5.11 Progettazione e fornitura dell'infrastruttura server inclusa l'infrastruttura di rete della sala server.

Il Concorrente dovrà proporre un progetto di infrastruttura server e infrastruttura di rete della sala server sulla base dei seguenti elementi:

- La configurazione attuale descritta in Allegato B;
- I requisiti di seguito elencati per la nuova configurazione della sala server.

Sulla base degli elementi sopra identificati, la nuova infrastruttura dovrà far fronte alle stime di crescita per tutta durata contrattuale.

In fase di offerta, il proponente dimensionerà i sistemi offerti e le possibili espansioni che potrà fornire nell'arco del contratto, su richiesta di ICP e senza oneri aggiuntivi, per far fronte alla crescita delle esigenze computazionali e di memoria dei sistemi ICP al di fuori di eventi d'inserimento di significative nuove applicazioni.

Il fornitore svilupperà la proposta sulla base di una propria valutazione fondata sui requisiti di seguito elencati e la propria esperienza professionale.

Il dimensionamento offerto sarà oggetto di valutazione.

Il Fornitore:

- Installerà e renderà operativa l'infrastruttura presso la sala server ICP;
- Sarà responsabile della pianificazione e del coordinamento di tutte le attività necessarie per il trasferimento delle applicazioni software e delle basi di dati in esercizio dall'infrastruttura attuale alla nuova infrastruttura;
- Concorderà con ICP e successivamente metterà in atto il passaggio tra l'esercizio della vecchia infrastruttura e la nuova, in modo che l'utenza ICP non abbia interruzioni di servizio.

Saranno a carico del fornitore i contratti di manutenzione adeguati al rispetto degli SLA contrattuali, per tutte le infrastrutture fornite e per la durata contrattuale.

La responsabilità globale di gestione dei contratti di manutenzione sarà in capo al fornitore senza alcun coinvolgimento di ICP.

ICP potrà, durante la durata del contratto, installare nuovi sistemi nell'infrastruttura della sala server. ICP metterà a disposizione del fornitore i contratti di manutenzione dei nuovi sistemi con caratteristiche adeguate rispetto agli SLA contrattuali.

I nuovi sistemi dovranno essere gestiti dal Fornitore con gli stessi criteri di responsabilità globale sopra esposti ed in accordo con il capitolo "Variazioni del servizio".

5.11.1 Requisiti

L'infrastruttura dovrà al minimo mettere a disposizione risorse di calcolo e memoria equivalenti a quelle ora in produzione.

La sala server dovrà essere dotata delle seguenti infrastrutture minime:

- Firewall e infrastruttura di accesso Internet, VPN;
- Infrastruttura di rete locale;
- SAN Storage;
- Infrastruttura di Backup;
- Infrastruttura di virtualizzazione

L'infrastruttura di sala server proposta non deve richiedere a ICP un incremento di costi o una riduzione di prestazioni relativamente ai contratti in essere di manutenzione di software applicativo .

Attualmente la memoria di massa utilizzata per la memorizzazione di dati è pari a 5 Tbytes (Sistema PACS e vari file server esclusi) e sulla base dell'evoluzione dei precedenti 3 anni, si stima che possa cresce almeno di 1,5 Tbyte. all'anno nei prossimi 5 anni.

5.12 Accesso e proprietà delle infrastrutture della sala server

Il personale ICP potrà in qualunque momento accedere alla sala server ed avrà visibilità completa di ogni attività svolta.

Le infrastrutture fornite, comprendendo sia l'infrastruttura server che di rete, resteranno di proprietà del fornitore durante la durata del contratto. Allo scadere del contratto il fornitore cederà a ICP la proprietà delle infrastrutture senza oneri aggiuntivi.

Tutti gli elementi delle infrastrutture fornite, compresi quelli aggiunti negli anni dal fornitore, saranno inventariati da ICP, all'installazione, come beni in comodato d'uso.

Nel caso ICP eserciti la facoltà di recesso dopo i tre anni, le infrastrutture fornite diventeranno di proprietà ICP e ICP riconoscerà al fornitore un ammontare pari al 12 (dodici) % dell'importo totale del contratto.

Nel caso ICP dichiari non compatibile il servizio e proceda alla risoluzione anticipata del contratto, le infrastrutture fornite diventeranno di proprietà ICP e ICP riconoscerà al fornitore un ammontare calcolato sulla base della seguente formula:

$$\text{ImportoRiconosciuto} = \frac{30/100 * \text{ImportoTotaleContratto} * \text{NumMesiNonForniti}}{\text{NumMesiTotaliContratto}}$$

5.13 Servizio di gestione dei Server

Il Servizio di Gestione dei Server include tutte quelle attività necessarie per prendere in carico, condurre e mantenere sempre efficiente l'infrastruttura server utilizzata per l'erogazione dei servizi informatici di ICP.

L'infrastruttura include:

- I sistemi server hardware e software e gli apparati ad essi connessi (es. Storage, library,…) della sala server;
- L'infrastruttura di rete della sala server (firewall e apparati di rete);
- Le infrastrutture server ICP presenti presso le sedi ICP al di fuori della sala server (Allegato E).

La configurazione dell'infrastruttura server e dell'infrastruttura di rete della sala server saranno il risultato della progettazione e fornitura, parte del presente Lotto 2 di appalto.

L'attuale configurazione delle infrastrutture server ICP presenti presso le sedi ICP al di fuori della sala server è definita in Allegato E.

In allegato E sono indicati anche alcuni server ora presenti presso le sedi ICP al di fuori della sala server, che presumibilmente saranno inclusi nella nuova sala server come server virtualizzati.

L'allegato E è da considerare, dal punto di vista contrattuale, indicativo della complessità dell'infrastruttura ma non esaustivo.

ICP potrà installare nella sala server dei server fisicamente distinti che il fornitore connetterà alla rete, ma che saranno gestiti direttamente da ICP o da fornitori nominati da ICP.

Il servizio dovrà essere fornito, senza oneri aggiuntivi e senza alcun vincolo, rispettando gli SLA contrattuali, relativamente alle configurazioni ed ai volumi che potranno risultare dalle evoluzioni che ICP deciderà, nel corso del periodo contrattuale, per il proprio Sistema Informativo (ad esempio modifiche ed incremento dei server).

In tale contesto si definisce "Sistema" o "Server" l'insieme di più componenti hardware e software (Sistema Operativo e componenti software come ad esempio Oracle o MS Exchange), assimilabili ad una unità elaborativa autonoma a supporto dello sviluppo, del test e dell'esercizio di uno o più servizi.

In tale contesto anche l'infrastruttura di rete della sala server è considerata come un "Sistema".

Il servizio coprirà l'intero ciclo di vita dei Sistemi, ed includerà quindi, tra gli altri:

1. Conduzione operativa dei Sistemi e misurazione delle prestazioni;
2. Change management locale o remoto (gestione ed esecuzione di modifiche riguardanti software di base, d'ambiente e di rete) con l'esclusione del software applicativo;
3. IMAC (movimentazione, aggiunta e cambiamento di componenti HW e periferiche);
4. Asset Management (gestione e controllo delle configurazioni installate);
5. Gestione degli incidenti, assistenza tecnica e manutenzione Hardware e Software;
6. Rendicontazione.

Il fornitore s'impegna a garantire il corretto funzionamento e la disponibilità richiesta dei servizi di elaborazione centrale, tramite adeguati servizi di assistenza sistemistica sui diversi ambiti che impattano l'operatività dei sistemi.

Il Fornitore dovrà garantire il rispetto dei livelli di servizio indicati al paragrafo relativo.

5.13.1 Requisiti

5.13.1.1 Censimento iniziale

Il Fornitore dovrà rilevare, mediante opportuna attività di censimento iniziale, tutto il parco server (di ogni genere e tipo) a disposizione di ICP, alimentando il CMDB.

5.13.1.2 Conduzione operativa dei server

La gestione operativa dei Server consiste nel presidio e controllo continuativo dei sistemi al fine di garantirne il funzionamento secondo quanto previsto nei livelli di servizio, ed include il supporto nella risoluzione di eventuali problemi operativi, con attività tra cui:

• Installazione/sostituzione dei componenti hardware, software e firmware, assicurandone il corretto funzionamento;

• Interazione con il servizio di manutenzione hardware;

• Personalizzazione ed aggiornamento della configurazione dei server quando opportuno mediante manutenzione ordinaria e straordinaria programmata, installando le modifiche e gli aggiornamenti necessari o richiesti, e mantenendoli allineati con gli aggiornamenti di sicurezza consigliati dai Costruttori;

• Definizione e realizzazione delle modifiche all'architettura delle risorse hardware e software e le personalizzazioni necessarie all'integrazione di altri prodotti software e per l'esercizio delle applicazioni;

• Installazione, personalizzazione, distribuzione, manutenzione e test del sistema operativo, dei sottosistemi e dei prodotti middleware (Web Server, Application Server, VMWare,ecc.);

• Definizione ed attuazione delle procedure di automazione operativa (accensione e spegnimento, produzione di stampe, start-up dei collegamenti, ecc.);

• Configurazione, erogazione e monitoraggio dei servizi secondo le modalità e regole indicate da ICP;

• Gestione dei carichi di lavoro in termini di caratterizzazione delle componenti ed assegnazione delle priorità;

• Pianificazione, esecuzione e controllo degli interventi di manutenzione sul software e sull'hardware (per esempio l'introduzione di patch);

• Implementazione di regole (policy) all'interno degli ambienti operativi ed applicativi atte a definire le modalità di erogazione dei Servizi.

In questa gestione rientrano anche tutte quelle attività di manutenzione e di controllo associate ai database aziendali. Tali attività sono tipicamente quelle di seguito elencate:

- Shutdown & Startup (schedulato e on demand);
- Backup & Restore (schedulato e on demand);
- Import & Export (schedulato e on demand);

- Attività di monitoraggio delle performances;
- Attività di ripristino in caso di errore;
- Attività per l'upgrade a nuove release;
- Gestione delle attività schedulate (pianificazione di job e lettura dei log di esecuzione).

5.13.1.3 Monitoraggio automatico dei sistemi e dei servizi applicativi

Il fornitore dovrà mettere in atto un sistema di monitoraggio anche automatico dei sistemi server ed anche dei servizi applicativi installati sui sistemi server (fisici e virtuali).

Il monitoraggio dovrà operare da remoto ed essere in grado di chiamare un servizio di reperibilità su urgenza del Fornitore con una disponibilità h24*7.

Il monitoraggio, a fronte di situazioni critiche dovrà essere in grado di avvisare (via sms, chiamata telefonica su cellulare e mail) il responsabile del Sistema Informativo ICP.

Il monitoraggio terrà sotto controllo:

- I principali parametri operativi dei sistemi server;
- La disponibilità delle risorse (ad esempio lo spazio disponibile per i DB e per il File System con diversi livelli di soglia);
- La disponibilità di istanze di DB;
- La funzionalità dei servizi applicativi sulla base di parametri (processi, informazioni di log,…) documentati dai fornitori del software applicativo;
- Anomalie hardware (come ad esempio warning/alert delle power unit, autonomia di funzionamento delle batterie cache, etc.);

Il monitoraggio innescherà l'emissione e la gestione di allarmi:

- Derivanti dalla rilevazione di anomalie;
- Derivanti dal superamento di soglie di indicatori rappresentativi del servizio (monitoraggio delle prestazioni).

5.13.1.4 Analisi del carico dei Sistemi e monitoraggio delle prestazioni

Sarà cura del Fornitore mantenere le prestazioni dei sistemi, controllando, misurando ed analizzando le prestazioni dei server (ad esempio in termini di occupazione di RAM, di occupazione di spazio disco a diverse soglie, di consumo di CPU, di swap su disco, etc.) e fornendo rapporti per la determinazione di eventuali interventi preventivi al fine di garantire i livelli di servizio.

Il Fornitore dovrà comunicare per tempo ai referenti ICP del servizio eventuali necessità di adeguamento/aggiornamento HW e/o SW dei Sistemi tali da consentire la corretta continuità dei Servizi erogati, come ad esempio in presenza di ampliamenti applicativi o di incremento delle utenze che potrebbero comportare anche adeguamenti hw.

5.13.1.5 Gestione degli incidenti, assistenza tecnica e manutenzione correttiva

Il Fornitore, a seguito della rilevazione di malfunzionamenti hardware o software o incidenti di sicurezza, dovrà operare per la risoluzione dell' incidente.

Le attività comprendono gli interventi su tutti i componenti hardware e software (di base e d'ambiente) dei sistemi e relativi accessori che per qualsivoglia ragione si dovessero guastare o presentare anomalie di funzionamento.

Più in dettaglio le attività possono riassumersi in:

- Risoluzione della causa del guasto tramite sostituzione di parti sulla base dello scambio e/o tarature elettroniche, meccaniche o software finalizzate al recupero delle prestazioni iniziali dell'apparecchiatura;
- Ripristino del servizio sui livelli preesistenti al guasto/anomalia;
- Collaudo del sistema in tutte le sue funzionalità per verificare l'avvenuta eliminazione della causa del guasto/anomalia;
- Ripristino della funzionalità del sistema attraverso sostituzione momentanea con un proprio apparato equivalente, in caso d'impossibilità a garantire la riparazione/manutenzione (ad esempio per indisponibilità delle parti di ricambio);
- Attivazione, se il caso, delle ditte fornitrici con le quali il fornitore ha in atto contratti di manutenzione.
- Attivazione, se il caso, e gestione delle ditte fornitrici con le quali il fornitore ha in essere clausole contrattuali di garanzia o d'intervento.
- Attivazione, se il caso, delle ditte fornitrici con le quali ICP ha in essere clausole contrattuali di garanzia o di intervento. Il Fornitore opera in collaborazione con le suddette ditte fornendo tutto il supporto necessario al fine di risolvere prontamente il problema.

La gestione degli incidenti è tracciata attraverso le modalità e lo strumento di trouble ticketing messo a disposizione dal servizio di Help Desk (Lotto 1).

5.13.1.6 Dominio e Domain Controllers

Compito del Fornitore sarà di gestire e mantenere sempre efficiente e disponibile il Dominio, ed in particolare gli elenchi degli account (Gruppi Utenti, Utenti, Gruppi Computer, Computer, Server, permessi utenti), provvedendo alla creazione, cancellazione e modifica degli stessi in base alle specifiche esigenze di ICP.

Dovrà inoltre provvedere alla gestione delle regole di policy già implementate o da implementare, tra cui le policy di sicurezza in accordo con le normative vigenti e i regolamenti aziendali.

Poiché il Dominio è di primaria importanza per il corretto funzionamento delle applicazioni di rete implementate, il Fornitore dovrà prevedere e implementare una procedura di rapido ripristino (Crash Recovery) del Dominio in caso di malfunzionamento dello stesso.

5.13.1.7 Gestione degli utenti

Il Fornitore sarà responsabile delle attività connesse alla gestione delle utenze definite sui server. In particolare il Fornitore dovrà occuparsi di attività inerenti all'abilitazione e disabilitazione degli utenti sull'Active Directory e nello specifico popolare l'Active Directory dei Domain Controller della rete di ICP con i dati di un nuovo utente, ovvero aggiornare quelli esistenti (nuova utenza di dominio, posta elettronica, internet, (elenco indicativo ma non esaustivo)).

ICP comunicherà al Fornitore tutte le informazioni necessarie per la gestione delle utenze di dominio, e la specifica di tutte le procedure che dovranno essere seguite nell'ambito della gestione utenti.

5.13.1.8 DHCP Server

Il servizio di DHCP è necessario alla configurazione in rete dei client della rete LAN. Il Fornitore condurrà una serie di interventi periodici atti a verificare e mantenere il servizio stesso, gestendo i seguenti aspetti:

- Disponibilità di indirizzi negli "scope" configurati, con eventuale configurazione di scope aggiuntivi e conseguente configurazione del routing verso le subnet aggiunte;
- Manutenzione (fix di eventuali problemi) del database dei "lease" degli indirizzi e conseguente backup dello stesso;
- Aggiunte di opzioni di scope o variazioni sugli scope esistenti (ad esempio aggiunta dell'indirizzo di un nuovo DNS server);
- Risoluzione di tutti gli eventuali problemi di "lease";
- Gestione del piano di indirizzamento privato, per gli indirizzi: dinamici e statici;
- Configurazione di eventuali "DHCP relay agent" su reti remote ICP (reti "ruotate"), in modo da mantenere un DHCP server centrale;
- Messa in opera di un'eventuale DHCP di emergenza in caso di malfunzionamento di quello principale, con importazione del database dei lease degli indirizzi dal server principale;

5.13.1.9 DNS Server

Il servizio DNS è utilizzato nella risoluzione dei nomi host, degli mx record, degli alias, ecc… dei domini e sottodomini ICP visibili su internet. Sarà cura del fornitore gestire le seguenti attività giornaliere, necessarie a far funzionare il servizio in piena operatività:

- Backup delle zone configurate sul DNS;
- Monitoraggio delle performance del server su cui è in funzione il servizio DNS;
- Monitoraggio dei log del servizio DNS (named);
- Verifica dei trasferimenti di zona necessari verso i server secondari definiti.

Inoltre dovranno essere compiute le seguenti operazioni in caso di necessità o esplicita richiesta da parte di ICP:

- Aggiornamento dei file di zona per aggiunta di nuovi host, alias, record;
- Aggiunta di un nuovo file di zona, per una zona definita (sottodominio o dominio);
- Verifiche dei tempi di aggiornamento delle modifiche sulle zone esistenti, con query e utilizzo di strumenti di verifica da internet (DIG server tool). Tali verifiche sono atte ad accertare la conseguente propagazione delle modifiche dal DNS di ICP verso i secondari e da qui verso i root-server DNS di internet;
- Variazioni al file di configurazione del servizio DNS (named), con conseguente backup dello stesso file;
- Aggiunta delle patch di sicurezza necessarie a “chiudere” eventuali falle sul servizio.

5.13.1.10 Servizio NAT

Il Servizio di Network Address Translation (NAT) ovvero traduzione degli indirizzi di rete, consiste nel modificare gli indirizzi IP dei pacchetti in transito sul sistema di firewalling di ICP.

Il Servizio è strutturato sia per modificare l'indirizzo sorgente (source NAT o SNAT) sia per modificare l'indirizzo destinazione (destination NAT o DNAT).

I pacchetti che viaggiano in senso opposto verranno modificati in modo corrispondente in modo da dare ad almeno uno dei due soggetti che stanno comunicando l'illusione di parlare con un indirizzo IP diverso da quello effettivamente utilizzato dalla controparte.

Il Fornitore dovrà:

- Fornire supporto per l’analisi del fabbisogno di questo servizio e per la definizione;
- Implementare il servizio ove richiesto, includendo anche verifica del funzionamento e monitoraggio.

5.13.1.11 Servizio FTP

Il servizio consente lo scambio di file dati, di qualsiasi formato, fra utenti ICP ed altri utenti esterni.

Il servizio è strutturato per soddisfare sia le esigenze di scambio sporadico di file fra utenti interni e utenti esterni non registrati (ftp anonymous), sia di scambio solo fra utenti registrati (interni ed esterni).

Le due modalità di accesso sono logicamente separate: i file di dati che dovranno essere visibili solo da utenti registrati non saranno accessibili da utenti anonimi e viceversa.

Gli utenti, compreso l’utente anonymus, hanno a disposizione uno spazio disco prefissato (quota).

In caso di necessità l’utente potrà richiedere un ampliamento della propria quota.

Il fornitore dovrà:

- Gestire le abilitazioni per l'accesso al servizio;
- Monitorare lo spazio disco utilizzato e in generale il funzionamento del servizio;

- Produrre le statistiche di traffico per gli scopi previsti.

5.13.1.12 File Servers

Il Fornitore, nel quadro delle attività di censimento iniziale, dovrà censire tutte le cartelle di rete condivise e le relative permission (utenti/gruppi abilitati e relativi ruoli) e mantenere costantemente aggiornato il Data Base le cui informazioni dovranno essere accessibili anche al personale autorizzato da ICP.

L'attività di gestione del File Sharing si sostanzierà nei seguenti punti:

- Inizializzare i dischi per l'attivazione nell'ambiente;
- Creare cartelle per servizio o unità operativa ed assegnare permessi per gruppi e per singolo utente;
- Controllare l'utilizzo dei dischi per assicurare la disponibilità di spazio, attraverso quote utente e monitorare il corretto utilizzo dei file server da parte degli utenti che non dovranno poter memorizzare file audio/video con copyright, software non licenziati, etc. e non dovranno poter eseguire file .exe (.mdb, etc.) direttamente sul file server.
- Riorganizzare gli archivi, per assicurare la massima efficienza;
- Eseguire il backup e ripristino dei dati con storicizzazione di almeno 30 giorni per il recupero di dati accidentalmente eliminati dagli utenti.

Saranno prodotti rapporti sull'utilizzo dello spazio, le prestazioni ed i trend di crescita di storage, per consentire valutazioni dettagliate inerenti l'immissione di nuovi servizi/applicazioni, e le eventuali necessità di espansione.

I dati sui dischi saranno classificati secondo le seguenti caratteristiche:

- Ambiente, inteso come sistema logico di appartenenza (sviluppo, collaudo, produzione ecc.);
- Categoria, (per es. dati di sistema, dati di prodotto, dati delle applicazioni ecc.);
- Tipo, identificabile all'interno di ogni categoria (per es. dati di sistema operativo, dati per la configurazione dell'application server, ecc.).

I criteri di gestione dello spazio sui dischi dipenderanno dall'insieme di appartenenza.

Tutti i dischi dei Sistemi dovranno essere sottoposti a backup centralizzato schedulato.

5.13.1.13 Print Servers

Il Fornitore dovrà gestire le code di stampa di tutte le stampanti di rete, mediante la configurazione delle stesse centralmente sui Print Server.

In particolare la gestione delle code di stampa comporterà la creazione (mediante l'installazione e la configurazione degli opportuni driver di periferica), la modifica, la cancellazione e le modalità di accesso delle stesse.

5.13.1.14 Server Applicativi

I server applicativi dovranno essere monitorati, ma il supporto alle applicazioni ed i relativi obiettivi di disponibilità sono di responsabilità di ICP o della relativa Terza Parte.

Per quanto riguarda i server che forniscono servizi applicativi non gestiti direttamente, il Fornitore provvederà:

- All'eventuale installazione, configurazione ed ottimizzazione del sistema operativo e del software d'ambiente (es. Application Server, Oracle Application, software di virtualizzazione);
- Alla configurazione dei parametri di sistema (partizioni, istanze, storage, RAM, CPU, etc.) per l'ambiente di test e di produzione degli applicativi;
- A supportare l'installazione degli applicativi e a definire di script di gestione (startup, shutdown, etc.) in collaborazione con il fornitore dell'applicativo;
- Alla connettività alla rete e ai servizi a valore aggiunto quali: il monitoraggio, la sicurezza (firewall), il backup centralizzato;
- Alla gestione delle code di stampa;
- Al supporto infrastrutturale, inclusa la consulenza sistemistica per l'ottimizzazione delle prestazioni;
- Alla gestione dei malfunzionamenti, a partire dal supporto Service Desk fino alla manutenzione tramite i contratti già in essere;
- A prevedere idonee misure di sicurezza per garantire l'integrità delle applicazioni in esercizio.

5.13.1.15 Web Server

Il Fornitore dovrà prendere in carico le attività di gestione sistemistica di tutti i servizi di pubblicazione su Internet, Extranet (aree riservate) ed Intranet, tra cui:

- Installazione ed ottimizzazione dei Web server (http server e web application server).
- Supporto tecnico specializzato per la creazione di nuovi domini e loro configurazione su Web server e DB.
- Gestione e monitoraggio sistemistico dei siti web aziendali.

5.13.1.16 Gestione sistemistica RDBMS

Il Fornitore dovrà gestire tutti gli aspetti di supporto sistemistico tra cui:

- Eventuale installazione, configurazione ed ottimizzazione del sistema operativo e del software d'ambiente (es. DB Server, software di virtualizzazione);
- Configurazione dei parametri di sistema (partizioni, istanze, storage, RAM, CPU, etc.) per l'ambiente di test e di produzione dei DB Server;
- Realizzazione della connettività alla rete ed erogazione di servizi a valore aggiunto quali: il monitoraggio, il backup centralizzato;

- Supporto infrastrutturale, inclusa la consulenza sistemistica per l'ottimizzazione dei sistemi software RDBMS installati (Oracle e SQLServer).
- Gestione dei malfunzionamenti, dal supporto Service Desk fino alla manutenzione tramite i contratti già in essere;
- Realizzazione di idonee misure di sicurezza per garantire l'integrità dei dati in esercizio.

5.13.1.17 Gestione dell'Asset

Il fornitore dovrà garantire l'Asset Management di tutti i sistemi oggetto del servizio.

I dati d'inventario dovranno essere memorizzati come per le PdL ed ogni altra apparecchiatura nell'apposito data base di Configuration Management (CMDB) messo a disposizione dal servizio di Help Desk (Lotto 1).

Il Fornitore avrà la responsabilità di implementare ed aggiornare l'inventario rispetto ad ogni attività di installazione, trasloco, aggiunta, cambiamento e dismissione al fine di garantirne il costante allineamento con la situazione reale.

Il Fornitore dovrà tracciare le configurazioni hardware e software dei sistemi, controllarne lo stato, le modifiche, il livello di aggiornamento, le interdipendenze, gestirne le condizioni di utilizzo, garantirne la rintracciabilità.

5.13.1.18 Installazione

Il Fornitore sarà responsabile della corretta installazione ed entrata in produzione dei nuovi server e relativi software.

A tal fine collaborerà con ICP nel definire gli standard tecnologici che dovranno essere garantiti per i nuovi server ed a comunicare alla stessa gli eventuali requisiti minimi richiesti.

La procedura normale d'installazione dovrà avvenire secondo quanto definito nella fase di avvio.

Il Fornitore dovrà inoltre prevedere una procedura d'urgenza che permetta l'installazione tempestiva di un nuovo server secondo le direttive concordate con ICP per ogni singolo caso.

Nel caso in cui ICP utilizzasse un Fornitore terzo per l'installazione di server, per motivi di urgenza particolare, il Fornitore dovrà rendere disponibili, verificare e certificare le specifiche tecniche e di configurazione al fine di farsi carico della successiva gestione.

5.13.1.19 Supporto specialistico

Il Fornitore dovrà farsi carico di tutte le attività volte a garantire la massima efficienza e disponibilità delle infrastrutture di elaborazione, garantendo il supporto specialistico sui server a fronte di problematiche hardware e software. Il supporto ha l'obiettivo di analizzare e risolvere problemi di particolare rilevanza.

Il servizio dovrà essere organizzato in modalità tale da prevedere la seguente lista (non esaustiva) di attività:

- Installare e configurare i componenti hardware necessari all'espletamento dei servizi;

- Installare sistemi operativi (SO) e configurarli;
- Installare software database (DB) (ad esempio Oracle, SqlServer);
- Analizzare l'utilizzo dei server e fornire report per permettere interventi di bilanciamento dei carichi e/o di incremento delle componenti;
- Ottimizzare SO e DB per migliorarne le prestazioni;
- Gestire e operare la manutenzione ordinaria e straordinaria di SO, DB;
- Gestire modifiche temporanee alle schedulazioni elaborative seguendo le indicazioni comunicate da ICP di volta in volta;
- Ottimizzare lo spazio su memoria di massa e ripristino dei dati in caso di guasto;
- Definire e preparare procedure e standard d'allocazione degli archivi;

5.13.1.20 Qualità del servizio

Il Fornitore dovrà analizzare la qualità del Servizio attraverso il monitoraggio costante di parametri significativi e fornire informazioni a ICP sullo stato dei sistemi tramite rapporti periodici.

5.14 Servizio di gestione del Software di base, d'ambiente e di rete

Il servizio di gestione è relativo a software di base, d'ambiente e di rete installato sui server.

Al fine di tenere sotto controllo le configurazioni installate in esercizio, il Fornitore, organizzerà la gestione del SW di base, d'ambiente e di rete rilasciato in ottica di Release Management secondo ITIL: si chiede a tale proposito al Fornitore, a fini di valutazione dei processi proposti, di descrivere le strategie di gestione raccomandate, per i principali ambienti HW e SW supportati.

Il Fornitore assicura l'installazione e l'aggiornamento del software.

Il Fornitore è tenuto a segnalare ad ICP la disponibilità di nuove versioni del software di base, d'ambiente e di rete in corrispondenza di eventi quali:

- Disponibilità di versioni significativamente più aggiornate rispetto a quelle in esercizio;
- Scoperta di malfunzionamenti nelle versioni in esercizio, per cui siano disponibili soluzioni "tampone" (patch) o rilasci di versioni che risolvano tali problemi;

In seguito a tale segnalazione sarà facoltà di ICP autorizzare o meno l'aggiornamento delle corrispondenti versioni. Nel caso che tale variazione implichi operazioni di aggiornamento che interessino unità in esercizio, il Fornitore è tenuto a concordarne tempi e modi con il Responsabile di ICP.

È responsabilità del Fornitore proporre eventuali variazioni o migliorie del SW di base, d'ambiente e di rete, sia in funzione delle norme contrattuali, che dell'evoluzione del mercato e della tecnologia hardware e software.

Il Fornitore dovrà garantire il rispetto dei livelli di servizio indicati al paragrafo relativo.

5.14.1 Requisiti

5.14.1.1 Censimento iniziale

Il Fornitore dovrà rilevare, mediante opportuna attività di censimento iniziale, la configurazione del software di base, d'ambiente e di rete a disposizione di ICP, alimentando il CMDB.

5.14.1.2 Supporto alle configurazioni SW

Il supporto per le configurazioni SW copre:

- Incident, problem, change and release management per tutti gli aspetti che riguardano le configurazioni software di base, d'ambiente e di rete;
- La manutenzione ed il supporto delle configurazioni ottimizzate;
- La gestione delle "major upgrades";
- La gestione delle "minor upgrades" che contengono:
  - Cambiamenti della configurazione;
  - Aggiornamento del middleware, dei driver, etc …
  - Installazione di patches di vulnerabilità;

Non è a carico del Fornitore l'installazione di software applicativo lato server. Il Fornitore sarà tenuto a dare alle terze parti fornitrici del software applicativo, tutto il necessario supporto sistemistico.

5.15 Servizio di manutenzione hardware

Il Fornitore dovrà mettere in opera una struttura organizzativa e tecnologica adeguata a far fronte alle richieste di interventi di manutenzione hardware che dovessero rendersi necessari per l'intera durata della fornitura.

Sono identificate le seguenti possibili categorie di interventi di manutenzione, a seconda del tipo di attività effettuata:

Manutenzione preventiva: l'insieme delle attività che si eseguono, secondo un Piano di manutenzione preventiva, al fine di garantire la disponibilità dei sistemi e degli apparati, anticipando, per quanto possibile, malfunzioni di natura Hardware e Software. Rientrano in questa categoria, per esempio, la verifica generale delle apparecchiature; la pulizia delle ventole e dei filtri; la pulizia e lubrificazione delle parti soggette a movimento, ecc.

Manutenzione correttiva: l'insieme delle attività intraprese in occasione delle segnalazioni di malfunzione parziale o totale delle apparecchiature, ivi comprendendo la diagnosi, la sostituzione di componenti, la sostituzione temporanea dell'apparecchiatura difettosa con altra equivalente, la riparazione dell'apparecchiatura, la sostituzione del componente o dell'apparecchiatura, l'attivazione dell'intervento della società che fornisce garanzia / supporto.

Il servizio di manutenzione contribuirà al soddisfacimento dei livelli di servizio indicati per gli altri servizi.

5.15.1 Requisiti

5.15.1.1 Manutenzione sistemi

Relativamente ai sistemi di proprietà del fornitore:

Il fornitore dovrà garantire un servizio di riparazione / sostituzione di componenti hardware coprendo tutti gli aspetti di servizio necessari.

Il servizio dovrà essere fornito per ogni sistema e per la durata del contratto, attraverso un contratto di manutenzione e assistenza con fornitori o garanzia equivalente che sia adeguato ai livelli di servizio contrattuali.

La fornitura dei pezzi di ricambio sarà inclusa nel servizio senza oneri aggiuntivi.

Qualora sia necessario sostituire integralmente un apparato, il Fornitore lo sostituirà con un apparato equivalente, al fine di ripristinare il servizio.

ICP potrà chiedere la sostituzione di un sistema già esistente con un sistema di proprietà ICP di caratteristiche non inferiori e con un contratto di manutenzione equivalente ai contratti di manutenzione in essere da parte del fornitore. Il sistema dovrà essere gestito come gli altri senza oneri aggiuntivi nel rispetto dei livelli di servizio contrattuali.

Relativamente a sistemi di proprietà ICP con contratto di manutenzione o garanzia:

ICP comunicherà al Fornitore l'elenco degli apparati sotto contratto di garanzia / manutenzione con terze parti.

ICP comunicherà al Fornitore i contratti e le interfacce, e il Fornitore sarà responsabile della gestione dei contratti di garanzia / manutenzione.

Relativamente a sistemi di proprietà ICP senza contratto di manutenzione o garanzia:

Il fornitore metterà in atto la riparazione del sistema con pezzi di ricambio forniti da ICP oppure sostituirà l'intero sistema con un sistema equivalente fornito da ICP.

5.15.1.2 Gestione degli interventi

Tutti gli interventi di manutenzione dovranno essere tracciati attraverso l'apertura di un ticket di intervento che dovrà essere inserito nel sistema di registrazione dei ticket (Lotto 1).

5.16 Servizio di Gestione del Backup

Il Servizio di Gestione e Manutenzione del Sistema di Backup centralizzato include tutte le attività necessarie a prendere in carico e condurre operativamente l'infrastruttura hardware e software utilizzata per l'esecuzione delle operazioni di backup/restore in tutte le sedi ICP.

Si definisce "Sistema di Backup Centralizzato" l'insieme delle componenti Hardware (Tape Library, server, infrastruttura di rete, ecc..) e Software (Sistema Operativo, Software di

backup in tutte le sue componenti, firmware, ecc..) necessarie per la gestione e l'esecuzione, in modalità automatica, delle operazioni di backup/restore di tutti i dati residenti e prodotti su tutti i server:

- Già operativi all'avvio dell'attività, inclusi quelli al momento non inclusi nelle procedure di backup;
- Installati in sostituzione di quelli già esistenti;
- Nuovi server installati.

Non è richiesta, se non su esplicita richiesta di ICP, l'implementazione e l'erogazione del Servizio sulle postazioni di lavoro, per le quali non si richiede l'esecuzione delle operazioni di backup/restore dei dati residenti localmente.

Il Servizio comprende:

- Il mantenimento e l'aggiornamento della configurazione del "Sistema";
- L'esecuzione e il controllo delle operazioni di backup e restore;
- Il mantenimento e l'aggiornamento delle policy di backup;
- La gestione della nastroteca e del materiale di consumo.

Per la corretta attivazione ed erogazione dei servizi sopra descritti, il Fornitore dovrà assicurare la presenza di un responsabile operativo del Servizio che garantirà:

- Il corretto indirizzamento delle esigenze di backup di ICP;
- Il rispetto della pianificazione degli interventi, in aderenza alle necessità operative di ICP;
- Il monitoraggio di tutte le fasi di gestione degli interventi e l'identificazione della responsabilità del risultato;
- Il recepimento delle variazioni delle esigenze di backup espresse da ICP, l'individuazione delle soluzioni da sottoporre per approvazione, la pianificazione delle attività necessarie all'implementazione della soluzione approvata, la gestione delle attività di aggiornamento/modifica e l'emissione della reportistica.
- La rendicontazione, su richiesta di ICP, dello stato di avanzamento della risoluzione delle malfunzioni HW/SW del "Sistema", ed il tracciamento /reportistica delle attività.

Il Servizio deve perseguire i seguenti obiettivi:

- Garantire la corretta esecuzione delle operazioni di backup nel rispetto delle policy dettate da ICP;
- Tracciare le configurazioni hardware e software del "Sistema", controllarne lo stato, le modifiche, il livello di aggiornamento, le interdipendenze, gestirne le condizioni di utilizzo, garantire la rintracciabilità (data-base degli asset);
- Mantenere funzionanti ed in piena efficienza operativa tutte le componenti Hardware e Software del "Sistema";

- Prevenire, gestire e risolvere tutti i problemi che comportano interruzione o degrado del servizio di backup/restore;
- Ridurre al minimo i tempi di fermo del “Sistema” a fronte di malfunzionamenti o errori e durante le operazioni di aggiornamento tecnologico;
- Gestire gli interventi in modo efficace, per tutto l’iter operativo, fino alla soluzione del problema;
- Garantire, su richiesta di ICP, il corretto aggiornamento tecnologico anche attraverso la definizione e realizzazione delle modifiche all’architettura del “Sistema” (espansione della tape library, sostituzione del server del “Sistema”, aggiunta di funzionalità del software di backup, ecc.);
- Garantire la disponibilità, la salvaguardia e l’integrità dei dati salvati per il loro ripristino.

Il Fornitore dovrà garantire il rispetto dei livelli di servizio indicati al paragrafo relativo.

5.16.1 Requisiti

5.16.1.1 Censimento iniziale

Il Fornitore dovrà rilevare, mediante opportuna attività di censimento iniziale, le policy e le esigenze di backup, adeguare le policy attuali alle esigenze espresse, concordate con ICP ed alimentare il CMDB.

5.16.1.2 Gestione Ambienti del “Sistema di Backup”

Quest'attività si sostanzierà nel fornire i servizi di supporto necessari per mantenere gli ambienti del “Sistema di Backup” stabili e tali da garantire il soddisfacimento dei requisiti operativi.

Essa consisterà nell’integrazione dei prodotti terze parti (software di backup in tutte le sue componenti, di monitoring e controllo, ecc..) con le componenti del sistema operativo dei server sui quali è richiesta l’esecuzione delle operazioni di backup. L’attività comprende, inoltre, gli aggiornamenti, i test di funzionalità e la distribuzione del software nel rispetto dell’evoluzione tecnologica dei sistemi, degli standard di mercato e dei livelli di servizio contrattuali.

La gestione ambienti del “Sistema” prevederà in particolare:

- L’installazione, l’aggiornamento, la personalizzazione, la distribuzione, la manutenzione e i test di tutti i software (lato client e lato server), compresi i firmware, del “Sistema”;
- L’implementazione di procedure automatiche per l’esecuzione a tempo di operazioni necessarie all’erogazione del Servizio;
- Le personalizzazioni necessarie all’integrazione di altri prodotti software;
- La gestione dei carichi di lavoro in termini di caratterizzazione delle componenti ed assegnazione delle priorità;

- La definizione e realizzazione, su richiesta di ICP, delle modifiche all'architettura delle risorse hardware e software (espansione della tape library, sostituzione del server del "Sistema", aggiunta di agent specifici del software di backup, ecc) necessarie per l'esercizio del servizio di backup/restore;
- La pianificazione, l'esecuzione e il controllo degli interventi di manutenzione sul software e sull'hardware (installazione di patch, upgrade del software di backup in tutte le sue componenti, ecc.).

5.16.1.3 Aggiunta di un server e sostituzione di un server esistente

Di seguito, anche se non esaustivamente, si riportano le attività necessarie per aggiungere/sostituire un server nel "Sistema":

- ICP presenta le esigenze di backup del server da aggiungere o sostituire al responsabile di servizio del Fornitore, che ne verifica la fattibilità e pianifica, in accordo con ICP, le attività necessarie all'implementazione della soluzione che soddisfa le esigenze espresse;
- Il Fornitore, in collaborazione con gli altri servizi di Gestione e Manutenzione, eventualmente in accordo con i fornitori di servizi applicativi e gestione Data Base, procederà all'installazione del software di backup sul server ed eseguirà le azioni necessarie che consentono l'esecuzione delle operazioni di backup in modalità automatica nel rispetto delle policy di backup;
- Il Fornitore procederà all'esecuzione dei test di funzionalità presentando i risultati ottenuti a ICP che ne valuterà l'accettabilità;
- Il Fornitore provvederà, quindi, ad aggiornare le configurazioni e gli asset.

5.16.1.4 Controllo delle operazioni di backup

Il Fornitore eseguirà il controllo giornaliero dell'esito delle operazioni di backup e la redazione del corrispondente report, al fine di rendicontare le operazioni.

Il Fornitore comunicherà tempestivamente a ICP l'esito negativo di ogni operazione di backup, eseguita secondo le policy definite.

5.16.1.5 Risoluzione failure

A fronte di un'operazione di backup terminata con esito negativo dovranno essere intraprese tutte le azioni necessarie a rimuovere il problema affinché la successiva operazione termini con esito positivo.

Qualora la failure dell'operazione sia stata causata da un guasto/malfunzionamento Hardware/Software del "Sistema", il tecnico addetto provvederà all'attivazione dell'intervento di manutenzione, seguendo i criteri esposti in generale per i server al paragrafo relativo.

5.16.1.6 Tuning

Il Fornitore, a fronte di failure delle operazioni di backup, imputabili alle prestazioni del "Sistema", dovrà intraprendere i necessari interventi di tuning mirati ad ottimizzarle e/o alla sincronizzazione delle operazioni di backup con la finestra temporale assegnata. Eventuali criticità dovranno essere tempestivamente segnalate a ICP.

5.16.1.7 Gestione delle operazioni di restore

Le richieste di restore saranno veicolate al tecnico addetto al Servizio attraverso l'Helpdesk. A fronte di una richiesta l'addetto eseguirà le attività necessarie al recupero dei dati richiesti ripristinandoli, salvo diverse indicazioni, nella loro locazione di origine. Nel caso in cui l'operazione non andrà a buon fine, dovranno essere intraprese tutte le azioni necessarie a rimuovere il problema. Eventuali criticità dovranno essere tempestivamente segnalate a ICP.

5.16.1.8 Gestione delle archiviazioni

Le richieste di archiviazione dati degli utenti saranno veicolate al tecnico addetto al Servizio attraverso l'Helpdesk.

Il tecnico contatterà l'utente per ottenere tutte le informazioni necessarie ad eseguire l'archiviazione dei dati (es. residenza, tipo, tempo di conservazione, tipo di supporto, modalità di archiviazione, numero di copie, ecc…), e provvederà ad intraprendere tutte le attività necessarie al soddisfacimento della richiesta.

Al fine di reperire i dati archiviati dovrà essere mantenuto dal Fornitore un Registro delle archiviazioni (in formato elettronico) nel quale verranno riportate almeno le seguenti informazioni:

- Data di esecuzione
- Utente richiedente
- Settore di appartenenza
- Tipo e size dei dati
- Server di provenienza (hostname, sistema operativo, path, ecc..)
- Tipo di supporto
- N. di copie
- Ubicazione dei supporti (in linea, depositata negli appositi siti, eventuale copia consegnata all'utente richiedente)
- Modalità di archiviazione
- Tempo di conservazione

5.16.1.9 Definizione e implementazione di un piano di Disaster Recovery

Dovrà essere definito e messo in opera un Piano di Business Continuity e Disaster Recovery con lo scopo di garantire la continuità e la disponibilità dei sistemi informatici e il loro rapido ripristino in seguito a gravi danneggiamenti causati da eventi accidentali, sabotaggi e disastri naturali.

Il piano dovrà essere definito durante la fase di avvio, approvato da ICP e messo in opera dal Fornitore.

Il Concorrente dovrà descrivere la metodologia che intende adottare per la definizione dei requisiti di Business Continuity e delle strategie di Disaster Recovery.

5.16.1.10 Gestione delle operazioni per recovery del servizio di backup/restore

Consisterà nell'eseguire tutte le attività/operazioni, definite nel piano "Piano di Recovery", per il ripristino del servizio di backup/restore a seguito di eventi disastrosi e imprevedibili.

5.16.1.11 Gestione supporti magnetici (Tape)

È l'insieme delle attività, svolte dal Fornitore, necessarie a garantire la continuità operativa dei backup/restore, nonché la localizzazione e l'individuazione univoca dei tape contenenti i dati da ripristinare a seguito di eventi che ne hanno causato la perdita. La gestione dei supporti magnetici comprende:

- Definizione dei siti

Sarà cura di ICP indicare al Fornitore i luoghi (armadi ignifughi, locali e siti appositi, ecc.) da adibire/adibiti a contenere i supporti magnetici (utilizzati per i backup, per le archiviazioni, doppie copie, ecc..) in conformità alle esigenze di sicurezza ed integrità dei dati trattati;

- Gestione spazio su supporti magnetici

L'attività prevederà l'esecuzione giornaliera di tutte le operazioni necessarie affinché nella tape library sia presente un numero di tape sufficiente a contenere i dati da salvare con le successive operazioni di backup previste. I supporti movimentati dovranno essere riposti nei luoghi appositamente adibiti a custodirli. Rientrerà in questa attività anche l'individuazione dei fabbisogni dei supporti magnetici (tape). A tal riguardo il responsabile del servizio informerà ICP, in tempo utile per poter espletare le procedure di acquisto, del fabbisogno (quantità e tipo di tape da acquistare, bar-code label, ecc…) consegnando un rapporto dettagliato sul numero di tape utilizzato e disponibile.

- Movimentazione dei tape

È l'insieme delle attività attraverso le quali, riguardo alle operazioni di backup/restore/doppia copia, i supporti magnetici sono trasferiti da un luogo all'altro (tape library, armadio ignifugo, locali e siti appositi, ecc.).

- Doppia copia

I set completi dei tape delle doppie copie dovranno essere custoditi nei luoghi (armadi ignifughi, locali e siti appositi, ecc.) indicati da ICP, di norma in edificio diverso da quello in cui vengono registrati. Inoltre, dovrà essere mantenuto un apposito registro, custodito nello stesso luogo delle doppie copie, che, per ogni set, riporti il numero e l'identificativo (bar code, label, altro) dei tape appartenenti al set.

5.17 Servizio di gestione della sicurezza

Al fine di consentire un'efficace ed efficiente gestione della sicurezza informatica sotto tutti gli aspetti, il Fornitore si impegna a rispettare le prescrizioni in materia di sicurezza informatica che saranno emanate da ICP e si impegna a fornire tutto il supporto necessario per la risoluzione di eventuali incidenti o situazioni di crisi per la sicurezza delle informazioni.

La gestione della sicurezza informatica implica l'esecuzione di compiti, fra i quali:

- Effettuare un costante monitoraggio di tutte le risorse, per intercettare e documentare tentativi di violazione di qualsiasi origine;
- Gestire gli incidenti di sicurezza, e le eventuali emergenze ad essi connesse, assicurando la formazione di task force, operanti nell' ambito di unità di crisi, finalizzate al superamento/soluzione in caso di eventi che compromettono le normali condizioni di operatività di funzionalità critiche per dimensione, durata ed estensione;
- Approntare e trasmettere con periodicità almeno mensile un rapporto sugli aspetti della sicurezza;
- Predisporre costantemente tutte le misure preventive, che possano ridurre i rischi (es. aggiornamenti per sistemi operativi, database firme antivirus, system hardening, etc…);
- Amministrare il sistema di diritti e profili d'utente secondo opportune policy di sicurezza;
- Raccomandare ad ICP nuovi approcci, che possano aumentare la sicurezza complessiva del servizio, ed in generale del Cliente.

Il Concorrente descriverà caratteristiche e modalità di erogazione dei servizi richiesti e documenterà nella apposita sezione dell'Offerta Tecnica un modello organico e articolato per la gestione della sicurezza informatica per le attività di competenza, a partire da tutto quanto richiesto nei successivi paragrafi.

Il servizio deve provvedere a:

- Garantire un adeguato livello di sicurezza per le risorse informatiche;
- Applicare e garantire le policy stabilite da ICP relativamente alle risorse e ai servizi informatici;
- Reagire prontamente ed efficacemente agli eventi di sicurezza segnalati dai canali stabiliti (monitoraggio, help desk, enti e organismi specializzati);
- Attivare tempestivamente i processi di escalation per il supporto decisionale;
- Fornire le statistiche sugli eventi registrati al fine di identificare carenze di sicurezza e definire le azioni necessarie alla riduzione del rischio;
- Mettere tempestivamente in atto gli aggiornamenti necessari per l'efficace funzionamento delle componenti fornite;
- Migliorare l'efficacia e l'efficienza nelle modifiche alle configurazioni richieste;
- Controllare ed analizzare i log dei sistemi e gli allarmi di tipo automatico;

- Effettuare una analisi periodica dello stato della sicurezza (sistemi e servizi) con emissione di relativo report.

I servizi erogati e le modalità di gestione dovranno essere conformi sia alle politiche per la sicurezza stabilite da ICP, sia quanto più possibile in linea con le norme ISO 17799.

Il Fornitore dovrà garantire il rispetto dei livelli di servizio indicati al paragrafo relativo.

5.17.1 Requisiti

5.17.1.1 Censimento iniziale

Il Fornitore dovrà rilevare, mediante opportuna attività di censimento iniziale, la configurazione di tutti gli aspetti relativi alla gestione della sicurezza in essere (ad esempio la configurazione attuale del firewall, le policy di gestione degli accessi, etc) alimentando il CMDB.

5.17.1.2 Responsabile della sicurezza informatica

Il Fornitore dovrà identificare un'apposita figura di responsabile della sicurezza informatica per il presente contratto, di cui fornirà riferimenti completi, che assumerà pieni poteri e responsabilità dalla data di inizio del contratto.

Il responsabile della sicurezza:

- Sarà il riferimento diretto ed **unico** per il comitato di sicurezza di ICP per ogni tipo di problema di sicurezza informatica relativo al contratto oggetto di questo appalto, alle cui riunioni dovrà partecipare se richiesto;
- Sarà poi responsabile del coordinamento, supervisione ed attuazione di tutti gli interventi tecnici relativi alla sicurezza informatica che saranno richiesti da ICP per quanto di competenza del Fornitore;
- E' considerato garante del rispetto delle disposizioni di sicurezza qui indicate e di tutte quelle emanate dal comitato di sicurezza;
- In caso di sua assenza temporanea o prolungata, dovrà essere tempestivamente identificato un sostituto avente delega completa, i cui riferimenti dovranno essere immediatamente comunicati ad ICP.

5.17.1.3 Strategia di gestione

Il servizio di Gestione della Sicurezza realizza e gestisce le contromisure di tipo tecnologico e procedurale volte alla difesa del sistema informativo di ICP: difesa perimetrale, controllo codice malevolo, analisi periodica dei sistemi/servizi, procedure di ripristino in seguito ad incidenti informatici, reportistica e rendicontazione.

Tutto ciò si realizza attraverso la gestione di idonei sistemi specializzati (firewall, antivirus, proxy etc.), verifica e rimozione di collegamenti esterni non controllati (es. modem), attività di monitoring e correzione di anomalie hardware/software, definizione ed applicazione di policy che regolano l'utilizzo delle risorse e dei servizi informatici erogati.

Un altro aspetto altrettanto importante è l'osservazione "a freddo" dei fenomeni e degli eventi relativi alla sicurezza delle risorse informatiche, al fine di poter adattare le contromisure e le policy alle nuove minacce e ai rischi ad essi associati; ciò viene realizzato sulla base di un rapporto periodico sullo stato delle risorse informatiche e degli eventi/incidenti occorsi, per la composizione del quale concorrono tutte le attività descritte in questo capitolo.

La sicurezza informatica è gestita attraverso le procedure qui descritte ed è prevalentemente di pertinenza delle figure professionali che se ne occupano; ma tutto il personale informatico impegnato nella gestione dell'infrastruttura informatica concorre nel mantenere un adeguato livello di sicurezza (informatica), poiché questa è intrinsecamente correlata a sistemi, procedure e applicazioni che compongono l'infrastruttura informatica nel suo insieme.

Il processo proposto per la gestione della sicurezza delle informazioni dovrà essere compatibile con le Best Practices for Security Management – ITIL.

In particolare il servizio si concretizza attraverso le seguenti attività:

- Gestione dei dispositivi di sicurezza perimetrale;
- Security host hardening;
- Monitoraggio ;
- Gestione incidenti informatici;
- Report Periodico Mensile di Sicurezza;
- Backup.

5.17.1.4 Sottosistemi di sicurezza perimetrale e modalità operative

Per ogni sottosistema gestito dovrà essere preparato un rapporto delle attività svolte, l'insieme di questi rapporti costituirà parte integrante del rapporto mensile.

Il servizio dovrà consentire di attuare la politica per la sicurezza sui dispositivi di difesa perimetrale (Firewall, VPN, RAS), provvedendo anche alla loro gestione sistemistica ed al supporto alla manutenzione.

Sistemi Firewall

La fornitura per la sala server dovrà includere un apparato firewall di tipo moderno, in grado di far fronte pienamente alle esigenze di ICP per l'intera durata del contratto. L'apparato dovrà svolgere tutte le funzioni che vengono attribuite a questo componente nelle moderne architetture di rete, andando ben aldilà della semplice configurazione e gestione delle comunicazioni tramite il filtraggio dei pacchetti. In particolare, il firewall, oltre ai normali servizi di configurazione di connessioni autorizzate e bloccate, dovrà gestire le VPN e dovrà offrire servizi di monitoraggio del traffico, ai fini del riconoscimento delle applicazioni e altre funzioni di supporto alla sicurezza. La ricchezza delle funzioni offerte dall'apparato e previste per la messa in opera saranno oggetto di valutazione tecnica.

Il salvataggio della configurazione, delle policy adottate (regole applicate) e dei log degli eventi andranno eseguiti in locale sul Modulo di Management tramite l'apposita unità di backup locale.

Qualsiasi variazione alla configurazione del Firewall deve essere valutata congiuntamente al personale di riferimento ICP ed espressamente autorizzata; dovrà essere documentata, con opportuna descrizione, nel rapporto mensile.

Con cadenza almeno settimanale dovranno essere analizzati gli eventi registrati sia dal software del firewall che dal S.O. delle workstation che lo ospitano. In caso di rilevamento di eventi anomali dovrà essere eseguita un'analisi più approfondita.

VPN

Le comunicazioni con Enti o utenti esterni potranno avvenire tramite VPN LAN-to-LAN o point-to-point. Il fornitore dovrà essere in grado di poter erogare tale servizio tramite metodi e architetture standard.

Gli utenti remoti o mobili che intendono connettersi alle risorse interne sono/dovranno essere preventivamente autorizzati; la connessione sarà effettuata esclusivamente su VPN tramite l'apposito programma Secure Client [Secure Remote].

Ogni utente remoto dovrà sottostare alle policy generali definite per questo tipo di connessione.

Per ogni utente remoto saranno definite ed abilitate alla connessione risorse e protocolli specifici a seconda dell'autorizzazione che l'utente ha ricevuto dal personale ICP preposto.

Per ogni utente definito sul firewall sarà stabilita ed imposta una data di scadenza oltre la quale sarà necessario ricevere una ulteriore autorizzazione per poter accedere alle risorse interne.

Al momento della creazione dell'utente sarà generata anche la richiesta del relativo certificato; il relativo codice sarà comunicato all'interessato in modo che possa trasferire l'effettivo certificato sulla propria stazione di lavoro.

Il personale di gestione supporterà gli utenti nella fase di istallazione e configurazione dello specifico software da istallare sul PC remoto.

SPC

Le comunicazioni con Enti esterni o tra le sedi potrà utilizzare il Sistema Pubblico di Connettività (SPC). Il fornitore dovrà essere in grado di riferirsi anche all'adozione di soluzioni tecniche ed architetturali conformi alle regole tecniche e di sicurezza definite nell'ambito del Sistema Pubblico di Connettività (D.P.C.M. 01-04-2008 – Regole Tecniche).

Informazioni da inserire nel Rapporto Mensile

- Variazioni della configurazione dei sistemi
- Variazioni delle regole di policy
- Analisi dei log
- Creazione/aggiornamento utenti

- Altre notizie di rilievo specifiche (eventi anomali, aggiornamenti software etc.)

5.17.1.5 Controllo del codice malevolo

Le licenze dei prodotti antivirus sono a carico di ICP.

Il sistema di controllo del codice malevolo (virus, spyware etc.) deve essere installato su tutti i sistemi server. Il Centro dispone di un sistema antivirus centralizzato che deve essere costantemente mantenuto aggiornato in particolare riferimento alle signature dei virus.

Il servizio di posta elettronica, veicolo privilegiato di virus, spam e altro codice malevolo, dovrà utilizzare un prodotto specifico per il controllo del contenuto dei messaggi installato sullo stesso sistema e complementare all'antivirus centralizzato.

La descrizione e la gestione di questo sistema per la posta elettronica è specificamente fornita nell'apposito Capitolo.

L'attività di controllo deve verificare che :

• Il processo automatico di reperimento degli aggiornamenti sia svolto con regolarità;

• Gli aggiornamenti siano resi disponibili per la distribuzione sulle PDL e su tutti i sistemi su cui è previsto.

Eventuali anomalie nella procedura di aggiornamento, in tutte le sue fasi, devono essere prontamente rilevate e risolte.

Nel Rapporto mensile devono essere inserite almeno le seguenti Informazioni:

- Variazioni della configurazione del sistema;
- Anomalie riscontrate;
- Virus o altro codice rilevato.

5.17.1.6 Monitoraggio di sicurezza

Il monitoraggio consiste di un insieme di attività il cui scopo principale è la rapida ed efficace risoluzione delle anomalie riscontrate e il ripristino del corretto funzionamento dell'infrastruttura:

- Una costante attività di analisi dei sistemi di sicurezza e dei sistemi critici dell'infrastruttura;
- Ricezione e valutazione delle notifiche e degli allarmi provenienti dall'esterno dell'organizzazione, quali fornitori dei prodotti, CERT, istituti di ricerca, organizzazioni governative etc.
- Rilevazione tempestiva di eventi ed allarmi critici per la sicurezza informatica;
- Attività periodica di scanning e penetration test (in modalità "non distruttiva"), con una frequenza trimestrale e generazione di relativo report.

È quindi necessaria una continua e consapevole osservazione dell'infrastruttura gestita al fine di:

- Prevenire i rischi;
- Verificare la corretta attuazione delle politiche di sicurezza e la loro efficacia;
- Individuare tempestivamente situazioni di allarme;
- Fornire un report periodico emesso mensilmente;
- Concorrere a dare una visione globale sull'attività svolta e lo stato di funzionamento sia dei sistemi di sicurezza;
- Supportare ICP nell'individuazione di strategie di miglioramento che possano simulare e contenere attacchi al sistema informatico con l'obiettivo di ottimizzazione delle risorse investite.

I dati e gli eventi da monitorare andranno raccolti attraverso:

- La console di monitoraggio e gestione dei dispositivi forniti (per es. IDS, firewall);
- I log dei dispositivi forniti con il servizio, ed eventuali log provenienti da altri dispositivi importanti dell'infrastruttura (per esempio, server di posta elettronica, router);
- Le notifiche e gli allarmi provenienti dall'esterno dell'organizzazione, quali fornitori dei prodotti, istituti di ricerca.

In particolare:

- La Rilevazione tempestiva di eventi ed allarmi critici per la sicurezza informatica è un elemento essenziale per poter fronteggiare nel più breve tempo possibile gli incidenti informatici di qualsiasi natura, al fine di evitare il propagarsi e l'aggravarsi del problema.
- Dove possibile devono essere attivati i servizi di notifica a mezzo e-mail (o in altro modo altrettanto efficace) verso il Security Manager/amministratore di sistemi/postazione di monitoraggio, sempre controllato durante l'orario stabilito di presidio.
- Ogni allarme o evento ed eventuali richieste da parte dell'Help Desk innescano il processo di gestione delle emergenze.
- L'attività di analisi periodica consiste nell'analisi dei log dei sistemi sopra citati alla ricerca di eventuali anomalie sul funzionamento o di eventi anomali (tentativi di accesso con password sbagliate etc.).
- L'aggiornamento dei sistemi di sicurezza e dei sistemi critici è effettuato in seguito al monitoraggio di notifiche e allarmi emessi dai fornitori degli stessi sistemi gestiti (hardware e software). Quest'attività è dettagliata nel par. Aggiornamenti.
- L'attività di "scansione" (scanning/pen-test) è un'ulteriore verifica del fatto che dall'esterno della rete ICP vengano effettivamente offerti solo i servizi previsti e che non sia possibile accedere a sistemi o servizi non previsti.

Si richiede un monitoraggio costante delle informazioni e delle componenti dell'infrastruttura definiti dalla politica per la sicurezza di ICP che permetta di:

- Prevenire i rischi;

- Verificare la corretta attuazione delle politiche di sicurezza e la loro efficacia;
- Individuare tempestivamente situazioni di allarme.

Gli allarmi generati avvieranno l'attività di gestione delle emergenze (escalation) che dovrà elaborare tali allarmi al fine di ripristinare:
- la disponibilità delle risorse (es. Dati, Software) rispettando i medesimi SLA previsti a seguito di guasti;

- la robustezza/consistenza originaria delle misure di sicurezza.

5.17.1.7 Scansione della rete

La "scansione" dovrà essere svolta in modalità "leggera" per non appesantire il traffico di rete e quindi evitare di produrre in questo modo un Denial Of Service (DOS) generico delle risorse che offrono servizi pubblici:

- Esaminando pochi indirizzi contemporaneamente;
- Effettuando un numero di test concorrenti limitato per non caricare i sistemi;
- E non effettuando test che possono comportare malfunzionamenti dei sistemi o dei servizi offerti, DOS, riavvii (automatici o necessari) dei sistemi.

L'attività sarà effettuata da postazioni:

1. Esterna alla rete ICP: verso tutti gli indirizzi IP pubblici assegnati a ICP, testando tutte le porte e i protocolli comunemente utilizzati (ftp, http, email, telnet etc.), e cercando di individuare tipo e versione del software che realizza i servizi offerti verso Internet, e la presenza di eventuali vulnerabilità da considerare e relative patch disponibili;
2. Sul segmento DMZ, testando tutte le porte e protocolli verso tutti gli indirizzi IP della sottorete DMZ.

È necessario che i prodotti software utilizzati, specialmente se non certificati e di pubblico dominio, siano nella versione più recente e che i moduli di testing siano dell'ultima versione disponibile. Tali prodotti devono essere utilizzati previa autorizzazione di ICP.

Prodotto e versione utilizzati per lo scanning, risultati dello "scanning" e variazioni effettuate/proposte andranno inseriti nel rapporto mensile.

5.17.1.8 Configuration management per la sicurezza

Il servizio provvede alla definizione, manutenzione e controllo delle politiche di configurazione e di aggiornamento dei sistemi server rilevanti per ICP, in termini di sistema operativo e applicazioni di base.

Tutte le configurazioni e le release del SW delle apparecchiature (a partire dai sistemi centrali e server) dovranno essere ottimizzate avendo in primo luogo attenzione al miglioramento della loro protezione e sicurezza; di conseguenza, quanto qui espresso dovrà informare le attività del Fornitore in tutte le attività di Configuration e Release Management.

Riguardo alle componenti SW presenti sulle apparecchiature che dovranno essere gestite dal Fornitore comprensive di software di base, software d'ambiente e software di rete il Fornitore avrà la responsabilità di:

1. Eseguire il security hardening delle apparecchiature, per limitare il livello di vulnerabilità delle risorse ICT del sistema operativo e delle applicazioni di base:
    - Producendo e implementando direttive di configurazione che eliminano le funzioni non necessarie e personalizzano i sistemi operativi per i soli servizi che essi devono offrire, seguendo le indicazioni fornite da ICP;
    - Monitorando e segnalando la disponibilità degli aggiornamenti, con relativo livello di criticità, e indicazione del tempo massimo di applicazione, e implementandoli di conseguenza; qualora non applicabili a causa di incompatibilità con software istallati, attuando correttivi o contromisure finalizzate a ridurre il rischio.
2. Eseguire l'installazione pianificata di aggiornamenti collettivi del software (nuove versioni di applicazioni standard o la distribuzione di file di definizioni antivirus aggiornate) presso gli utenti, con regole concordate con ICP;
3. Eseguire l'installazione di aggiornamenti per la correzione mirata di vulnerabilità critiche nel caso possano mettere in serio pericolo la sicurezza del Sistema Informativo di ICP;
4. Configurare e (far) utilizzare ogni apparecchiatura al livello minore ("più sicuro") di accesso utilizzatore necessario per l'uso corrispondente (es. "tutte" le PdL in modalità "user"; accesso ed operatività in modalità "administrator" anche sui server per lo stretto necessario);
5. Produrre una relazione semestrale comprensiva sia di nuove release che di patch o correzione di bug, o per integrazione di nuove funzioni, rilasciate ufficialmente dai produttori di software specifici installati, anche di proprietà di ICP.

5.17.1.9 Aggiornamenti

Ci si riferisce qui all'aggiornamento dei sistemi di sicurezza, attività avviata solitamente a seguito della disponibilità di nuovi rilasci da parte dei fornitori dei prodotti, finalizzati a proteggere da minacce note e/o prevenirne di nuove; ad esempio:

- Database delle signature degli antivirus;
- Aggiornamenti critici per i sistemi operativi e le applicazioni di base;
- Black list per sistemi di content filtering;
- Database dei pattern di attacco degli IDS.

La rapidità nella distribuzione degli aggiornamenti varia in base al tipo di servizio ed in funzione dell'entità del rischio derivante dalla mancata od intempestiva esecuzione dell'attività.

In ottica di Change Management (e di conseguenza tenendo conto dei rischi derivanti dai ripetuti cambi di configurazione), si richiede al Concorrente di formulare una proposta

relativa alla tempestività degli aggiornamenti, da perfezionare in sede di contratto in accordo con la politica per la sicurezza stabilita di ICP.

5.17.1.10 Verifica della conformità

È necessario verificare l'allineamento dell'insieme della configurazione installata sul parco alle direttive stabilite in materia di sicurezza delle configurazioni (risultato delle scelte concordate del Fornitore e di ICP, mettendo in pratica direttamente le indicazioni dei produttori dei sistemi operativi o delle applicazioni stesse, e/o personalizzando le configurazioni in base alle specifiche dell'infrastruttura in cui i sistemi si trovano ad operare).

È opportuno che la verifica esamini cambiamenti importanti della configurazione:

- Su base periodica, per l'intero parco macchine al quale il servizio è rivolto;
- Prima del rilascio in esercizio delle applicazioni;
- A seguito di modifiche importanti ai servizi erogati.

È necessaria inoltre una verifica periodica:

- Sia delle direttive definite per eventuali miglioramenti e adeguamenti a fronte di nuove vulnerabilità,
- Sia della conformità delle configurazioni dei sistemi alle direttive approvate.

A tale proposito si chiede al Fornitore, un'autocertificazione periodica dell'attuazione delle regole e delle policy decise da ICP e la cui implementazione è stata richiesta al Fornitore stesso mediante le opportune procedure.

In particolare tale documentazione deve includere:

- La descrizione delle regole implementate;
- Il risultato dei test effettuati atti a garantire l'effettivo rispetto di tali regole.

5.17.1.11 Gestione degli incidenti di sicurezza informatica

L'attività di gestione degli incidenti di sicurezza informatica (gestione delle emergenze) ha l'obiettivo di fornire rapide ed efficaci risoluzioni delle anomalie riscontrate in termini di sicurezza informatica, fino al ripristino del corretto funzionamento dell'infrastruttura nel rispetto dei livelli di servizio indicati.

La gestione degli incidenti informatici deve assumere una più alta priorità di intervento rispetto ad altri eventi in relazione alla entità degli stessi; più è elevata la gravità dell'evento più alta sarà la priorità assegnata.

Il processo è attivato a seguito di una segnalazione od evento potenzialmente critico. La segnalazione può essere notificata da:

1. Un allarme generato dal processo di monitoraggio di sicurezza;
2. Una richiesta o una segnalazione del Help Desk (primo o secondo livello).

La segnalazione determinerà l'intervento di un gruppo specialistico di gestione della sicurezza informatica messo a disposizione dal Fornitore.

Il gruppo specialistico di gestione della sicurezza informatica si configura dal punto di vista dei flussi di supporto come un gruppo "di terzo livello":

1. Che naturalmente non appena riscontrato l'allarme si metterà subito all'opera nel primo caso; per avere una corretta gestione degli incidenti, si richiede al Fornitore che i sistemi di monitoraggio vengano integrati e configurati in modo da generare automaticamente il relativo ticket sul sistema di Help Desk.
2. Nel secondo caso il gruppo sarà stato coinvolto a seguito della seguente escalation (rappresentativa del processo normale di Help Desk):
   - Accertamento della natura e severità dell'incidente;
   - Classificazione definitivamente dell'incidente come di sicurezza informatica, secondo uno schema che sarà concordato con ICP;
   - Escalation dopo la prima diagnosi, in modo che l'incidente sia gestito dalle strutture più adeguate per una risoluzione efficace.

In funzione del tipo di segnalazione il gruppo specialistico procederà con una rapida e tempestiva indagine per confermare o meno la presenza di una potenziale minaccia o per arginare una minaccia concretizzata.

In caso di conferma:

- Controllerà l'evoluzione della risoluzione dell'incidente e coordinerà la risposta, facendo in modo che tutte le funzioni interessate siano informate sull'accadimento dell'evento ed eventualmente della sua evoluzione;
- Fornirà tempestivamente alle strutture di riferimento di ICP una stima dei tempi di risoluzione dell'incidente;
- Reperirà le eventuali risorse tecniche (es. strutture internazionali di supporto antivirus) o professionali mancanti (skills particolari momentaneamente non disponibili) e coordinerà l'attuazione delle contromisure, per le parti di propria competenza;
- Richiederà al responsabile per la sicurezza di ICP l'eventuale autorizzazione alla messa in atto dell'azione correttiva;
- Procederà rapidamente con l'azione correttiva di pertinenza (come per esempio il blocco immediato del traffico pericoloso) in modo da risolvere l'emergenza (Risoluzione dell'emergenza);
- Eseguirà la chiusura definitiva dell'incidente (chiusura del ticket), registrando anche la storia, i dati principali (i cui dettagli naturalmente saranno stati raccolti anche dai log degli strumenti coinvolti), le indagini ed i tempi dello stesso;
- Informerà tutte le funzioni interessate, qualora non fossero già state avvisate, confermando il superamento dell'emergenza ed il ripristino della normalità.

L'attività determina, secondo le procedure ICP, la produzione di un dettagliato rapporto (Rapporto di incidente) che riepiloga ed analizza gli eventi al fine di individuare le cause imputabili all'emergenza e descrive le attività svolte per affrontarla, documentando:

1. Il tipo di azione perpetrata;
2. Le cause all'origine dell'incidente (bug di un sistema, attacco informatico, malfunzionamento etc.);
3. Le conseguenze dell'accaduto;
4. I tempi e le modalità di rilevazione dell'incidente;
5. I tempi e le modalità di ripristino;
6. Eventuali altre anomalie riscontrate.

5.17.1.12 Backup

Il salvataggio e la disponibilità dei dati in generale sono garantiti dal servizio di backup centralizzato dei dati, salvo che:

- I messaggi generati dal sistema firewall dovranno essere registrati e conservati sull'apposita unità di backup locale con frequenza concordata con ICP;
- I file di configurazione dei sistemi di sicurezza saranno registrati e mantenuti aggiornati su un apposito supporto, e conservati in luogo sicuro ad accesso controllato sotto la responsabilità del Security Manager.

5.17.1.13 Rendicontazione

Il particolare rilievo della sicurezza informatica enfatizza l'attenzione sul superamento/non superamento dei parametri di controllo del servizio, ma ancor più sulle opportunità di miglioramento continuo.

A tale proposito, serviranno analisi ed elaborazioni di dati quali:

1. Le registrazioni degli eventi significativi per la sicurezza e quelli relativi ai guasti/malfunzioni;
2. I log dei dispositivi come firewall e IDS che realizzano l'infrastruttura di sicurezza;
3. Gli allarmi che hanno attivato la gestione ordinaria o delle emergenze;
4. I valori prestazionali collezionati dai sistemi di monitoraggio.

Le elaborazioni saranno finalizzate alla produzione periodica di un Rapporto sulla sicurezza logica che

- Permetta di analizzare l'andamento del servizio;
- Evidenzi eventuali carenze nella sicurezza, per la definizione di azioni necessarie alla riduzione del rischio.

I contenuti del rapporto devono trattare, per ciascun servizio erogato:

a) Le anomalie riscontrate rispetto alle politiche di sicurezza definite, relativamente alle specificità del corrispondente servizio; aggregate ove possibile in base alla tipologia, alla sorgente, alla destinazione ed alla fascia oraria degli eventi registrati come non conformi alle politiche di sicurezza;

b) L'andamento nel tempo dei parametri prestazionali significativi per il servizio e per gli strumenti utilizzati. Ad esempio:
   - Utilizzo della CPU, della memoria, delle interfacce di rete degli strumenti adottati;
   - Lunghezza della coda dei messaggi di posta elettronica in attesa di controllo antivirus, numero di connessioni contemporanee gestite da un dispositivo firewall, per i servizi specifici.

5.17.1.14 Gestione delle utenze

Per la gestione delle utenze di dominio il fornitore dovrà fare riferimento a quanto definito alla sezione "Gestione degli utenti" in "Servizio di Gestione dei server".

Utenze amministrative:

- Il loro numero deve essere ridotto al minimo possibile, facendo sì che ogni addetto abbia visibilità di tutte e sole le utenze amministrative relative agli apparati di cui è responsabile;
- Devono essere tutte registrate con le relative credenziali in una o più liste:
    - Mantenute aggiornate e rese disponibili agli addetti preposti alla manutenzione ed a ICP;
    - Le liste di credenziali devono essere immagazzinate su supporti elettronici rimovibili e protette tramite meccanismi di cifratura adeguati;
    - Non ne è consentita la stampa, la copia per usi estranei al semplice backup dei supporti su cui sono immagazzinate e la diffusione e pubblicazione anche in forma protetta su strumenti in rete.

Nomi utente (username):

- Quelli delle utenze amministrative non devono essere di tipo standard (ad esempio administrator, admin,..) o contenere informazioni riconducibili agli addetti alla manutenzione;
- Non sono ammesse utenze di test con username riconoscibili (ad esempio test, guest, ...), nè la creazione di utenze anche temporanee non riportate nelle liste sopra indicate, per alcun motivo, neppure in fase iniziale di installazione.

Password:

- Devono avere una lunghezza almeno di 8 caratteri;
- Contenere se possibile numeri, lettere e caratteri speciali;
- Non devono contenere parole di senso compiuto o dati ricavabili dall'identità degli addetti o da altro genere di informazioni;
- Devono essere cambiate con frequenza trimestrale, riportando il cambiamento nelle liste sopra indicate; per gli utenti amministrativi si potrà definire una frequenza mensile di rinnovo.

ICP identificherà i nominativi del proprio personale (nominato come Amministratore di Sistema) che potrà disporre di account amministrativa definita secondo le specifiche definite.

5.17.1.15 Verifiche di sicurezza

Il Fornitore s'impegna a fornire la propria disponibilità e supporto tecnico, con la supervisione del responsabile della sicurezza, a tutte le attività di controllo del livello di sicurezza informatica decise da ICP.

Le attività di controllo della sicurezza potranno riguardare qualsiasi tipo di apparato o sistema facente parte della nuova rete di ICP, a qualsiasi livello, sia fisico sia logico.

ICP si riserva di far eseguire, eventualmente anche a terze parti, verifiche del livello di sicurezza informatico, senza alcun preavviso o notifica diretta al responsabile della sicurezza, al fine di mantenere sotto controllo costante il rispetto delle prescrizioni e direttive emanate.

5.17.1.16 Servizi di sicurezza fisica

Nell'ambito dell'area servizi di sicurezza, il Fornitore dovrà prendersi carico della gestione delle problematiche riguardanti la sicurezza fisica dell'infrastruttura della quale è direttamente responsabile.

5.17.1.17 Identificazione del personale

Il personale che opera per la fornitura dei servizi deve essere chiaramente identificabile. L'elenco completo del personale addetto e dei relativi recapiti, compiti e permessi amministrativi dovrà essere mantenuto aggiornato e accessibile dal CMDB. Ogni variazione a questo elenco dovrà essere segnalata preventivamente ad ICP; nessun addetto all'infuori di quelli elencati ed approvati avrà autorizzazione ad accedere alle sedi di ICP.

5.17.1.18 Supporto alle operazioni

Il Fornitore s'impegna a fornire, tramite la supervisione del proprio responsabile della sicurezza, tutto il supporto tecnico necessario nel caso ICP decidesse di implementare nuove funzionalità di sicurezza sulla propria infrastruttura.

Il Fornitore s'impegna altresì a fornire tutto il supporto tecnico necessario, e per tutto il tempo entro il quale questo sarà richiesto, in caso di risoluzione di incidenti relativi alla sicurezza delle informazioni ed in caso di disastro che porti all'interruzione del servizio di parti dell'infrastruttura.

5.17.1.19 Accesso ai dati circolanti in rete

Il Fornitore non potrà mai, salvo esplicita autorizzazione di ICP, accedere ai dati trasportati sulla rete di ICP, con l'esclusione della parte necessaria alla corretta erogazione dei servizi richiesti.

Ogni abuso in questo senso sarà sottoposto agli organi competenti per la valutazione di potenziali ripercussioni anche di tipo legale.

5.17.1.20 Supporto al rispetto della normativa sulla privacy

Il Fornitore s'impegna a realizzare le misure di sicurezza e a fornire tutto il supporto tecnico necessario a ICP, in ottemperanza alla normativa vigente sulla privacy (DLgs. 196/2003 e suoi aggiornamenti) e ai Provvedimenti del Garante della Privacy, in particolare il Provvedimento del 27 novembre 2008 che comprende le seguenti indicazioni:

- Registrazione degli accessi

  Adozione di sistemi di controllo che consentano la registrazione degli accessi effettuate dagli amministratori di sistema ai sistemi di elaborazione e agli archivi elettronici.

  Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e devono essere conservate per un congruo periodo, non inferiore a sei mesi.

- Verifica della attività

  Supporto alla verifica almeno annuale da parte della Direzione Generale sulla rispondenza dell'operato degli amministratori di sistema alle misure organizzative, tecniche e di sicurezza previste dalla legge per i trattamenti di dati personali.

- Elenco degli amministratori di sistema e loro caratteristiche

  Supporto all'inserimento nel DPS (documento programmatico della sicurezza) degli estremi identificativi degli amministratori di sistema e dell'elenco delle funzioni loro attribuite.

Le attività per cui il Fornitore dovrà offrire supporto, comprendono anche:

- Il controllo della conformità dei trattamenti informatici di dati personali a leggi e regolamenti e la segnalazione ai responsabili dei trattamenti delle modifiche da adottare per conseguire tale conformità;
- L'esame delle segnalazioni e dei reclami degli interessati;
- Il blocco del trattamento informatico di dati personali quando per la loro natura, oppure per le modalità o gli effetti di tale trattamento, vi sia il rischio concreto di un rilevante pregiudizio per l'interessato;
- La predisposizione di una relazione annuale sull'attività svolta e sullo stato di attuazione della legge.

Il Concorrente dovrà individuare uno Specialista responsabile di queste attività e dovrà presentare il suo curriculum che dimostri le capacità tecniche e l'esperienza maturata negli ultimi 3 anni nella definizione e realizzazione di misure di sicurezza tecniche e organizzative nel pieno rispetto della normativa in materia di protezione dei dati personali. Tale Specialista farà parte dell'Incident Response Team (IRT) di ICP previsto dalla normativa.

Inoltre, il Concorrente dovrà presentare i curriculum degli amministratori di sistema che dimostrino esperienza, capacità e affidabilità delle persone che dovranno essere in grado di garantire il pieno rispetto della normativa in materia di protezione dei dati personali, compreso il profilo della sicurezza.

Gli strumenti software necessari per il supporto al rispetto della normativa sulla privacy saranno a carico del Fornitore.

5.17.1.21 Certificazioni di sicurezza informatica

Il Concorrente dovrà indicare nell'offerta tecnica le eventuali certificazioni sulla sicurezza informatica delle quali è in possesso, e di qualunque altro tipo di test o verifica della sicurezza alla quale la propria infrastruttura è stata sottoposta.

ICP si riserva la facoltà di richiedere ogni tipo di documentazione attestante quanto dichiarato dal Concorrente.

5.17.1.22 Conformità a norme e standard

L'erogazione dei servizi di sicurezza sarà in linea con le regole d'arte correnti nell'industria (best practices) ed almeno in linea con le seguenti normative:

ISO/IEC 17799:2005: Information Security Management – Code of practice for information security management, 2005;

ISO/IEC 27001:2005: Information security management systems – Requirements, 2005;

Ministero per l'Innovazione Tecnologica – La sicurezza Informatica e delle Telecomunicazioni (ICT Security) – Allegato 2, Gennaio 2002;

Dlgs 196/2003 e suoi aggiornamenti– Codice in materia di protezione dei dati personali, Allegato B. Disciplinare tecnico in materia di misure minime di sicurezza;

Provvedimenti del Garante della Privacy

DigitPA – Linee guida per la sicurezza ICT delle Pubbliche Amministrazioni.

5.18 Servizio di Gestione della Posta Elettronica

Il servizio di posta elettronica fornisce al personale di ICP la possibilità di creare, spedire e ricevere e-mail dalle postazioni di lavoro individuali con:

• Entità interne, ovvero utenti appartenenti ad ICP;

• Entità esterne, ovvero utenti non appartenenti ad ICP.

Il servizio è strutturato con architettura centralizzata ed è erogato "on-site" presso ICP. Il servizio dovrà essere gestito dal fornitore utilizzando l'architettura già disponibile in ICP, le cui eventuali evoluzioni saranno gestite secondo i termini e le modalità definite nel seguito di questo documento.

Il Fornitore prenderà in carico hardware e software e tutte le componenti del sistema di posta elettronica.

Gli obiettivi della Fornitura del servizio sono così definiti:

- Gestione del servizio di posta elettronica del dominio di posta e di eventuali sottodomini, manutenzione dell'HW e del SW dedicato al servizio.

- Gestione/creazione/eliminazione degli indirizzi di posta elettronica, assegnati a ciascun utente o a liste di distribuzione, univocamente definiti e corrispondenti a una mailbox su un server dedicato, con quota massima prefissata al raggiungimento della quale l'utenza è avvisata ed invitata a cancellare i messaggi già letti;
- Gestione delle liste di distribuzione attivabili su richiesta degli utenti con indirizzi di entità interne ed esterne; tali liste possono essere moderate (tutti i messaggi devono essere approvati da un moderatore), non moderate (tutti gli iscritti possono inviare messaggi alla lista), aperte (chiunque abbia accesso al servizio può iscriversi autonomamente) e chiuse (solo il moderatore/gestore della lista può effettuare le iscrizioni);
- Backup delle mailbox e dei messaggi delle liste di distribuzione;
- Controllo anti-spamming sul sistema di posta centrale;
- Controllo antivirus su sistema di mail centrale;
- Consentire agli utenti di accedere al servizio in modo semplice e rapido;
- Garantire il servizio di assistenza per qualsiasi problema relativo alla posta, "lato utente";
- Garantire il servizio di assistenza per qualsiasi problema relativo al servizio o ad ogni parte dell'architettura hardware e software;
- Garantire i requisiti minimi di sicurezza dei dati scambiati attraverso il sistema, con: integrità, confidenzialità dei dati sia nella comunicazione, sia nella custodia ed accesso;
- Garantire adeguate misure di sicurezza al fine di evitare usi impropri dei server che costituiscono l'architettura del servizio di posta elettronica;
- Disporre di una configurazione delle cassette postali che ne garantisca la protezione, consentendo un'identificazione univoca dell'utilizzatore, mediante accesso controllato con identificativo utente;
- Gestire e manutenere le cassette postali degli utenti con policy di sicurezza e diritti di accesso sia monoutente che multiutente, restrizioni d'invio e recapito, limitazione di archiviazione;
- Creare e aggiornare i gruppi di distribuzione con policy di sicurezza;
- Garantire un'adeguata misura di controllo antivirus, per mail da e verso il sistema;
- Garantire un efficace livello di performance del servizio. Eseguire la compattazione dello spazio con cadenza almeno mensile.
- Garantire tempi rapidi di ripristino del servizio o di ogni sua parte componente, predisponendo ed ottimizzando le procedure di crash-recovery.

Il servizio si rivolge agli utenti ICP e a tutti quelli che rientrano nell'organizzazione e hanno assegnata una mailbox.

Il Fornitore dovrà garantire il rispetto dei livelli di servizio indicati al paragrafo relativo.

5.18.1 Requisiti

5.18.1.1 Censimento iniziale

Il Fornitore dovrà rilevare, mediante opportuna attività di censimento iniziale, lo stato attuale del servizio ed alimentare il CMDB.

5.18.1.2 Vincoli

I vincoli che caratterizzano la fornitura del servizio sono i seguenti:

• Scambio dei messaggi con l'esterno mediante standard SMTP per i messaggi di tipo testuale e ESMTP/MIME (Enhanced SMTP / Multipurpose Internet Mail Extension) per messaggi non solo testuali;

• DSN (Delivery Status Notification) e MDN (Message Delivery Notification) garantite almeno all'interno dell'organizzazione (per consentire agli utenti di verificare l'avvenuto recapito del messaggio nella cassetta postale del destinatario ed eventualmente anche la sua effettiva apertura / lettura);

• Accesso alle cassette postali possibile solo mediante l'inserimento delle credenziali utente;

• Spedizione di messaggi in modalità SMTP da parte degli utenti possibile solo se esiste la corrispondenza di due fattori: credenziali utente ed esatta corrispondenza dell'indirizzo SMTP del mittente con quello definito sul sistema (anti-relaying ed "address-spoofing");

• Sistema protetto da antivirus con aggiornamento automatico ad intervalli di tempo non superiori alle 24 ore – ed immediati nel caso di rilasci di "signature" antivirus su eventi di sicurezza; la correttezza dell'aggiornamento sarà da verificare con cadenza giornaliera;

• Sistema che consentirà agli utenti interni, su inserimento delle credenziali utente, la consultazione della rubrica o indice degli utenti ospitati mediante protocollo LDAP (Lightweight Directory Access Protocol). L'aggiornamento continuo della rubrica comune avverrà ad opera del Fornitore;

• Il sistema disporrà di un servizio automatico di sincronizzazione del tempo ufficiale di rete da una fonte attendibile mediante protocollo NTP (Network Time Protocol) con collegamento ad almeno due server esterni. Attendibilità dell'orario ed avvenuta sincronizzazione a cura del fornitore;

• Procedure di salvataggio dei dati che consentono, in caso di perdita delle mailbox sul sistema, la ricostruzione delle stesse almeno alle 24 ore precedenti;

• Archiviazione su supporto dedicato e conservazione per un tempo non inferiore a 12 mesi, dei tracciati log relativi al transito di tutti i messaggi ricevuti ed inviati;

• Collegamento degli utenti al sistema di Posta Elettronica in modalità accesso MAPI; mediante applicazioni client di posta elettronica;

• Presenza di apposite procedure di ripristino necessarie a ridurre al minimo i fermi del sistema dovuti a guasti o a manutenzioni programmate. A tal fine sarà presente un adeguato servizio di salvataggio a caldo dei dati che preveda delle politiche di lavoro che garantiscano, in caso di disastro, il ripristino del sistema di posta elettronica almeno alle 24 ore precedenti.

5.18.1.3 Attività di gestione e modalità operative

Nella gestione del servizio rientrano tutti i componenti hardware dell'architettura di posta elettronica: server mail interno e le relative componenti software costituenti (ad esempio il sistema operativo, Gestore software di posta, sistema anti-spam, antivirus, ecc…).

Il Fornitore dovrà:

• Concordare in anticipo con i responsabili ICP le attività da svolgere e quindi pianificare, sviluppare, collaudare ed applicare tutti gli aggiornamenti infrastrutturali e/o procedurali necessari per mantenere il servizio alla massima funzionalità, oltre che mantenerne adeguata documentazione per corretta gestione delle configurazioni;

• Garantire la disponibilità dei sistemi e prestazioni adeguate;

• Assicurare un presidio specialistico, con conoscenze adeguate sulle componenti principali dell'architettura, continuo nelle ore di servizio garantito, al fine di controllare lo stato dei sistemi e dei collegamenti, individuare criticità o malfunzionamenti ed intraprendere le azioni necessarie;

• Prevenire, gestire e risolvere tutti i problemi che comportano interruzione o degrado del servizio, nel qual caso i responsabili ICP dovranno essere prontamente informati;

• Presentare un piano dei tempi di risoluzione necessari, nel caso in cui questi non ricadano negli SLA (ad esempio per eventi eccezionali o non pianificabili in anticipo);

• Ottimizzare l'utilizzo dello storage in termini di razionalizzazione degli accessi e garantire la disponibilità, la salvaguardia e l'integrità dei dati. Qualunque razionalizzazione degli accessi o dello storage delle mailbox, sarà comunque preventivamente concordato con i responsabili ICP;

• Garantire l'efficienza dei sistemi rispetto all'utilizzo delle risorse hardware e software;

• Controllare l'impatto sulla tecnologia esistente e garantire l'adeguamento degli ambienti elaborativi a fronte dell'immissione in esercizio di modifiche correttive e/o evolutive di applicazioni esistenti.

• Garantire la conduzione operativa dei sistemi (accensione e spegnimento, produzione di stampe, start-up dei collegamenti, ecc.);

• Gestire i backup/restore dei dati di sistema;

• Gestire la configurazione e la definizione delle modalità di utilizzo dello storage in termini di regole di allocazione e movimentazione dei dati;

• Gestire il "Patching" software e hardware nel caso di esigenze evidenti di importanti adeguamenti per garantire il corretto funzionamento e la sicurezza del servizio (ad esempi patching che "chiudano" pericolosi "bug" sulla sicurezza del sistema operativo). Dovrà comunque essere analizzato l'impatto della/e patch da applicare documentando benefici ed eventuali rischi associati, e informando per tempo i riferimenti ICP.

5.18.1.4 Risoluzione failure

Qualora la failure del servizio sia stata causata da un guasto/malfunzionamento Hardware/Software del "Sistema", il tecnico addetto provvederà all'attivazione dell'intervento di manutenzione, seguendo i criteri esposti in generale per i server.

5.19 Servizio di Configuration Management

Il servizio ha lo scopo di rilevare le variazioni nella composizione del parco a seguito dell'introduzione di nuove apparecchiature o di variazioni dell'infrastruttura ICT di ICP ed il mantenimento delle informazioni inventariali da comunicare secondo necessità ad altri uffici di ICP.
Obiettivo di ICP è il mantenimento delle informazioni relative al parco ICT non solo in termini di volumi (tipologie e quantità di hardware e software) ma anche in termini di attribuzione ai singoli centri di costo dell'Amministrazione e di assegnazione ai singoli Utenti (cambio di ubicazione, cambio di utenza, spostamento organizzativo).

Tutte le informazioni dovranno essere conservate in unico database sul quale dovranno essere registrati tutti i dati di configurazione, secondo il modello del CMDB suggerito da ITIL.

Il CMDB (integrato con lo strumento di gestione dei ticket) sarà gestito attraverso le modalità e lo strumento messo a disposizione dal servizio di Help Desk (Lotto 1).

Dovranno essere gestiti fra gli altri (elenco non esaustivo):

- Rapporti di Help Desk ("ticket"), e relative statistiche;
- Rapporti sugli interventi di manutenzione - programmata e non;
- Livelli di servizio, di modo che ICP e Fornitore siano in grado di intervenire in tempo reale in caso di scostamenti rispetto agli obiettivi;
- Configurazioni di tutte le apparecchiature supportate e loro modifiche nel tempo, nonchè relazioni fra i componenti (Configuration Items – CI) che le costituiscono, più una serie di attributi che ne permettano la gestione non solo tecnica ma anche amministrativa e finanziaria ("Asset management");
- Specifiche, manuali etc. dei prodotti supportati;
- Rapporti contenenti le statistiche provenienti da sistemi di monitoraggio automatico (es. di sistemi o di reti);
- Rapporti relativi ai test periodici per la verifica di parametri degli SLA. I rapporti dovranno esplicitare con chiarezza i valori di misura da cui si evidenzi il soddisfacimento o meno degli SLA con possibilità di visualizzare nel dettaglio i ticket fuori SLA;
- Database di FAQ, Known-errors etc …
- Ogni altra documentazione prodotta dal personale di ICP o del Fornitore per qualsiasi tipo di motivo inerente al controllo della fornitura;
- In generale tutta la documentazione o i dati che, a vario titolo, sono connessi alla gestione tecnica ed amministrativa del contratto, nel corso del suo svolgimento.

Il Fornitore dovrà garantire il rispetto dei livelli di servizio indicati al paragrafo relativo.

5.19.1 Requisiti

5.19.1.1 Accesso del personale ICP al CMDB

Il personale di ICP dovrà essere reso autonomo nell'accesso e nell'elaborazione delle informazioni gestite dal CMDB e dovrà poter disporre di tutti gli strumenti di reporting.

Di conseguenza, indipendentemente dalle attività di reporting periodico richieste al Fornitore, ICP potrà utilizzare ed elaborare tutti i dati memorizzati, in ogni momento senza vincoli da parte del Fornitore.

Tutti i dati caricati ed i report prodotti dovranno essere esportabili in formati standard (ad esempio csv).

5.19.1.2 Asset Management

La componente più strettamente di Configuration Management del CMDB costituisce una piattaforma per lo svolgimento del servizio normalmente definito come Asset Management, e di cui un componente essenziale ma parziale è l'inventario.

Il fornitore registrerà tutti gli asset gestiti da contratto e aggiornerà in maniera automatica tutti i dati relativi agli asset che lo consentono. Questo sistema sarà integrato con il sistema di Helpdesk e farà riferimento allo stesso database contenuto nel CMDB.

Le principali operazioni da supportare saranno:

- Raccogliere, mantenere e distribuire informazioni accurate e aggiornate sulle apparecchiature supportate per poterne gestire le dotazioni;
- Controllare lo stato di operatività dei beni, per pianificare con efficienza gli upgrade in relazione alle richieste e necessità degli obiettivi del Cliente;
- Generare i report necessari alla valutazione dell'inventario per un'eventuale pianificazione di rinnovo tecnologico.

Il servizio dovrà essere svolto implementando e manutenendo un database iniziale di gestione del ciclo di vita completo del parco delle attrezzature informatiche hardware e software.

Il sistema dovrà essere integrato con quello di Help Desk, per permettere agli operatori di aprire e chiudere i ticket. Nel caso la richiesta sia passata a terze parti, dovranno essere predisposte delle modalità che garantiscano la registrazione della chiusura della richiesta sullo strumento di supporto.

Il servizio è attivato come conseguenza dell'erogazione di altri servizi che causano la necessità di aggiornamento della base dati inventariale, e si chiude successivamente alla variazione inventariale.

L'aggiornamento deve essere tempestivamente assicurato per ogni variazione.

In generale il Fornitore avrà la responsabilità di effettuare il controllo della configurazione completa di ogni sistema in gestione. Per "configurazione" s'intende non solo i parametri

d'installazione dell'apparato, ma anche tipo e versione del sistema operativo e software applicativo installati e tutti gli eventuali aggiornamenti. Le attività richieste sono:

- Identificazione e controllo della configurazione;
- Registrazione dello stato di configurazione;
- Audit sulla configurazione.

Ogni tipologia di richiesta che comporti il cambiamento alla configurazione effettuata dal Fornitore su sistemi dovrà comunque essere sempre documentata e nel caso comporti un potenziale pericolo ai sistemi informativi di ICP, il Fornitore dovrà produrre un'analisi delle motivazioni e dell'impatto da sottoporre ai corrispettivi riferimenti di ICP che decideranno in merito all'attuazione dello stesso ("change management").

5.20 Formazione in affiancamento

Il personale operativo del Fornitore potrà essere affiancato da personale ICP in tutte le attività di fornitura dei servizi. Gli scopi dell'affiancamento saranno:

- Rendere nota e condivisa con il personale ICP tutta l'operatività relativa alla fornitura dei servizi e tutte le informazioni e documentazioni associate.
- Formare in affiancamento il personale ICP.

L'affiancamento non altererà in alcun modo la totale responsabilità del Fornitore rispetto ai servizi dovuti contrattualmente.

Il carico di lavoro di formazione per affiancamento di personale ICP non eccederà il 10% del carico di lavoro totale del Fornitore.

5.21 Rilascio di rapporti di servizio

Il Fornitore dovrà produrre, nell'ambito dello svolgimento dei servizi previsti, un insieme di rapporti periodici.

La rendicontazione ha sia l'obiettivo di verificare l'andamento del servizio che di fornire informazioni utili all'evoluzione delle forme contrattuali.

La descrizione dei servizi previsti precedentemente fornita include alcune specifiche relative ai rapporti da emettere.

In generale si prevede l'emissione di rapporti che contengono i dati fondamentali relativi ad ogni servizio fornito ed ICP concorderà con il Fornitore, nella fase di avvio del contratto, gli specifici contenuti, la periodicità ed i formati con cui i rapporti saranno prodotti.

5.22 Supporto al progetto CRS-SISS

Il fornitore dovrà garantire idoneo supporto al processo di adesione di ICP al Progetto Regionale CRS-SISS con particolare riferimento al rispetto delle specifiche tecniche di progetto previste da Lombardia Informatica/Regione Lombardia.

Il fornitore dovrà effettuare il monitoraggio di natura sistemistica della Piattaforma Regionale del progetto SISS tramite anche strumenti che verranno messi a disposizione da Lombardia Informatica.

Il Fornitore è anche tenuto a dare supporto sistemistico a terze parti che abbiano necessità, su incarico di ICP, di installare software applicativo CRS-SISS sulle PdI.

Il Fornitore dovrà realizzare tutto il necessario per comunicare con gli altri Enti all'interno del progetto CRS-SISS (come ad esempio collegamento con Domini esterni, NAT di indirizzi, etc.)

Saranno valutate positivamente le competenze ed esperienze avute dal Concorrente nell'ambito del progetto SISS che potranno portare del valore aggiunto a ICP.

5.23 Strumenti di gestione

Il fornitore utilizzerà un sistema hardware e software messo a disposizione da ICP che includerà gli strumenti software adeguati a svolgere le seguenti funzioni:

- Gestione ticket;
- Gestione CMDB;
- Monitoraggio infrastruttura di rete;
- Monitoraggio server e applicazioni software installate sui sistemi server;
- Distribuzione software di base e applicativo.

Il sistema, con elevati requisiti di disponibilità, sarà indipendente dai sistemi ICP.

Tutti gli strumenti software (funzionalità e dati gestiti) saranno accessibili da remoto attraverso interfacce web.

Sarà cura del fornitore del lotto 1:

- Installare e rendere operativo il sistema presso la sala server ICP in modo che possa essere utilizzato anche dal personale ICP o da personale nominato da ICP;
- Mettere a disposizione il contratto di manutenzione hardware del sistema, per tutta la durata del contratto e con livelli di servizio adeguati al rispetto degli SLA contrattuali.

Il sistema sarà utilizzato sia dal fornitore del lotto 1 che dal fornitore del lotto 2 (ad esempio per gestione ticket, gestione CMDB e monitoraggio server e rete sala server).

Il sistema hardware e software di base sarà gestito dal fornitore del lotto 2.

Gli strumenti software installati sul sistema saranno gestiti dal fornitore del lotto 1.

5.24 Specifica dei livelli di servizio minimi richiesti

Il modello di specifica dei livelli di servizio è teso a garantire il mantenimento dell'alto livello di affidabilità che caratterizza i sistemi informativi ICP, con livelli di continuità del servizio superiori al 99,9%.

Il Fornitore responsabile del I^{o} lotto avrà la piena responsabilità di garantire il mantenimento dell'alto livello di servizio. Egli risponderà per ogni interruzione osservata. Il mancato

raggiungimento degli obiettivi di continuità comporta il pagamento di penali che sono dimensionate in base all'impatto rispetto all'erogazione del servizio.

Il Fornitore potrà presentare evidenze che trasferiscano la responsabilità del disservizio ad altri fornitori di ICP (ad es., Fornitore responsabile del 2° lotto, fornitori delle applicazioni, fornitori della connettività di rete). Solo nel caso in cui le evidenze consentano effettivamente il trasferimento della responsabilità in capo ad altri, il Fornitore sarà esentato dal pagamento delle penali. Nel caso non venga raggiunto un accordo sull'assunzione di responsabilità, ICP assume il ruolo di arbitro con parere vincolante.

Il modello che valuta il livello di servizio ha una struttura con tre componenti principali.

1. Il primo componente è rappresentato da un modello quantitativo che ha come obiettivo la stima della continuità del servizio erogato. Diversi servizi sono caratterizzati da diversi livelli di importanza.
2. Il secondo componente è costituito da un insieme di indicatori di livello di servizio (SLA), i quali hanno come obiettivo quello di imporre vincoli relativi alla capacità da parte del sistema di fornire una risposta pronta alle richieste di intervento e di verificare il soddisfacimento delle richieste di ICP per quanto riguarda tutte le attività che non comportino un impatto immediato sulla continuità di erogazione del servizio. Si prevedono SLA relativi ai tempi di gestione delle chiamate telefoniche verso il servizio HelpDesk, tempi per la gestione di richieste IMAC, tempi per la gestione dei traslochi. Per ogni servizio sono di seguito identificati i corrispondenti SLA minimi.
3. Il terzo componente è rappresentato dalla esecuzione di verifiche ispettive. La visita ispettiva verificherà che le modalità di attuazione del servizio soddisfino i vincoli del presente capitolato e tutti gli altri vincoli derivanti dal contratto con il Fornitore. L'obiettivo di questa attività di verifica è di tenere sotto controllo sia gli aspetti quantitativi sia quelli qualitativi.

5.24.1 Modello di valutazione della continuità del servizio

Come già attualmente in essere, la continuità del servizio sarà misurata attraverso un modello che valuta la disponibilità dei sistemi agli utenti. Il modello considera attentamente la variabilità del livello di criticità nelle diverse applicazioni e il grado di necessità di un pronto intervento nella risoluzione dei problemi. Il parametro "Peso" rappresenta la criticità di ogni attività. E' da notare che il parametro "Peso" è cumulabile e qualora un guasto pregiudichi sulla stessa PdL la esecuzione di una varietà di servizi, il valore di "Peso" da applicare sarà dato dalla somma dei diversi valori. Per quanto riguarda la prontezza di intervento, il modello specifica una "franchigia" per le attività in cui un breve periodo di non disponibilità del servizio produce un impatto limitato sull'effettivo servizio erogato. La franchigia rappresenta un valore soglia di minuti che non comporta un contributo del guasto alla misura del livello di servizio, applicabile una sola volta per data e un massimo di 15 volte per periodo mensile di valutazione mensile. Se la risoluzione del problema avviene oltre la durata della franchigia, l'intero ammontare di minuti di non disponibilità contribuirà alla misura del livello di servizio. Le attività di manutenzione che sono svolte seguendo un piano approvato da ICP non contribuiscono alla misura, purché l'esecuzione avvenga rispettando il piano concordato.

Nella tabella seguente, sono elencate le componenti del servizio, con il corrispondente peso relativo e l'eventuale franchigia. I coefficienti devono essere intesi come misurati su ciascuna PdL.

DOMINIO APPLICATIVO	PESO	TEMPO DI FRANCHIGIA (MIN)
Servizi base di infrastruttura	**114**	
Impossibilità di accesso al sistema di ticketing e ritardo nella registrazione dell'istante di inizio dei guasti/disservizi	100	
Accessibilità utenti a Internet	6	30
Posta elettronica	6	30
Antivirus	2	240
Servizi Area Sanitaria	**70**	
LIS	7	
CUP	7	
ADT	7	
Reparto	7	
Ambulatoriale	7	
PS	7	
Blocco operatorio	7	
Interfaccia HOpera-LIS	7	
Interfaccia HOpera- RIS	7	
Interfaccia HOpera-BDA/RS-SISS	7	
Servizi Area Amministrativa	**45**	
Protocollo	3	15
Portale WEB	3	15
Intranet (Share Point)	3	15
Gestione Contabile-Amministrativa (NFS)	4	
Gestione personale (giuridico-economico – 25/10)	2,5	
Gestione personale (giuridico-economico – 11/24)	5	
Gestione personale (gestione presenze WEB)	4	

DOMINIO APPLICATIVO	PESO	TEMPO DI FRANCHIGIA (MIN)
Gestione Determine	4	15
Gestione Delibere	4	15
Data Warehouse	2,5	15
Khalix	4	15
Produttività individuale	3	15
File server	3	10

Sulla base di questi domini applicativi la seguente formula stabilisce il disservizio totale sommando i disservizi dei singoli sistemi applicativi:

$$Serv = 1 - \frac{\sum_{j=1}^{n} Peso_j \left(\sum_{i=1}^{m} \beta_i \sigma_i \quad t_i \, d_i \quad \right)}{\sum_{j=1}^{n} T_j \, D_j}$$

Dove:

j = 1,n	applicativi gestiti
$Peso_j$	peso attribuito all'applicativo j
i = 1,m	eventi negativi registrati (disservizi)
β_i	Indicatore sul superamento della franchigia (0, 1)
σ_i	criticità del disservizio: 0,5 = degrado delle prestazioni (efficienza diminuita) 1 = blocco totale (non si possono completare le transazioni)
t_i	tempo di non disponibilità registrato (durata del disservizio)
d_i	numero di postazioni bloccate
T_j	Tempo complessivo di disponibilità del servizio
D_j	Numero di postazioni che erogano il servizio

A titolo d'esempio, si supponga che vi siano solo due servizi con peso 5 con franchigia di 5 minuti erogati da 1000 postazioni che sono attive 24/7. Si assuma poi che in un mese di 30 giorni si siano verificati: un guasto g1 non bloccante di 4 minuti sul primo servizio che ha coinvolto 10 postazioni, un guasto g2 non bloccante di 10 minuti sul primo servizio che ha

coinvolto 100 postazioni, e un guasto g3 bloccante di 30 minuti sul secondo servizio che ha coinvolto 20 postazioni. Il livello di servizio *Serv* sarà pari a:

1-(5 *peso* * ((0 * 0,5 σ * 4 *min* * 10 *PdL*)$_{g1}$ + (1 * 0,5 σ * 10 *min* * 100 *PdL*)$_{g2}$) + 5 *peso* * (1 * 1 σ * 30 *min* * 20 *PdL*)$_{g3}$) / (30*24*60*1000+30*24*60*1000)

= 1 – ((0 + 2500) + 3000)/86400000

= 0,9999363

E' da notare che la presenza del fattore "Peso" rende il risultato dell'applicazione della formula diverso da quello convenzionalmente adottato in ambito tecnico per valutare l'affidabilità dei sistemi.

Si osservi che per "numero di postazioni" s'intende il numero di PdL da cui uno specifico servizio può essere invocato. Ad esempio l'accesso al sistema di ticketing riguarda tutte le PdL da cui è possibile aprire un ticket via web.

5.24.2 SLA

Per ogni servizio sono di seguito identificati i corrispondenti SLA minimi.

Ogni SLA è identificato da una o più misure o da modalità di verifica. Ove non altrimenti specificato, per "ore / giorni" si intende "ore / giorni lavorativi".

<u>Servizio di gestione dei Server; Servizio di gestione del Software di base, d'ambiente e di rete; Servizio di Gestione del Backup; Servizio di gestione della sicurezza; Servizio di Gestione della Posta Elettronica e Servizio di Configuration Management (con inclusione delle attività di riparazione conseguenti a guasti non bloccanti).</u>

- Tempo massimo di esecuzione (dall'apertura alla chiusura di ticket) di una richiesta di attività IMAC (movimentazione, aggiunta, cambiamento, installazione, disinstallazione, sostituzione, dismissione) e di attività di riparazione conseguenti a guasti non bloccanti.

  giorni 1

- Rispetto del piano di esecuzione per interventi concordati con ICP:

  100% nei tempi pianificati

- Esito positivo delle verifiche ispettive.

<u>Servizio di manutenzione hardware</u>

Il servizio di manutenzione contribuirà al soddisfacimento dei livelli di servizio indicati per gli altri servizi.

- Esito positivo delle verifiche ispettive.

5.24.3 Verifiche ispettive

Nella fase di esecuzione del servizio, ICP eseguirà periodicamente e/o in specifiche occasioni un'attività di verifica ispettiva. ICP prevede di attivare una Commissione di valutazione, di norma costituita da personale ICP e da esperti esterni di terza parte. La verifica valuterà la

corretta esecuzione del servizio raccogliendo tutte le necessarie evidenze dall'operatività e dalle informazioni gestite.

La verifica produrrà un rapporto nel quale potranno essere evidenziate:

- Carenze minori,
- Non conformità,

che saranno notificate al Fornitore.

Si intende per non conformità un comportamento o uno stato del sistema di informazioni gestito che potrebbe, se non corretto, compromettere in maniera sostanziale l'efficacia e l'efficienza dei servizi forniti.

Possibili esempi di non conformità sono:

- L'evidenza che le procedure definite per la gestione dei server non sono state applicate;
- La presenza di un disallineamento significativo nel CMDB rispetto allo stato di fatto dei sistemi installati;
- La ripetuta non corretta registrazione dei ticket rispetto alle evidenze raccolte presso gli utenti del servizio (come ad esempio la chiusura di ticket anche se il problema non è stato risolto e quindi la ripetuta apertura di ticket a fronte dello stesso problema);

La visita ispettiva avrà esito positivo se:

- Il Fornitore risolverà tutte le non conformità entro 10 giorni lavorativi o ripristinando le condizioni di conformità o ponendo in atto azioni che impediscano il ripetersi della non conformità. Al termine di questo periodo sarà eseguita un'ulteriore verifica che produrrà un rapporto sullo stato di risoluzione dei problemi evidenziati.
- Il Fornitore risolverà tutte le carenze minori entro la successiva visita ispettiva.

Altrimenti la visita ispettiva avrà esito negativo.

La presenza della stessa non conformità in due successive visite ispettive determinerà l'esito negativo, anche nel caso in cui il Fornitore risolva la non conformità entro 10 giorni lavorativi.

5.24.4 Strumenti di misura dei livelli di servizio minimi richiesti

Il Fornitore del lotto 1 metterà a disposizione uno strumento software per la raccolta dei dati, il calcolo dei livelli di servizio (modello di valutazione della continuità di servizio e SLA) e la generazione del report mensile relativo.

Lo strumento garantirà la tracciabilità dei dati (provenienti dal ticketing system) in modo che i livelli di servizio calcolati siano chiaramente riconducibili ai singoli dati che li hanno originati.

Lo strumento coprirà anche la misura dei livelli di servizio riguardanti l'infrastruttura server e l'infrastruttura di rete della sala server.

Lo strumento sarà integrato con gli strumenti software di gestione ticket e di monitoraggio.

5.24.5 Report periodico per la misura dei livelli di servizio minimi richiesti

Il report mensile (comprensivo sia delle attività del lotto 1 che del lotto 2) sulla base del quale sarà possibile verificare la corrispondenza del servizio con il livello di servizio minimo richiesto (modello di valutazione della continuità del servizio) e gli SLA attesi sarà prodotto e consegnato a ICP a cura del fornitore del lotto 1.

5.25 Penali

Per ogni giorno solare di ritardo relativo al termine della fase di installazione e trasferimento (vedi paragrafo "Modalità di esecuzione della fornitura") è applicata una penale di:

1.500 (Millecinquecento) euro.

Per quanto riguarda la valutazione del livello di servizio, la tolleranza è data dal livello di servizio pari al 99,99%, così come calcolato in base alla formula sopra descritta.

Per ogni 0,1% o frazione di scostamento da tale valore per il periodo di osservazione (mensile), è applicata una penale pari allo 0,3% del canone mensile.

Per quanto riguarda il rispetto degli SLA e l'esecuzione delle verifiche ispettive, si riportano di seguito le penali che saranno applicate al Fornitore, distinte per le varie tipologie di servizi.

Servizio di gestione dei Server; Servizio di gestione del Software di base, d'ambiente e di rete; Servizio di Gestione del Backup; Servizio di gestione della sicurezza; Servizio di Gestione della Posta Elettronica e Servizio di Configuration Management (con inclusione delle attività di riparazione conseguenti a guasti non bloccanti).

Superamento dello SLA relativo al tempo massimo di soluzione di un ticket per tre volte in un mese di calendario:

10.000 (Diecimila) euro

Mancato rispetto della pianificazione per interventi concordati con ICP:

10.000 (Diecimila) euro

Esito negativo di una visita ispettiva:

10.000 (Diecimila) euro

Nel caso di perdite di dati causate da negligenza del fornitore, ICP potrà rivalersi nei confronti del Fornitore per i danni subiti.

Nel caso di danni derivanti da problemi di sicurezza causati da negligenza del fornitore, ICP potrà rivalersi nei confronti del Fornitore per i danni subiti.

ICP potrà condurre una visita ispettiva relativa ad uno o più servizi. Nel caso in cui una singola visita ispettiva generi un esito negativo relativo a più servizi, la penale sarà applicata una sola volta.

ICP si riserva il diritto di dichiarare non compatibile il servizio e di procedere alla risoluzione del contratto dopo l'applicazione di 3 (tre) penalità derivanti dal mancato rispetto degli SLA o da esito negativo delle visite ispettive.

5.26 Struttura organizzativa

Sono di seguito definite la struttura organizzativa, i ruoli e le responsabilità del personale del Fornitore e le modalità di interazione con ICP.

5.26.1 Struttura e responsabilità

Il servizio sarà fornito attraverso un gruppo di lavoro che opererà durante l'orario di copertura del servizio.

Il gruppo di lavoro sarà costituito da personale di competenza adeguata alla fornitura dei vari servizi.

Il gruppo di lavoro sarà coordinato e dipenderà da un Responsabile Operativo nominato dal Fornitore.

Il Responsabile Operativo farà parte del gruppo di lavoro del Fornitore ed opererà durante l'orario di copertura del servizio.

ICP nominerà un Responsabile ICP che opererà come unico referente ICP del Responsabile Operativo. Il Responsabile Operativo del Fornitore costituirà l'unico referente del gruppo di lavoro nei confronti del Responsabile ICP.

Relativamente ad attività di verifica degli SLA contrattuali ed in generale della qualità e del buon andamento dei servizi, ICP potrà avvalersi di terze parti che opereranno per conto di ICP.

Il Fornitore nominerà un Responsabile di contratto che opererà come referente degli aspetti contrattuali complessivi (valutazione complessiva dell'esecuzione del contratto, aspetti amministrativi e legali) nei confronti del corrispondente Responsabile di contratto ICP o suo delegato.

5.26.2 Dimensione e caratteristiche del gruppo di lavoro

Il gruppo di lavoro sarà costituito da un insieme di figure professionali adeguate a coprire i vari ruoli necessari per svolgere i servizi inclusi nel contratto.

Sarà cura del Concorrente offrire il dimensionamento del gruppo di lavoro e descrivere caratteristiche e ruoli coperti in accordo con i criteri esposti in "Caratteristiche del personale".

Certificazioni attinenti ai servizi che costituiscono il contratto, relative all'azienda concorrente saranno considerati durante la valutazione.

5.26.3 Sostituzione del personale

E' responsabilità del Fornitore sostituire il personale assente dal servizio per qualsivoglia motivo (ad esempio per malattia) con personale di equivalente profilo professionale.

ICP si riserva, a suo insindacabile giudizio e senza giustificazione, di richiedere per scritto ed ottenere la sostituzione di personale del gruppo di lavoro (incluso il Responsabile Operativo) con personale equivalente per ruolo, profilo professionale, certificazioni e curriculum.

5.27 Modalità di esecuzione della fornitura

L'esecuzione della fornitura si svilupperà attraverso le seguenti fasi:

- Fase di installazione e trasferimento.

  Durata: 40 gg lavorativi decorrenti dalla scadenza del termine dilatorio previsto all'art. 11 comma 10 del D. Lgs. 163/2006 e ss.mm.ii. (pari a 35 giorni solari dall'invio dell'ultima delle comunicazioni del provvedimento di aggiudicazione definitiva);

- Fase di avvio.

  Durata: 40 gg lavorativi dal termine della fase di installazione e trasferimento.

- Fase di esercizio.

  Durata: dal termine della fase di avvio al termine del periodo contrattuale.

- Fase di transizione finale.

  Durata: gli ultimi 60 gg lavorativi prima della scadenza del periodo contrattuale o comunque del termine del rapporto contrattuale (qualunque ne sia la causa).

5.27.1 Fase di installazione e trasferimento

La fase d'installazione e trasferimento include tutte le attività svolte dal Fornitore al fine di installare i sistemi e prendere carico dei servizi affiancando il personale ICP e gli attuali fornitori.

ICP sarà a supporto per ogni aspetto relativo all'interazione con le strutture e gli impianti esistenti in sala server.

Le attività saranno pianificate in accordo con le seguenti fasi:

1. Installazione

   Il fornitore installa tutti i sistemi hardware, software di base, software d'ambiente e software di rete. Il fornitore, in collaborazione con gli specifici fornitori, installa tutte le applicazioni software e le basi di dati attualmente in produzione. Al termine dell'attività la nuova sala server sarà in grado di operare come ambiente di test funzionalmente equivalente all'ambiente al momento in produzione.

2. Test

   Il fornitore definisce un piano di test funzionale per ogni applicazione / sistema che verifichi il funzionamento dal punto di vista sistemistico (installazione, interoperabilità tra i server coinvolti, accesso dai client, prestazioni). Il piano è approvato da ICP ed eseguito dal fornitore. ICP approva i risultati autorizzando il passaggio in produzione di ogni applicazione / sistema.

3. Avvio in produzione

   Il fornitore e ICP concordano un piano di passaggio progressivo in produzione delle applicazioni / sistemi e delle basi dati in modo che non si abbia interruzione di servizio. A questo fine le attività di avvio in produzione potranno essere eseguite fuori dall'orario di

servizio al di fuori dell'ammontare globale previsto per la durata del contratto (si veda il capitolo "Orari di copertura dei servizi"). Il fornitore prende in carico il livello di servizio minimo richiesto (modello di valutazione della continuità del servizio) e lo SLA relativo per ogni applicazione che entra in produzione.

5.27.2 Fase di avvio

Al termine della fase di installazione e trasferimento il gruppo di lavoro del fornitore sarà in grado di prendersi carico completamente dei servizi ed il fornitore assumerà piena ed esclusiva responsabilità della gestione dei servizi.

Il fornitore, per il solo fatto di partecipare alla presente gara, si obbliga ad accettare di garantire il servizio per tutte le componenti dell'infrastruttura ICT, così come identificate nelle loro caratteristiche essenziali (ma non esaustive) negli Allegati per tutta la durata contrattuale, nello stato in cui si trovano all'atto dell'affidamento del servizio, senza opporre alcuna riserva in merito allo stato degli impianti, degli apparati, dei sistemi e dei terminali, sulle versioni hardware e/o software, sui modelli e/o versioni degli stessi, nonché sul livello di aggiornamento della documentazione associata.

Il Fornitore è consapevole che quanto specificato nel presente documento (inclusi gli Allegati) identifica il dimensionamento dell'infrastruttura e non il dettaglio dello stato di fatto.

Con la presa in consegna degli impianti, il Fornitore assume le responsabilità previste dalle vigenti normative e dal presente Contratto ed è responsabile della buona e diligente conservazione del materiale ricevuto, rispondendo nei confronti dell'Amministrazione e di terzi per l'eventuale incuria o negligenza sulla gestione e conduzione degli impianti, nell'uso della documentazione e delle modalità di accesso fisico e logico agli apparati.

Il Fornitore eseguirà tutte le operazioni di censimento ed il caricamento del CMDB.

Il Fornitore concorderà con ICP l'insieme delle procedure operative che dovranno descrivere le modalità di esecuzione dei servizi e le regole connesse (ad esempio le procedure di incident management, change management, backup, disaster recovery, security management). L'insieme di tali procedure sarà utilizzato come riferimento operativo durante l'erogazione dei servizi e riferimento di controllo durante le verifiche ispettive.

Il fornitore scriverà le procedure concordate che saranno sottoposte ad approvazione da parte di ICP.

Il fornitore metterà in esercizio tutte le procedure operative necessarie.

Il Fornitore opererà sulla base del livello di servizio minimo richiesto (modello di valutazione della continuità del servizio) e degli SLA definiti che saranno misurati / valutati.

In questa fase le visite ispettive non valuteranno gli aspetti relativi al caricamento del CMDB ed alle procedure operative.

Il questa fase, ICP collaborerà con il Fornitore al fine di raggiungere la piena operatività.

5.27.3 Fase di esercizio

Il Fornitore opererà sulla base del livello di servizio minimo richiesto (modello di valutazione della continuità del servizio) e degli SLA definiti che saranno misurati / valutati.

Le visite ispettive valuteranno tutti gli aspetti.

5.27.4 Fase di transizione finale

In questa fase il Fornitore si impegna, oltre che a fornire il servizio contrattualmente dovuto, ad affiancare ICP o un nuovo Fornitore indicato da ICP, che subentrerà nella gestione, trasferendo tutta l'informazione e le procedure di gestione in essere in modo da permettere un ordinato ed efficiente passaggio di consegne.

Alla scadenza del contratto, ICP ed il Fornitore procederanno alla visita degli impianti per accertare la buona conservazione degli stessi, nonché per accertare l'adempimento da parte del Fornitore degli obblighi contrattuali.

Qualora il Fornitore non dovesse intervenire alle operazioni di riconsegna entro dieci giorni dalla data di comunicazione dell'inizio delle operazioni di riconsegna, si procederà comunque alle operazioni alla presenza di un testimone.

Le operazioni di verifica saranno avviate almeno 30 (trenta) giorni prima del termine fissato per l'ultimazione del servizio e saranno ultimate entro la data di scadenza dello stesso.

Il Fornitore si renderà disponibile ad intervenire su richiesta per piccoli interventi per un periodo di ulteriori 2 (due) mesi dopo la scadenza del contratto.

Il Fornitore cederà in proprietà ad ICP tutte le parti di ricambio installate nel corso del periodo contrattuale.

6 PARTE II – CONDIZIONI GENERALI DEL CONTRATTO

6.1.1 Clausola di salvaguardia

Nel caso in cui durante il periodo di vigenza del contratto – in relazione ad eventuali provvedimenti delle competenti autorità regionali – l'assetto strutturale dell'A.O. dovesse subire ulteriori modificazioni mediante lo scorporo di una o più strutture (sia ospedaliere che territoriali) interessate al servizio oggetto del presente Capitolato, l'appaltatore si obbliga sin d'ora a proseguire il servizio a favore dell'ente assegnatario delle strutture alle stesse condizioni contrattuali, salva la facoltà dell'ente stesso di recedere dal contratto previa comunicazione, a mezzo lettera A/R entro 6 mesi dalla data di efficacia del provvedimento che dispone la modifica strutturale. Resta inteso che all'appaltatore saranno riconosciute le prestazioni già eseguite.

6.1.2 Responsabilità civile, copertura assicurativa

La ditta appaltatrice risponderà direttamente di ogni danno a cose e/o persone che, per fatto proprio o del proprio personale, possa derivare all'Azienda Ospedaliera ed a terzi nell'espletamento del servizio, anche in relazione all'operato e alla condotta dei propri collaboratori e/o di personale di altre imprese a diverso titolo coinvolte.

La ditta appaltatrice dovrà contrarre apposita polizza d'assicurazione che preveda la copertura dei rischi relativi per un importo non inferiore a euro 2.500.000,00 (euro) per sinistro. Ogni documento assicurativo dovrà essere prodotto in copia all'A.O. ICP a semplice richiesta.

L'Azienda Appaltante sarà esonerata da ogni responsabilità per danni, infortuni o altro che dovessero accadere al personale di cui si avvarrà a qualsiasi titolo l'appaltatore nell'esecuzione del contratto , convenendosi a tale riguardo che qualsiasi eventuale onere è già compensato e compreso nel corrispettivo del contratto

Non sarà neppure responsabile dei danni diretti o indiretti che l'appaltatore dovesse subire in conseguenza di un fatto doloso o colposo di terzi, compresi i dipendenti dell'A.O. ICP, in particolare, in conseguenza di furti.

L'Impresa aggiudicataria è sottoposta a tutti gli obblighi verso i propri dipendenti risultanti dalle disposizioni legislative e regolamentari in materia di lavoro e di assicurazioni sociali ed assume a suo carico tutti gli oneri relativi.

L'Impresa è responsabile dell'esatto adempimento delle condizioni dell'appalto e della perfetta riuscita del servizio.

Il rispetto delle scadenze temporali previste è condizione indispensabile a garanzia della regolare realizzazione ed espletamento dell'attività contrattuale.

L'aggiudicatario inoltre è responsabile dell'osservanza di tutte le disposizioni emanate da qualunque autorità comunitaria, governativa, regionale o municipale, nonché di danni comunque arrecati alle persone ed alle cose sia dell'Amministrazione che di terzi.

L'Impresa aggiudicataria è direttamente responsabile della regolare esecuzione del servizio e ne risponde civilmente, penalmente ed amministrativamente per eventuali fatti illeciti e conseguenti danni causati dalla medesima o dal suo personale.

6.1.3 Deposito cauzionale

Ai sensi dell'art. 113, comma 1, del D.Lgs. n. 163/2006, l'aggiudicatario del contratto è obbligato a costituire una garanzia fideiussoria (fideiussione bancaria o polizza assicurativa) di importo pari al 10% dell'importo contrattuale (iva esclusa). La garanzia di cui sopra deve prevedere espressamente:

- la rinuncia al beneficio della preventiva escussione del debitore principale;
- la rinuncia all'eccezione di cui all'art.1957, comma 2 del codice civile;
- la operatività della garanzia entro 15gg, a semplice richiesta scritta dell'Azienda Ospedaliera.

La garanzia è progressivamente svincolata in misura dell'avanzamento dell'esecuzione del contratto, sino al limite massimo del 75% dell'importo iniziale.

La progressione dello svincolo è a cadenza annuale come di seguito esposto:

1 anno 100%

2 anno 80%

3 anno 60%

4 anno 40%

5 anno 20%

A richiesta dell'aggiudicatario, l'Azienda Appaltante rilascerà, qualora non vi siano motivi ostativi, idoneo documento – da consegnare all'istituto garante – comprovante lo stato di avanzamento dell'esecuzione del contratto.

L'ammontare residuo della garanzia è svincolato al termine del contratto, alla data di emissione del certificato di regolare esecuzione del servizio, da effettuarsi normalmente, entro 90 giorni da detta scadenza. Il termine per l'emissione del certificato di regolare esecuzione, rimane sospeso in caso di contestazioni sul servizio da parte dell'Azienda Appaltante, opportunamente comunicati all'aggiudicatario. Il termine ricomincia a decorrere dalla data di definizione della contestazione.

Il deposito cauzionale definitivo è prestato a garanzia dell'adempimento di tutte le obbligazioni del contratto, del risarcimento di eventuali danni derivanti dall'inadempimento, parziale o totale, delle obbligazioni, nonché del rimborso all'A.O. ICP delle somme che questi abbia eventualmente pagato in più, durante l'esecuzione del servizio, in confronto all'effettivo credito del fornitore.

La cauzione provvisoria sarà restituita dopo la consegna della cauzione definitiva.

Nell'attesa della cauzione definitiva, l'Azienda Ospedaliera potrà rivalersi, per le inadempienze contrattuali dell'aggiudicatario, anche sulla cauzione provvisoria e/o sulle fatture in attesa di liquidazione.

Nessun interesse è dovuto sulle somme costituenti i depositi cauzionali.

6.1.4 Cessione del contratto, del credito e subappalto

Il contratto non può essere ceduto, a pena di nullità fatto salvo quanto previsto dall'art.116 del D. Lgs. n. 163/2006.

La cessione del credito dell'aggiudicatario, di cui all'art.1260 c.c. e seguenti, è regolata dalle disposizioni di cui all'art. 117 del D.Lgs. n.163/2006.

Ai sensi dell'art.118, comma 2, del D.Lgs. n.163/2006, l'aggiudicatario non potrà cedere a terzi il contratto, o comunque dare in subappalto parte del servizio (comunque non superiore al 30%), senza la preventiva autorizzazione scritta dell'Azienda Appaltante.

Quanto sopra alle seguenti condizioni:

- L'aggiudicatario dovrà avere indicato, in sede di offerta, la propria intenzione a ricorrere al subappalto, con specificazione dei servizi, forniture o parti di servizi o forniture che intende subappaltare (art. 118, comma 2, punto 1) D.Lgs. n. 163/2006);
- L'aggiudicatario provvederà al deposito del contratto di subappalto (cui è da allegare dichiarazione circa la sussistenza o meno di eventuali forme di controllo o di collegamento ex art. 2359 del codice civile con il titolare del subappalto) presso l'Azienda, almeno venti giorni prima della data di inizio delle relative prestazioni, con contestuale trasmissione:
  a) Della certificazione attestante il possesso, da parte del subappaltatore, dei requisiti di qualificazione prescritti in relazione alla prestazione subappaltata (art. 118, comma 2, punto 3) D. Lgs. n. 163/2006);
  b) Dichiarazione del subappaltatore attestante il possesso dei requisiti di ordine generale di cui all'art. 38 del D. Lgs. n. 163/2006;
- Insussistenza, in capo al subappaltatore, di divieti previsti dalla vigente legislazione antimafia (art. 10 della legge 31 maggio 1965, e ss. mm.) (art. 118, comma 2, punto 4) D. Lgs. n. 163/2006).

Ai sensi dell'art. 3, comma 9, della Legge 13 agosto 2010 n. 136, e ss.mm.ii. nei contratti sottoscritti con i subappaltatori e i subcontraenti della filiera delle imprese a qualsiasi titolo interessate ai lavori, ai servizi e alle forniture inerenti l'esecuzione del contratto di cui al presente appalto deve essere inserita, a pena di nullità assoluta, un'apposita clausola con la quale ciascuno di essi assume gli obblighi di tracciabilità dei flussi finanziari di cui alla citata Legge.

Gli obblighi inerenti la tracciabilità dei flussi finanziari previsti dalla Legge n. 136/2010 gravano, pertanto, anche sui soggetti subappaltatori o subcontraenti, i quali sono tenuti, nel caso in cui abbiano notizia dell'inadempimento della propria controparte agli obblighi di

tracciabilità finanziaria, a procedere all'immediata risoluzione del rapporto contrattuale, informandone contestualmente la Stazione Appaltante e la Prefettura-ufficio territoriale del Governo territorialmente competente (art. 3, comma 8, della L. 136/2010).

L'autorizzazione al subappalto è rilasciata dall'Azienda entro trenta giorni (art. 118, comma 8 D. Lgs. n. 163/2006) dalla richiesta, subordinatamente alla completezza e regolarità della documentazione fornita. Per subappalti di importo inferiore al 2 per cento dell'importo contrattuale o di importo inferiore a 100.000 €uro, detto termine è dimezzato (art. 118, comma 8 D. Lgs. n. 163/2006).

L'aggiudicatario e, per suo tramite, i subappaltatori trasmettono all'Azienda prima dell'avvio del servizio la documentazione di avvenuta denuncia agli enti previdenziali, nonché copia del piano di sicurezza.

Ai fini del pagamento degli stati di avanzamento dei lavori o dello stato finale dei lavori, all'affidatario e, per suo tramite, ai subappaltatori, l'Azienda Appaltante provvederà all'acquisizione d'ufficio del DURC documento unico di regolarità contributiva.

L'A.O. ICP provvederà al pagamento delle prestazioni eseguite dal subappaltatore all'aggiudicatario del servizio. E' fatto obbligo al fornitore di trasmettere, entro venti giorni dalla data di ciascun pagamento copia delle fatture quietanzate relative ai pagamenti da essi corrisposti al subappaltatore, con indicazione delle ritenute di garanzia effettuate (art. 118, comma 3, D. Lgs. n. 163/2006).

L'A.O. provvederà al pagamento all'aggiudicatario del corrispettivo dovuto al subappaltatore previa esibizione, da parte di quest'ultimo, della documentazione attestante che l'effettuazione e versamento delle ritenute fiscali sui redditi di lavoro dipendente e del versamento dei contributi previdenziali e dei contributi assicurativi obbligatori per gli infortuni sul lavoro e le malattie professionali dei dipendenti, a cui è tenuto il subappaltatore in relazione all'opera, servizio o fornitura affidati, sono stati correttamente eseguiti (art. 35, commi 28 e 32 D.L. 04 luglio 2006, n. 223 – convertito con legge 04 agosto 2006, n. 248). L'Azienda può sospendere il pagamento del corrispettivo di cui trattasi fino all'esibizione della predetta documentazione; tale situazione interrompe i termini per il pagamento, di cui all'art. 14 del presente Capitolato.

La partecipazione alla gara comporta, di regola, l'esclusione della possibilità, per i soggetti concorrenti, di essere successivamente autorizzati ad assumere la veste di subappaltatori.

L'esecuzione delle prestazioni affidata in subappalto non può formare oggetto di ulteriore subappalto (art. 118, comma 9, D. Lgs. n. 163/2006).

6.1.5 Scioperi e cause di forza maggiore

Trattandosi di servizio di pubblica utilità, nel caso di scioperi o di assemblee sindacali interne e/o esterne, si rimanda a quanto previsto dalla Legge 146/90, che prevede l'obbligo di assicurare i servizi minimi essenziali secondo le intese definite dal CCNL e dai contratti decentrati a livello nazionale per quanto concerne i contingenti di personale.

La Ditta pertanto, applicherà in detti casi, il proprio piano operativo – illustrato nel progetto tecnico di offerta – necessario a garantire i servizi minimi essenziali, previ accordi con il Servizio Informatico Aziendale dell'Azienda Ospedaliera .

Pertanto, in caso di scioperi o di agitazioni del proprio personale, la ditta aggiudicataria deve darne tempestiva comunicazione scritta all'Azienda Appaltante, con almeno 72 ore di anticipo, segnalando la data effettiva dello sciopero programmato e/o la data dell'assemblea sindacale interna e/o esterna.

La Ditta dovrà garantire, anche in tali circostanze, la reperibilità del suo rappresentante o delegato.

L'Azienda Ospedaliera si riserva la facoltà di trattenere un importo forfettario, per la prestazione non eseguita.

Qualora, al verificarsi di cause di forza maggiore, il servizio di emergenza non risultasse idoneo a soddisfare le esigenze dell'Azienda Ospedaliera, quest'ultima provvederà allo svolgimento dello stesso nel modo che riterrà più opportuno, riservandosi di addebitare alla Ditta inadempiente il maggior onere sostenuto.

Le parti non saranno ritenute inadempienti qualora l'inosservanza degli obblighi derivanti dal contratto sia dovuto a forza maggiore,

Con l'espressione forza maggiore si fa riferimento a titolo indicativo, a guerre, insurrezioni, disordini, catastrofi, epidemie e, in genere, a qualunque altro evento che sfugga alla volontà delle parti e che sia imprevedibile anche mediante l'uso della necessaria diligenza (non rientrano in tale fattispecie gli eventi atmosferici ordinari tipo nevicate etc.).

Verificatosi un caso di forza maggiore che impedisca ad una parte l'esatta e puntuale osservanza degli obblighi contrattuali, la stessa è tenuta a darne tempestiva comunicazione all'altro contraente, indicando anche il tempo prevedibile di impedimento.

La parte che non ha potuto adempiere, per causa di forza maggiore, ha diritto ad una proroga dei termini in misura pari alla durata dell'evento impeditivo.

Tuttavia, qualora la forza maggiore duri più di 60 giorni continuativamente, ciascuna parte, con preavviso di 30 giorni, avrà facoltà di procedere alla risoluzione del contratto.

6.1.6 Risoluzione del contratto e disdetta del contratto

L'A.O. può richiedere la risoluzione del contratto nei seguenti casi:

a) in qualsiasi momento dell'esecuzione, avvalendosi della facoltà consentita dall'art. 1671 del codice civile, tenendo indenne la ditta dalle spese sostenute, dai servizi eseguiti, dai mancati guadagni;

b) per sopravvenuti gravi motivi di interesse pubblico; in tal caso l'A.O. sarà tenuta al pagamento delle prestazioni regolarmente eseguite ai prezzi del contratto;

c) in ottemperanza alle disposizioni di cui all'art. 3, c. 8, della Legge 13 agosto 2010 n. 136 e ss.mm.ii., il contratto d'appalto si intenderà risolto di diritto, ai sensi e per gli effetti dell'art. 1456 cc., nel caso in cui le transazioni siano state eseguite senza l'utilizzo del

bonifico bancario o postale ovvero degli altri strumenti idonei a consentire la piena tracciabilità delle operazioni;

d) in caso di grave negligenza e di contravvenzione nell'esecuzione degli obblighi e condizioni contrattuali, tali da compromettere la regolare esecuzione del servizio ed ove siano state applicate almeno 3 penalità, a meno che la gravità dell'inadempimento non sia tale da configurare, di per sé, giusta causa di risoluzione;

e) quando a carico dell'affidatario sia stata emessa sentenza penale di condanna passata in giudicato per frode, o per qualsiasi reato che incida sulla sua moralità professionale, o per delitti finanziari, o per contravvenzione alle disposizioni di cui al D.Lgs. 231/2001;

f) in caso di cessione dell'azienda, di cessazione dell'attività, oppure nel caso di concordato preventivo, di fallimento e di atti di sequestro o di pignoramento a carico dell'aggiudicatario;

g) in caso di cessione del contratto e/o di subappalto non autorizzato;

h) nei casi di morte dell'aggiudicatario, quando la considerazione della sua persona sia motivo determinante dell'aggiudicazione;

i) inadempimento degli oneri ed obblighi previsti a carico dell'aggiudicatario in favore dei propri dipendenti;

j) in caso di violazioni del Codice Etico aziendale e del Codice etico degli appalti regionali

Ove l'A.O. ICP ravvisi la sussistenza di una delle cause sopra descritte, dalla lettera d) alla lettera j), procederà alla contestazione per iscritto all'Aggiudicatario con la prefissione di un termine non inferiore a 20 giorni per le controdeduzioni. Decorso tale termine l'A.O. adotterà le determinazioni ritenute più opportune.

Per qualsiasi ragione si addivenisse alla risoluzione del contratto, l'Aggiudicatario – ad eccezione delle ipotesi di cui alle lettere a), b) e h) - oltre a incorrere nell'immediata perdita del deposito cauzionale a titolo di penale, sarà tenuto al completo risarcimento di tutti i danni diretti ed indiretti ed al rimborso delle maggiori spese che l'A.O. dovesse affrontare per il rimanente periodo contrattuale.

Per quanto non contemplato nel presente capitolato, si fa riferimento alla normativa vigente con particolare riferimento agli artt. 1452 e seguenti del codice civile.

Qualora l'Aggiudicatario dovesse disdettare il contratto prima della scadenza convenuta, l'A.O. tratterrà senz'altro a titolo di penale, il deposito cauzionale ed addebiterà, inoltre le maggiori spese comunque derivanti per l'assegnazione del servizio ad altra ditta, a titolo di risarcimento danni. L'Aggiudicatario sarà comunque tenuto ad effettuare una comunicazione a mezzo raccomandata A/R all'A.O. e la disdetta avrà effetto decorsi 6 mesi dal ricevimento della stessa.

Nel caso di fallimento dell'Aggiudicatario, il contratto si riterrà risolto a pieno diritto a datare dal giorno della dichiarazione di fallimento, salva la facoltà dell'A.O. di ricorrere ad azione di rivalsa sulla cauzione e sui crediti maturati per tutte le eventuali ragioni di danni.

In caso di morte del fornitore le obbligazioni derivanti dal contratto saranno assunte solidalmente dagli eredi, riservandosi comunque l'A.O. la facoltà di ritenere risolto il contratto per colpa dell'Aggiudicatario e quindi con incameramento del deposito cauzionale.

6.1.7 Codice etico aziendale e Codice etico regionale degli appalti

La ditta, nei rapporti inerenti al presente contratto, s'impegna ad osservare tutte le disposizioni e ad ottemperare a tutti i principi contenuti nel Codice Etico adottato dall'A.O. ICP e pubblicato sul sito www.icp.mi.it

La ditta aggiudicataria s'impegna, altresì, a rispettare tutte le disposizioni e ad ottemperare a tutte le obbligazioni contenute nel "Codice etico degli appalti regionali", approvato con DGR Regione Lombardia 4 maggio 2011, n. IX/1644.

La ditta è pertanto consapevole che eventuali proprie violazioni del Codice Etico aziendale e del Codice etico degli appalti regionali costituiscono causa espressa di risoluzione del rapporto contrattuale, ai sensi e per gli effetti dell'art. 1546 c.c., fatto salvo ogni ulteriore diritto al risarcimento per i danni che ne dovessero conseguire.

6.1.8 Tracciabilità dei flussi finanziari

La Ditta aggiudicataria, conformemente a quanto previsto dall'art. 3, L. 13 agosto 2010, n. 136 e ss.mm.ii., si impegna ad utilizzare uno o più conti correnti bancari o postali, accesi presso banche o presso la società Poste Italiane SpA, dedicati, anche non in via esclusiva, alle commesse pubbliche, ivi compresa quella oggetto della presente procedura di gara. Gli estremi identificativi del/i conto/i corrente/i dedicato/i saranno comunicati alla Stazione Appaltante in occasione della sottoscrizione del contratto, unitamente alle generalità e al codice fiscale delle persone delegate ad operare su di essi. In ogni caso, ogni variazione dovrà essere comunicata alla Stazione Appaltante entro 7 gg. dall'accensione del nuovo conto corrente dedicato.

Tutti i movimenti finanziari relativi all'esecuzione del contratto oggetto della presente procedura di gara – ivi compresi i pagamenti destinati a dipendenti, consulenti e fornitori di beni e servizi rientranti tra le spese generali nonché quelli destinati all'acquisto di immobilizzazioni tecniche – devono essere registrati sui conti correnti dedicati e, salvo quanto previsto al comma 3 della citata Legge, devono essere effettuati tramite lo strumento del bonifico bancario o postale, ovvero con altri strumenti di pagamento idonei a consentire la piena tracciabilità delle operazioni.

Ai fini della tracciabilità dei flussi finanziari, ciascun bonifico bancario o postale deve riportare, in relazione a ciascuna transazione posta in essere, il Codice Identificativo Gara (CIG) relativo al contratto oggetto della presente procedura di gara, fornito dalla Stazione Appaltante.

Il mancato utilizzo del bonifico bancario o postale ovvero degli altri strumenti idonei a consentire la piena tracciabilità delle operazioni determina la risoluzione di diritto del contratto.

La Ditta aggiudicataria prende atto della circostanza che gli obblighi inerenti la tracciabilità di cui ai commi precedenti, gravano, altresì, sui soggetti subappaltatori o a qualsiasi titolo subcontraenti dei soggetti appaltatori, i quali sono tenuti, nel caso in cui abbiano notizia dell'inadempimento della propria controparte agli obblighi di tracciabilità finanziaria, a procedere a darne immediata comunicazione all'A.O. contraente e alla Prefettura – Ufficio territoriale del Governo di Milano.

6.1.9 Fatturazione e pagamenti

L'Azienda aggiudicataria provvederà ad emettere fattura con cadenza mensile, entro il giorno 15 del mese successivo al mese preso in considerazione.

Le fatture dovranno essere intestate a:

Azienda Ospedaliera
ISTITUTI CLINICI DI PERFEZIONAMENTO
Via Castelvetro n. 22 - 20154 Milano
Cod. Fiscale 80031750153 - Part. IVA 04408300152

Il prezzo pattuito per il servizio è comprensivo di tutte le retribuzioni del personale e relativi oneri riflessi, di tutto il materiale, degli automezzi, d'ogni altra attrezzatura necessaria allo svolgimento del servizio, nonché d'ogni onere in proposito che non sia espressamente escluso.

Ai sensi del combinato disposto dell'art.4 comma 4 e dell'art. 7 del D. Lgs. 231/2002, le Parti nell'ambito della propria libertà contrattuale stabiliscono che il pagamento delle fatture sarà effettuato dall'A.O. entro 60 giorni dal ricevimento della relativa fattura, purchè non vi siano motivi ostativi. Per individuare la data di decorrenza del pagamento, si farà riferimento alla data di ricevimento della fattura presso l'Ufficio Protocollo Generale dell'Azienda Ospedaliera.

In conformità alle disposizioni di cui all'art. 3 della L. 136/2010, il pagamento delle fatture verrà effettuato dall'Azienda Appaltante sul conto corrente bancario o postale dedicato, anche non in via esclusiva, alle commesse pubbliche, i cui estremi identificativi saranno comunicati dall'appaltatore a seguito aggiudicazione dell'appalto.

L'U.O. Provveditorato Economato, previa acquisizione dell'attestato di regolare esecuzione del servizio da parte del Servizio Informatico Aziendale, procederà alla liquidazione della fattura.

La liquidazione delle fatture resta, comunque, subordinata al rispetto integrale da parte della Ditta aggiudicataria del presente Capitolato speciale, del contratto e di tutte le eventuali integrazioni pattizie intervenute in corso di vigenza del contratto e debitamente documentate; in caso contrario, il termine sopra indicato rimane sospeso, a favore dell'Azienda Ospedaliera, fino alla rimozione totale dell'impedimento da parte del fornitore.

Il pagamento delle fatture non contestate libera l'A.O. da qualsiasi rivendicazione economica dell'Appaltatore.

In caso di ritardo dei pagamenti, il saggio di eventuali interessi moratori sarà pari, in ragione d'anno, al saggio degli interessi legali stabilito dall'art. 1284, 1° comma , del codice civile. Si da atto, che la suddetta regolamentazione, in relazione alla corretta prassi commerciale, alla natura del servizio oggetto del contratto, alla condizione dei contraenti ed ai rapporti commerciali, risulta equa.

Si precisa che, in ogni caso, il ritardato pagamento non può essere invocato come motivo per la risoluzione del contratto, o per l'interruzione del servizio da parte della ditta aggiudicataria, la quale è tenuta a continuare il servizio sino alla scadenza naturale del contratto.

6.1.10 Revisione prezzi

Il corrispettivo, determinato in sede di gara, si intende esaustivo di tutte le prestazioni richieste al fornitore e resta fisso e invariabile per tutta la durata contrattuale. L'imposta sul valore aggiunto è a carico dell'Azienda Ospedaliera.

La revisione prezzi non si applica alle prestazioni rese nel corso dei primi dodici mesi, ma si applica esclusivamente (qualora la successiva istruttoria condotta dall'ufficio competente dimostri che essa è dovuta) alle prestazioni rese dopo la data di ricezione della richiesta revisionale da parte dell'Azienda Ospedaliera, a tal scopo farà fede il timbro di ricevimento posto dall'ufficio protocollo dell'A.O. ICP.

Sarà, pertanto, onere dell'appaltatore inviare circostanziata e documentata istanza revisionale. La prima istanza di revisione potrà essere presentata alla scadenza del primo anno di contratto.

La revisione viene operata sulla base di un'istruttoria, condotta dal predetto ufficio, con riferimento ai costi standardizzati determinati e pubblicati – ai sensi dell'art. 7, comma 4, lett. c) del D.Lgs. n. 163/2006 – dall' "Osservatorio dei contratti pubblici relativi a lavori, servizi e forniture" di cui all'art. 7 del citato D.Lgs., nonché sulla base degli elenchi dei prezzi rilevati dall'ISTAT e pubblicati, con cadenza almeno semestrale, sulla Gazzetta Ufficiale della Repubblica Italiana ai sensi del comma 5 dell'art. 7 del D.Lgs. n. 163/2006.

In assenza dei dati di cui al comma precedente, fatte salve emanande nuove disposizioni in materia, per il calcolo del compenso revisionale si utilizzeranno gli indici ISTAT dei prezzi al consumo per le famiglie di operai ed impiegati, pubblicati sulla Gazzetta Ufficiale della Repubblica Italiana; il mese iniziale di riferimento sarà quello di avvio dell'esecuzione del servizio.

6.1.11 Obblighi dell'Impresa aggiudicataria

L'Impresa è ben consapevole di stipulare un contratto con una Struttura Pubblica e pertanto non potrà accampare qualsivoglia scusa, compreso il ritardato pagamento, per ritardare o non ottemperare alla fornitura e/o prestazione in tutto o in parte.

Tale inadempimento comporta, oltre agli eventuali rilievi contemplati dal Codice Civile, anche eventuali violazioni, nel caso ne ricorressero gli estremi, di carattere penale quale interruzione di pubblico servizio (art. 331 e seguenti c.p.).

L'Impresa dovrà garantire la continuità del servizio, e collaborare con l'Azienda Ospedaliera ICP e, nella fase transitoria iniziale, con il precedente gestore, al fine di evitare interruzioni dello stesso.

L'Impresa si obbliga ad eseguire le prestazioni oggetto del contratto a perfetta regola d'arte e nel rispetto di tutte le norme e prescrizioni, anche tecniche e di sicurezza, in vigore e di quelle che dovessero essere emanate nel corso di durata del contratto, nonché secondo le condizioni, le modalità, i termini e le prescrizioni contenute nel contratto.

L'Impresa si impegna ad eseguire le attività contenute e le modalità indicate nelle Disposizioni Tecniche del presente Capitolato o secondo quelle diversamente concordate tra le Parti.

L'Impresa si obbliga a rispettare tutte le indicazioni relative all'esecuzione contrattuale che dovessero essere impartite dall'Azienda Ospedaliera ICP.

L'Impresa si obbliga a dare immediata comunicazione all'Azienda Ospedaliera ICP di ogni circostanza che abbia influenza sull'esecuzione del contratto e di comportarsi con buona fede e correttezza.

6.1.12 Norme di comportamento

La Ditta aggiudicataria e, per essa, il suo personale dipendente, devono uniformarsi a tutte le norme di carattere generale emanate dall'Azienda Ospedaliera per il proprio personale ed attenersi a tutte le norme di sicurezza del lavoro.

Il personale in servizio è tenuto a rispettare le consuete norme di educazione che definiscono i criteri di un comportamento civile e di correttezza nel lavoro. In particolare deve:

a) svolgere il servizio negli orari e nei giorni prestabiliti: non sono ammesse variazioni dell'orario di servizio e dei giorni se non preventivamente concordate;

b) rispettare gli ordini di servizio seguendo le operazioni affidate secondo le metodiche e le frequenze stabilite;

c) essere sempre presente nelle rispettive zone di lavoro negli orari concordati tra il committente e l'impresa aggiudicataria;

e) non prendere visione dei documenti, mantenere il segreto d'ufficio su fatti o circostanze concernenti i degenti, il personale, l'organizzazione e l'andamento dell'Azienda Ospedaliera ICP, delle quali abbia avuto notizia durante l'espletamento del servizio. Il mancato rispetto del segreto d'ufficio, se accertato, comporterà l'allontanamento dell'operatore dall'Azienda Ospedaliera ICP ed eventuali provvedimenti inerenti al caso.

L'impresa aggiudicataria assume l'obbligo di agire in modo che il personale dipendente, incaricato di effettuare le prestazioni contrattuali, mantenga riservati i dati e le informazioni di cui venga in possesso, non li divulghi e non ne faccia oggetto di sfruttamento.

Tale obbligo permane anche successivamente alla conclusione delle prestazioni e servizi resi a titolo contrattuale.

L'Appaltatore deve fornire all'Azienda Ospedaliera ICP l'elenco nominativo, con relative qualifiche, del personale adibito sia al controllo che allo svolgimento del servizio, compresi i sostituti, nonché la prova e, mensilmente, la documentazione necessaria certificante l'adempimento degli obblighi assicurativi di legge e contrattuali.

L'elenco del personale deve essere periodicamente aggiornato per le variazioni che dovessero intervenire.

6.1.13 Brevetti industriali e diritti d'autore

L'Appaltatore assume ogni responsabilità conseguente all'uso di dispositivi o all'adozione di soluzioni tecniche o di altra natura che violino diritti di brevetto, di autore ed in genere di privativa altrui.

Qualora venga promossa nei confronti dell'Azienda Ospedaliera ICP azione giudiziaria da parte di terzi che vantino diritti su beni acquistati o in licenza d'uso, l'Appaltatore manleverà e terrà indenne l'Azienda Ospedaliera ICP, assumendo a proprio carico tutti gli oneri conseguenti, inclusi i danni verso terzi, le spese giudiziali e legali a carico dell'Azienda Ospedaliera ICP.

6.1.14 Obblighi connessi alla sicurezza ai sensi dell'art. 26 del D.Lgs. 81/08

Al fine di promuovere la cooperazione ed il coordinamento in materia di prevenzione e sicurezza, nonché di fornire informazioni circa i rischi specifici esistenti negli ambienti dell'Azienda Appaltante, in allegato alla documentazione di gara, e più precisamente al Disciplinare di gara (di cui costituisce l'Allegato n. 10), viene posto l'Opuscolo Informativo *"rischi lavorativi specifici negli ambienti dell'Azienda Ospedaliera ICP e misure di prevenzione e emergenza. Informazioni di sicurezza rivolte alle imprese appaltatrici ed ai lavoratori autonomi per lavori affidati all'interno dell'Azienda ai sensi dell'art. 26 del Decreto Legislativo 81/08 – Rev. 05"*, redatto dall'A.O. nel mese di luglio 2011.

Inoltre, si allega, sempre al succitato Disciplinare di gara (all'Allegato n. 11), il modello di DUVRI (Documento Unico di Valutazione dei Rischi da Interferenze); all'atto della formalizzazione dell'incarico, l'Azienda Appaltante e l'Aggiudicatario completeranno la redazione del DUVRI ex art. 26 del D.Lgs. 81/08 e s.m.i., in conformità alla regolamentazione vigente nell'Azienda Appaltante.

6.1.15 Controversie

Ai sensi dell'art. 239 del D. Lgs. 163/06 e successive modifiche, le controversie relative a diritti soggettivi derivanti dall'esecuzione del contratto potranno sempre essere risolte mediante transazione, nel rispetto del codice civile.

Tutte le controversie che dovessero insorgere dal presente contratto, saranno devolute al giudice competente per giurisdizione ai sensi dell'art. 244 del D.Lgs 163/06.

Le Parti concordano di eleggere quale foro esclusivo e non concorrente il Foro di Milano, rinunciando espressamente agli altri fori concorrenti previsti dal c.p.c. .

6.1.16 Spese contrattuali

Ogni spesa riguardante il contratto, tassa di registro, bolli, quietanze, così come ogni altra tassa ed imposta cui potesse dare titolo il contratto, sono a carico dell'Appaltatore, fatta eccezione per l'Iva che è a carico dell'A.O. ICP, secondo le aliquote stabilite dalla Legge.

La Ditta aggiudicataria dovrà provvedere al versamento delle spese di bollo e di registro entro 15 giorni dalla relativa richiesta dell'U.O. Provveditorato-Economato.

6.1.17 Rinvio ad altre norme

Per quanto non espressamente previsto dal presente capitolato speciale e dal contratto d'appalto, trovano applicazione le disposizioni contenute nel codice civile, nel CCNLL di settore, nelle leggi e regolamenti vigenti e disciplinanti la materia oggetto del presente capitolato ed in particolare quelle contenute nel Regolamento per l'Amministrazione del Patrimonio e la Contabilità Generale dello Stato, approvato con R.D. 23/5/1924 n. 827 e s.m.i., nel D.Lgs. 163/2006, nel D.P.R. 207/2010 e nel D.Lgs. 81/2008 e successive modificazioni ed integrazioni.

(firma del Legale Rappresentante della Ditta)

_____

Per specifica accettazione degli articoli n. 4.2, 4.7, 4.8, 4.18, 4.19, 4.21, 5.2, 5.8, 5.9, 5.24, 5.25, 5.27, 6.1.1, 6.1.6, 6.1.7, 6.1.8, 6.1.9, 6.1.10, 6.1.13, 6.1.15 del presente Capitolato Speciale anche ai fini di cui all'art. 1341 del C.C.

(firma del Legale Rappresentante della Ditta)

_____

7 Allegati per il lotto 1

Allegato A: Sedi ICP

Allegato B: Componenti hardware e software della sala server attuale

Allegato C: Infrastruttura di rete ICP

8 Allegati per il lotto 2

Allegato A: Sedi ICP

Allegato B: Componenti hardware e software della sala server attuale

Allegato C: Infrastruttura di rete ICP

Allegato D: Caratteristiche della sala server

Allegato E: Infrastrutture server ICP presenti presso le sedi ICP al di fuori della sala server.