Allegato Tecnico 1

Fornitura e servizi
Consolidamento Datacenter
nuovo ospedale:
server & backup in architettura Unified Storage

Sommario

0 INTRODUZIONE E PRINCIPI GENERALI

0.1 GLOSSARIO

Definizione	Significato	Descrizione
NIGUARDA	AZIENDA OSPEDALIERA NIGUARDA CA GRANDA MILANO	Ente appaltatore
CCE	Cartella Clinica Elettronica	Soluzione di Cartella Clinica Elettronica
GTIS	Farmaco Prescrizione	Soluzione per la gestione della farmaco prescrizione
PROT	Gestione documentale	Soluzione per la gestione del protocollo e gestione documentale
IOP	Interoperabilità	Sistema middleware e componenti della piattaforma regione lombardia
SIO	Sistema Informativo Ospedaliero	Il complesso dell'architettura hardware e software di supporto ai processi clinico-scientifici ed amministrativi all'interno dell'azienda sanitaria
DIS	Sistemi informativi dipartimentali	Identificazione di un sistema generico dipartimentale
FRO	Sistema informativo di accoglienza	Sistemi informativi di sportello accoglienza degli utenti (ADT: accettazione ricoveri, CUP: sistema di prenotazioni ambulatoriali, PS: pronto soccorso, QUEUE: elimina code)
SISS	Sistema Informativo Socio-Sanitario della Regione Lombardia	Network regionale per l'integrazione dei flussi informativi per i servizi socio-sanitari al cittadino/paziente
BACKUP	Sistema di gestione del backup centralizzato	Infrastruttura hardware e software per la gestione del backup dei dati e configurazione logiche dei sistemi informativi

0.2 OGGETTO APPALTO

L'Ospedale Niguarda intende, nell'arco dei prossimi anni, consolidare gli impianti attestati sull'infrastruttura attuale su un'infrastruttura consolidata e con architettura Unified Storage, anche attraverso un uso più intensivo delle tecnologie di virtualizzazione.

Il disegno complessivo della soluzione proposta deve essere coerente con l'evoluzione dell'intero datacenter aziendale, mentre le attività iniziali sono rivolte al:

- consolidamento di un sottoinsieme degli impianti, meglio specificati nel capitolo seguente.
- all'integrazione nell'architettura target dei restanti impianti
- convergenza di tutti gli impianti del datacenter sul nuovo sistema di backup (presentata dal presente appalto)

L'oggetto del presente appalto, nell'ambito della imminente attivazione del nuovo blocco ospedaliero, con relativa entrata in funzione della nuova server farm aziendale include:

- progetto di evoluzione dell'attuale architettura di server e Backup aziendale
- fornitura, l'installazione la messa in produzione di componenti Hw e Sw aggiuntive e/o sostitutive in grado di superare le attuali limitazioni del sistema che verranno di seguito descritte
- migrazione degli impianti sulla soluzione target

- gestione chiavi in mano del datacenter (sistemistica: hardware, ambiente e rdbms): monitoraggio, manutenzione ordinaria, straordinaria ed evolutiva

Garantire il fabbisogno di capacità elaborativa necessaria a sostenere le fasi successive del progetto, i sistemi oggetto di acquisizione dovranno essere scalabili in funzione delle future esigenze.

Gli obiettivi di tale percorso sono:

- la dismissione dei sistemi fisici oggetto di consolidamento;
- la riduzione dei consumi energetici, delle esigenze di condizionamento, degli ingombri e dei costi gestionali;
- l'aumento del livello di utilizzo delle risorse elaborative, condivise tra più macchine virtuali;
- la riduzione del numero complessivo di schede per il collegamento alla rete ed ai dati.

Il fornitore dovrà proporre la soluzione che ritiene piu' idonea e innovativa sia dal punto di vista tecnico che dal punto di vista economico, sia che essa preveda l'inserimento/la sostituzione o l'integrazione dell'attuale impianto con nuove componenti Hw e Sw, purche' in linea con gli obiettivi posti dall'azienda e di seguito specificati.

Il progetto deve essere del tipo "Chiavi in mano", ovvero consegnato all'Ente perfettamente funzionante in ogni sua componente e si riterrà consegnato solo a valle del collaudo formale.

Il documento è strutturato come segue:

- il Capitolo 1 descrive l'organizzazione e l'infrastruttura attuale dell'Ente
- il Capitolo 2 descrive l'oggetto della fornitura ed i requisiti generali;
- il Capitolo 3 dettaglia i requisiti richiesti al fornitore per formulare l'offerta.

Si specifica che le caratteristiche riportate nel seguito del documento sono da considerarsi quali requisiti minimi per la formulazione dell'offerta tecnica.

A seguito della assegnazione della gara e partenza del progetto, eventuali errori nella configurazione hardware e/o software dei sistemi oggetto di gara saranno imputate, come responsabilità, alla ditta vincitrice la quale avrà l'onere di operare tutte le variazioni hardware, software e di architettura funzionali alla corretta implementazione del progetto.

1 ORGANIZZAZIONE E INFRASTRUTTURA ATTUALE

1.1 ORGANIZZAZIONE ATTUALE

La gestione attuale degli impianti interessati dal presente appalto si identificano come segue:

- gestione sistemistica (hardware, sistemi operativi, fino alla virtualizzazione) di tutti i server: fornitore appalto fleet aziendale : fornitore (IBM AXIOM)
- gestione rdbms : delegata a ciascun fornitore della soluzione applicativa
- gestione backup: fornitore specifico (fornitore AXIOM)

1.1.1 Modello generale di organizzazione dei servizi in uso presso l'Ente

I servizi richiesti in fornitura si inquadrano ed interagiscono nel modello generale di organizzazione già in uso presso l' Ente. Tale modello è di seguito descritto.

Il modello è uno schema classico di supporto a più livelli. Prevede che un Help/Service Desk (HD) di primo livello riceva le chiamate di assistenza e le richieste da parte degli utenti. L'HD qualifica la chiamata / richiesta di servizio, eroga un primo livello di supporto e se necessario inoltra la chiamata alla coda di competenza, in questo caso "Gestione Code" per un secondo livello di supporto più specifico.

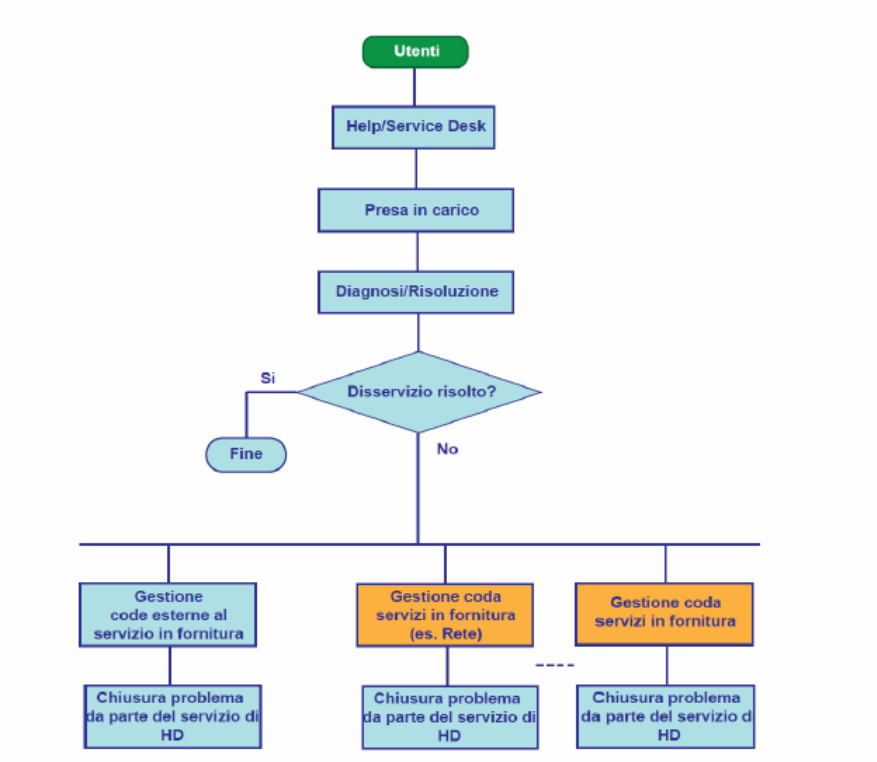


Figura 1

Nel modello sopra esposto l'HD (help desk di primo livello) è una struttura già operante e non deve essere inclusa nella fornitura.

L'HD rappresenta l' unico punto di contatto (SPOC – Single Point Of Contact) per ogni tipo di richiesta di supporto o di informazione da parte degli utenti.

Le chiamate possono riguardare:

1. Richieste di Supporto per problemi Hw
2. Richieste di Supporto per problemi Sw
3. Richieste di nuove Installazioni
4. Richieste di nuovi servizi/prodotti
5. Richieste di servizio per Move, Add, Change
6. Richieste di informazioni e istruzione per l'impiego
7. Solleciti su chiamate già aperte
8. etc.

L'HD è una funzione comune "propedeutica" alle altre funzioni è perciò sempre attivata per prima.
In particolare, una volta recepita la richiesta di supporto, effettua una diagnosi on-line e, quando possibile, ripristina la corretta fruizione del prodotto/servizio da parte dell' utenza.
Nel caso in cui la soluzione non possa essere fornita direttamente on-line, l' HD ha comunque la responsabilità di individuare la natura del malfunzionamento e dispacciare correttamente la chiamata alla/le linea/e operativa/e cui compete la soluzione del problema. Ciò ricorrendo al suo interno a sistemisti di secondo livello o, se necessario, facendosi aiutare dalle linee operative. Fino però al dispacciamento del problema l' HD ne rimane l' unico responsabile.

Compito dell' HD è anche l'apertura, il monitoraggio ed, a conclusione del processo di problem solution, la chiusura del Trouble Ticket, da effettuare solo dopo verifica con il cliente del servizio fornito (call-back).
Per ogni chiamata, ad esclusione dei solleciti, viene aperto un ticket all' interno del sistema di trouble ticketing dell' HD. Il ticket rimane aperto fino alla soluzione dell' anomalia o alla conclusione della richiesta di servizio.

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

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

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

Fa parte del servizio di Help Desk anche la preparazione del reporting mensile delle chiamate gestite.

1.2 INFRASTRUTTURA ATTUALE (AS-IS)

Nella tabella seguente a titolo riepilogativo si riporta l'elenco delle componenti harware presenti al momento in azienda, che pertanto sono oggetto della presa in carico del presente appalto.
L'elenco potrà variare al momento della presa in carico del servizio di gestione in funzione delle attività evolutive in corso.

1.2.1 Server Fisici

Tipo Apparato	Impianto	Servizio/Funzione	Marca Apparato	Modello Apparato	S.O.	Modello CPU	Nr. CPU Totali	Nr. Core Totali	RAM (Gb)	Nr. Dischi Totali	Dimensione Tot. HDU (Gb)	Manutentore Applicativo
Server	FARMACIA	Application server Farmacia	IBM	SYSTEM X3650 M3	N/A	N/A	N/A	N/A	N/A	2	146	Swisslog
Server	FARMACIA	DB Farmacia	IBM	SYSTEM X3650 M3	N/A	N/A	N/A	N/A	N/A	2	146	Swisslog
Server	SOST	Archiviazione sostitutiva	IBM	SYSTEM X3550 M3	N/A	N/A	N/A	N/A	N/A	2	146	NEXERA
Server	SOST	Archiviazione sostitutiva	IBM	SYSTEM X3550 M3	N/A	N/A	N/A	N/A	N/A	2	146	NEXERA
Server	Ingegneria Clinica	Applicativo Terapia intensiva DEA	DELL	POWEREDGE R210 II	N/A	N/A	N/A	N/A	N/A	N/A	N/A	UMS
Server	SOST	Archiviazione sostitutiva	DELL	POWEREDGE 860	Microsoft Windows Server 2008 R2 Standard Edition	Intel Xeon ® X3430 2.40GHz 4 core	1	4	4	2	470	NEXERA
Server	QUEUE	elimina code appserver	IBM	SYSTEM X3550 M3	N/A	N/A	N/A	N/A	N/A	2	146	SMARTV
Server	QUEUE	elimina code appserver	IBM	SYSTEM X3550 M3	N/A	N/A	N/A	N/A	N/A	2	146	SMARTV
Server	CAUDULLO	Supervisione ups per caudullo	DELL	POWEREDGE R210 II	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Caudullo
Server	REMEDES	Comunicazione con LISPA	HP	PROLIANT DL 360G3	Microsoft Windows Server 2003 R2 Standard Edition	N/A	N/A	N/A	N/A	2	73	LOMBARDIA CALL
Server	SOST	Archiviazione sostitutiva	DELL	POWEREDGE R210	Microsoft Windows Server 2008 R2 Standard Edition	Intel Xeon ® E5620 2.40GHz 4 core	1	4	6	2	1820	NEXERA
Server	PSICHE	PSICHE Server	IBM	XSeries 335	Microsoft Windows 2000 Terminal Server	Intel Xeon ® 2.00GHz 1 core	1	1	2	2	73	Lispa
Blade Center H	FLEET	Blade center H	IBM	Blade Center H	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Axiom

Server	FLEET	Gestore VM VMWARE nodo del Cluster VMWCluster01 (por-vmprod04)	IBM	Blade HS22	VMWare ESXI 5.0.0	Intel Xeon ® E5670 2.93GHz 6 core	2	12	64	2	146	Axiom
Server	FLEET	Gestore VM VMWARE nodo del Cluster VMWCluster02	IBM	Blade HS22	VMWare ESXI 5.0.0	Intel Xeon ® E5667 3.06GHz 4 core	2	8	24	2	146	Axiom
Server	FLEET	Gestore VM VMWARE nodo del Cluster VMWCluster01 (por-vmprod03)	IBM	Blade HS22	VMWare ESXI 5.0.0	Intel Xeon ® E5670 2.93GHz 6 core	2	12	64	2	146	Axiom
Server	FLEET	Host VmWare per ambiente di Test	IBM	Blade HS22	Linux Red Hat Enterprise 5.5	Intel Xeon ® E5530 2.40 GHz 4 core	2	8	64	2	146	AXiom
Server	RISPACS	AGFA GESTIONE IMMAGINI RADIOGRAFICHE	SUN	SPARC ENTERPRISE T5120	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Agfa
Server	RISPACS	AGFA GESTIONE IMMAGINI RADIOGRAFICHE	SUN	SPARC ENTERPRISE T5120	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Agfa
Server	RISPACS	AGFA GESTIONE IMMAGINI RADIOGRAFICHE	SUN	SPARC ENTERPRISE T5120	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Agfa
Server	RISPACS	AGFA GESTIONE IMMAGINI RADIOGRAFICHE	DELL	POWEREDGE 2950	N/A	N/A	N/A	N/A	N/A	2	300	Agfa
Server	RISPACS	AGFA GESTIONE IMMAGINI RADIOGRAFICHE	HP	PROLIANT DL385 G7	N/A	N/A	N/A	N/A	N/A	2	300	Agfa
Server	RISPACS	AGFA GESTIONE IMMAGINI RADIOGRAFICHE	HP	PROLIANT DL385 G7	N/A	N/A	N/A	N/A	N/A	2	300	Agfa
Server	RISPACS	AGFA GESTIONE IMMAGINI RADIOGRAFICHE	DELL	POWEREDGE 2950	N/A	N/A	N/A	N/A	N/A	2	146	Agfa
Server	RISPACS	AGFA GESTIONE IMMAGINI RADIOGRAFICHE	DELL	POWEREDGE 2950	N/A	N/A	N/A	N/A	N/A	2	146	Agfa
Server	RISPACS	AGFA GESTIONE IMMAGINI RADIOGRAFICHE	DELL	POWEREDGE 2950	N/A	N/A	N/A	N/A	N/A	2	146	Agfa
Server	RISPACS	AGFA GESTIONE IMMAGINI RADIOGRAFICHE	FUJITSU SIEMEN	BIG IP 3600 SERIES	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Agfa

			S									
Server	RISPACS	AGFA GESTIONE IMMAGINI RADIOGRAFICHE	FUJITSU SIEMENS	BIG IP 3600 SERIES	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Agfa
Server	RISPACS	AGFA GESTIONE IMMAGINI RADIOGRAFICHE	FUJITSU SIEMENS	PRIMERGY TX300-S3	N/A	N/A	N/A	N/A	N/A	6	N/A	Agfa
Server	RISPACS	AGFA GESTIONE IMMAGINI RADIOGRAFICHE	FUJITSU SIEMENS	PRIMERGY TX300-S3	N/A	N/A	N/A	N/A	N/A	6	N/A	Agfa
Server	RISPACS	AGFA GESTIONE IMMAGINI RADIOGRAFICHE	SUN	SUNFIRE X4200	N/A	N/A	N/A	N/A	N/A	2	N/A	Agfa
Server	RISPACS	AGFA GESTIONE IMMAGINI RADIOGRAFICHE	FUJITSU SIEMENS	PRIMERGY TX300-S3	N/A	N/A	N/A	N/A	N/A	2	73	Agfa
Server	RISPACS	AGFA GESTIONE IMMAGINI RADIOGRAFICHE	FUJITSU SIEMENS	PRIMERGY TX300-S3	N/A	N/A	N/A	N/A	N/A	4	146	Agfa
Server	RISPACS	AGFA GESTIONE IMMAGINI RADIOGRAFICHE	DELL	POWEREDGE 2950	N/A	N/A	N/A	N/A	N/A	2	146	Agfa
Server	RISPACS	AGFA GESTIONE IMMAGINI RADIOGRAFICHE	DELL	POWEREDGE 2950	N/A	N/A	N/A	N/A	N/A	2	300	Agfa
Server	RISPACS	AGFA GESTIONE IMMAGINI RADIOGRAFICHE	DELL	POWEREDGE 2950	N/A	N/A	N/A	N/A	N/A	2	300	Agfa
Server	RISPACS	AGFA GESTIONE IMMAGINI RADIOGRAFICHE	DELL	POWEREDGE 860	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Agfa
Server	RISPACS	AGFA GESTIONE IMMAGINI RADIOGRAFICHE	HP	PROLIANT DL380 G7	N/A	N/A	N/A	N/A	N/A	8	N/A	Agfa
Blade Center H	AIS	Blade center H	IBM	Blade Center H	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Axiom
Server	AIS	Invio proposte a G3S (NFS)	IBM	XSeries 335	Microsoft Windows 2000 Terminal Server	Intel Xeon ® 2.40GHz 1 core	1	1	4	2	36,4	Dedalus
Server	AIS	Gestione scansioni immagini Rag. E farmacia	FUJITSU	PRIMERGY RX300 S6	Microsoft Windows	Intel Xeon ® X5506	N/A	4	6	2	500	Dedalus

					Server 2008 R2 Standard Edition	2.13GHz 4 core					
Server	AIS	Cluster Oracle Db - Nfs	IBM	Blade HS22	Linux Red Hat Enterprise 5.5	Intel Xeon ® X5560 2.80GHz 4 core	2	8	16	2	146	Dedalus
Server	AIS	Cluster Application Server - Nfs	IBM	Blade HS22	Microsoft Windows Server 2003 R2 Standard Edition	Intel Xeon ® X5560 2.80GHz 4 core	2	8	4	2	146	Dedalus
Server	AIS	Cluster Oracle Db - Nfs	IBM	Blade HS22	Linux Red Hat Enterprise 5.5	Intel Xeon ® X5540 2.60GHz 4 core	2	8	16	2	146	Dedalus
Server	AIS	Cluster Application Server - Nfs	IBM	Blade HS22	Microsoft Windows Server 2003 R2 Standard Edition	Intel Xeon ® X5560 2.80GHz 4 core	2	8	4	2	146	Dedalus
Server	FRO	CUP - ADT STANDBY SERVER	IBM	xSeries 3650 M3	Linux Oracle Enterprise server 5.4	Intel Xeon ® 5640 2.67 GHz 4 core	2	8	32	8	200	Hitech
Server	FRO	CUP - ADT (ORACLE RAC) + AS	IBM	xSeries 3650 M3	Linux Oracle Enterprise server 5.4	Intel Xeon ® 5640 2.67 GHz 4 core	2	8	32	3	160	Hitech
Server	FRO	CUP - ADT (ORACLE RAC) + AS	IBM	xSeries 3650 M3	Linux Oracle Enterprise server 5.4	Intel Xeon ® 5640 2.67 GHz 4 core	2	8	32	3	200	Hitech
Server	Ingegneria Clinica	N/A	SUN	SUNFIRE X4170	N/A	N/A	N/A	N/A	N/A	2	300	KARL STORZ
Server	Ingegneria Clinica	N/A	SUN	SUNFIRE X4170	N/A	N/A	N/A	N/A	N/A	2	300	KARL STORZ
Server	Ingegneria Clinica	Syngo.Via	HP	PROLIANT ML350P GEN8	Windows Server 2008 R2 Enterprise	N/A	N/A	N/A	N/A	16	N/A	Siemens
Server	Ingegneria Clinica	SERVER CONTROLASSET ELLF	ASUS	RS520-E6	Windows Server 2008 R2 Standard	N/A	N/A	N/A	N/A	8	N/A	ELLF
Server	Ingegneria Clinica	Server Laboratiorio	ASSEMBLATO	ASSEMBLATO	Windows 7 Pro	Intel Pentium G860 3 GHZ	1	2	4	2	1000	BIO-RAD

Server	FLEET	Gestore Macchine Virtuali	IBM	xSeries 3550 M3	VMWare ESXI 5.0.0	Intel Xeon ® E5506 2.13GHz 4 core	N/A	4	16	3	420	Axiom
Server	IM	DNS Server Pubblico (Niguardaonline.it)	IBM	XSeries 306	Linux Slackware 12.0	Intel Pentium 4 ® 3.40 Ghz 1 core	1	1	1	2	146	Axiom
Appliance	INTERNET	Antispam	McAfee	SIG 3300	Email and Web Security Appliance (3300) v5.6	Intel Xeon ® 5130 2.00GHz 2 core	2	4	N/A APPLIANCE	N/A APPLIANCE	N/A APPLIANCE	Axiom
Appliance	INTERNET	Web filter	McAfee	SIG 3300	Email and Web Security Appliance (3300) v5.5	Intel Xeon ® 5130 2.00GHz 2 core	2	4	N/A APPLIANCE	N/A APPLIANCE	N/A APPLIANCE	Axiom
Appliance	AAA	Servizio VPN	Juniper	SA-4000	IVE 6.5R8	N/A APPLIANCE	N/A APPLIANCE	N/A APPLIANCE	N/A APPLIANCE	N/A APPLIANCE	N/A APPLIANCE	Axiom
Server	AAA	Servizio RSA	IBM	XSeries 3550	Microsoft Windows Server 2003 R2 Standard Edition	Intel Xeon ® E5620 2.40GHz 4 core	1	2	2	2	146	Axiom
Server	FLEET	Gestore Macchine Virtuali	IBM	xSeries 3550 M3	VMWare ESXI 5.0.0	Intel Xeon ® E5620 2.40GHz 4 core	2	4	32	2	146	Axiom
Server	DR	Server Backup Tivoli TSM	IBM	XSeries 345	Microsoft Windows Server 2003 Standard Edition	Intel Xeon ® 2.40GHz 1 core	1	1	4	4	400	Axiom
Server	FLEET	Gestore Macchine Virtuali	IBM	xSeries 3550 M3	VMWare ESXI 5.0.0	Intel Xeon ® E5620 2.40GHz 4 core	2	4	32	2	146	Axiom
Appliance	FLEET	Log amministratori	Juniper	STRM500-A	Junos	N/A APPLIANCE	N/A APPLIANCE	N/A APPLIANCE	N/A APPLIANCE	N/A APPLIANCE	N/A APPLIANCE	Axiom
Server	FLEET	Gestore Macchine Virtuali	IBM	xSeries 3550 M3	VMWare ESXI 5.0.0	Intel Xeon ® E5620 2.40GHz 4	1	4	32	4	1360	Axiom

						core						
Server	INTERNET	Reverse Proxy Cluster	IBM	XSeries 3250 M2	Linux Debian Lenny 5.0.6	Intel Xeon ® X3320 2.50GHz 4 core	1	4	1	2	160	Axiom
Server	INTERNET	Reverse Proxy Cluster	IBM	XSeries 3250 M2	Linux Debian Lenny 5.0.6	Intel Xeon ® X3320 2.50GHz 4 core	1	4	1	2	160	Axiom
Appliance	INTERNET	Antispam	McAfee	SIG 3300	Email and Web Security Appliance (3300) v5.6	Intel Xeon ® 5130 2.00GHz 2 core	2	4	N/A APPLIANCE	N/A APPLIANCE	N/A APPLIANCE	Axiom
Appliance	INTERNET	Web filter	McAfee	SIG 3300	Email and Web Security Appliance (3300) v5.5	Intel Xeon ® 5130 2.00GHz 2 core	2	4	N/A APPLIANCE	N/A APPLIANCE	N/A APPLIANCE	Axiom
Server	IM	DNS Server Pubblico (Niguardaonline.it)	IBM	XSeries 306	Linux Slackware 12.0	Intel Pentium 4 ® 3.40 Ghz 1 core	1	1	1	2	80	Axiom
Server	INTERNET	Quarantena	IBM	XSeries 3650	Microsoft Windows Server 2003 R2 Standard Edition	Intel Xeon ® 5410 2.33 GHz 4 core	1	4	2	5	570	Axiom
Server	AAA	RSA - Accesso Web Autenticazone RSA Server	IBM	xSeries 3550	Microsoft Windows Server 2003 R2 Standard Edition	Intel Xeon ® 5160 3.00GHz 2 core	1	2	2	2	146	Axiom
Appliance	AAA	Servizio VPN	Juniper	SA-4000	IVE 6.5R8	N/A APPLIANCE	N/A APPLIANCE	N/A APPLIANCE	N/A APPLIANCE	N/A APPLIANCE	N/A APPLIANCE	Axiom
Server	IM	Domain Controller - Ospedaleniguarda.it	IBM	XSeries 335	Microsoft Windows Server 2003 Standard Edition	Intel Xeon 2.40 Ghz	1	2	4	2	73	Axiom
Server	INTERNET	Servizio FTP Pubblico	IBM	XSeries 335	Microsoft Windows Server 2003 R2 Standard	Intel Xeon 2.40 Ghz	1	2	2,5	2	36,4	Axiom

					Edition							
Server	FLEET	Monitoring server IBM Director	IBM	XSeries 335	Microsoft Windows Server 2003 Standard Edition	Intel Xeon 2.40 Ghz	1	2	4	2	36,4	Axiom
Server	FLEET	Archiviazione LOG (PIX, Juniper, Proxy, etc)	IBM	XSeries 335	Microsoft Windows Server 2003 Enterprise Edition	Intel Xeon 2.40 Ghz	1	2	4	2	73	Axiom
Server	IM	Domain Controller - Ospedale Niguarda.schema	IBM	XSeries 335	Microsoft Windows Server 2003 Standard Edition	Intel Xeon 2.60 Ghz	1	2	N/A	2	36	Axiom
Server	IM	Domain Controller - Ospedaleniguarda.it	IBM	XSeries 3550 M2	Microsoft Windows Server 2003 Standard Edition	Intel Xeon ® E5520 2.26GHz 4 core	1	4	3	2	50	Axiom
Server	IM	Domain Controller - Ospedaleniguarda.it	IBM	XSeries 3550 M2	Microsoft Windows Server 2003 Standard Edition	Intel Xeon ® E5520 2.26GHz 4 core	1	4	3	2	50	Axiom
Server	BADGE	Server controllo accessi	ASSEMBLATO	ASSEMBLATO	Linux Suse Enterprese 11	Intel E5300 2.600GHz 2 core	1	2	2	1	250	Selesta
Server	EMO	Nodo Cluster Simt	DELL	PowerEdge 2950	Linux Red Hat Enterprise 5.2	Intel Xeon ® E5405 2.00GHz 4 core	1	4	1			Insiel
Server	EMO	Nodo Cluster Simt	DELL	PowerEdge 2950	Linux Red Hat Enterprise 5.2	Intel Xeon ® E5405 2.00GHz 4 core	1	4	1			Insiel
Server	EMO	Host esxi per emonet-web	IBM	xSeries 3550	Microsoft Windows Server 2003 R2 Standard Edition	Intel Xeon ® 5120 1.86GHz 2 core	1	2	4	2	146	Insiel

Server	SIMP	DB SIMP	IBM	XSeries 3650 M3	N/A	N/A	N/A	N/A	N/A	3	N/A	TESI
Server	SIMP	AS SIMP	IBM	xSeries 3250 M3	N/A	N/A	N/A	N/A	N/A	3	N/A	TESI
Server	INTRANET	Db Server Intranet	IBM	xSeries 3550 M2	N/A	N/A	N/A	N/A	N/A	4	N/A	Connexxa
Server	INTRANET	Db Server Intranet	IBM	xSeries 3550 M2	N/A	N/A	N/A	N/A	N/A	4	N/A	Connexxa
Server	INTRANET	Web Server Intranet	IBM	xSeries 3550 M2	N/A	N/A	N/A	N/A	N/A	4	N/A	Connexxa
Server	INTRANET	Web Server Intranet	IBM	xSeries 3550 M2	N/A	N/A	N/A	N/A	N/A	4	N/A	Connexxa
Server	FLOWNET	Db Server Flownet	IBM	xSeries 3650	Linux CentOs 5.9	Intel Xeon ® 5405 2.00 GHz 4 core	1	4	36	6	900	Oslo
Server	FLOWNET	App. Server - DataWarehouse	IBM	xSeries 345	Microsoft Windows Server 2003 R2 Standard Edition	Intel Xeon ® 3.06GHz 2 core	1	2	3	5	292	Oslo
Server	Project	Project Server	IBM	xSeries 345	Microsoft Windows Server 2003 Standard Edition	Intel Xeon ® 3.06GHz 2 core	1	2	3,75	6	263	NEXERA
Server	MAIL	Posta Elettronica - back end	IBM	XSeries 345	Microsoft Windows Server 2003 Enterprise Edition	Intel Xeon ® 2.40GHz 1 core	1	1	3	3	36	Axiom
Server	MAIL	Posta Elettronica - back end	IBM	XSeries 345	Microsoft Windows Server 2003 Enterprise Edition	Intel Xeon ® 2.40GHz 1 core	1	1	3	3	36	Axiom
Server	PRO	Db Server - Cluster Oracle Nodo2 - Protocollo Informatico e Gestione Documentale	IBM	XSeries 345	Microsoft Windows Server 2003 Enterprise Edition	Intel Xeon ® 2.40GHz 1 core	1	1	3	3	36	Insiel
Server	PRO	Db Server - Protocollo Informatico e Gestione Documentale - Cluster Oracle Nodo1 (Default: Virgilio)	IBM	XSeries 345	Microsoft Windows Server 2003 Enterprise Edition	Intel Xeon ® 2.40GHz 1 core	1	1	3	3	36	Insiel
Server	PRO	App. Server - Protocollo	IBM	XSeries 335	Microsoft	Intel Xeon ®	1	1	2,5	2	36	Insiel

		Informatico e Gestione Documentale			Windows Server 2003 Standard Edition	2.40GHz 1 core						
Server	PRO	App. Server - GES. DOC. - Protocollo Informatico e Gestione Documentale	IBM	XSeries 335	Microsoft Windows Server 2003 Standard Edition	Intel Xeon ® 2.40GHz 1 core	1	1	2,5	2	36	Insiel
Server	MAIL	Posta Elettronica - front end	IBM	XSeries 335	Microsoft Windows Server 2003 Standard Edition	Intel Xeon ® 2.40GHz 1 core	1	1	2,5	2	36	Axiom
Server	MAIL	Posta Elettronica - front end	IBM	XSeries 335	Microsoft Windows Server 2003 Standard Edition	Intel Xeon ® 2.40GHz 1 core	1	1	2,5	2	36	Axiom
Server	RDTP	Nodo 1 servizio MOSAIQ	HP	PROLIANT DL 360G7	Microsoft Windows Server 2008 R2 Enterprise	Intel Xeon E5606 ® 2.13 Ghz 4 core	1	4	20	2	146	Elekta
Server	RDTP	Nodo 2 server MOSAIQ	HP	PROLIANT DL 360G7	Microsoft Windows Server 2008 R2 Enterprise	Intel Xeon E5606 ® 2.13 Ghz 4 core	1	4	20	2	146	Elekta
Server	RDTP	MOSAIQ	HP	PROLIANT DL 360G7	Microsoft Windows Server 2008 R2 standard	Intel Xeon E5606 ® 2.13 Ghz 4 core	1	4	4	2	146	Elekta
Server	RDTP	MOSAIQ	HP	PROLIANT DL 360G7	Microsoft Windows Server 2003 R2 Standard Edition	Intel Xeon E5606 ® 2.13 Ghz 4 core	1	4	4	2	146	Elekta
Server	RDTP	Plan terapia - Radioterapia	IBM	xSeries 3550 M3	Microsoft Windows Server 2003 R2 Standard Edition	Intel Xeon ® E5620 2.40GHz 4 core	2	4	6	5	724	Elekta
Blade Center E	FLEET	Blade center H	IBM	Blade Center H	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Axiom

Server	FILE SERVER	NODO FILE SERVER CLUSTER GEMINI	IBM	XSeries 346	Microsoft Windows Server 2003 R2 Enterprise Edition	Intel Xeon ® 3.40GHz 1 core	1	2	6	5	73	Axiom
Server	FILE SERVER	NODO FILE SERVER CLUSTER GEMINI	IBM	XSeries 346	Microsoft Windows Server 2003 R2 Enterprise Edition	Intel Xeon ® 3.40GHz 1 core	1	2	6	5	73	Axiom
Server	CCE	è un nodo del cluster MySQL “Steno” su cui insistono i DB “Spefar”, “Mereafaps”,	IBM	Blade HS20	Microsoft Windows Server 2003 Enterprise Edition	Intel Xeon ® 3.60GHz 2 core	1	2	3	2	36	Webscience
Server	CCE	Dbms Test Portale	IBM	Blade HS20	Linux Red Hat EL AS 4	Intel Xeon ® 3.60GHz 2 core	1	2	4	2	73	Webscience
Server	INTERNET	Nodo Proxy	IBM	Blade HS20	Microsoft Windows Server 2003 R2 Standard Edition	Intel Xeon ® 3.60GHz 2 core	1	2	3	2	73	Axiom
Server	CCE	nodo del cluster MySQL “Steno” su cui sono i DB “Spefar”, “Mereafaps” - NODO EURIALE CLUSTER GORGONE	IBM	Blade HS20	Microsoft Windows Server 2003 Enterprise Edition	Intel Xeon ® 3.60GHz 2 core	1	2	3	2	36	Webscience
Server	INTERNET	Nodo Proxy	IBM	Blade HS20	Microsoft Windows Server 2003 R2 Standard Edition	Intel Xeon ® 3.60GHz 2 core	1	2	3	2	73	Axiom
Server	FLEET	Host VmWare per ambiente di Test	IBM	Blade HS22	Linux Red Hat Enterprise 5.5	Intel Xeon ® E5530 2.40 GHz 4 core	2	8	64	2	146	AXiom
Server	CCE	Host virtualizzazione su cui gira Jessica	IBM	Blade HS20	Linux Red Hat Enterprise 5.5	Intel Xeon ® 3.60GHz 2 core	1	2	4	2	20	Webscience
Blade Center H	FLEET	Blade center H	IBM	Blade Center H	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Axiom
Server	FLEET	Gestore VM VMWARE nodo del	IBM	Blade HS22	VMWare ESXI	Intel Xeon ®	2	12	64	2	146	Axiom

		Cluster VMWCluster01 (por-vmprod01)			5.0.0	E5670 2.93GHz 6 core						
Server	CCE	IN PRODUZIONE 2012_02_27 - Database Server Portale	IBM	Blade HS22	Linux Red Hat Enterprise 5.5	Intel Xeon ® E5640 2.67GHz 4 core	2	8	24	2	146	Axiom
Server	FLEET	Gestore VM VMWARE nodo del Cluster VMWCluster02	IBM	Blade HS22	VMWare ESXI 5.0.0	Intel Xeon ® E5667 3.06GHz 4 core	2	8	24	2	146	Axiom
Server	FLEET	Gestore VM VMWARE nodo del Cluster VMWCluster01 (por-vmprod02)	IBM	Blade HS22	VMWare ESXI 5.0.0	Intel Xeon ® E5670 2.93GHz 6 core	2	12	64	2	146	Axiom
Server	IOP	Server di Test PRI - evoluzione	IBM	xSeries 3550 M3	Linux Red Hat Enterprise 5.3	Intel Xeon E5506 ® 2.13 Ghz 4 core	1	4	16	3	420	Santer
Server	IOP	Server di Test PRI - pre_produzione	IBM	XSeries 335	Microsoft Windows Server 2003 Standard Edition	Intel Xeon 2.40 Ghz	1	2	4	2	73	Santer
Server	IOP	Epr Test + POR Test	IBM	xSeries 345	Linux Red Hat EL AS 4	Intel Xeon ® 3.06GHz 2 core	1	2	8	6	230	Santer
Server	TLP	Server 4 cluster Citrix XenDesktop	HP	DL380G7	Xenserver 5	N/A	N/A	N/A	N/A	2	146	Atos
Server	TLP	Server 3 cluster Citrix XenDesktop	HP	DL380G7	Xenserver 5	N/A	N/A	N/A	N/A	2	146	Atos
Server	TLP	Server 2 cluster Citrix XenDesktop	HP	DL380G7	Xenserver 5	N/A	N/A	N/A	N/A	2	146	Atos
Server	TLP	Server 1 cluster Citrix XenDesktop	HP	DL380G7	Xenserver 5	N/A	N/A	N/A	N/A	2	146	Atos
Server	TLP	Proxy server e confioguration server	FUJITSU SIEMENS	PRIMERGY X150-S7	Linux Red Hat ES 4	N/A	N/A	N/A	N/A	1	146	Atos
Server	TLP	Database configurazioni e utenti Himed	FUJITSU SIEMENS	PRIMERGY X150-S7	Linux Red Hat ES 4	N/A	N/A	N/A	N/A	2	146	Atos
Server	AIS	Rilevazioni presenze, Anagrafica personale, Parte stipendiale	IBM	iSeries 9406	OS 400	N/A	N/A	N/A	N/A	N/A	N/A	Dedalus

Server	IOP	Db Server - PS_R DB - DB Siss - Nodo Fisico Euclide	IBM	XSeries 346	Linux Red Hat EL AS 3	Intel Xeon ® 3.40GHz 2 core	1	2	8	2	146	Santer
Server	IOP	Db Server - DB Siss - Talete Nodo Fisico	IBM	XSeries 346	Linux Red Hat EL AS 3	Intel Xeon ® 3.40GHz 2 core	1	2	8	2	146	Santer
Blade Center E	LIS	Blade center H	IBM	Blade Center H	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Axiom
Server	LIS	DNWEB App. Server	IBM	Blade HS21	Microsoft Windows Server 2003 Standard Edition	Intel Xeon ® E5140 2.33 GHz 2 core	1	2	4	2	73	NoemaLife
Server	LIS	WP App. Server	IBM	Blade HS21	Microsoft Windows Server 2003 Standard Edition	Intel Xeon ® 5130 2.00GHz 2 core	1	2	2	2	73	NoemaLife
Server	LIS	Server TEST LIS	IBM	Blade HS21	Microsoft Windows Server 2003 Enterprise Edition	Intel Xeon ® E5140 2.33 GHz 2 core	1	2	8	2	73	NoemaLife
Server	LIS	WP GWY	IBM	Blade HS21	Microsoft Windows Server 2003 Enterprise Edition	Intel Xeon ® E5140 2.33 GHz 2 core	1	2	8	2	73	NoemaLife
Server	LIS	DNLAB DB	IBM	Blade HS21	Linux Red Hat Enterprise 5.5	Intel Xeon ® E5335 2.00 GHz 4 core	2	8	8	2	73	NoemaLife
Server	LIS	DNWEB App. Server	IBM	Blade HS21	Microsoft Windows Server 2003 Standard Edition	Intel Xeon ® E5140 2.33 GHz 2 core	1	2	4	2	73	NoemaLife
Server	LIS	DNLAB DB	IBM	Blade HS21	Linux Red Hat Enterprise 5.5	Intel Xeon ® E5335 2.00 GHz 4 core	2	8	8	2	73	NoemaLife
Server	LIS	WP GWY	IBM	Blade HS21	Microsoft Windows Server 2003	Intel Xeon ® E5140 2.33 GHz 2 core	1	2	8	2	73	NoemaLife

					Enterprise Edition							
Server	LIS	Server Applicativo PICASSO	IBM	Blade HS21	Linux CentOs 5.9	Intel Xeon ® E5140 2.33 GHz 2 core	2	4	8	2	73	NoemaLife
Server	LIS	DNLAB DOC	IBM	Blade HS21	Microsoft Windows Server 2003 Standard Edition	Intel Xeon ® E5140 2.33 GHz 2 core	1	2	4	2	73	NoemaLife
Server	LIS	DNLAB DOC	IBM	Blade HS21	Microsoft Windows Server 2003 Standard Edition	Intel Xeon ® 5130 2.00GHz 2 core	1	2	2	2	73	NoemaLife
Server	LIS	DNLAB DOC	IBM	Blade HS21	Microsoft Windows Server 2003 Standard Edition	Intel Xeon ® 5130 2.00GHz 2 core	1	2	2	2	73	NoemaLife
Server	LIS	DNLAB DOC	IBM	Blade HS21	Microsoft Windows Server 2003 Standard Edition	Intel Xeon ® 5130 2.00GHz 2 core	1	2	2	2	73	NoemaLife
Server	LIS	DNLAB DOC	IBM	Blade HS21	Microsoft Windows Server 2003 Standard Edition	Intel Xeon ® 5130 2.00GHz 2 core	1	2	2	2	73	NoemaLife
Server	EIS	Percorso Chirurgico	IBM	XSeries 346	Linux Red Hat Enterprise 5.3	Intel Xeon ® 3.20GHz 1 core	1	N/A	N/A	4	146	Cbim
Server	EIS	Host TOBIA	IBM	XSeries 3650 M2	Linux Red Hat Enterprise 5.3	Intel Xeon ® E5530 2.40 GHz 4 core	1	4	14	4	740	Cbim
Server	EIS	Host PIESSE-STB	IBM	XSeries 3650 M2	Linux Red Hat Enterprise 5.3	Intel Xeon ® E5530 2.40 GHz 4 core	1	4	14	4	740	Cbim
Server	EIS	Host PIESSE-AS	IBM	XSeries 3650 M2	Linux Red Hat Enterprise 5.3	Intel Xeon ® E5530 2.40 GHz 4 core	1	4	14	4	270	Cbim

Server	EIS	Application Server PS	IBM	XSeries 335	Microsoft Windows Server 2003 Standard Edition	Intel Xeon ® 2.80GHz 1 core	1	2	1	2	36	Cbim
Server	RDTP	RECORD VRF	IBM	XSeries 346	Microsoft Windows Server 2003 Standard Edition	Intel Xeon ® 3.00GHz 2 core	1	2	1	6	20	Axiom
Server	RDTP	INTEGRAZIONE CUP-RTP - Radioterapia	IBM	XSeries 346	Microsoft Windows Server 2003 Standard Edition	Intel Xeon ® 3.00GHz 2 core	1	2	1	6	73	Axiom
Server	CCE	Server Grouper + DRG	IBM	XSeries 335	Microsoft Windows Server 2003 Standard Edition	Intel Xeon ® 2.80GHz 1 core	1	1	1	2	36	webscience

1.2.2 Storage

Tipo Apparato	Impianto	Servizio/Funzione	Marca Apparato	Modello Apparato	Nr. Dischi Totali	Dimensione Tot. HDU (Gb)	Manutentore Hw/S.O
Storage	SOST	Archiviazione sostitutiva	IBM	DS3512	3	3000	NEXERA
Storage	FARMACIA	Storage FARMACIA	IBM	DS3512	8	2400	Swisslog
Storage	FLEET	Storage per VMWProdCluster01	IBM	StoreWize V7000	24	7600	Axiom
Server	RISPACS	AGFA GESTIONE IMMAGINI RADIOGRAFICHE	SUN	SUN STORAGE	16	N/A	Agfa
Server	RISPACS	AGFA GESTIONE IMMAGINI RADIOGRAFICHE	SUN	SUN STORAGE	16	N/A	Agfa
Server	RISPACS	AGFA GESTIONE IMMAGINI RADIOGRAFICHE	SUN	SUN STORAGE	16	N/A	Agfa
Server	RISPACS	AGFA GESTIONE IMMAGINI RADIOGRAFICHE	SUN	SUN STORAGE	16	N/A	Agfa
Server	RISPACS	AGFA GESTIONE IMMAGINI RADIOGRAFICHE	SUN	SUN STORAGE	16	N/A	Agfa
Storage	RISPACS	Storage VMTELE	SUN	N/A	12	N/A	Agfa
LT04 Library	RISPACS	AGFA GESTIONE IMMAGINI RADIOGRAFICHE	HP	STORAGEWORKS MSL4048	N/A	N/A	Agfa
Storage	AIS	Storage NFS	IBM	DS3950	14	1640	Axiom
Storage	FRO	CUP/ADT Storage	IBM	DS3512	5	836	Axiom
Storage	Ingegneria Clinica	STORAGE SISTEMA STORZ	HITACHI	AMS 2100	N/A	N/A	KARL STORZ
Tape Library	DR	Libreria Tivoli TSM	IBM	TS3200	44	N/A	Axiom
Storage	FLEET	Storage Gestori Macchine Virtuali Holly e Benji	IBM	DS3200	6	1670	Axiom
Storage	DR	Storage Tivoli	IBM	DS4100	14	3200	Axiom
Tape Library	DR	Libreria Tivoli TSM	IBM	TS3200	32	N/A	Axiom
Storage	DR	NAS Tivoli	Synology	RS409RP+	4	2740	Axiom
Storage	FLEET	Storage Archiviazione LOG (PIX, Juniper, Proxy, etc)	IBM	EXP300	14	2200	Axiom
NAS	FLEET	File Server Video Psichiatria	Synology	RS409RP+	4	2740	Axiom
NAS	AIMS	File Server AIMS - Log Server	Synology	RS409RP+	4	2740	Axiom
Storage	INTRANET	Storage Intranet	IBM	DS3950	4	N/A	Connexxa

Storage	EMO	Storage-Emonet	DELL	AX4-5	7	300	Axiom
Storage	PRO	Storage Subsystem FastT700 Telecom DS4400	IBM	FAStT700 17421RX	26	2600	Axiom
Storage	PRO	Storage Protocollo ed Exchange	IBM	EXP700	13	950	Axiom
Storage	PRO	Storage Protocollo ed Exchange	IBM	EXP700	13	950	Axiom
Storage	RDTP	MOSAIQ	HP	STORAGEWORKS P2000	12	3200	Elekta
Storage	FILE SERVER/CCE	FILE SERVER/CCE	IBM	EXP710	14	880	Axiom
Storage	FILE SERVER/CCE	FILE SERVER/CCE	IBM	FAStT600	14	670	Axiom
Storage	FILE SERVER	STORAGE File Server Gemini	IBM	DS4700	16	1900	Axiom
Storage	FLEET	Storage per VMWCluster01/02 - DBS	IBM	StoreWize V7000	24	10000	Axiom
NAS	CCE	Backup DB CCE	Synology	RS409RP+	4	2740	Axiom
Storage	TLP	Board management Storage	NETAPP	FAS2020	N/A	N/A	ATOS
Storage	IOP	Storage IOP Database	IBM	EXP810	11	1640	Axiom
Storage	LIS	Storage Subsystem DS4700_Noemalife	IBM	DS4700	16	2348	Axiom
Storage	LIS	Storage Subsystem DS4700_Noemalife	IBM	EXP810	8	1174	Axiom
Storage	EIS	Storage PS	IBM	DS3400	10	2800	Axiom
Storage	EIS	Storage PS BKP	IBM	DS3300	4	1800	Axiom
Storage	FLEET	SCORAGE01-BST	HP	MSA2312FC	10	970	Axiom

1.2.3 Switch

Tipo Apparato	Impianto	Marca Apparato	Modello Apparato	Manutentore
Switch FC	AIS	IBM	20301	Axiom
Switch FC	AIS	IBM	20301	Axiom
Switch FC	FRO	IBM	SAN24B-4	Axiom
Switch FC	FRO	IBM	SAN24B-4	Axiom
Switch FC	INTRANET	IBM	249824E	Connexxa
Switch FC	INTRANET	IBM	249824E	Connexxa
Switch FC	DR	IBM	249824e	Axiom
Switch FC	FLEET	IBM	249824e	Axiom
Switch FC	FLEET	IBM	249824e	Axiom
Switch FC	EIS	IBM	249824e	Axiom
Switch FC	EIS	IBM	249824e	Axiom
Switch FC	PRO/MAIL	IBM	249824e	Axiom
Switch FC	PRO/MAIL	IBM	249824e	Axiom
Switch FC	IOP	IBM	2500B16	Axiom
Switch FC	IOP	IBM	2500B16	Axiom
Switch FC	IOP	IBM	2500-16B	Axiom
Switch FC	IOP	IBM	2500-16B	Axiom
Switch FC	LIS	IBM	32R1818	Axiom
Switch FC	LIS	IBM	32R1818	Axiom
Switch FC	FLEET	IBM	26K5620	Axiom
Switch FC	FLEET	IBM	26K5620	Axiom
Switch FC	FLEET	IBM	20301	Axiom
Switch FC	FLEET	IBM	20301	Axiom
Switch FC	FLEET	IBM	20301	Axiom
Switch FC	FLEET	IBM	20301	Axiom
Switch FC	FLEET	BRD	300	Axiom
Switch FC	FLEET	BRD	300	Axiom

Switch FC	FLEET	IBM	2005-16B	Axiom
Switch FC	FLEET	IBM	2005-16B	Axiom
Switch Network	FLEET	IBM	32R1866	Axiom
Switch Network	FLEET	IBM	32R1866	Axiom
Switch Network	FLEET	IBM	32R1866	Axiom
Switch Network	FLEET	IBM	32R1866	Axiom
Switch Network	FLEET	IBM	32R1866	Axiom
Switch Network	FLEET	IBM	32R1866	Axiom
Switch Network	FLEET	IBM	32R1866	Axiom
Switch Network	FLEET	IBM	32R1866	Axiom
Switch Network	FLEET	IBM	316210-A	Axiom
Switch Network	FLEET	IBM	316210-A	Axiom
Switch Network	LIS	IBM	32R1818	Axiom
Switch Network	LIS	IBM	32R1818	Axiom
Switch Network	AIS	IBM	41Y8519	Axiom
Switch Network	AIS	IBM	41Y8519	Axiom
Switch FC	RISPACS	IBM	BROCADE 300 SWITCH FC	AGFA
Switch FC	RISPACS	IBM	BROCADE 300 SWITCH FC	AGFA
Switch FC	TLP	BROCADE 300 SWITCH FC	B300	ATOS
Switch FC	TLP	BROCADE 300 SWITCH FC	B300	ATOS

L'attuale infrastruttura tecnologica ICT e' nel corso di profonde trasformazioni su vari fronti, principalmente:

- Virtualizzazione e Consolidamento dei Server su piattaforma VMWARE
- Revisione architetturale per abilitare la Business Continuity e Disaster Recovery
- Attivazione della nuova Server Farm aziendale
- Acquisizione di servizi in Cloud

Nell'ambito di tutti gli impianti del datacenter che devono essere presi in gestione, una parte di essi nel seguito indicati dovranno convergere immediatamente nella nuova architettura definita dal progetto stesso.

Tali impianti critici sono:

impianto	Criticità	Fornitore soluzione applicativa
CCE Niguarda : cartella clinica elettronica	Mission critical H24	Niguarda
GTIS: sistema di farmaco prescrizione	Mission critical H24	Dedalus
IOP: sistema di interoperabilità	Mission critical H24	Reply Santer
PROT: sistema di Protocollo e gestione documentale	Normale	Insiel Mercato
Fileserver: sistema di storage per memoria di massa ad utilizzo degli utenti tramite il dominio aziendale (share)	normale	NA

A titolo indicativo l'infrastruttura sulla quale insistono tali impianti è la seguente:

Numero	Tipologia Host
34	xSeries server
34	eServer Blade
5	PC/Server

Numero	Tipologia Sistema Operativo
35	Microsoft Windows
34	Linux
4	Vmware vSphere

Numero	Tipologia Repository
25 TB	Storage in uso
2	Backup library
1	Backup appliance

Numero	Tipologia Device
Storage	DS4300
Storage	DS4700
Storage	DS4800
Storage	FASTt700
Storage	DS4400
Storage	DS4000
Nas	DR NAS BACKUP
Storage	Storwize v7000
Libreria	TS3200

1.2.4 IMPIANTO CCE Niguarda

ITEM	DESCRIZIONE AS-IS

Application	**CCE**
Library and datasource	Misc
Application Server	JBoss 4.2.3
Java Engine	Java Engine Hot Spot 1.6 64bit
OS	RedHat 6.3 64bit
Virtual Server	VmWare 5.0
Oracle	stdE 9.2.0.8

Ambiente di Produzione (PROD)

L'infrastruttura attuale sulla quale insiste l'ambiente attuale di produzione CCE è composta da:

- N. 4 lame fisiche suddivise (2+2) tra BL04 (Rack A21) e BL05 (RackA02), e che compongono i 4 nodi VMWProd01, VMWProd02, VMWProd03, VMWProd04 del cluster VMware VMWProdCluster01 dedicato alla componente Front-End.
- N. 1 lama fisica in BL04 (RackA21) che costituisce il database server CCE.
- N. 2 storage (Storage01-PROD e Storage02-PROD) sui quali sono ripartiti i dati di produzione del Front-End, i Datafile Oracle del DB CCE e il Backup CCE.

Per quanto riguarda la componente Front-End,al fine di garantire la massima continuità operativa in caso di fault di uno storage, esse sono suddivise sugli Storage per uno spazio totale allocato pari a 1TB netto in RAID5 e uno spazio totale occupato pari a circa 600GB netti in RAID5.

L' RDBMS scelto per la CCE è Oracle, e la versione attualmente in produzione è 9i (precisamente Oracle9i Standard Edition Release 9.2.0.8.0 - 64bit). L'attuale dimensione del DB CCE è 1,7TB netti, con una crescita/mese di circa 59GB. . I Datafile risiedono attualmente sullo Storage01-PROD sulla LUN dedicata in RAID10 (capacità allocata 3,3TB).

E' attualmente in fase di completamento un progetto di evoluzione della componente back end di CCE su piattaforma virtualizzata VMware, che porterà alla dismissione dell'attuale DB Server CCE, alla sua sostituzione con l'infrastruttura di seguito descritta e al ribilanciamento dei dati tra i due storage:

- N. 2 lame fisiche suddivise (1+1) tra BL04 (Rack A21) e BL05 (RackA02), attualmente posizionati nella nuova server farm (Nuova Server Farm ICT), che compongono i 2 nodi VMWProd05 e VMWProd06 del cluster VMware VMWProdCluster02 dedicato alla componente Back-End.

Il progetto non coinvolge invece lo strato Data Storage per il DB CCE che rimane invariato.

Dal punto di vista network l'infrastruttura è composta dai seguenti apparati esterni ai Blade:
- N. 2 switch Ethernet (Cisco Catalyst 3750) per la connessione alla Intranet Niguarda
- N. 2 switch FC (Brocade SAN24B-4) per la connessione dei BL04 e BL05 agli Storage 1 e Storage 2

L'ambiente di produzione include, oltre ai server di Front-End e di Back-End, anche altri server:

- macchine virtuali installate sul Cluster VMware VMWProdCluster01:
  - CCE-MG01-PROD: Server di gestione es. di log, tuning, reportistica.
  - CCE-WSS01-PROD: Server che espone Web Services verso il mondo esterno a CCE.
  - CCE-BCK01-PROD: Server per la gestione del backup.
  - CCE-LB01-STAG: Web Server CCE di Staging

- macchine fisiche:

- CCE-INT01-PROD, che è il gateway HL7 della CCE e che contiene script di integrazione con i diversi sistemi collegati a CCE.
- CCE-SERV02-PROD, contenente lo strumento di configurazione di CCE (PortaleBO) in PROD e TEST e Eventi (motore parsing msg HL7) in PROD e di TEST spenta.

Si segnala che è inoltre al momento in corso un progetto di fix dell'infrastruttura CCE volto a razionalizzare l'impiego delle risorse disponibili e consolidare le diverse componenti sull'infrastruttura virtualizzata di riferimento.

Ambiente di Test e Sviluppo (NOPROD)

L'infrastruttura attuale dedicata agli ambienti di Test e Sviluppo CCE comprende le seguenti componenti:

- N. 1 macchina fisica (Dbms Test Portale)
- N 3 macchine virtuali:
  - AS Sviluppo CCE e Web server Sviluppo CCE installate sul Cluster VMware VMWProdCluster01
  - server SVN per lo sviluppo del Portale installato su macchina fisica

E' attualmente in corso un progetto per la migrazione delle componenti di Test e Sviluppo CCE su un'infrastruttura dedicata composta da:

- N. 4 lame fisiche suddivise (2+2) tra BL04 (Rack A21) e BL05 (RackA02), e che compongono i 4 nodi VMWNOPROD01, VMWNOPROD02, del cluster VMware VMWNOPRODCluster01
- N. 1 storage (Storage03-NOPROD).

Backup CCE

La politica di backup attualmente implementata prevede:

- Un backup full giornaliero della base dati di produzione.
- Al completamento di questo processo viene eseguita una seconda copia del backup full più recente. Il processo così implementato garantisce quindi il mantenimento in linea di 2 copie del backup full.
- Un backup incrementale giornaliero, schedulato ogni 15 min.

A livello fisico l'infrastruttura dedicata al backup CCE include:

- Una macchina virtuale - CCE-BCK01-PROD - appartenente al Cluster VMWProdCluster01, che rappresenta il Server di Backup del Database CCE di produzione.
- La LUN CCE-DBBCK01-PROD sullo Storage02-PROD – su questa LUN viene memorizzato il backup full giornaliero ed i backup incrementali giornalieri.
- Una NAS – sulla quale viene memorizzata la seconda copia del backup full giornaliero.

Si segnala che è attualmente in corso un progetto di revisione del processo di backup implementato e della relativa infrastruttura.

1.2.5 IMPIANTO GTIS

Il presente paragrafo riporta le specifiche esigenze della soluzione Farmasafe per la gestione della farmaco prescrizione del fornitore Dedalus.

L'infrastruttura attuale adibita al funzionamento di tale impianto è costituita da un ambiente di virtualizzazione vmware su 4 lame biprocessore con 64GbRAM cadauno e storage IBM V7000 con allocato 1,2 Tb e occupato 0,334TB netti in RAID5.

ambiente	**Versione al momento in uso**
DBserver FarmaSafe@	Versione oracle 11 std
Application Sever	Tomcat 5.5.26 , Tomcat 6.0.33
WEB Server	Apache 2.2.15

1.2.6 IMPIANTO IOP

Il presente paragrafo riporta le specifiche esigenze della soluzione Piattaforma di Integrazione , della regione lombardia in gestione da parte del fornitore Santer.

Pertanto l'ambito di utilizzo risulta essere segnatamente il seguente :

1) **Area Sanitaria-Piattaforma Regionale di Integrazione**
   - JCAPS Middleware di integrazione
   - BAC Banca dati Aziendale
   - SISSWay Modulo di integrazione SISS
   - EPR-Repository Referti

I Sistemi che garantiscono l'operatività della piattaforma sono costituiti da:
- Database Server che ospitano la componente Oracle dei sistemi
- Application Server che ospitano la componente Applicativa dei sistemi
- Test Server che ospitano gli ambienti di test e pre-produzione

Tutte le componenti devono essere garantite da malfunzionamenti hardware mediante meccanismi che li rendano maggiormente affidabili rispetto ad un sistema singolo. Il fornitore dell'applicativo indica che il meccanismo utilizzato nella maggior parte delle installazioni prevede l'utilizzo della tecnologia Cluster Active / Passive tramite virtualizzazione di middleware VmWare 5.x Enterprise.

La configurazione prevederà quindi:
- 2 Database Server (BDA , EPR)
- 2 Application server (Jcaps, tomcats)

Puramente a titolo esemplificativo e di riferimenti dal punta di vista logico la soluzione applicative evidenzia le seguenti esigenze

Ruolo	**NOTE**
SERVER	NODO APPLICATIONS S.O. Oracle Linux 5.x 64 bit / RH 5.x 64Bit
SERVER	NODO APPLICATIONS S.O. Oracle Linux 5.x 64 bit / RH 5.x 64Bit
SERVER	NODO Database Server: S.O. Oracle Linux 5.x 64 bit / RH 5.x 64Bit. Oracle RDBMS V10 o superiore
SERVER	NODO Database Server: S.O. Oracle Linux 5.x 64 bit / RH 5.x 64Bit. Oracle RDBMS V10 o superiore
SERVER	PRI TEST : Oracle Linux 5.x x bit / RH 5.x 64Bit NAGIOS – MONITOR PRI SW BACKUP- MANAGEMENT STORAGE Vcenter 5.x
STORAGE	Doppio Controller Fc < 8Gbits
Backup	Agent Tivoli per connessione Backup server Centralizzato

Per il corretto funzionamento della PRI si necessitano STORAGE (ridondati) ospitanti l'ambiente VmWare tale da garantire massima affidabilità e HA .

Lo spazio minimo per le componenti PRI (APPLICATIONS , DB EPR, DB BAC, TESTS SERVER, NAGIOS) sarà di 3 Tbytes di spazio utile (al netto della parità) distribuiti equamente sui due storage.

La soluzione applicativa viene indicata compatibile ad architetture VmWare Enterprise 5.x

La procedura standard di backup e ripristino viene indicativamente così prevista :

- Backup tramite rman su LUN presentata sul server
- Restore in caso di bisogno sempre dalla LUN presentata
- L' agente di backup darà accesso alla LUN per la storicizzazione su server backup centralizzato
- Una volta ogni 6 mesi verrà messa in atto una procedura di restore su ambiente parallelo atto a consolidare la procedura di backup/restore

1.2.7 IMPIANTO PROT

Il presente paragrafo riporta le specifiche esigenze della soluzione di Protocollo e di Gestione Documentale del fornitore INSIEL.

Per quanto riguarda il sistema di Protocollo vengono presi in considerazione l'applicazione di Protocollo Client/Server attualmente in uso unitamente all'applicazione Protocollo WEB di prossima attivazione.

Vengono inoltre considerate le applicazioni:

- IOP di Protocollo (per la gestione della Interoperabilità di Protocollo) ed il collegamento ai sistemi PEC
- WS di Protocollo per la chiamata dei servizi di protocollo da parte di applicazioni esterne

Per quanto riguarda il data base di Protocollo le stime si basano su una media di circa 45.000 protocolli all'anno dei quali il 50% in arrivo.

I protocolli in arrivo hanno una media di 3,5 allegati per un totale di circa 80.000 documenti all'anno.

All'atto della protocollazione in partenza non si ha la scansione dei documenti per cui devono essere considerati i "soli" allegati a messaggi PEC o IOP in partenza in continuo incremento (ragionevole 30% all'anno).

Attualmente il DB di Protocollo occupa uno spazio di circa 100 Gb. In ambiente Oracle 9iR2 (peraltro de supportato dalla Oracle).

Il DB si trova in un Cluster Microsoft configurato in Attivo-Passivo mediante Oracle Fail Safe.

Sullo stesso cluster si trovano i database del Portale (Oracle Portal) e di FileNet.

E' al momento presente una promiscuità dei Data Base Server attuali sui quali insistono altri DB, e occorre pertanto una ricollocazione fisica su altra infrastruttura.

Il progetto, di concerto col fornitore software, deve prevedere un upgrade tecnologico, volto all'aggiornamento del software a una versione supportata quale la Oracle 11gR2. Nel progetto deve essere quotata la licenza Oracle sull'hardware proposto.

Il fornitore dell'applicativo indica una soluzione a due DB server per l'RDBMS Oracle per garantire una affidabilità di tipo attivo-attivo. L'appalto in oggetto deve comunque definire la soluzione più idonea.

Per quanto riguarda gli application server per il Protocollo WEB, per l'IOP e per i WS di Protocollo vengono richieste macchine virtuali in ambiente Linux, da crearsi in alta affidabilità su server fisici preposti all'ambiente di virtualizzazione

La progettazione del sistema HW relativo alla gestione documentale deve tener conto delle seguenti rilevazioni:

- numero di utenti complessivi che accederanno al sistema di Gestione Documentale Alfresco 800/850 utenti

- Incremento annuo previsto di documenti che verranno archiviati su Alfresco (comprensivo dei documenti che arrivano dal Protocollo e dei documenti che vengono archiviati direttamente su Alfresco) pari al 10%
- quantificazione di base a partire dall'ipotesi che tutti i documenti associati al protocollo vengano caricati sul sistema di gestione documentale
- scenario in coerenza con l'utilizzo della versione Comunity di Alfresco

L'infrastruttura predisposta dovrà essere condivisa per le esigenze del fornitore del software che eseguirà le operazioni di migrazione della soluzione dalla attuale soluzione.

Il fornitore dell'applicativo indica come sistema operativo di tutti i server : Oracle Enterprise Linux..

Il servizio oggetto di questo paragrafo dovrà essere previsto per i seguenti ambienti:
- PRODUZIONE
- TESTING

L'ambiente di TESTING, sui quali verranno effettuati anche i test automatici e di carico, dovrà avere un dimensionamento tale da poter essere paragonato all'ambiente di produzione.
I sistemi dovranno essere accessibili in remoto dal personale ENTE o fornitori esterni da ENTE autorizzati secondo le regole che ENTE indicherà in Fase 1.
Tutte le attività di rilascio applicativo e di base dati, dovranno essere effettuate da personale ENTE o fornitori esterni da ENTE autorizzati. Tali attività non riguarderanno tutto ciò che riguarda la manutenzione/evoluzione dei software di terze parti, che dovranno essere effettuate dal personale specializzato del Fornitore e concordate preventivamente con ENTE.
Il Fornitore dovrà garantire la certificazione Red Hat per i sistemi sui quali saranno ospitati i web server e gli application server.

1.2.8 IMPIANTO FILESERVER

Il presente paragrafo riporta le specifiche esigenze della soluzione di files server : memoria di massa per le postazioni di lavoro, in gestione attualmente da parte del fornitore Axiom e che andrà in carico al fornitore dell'appalto in gara.

L'infrastruttura attuale comprende le seguenti componenti:

- N. 2 server fisici costituenti i due nodi di un cluster di S.O. (Microsoft Windows Server 2003 R2 Enterprise Edition)
- N. 2 Storage: DS4700Niguarda, dimensione totale 1,9TB raw – DS4300niguarda, dimensione totale 1,55Tb raw

1.2.9 Backup

Alla data attuale, la composizione del parco macchine coinvolto nelle operazioni di backup (su tivoli) risulta cosi' composto:

- Server Fisici: 120
- Server Virtuali: 65
- Storage: 20

I Sistemi Operativi sono riportati in tabella:

Linux CentOs 5.5

Linux CentOs 5.6
Linux CentOs 5.9
Linux Debian Lenny 5.0.6
Linux Oracle Enterprise server 4.8
Linux Oracle Enterprise server 5.4
Linux Oracle VM Server 3.1.1
Linux Red Hat EL AS 3
Linux Red Hat EL AS 4
Linux Red Hat Enterprise 5.2
Linux Red Hat Enterprise 5.3
Linux Red Hat Enterprise 5.5
Linux Slackware 12.0
Linux Suse Enterprese 11
Linux Ubuntu 11.04
Microsoft Windows Server 2003 Enterprise Edition
Microsoft Windows Server 2003 R2 Enterprise Edition
Microsoft Windows Server 2003 R2 Standard Edition
Microsoft Windows Server 2003 Standard Edition
Microsoft Windows Server 2008 R2 standard
Microsoft Windows Server 2008 R2 Standard Edition
MS Windows Server 2008 R2
Oracle VM server release 2.1.2
OS 400
VMWare 5.0.0
VMWare ESXI 5.0.0
VMWARE ESXI 5.1

L'infrastruttura di Backup e' composta dai seguenti componenti:

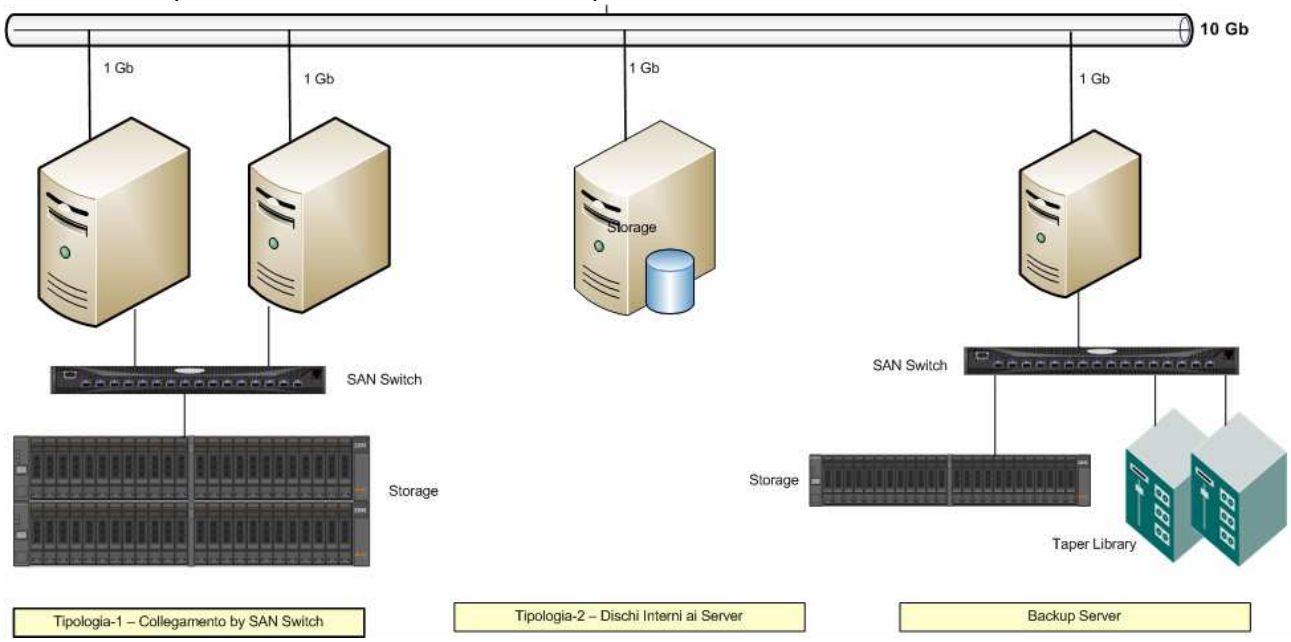
Tipo Apparato	Nome Logico	Servizio/Funzione	Marca Apparato	Modello Apparato	S.O.	Modello CPU	Nr. CPU Totali	Nr. Core Totali	RAM (Gb)	Nr. Dischi Totali	Dimensione Tot. HDU (Gb)
Server	SRV_BACKUP	Tivoli storage manager	IBM	X345	Windows 2003 Server	XEON	2	2	4	6	300
Libreria	TS3200	Backup	IBM	TS3200							
Libreria	TS3200	Backup									
Storage	DS4000	Backup	IBM	DS4100						14	3400
Nas	DR_NAS_BACKUP	Storage nas BACKUP	SYNOLOGY	RS409-RP+						4	2500

La soluzione di backup attuale utilizza:

- Tivoli Storage Manager Extended Edition Ver. 5.4
- (Numero di Licenze Tivoli Possedute ed in manutenzione: 13.440)
- Un server di Backup a cui e' collegato uno Storage, una NAS, e due librerie TS3200 in grado di gestire un totale di 80 tape (LTO4)

Ai fini del Backup, la schematizzazione dei server di Server Farm e' rappresentata nella figura di seguito, nella quale si evidenzia quanto segue:

- I server sono collegati tra loro tramite una dorsale a 10 Gb
- Ogni Impianto Tecnologico (es.: Pronto Soccorso, Cartella Clinica, Laboratorio, etc.) costituisce silos separato.
- Gli storage sono collegati ai server con Switch Fiber Channel Brocade (vari modelli)
- Ci sono due configurazioni di collegamento dei dischi: tramite SAN Switch, oppure dischi interni
- Non c'e' un'unica SAN a livello di Server Farm;
- Sono presenti varie SAN a livello di Impianto.



Dimensionamento attuale del Backup

- Volume dei dati nel Primary Storage Pool di Tivoli: 45 TB
- Volume dei dati backuppati giornalmente (valore medio): 3 Tb
- Volume dei dati di primo backup: 28 Tb
- Finestra di backup: dalle 20:00 alle 06:00

- Il sistema di backup viene gestito centralmente da un unico fornitore di servizi che si occupa della gestione e monitoraggio del Server Tivoli e dei backup sui singoli server.
- Le policy di backup vengono impostate dai fornitori degli applicativi, con la partecipazione del servizio centralizzato
- Il backup dei database producono un dump su disco locale (RMAN di Oracle) e successivamente l'agent Tivoli locale si occupa di trasferire i dati al server Tivoli centrale

I limiti principali dell'attuale infrastruttura di backup sono i seguenti:

- Congestione della rete durante il trasferimento dei dati sul server centrale Tivoli
- Tempi di backup molto lunghi; per i DB di piu' grandi i tempi di backup superano l'arco delle 24 ore.
- Tempi lunghi di restore dei dati da nastro.
- Obsolescenza del Server Tivoli di Backup centralizzato
- Obsolescenza della Versione Tivoli (es: Non supporto agli ambienti virtualizzati)
- Licensing Tivoli per device e non per TB di dati.

2 OGGETTO DELLA FORNITURA E REQUISITI GENERALI

Oggetto del presente capitolo è la disciplina delle attività di fornitura e di predisposizione dell'infrastruttura, comprensiva delle relative licenze, nonché attività specialistiche relative all'infrastruttura stessa e servizi di gestione sistemistica come precedentemente indicato.

Le attività di seguito riportate si ritengono incluse nel corrispettivo della fornitura ed il fornitore non potrà vantare diritto ad altri compensi:

- presa in carico del servizio/governo della Fornitura e delle singole prestazioni, inclusa la pianificazione e consuntivazione periodica e in generale qualsiasi attività di coordinamento svolta dai referenti del contratto;
- sviluppo della documentazione di fornitura;
- predisposizione e gestione di un portale documentale;
- predisposizione di un sistema di ticket management per la gestione di incident e richieste;
- assicurazione qualità;
- assicurazione della sicurezza e della riservatezza dei dati personali;
- predisposizione degli ambienti richiesti;
- predisposizione del sito e del piano di disaster recovery;
- erogazione della fornitura;
- passaggio di consegne al termine della fornitura.

Spunti per la progettazione del nuova architettura possono essere così sintetizzati:

- allestimento di due Data Center virtualizzati per la Business Continuity (BC), da collocarsi inizialmente nelle medesima server farm, con predisposizione per spostamento a sito secondario (specificare connettività richiesta per collegamento data center). (copia sincrona dei dati)
- allestimento di un Data Center virtualizzato di Disaster Recovery (DR (copia asincrona dei dati)
- virtualizzazione e continuità operativa degli strati application, middleware e database
- si ipotizza il seguente carico di lavoro per ciascun server del perimetro:
    - 60% Avg CPU util
    - 80% Avg RAM util
    - 440 Avg IOPS
    - 55Mbps Avg Network Throughput
- Benche' alcune situazioni possano richiedere server fisici, si indica la potenziale massimizzazione della soluzione già in produzione di virtualizzatori Vmware
- Messa in sicurezza degli impianti critici → attraverso ridondanza della tecnologia
- Migliore utilizzo delle risorse di infrastruttura (RAM, CPU, Network, Storage) → attraverso consolidamento e virtualizzazione, scalabilità dell'infrastruttura
- Garanzia di massima disponibilità dei servizi erogati → attraverso architettura di BC
- Garanzia di efficienza del ripristino dei servizi erogati in caso di disastro → attraverso architettura di DR
- Ottimizzazione efficienza operativa anche nell'implementazione di nuovi servizi IT
- Ottinizzazione della gestione
- Ottimizzazione costi di esercizio e di manutenzione / riduzione TCO
- Minimizzazione costi di licenza (es. DB e virtualizzazione)
- Scalabilità ad altri impianti al di fuori del perimetro attuale
- Soluzione in campus con RPO e RTO nulli
- Storage efficiency in grado di far risparmiare diffusamente spazio disco (deduplica, thin provisioning, compressione, flexclone, snapshot …)

- Possibilità di sfruttare la connettività 10G per accesso tramite *NFS* o FCoE (in aggiunta al tradizionale FC)
- Integrazione possibile con gli ambienti applicativi per avere molteplici copie consistenti dei database nel corso della giornata (*SnapManager*)
- Possibilità di sfruttare in maniera altamente prestazionale anche lo spazio SATA grazie alle *Flash Cache*
- Disponibilità del dato con protezione geografica
- Minimizzazione di perdita di dati
- Semplicità nella gestione e downtime dei sistemi ridotti
- Rapidità di recovey in caso di disastri
- Minimizzazione interruzioni applicative per gli utenti
- Ridondanza e complessità
- Linearità e semplificità nel risalire alle cause in caso di down
- Riuso e razionalizzazione hardware esistente
- Garanzia di Supporto di tutti i S.O. in uso
- Garanzia di Supporto di tutti i DB in uso
- Garanzia di Ridondanza logica e fisica delle componenti e del dato
- Integrazione con architettura di backup centralizzata target

2.1 PREDISPOSIZIONE DELL'INFRASTRUTTURA TARGET (FASE INFRASTRUTTURA)

Il Fornitore dovrà a proprio esclusivo onere e spese, senza alcun costo aggiuntivo per l'Ente, procedere alla predisposizione dell'infrastruttura.

Tali attività dovranno essere concluse, pena l'applicazione delle penali di cui al contratto, entro il termine perentorio di due (2) mesi solari decorrenti dalla data di ricezione dell'ordinativo di acquisto.

Durante il periodo di predisposizione dell'infrastruttura, dovranno essere svolte le seguenti attività da parte del Fornitore aggiudicatario:

1. redazione del progetto esecutivo
2. predisposizione del modello organizzativo;
3. formalizzazione del piano di comunicazione;
4. predisposizione sistema per reportistica periodica;
5. predisposizione del piano della qualità;
6. predisposizione e condivisione della proposta del supporto sistemistico;
7. definizione delle modalità di accesso agli ambienti da parte dell'ENTE e dei suoi fornitori applicativi;
8. ricezione da parte del fornitore uscente del know how e delle informazioni necessarie alla presa in carico. Il risultato dell'attività (per esempio documentazione tecnica ed operativa) dovrà essere successivamente trasferito al personale dell'ENTE, o a terzi da essa designati;
9. progettazione e predisposizione dell'infrastruttura relativa a tutti gli impianti e gli ambienti previsti, comprendendo il sito di Disaster Recovery ed il relativo Piano;
10. progettazione dei sistemi di backup/restore e relativo piano di collaudo;

2.1.1 Progetto e crono programma esecutivo

Il Fornitore dovrà produrre un progetto esecutivo che esplichi in maniera esaustiva le modalità di attuazione della fornitura presso l'Ente dettagliando attività, tempi, risorse e procedure operative.

Il progetto esecutivo include la pianificazione di massima che consente di individuare i "major deliverables" e le date con i principali milestones di progetto.

Il piano deve essere suddiviso in più fasi, come di seguito riportate:

Per quanto riguarda il progetto esecutivo , relativo alle attività da svolgere per la configurazione degli apparati e la loro predisposizione per l'avvio della fase di consolidamento, dovranno essere specificate e documentate le configurazioni di dettaglio riguardanti:

- la definizione delle partizioni logiche (in termini di CPU, RAM, dispositivi di I/O);
- l'assegnazione delle risorse virtuali alle partizioni logiche;
- la strategia e le modalità di migrazione relative a tutti gli impianti ed ambienti interessati dalla prima fase del progetto
- l'insieme dei test da eseguire nell'ambito del Collaudo Infrastrutturale
- l'insieme dei test da eseguire nell'ambito del Collaudo Funzionale.

Il progetto esecutivo, comprensivo del crono programma esecutivo, dovrà essere concordato e quindi accettato dall'ENTE.
Il FORNITORE si impegna a presentare il progetto e cronoprogramma esecutivo **entro e non oltre 20 gg solari** a partire dalla data di inizio del progetto (data di ricezione dell'ordinativo di acquisto).

Si specifica quanto definito e documentato nel progetto esecutivo sarà oggetto di valutazione e certificazione da parte dell'ENTE. Il FORNITORE ha obbligo di apportare, senza oneri aggiuntivi, le eventuali modifiche che dovessero rendersi necessarie a seguito di tali valutazioni.

2.1.2 Consegna, Installazione e Collaudo Hardware

Le apparecchiature dovranno essere consegnate ed installate presso la Server Farm dell'ENTE e i materiali di risulta d'imballo saranno ritirati a cura del FORNITORE.

Il FORNITORE dovrà procedere alla consegna del materiale richiesto in fornitura **entro massimo 30 gg solari** dalla data di inizio del progetto (data di ricezione dell'ordinativo di acquisto).
L'installazione degli apparati è prevista **entro 15 gg solari** dalla consegna degli stessi presso la Server Farm dell'ENTE.

Si specifica che non verrà permesso l'inizio delle installazioni in assenza del progetto esecutivo definitivo approvato dall'ENTE.

Nel piano d'installazione (incluso nel cronoprogramma esecutivo complessivo) si dovrà tenere conto di quanto segue:

- è facoltà dell'ENTE stabilire le priorità d'installazione;
- potrà essere richiesto di espletare alcune fasi al di fuori del normale orario di lavoro, anche in orari notturni e/o festivi;
- è compito del fornitore certificare il completo funzionamento degli apparati coinvolti

In merito alla fase di verifica delle funzionalità di base, l'ENTE collauderà tutte le componenti hardware e software oggetto della fornitura. Ogni componente dovrà risultare conforme a quanto dichiarato dal produttore e soddisfare quanto specificato dal presente capitolato tecnico. Per l'accettazione da parte dell'ENTE del collaudo delle parti (Collaudo Hardware), il fornitore dovrà predisporre dei test da eseguire sui singoli sottosistemi (RAM, CPU, dischi, dispositivi di I/O etc.) producendo un report sull'esito dei test, per consentire all'ENTE di poter accertare la presenza di tutte le parti oggetto di fornitura.

2.1.3 Configurazione e Collaudo Infrastrutturale

La configurazione degli apparati è prevista **entro 15 gg solari** dal termine dell'installazione e dal relativo collaudo hardware e si conclude a sua volta con il collaudo infrastrutturale.

Al termine della predisposizione dell'infrastruttura, il fornitore dovrà garantire la disponibilità di tutto ciò che è necessario alla corretta e completa gestione del servizio, in linea con le performance e secondo i livelli di servizio richiesti.

Durante la fase di predisposizione dell'infrastruttura, i servizi infrastrutturali in esercizio continueranno a essere erogati dal Fornitore uscente.

2.1.4 Migrazione e Collaudo Funzionale

Superato il Collaudo Infrastrutturale, avrà inizio la fase di migrazione degli impianti.

Tale attività dovrà essere svolta nel rispetto dei seguenti requisiti:

- la strategia di migrazione dovrà essere tale da salvaguardare la continuità operativa e minimizzare gli eventuali impatti sugli impianti;
- dovranno essere mantenuti e verificati i livelli di Alta Affidabilità (cluster, ridondanza dell'hardware e delle connessioni) e di Disaster Recovery almeno pari a quelli in essere per gli attuali impianti.

L'attività di migrazione dei suddetti sistemi, comprensiva dei Collaudi Funzionali descritti di seguito, avrà una **durata massima di 60 gg solari dal Collaudo Infrastrutturale**, al termine dei quali i servizi migrati dovranno essere attivi sui nuovi sistemi, nel rispetto dei requisiti citati in precedenza.
Al termine dell'attività di migrazione di ciascuno dei servizi riportati nel precedente elenco, si procederà al relativo Collaudo Funzionale, in cui i nuovi servizi saranno comparati a quelli erogati dall'attuale infrastruttura.

L'ente procederà all'accettazione formale del Collaudo Funzionale una volta riscontrato il superamento dei test definiti all'interno del progetto esecutivo. Condizione indispensabile per l'accettazione del Collaudo Funzionale sarà inoltre il rilascio di tutta la documentazione esecutiva relativamente al progetto, all'architettura ed ai sistemi implementati e delle relative note operative per le procedure di Alta Affidabilità e Disaster Recovery, qualora siano necessarie modifiche alle attuali procedure.

Il progetto si considera concluso con l'accettazione da parte dell'ENTE dei Collaudi di tutti gli impianti.

2.1.5 Collaudo della Fase INFRASTRUTTURA

Il collaudo della Fase 1 si articolerà in due momenti formali:

1. Il fornitore, 2 (due) settimane prima del termine perentorio di **90gg solari decorrenti dalla data di ricezione dell'ordinativo di acquisto**, dovrà fornire all'ENTE documentazione completa di verifica esaustiva contenente tutti i test eseguiti e le attività condotte. Tali test dovranno attestare il corretto funzionamento delle componenti dal punto di vista sistemistico, prestazionale e funzionale.
2. Entro il termine perentorio di **120gg solari decorrenti dalla data di ricezione dell'ordinativo di acquisto**, il Fornitore e l'ENTE dovranno eseguire e concludere in contraddittorio le attività di verifica dell'esatta esecuzione della predisposizione dell'infrastruttura, nonché a collaudare ed eseguire le dovute prove di accettazione e collaudo, alla presenza del personale tecnico del Fornitore ed in presenza di un rappresentante dell'ENTE.

A seguito della verifica della corretta ed avvenuta esecuzione di tali attività verrà redatto un apposito "verbale di conclusione della fase Predisposizione dell'infrastruttura". La data riportata nel predetto firmato dalle parti, è da considerarsi quale "Data di Accettazione del Servizio", e di avvio in produzione dell'infrastruttura nel suo complesso.

2.1.6 Garanzia e aggiornamento tecnologico

La garanzia (per la durata contrattuale) di tutte le componenti di infrastruttura incluse in fornitura comprende tutti gli oneri, nessuno escluso, per il ripristino del corretto funzionamento in caso di impianto mal funzionante.

La data di decorrenza della garanzia decorre dalla data di collaudo della Fase Infrastruttura.

Durante il periodo di garanzia, l'Impresa è obbligata a garantire gratuitamente l'aggiornamento tecnologico della strumentazione installata.

Nel predisporre l'offerta l'Impresa provvederà a fornire una descrizione dettagliata di tutti i componenti di mercato e l'indicazione di eventuali componenti esclusivi.

2.2 EROGAZIONE DEL SERVIZIO DI GESTIONE SISTEMISTICA (FASE SERVIZI)

La Fase Servizi, "Erogazione del Servizio di Gestione Sistemistica", è la fase in cui il Fornitore garantisce l'erogazione dei servizi di manutenzione e monitoraggio sistemistica (fino al livello RDBMS incluso) per tutto il periodo di validità del Contratto. Durante questa fase il fornitore dovrà garantire la produzione e l'aggiornamento della documentazione relativa a tutti gli aspetti sistemistici ed applicativi che ne consentano la conduzione.
Per l'intera durata della fase di erogazione dei servizi, dovranno essere previsti dei momenti di verifica periodici durante i quali verranno rilevati i livelli effettivi di servizio rispetto a tutti gli indicatori di qualità definiti.
Il servizio essere organizzato a partire da note best practice e/o metodologie standard (ITIL, COBIT, ISO ed altri).

La presa in carico dei servizi deve avvenire in 90 gg solari con la seguente modalità:

Fase	Descrizione
P1	Fase di Adempimenti Contrattuali (dalla data di ricezione dell'ordinativo di acquisto alla firma del contratto)
P2 (durata 1 mesi calendariale)	Fase di Predisposizione dei servizi (periodo in cui il Fornitore si prepara ad erogare i servizi in fornitura e predispone il progetto esecutivo) in tale arco temporale le risorse potrà essere inferiore a quanto dichiarato in offerta, gli SLA saranno a carico del Fornitore uscente.
P2 bis (durata 1 mese calendariale)	Fase di Predisposizione dei servizi (periodo in cui il Fornitore si prepara ad erogare i servizi in fornitura) in tale arco temporale le risorse dovrà essere quanto dichiarato in offerta, gli SLA saranno a carico del Fornitore uscente.
P3 (durata 1 mese calendariale)	Fase di Ramp-Up (fase in cui il Fornitore prende effettivamente in carico i servizi in fornitura a seguito dell'approvazione del progetto esecutivo) le risorse dovranno essere quanto dichiarato in offerta, gli SLA saranno a carico del Fornitore aggiudicatario.
P4	Fase di Regime Operativo (INIZIO PERIODO CONTRATTUALE)

Le componenti principali del servizio richiesto possono essere così riepilogate:

- Manutenzione Ordinaria
- Manutenzione Straordinaria
- Manutenzione Evolutiva
- Monitoring e Performance
- Reperibilità

Nel capitolo 4, vengono dettagliati i requisiti per le componenti di servizio richieste.

2.3 PIANIFICAZIONE DELLE FASI OPERATIVE

Viene di seguito riportata una pianificazione di alto livello delle fasi operative che sintetizza le scadenze riportate nei paragrafi precedenti:

milestones dalla data di ricezione dell'ordinativo di acquisto
- crono programma esecutivo -> 20 gg solari
- consegna materiale e installazione e configurazione -> 60 gg solari
- attivazione di tutti i servizi gestionali -> 90 gg solari

- migrazione con collaudo funzionale nuova infrastruttura -> 120 gg solari

2.4 CHIUSURA E PASSAGGIO DI CONSEGNE (FASE FINE CONTRATTO)

Al termine della fase di erogazione dei servizi, al Fornitore aggiudicatario, senza ulteriore costo aggiuntivo per l'ENTE, è richiesto di assicurare il trasferimento di know-how e tecnologico al/ai nuovo/i fornitore/i subentrante/i (Fase Fine Contratto) e produrre la relativa documentazione.
Il Fornitore subentrante dovrà essere messo nella condizione di accedere alla documentazione prodotta durante la Fase INFRASTRUTTURA e Fase SERVIZI del Contratto.

2.5 MODELLO ORGANIZZATIVO, RESPONSABILI CONTRATTUALI E REFERENTI TECNICI

Il fornitore dovrà, proporre un modello organizzativo per gestire l'erogazione dei servizi e dei rapporti con l'ENTE. A corredo della proposta organizzativa dovranno essere consegnati i CV delle risorse che verranno impegnate in modo tale che ENTE ne valuti l'adeguatezza rispetto ai criteri di seguito riportati.

Il fornitore dovrà mettere a disposizione un gruppo di figure professionali di coordinamento composto almeno dai profili di seguito riportati:

- Responsabile del Contratto
- Project Manager
- Manager

In caso di sostituzione delle risorse nel corso del Contratto di Fornitura, il Fornitore dovrà tempestivamente darne comunicazione scritta all'ENTE, garantendo inoltre un adeguato affiancamento che non generi discontinuità nel servizio. In particolare, per quanto riguarda la figura del Project Manager, l'eventuale nomina di un nuovo Project Manager in sostituzione del precedente deve essere comunicata all'ENTE con un anticipo di almeno 15 (quindici) giorni solari rispetto alla data di attuazione del provvedimento. L'ente si riserva di confermare o meno la richiesta di sostituzione, come richiedere la sostituzione di personale già allocato. In caso di parere negativo di allocazione di risorsa da parte dell'ente il fornitore dovrà immediatamente riproporre altra candidatura.

2.5.1 Responsabile del Contratto

A partire dalla data di attivazione del Contratto, pena l'applicazione delle penali, e per tutta la durata dello stesso, il Fornitore dovrà mettere a disposizione un Responsabile del Contratto, i cui riferimenti dovranno essere indicati all'ENTE nella documentazione richiesta ai fini della stipula del contratto, secondo quanto indicato nel Disciplinare di gara.
Il Responsabile del contratto dovrà essere in grado di:
- implementare le azioni necessarie per garantire il livello dei servizi attesi nonché il rispetto delle prestazioni richieste;
- essere punto di riferimento a cui l'ENTE potrà fare continuamente riferimento per ogni attività o problema riguardante la fornitura stessa e che sarà anche responsabile;
- gestire tempestivamente gli eventuali reclami/disservizi anche tramite l'attivazione delle opportune escalation al proprio interno nel caso di problemi rilevanti la cui risoluzione possa richiedere l'attivazione di livelli gerarchici superiori.

E' fatta salva la possibilità per il Fornitore di mettere a disposizione ulteriore personale specializzato per una corretta prestazione di servizi.

2.5.2 Project Manager

Di seguito la descrizione delle principali mansioni che dovranno essere ricoperte dal Project manager:

- costituisce l'interfaccia strategica verso ENTE, in accordo con la quale definisce le linee strategiche relative alle singole aree di attività e recepisce i risultati intermedi e finali ottenuti, valutandone la coerenza con le linee strategiche definite;

- valuta l'impatto strategico di eventuali criticità o problematiche sorte nel corso dello svolgimento delle attività, proponendo soluzioni e azioni correttive;
- rappresenta il riferimento del Gruppo di Lavoro per le tematiche di tipo strategico.
- è responsabile, fra gli altri, dei seguenti adempimenti:
  - delle relazioni con l'ENTE;
  - del rilascio nei tempi previsti di tutta la documentazione di progetto;
  - della disponibilità delle risorse e del personale specializzato per le attività di realizzazione;
  - del coordinamento di tutte le comunicazioni previste dal contratto;
  - dell controllo delle scadenze sulla base delle pianificazioni concordate;
  - nel rappresentare il fornitore nelle riunioni di avanzamento e di coordinamento lavori nelle fasi di realizzazione e di esercizio.

Requisiti minimi:
- laurea
- certificazione in Project Management (PMP, Prince2 od altre)
- esperienza di almeno 10 anni nel ruolo (indicare referenze)

2.5.3 Manager

Il fornitore dovrà mettere disposizione un referente specifico (Manager) per le attività di carattere infrastrutturale, a cui farà riferimento il "gruppo di progetto" dedicato alla gestione dell'infrastruttura. Il Manager si interfaccia con ENTE per tutte le questioni di tipo tecnico/infrastrutturale ed è costantemente in contatto con il Project Manager, ai fini del corretto coordinamento e pianificazione delle iniziative.

Requisiti minimi del Manager:
- laurea in discipline tecniche
- esperienza di almeno 10 anni nel ruolo
- certificazione in Project Management (PMP, Prince2 od altre) ed una esperienza nel ruolo di almeno 5 anni.

2.5.4 Gruppo di Progetto

Tale gruppo di progetto dovrà essere composto da un adeguato numero di risorse aventi comprovata esperienza e professionalità idonee a garantire la realizzazione e la gestione della piattaforma infrastrutturale e delle componenti applicative collegate. Il gruppo dovrà comprendere i profili descritti di seguito.

I Profili professionali del Gruppo di Progetto sono i seguenti :

2.5.4.1.1 RDBMS DATABASE ADMINISTRATOR

Laureato con almeno 5 anni di anzianità nel ruolo. Si richiede la certificazione Oracle e comprovata esperienza nella gestione operativa di database mission critical, attività di monitoraggio, tuning e troubleshooting.

2.5.4.1.2 SISTEMISTA SYSTEM MANAGEMENT

E' una figura professionale caratterizzata dai seguenti skill:
- capacità di pianificare ed eseguire l'installazione e la configurazione degli ambienti operativi situati presso l'Ente dettagliati negli Allegati 1a, 1b, 1c ed in particolare nei sistemi di seguito riportati;
- esperienza nella gestione di server (Windows NT/2000/2003/2008, linux);
- conoscenza ed esperienza su sistemi:
  - Microsoft Windows NT 4.0 Server e workstation;
  - Microsoft Windows 2000/2003/2008/NT/XP;
  - Mac
  - Linux;
  - Unics;
  - Aix;
  - SAN;
  - MySQL;
  - Sun Solaris;

- Oracle-rdbms
- SQLServer;
- Symantec Antivirus, McAfee

• capacità di operare in ambienti server critici dal punto di vista dell'affidabilità e del numero di utenti supportati;
• conoscenze tecniche d'analisi e risoluzione problemi complessi negli ambienti sopra citati;
• gestione della Software Distribution;
• gestione della Patch Distribution;
• gestione configurazione Sistema Antivirus.
• capacità di interfacciarsi con supporto di terzo livello della propria struttura o di fornitori terzi per risolvere problematiche inerenti ai sopra citati sistemi.

2.5.4.1.3 REDHAT ADMINISTRATOR

Laureato con almeno 5 anni di esperienza nel ruolo. Si richiede comprovata esperienza nella gestione di sistemi RedHat:
- Gestione ed aggiornamento dei sistemi
- Capacità di troubleshooting dei sistemi
- Tuning e monitoraggio dei sistemi

Viene richiesta la certificazione RedHat. Costituirà titolo preferenziale, l'esperienza nella gestione di applicativi basati su Jboss EAP su sistemi RedHat.

2.5.4.1.4 JBOSS ADMINISTRATOR

Laureato con almeno 5 anni di esperienza nel ruolo. Si richiede comprovata esperienza nella gestione di application server JBoss EAP:
- Gestione ed aggiornamento dei sistemi
- Capacità di troubleshooting dei sistemi
- Tuning e monitoraggio dei sistemi

Viene richiesta la certificazione RedHat su JBoss. Costituirà titolo preferenziale, l'esperienza nella programmazione di applicazioni J2EE.

2.5.4.1.5 ESPERTO DI SISTEMI DI MONITORAGGIO

Laureato con almeno 5 anni di esperienza nel ruolo. Si richiede comprovata esperienza nella gestione di sistemi di monitoraggio. :
- Gestione ed aggiornamento dei sistemi
- Capacità produrre adeguate reportistiche.

Costituirà titolo preferenziale, l'esperienza nel monitoraggio di sistemi J2EE mission critical.

3 INFRASTRUTTURA TARGET: DESCRIZIONE RICHIESTA E REQUISITI

3.1 INTRODUZIONE

In questo capitolo viene descritta l' infrastruttura target richiesta, indicando obiettivi, caratteristiche principali e requisiti.
Oltre ai requisiti specifici indicati nel presente capitolo, alla fornitura dei servizi infrastrutturali si applicano comunque i requisiti generali indicati.

Ciascun concorrente alla Gara deve fornire in sede di offerta tecnica l'architettura e il progetto tecnico per la realizzazione dell'infrastruttura, da cui si possa verificare l'adeguatezza rispetto alle applicazioni da prendere in carico e ai livelli di servizio e di sicurezza richiesti. Tali descrizioni saranno oggetto di valutazione specifica nell'ambito della valutazione della componente qualitativa dell'offerta.

Ciascun concorrente dovrà includere all'interno dell'offerta tecnica apposita documentazione in cui verranno indicati:

- descrizione dell'infrastruttura proposta per i vari ambienti richiesti e di come questa soddisfi ciascun requisito indicato punto per punto, le principali best practice o standard di settore adottati;
- descrizione del progetto di presa in carico ed implementazione della infrastruttura target con relativo piano e tempistiche.

Tali aspetti saranno oggetto di analisi in fase di valutazione dell'offerta stessa.

Il servizio gestisce tutti gli apparati/server dell'ente indicati nel presente documento.

3.2 DESCRIZIONE RICHIESTA

3.2.1 Descrizione dell'Infrastruttura Target

Il concorrente dovrà presentare un progetto dettagliato di implementazione dell'infrastruttura target, con il dettaglio per ciascun impianto ed ambiente gestito.

Andranno dettagliate le varie opzioni disponibili con i relativi pro e contro di natura tecnica (standard di mercato e best practice), economica (acquisto e TCO), gestionale ed operativa (come risponde ai requisiti elencati). Andrà inoltre definita una mappa completa degli indicatori usati per la valutazione ed, infine, andrà indicata l'opzione ritenuta più efficace per gli obiettivi e i requisiti indicati.
Per la soluzione individuata dovrà essere presentata un'analisi di rischi e le relative azioni intraprese per mitigarli o controllarli.

3.3 REQUISITI DI INFRASTRUTTURA

Di seguito vengono riportati sia i requisiti che il fornitore dovrà rispettare sia ulteriori elementi, utili per la presentazione dell'offerta tecnica.

Si richiede che i sistemi proposti mantengano la medesima configurazione attualmente in essere in termini di software di sistema (vendor e versione). Questo significa che, in particolar modo per l'ambiente di produzione, tutti i software di terze parti (versioni di sistemi operativi, database, application server, web server...) dovranno essere i medesimi.

L'infrastruttura per gli ambienti di PRODUZIONE e PRE-PRODUZIONE dovrà rispondere ai seguenti requisiti:

- Performance
- Scalabilità
- Sicurezza
- Protezione
- Continuità di servizio e fault tolerance
- Disaster Recovery
- Backup & Recovery
- Aggiornamento e licenze
- Supporto sistemistico
- Monitoraggio

Sarà onere dell'offerente indicare se e come tali requisiti saranno disponibili anche sugli altri ambienti di FORMAZIONE, TESTING e SVILUPPO.

3.3.1 Scalabilità

L'infrastruttura proposta in sede d'offerta dovrà garantire la massima flessibilità in funzione dell'evoluzione dei carichi che potranno variare sulla base di variazioni normative o scelte funzionali. Si richiede la progettazione di un'infrastruttura che possa, grazie alle scelte metodologiche, adattarsi in maniera incrementale alle nuove condizioni del servizio in termini di:

- Capacità elaborativa
- Banda dati
- Storage
- Distribuzione dei carichi
- Throughput
- Numero di utenti.

Al verificarsi di tali condizioni il Fornitore sarà tenuto a predisporre opportuna documentazione in cui verranno descritti gli interventi da effettuare in base all'analisi fatta ed assieme all'ENTE verranno concordate le azioni opportune.
Tali interventi dovranno essere effettuati a valle di indicazioni fornite dall'ENTE circa variazioni normative e funzionali note a priori, sia in base ad un approccio proattivo dettato da un'attenta analisi dei trend di evoluzione dei carichi.

3.3.2 Sicurezza

Andranno predisposte tutte le necessarie configurazioni in modo da garantire il massimo controllo nell'accesso all'infrastruttura. Andrà garantita la sicurezza sia a livello fisico che logico degli apparati e dei dati. L'infrastruttura dovrà inoltre essere progettata secondo le best practice e gli standard di mercato in modo da garantire la sicurezza degli accessi ed intercettare tentativi di accesso fraudolento sollevando opportuni allarmi e segnalazioni.
Tali eventi dovranno essere tracciati in apposti repository per un'analisi storica successiva.
In sede di offerta tecnica il concorrente dovrà descrivere tutti gli accorgimenti che intenderà adottare per limitare le situazioni insicure ed un opportuno studio di analisi dei rischi in cui evidenziare i possibili impatti e come si intende mitigarli.

3.3.3 Protezione

Il fornitore dovrà predisporre tutte le misure necessarie a garantire la massima protezione dei dati gestiti ed immagazzinati dall'infrastruttura. Pertanto l'infrastruttura dovrà essere progettata in modo da garantire la protezione dei dati e l'impossibilità da parte di persone non autorizzate, anche interne all'infrastruttura, di accedervi. Il concorrente dovrà quindi definire ruoli e responsabilità in modo da non creare inutili limitazioni e complessità alle persone autorizzate nell'accedere ai dati, ma al contempo impedendo ai non autorizzati qualsiasi tipo di accesso.
Andranno inoltre predisposti meccanismi di audit in grado di registrare tutte le operazioni eseguite su dati ritenuti sensibili.
La protezione andrà garantita a tutti i livelli coerentemente con gli obiettivi specificati. In particolare andranno predisposte misure opportune nella protezione dei dati sensibili a livello di database, log, memoria applicativa, comunicazioni di rete.

Andranno indicati tutti i processi tramite cui sarà possibile consentire al personale autorizzato di richiedere i permessi necessari per operare sui dati sensibili.

3.3.4 Continuità di servizio e fault tolerance

L'infrastruttura dovrà garantire la continuità di servizio in tutti i componenti infrastrutturali e le linee dati utilizzate.

Tutti gli elementi dell'infrastruttura dovranno essere ridondati in maniera da eliminare qualsiasi single point of failure. La ridondanza dovrà essere garantita a partire dalle linee dati di ingresso nell'infrastruttura, per tutti i componenti di rete previsti (firewall, switch, load balancer, linee dati) e relativi software installati, fino ai server, agli application server, alle basi dati ed agli storage.
L'infrastruttura dovrà essere progettata in modo da garantire il massimo livello di continuità di servizio tramite l'utilizzo di opportune tecniche di ridondanza ed eliminazione dei single point of failure secondo le più aggiornate best practice disponibili.
In particolare andranno previste soluzioni a tutti i possibili problemi legati al malfunzionamento o alla manutenzione di componenti di rete, firewall, proxy e reverse proxy, server, software di sistema e di infrastruttura, storage e linee di comunicazione.

Tali attività dovranno essere eseguite in maniera trasparente senza evidenti impatti sul servizio offerto.

Il fornitore dovrà proporre e concordare con ENTE tutti i principali KPI e SLA, ulteriori rispetto agli sla minimi richiesti e/o offerti, che si intende garantire e come questi potranno essere calcolati in maniera automatica durante l'esercizio della piattaforma. Periodicamente dovranno essere presentati report sull'andamento dei parametri indicati.

3.3.5 Disaster Recovery

In ottemperanza all'art.50-bis del Codice dell'Amministrazione Digitale (CAD) il Fornitore dovrà predisporre e fornire ad ENTE il piano di Disaster Recovery; a seguito di opportuna analisi degli impatti (BIA) dovrà essere progettata e quindi predisposta un'infrastruttura di Disaster Recovery in modo da garantire continuità operativa in caso di grave problema legato al sito primario.
Il dimensionamento delle risorse di connettività ed elaborative dovrà essere coerente con i risultati evidenziati nell'analisi di impatti e dovrà garantire prestazioni ragionevoli per la durata del disservizio del sito primario.

E' oggetto di Disaster Recovery solo l'ambiente di Produzione della piattaforma.

Relativamente alle procedure di gestione del sito di Disaster Recovery si richiede di implementare tutte le relative best practice già definite a livello di soluzioni standard.

Anche sul sito secondario dovranno essere attivi i sistemi di monitoraggio ed allarme previsti per l'ambiente di produzione principale.

3.3.6 Backup e Restore

Il fornitore dovrà proporre e concordare con l'Ente il piano di gestione di backup e restore.

Andrà predisposto un piano periodico di backup di tutti gli impianti gestiti in modo da garantire in qualsiasi momento il ripristino in tempi rapidi. Nel piano andranno evidenziate le misure atte al mantenimento delle copie di backup ed alla loro protezione in appositi siti sicuri.

Il backup riguarderà dati, log e tutto l'ambiente applicativo che si riterrà utile salvare.

L'intero processo di Backup e Restore dovrà essere contenuto in un documento, costantemente aggiornato ed accessibile all'Ente, indicante i processi predisposti, i riferimenti operativi e gli SLA garantiti in caso di ripristino.

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

Si riepilogo le principali attività da prevedere:

- gestire il sistema di backup dell'Ente;
- eseguire le procedure di backup e recovery con frequenza concordata tra Ente e Fornitore;
- eseguire le procedure di backup secondo le modalità previste;
- controllo delle unità di backup, dei supporti e manutenzione preventiva;
- garantire la capacità di ripristino dei dati necessari al funzionamento del servizio;
- garantire l'integrità e la disponibilità dei dati necessari al funzionamento del servizio in caso di eventi che comportino perdite di dati statici e variabili;
- controllare che tutte le attività di salvataggio siano congruenti allo status di esercizio ed abbiano avuto buon esito;
- proporre contenuto report riassuntivi backup/restore;
- fornire report riassuntivi backup/restore;
- eseguire operazioni di backup e restore (365xh24);
- fornire indicazioni sulle soluzioni per migliorare le capacità di ripristino dati;
- notificare in caso di mancato backup i referenti dell'Ente e al gestore dell'applicativo di competenza.
- Controllare lo stato del licensing e notificare all'ente la situazione di conformità

Gli obiettivi del nuova infrastruttura possono essere così riassunti:

- Decongestionamento della rete aziendale, realizzando modalità alternative per il transito dei dati di backup verso il server centrale.
- Riduzione dei volumi di dati backuppati giornalmente utilizzando le tecniche di deduplica intelligente
- Velocità di Backup e Riduzione dei tempi di restore,
- Mantenimento del livello di archiviazione su tape, affinacato a soluzioni tecnologiche che prevedono l'inserimento di sistemi definiti Virtual Tape library (VTL)
- Restore "istantanei" per i sistemi mission critical
- Scalabilità all'aumentare dei volumi da backuppare
- Licensing del Sw di backup per volume di dati backuppati (TB), indipendentemente dai device dove vengono prodotti i dati da backuppare
- Supporto per agli ambienti virtualizzati

Al fornitore e' richiesto di descrivere con adeguato dettaglio la soluzione di backup proposta, specificando:

- L'architettura generale del nuovo sistema di backup, in rapporto agli obiettivi di progetto
- Le modalità di inserimento del nuovo sistema di backup all'interno dell'architettura dell'Ente, in particolare se e come si integra con il sistema di backup attualmente presente, ovvero se prevede o meno la completa sostituzione del sistema attuale.
- Le caratteristiche tecniche salienti della soluzione proposta ed i benefici che apporta all'Ente
- Il dimensionamento del sistema proposto, e la sua espandibilità per le esigenze future
- L'ambiente ed i tool di gestione, statistica, tuning e plannig centralizzati.

Il fornitore consideri attentamente l'importanza e la criticità dei sistemi informativi in produzione, proponendo una soluzione di altissima qualità sia in termini di componenti che di servizi, dovendo garantire funzionalità h24 per 365 giorni/anno.

Il Nuovo Sistema di backup deve essere dimensionato per i volumi attuali e garantire facilità di espansione a fronte delle esigenze future.
Il sistema proposto deve avere una capienza di backup di almeno 50 TB, espandibili fino ad 80 TB con moduli di espansione, ad ogni modo in linea con l'occupazione degli storage o archivi di alimentazione.

Le licenze del Sw di Backup devono coprire le esigenze dei volumi di dati da archiviare.

Il sistema VTL proposto dovra' avere le seguenti caratteristiche minime (stime riferite all'impiego odierno, da rivalutare in sede di progetto):

- Spazio utile fisico di almeno 25 TB di spazio utile fisico per l'archiviazione, scalabile fino a 50 TB (non sono ammesse attivita distruttive come il cambio dei controller oppure l'associazione di piu sistemi in parallelo)
- La fornitura dovra essere comprensiva di tutte le funzionalita Software disponibili per la soluzione (unica componente opzionale non richiesta al momento la funzione di replica remota). In particolar modo la soluzione deve essere dotata di funzioni VTL con accesso FC all'attuale infrastruttura.
- Connettivita di tipo FC a 8Gbps
- L'algoritmo di deduplica deve garantire il 100% di integrita del dato. In modo specifico non sono amesse soluzioni che presentano il rischio di collisione degli identificativi (hash) usati per il processo di deduplica e che di fatto non garantiscono la completa integrita del dato.
- Anche se non richieste nella fase di progetto attuale, il sistema deve disporre di funzioni di replica mono e bidirezionale, punto-punto e multisito, con granularita fino alla singola cassetta virtuale.
- Il sistema deve garatire la scalabilita senza impatti sulle performance riuscendo a gestire l'indice dei dati interamente nella memoria ram
- La soluzione deve permettere di riversare il dato nativamente dalla Virtual Tape Library alla libreria nastri fisica senza impattare il back-up server al fine di generare un secondo livello di back-up del dato che possa essere movimentato verso altre sedi aziendali ai fini di avere una salvaguardia anche in ottica disaster recovery del sito di produzione.
- Disponibilita di adeguato sistema di interfaccia di gestione e reportistica.

4 SERVIZI DI GESTIONE SISTEMISTICA: DESCRIZIONE RICHIESTA E REQUISITI

4.1 DESCRIZIONE RICHIESTA

Dovrà essere predisposto un documento indicante tempistiche, modalità e ruoli convolti nel processo di presa in carico dell'infrastruttura attuale: cioè un piano ragionato sulle azioni e sulle tempistiche dalla data di ricezione dell'ordinativo di acquisto fino al completo esercizio dell'infrastruttura.
Il piano dovrà inoltre indicare i ruoli con cui sarà necessario interfacciarsi presso il precedente fornitore ed indicare gli tempi di risposta attesi a livello di comunicazione con i vari attori coinvolti.
Dovranno inoltre essere elencate in maniera dettagliata:

- elenco degli attori (a livello di ruolo)
- le informazioni da raccogliere per attore
- pianificazione delle azioni da concordare con il precedente fornitore
- piano complessivo
- criticità
- contingency

4.2 REQUISITI DEI SERVIZI RICHIESTI

L'Impresa è tenuta a prestare la necessaria assistenza tecnica, h24 x 365 gg, rispettando rigorosamente le condizioni ed i tempi di intervento prescritti, e cioè:

- in caso di chiamata la presa in carico deve essere effettuata entro 15 minuti; per problemi bloccanti deve essere garantita la risoluzione del problema entro 1 ora;
- in caso di rotture non bloccanti, la sostituzione delle componenti in garanzia deve essere garantita al massimo il giorno successivo non festivo; se la chiamata avviene il venerdì o prefestivi l'intervento tecnico deve essere assicurato entro il primo giorno successivo non festivo; la chiusura delle chiamate relative alla sostituzione di componenti non in garanzia dovrà essere garantita entro due ore dalla disponibilità del componente
- l'Impresa è tenuta ad utilizzare per le richieste di assistenza gli strumenti di trouble ticketing messi a disposizione dall'A.O. integrandoli eventualmente nella propria gestione.

Tutte le componenti oggetto della fornitura e quelle prese in carico dovranno essere coperte in modalità full risk H24 per 365 giorni all'anno, con monitoraggio proattivo, con tempi di ripristino compatibili gli SLA sopra indicati.

E' richiesto nella presente fornitura che l'Impresa integri nella propria organizzazione lo strumento di trouble ticketing (accedibile WEB) messo a disposizione dall'Ente.

Di seguito una descrizione delle componenti principali del servizio richiesto.

4.2.1 Manutenzione ordinaria

- verifica corretto funzionamento dei server attualmente in uso (per i DB server con particolare attenzione a: frammentazione di tabelle, indici, tablespace; monitoraggio datafiles e attività mirate alla affidabilità del database)
- problem solving relativo agli incident occorsi
- consulenza su possibili migliorie/migrazioni dell'infrastruttura
- allestimento e monitoraggio delle procedure di salvataggio dati che si interfaccia col sistema di backup e di conservazione sostitutiva aziendale

4.2.2 Manutenzione straordinaria

- implementazione nuovi servizi
- nuove installazioni
- migrazioni di ambienti (previa progettazione già discussa e autorizzata)

4.2.3 Manutenzione evolutiva

- riconfigurazioni di allocazioni o dimensionamenti per evoluzioni dell'impianto di pertinenza
- installazioni di nuovi impianti
- migrazione di impianti non all'interno del perimetro degli impianti critici

4.2.4 Reperibilità

- servizio h24 di intervento a fronte di malfunzionamenti bloccanti esclusivamente per gli ambienti di produzione
-

4.2.5 Monitoraggio

- monitoraggio proattivo h24 (comprensivo di tutte le componenti previste nella manutenzione ordinaria)
- attivazione di procedure di intervento a fronte di malfunzionamenti rilevati
- attivazioni di fornitori applicativi a fronte di query non performanti

Il Fornitore dovrà predisporre tutte le misure necessarie a garantire il monitoraggio in tempo reale e l'analisi storica delle richieste applicative dall'ingresso dell'infrastruttura fino agli application server e ai database. Andranno predisposti opportuni cruscotti ed allarmi in grado di attivare interventi di trouble shooting in maniera proattiva. Dovrà essere possibile predisporre cruscotti personalizzati. Dovrà essere possibile generare report automatici periodici da inviare al personale interessato. I sistemi di monitoraggio dovranno essere accessibili in remoto dal personale ENTE o fornitori esterni autorizzati.
Il concorrente dovrà descrivere gli strumenti e le metodologie di monitoraggio dei sistemi in esercizio che consenta un'analisi in tempo reale o su base storica delle metriche raccolte in modo da operare in maniera efficace e proattiva all'identificazione di problemi applicativi e colli di bottiglia.
L'infrastruttura di monitoraggio dovrà essere sufficientemente dinamica da adattarsi facilmente alle eventuali evoluzioni dell'infrastruttura e presentare un overhead inferiore al 5% sul costo complessivo di ciascuna transazione.
In particolare è richiesto di monitorare il funzionamento di tutti gli apparati di rete tramite appositi protocolli e di salvare le informazioni sullo stato e le performance (banda, traffico e tutto quanto possa risultare utile per l'esecuzione di trouble shooting o gestione proattiva dell'infrastruttura) di questi apparecchi in un opportuno reporitory consultabile online in qualsiasi momento. Andranno inoltre generati e gestiti tutti gli allarmi relativi alle condizioni critiche di funzionamento ed andranno definiti i processi di escalation per portare all'attenzione del personale di ENTE degli eventi principali.
Per quanto riguarda i server dovranno essere predisposte opportune sonde per il monitoraggio di tutti i principali parametri di performance: spazio su disco, tempo di accesso al disco, memoria, CPU, thread, traffico di rete,
Per quanto riguarda le applicazioni dovranno essere predisposti strumenti adeguati per l'esecuzione sintetica di alcuni semplici processi applicativi (login, visita la pagina ..., visita la pagina, ..., logoff) in grado di mantenere evidenza della capacità di risposta dl sistema e di generare allarmi in caso di risposta mancata o tempi di risposta eccessivi in modo da attivare prontamente le attività di rispristino del sistema.
Dovrà essere predisposto un sistema di tracciatura automatica di tutte le richieste "http", inclusive dei relativi parametri ricevuti e dei relativi tempi di risposta sia lato server, sia lato client, in modo da identificare anche il tempo di risposta percepito dall'utente.
Con riferimento agli application server, andranno predisposti appositi strumenti in grado di tracciare dettagliata nel dettaglio le operazioni effettuate a livello di componenti standard (JSP, EJB, etc...), oltre a consentire la possibilità di definire componenti applicative specifiche da monitorare a livello di metodo.
Dovrà essere possibile ottenere l'analisi dettagliata di ciascuna transazione in tempo reale o storicizzarla per un esame successivo. Le informazioni raccolte dovranno essere rese disponibili tramite cruscotti personalizzabili ed accessibili da remoto. Dovrà inoltre essere possibile compiere analisi storiche sulle metriche raccolte per finalità

di trouble shooting. Dovrà essere possibile configurare allarmi, da generare in caso di particolari condizioni, e SLA applicativi.
Per quanto riguarda il database dovrà essere possibile monitorare in real time (e/o su base storica) i principali parametri di performance. Periodicamente dovrà essere possibile produrre reportistica che evidenzi eventuali anomalie e consenta un approccio proattivo alla risoluzione dei problemi.
Tutte le informazioni di monitoraggio dovranno essere consultabili da remoto tramite opportuna autenticazione. Dovrà essere possibile configurare la generazione e l'invio di report automatici.

Si riepilogano le principali attività di competenza:

- identificare ed eseguire in prima istanza un assessment sulle prestazioni degli apparati;
- monitorare gli allarmi e il superamento soglie sui server oggetto di fornitura controllando le prestazioni (occupazione RAM, paginazione della memoria, utilizzo CPU, spazio disco ecc) il superamento delle soglie preimpostate;
- identificare in modo proattivo le necessità di ulteriori risorse per anticipare o risolvere problemi di performance applicativa;
- identificare potenziali impatti sulle performance degli apparati dovuti all'inserimento di nuove applicazioni o funzionalità;
- proporre azioni correttive in presenza di performance anomale degli apparati;
- collaborare alla progettazione delle evoluzioni degli apparati;
- proporre quali sistemi debbano essere monitorati, quali tool saranno utilizzati e dove le misure saranno effettuate;
- proporre i dati che devono essere collezionati ed implementare il meccanismo di raccolta;
- raccogliere ed analizzare i dati sulle prestazioni dell'intero parco oggetto di fornitura, allo scopo di identificare eventuali problemi di dimensionamento hardware;
- proporre il modello dei report delle performance con evidenza del superamento delle soglie di controllo stabilite;
- mettere a disposizione periodicamente i report, evidenziando il superamento delle soglie di controllo stabilite;
- gestire log di sistema, ossia verificare le eventuali anomalie riscontrate e riportate nell'event log dei sistemi e l'adozione della conseguente procedura concordata.

4.2.6 Supporto Sistemistico

Per tutta la durata del contratto, andranno predisposti processi e strumenti per la gestione della comunicazione con gruppo di supporto incaricato della gestione dell'infrastruttura. Al contempo andranno definiti gli SLA di ingaggio per le varie attività e le caratteristiche del personale preposto a tale funzione.
Durante la fase di pianificazione e condivisione delle attività di manutenzione e rilascio degli applicativi, il fornitore dovrà verificare la presenza delle figure professionali adeguate all'attività, rispetto al presidio esistente.

In particolare:

- dovranno essere documentati tutti i processi di gestione sistemistica previsti ed i relativi documenti prodotti. Tra questi rientrano molti dei requisiti già esposti;
- nei processi, dovranno essere forniti i profili proposti per la gestione dei singoli componenti dell'infrastruttura con le relative certificazioni rilasciate dai produttori;
- dovranno essere fornite evidenze delle tipologie di contratto di supporto previsto con i produttori;
- dovranno essere definiti canali e modalità di ingaggio da parte dell' ENTE dei profili e relativi livelli di servizio per fascia oraria;
- dovranno essere indicati canali preferenziali da usare in caso di elevata criticità in cui è a rischio l'efficacia del servizio ed in grado di operare con la massima efficacia e tempestività alla risoluzione dei problemi individuati.

4.2.7 Aggiornamento e licenze

Il Fornitore dovrà predisporre tutte le attività necessarie a garantire l'aggiornamento di tutto il software di sistema dei server e degli altri componenti di rete.

Il Fornitore dovrà predisporre un piano periodico di validazione e verifica degli aggiornamenti del software sistemistico dei vari componenti dell'infrastruttura in modo da garantirne in qualsiasi momento l'allineamento alle ultime release stabili disponibili ed il migliore funzionamento possibile in funzione dei requisiti dell'infrastruttura. Tale attività dovrà produrre apposita documentazione in cui saranno mantenute aggiornate tutte le informazioni relative alle versioni del software installato. La gestione degli aggiornamenti dovrà essere condotta di comune accordo con i relativi fornitori in modo da garantire continuità nel servizio.
Il costo delle licenze dei componenti dell'infrastruttura e degli aggiornamenti è da considerarsi parte integrante dell'offerta; l' ENTE non dovrà subire aggravi di costo alcuno. In nessun caso costi legati alla sostituzione di componenti facenti parte dell'infrastruttura o a loro aggiornamento potranno essere imputati all' ENTE.
L' ENTE si riserva il diritto di richiedere in qualsiasi momento l'aggiornamento gratuito a versioni più avanzate di un qualsiasi componente facente parte dell'infrastruttura che dimostri limiti in contraddizione con i livelli di servizio attesi, senza alcun costo aggiuntivo.

4.3 LIVELLI DI SERVIZIO RICHIESTI

Lo scopo di questo paragrafo è quello di fornire la descrizione dei livelli di servizio (SLA) che dovranno essere garantiti durante l'intera durata del contratto.

I livelli di servizio potranno essere applicati, se previsto, in base alle fasce orarie di erogazione del servizio ed ovvero:
Alta Operatività (AO)

- Lunedi-venerdi non festivi h 07.00 - 19.00.
- Sabato non festivo h 08.00 - 13.00.

Bassa Operatività (BO)

- Giornate festive (h 0.00 - 24.00).
- Orari non compresi in AO.

Finestra temporale di erogazione: 24h, 7 giorni su 7.

I tempi di risoluzione in caso dei livello di servizio riportati nei successivi paragrafi devono prevedere la produzione della documentazione contenente analisi, risoluzione e test eseguiti.

Gli SLA dovranno essere tutti indicati in maniera chiara ed esaustiva sui report periodici, report la cui struttura dovrà essere prodotta dal Fornitore ed approvata dall'Ente.

Tutti i report dovranno essere prodotti su base mensile (dove non diversamente specificato) e inviati entro la prima decade del mese successivo.

In generale, durante l'esecuzione del contratto, l'Ente potrà richiedere al Fornitore di sottostare ad attività di auditing dei servizi forniti. Tali attività potranno essere svolte dai Responsabili individuati dall'Ente, da persone espressamente delegate, o da una Società esterna appositamente incaricata.
Scopo delle attività di auditing sarà la valutazione dello stato delle attività svolte dal Fornitore e la verifica della loro conformità rispetto alla programmazione concordata e al contratto.
Le attività di auditing, che potranno avere per oggetto qualunque porzione o l'intero complesso dei servizi oggetto della presente fornitura, saranno svolte con due diverse modalità su insindacabile scelta dell'Ente:

- dando al Fornitore un preavviso di almeno 15 giorni con la specificazione dell'oggetto dell'attività di auditing;

- dando al Fornitore un preavviso di un'ora senza specificare la tipologia di attività che verrà sottoposta ad esame;

4.3.1 SLA per Manutenzione ordinaria

Il servizio dovrà essere attivato ogniqualvolta un **guasto o malfunzionamento** del sistema ne impediscano l'accesso e/o la fruizione delle funzionalità per cause infrastrutturali. Nel caso in cui il fornitore non attribuisca a componenti infrastrutturali in sua gestione, la causa del malfunzionamento, dovrà produrre adeguata documentazione di analisi.

I livelli di servizio richiesti riguardano la tempestività e la capacità di risoluzione dei guasti/malfunzionamenti.

- Il livello MO1 rappresenta anomalie che compromettono l'utilizzo **dell'intero sistema**
- Il livello MO2 rappresenta anomalie che compromettono **parzialmente** l'utilizzo del sistema
- Il livello MO3 rappresenta anomalie che pur non compromettendo parzialmente od interamente l'utilizzo del sistema, **ne rendono difficoltosa la normale fruizione**.

Indicatore	Soglia minima richiesta	Frequenza di monitoraggio
Tempestività di presa in carico di anomalie di livello MO1	Entro 10 minuti	Mensile
Tempestività nella risoluzione di anomalie di livello MO1	Entro 30 minuti	Mensile
Tempestività di presa in carico di anomalie di livello MO2	Entro 10 minuti	Mensile
Tempestività nella risoluzione di anomalie di livello MO2	Entro 30 minuti	Mensile
Tempestività di presa in carico di anomalie di livello MO3	Entro 20 minuti	Mensile
Tempestività nella risoluzione di anomalie di livello MO3	Entro 1 ora	Mensile

Ove:

- Per presa in carico si intende la ricezione del ticket/allarme con invio della conferma di avvio dell'analisi. Entro 30 minuti dalla presa in carico, dovrà essere comunicato un documento contenente l'analisi preliminare.
- Per risoluzione si intende la risoluzione dell'anomalia e la produzione di un documento di descrizione degli interventi e dei test eseguiti a conferma dell'avvenuta risoluzione.
- Nel caso in cui l'evento cominci in BO e termini in AO, verranno presi in considerazione i livelli di servizio di AO. Nel caso opposto, verranno comunque presi in considerazione i livelli di servizio di AO

4.3.2 SLA per Manutenzione straordinaria ed evolutiva

Il servizio deve essere erogato al fine di mantenere il corretto esercizio del sistema per tutto l'arco della Fornitura; gli interventi straordinari ed evolutivi, opportunamente pianificati e concordati con l'ENTE, andranno effettuati nei tempi concordati.

Indicatore	Soglia minima richiesta	Frequenza di monitoraggio
Interventi non effettuati rispetto agli interventi pianificati	0	Mensile
Tempo di esecuzione	Definita dalla pianificazione	Mensile

4.3.3 SLA per Monitoraggio

Il servizio è attivato per tutta la durata della Fornitura e sarà mirato alla verifica continua del buon funzionamento e alle performance del sistema.

Indicatore	Soglia minima richiesta	Frequenza di monitoraggio
Allarmi non prodotti (allarmi non inviati quando previsti)	0	Mensile

4.3.4 SLA per Supporto Sistemistico

Il servizio è attivato per tutta la durata della Fornitura e sarà attivato su due modalità di ingaggio da parte dell'ENTE.

- SS1 rappresenta l'ingaggio da parte dell'ENTE per interventi **urgenti** di troubleshooting sistemistico
- SS2 rappresenta l'ingaggio da parte dell'ENTE per interventi **non urgenti** di troubleshooting sistemistico o pianificati.

Indicatore	Soglia minima richiesta	Frequenza di monitoraggio
Tempestività di presa in carico di interventi di livello SS1	Entro 20 minuti in AO Entro 40 minuti in BO	Mensile
Tempestività nella risoluzione di interventi di livello SS1	Entro 2 ore in AO Entro 4 ore in BO	Mensile
Tempestività di presa in carico di interventi di livello SS2	Entro 1 gg	Mensile
Tempestività nella risoluzione di interventi di livello SS2	Entro 2 gg	Mensile