Servizio di supporto sistemistico 2015 - 2017

Capitolato tecnico

Versione 1.0

Indice

1 OGGETTO DELLA GARA

L'Istituto Zooprofilattico Sperimentale della Lombardia ed Emilia Romagna, di seguito denominato IZSLER, dispone di un Sistema Informativo articolato e complesso basato su un Sistema centrale, una rete geografica ed una serie di sistemi periferici.
Il sistema riveste una cruciale rilevanza per la maggior parte delle attività operative e decisionali ed è pertanto fondamentale provvedere alla sua costante efficienza; la mancata funzionalità di una qualsiasi delle componenti del sistema informativo rappresenta un elemento di forte criticità per la funzionalità dell'Ente.
L'evoluzione costante delle tecnologie che determina la necessità di un costante aggiornamento, la messa a punto delle stesse, la loro diffusione e gestione richiede una disponibilità crescente in termini di numero e di qualità di risorse umane.
L'impossibilità o la difficoltà a disporre di risorse adeguate interne determina l'esigenza che il Sistema Informativo Izsler debba essere oggetto di un accurato e diligente "Servizio di Assistenza Informatica Specialistica" affidato in outsourcing ed in grado di assicurare la funzionalità del sistema stesso e di garantirne un alto grado di efficienza e di sicurezza.
Allo scopo, è necessario far ricorso ad organizzazioni esterne in grado di mettere a disposizione le risorse altamente qualificate che opereranno sulla base di precise specifiche definite dal Dirigente Responsabile dei Sistemi Informativi o suo delegato.

2 DURATA DEL CONTRATTO

Trentasei mesi a far data dall'effettivo avvio delle attività.

3 GLOSSARIO DELLE PRINCIPALI DEFINIZIONI UTILIZZATE

Nell'ambito del presente documento si intende per:

- *Infrastruttura informatica*: l'insieme delle componenti hardware, software e di connettività del sistema elaborativo centralizzato, gli storage (SAN & NAS), le piattaforme (VMWARE, NETAPP, CITRIX, Linux, BLADE Server, Commvault, ecc.) presenti al momento della attivazione del contratto e di quelle che saranno eventualmente aggiunte nel periodo di durata del contratto. Di seguito si farà riferimento ad essa anche come "sistema informatico".

- *Infrastruttura di comunicazione*: l'insieme degli apparati di rete e delle connessioni che garantiscono connettività: LAN, WAN e WiFi.

- *Intrusion Detection*: dispositivo o software applicativo che controlla le attività di rete o di sistema per rilevare criticità in termini di sicurezza o violazioni delle policy aziendali.

- *Disaster Recovery (*DR): nell'ottica dell'art. 50 bis del CAD, l'insieme delle misure tecniche e organizzative adottate per assicurare all'organizzazione il funzionamento del centro elaborazione dati e delle procedure e applicazioni informatiche dell'organizzazione stessa, in siti alternativi a quelli primari/di produzione, a fronte di eventi che provochino, o possano provocare, indisponibilità prolungate.

- *Infrastruttura critica*: un'infrastruttura che è essenziale per garantire la continuità dei servizi informativi.

- *Piano di Disaster Recovery* (PDR): il Piano che, costituisce parte integrante del Piano di continuità operativa e stabilisce le misure tecniche ed organizzative per garantire il funzionamento dei centri elaborazione dati e delle procedure informatiche rilevanti in siti alternativi a quelli di produzione.

- *Politiche di sicurezza*: le regole tecniche e le politiche adottate per garantire l'esattezza, la disponibilità, l'accessibilità, l'integrità e la riservatezza dei dati, dei sistemi e delle infrastrutture, la prevenzione e gestione degli incidenti di sicurezza informatica nonché per assicurare che i

documenti informatici siano custoditi e controllati in modo tale da ridurre al minimo i rischi di distruzione, perdita, accesso non autorizzato o non consentito o non conforme alla finalità della raccolta.

- *Servizio Cloud*: Con il termine cloud computing si intende la disponibilità, in modalità on demand, di risorse informatiche (applicazioni, DB, file service...) viste come servizi tramite l'accesso ad una rete di computer la cui reale dislocazione sul territorio di norma può essere sconosciuta all'utente, il quale,quindi, può operare ignorando la reale natura, struttura e collocazione delle risorse impiegate, utilizzandole in modalità "service" e accedovi tramite Internet (Public cloud) o tramite intranet private (Private cloud).

4 DESCRIZIONE DEL SERVIZIO

Il servizio di **assistenza sistemistica** è finalizzato sia a supportare il personale dei Sistemi Informativi con compiti di "amministrazione dell'infrastruttura informatica" sia ad intervenire direttamente nella gestione dell'infrastruttura stessa su richiesta del responsabile dei Sistemi Informativi o suoi delegati.

Le attività richieste sono quelle necessarie a:

1. Mantenere le infrastrutture elaborative e gli storage ad un livello di piena efficienza, affidabilità e sicurezza;
2. Rimuovere tutti i problemi che dovessero manifestarsi sull'infrastruttura informatica;
3. Collaborare con il personale interno ed eventualmente con personale di aziende esterne incaricate di effettuare test di Intrusion Detection, nella messa a punto dei correttivi necessari a garantire la sicurezza delle infrastrutture informatiche;
4. Collaborare alla realizzazione degli interventi che saranno ritenuti necessari per garantire la continuità operativa dei Sistemi Informativi; in merito è in via di definizione il piano di Business Continuity;
5. Garantire la supervisione del sistema informatico in determinati giorni dell'anno;
6. Fornire informazioni tecniche di supporto al personale dei Sistemi Informativi per lo svolgimento delle attività ordinarie e straordinarie di gestione e evoluzione del sistema informatico

Più in dettaglio, le attività previste sono quelle di seguito elencate:

a. Installare, configurare, personalizzare, mantenere in efficienza e concorrere alla corretta gestione del sistema informatico nelle sue componenti hardware (compresa la connettività interna alle infrastrutture e quella fra esse e il core di rete) e software collaborando, quando necessario, anche con personale tecnico dei fornitori.
b. Gestire tutte le problematiche inerenti il software di base e gli ambienti operativi individuandone i malfunzionamenti e i rallentamenti e concorrere alla loro eliminazione.
c. Intervenire a livello di postazioni utente (periferiche comprese) per risolvere problematiche che precludano la possibilità di utilizzo delle infrastrutture centralizzate;
d. Supportare gli addetti dei sistemi informativi sia alla messa a punto ed alla gestione dei sistemi di backup sia, se necessario, nella esecuzione dei ripristini dei dati e delle configurazioni; i ripristini devono poter essere realizzati anche in autonomia;
e. Provvedere a mantenere efficiente il sistema di Active Directory garantendo il relativo supporto al personale interno nella stesura e nell'applicazione delle policy e degli script di login al dominio;
f. Collaborare, quando richiesto dal personale interno, con il personale sistemistico di altri fornitori IZSLER di servizi applicativi, di rete, gestionali, ecc.
g. Produrre ed aggiornare la documentazione tecnica di riferimento, nell'ambito delle indicazioni ricevute, relativamente: alla configurazione del sistema, alle procedure operative, alla soluzione dei problemi;
h. Attività di supervisione e gestione del sistema informatico dell'istituto per l'intera giornata (anche in teleassistenza)
i. Fornire al personale dei Sistemi informativi tutte le informazioni necessarie o utili alla gestione ed

evoluzione dell'intero sistema informatico dell'istituto: sono quindi comprese anche eventuali attività di "hands-on" training e proposte di utilizzo di soluzioni innovative o migliorative di quelle attualmente utilizzate

4.1 Tipologie di servizio richieste

Le tipologie di servizio richieste sono:

1. **Help desk con sistema di tracking delle segnalazioni** e supporto tecnico di primo e di secondo livello al/ai referenti tecnici interni.
2. **Teleassistenza** di supporto volta al ripristino delle funzionalità dei componenti. Se il supporto in teleassistenza non fosse risolutivo programmazione di un intervento on site; in caso di priorità alta o normale l'intervento on site dovrà avvenire tempestivamente al fine di garantire i tempi previsti dal capitolato.
3. **Installazioni e configurazioni sia in teleassistenza che on site**
4. **Supporto tecnico on site** per la risoluzione di problemi non risolvibili in teleassistenza o per attività pianificate (comprese installazioni e configurazioni) con il dirigente responsabile dei Sistemi Informativi o suo delegato. L'orario di intervento richiesto in queste situazioni sarà generalmente dalle 09:00 alle 16:00, salvo esigenze diverse dettate dal tipo di intervento che dovrà essere effettuato.

   Per questo tipo di interventi va previsto un monte complessivo di **1000 ore comprensive di quelle erogate in teleassistenza.**
5. **Supervisione e gestione del sistema informatico (on site o in teleassistenza),** compresa la gestione ordinaria, per l'intera giornata: l'orario di copertura del servizio richiesto è dalle 08:00 alle 16:00. Durante tali giornate si dovranno garantire anche la verifica del buon esito delle operazioni notturne (ad esempio i backup schedulati dei server) e tutti gli interventi necessari per garantire il corretto funzionamento del sistema informando i Sistemi Informativi delle eventuali problematiche rilevate, degradi dei servizi e attività di intervento svolte; eventuali richieste di intervento da parte dei Sistemi Informativi effettuate in tali giornate durante l'orario di copertura non verranno detratte dal monte annuo previsto al punto 4. Per questo tipo di servizio va previsto un monte complessivo di **50 giornate**; tali giornate potranno essere svolte separatamente o in maniera continuativa (ad esempio ogni giorno per due settimane consecutive) a discrezione del responsabile dei Sistemi Informativi o suo delegato.

4.2 Attività non oggetto del presente contratto

1. Amministrazione degli applicativi utilizzati dall'Izsler (quali a titolo di esempio la "gestione della contabilità", la "gestione del Protocollo" e la "gestione del Personale");

   In questi casi il personale dei Sistemi Informativi si avvarrà del supporto dei fornitori, unici erogatori del servizio di assistenza e manutenzione sugli specifici software.
2. Gestione delle postazioni di lavoro utente.
3. Risoluzione di problematiche: hardware o di cablaggio WAN, Lan e Wifi.

4.3 Priorità di intervento

Le richieste di intervento possono essere fatte sia da personale dei Sistemi Informativi sia da tecnici di aziende esterne che hanno in appalto la gestione delle infrastrutture.

La classificazione della priorità dell'intervento viene decisa in fase di chiamata, i livelli di priorità degli interventi sono i seguenti:

1. **Priorità alta:** si tratta di problemi bloccanti su infrastrutture critiche che non permettono agli

utenti l'accesso alle risorse elaborative, alle applicazioni, agli storage.

2. **Priorità normale**: riguarda criticità non bloccanti.
3. **Priorità bassa:** tipicamente l'aggiunta di funzionalità, migliorie nella configurazione, ecc.
4. **Pianificate** secondo tempistiche concordate di volta in volta con il responsabile dei Sistemi Informativi o suo delegato.

4.4 Disponibilità del servizio

È richiesta la seguente disponibilità:

1. **Per gli interventi in priorità "normale" o "bassa":** dalle 8:00 alle 18:00 dal Lunedì al Venerdì.
2. **Per gli interventi in priorità "alta":** dalle 8:00 alle 18:00 dal Lunedì al Venerdì.

   Un massimo di 4 interventi l'anno potranno essere richiesti anche il sabato, ad esempio per attività di manutenzione straordinaria.

   Le richieste di intervento il sabato potranno essere richieste dal responsabile dei Sistemi Informativi o suo delegato**.**

Per orario lavorativo conteggiato ai fini del calcolo dei tempi di intervento si intende la fascia di orario che va dalle 8:00 alle 18:00 dal lunedì al venerdì.

4.4.1 Tempi di intervento

4.4.1.1 Priorità alta

Soluzione del problema, con ripristino della piena funzionalità, **entro due ore lavorative dalla chiamata**.

È di esclusiva competenza del dirigente responsabile dei Sistemi Informativi o suo delegato classificare l'intervento nella tipologia "alta priorità".
Il numero massimo di interventi annui di questa tipologia potrà essere di 30.

4.4.1.2 Priorità normale

Soluzione del problema, con ripristino della piena funzionalità **entro 6 ore lavorative dalla chiamata**. Rientrano gli interventi necessari a ripristinare servizi non funzionanti ma comunque non ritenuti "prioritari" dai Sistemi Informativi.

4.4.1.3 Priorità bassa

Si tratta di interventi mirati alla soluzione o prevenzione di problemi che non determinano interruzioni di servizio, con ripristino della piena funzionalità **entro 12 ore lavorative dalla chiamata**.

Deve essere possibile cambiare il tipo di priorità assegnata ad un intervento e tale possibilità è riservata esclusivamente al responsabile dei sistemi informativi o suo delegato.

4.5 Call Center

La ditta aggiudicataria deve mettere a disposizione un servizio di call center che costituisce l'unico punto di chiamata dell'utente verso il supporto.

Il contatto deve prevedere le seguenti modalità:

1. **Telefonica**
2. Via **WEB** con un form dedicato
3. Via **e-mail**
4. **Fax**, secondo modulistica fornita dalla ditta aggiudicataria.

Sarà cura della ditta aggiudicataria attivare tutte le modalità di ricevimento chiamate entro sette giorni dalla data d'inizio del servizio, il call center deve essere allestito a cura del fornitore, in locali e con infrastrutture di sua pertinenza.

Il call center è l'unica unità del servizio che può attribuire un numero di chiamata.

Il numero di chiamata deve essere l'identificativo univoco della chiamata, indipendentemente dalla modalità di richiesta.

Indipendentemente dalla modalità utilizzata, una conferma sulla presa in carico della stessa dovrà essere inviata tramite mail ad un indirizzo di posta elettronica che sarà comunicato all'avvio del servizio. La mail dovrà avere in oggetto il numero di chiamata e nel corpo la descrizione del problema segnalato.

Il servizio di ricevimento telefonico delle chiamate dovrà essere presidiato dalle ore 8:30 alle 17:00 dal lunedì al venerdì. Gli altri canali (web, mail e fax) di ricevimento delle chiamate dovranno essere sempre attivi.

Le chiamate saranno fatte solo da personale dei Sistemi Informativi ed eventualmente da altro personale autorizzato dell'azienda che fornisce il servizio di manutenzione ordinaria delle Pdl, Server, infrastrutture di rete, ecc.

4.6 Avvio del servizio

All'avvio del servizio sarà fornito il nominativo del referente interno delegato dal responsabile dei sistemi informativi e l'elenco del personale autorizzato ad effettuare le chiamate il cui numero previsto è di **massimo 6 utenti**.

Per le chiamate fatte tramite mail, la ditta aggiudicataria deve sempre confermare la ricezione.

4.7 Chiusura dell'intervento

Al termine di un intervento on site o in teleassistenza, la ditta aggiudicataria dovrà produrre un rapporto di intervento che:

a. Riporti l'elenco delle operazioni effettuate;
b. Sia sottoscritto dal tecnico dei Sistemi Informativi che ha istruito la chiamata o dal referente interno designato in fase di avvio del servizio.

Tale rapporto deve essere messo a disposizione dei Sistemi Informativi (trasmissione via mail o download dal portale di gestione delle chiamate) e si ritiene condiviso se non contestato entro due giorni lavorativi.

5 DESCRIZIONE DELL'ORGANIZZAZIONE E DELLE INFRASTRUTTURE

L'Istituto Zooprofilattico Sperimentale della Lombardia e dell'Emilia-Romagna opera nell'ambito del SSN come strumento tecnico-scientifico dello Stato e delle due Regioni di giurisdizione, garantendo ai Servizi Veterinari le prestazioni e la collaborazione in materia di igiene e sanità pubblica.
Per garantire tale operatività nel corso degli anni l'Istituto ha realizzato una rete di 17 Sezioni diagnostiche distribuite nel proprio territorio di competenza, rispettivamente 9 in Lombardia e 8 in Emilia Romagna, strettamente collegate alla Sede di Brescia.

Le sedi operative sono così dislocate:

- Sede di Brescia - Via Bianchi, 9 – 25124 BRESCIA – TEL. 030/2290221
- Sezioni Diagnostiche presenti in Lombardia:
  - BERGAMO - Via Pietro Rovelli 53 - 24125 (BG) - TEL. 035/4236036
  - BINAGO – Via Dante 6Bis, - 22070 (CO) - TEL. 031/940870-940992
  - CREMONA – Via Cardinal Massaia 7 - 26100 (CR) - TEL. 0372/434637
  - MANTOVA – Strada Circonvallazione Sud 21/A, - 46100 (MN) – TEL. 0376/380493
  - MILANO – Via Celoria 12 - 20133 (MI) - TEL. 02/70600116-153
  - LODI – Via Einstein – LOC. CASCINA CODAZZA - C/O PARCO TECNOLOGICO PADANO - 26900 (LO) - TEL. 0371/439354
  - PAVIA – Strada Campeggi 59/61- 27100 (PV) - TEL. 0382/526529-422006
  - SONDRIO – Via Bormio 30 - 23100 (SO) - TEL. 0342/214312
- Sezioni Diagnostiche presenti in Emilia Romagna:
  - BOLOGNA – Via Pietro Fiorini 5 - 40127 (BO) - TEL. 051/4200011 – FAX 051/4200038
  - FERRARA – Fraz. Cassana - VIA MODENA 483 - 44044 (FE) - TEL. 0532/730058
  - FORLI' - Via Don Eugenio Servadei S/N Loc. Pieve Acquedotto 47122 - TEL. 0543/721343
  - LUGO DI ROMAGNA – Via del Limite 2 - 48022 (RA) - TEL. 0545/23225
  - MODENA – Via E. Diena 16, - 41100 (MO) - TEL. 059/453511
  - PARMA – Via dei Mercati 13/A - 43100 (PR) - TEL. 0521/293733
  - PIACENZA – Fraz. Gariga di Podenzano – Strada della Faggiola 1 - 29027 (PC) - TEL. 0523/524076- 524253
  - REGGIO EMILIA – Via Pitagora 2- 42100 (RE) - TEL. 0522/277996-921733

La **Sede Centrale** dell'IZSLER è a Brescia ed è articolata in 3 Aree a loro volta suddivise in Reparti (strutture complesse) e Laboratori (strutture semplici):

- Area Diagnostica
- Area delle Attività di Servizio
- Area Controllo degli Alimenti e delle Trasformazioni

Nelle Regioni di competenza operano, con prevalente distribuzione provinciale, articolazioni periferiche dell'Istituto: le **"Sezioni Diagnostiche"**. Il raccordo funzionale tra la rete delle Sezioni e la Sede si concretizza in due specifiche aree organizzative regionali:

- Area Territoriale Lombardia
- Area Territoriale Emilia Romagna

L'IZSLER, di concerto con le Regioni ha attivato due "Osservatori per la Sorveglianza epidemiologica":

- O.E.V.R.L. (Osservatorio Epidemiologico Veterinario Regione Lombardia) c/o Sede di Brescia
- C.E.R.E.V. (Centro Emiliano Romagnolo di Epidemiologia Veterinaria) c/o Sezione di Bologna

le cui funzioni sono eminentemente di consulenza tecnico-scientifica e informativa, riguardanti la sanità animale e l'igiene degli alimenti che coinvolgono le attività delle AA.SS.LL., delle Strutture centrali e territoriali dell'Istituto e dei Servizi Veterinari Regionali.

Mentre in sede l'attività è distribuita in 16 palazzi, nelle periferie in un unico stabile normalmente su più piani.

All'indirizzo http://www.izsler.it/izs_home_page/sede___mappa_interattiva/00000599_Sede.html è visibile la mappa interattiva dei palazzi presenti in Sede a Brescia.

Mentre nei palazzi n° 2,3,4,5 e 6, oltre alle Direzioni (generale, sanitaria e amministrativa) e alla Presidenza, sono concentrati i servizi amministrativi e tecnici, nei restanti palazzi sono distribuiti i reparti tecnico/sanitari; questi ultimi sono particolarmente concentrati nei palazzi 1,10,11,12 e 13.

5.1 Infrastrutture di rete

In ogni palazzo della Sede sono presenti uno o più armadi di palazzo, la connessione fra i palazzi e le sale è in fibra. I palazzi adiacenti al palazzo tre (dove sono allocate le sale macchine) sono connessi direttamente ad esse, i palazzi più lontani si connettono ad un centro di smistamento della fibra da cui partono le connessioni verso le sale macchine.

In tutte le sedi periferiche sono presenti connessioni di rete locale (Lan) e ogni sede è interconnessa con le altre tramite una rete geografica (SPC-MPLS).

5.1.1 Infrastruttura di rete geografica

L'interconnessione geografica fra la sede e le periferie viene garantita da Telecom tramite architettura di rete HYPERWAY VPN IP MPLS, in grado di gestire una VPN IP con il protocollo MPLS (Multi Protocol Label Switching).

In funzione della mole di lavoro sviluppata in ciascuna sede e della tipologia di esercizio necessaria per ogni specifica esigenza, sono utilizzati apparati diversi in funzione del profili di connettività necessari.

Per la sede core di Brescia è in uso una soluzione di High Performance mediante l'impiego di fibra ottica a 100M con massima ridondanza.

È in sostanza stato realizzato un anello completo con doppia portante ottica per garantire la massima affidabilità del circuito.

Gli apparati ottici di attestazione e le porte utilizzate sono anch'esse diversificati.

Sul medesimo portante ottico è inoltre aperto un canale di trasmissione, anch'esso con velocità 100Mb/s per garantire il traffico verso la rete Internet.

Tutto il traffico verso la WAN e dalla WAN sia della Sede che delle periferie è centralizzato in Sede e la soluzione di FireWall adottata per garantire la sicurezza dell'accesso si appoggia su apparati SonicWall modello NSA2400 in HA; la configurazione del lato WAN comprende sia la visibilità degli apparati Telecom sia degli apparati GARR e Lombardia Integrata.

I due apparati SonicWall sono installati nella stessa sala macchine ed integrano gateway Anti-Virus, Anti-Spyware, Intrusion Prevention.

Tutte le sedi periferiche sono attrezzate con un doppio circuito 4xHDSL.

I circuiti sono attestati su 2 router CISCO con porta IMA-HDSL a bordo.

In caso di caduta del link principale il router provvede a dirottare il traffico sul secondo apparato opportunamente configurato in HSRP in modo da ridurre al minimo l'eventuale interruzione di servizio.

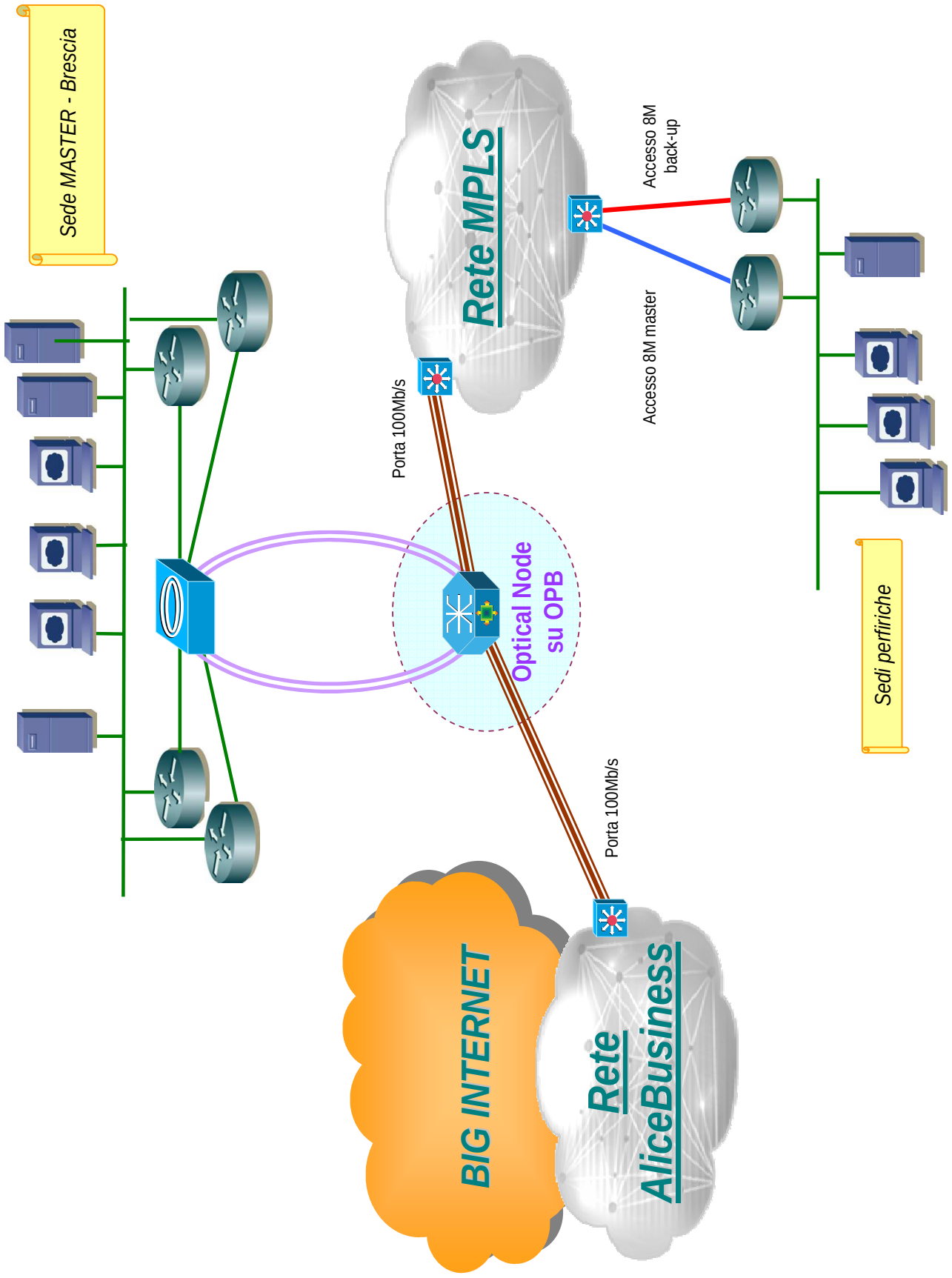
Nella tabella sono riportati, sede per sede, gli accessi previsti, la tipologia dei collegamenti e la banda minima garantita.

Sede	Collegamenti	BMG	Note
BRESCIA	1 HeadQuarter MPLS 100Mb/s con backup	100Mb/s	Rilegamento con doppio anello in Fibra Ottica
BRESCIA	1 accesso Internet 100Mb/s con backup	100Mb/s	Rilegamento con doppio anello in Fibra Ottica
BINAGO	1 HeadQuarter 8M con back-up	4Mb/s	Due circuiti 4xHDSL attestati su doppio router CISCO con porta IMA-HDSL e in configurazione di Back-up HSRP.
FERRARA	1 HeadQuarter 8M con back-up	4Mb/s	
LODI	1 HeadQuarter 8M con back-up	4Mb/s	
SONDRIO	1 HeadQuarter 8M con back-up	4Mb/s	
BERGAMO	1 HeadQuarter 8M con back-up	4Mb/s	
CREMONA	1 HeadQuarter 8M con back-up	4Mb/s	
FORLI'	1 HeadQuarter 8M con back-up	4Mb/s	
LUGO	1 HeadQuarter 8M con back-up	4Mb/s	
MANTOVA	1 HeadQuarter 8M con back-up	4Mb/s	
MILANO	1 HeadQuarter 8M con back-up	4Mb/s	
MODENA	1 HeadQuarter 8M con back-up	4Mb/s	
PARMA	1 HeadQuarter 8M con back-up	4Mb/s	
PAVIA	1 HeadQuarter 8M con back-up	4Mb/s	
PODENZANO	1 HeadQuarter 8M con back-up	4Mb/s	
REGGIO EMILIA	1 HeadQuarter 8M con back-up	4Mb/s	
BOLOGNA	1 HeadQuarter 8M con back-up	4Mb/s	

I Router e gli apparati necessari per realizzare i collegamenti sopradescritti sono stati installati dalla società PAth.NET SpA del gruppo TELECOM Italia in adesione al contratto OPA dei servizi di connettività e sicurezza nell'ambito del sistema pubblico SPC DIGIT PA CNIPA e gestiti dalla stessa.

Tutti gli apparati utilizzati sia per l'infrastruttura WAN che per quella LAN sono oggetto di monitoring continuo attraverso un servizio appaltato ad un fornitore esterno (Lutech).

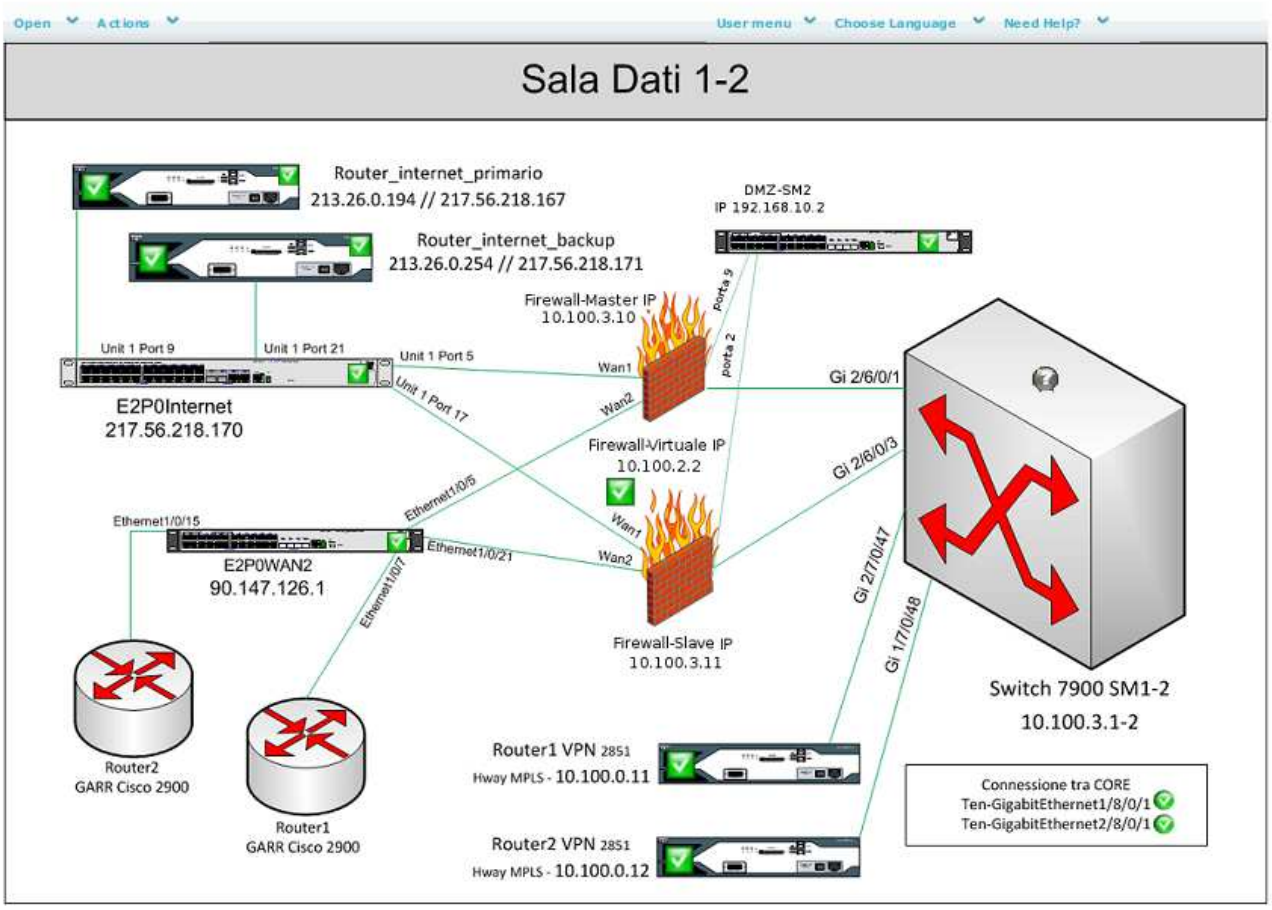
L'immagine che segue rappresenta l'infrastruttura di connessione fra la Sede e le periferie:


Sede MASTER - Brescia
Rete MPLS
Accesso 8M back-up
Accesso 8M master
Porta 100Mb/s
Optical Node su OPB
Sedi perfiriche
Porta 100Mb/s
BIG INTERNET
Rete AliceBusiness

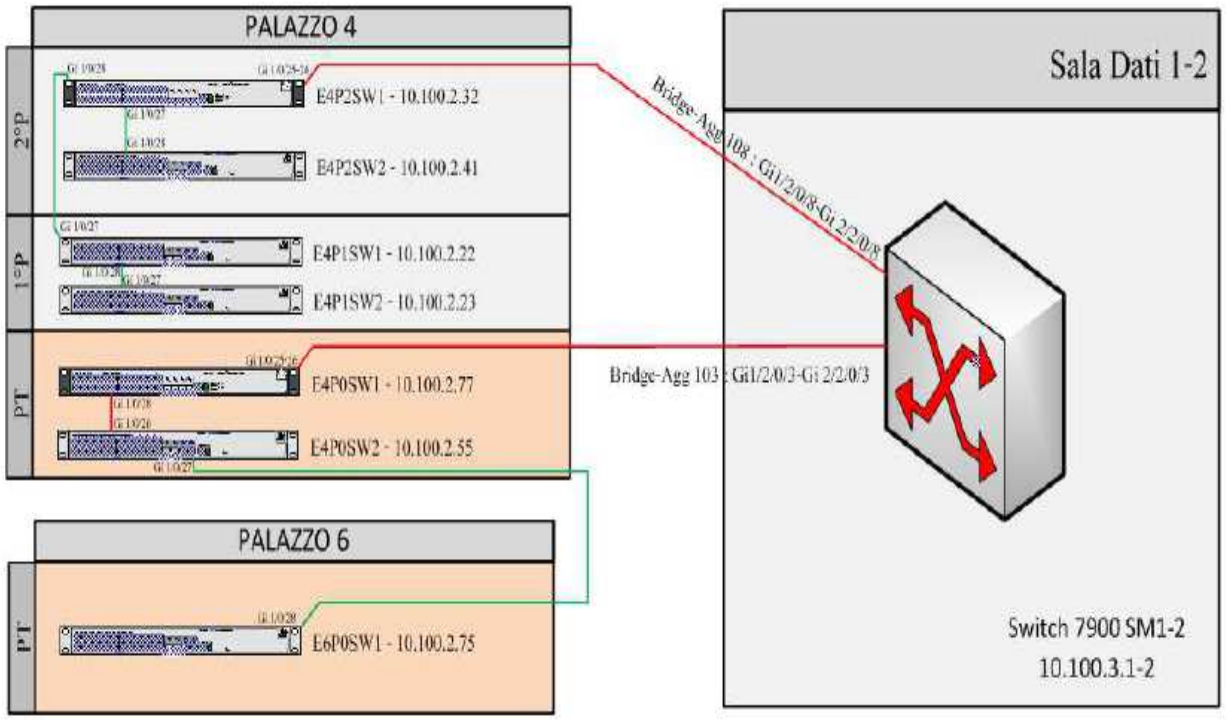
5.1.2 Infrastruttura Lan

L'immagine che segue illustra le infrastrutture di rete nella sala macchine 2; lo switch di core 7900 si compone di due nodi, il secondo nodo è in sala macchine 1 e i nodi sono visti come un unico apparato tramite una connessioine in FO a 10 Gbit/s.

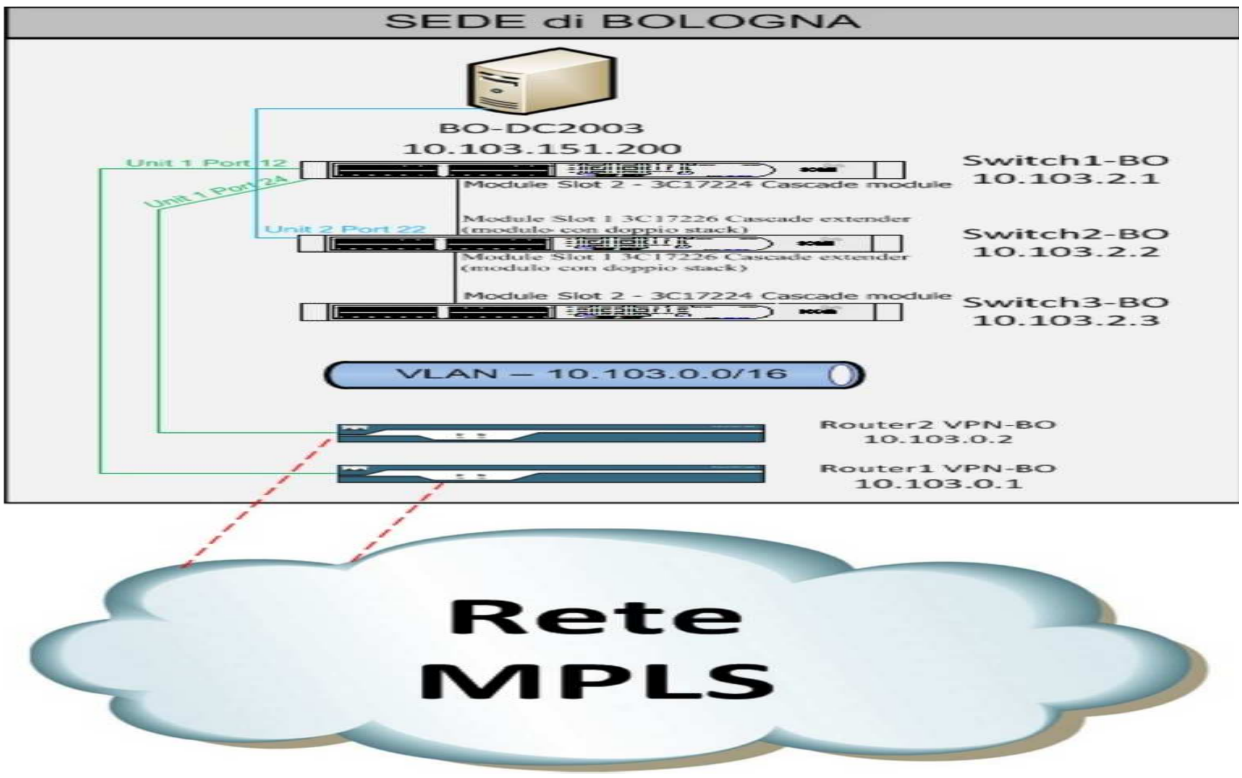
Ogni palazzo delle Sede (16 palazzi) è interconesso in Fibra multimodale (1Gbit/s) sui due core.



L'immagine seguente è un esempio delle infrastrutture di palazzo e raffigura le infrastrutture di rete dei palazzi 4 e 6 e la loro interconnessione con lo switch di core 3Com 7900 di sala macchine 1 e 2.



La figura successiva rappresenta la sezione di Bologna, nelle altre sezioni la modalità di interconnessione fra le infrastrutture LAN e WAN non cambia mentre possono cambiare in termini quantitativi gli apparati LAN a seconda della dimensione della sezione e quindi del numero di postazioni e stampanti da connettere.



5.1.3 Connessioni WiFi

Sono disponibili in alcuni piani di palazzi della Sede e in sezione diagnostica a Milano in dettaglio:

Palazzo	Piano/i
2	Terra
3	Terra e 2
4	1 e 2
5	Terra
6	Terra
10	1
12	Terra
Foresteria	Terra e 1

Sono configurate:3 SSID con autenticazione pre-shared + 1 SSID open.

Tutte le wireless permettono di navigare, l'accesso alle share di rete è possibile per gli utenti che dispongono di credenziali.

5.1.4 Utenti utilizzatori

Sono di tre tipologie:

- **Interni** cioè che accedono alla rete tramite connessioni locali o Wifi: più di 600 dipendenti, questi utenti sono i maggiori utilizzatori della rete e hanno il relativo profilo in Active direcory in un dominio Microsoft 2008.

  Inoltre più di un centinaio fra borsisti, contrattisti, che accedono alla rete più o meno saltuariamente e la maggior parte con diritti limitati consistenti nell'accesso alla postazione locale, a risorse di rete condivise e alla navigazione internet.

  Accedono alla rete sia tramite connessioni fisse che mobili, alcuni, saltuariamente anche da remoto per esigenze di verifica o manutenzione (amministratori di sistema).
- **Esterni**: si tratta sia di soggetti terzi dipendenti da ditte esterne che hanno un contratto di manutenzione di apparati (Server, Pdl, strumenti) sia di utenti che accedono a servizi/applicazioni esposte in extranet. Nel primo caso la connessione viene gestita dai firewall perimetrali e l'accesso è sottoposto a regole che verificano sia l'origine della connessione (Ip) che i protocolli e le porte abilitate, nel secondo caso tramite credenziali e certificati. Questi utenti possono avere o meno un profilo in AD.
- **Saltuari**: si tratta in genere di commerciali o consulenti che si connettono, una tantum, in WiFi alla rete e che sono abilitati alla sola navigazione Internet.

5.1.5 Tipologie di traffico

- **Ad oggi, le tipologie di traffico generate sono classificabili in:**
- **Applicativo:** consistente nell'utilizzo delle applicazioni centralizzate documentate nelle pagine successive, (DARwin, Archipro&Infatti, SAI "SistemaAmministrativoIntegrato", gestione presenze e del personale, firma digitale RDP, SISI, ecc.).

  Questo tipo di traffico transita principalmente sulla rete MPLS ma anche su quella Gigabusiness (internet) nel caso di gestione del personale o di accesso dei fornitori per quanto concerne la gestione amministrativa di alcuni servizi.
- **Posta elettronica:** tutta la posta è stata migrata su un servizio Microsoft in Cloud esterno e quindi qualsiasi mail, anche fra utenti aziendali, transita sia sulla rete MPLS sia su quella Gigabusiness (internet);

- **Video conferenza:** tramite un servizio in Cloud su piattaforma Microsoft Office 365 (Lync).
- **Intranet**: le applicazioni richiamabili tramite browser, visto che la gestione del sito è esterna, transitano sia su LAN, MPLS che Gigabusiness (internet);
- **Internet:** tutto il traffico transita sia su LAN, MPLS che Gigabusiness.
- **Documentale:** gran parte della documentazione scambiata fra le periferie o fra le periferie e la sede transita oltre che in LAN, sulla rete MPLS.

  Tramite la piattaforma Microsoft Office 365, per 200 utenti è previsto il rilascio di funzionalità Sharepoint di condivisone e scambio documenti; per questo motivo è prevedibile che il traffico sulla parte Gygabusiness aumenti considerevolmente**.**
- **Gestionale:** controllo dei sistemi in termini di sicurezza (sistema antivirus, rilascio continuo di aggiornamenti per il mantenimento a norma dei sistemi, installazione automatica di applicativi di terze parti (adobe reader, flash, Java, drivers, ecc.).

5.2 Infrastrutture elaborative e storage

5.2.1 Infrastrutture elaborative

Tutte le applicazioni più importanti sono ospitate su infrastrutture ridondate.

Le infrastrutture fisiche principali utilizzate sono dei Blade server distribuiti nelle due sale macchine della Sede di Brescia.

Oltre alle blade infrastructure sono ancora attivi alcuni server fisici il cui ruolo, in alcuni casi, è però determinante per la continuità operativa almeno per parte dell'utenza.

Tutte le informazioni relative ad ogni singolo server e necessarie a conoscerne le funzionalità (servizi erogati), definirne, in base alla tipologia dei dati, il trattamento, conoscerne la modalità di backup, e altro, sono contenute in una base dati gestita dagli amministratori di dominio.

Al momento i server sono 157 di cui:

- 108 virtualizzati tramite VMware;
- 17 server fisici di cui:
  - 2 su lame Blade in sala macchine 1
  - 11 rackmountable installati nelle sale macchine
  - 4 Tower installati nei reparti della Sede
- 32 Tower installati nelle sezioni diagnostiche provinciali (2 per ogni sezione) di cui uno con funzioni di domain controller periferico e uno come file-server.

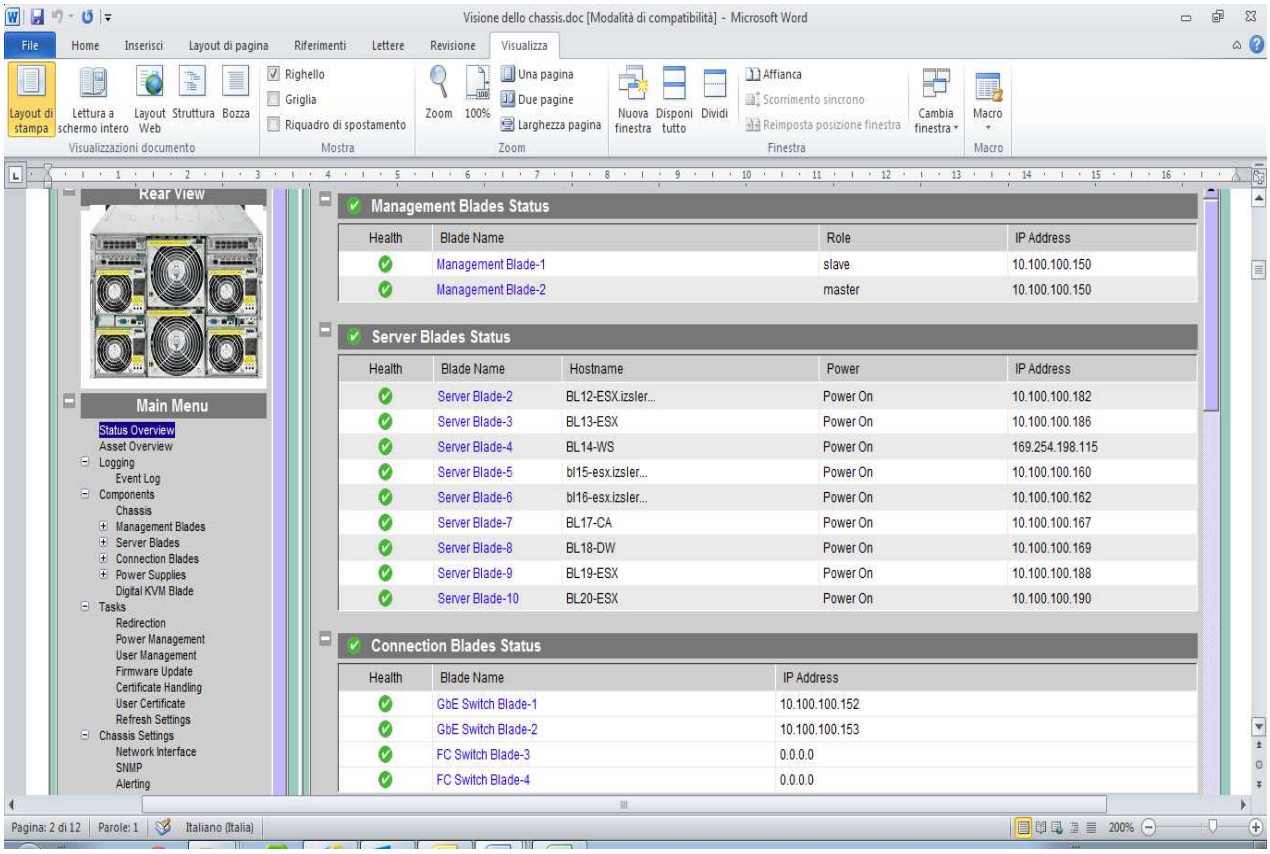
Tutta l'infrastruttura elaborativa è monitorata in termini di disponibilità e di servizi da due applicazioni:

- Lutech: la stessa che verifica, sulla base di parametriche concordate con gli amministratori, la disponibilità delle infrastrutture di rete, monitorizza disponibilità, e le risorse a livello di ogni server.
- Server-Monitor: applicazione che verifica lo stato dei server in termini di disponibilità dei servizi e i livelli di performance inviando alert agli amministratori sulla base di soglie predefinite.

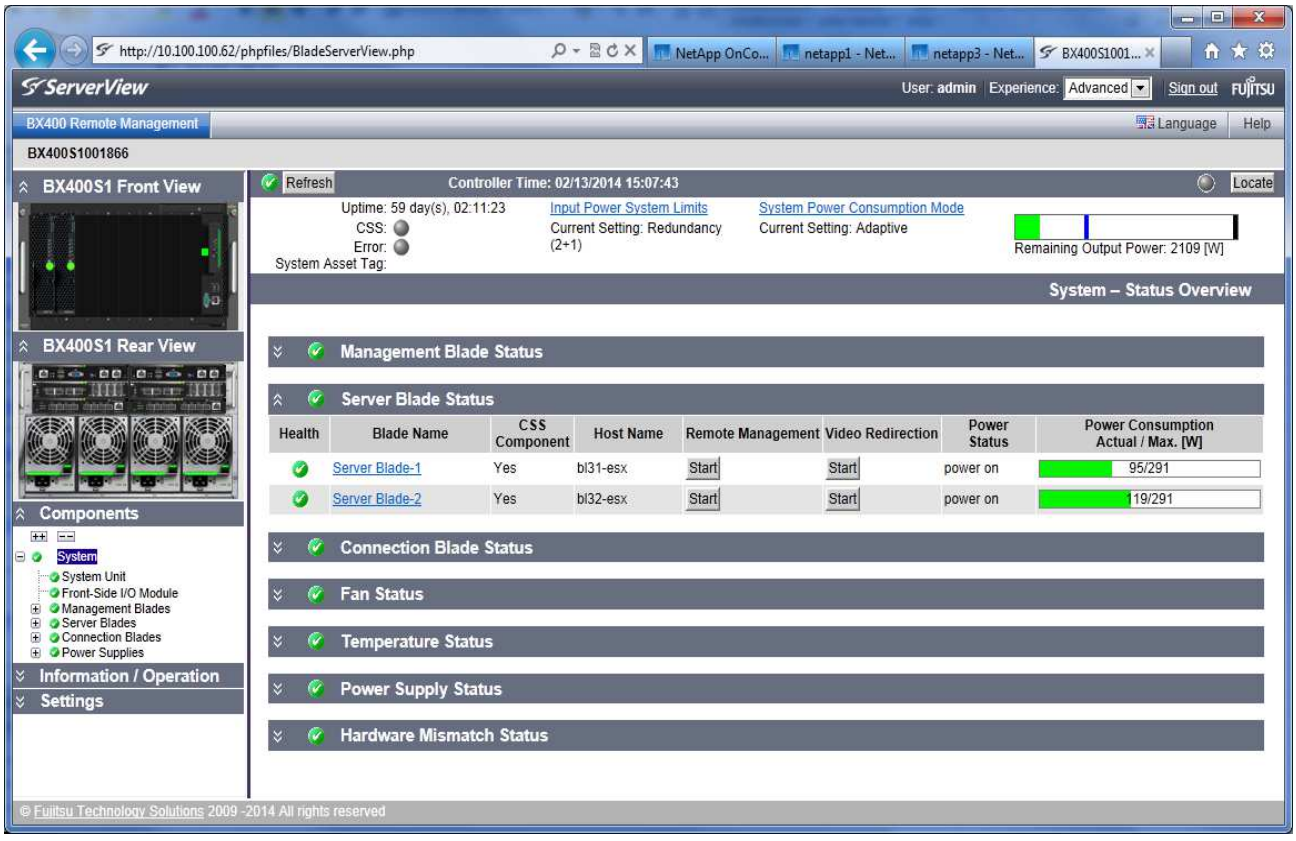
Le risorse elaborative centrali, se si escludono 11 server fisici, consistono in tre infrastrutture Blade Fujitsu distribuite fra le due sale macchine.

Le risorse "periferiche" sono 16 domain controller (in fase di dismissione) e 16 file server.

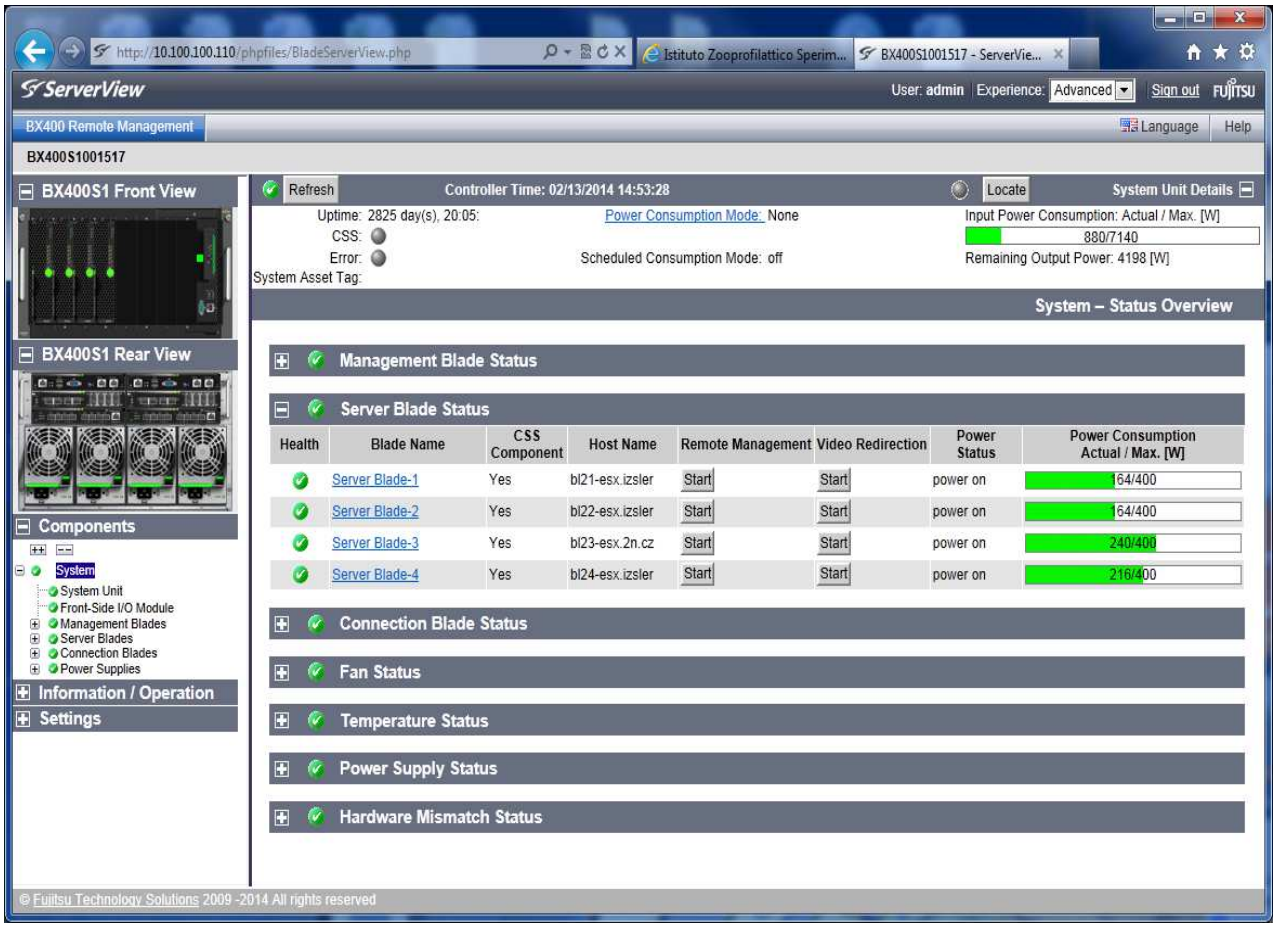
In figura si vede lo chassis dell'infrastruttura più datata, presente in sala macchine 1; la dotazione è di 9 lame di cui otto Bi-processore e una Quadri-processore (Bl12-esx).



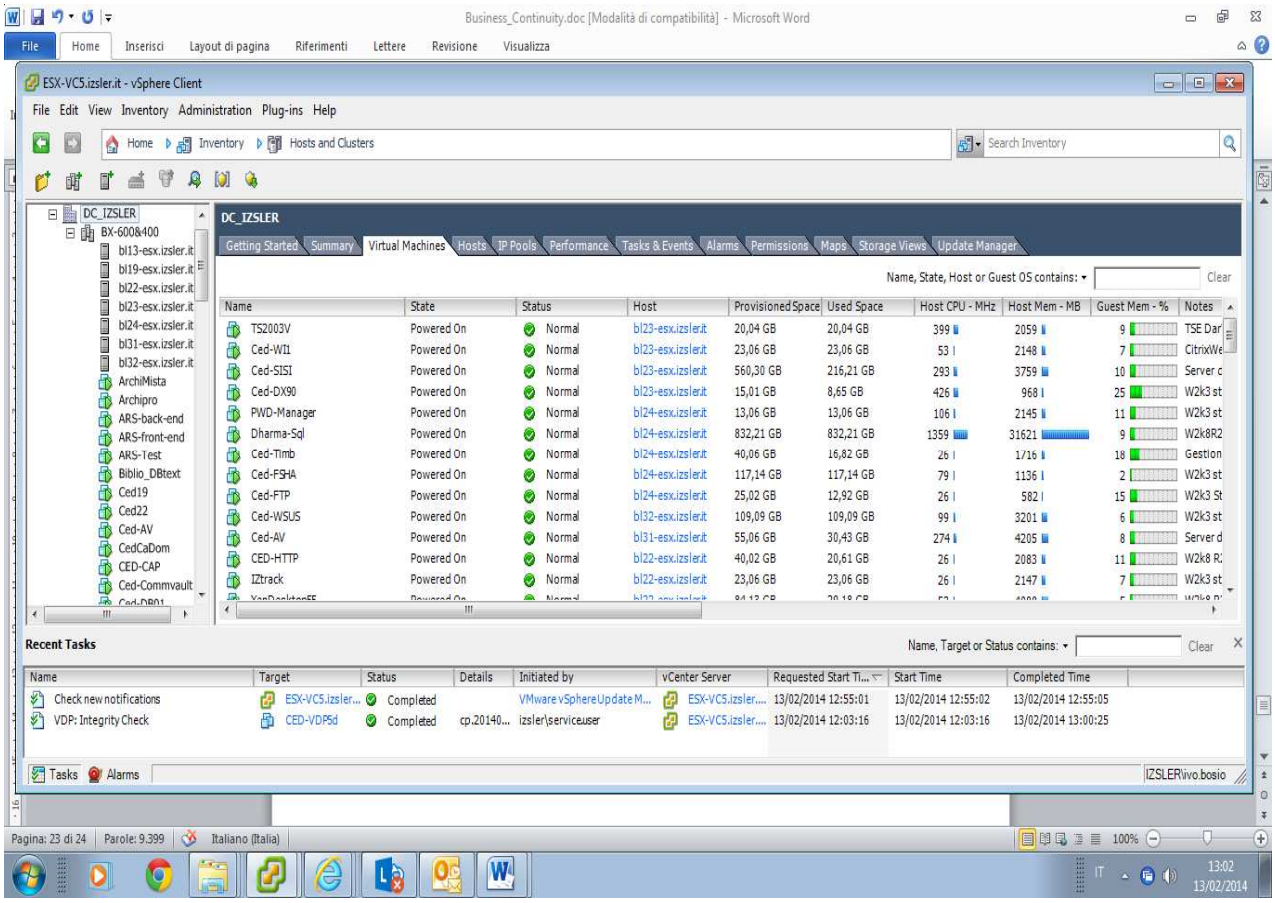
Nella successiva figura si vede lo chassis della seconda infrastruttura Blade Fujitsu più recente, presente sempre in sala macchine 1; la dotazione è di 2 lame Byprocessor Esacore (Bl31-esx e Bl32-esx) gestite da Vmware nella versione Vsphere5.



Segue la visualizzazione dello chassis della terza infrastruttura Blade Fujitsu, presente in sala macchine 2; la dotazione è di 4 lame Byprocessor Esacore (Bl21-esx, Bl22-esx, Bl23,esx e Bl24-esx) gestite da Vmware nella versione Vsphere5.



La figura che segue riporta un esempio della console di gestione Vmware Vspher5



5.2.1.1 *Attività in corso*

È in corso la riscrittura di alcune applicazioni che permetterà di dismettere server fisici obsoleti ed è previsto sia pianificata la formazione del personale alla gestione amministrativa dei server Linux.

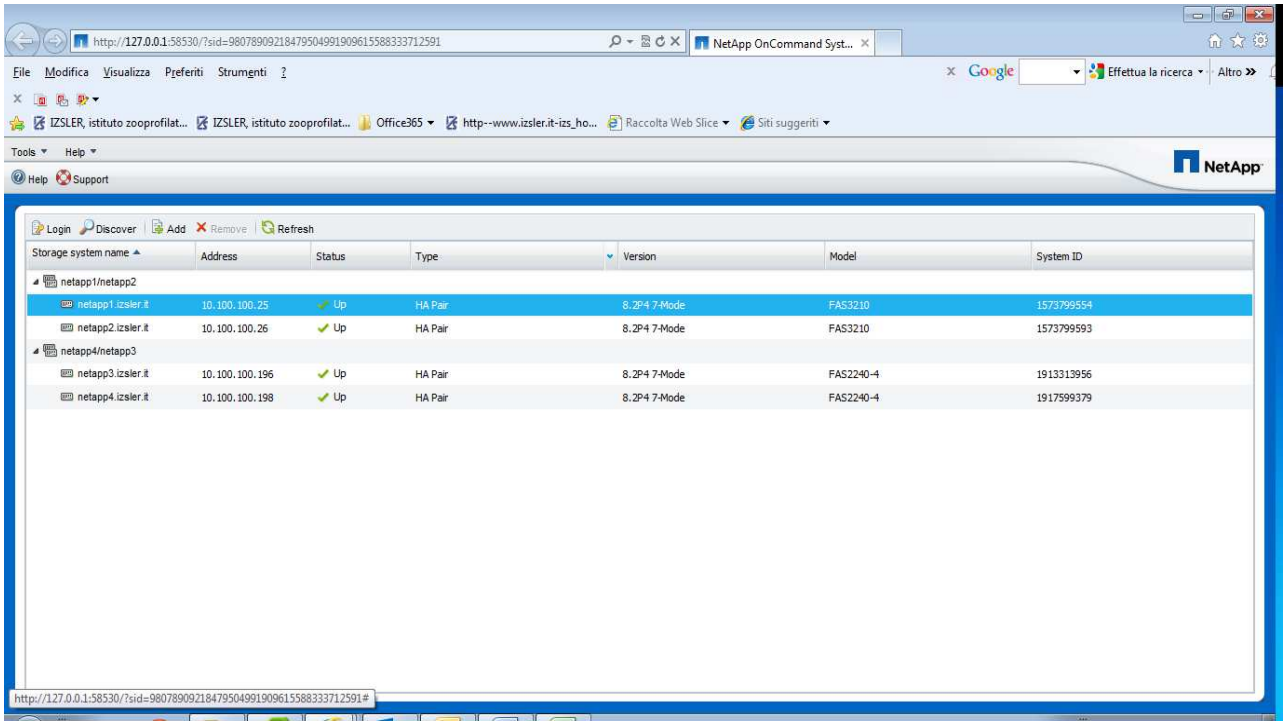
5.2.2 *Storage*

Per storage si intendono non singole risorse disco aggiuntive removibili utilizzate su postazioni di lavoro personali ma vere e proprie infrastrutture installate centralmente nelle sale macchine di Brescia (e una unità Netapp a Parma) e proprio per questo soffrono la criticità decritta in fase di analisi delle infrastrutture LAN (CR-3-Sale-Macchine).

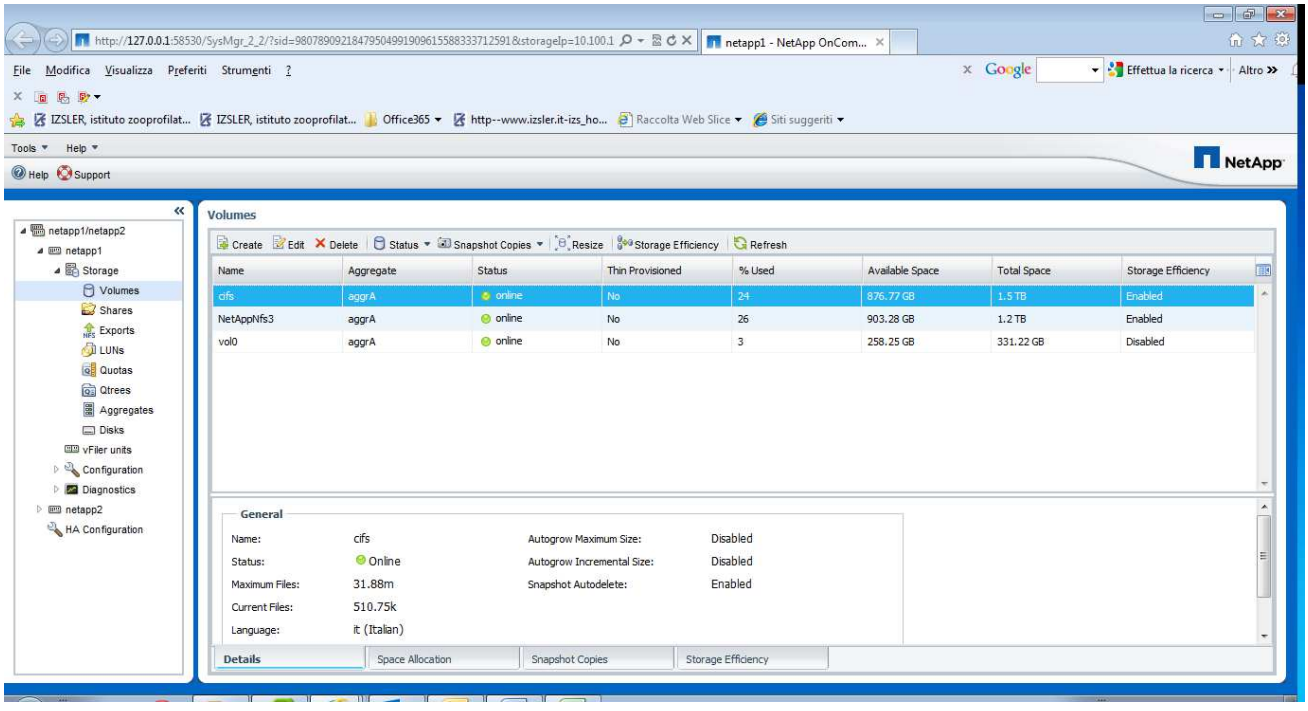
Sono presenti le seguenti infrastrutture Netapp e SAN Fujitsu, più in dettaglio:

- Netapp Mod. 2240A 24x2 TB SATA in Raid installata in sala macchine uno, dedicata ai backup, al file-sharing e macchine virtuali secondarie (in termini di performance)
- Netapp Mod. 2240A 24x2 TB SATA in Raid installata nella sezione diagnostica di Parma e utilizzata sia per la storicizzazione dei dati prodotti da una strumentazione sia come file-sharing e area di storage a disposizione della sezione.
- NetApp Mod. 3210A in modalità Metrocluster sala macchine 1 e 2 doppia testa, 4 shelf 14x450 GB SAS; ospitano macchine virtuali e basi dati; i dischi di ognuno sono in raid 5 con fault tolerance garantita a livello di 3 dischi;

L'immagine che segue rappresenta i due sistemi installati in Sede:

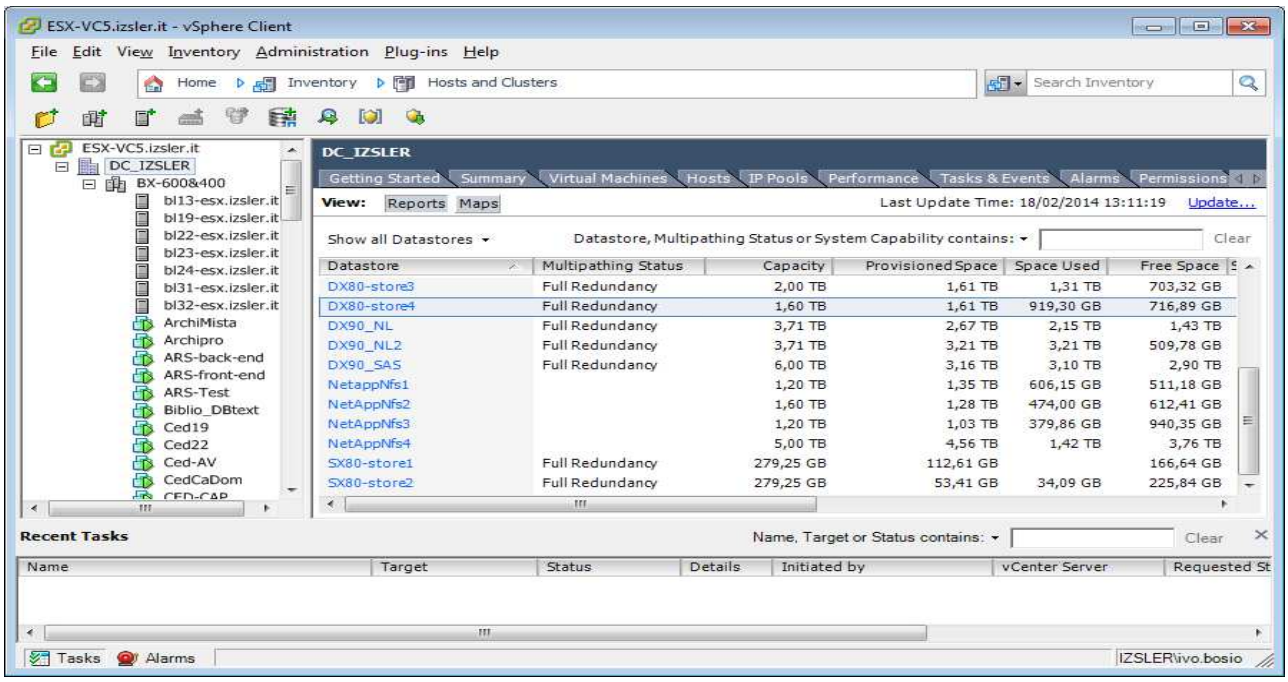


ed evidenzia il contenuto di una delle due teste del sistema 3210



- SAN Fujitsu in sala macchine uno, due sottosistemi:
  - Sx80 (12 dischi SAS da 450 GB), acquistato nel 2008 RAID 5 con due dischi hotspare, ospita principalmente macchine virtuali non prioritarie e lame dedicate a due server fisici: bl17-ca- bl14WS.
  - Dx80 (12 dischi SAS da 450 GB), acquistato nel 2010, RAID 5 con due dischi hotspare, ospita principalmente macchine virtuali non primarie.
- SAN Fujitsu con due storage DX90 distribuiti in sala macchine uno e due e in replica sincrona i dischi sono SAS (N° 34 Fujitsu DX8090 S2 HD SAS 600G 15k 3.5) e N° 20 Fujitsu DX8090 S2 HD NLSAS (Sata) 1TB; ospitano macchine virtuali

Dalla figura che segue si nota che gli storage sono indirizzabili da qualsiasi lama dell'infrastruttura blade Fujitsu gestita tramite la piattaforma VMware Wsphere 5.



5.2.3 Sistema di backup e ripristino – garanzia di disponibilità dei dati

I backup sono organizzati, in termini di risorse dedicate e modalità, in modo diversificato a seconda delle tipologia e dell'importanza degli oggetti da salvare.

Gli oggetti considerati sono di tre tipologie:

- Dati prodotti con applicazioni di Office automation: i dati trattati possono essere sulla postazione di lavoro personale o in aree disco condivise a loro riservate.
  Per quanto concerne i dati trattati su risorse condivise, centralizzate e ridondate fra le due sale, tramite Netapp 3210, il meccanismo di backup utilizzato si basa sulla produzione di snapshot.
- Dati prodotti da backup schedulati dai gestori di basi dati centralizzate: (Sql, Oracle,ecc.), in questo caso i DB administrator dispongono di risorse disco a loro assegnate (netapp3\BackupSQL1 e netapp3\BackupSQL2), per queste sono previsti meccanismi di snapshot automatici e le copie su tape fanno riferimento a specifiche sotto cartelle di queste aree:
  netapp3\BackupSQL1\OnTape, netapp3\BackupSQL2\OnTape
  e netapp3\BackupSAI\OnTape.
- Server fisici e Virtual Machine, sono previste aree disco assegnate per operazioni di backup schedulato tramite Vmware Data Protection prima dei backup su tape.

Sia la frequenza sia le risorse assegnate cambiano a seconda della tipologia e del livello di importanza degli oggetti da salvare e sono documentate nei paragrafi che seguono.

5.2.3.1 Backup dei server e delle basi dati centralizzate

Nel caso dei backup delle basi dati la schedulazione è in carico all'amministratore della base dati, nel caso dei server (fisici o virtuali) o dei documentali la frequenza è gestita dai Sistemi Informativi tenendo presente sia l'importanza dell'oggetto da salvare sia la frequenza di aggiornamento dello stesso.

A fronte di alcune criticità riscontrate, imputabili alla assegnazione di risorse disco di appoggio non opportunamente ridondate o a guasti hardware del sistema di gestione del riversamento su tape, sono stati introdotti dei correttivi in modo da garantire sempre la disponibilità di copie di

backup rendendo indipendente la fase di backup su disco da quella successiva su tape; ne consegue che la copia su tape può essere fatta anche a distanza di giorni in quanto le risorse disco assegnate sono ridondate e un backup successivo nella stessa area disco determina la creazione automatica e preventiva di una snapshot.

Le tecnologie utilizzate sono diverse e sono, per quanto concerne i server:

- CA-ArcServe
- Vmware Data Protection
- Commvault

La modalità di backup dei server sono dettagliate in una base dati specifica. La form che esegue è un estratto di esempio di tale base dati:

Name	ESX-VC5 Backup giornaliero su HD CED-VDP5a start ore 17	ESX-VC5 Backup giornaliero su HD CED-VDP5b start ore 19	backup Giornaliero su tape con BL17-CA	backup Mensile 1^Dom. su tape BL17-CA	backup Mensile 2^Dom. su tape BL17-CA	backup Mensile 3^Dom. su tape BL17-CA	backup Mensile 4^Dom. su tape BL17-CA
ArchiMista		X		X			
Archipro	X			X			
ARS-back-end							X
ARS-front-end							X
ARS-Test							X

5.3 Applicazioni

Sono raggruppabili in tre macro categorie:

- **Tecniche**, cioè realizzate per gestire l'attività dei reparti e laboratori, utilizzate esclusivamente da personale tecnico.
- **Amministrative**, quelle necessarie all'amministrazione (paghe, magazzino, contabilità, protocollo, ecc.) tipicamente a disposizione del personale amministrativo assegnato alle U.O. dell'Amministrazione ma in certi casi in organico a reparti della Sede e delle sezioni diagnostiche provinciali.
- **Di servizio,** quali la posta elettronica, il controllo antivirus, il rilascio degli aggiornamenti per la sicurezza, alerting, ecc.

Mentre le principali applicazioni utilizzate nell'area tecnica sono state scritte e sono gestite da personale interno, le applicazioni amministrative sono state acquisite e sono gestite da fornitori esterni.

Ci sono infine applicazioni, acquisite e gestite da terzi per monitoraggio o gestione di attività trasversali.

Se si esclude la gestione del personale che è su infrastruttura esterna a cui gli utenti accedono tramite Client access, la gran parte, sia di quelle amministrative che di quelle tecniche è centralizzata e utilizzata in modalità Web o tramite Citrix e terminal services di Microsoft, tramite server che sono virtualizzati e in alta affidabilità.

Le basi dati principali sono Microsoft SQLServer, Oracle e MySQL.

Ci sono anche applicazioni locali spesso residenti su postazioni di lavoro (personal computer) che utilizzano prodotti di office automation (Microsoft Office) o programmi specifici per gestire strumenti di analisi o piccoli database. Questo succede sia nei reparti che in amministrazione.

Ci sono applicazioni che pur essendo centralizzate sono state scritte con linguaggi ormai obsoleti, che sono incompatibili con sistemi operativi e basi dati avanzate e che quindi sono da riscrivere o sostituire.

Fra le applicazioni "tecniche e amministrative" quelle più utilizzate e significative, da gran parte del personale sono:

- DARWin (Diagnosi, Analisi, Ricerche in ambiente Windows): è l'applicazione utilizzata in tutti i reparti sanitari della Sede e delle Sezioni Diagnostiche Provinciali per la gestione di tutte le fasi che vanno dalla accettazione dei campioni alla produzione dei rapporti di prova. Integra servizi web di interazione applicativa con applicazioni sviluppate da altre enti pubblici che svolgono attività di prelievo, controllo e consulenza sul territorio (AUSL, NAS, ecc.).
- SISI: gestione dei campioni dei laboratori latte, dei campioni TSE, della firma digitale e successivo delivery automatizzato dei Rapporti di Prova
- SAI: Sistema Amministrativo-contabile Integrato
- SIGMA: Gestione del personale e delle presenze
- ARCHIPROWEB & INFATTIWEB: gestione protocollo e atti dell'Ente
- FORMAZIONE Residenziale e a distanza

Fra le applicazioni di "servizio" quella utilizzata da tutto il personale dipendente e non solo è la "posta elettronica", tale servizio viene erogato in Cloud da Microsoft con la piattaforma Office 365 che integra anche il servizio di videoconferenza (Lync), Onedrive e Sharepoint.

Le altre applicazioni di servizio sono utilizzate dal personale dei sistemi informativi per la prevenzione o per il controllo hardware e software sia delle componenti centralizzate che periferiche.

6 PROGETTI E ATTIVITÀ IN CORSO

È in corso la definizione di un piano per la Business Continuity anche a fronte di Disaster Recovery. Nel piano sono previsti interventi di potenziamento in termini di ridondanza sia per quanto concerne le infrastrutture di comunicazione (WAN, LAN e WiFi) che per quanto concerne le risorse elaborative (sito di DR in cloud).

È in valutazione la realizzazione di un progetto per la diffusione di connettività Wifi in ogni struttura sia della Sede che nelle sezioni diagnostiche provinciali.

7 SICUREZZA

Il traffico di rete fra LAN, WAN e DMZ è regolamentato da un firewall in HA (vedi paragrafo infrastrutture di rete).

La grandissima maggioranza delle PDL (più del 95%) è sottoposta alle policy di dominio e gli utenti, salvo eccezioni giustificate non hanno diritti amministrativi sulle PDL.

Sia i server che le PDL ricevono in automatico, salvo rare eccezioni motivate, gli aggiornamenti per la sicurezza tramite un servizio di distribuzione centralizzato (Microsoft Wsus).

Sulle PDL e sui Server, a grandissima maggioranza e salvo rari casi (incompatibilità applicativa per postazioni assegnate a strumenti di analisi) è presente un antivirus (Sophos) la cui distribuzione, monitoraggio e relativi interventi è gestita attualmente da personale dei Sistemi Informativi e della ditta che si occupa della assistenza sulle PDL.

7.1 Criticità

a. Nonostante le azioni preventive messe in atto, il livello di obsolescenza di alcuni server e delle applicazioni nonché a volte l'impossibilità di applicare policy restrittive, ha permesso di rilevare, ad un test di Intrusion detection, criticità che dovranno essere rimosse.
b. Gli accessi alle risorse di dominio sono controllati solo logicamente attraverso la richiesta di credenziali nel momento in cui si cerca di accedere ad una risorsa in dominio ma non è controllato ne l'accesso Wifi e nemmeno la connessione fisica alle borchie di rete.

   In merito è prevista l'implementazione di un sistema per migliorare il controllo accessi che prevede due modalità:

   - Wired e SSID Wireless Corporate: Autenticazione 802.1x su AD con credenziali di dominio (in transparent). Cambio di VLAN in base all'utenza. Possibilità di MacBypass per PC non in dominio / dispositivi mobile dirigenti.
   - Wireless Guest: Autenticazione tramite guest portal. Possibilità di autoregistrazione o creazione credenziali da guest portal.

8 VERIFICHE QUALITÀ DEL SERVIZIO E SLA

8.1 Valutazioni sullo stato del servizio

I Sistemi Informativi dell'Istituto faranno analisi periodiche sulle chiamate e sul servizio in genere al fine di verificare che questi rispondano ai requisiti descritti nel capitolato; queste analisi devono essere possibili anche attraverso un servizio di consultazione e reporting messo a disposizione dalla ditta aggiudicataria; i dati devono essere esportabili in un formato standard condiviso dai Sistemi Informativi. Potrà essere richiesta la trasmissione periodica del report con frequenza che sarà concordata in fase di avvio del servizio e che potrà cambiare a discrezione della direzione dei sistemi informativi o suo delegato.

Il responsabile dei Sistemi Informativi dell'Istituto o suo delegato incaricherà uno o più referenti per la verifica dell'esecuzione del contratto.

8.2 Accesso a tracciatura e rendicontazione delle registrazioni

La ditta aggiudicataria dovrà mettere a disposizione dell'Istituto, in modalità web, il sistema per consentire, al Responsabile dei sistemi informativi o ai suoi delegati di:

a. Verificare puntualmente i tempi di ogni chiamata e la storia degli interventi effettuati;
b. Produrre un'estrazione completa e dettagliata di tutti gli interventi ancora in corso;
c. Produrre report di analisi della qualità del servizio.

8.3 SLA e penalità

8.3.1 Tabella riassuntiva

Di seguito si elencano i tempi da rispettare nell'esecuzione del servizio, al di fuori dei quali saranno applicate, le penali indicate.

La penale potrà essere applicata solo se il superamento dei tempi non sia stato determinato da problemi non di competenza della ditta aggiudicataria quali ad esempio guasti hardware, indisponibilità della rete (Wan e/o LAN), impossibilità di accedere ai locali (Sale macchine e/o uffici), indisponibilità del personale tecnico interno, ecc.

#	Descrizione servizio	Tempistica	Penalità
1	Avvio del servizio	Entro 15 gg lavorativi dall'assegnazione dell'appalto comunicata in forma scritta	Per ogni giorno o frazione dello stesso di ritardo la penalità è di € 500,00.
2	Avvio del Call center	Entro 7 gg lavorativi dall'avvio del servizio	Per ogni giorno o frazione dello stesso di ritardo la penalità è di € 500,00.
3	Interventi di alta priorità	Soluzione, entro 2 ore lavorative dalla classificazione/comunicazione da parte dei Sistemi Informativi e secondo le modalità definite	Quando la tempistica è superata per 60 minuti lavorativi la penalità è di € 500,00 per ogni ora oltre le due ore previste.
4	Interventi di priorità normale	Soluzione entro 6 ore lavorative dal manifestarsi del problema	Se trimestralmente il 5% degli interventi supera i tempi previsti la penalità è di € 1.000,00; in ogni caso quando si superano le 12 ore lavorative (inclusa la tempistica) per un intervento la penalità è di € 500,00.
5	Interventi di priorità bassa	Soluzione entro 12 ore lavorative dal manifestarsi del problema	Se trimestralmente il 5% degli interventi supera i tempi previsti la penalità è di € 1.000,00; in ogni caso quando si superano le 24 ore lavorative per un intervento se non differentemente concordato con i Sistemi Informativi la penalità è di € 200,00.
11	Call center e Help desk	8:00 - 17:00 dal lunedì al venerdì	Dopo 3 chiamate senza risposta, oppure assenza della mail di conferma e presa in carico del problema, scatta la penale pari ad € 1.000,00.
12	Call center (modalità web)	Sempre attivo	L'interruzione per più di un'ora consecutiva con assenza della mail di conferma e presa in carico del problema, comporta una penale di € 1000,00.

9 REQUISITI MINIMI PER IL FORNITORE

Per partecipare alla gara, le imprese devono soddisfare i seguenti requisiti minimi:

1. Dimostrare di disporre delle seguenti certificazioni minime:
   - NetApp Gold

- Citrix Gold
- Vmware Enterprise
- Microsoft Partner

In particolare, nell'ambito Microsoft, sono richieste competenze elevate almeno sui sistemi operativi (client e server), SQL server, MS Office e Office 365, Lync/Skype, Sharepoint/Onedrive, piattaforma Azure.

2. Il fornitore dovrà indicare un suo responsabile di progetto, reperibile in orario lavorativo, 8:00 – 18:00, che:
   a. Abbia la gestione dell'intero servizio di assistenza
   b. Sia in grado di interagire con l'Istituto per problematiche, sia per le parti tecniche che applicative che funzionali
   c. Sia in grado di pianificare e gestire i tempi di intervento

10 DOCUMENTAZIONE TECNICA DEL FORNITORE

L'offerta deve essere corredata da documentazione tecnica che permetta all'Istituto sia di conoscere e valutare le modalità previste per l'erogazione dei servizi richiesti sia di sapere quali e quante risorse umane saranno assegnate.
Tutte le certificazioni indicate ed altre prodotte dalla ditta devono essere valide ed aggiornate per tutto il periodo di espletamento del servizio in oggetto; saranno valutate positivamente le seguenti certificazioni aggiuntive:

- Commvault administrator
- Linux administrator
- Sophos Platinum
- CA Gold (Arcserve)
- Oracle Gold

Il gruppo tecnico deve possedere buone conoscenze sia delle principali infrastrutture utilizzate in Istituto sia del mondo open source (installazione, configurazione e gestione).

Nella relazione tecnica dovranno essere comunicati, in documenti separati, e saranno oggetto di valutazione:

- il curriculum professionale e le eventuali certificazioni del responsabile di progetto
- i curriculum e le caratteristiche professionali dei componenti del gruppo di lavoro che realizzerà il servizio e le eventuali certificazioni possedute

Una volta avviato il servizio, l'eventuale sostituzione del responsabile di progetto sarà sottoposta a verifica da parte del dirigente dei Sistemi Informativi o suo delegato che potranno anche non accettare la proposta qualora non ritenuta idonea.

La direzione dei Sistemi Informativi potrà richiedere documentazione aggiuntiva qualora quella fornita in sede di offerta fosse ritenuta insufficiente. L'Istituto si riserva la possibilità di non considerare valide le offerte non sufficientemente documentate.

Tutto il materiale fornito, o sua assenza/incompletezza, sarà usato per valutare l'offerta tecnica del Fornitore.

11 CRITERI DI VALUTAZIONE DELL'OFFERTA E MODALITÀ DI AGGIUDICAZIONE

L'appalto sarà aggiudicato ai sensi dell'articolo 83 del D. Lgs. 12/04/2006 n. 163 a favore dell'offerta economicamente più vantaggiosa, sulla base dei criteri successivamente specificati.

Le offerte presentate saranno valutate dall'apposita commissione giudicatrice nominata ai sensi dell'art. 84 del D.Lgs. 163/2006.

La commissione procederà alla valutazione secondo i criteri sotto descritti, attribuendo complessivamente il punteggio massimo di 100 punti:

I criteri di valutazione sono i seguenti:

- **offerta tecnica punteggio max 60.**

- **prezzo punteggio max 40**;

La commissione procederà alla valutazione dell'offerta tecnica attribuendo complessivamente il punteggio massimo di 60 punti così suddivisi:

1) **Gestione delle problematiche [25 punti assegnati]** - Le caratteristiche che saranno oggetto di valutazione sono:
   a. **Il supporto specialistico**: saranno preferite soluzioni, dove è previsto un supporto specialistico di secondo e terzo livello che possa contare su un numero significativo di sistemisti per risolvere i problemi.
      Punteggio massimo 5;
   b. **Il processo di gestione dell'anomalia dal momento della sua registrazione**: il suo ciclo di vita (workflow specifico), come la stessa viene tracciata, la sua storicizzazione, la reportistica disponibile, la sua utilizzabilità, sua eventuale personalizzabilità, i livelli di escalation, le connessioni con terze parti, il passaggio di responsabilità.
      Punteggio massimo 5;
   c. **La metodologia di gestione degli alert e delle chiamate**: saranno preferite soluzioni mirate a garantire la massima disponibilità del call center e del responsabile del servizio e che utilizzano le metodologie di comunicazione più diffuse e disponibili.
      Punteggio massimo 5;
   d. **Proposte migliorative** rispetto al numero di ore richieste, disponibilità del servizio e tempi di intervento.
      Punteggio massimo 10;

2) **Curriculum e certificazioni [35 punti assegnati]** – Le caratteristiche che saranno oggetto di valutazione sono:
   a. **Curriculum** dell'intero gruppo di lavoro: saranno valutate positivamente esperienze pregresse nella realizzazione di progetti di BC/DR e di migrazione e gestione di sistemi informatici in cloud.
      Punteggio massimo 20;
   b. **Certificazioni**: saranno valutate le certificazioni aggiuntive presentate, in particolare quelle indicate nel paragrafo 10, da parte del personale che realizzerà il servizio.
      Punteggio massimo 15;

La valutazione dei singoli elementi sarà effettuata con il metodo aggregativo-compensatore, attraverso l'utilizzo della seguente formula:

$$C(a)= \Sigma_n[W_i * V(x)_i]$$

dove:

- **C(a) =** indice di valutazione dell'offerta (**a**);
- **n** = numero totale di requisiti rispetto ai quali vengono fatte le valutazioni;
- W_i = peso o punteggio attribuito al requisito (i);
- $V(a)_i$ = coefficiente della prestazione dell'offerta (**a**) rispetto al requisito (**i**), variabile tra zero ed uno;
- Σ_n = sommatoria.

I coefficienti **V(a)i** sono determinati, per quanto riguarda la valutazione degli elementi tecnici proposti di natura qualitativa, attraverso la media dei coefficienti, variabili tra **0** (zero) ed **1** (uno), calcolati da ciascun commissario mediante il << confronto a coppie >>, seguendo le linee guida riportate nell'allegato G del D.P.R. 5-10-2010 n.207 *(Regolamento di attuazione del Codice dei Contratti).*

Vengono ammessi alla successiva fase di gara esclusivamente i concorrenti che raggiungono un punteggio tecnico pari o superiore a 25.

Requisito economico

Valutazione offerta economica

Il punteggio del requisito economico (Valutazione economica) è determinato, attraverso il sistema di calcolo di seguito specificato:

al corrispettivo economico complessivo più basso, derivante - ai soli fini dell'applicazione del punteggio - dall'applicazione del ribasso offerto sull'importo totale dell'appalto, sarà attribuito il punteggio massimo di 40 punti ed alle altre offerte sarà assegnato un punteggio proporzionale, attribuito mediante applicazione della seguente formula:

$$X = \frac{Pi \times C}{Po}$$

Dove:

X	=	punteggio attribuibile alla società in esame;
Pi	=	corrispettivo economico complessivo più basso;
C	=	punteggio massimo attribuibile (40 punti);
Po	=	corrispettivo economico complessivo offerto dalla società in esame.

Non sono ammessi ribassi del 100%.

Secondo quanto previsto dall'art. 86 del D.Lgs. 163/2006 sarà valutata la congruità delle offerte in relazione alle quali sia i punti relativi al prezzo, sia la somma dei punti relativi agli altri elementi di valutazione, sono entrambi pari o superiori ai quattro quinti dei corrispondenti punti massimi previsti dal bando di gara.

Le offerte anormalmente basse saranno trattate secondo quanto disposto dagli artt. 87 e 88 del D.Lgs. 163/2006 e s.m.i.

In caso di parità di punteggio delle offerte risultate economicamente più convenienti, sarà privilegiata l'offerta che avrà riportato il punteggio più alto riferito all'elemento Offerta tecnica.

11.1 Importo base d'asta e modalità di partecipazione

L'investimento massimo previsto è di 130.000,00 Euro.

La partecipazione può essere come impresa singola o associata (RTI e Consorzi).

12 DISPOSIZIONI PER L'ESECUZIONE DEL CONTRATTO

12.1 Risoluzione del contratto

Qualora venga riscontrato, durante le operazioni di collaudo o durante le verifiche in fase di avvio del progetto, che la fornitura del servizio in tutto o in parte non è rispondente alle specifiche richieste, l'Impresa dovrà impegnarsi ad adeguare tempestivamente, e comunque entro 10 giorni lavorativi dalla richiesta, senza oneri aggiuntivi per l'l'Ente e fatta salva la possibilità, da parte di quest'ultima, di applicare le penali prima descritte.

Qualora il servizio correttivo o sostitutivo non venisse effettuato nei tempi richiesti e nei tempi concordati, l'IZSLER potrà risolvere il contratto per colpa grave dell'Impresa.

La risoluzione del contratto può essere richiesta dall'Ente anche:

nel caso di interruzione del servizio senza giusta causa;

- nel caso di subappalto non autorizzato;
- in caso di cessione dell'Impresa, di cessazione dell'attività, oppure nel caso di concordato preventivo, di fallimento e di conseguenti atti di sequestro o di pignoramento a carico dell'Impresa;
- nel caso in cui il totale delle penalità e detrazioni superi il 10% dell'importo contrattuale complessivo;
- nel caso di grave inadempimento contrattuale;
- nel caso di mancata ottemperanza degli obblighi previsti nel contratto a seguito di diffida scritta ad adempiere;
- nel caso di perdita da parte della ditta della capacità di contrattare con la pubblica amministrazione.

Resterà inoltre salva per l'IZSLER la possibilità di applicare tutte le norme di legge e di regolamenti in materia.

12.2 Tracciabilità dei flussi finanziari

La ditta aggiudicataria della fornitura assume su di sé gli obblighi di tracciabilità dei flussi finanziari di cui alla L.136 del 13/08/2010 e ss. mm. ii.

La ditta deve comunicare all'Istituto gli estremi identificativi di uno o più conti correnti bancari o postali, accesi presso banche o presso la società Poste italiane Spa, dedicati, anche non in via esclusiva alle commesse pubbliche o, nel caso di conti correnti già esistenti, dalla loro prima utilizzazione in operazioni finanziarie relative ad una commessa pubblica, entro 7 giorni dalla loro accensione. In entrambi i casi le coordinate del conto corrente dovranno essere trasmesse insieme alle generalità, al codice fiscale delle persone delegate ad operare su di esso (art.3 comma 7).

Tutte le comunicazioni di cui sopra sono fatte mediante dichiarazione sostitutiva dell'atto di notorietà ex art. 47 D.P.R. n. 445/2000 da inviarsi a mezzo posta o fax (nr. 030/2425251) alla U.O. Economico Finanziaria, corredata da copia di un documento di identità del sottoscrittore in corso di validità.

In pendenza della comunicazione dei dati di cui sopra, l'Istituto non eseguirà alcun pagamento a favore dell'appaltatore. Di conseguenza, i termini di pagamento si intenderanno sospesi.

La ditta si impegna altresì a comunicare ogni modifica relativa ai dati trasmessi entro sette giorni da quello in cui la variazione è intervenuta.

La ditta aggiudicataria deve trasmettere all'Ufficio Gare e Contratti della U.O. Provveditorato Economato e Vendite dell'Istituto, entro quindici giorni dalla stipulazione, copia dei contratti sottoscritti con i subcontraenti della filiera delle imprese a qualsiasi titolo interessate al presente appalto, per la verifica dell'inserimento dell'apposita clausola con la quale i contraenti assumono gli obblighi di tracciabilità dei flussi finanziari di cui alla legge n. 136/2010 e s.m.i., ivi compreso quello di comunicare alla Stazione Appaltante i dati di cui sopra, con le modalità e nei

tempi ivi previsti. Si impegna altresì a dare immediata comunicazione all'Istituto ed alla prefettura-ufficio territoriale di Brescia della notizia dell'inadempimento della propria controparte (subcontraente) agli obblighi di tracciabilità finanziaria.

Per quanto non espressamente indicato, si rinvia integralmente agli artt. 113, 114, 115 e seguenti del D.lgs 163/2006.

12.3 Esecuzione del contratto

Per quanto non espressamente indicato, si rinvia integralmente agli artt. 113, 114, 115 e seguenti del D.lgs 163/2006.

Ai sensi dell'art. 119 del Codice dei contratti, l'Istituto verifica il regolare andamento dell'esecuzione del contratto da parte dell'esecutore attraverso il responsabile del procedimento il quale verifica che le attività e le prestazioni contrattuali siano eseguite dal contraente in conformità dei documenti contrattuali.

L'esecutore è tenuto a seguire le istruzioni e le direttive fornite per l'avvio dell'esecuzione del contratto; qualora l'esecutore non adempia, l'Istituto ha facoltà di risolvere il contratto.

12.4 Terminazione

Per terminazione si intendono tutte le attività necessarie che l'aggiudicatario dovrà porre in essere per trasmettere al personale incaricato da IZSLER (o al personale di altro fornitore subentrante) tutte le informazioni acquisite nel corso dell'esecuzione della fornitura del servizio, nonché quant'altro, anche a livello documentale, risulti necessario per garantire la regolare prosecuzione del servizio medesimo. In particolare, il servizio di Terminazione include:

un periodo di affiancamento di tre mesi precedenti la scadenza contrattuale, durante il quale il Fornitore garantisce la piena collaborazione al personale IZSLER (o di altro fornitore subentrante) se richiesta;

la disponibilità di tutte le risorse professionali, di adeguato profilo ed esperienza, necessarie a garantire il predetto affiancamento ed il completo passaggio di consegne;

realizzare e consegnare ad IZSLER ogni tipo di documentazione tecnica che dovesse rendersi necessaria per garantire l'efficacia del trasferimento delle conoscenze dal Fornitore della presente gara al personale IZSLER (o di altro fornitore subentrante).

12.5 Responsabile esterno trattamento dati

L'Istituto nominerà l'aggiudicatario della procedura Responsabile esterno del trattamento dei dati, nel rispetto di quanto disposto dal decreto legislativo 30 giugno 2003, n. 196, "Codice in materia di protezione dei dati personali".

L'aggiudicatario deve, in ogni caso, comunicare all'Istituto i nominativi dei suoi collaboratori incaricati del trattamento dei dati.

12.6 Riservatezza

Il personale della ditta aggiudicataria si impegna a non diffondere a terzi, anche dopo la scadenza contrattuale, nessuna informazione di qualsiasi tipo su dati, organizzazione, procedure, configurazioni o altro di proprietà dell'Istituto, di cui venisse a conoscenza durante lo svolgimento del servizio.

Se la ditta aggiudicataria, per necessità inerenti allo svolgimento del servizio, ritenesse di dover importare nel proprio ambiente i dati e le informazioni di cui sopra, dovrà ottenerne preventiva autorizzazione da parte dell'Istituto. La richiesta di autorizzazione dovrà specificare: le

informazioni e i dati che verranno importate, e le motivazioni per cui è necessario importare le informazioni stesse.

La ditta aggiudicataria si impegna inoltre a:

Proteggere il materiale importato dalla sua diffusione a terzi;

Utilizzare le informazioni solo per le necessità inerenti allo svolgimento del servizio;

Cancellare i dati a conclusione di ogni intervento e comunque a scadenza del contratto o su richiesta dell'Istituto.

Dovrà in ogni caso rispettare scrupolosamente quanto previsto dalla normativa in vigore.

12.7 Rinvii al Capitolato generale

Per quanto non previsto dal presente allegato, si richiama espressamente il Capitolato Generale (Delibera Direttore Generale n. 443 del 17.09.2010), consultabile all' Albo on Line sul sito www.izsler.it, e segnatamente i seguenti articoli: art. 7 (Cessione del contratto, subappalto e cessione del credito), art. 8 (Esecuzione del contratto) e art. 19 (Foro competente).

12.8 Codice di Comportamento

Il committente informa la propria attività contrattuale secondo i contenuti di cui al Codice di Comportamento, quale dichiarazione dei valori, insieme dei diritti, dei doveri e delle responsabilità, nei confronti dei portatori di interesse (dipendenti, fornitori, utenti, ecc.), approvato con deliberazione del Direttore Generale n. 41 del 04/02/2014, in ottemperanza a quanto previsto dall'art. 54 del D. Lgs. n. 165/2001 così come sostituito dall'art. 1, comma 44 della L. 190/2012 recante "Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella pubblica Amministrazione", documento che integra e specifica il Codice di Comportamento dei dipendenti pubblici di cui al DPR n. 62/2013.

Le norme contenute nel Codice si applicano, per quanto compatibili, ai titolari di contratti di consulenza o collaborazione a qualsiasi titolo, anche professionale, ai titolari di organi e di incarichi negli uffici di diretta collaborazione dei vertici politici dell'amministrazione, nonché ai collaboratori a qualsiasi titolo, anche professionale, di imprese fornitrici di servizi in favore dell'Istituto.

Tutti i fornitori, quali soggetti terzi sono tenuti nei rapporti con il Committente, ad uniformare la loro condotta ai criteri fondati sugli aspetti etici della gestione dei contratti definiti nel Codice di Comportamento, tenendo presente che la violazione dello stesso comporterà la risoluzione di diritto del rapporto contrattuale in essere, nonché il pieno diritto del Committente di chiedere ed ottenere il risarcimento dei danni patiti per la lesione della sua immagine ed onorabilità.

I fornitori dovranno altresì, attenersi a quanto previsto dal DPR 16.04.2013, N. 62: "Regolamento recante codice di comportamento dei dipendenti pubblici, a norma dell'art. 54 del D.Lgs. 30 marzo 2001, n. 165" che al comma 3 dell'art. 2 stabilisce che le pubbliche amministrazioni estendono gli obblighi di condotta previsti dal presente codice nei confronti di imprese fornitrici di beni e servizi.

A tal fine, nel caso di violazione degli obblighi derivante dal citato codice, il committente potrà procedere alla risoluzione o decadenza del rapporto contrattuale.

Il Codice è reperibile sul sito internet aziendale: www.izsler.it, nella sezione "Amministrazione Trasparente "– "Disposizioni generali" – sotto-sezione di primo livello "Atti generali", sotto-sezione di secondo livello "Codice disciplinare e codice di condotta".