OSPEDALI DEI COLLI
MONALDI - COTUGNO - C.T.O.
"AZIENDA OSPEDALIERA SPECIALISTICA DEI COLLI"
Monaldi - Cotugno - C.T.O.

AZIENDA OSPEDALIERA DEI COLLI

80131 NAPOLI VIA LEONARDO BIANCHI s.n.c.
U.O.C. Servizio Informativo Aziendale - E-mail: ced@ospedalideicolli.it
Tel. +39 0817062280/2289/2220/5108 – Fax +39 0817062526
www.ospedalideicolli.it - info@ospedalideicolli.it

AVVISO VOLONTARIO PER LA TRASPARENZA EX ANTE

Indagine di mercato e avviso volontario per la trasparenza preventiva relativa alla procedura negoziata, senza previa pubblicazione del bando di gara (D.Lgs 50/2016 e s.m.i.) per l'affidamento della "Fornitura di hardware e software supplementari rispetto a quelli previsti dal contratto quadro CONSIP SPC CLOUD Lotto 1 – Servizi di Cloud Computing.".

L'A.O. dei Colli di Napoli ha aderito al contratto quadro Consip Lotto 1 – Servizi di Cloud Computing - ed ha l'esigenza di acquisire la fornitura di Hardware e Servizi supplementari rispetto a quelli previsti dal su citato contratto Consip.

L'operatore economico in favore del quale è stata adottata la decisione di aggiudicazione dell'appalto è: **TELECOM ITALIA S.p.A.** (nel seguito **TIM**).

Il valore totale finale dell'appalto stimato è pari a € 858.270,71 oltre IVA.

Nella tabella seguente sono riepilogate le componenti oggetto di indagine:

ID	Descrizione componente
1	4 server fisici per DB ORACLE
2	Colocation DB IDC di Acilia + collegamento a 100MB fra Acilia e Pomezia
3	Colocation DB IDC di Pomezia
4	VDCN Napoli-Acilia 1 GB + Colocation Apparati in IDC Napoli
5	VDCN Napoli-Pomezia 1 GB + Colocation Apparati in IDC
6	Servizi di Sicurezza (FW, WAF, AV, IPS, Vulnerability assessment, Penetration Test infrastrutturali e applicativo
7	Servizi di Patching software applicativo di Nexera S.p.A.
8	Servizi di Patching software applicativo di Engineering Ingegneria Informatica S.p.A.
9	Servizi di Patching software applicativo di Dedalus Italia S.p.A.
10	Manutenzione Piattaforma HW sito DR (server blade HP con SLA NBD. non è compreso il supporto per RedHat e Windows) e DataProtector Software
11	Manutenzione server radiologie (sono esclusi i robottini e le stazioni video di refertazione) e UPS Radiologie
13	Supporto licenze VMWare
14	Upgrade memoria e RAM piattaforma di DR
15	N°6 Server per gestione locale laboratori + 3 Rack + 3 UPS etc..+Installazione + Man Server (24 mesi)+Adattatori (RS232/Lan)
16	Licenze COBOL per applicativo HR
17	Dark Fiber (Fibra Spenta) Monaldi - TIM IDC Napoli in doppia via con diversificazione di circuiti e apparati
18	Dark Fiber Monaldi - CTO in doppia via con diversificazione di circuiti e apparati
19	Dark Fiber Monaldi - Cotugno + Interconnessione in FO per 2°via per la diversificazione di circuiti e apparati
20	Apparati switch Tipo (#8) + Moduli SPF 10GB (#10) + Moduli SPF 1GB (#6)+Alimentazione ridondata (#8)+UPS (#4 3000)+RACK + Installazione + Configurazione + Manutenzione + Accentramento chiamate
21	300 token usb di Firma Digitale

L'oggetto dell'appalto è di seguito descritto:

1. INFRASTRUTTURA TECNOLOGICA

1.1. SERVER FISICI DEDICATI AL DB ORACLE

Nella realizzazione dell'infrastruttura sono previsti due coppie di server fisici dedicati alla realizzazione di due Cluster per il DB. La coppia di Cluster saranno ospitati in colocation presso gli IDC TIM di Acilia e Pomezia.
I due cluster saranno collegati tramite un collegamento dedicato su rete MPLS con Velocità di 100Mbps, ed i due DB saranno allineati, in modalità asincrona, tramite il software Oracle Data Guard.
Le configurazioni delle macchine fisiche previste sono riportate di seguito:

- N. 4 PowerEdge R640 Server ciascuno con le seguenti caratteristiche:
  Intel® Xeon® Gold 5120 2.2G, 14C/28T, 10.4GT/s 2UPI, 19M
  64 GB RAM
  Red Hat Enterprise Linux 7.5
- SAN 6 TB da infrastruttura TIM nel Data Center Acilia
- SAN 6 TB da infrastruttura TIM nei Data Center Pomezia

I due cluster server dovranno ospitare il RDBMS Oracle, le cui licenze in modalità UNLIMITED LICENSE AGREEMENT (ULA) sono state acquisite dall'A.O. tramite il contratto quadro So.Re.Sa. della Regione Campania I server dovranno essere installati presso i due Data Center di TIM di Acilia e Pomezia.

1.2. RISORSE FISICHE DA DESTINARE AI LABORATORI DI ANALISI E LE RADIOLOGIE

Per i laboratori del Monaldi, Cotugno e CTO sono previsti la fornitura di N° 3 cluster, ognuno composto da N°2 nodi, che consentano l'ottimizzazione operativa del collegamento strumentale. Tali cluster comunicheranno al software LIS (Laboratory Information System), collocato nell'IDC, gli esiti delle indagini richieste e non avranno nessun altro legame operativo con gli IDC previsti nelle sedi di TIM.

Tale soluzione assicura che la comunicazione tra gli strumenti elettromedicali e il sistema di software gestionale LAS (Laboratory Automation System) avvenga con tempi di risposta compatibili con le specifiche degli apparati elettromedicali e pertanto indipendenti dai tempi di latenza della rete di comunicazione.
Inoltre, la soluzione assicura la copia dei dati generati dalle strumentazioni elettromedicali.
In situazioni di emergenza dovute al mancato raggiungimento dell'infrastruttura LIS in Cloud, e nelle more che venga attuato il piano di DR, si farà ricorso al solo LAS che consentirà di consultare, in forma non organizzata, i risultati delle analisi appena eseguite. Infatti, i dati delle lavorazioni strumentali possono essere accessibili tramite la piattaforma LAS e stampabili grazie agli strumenti browser installati sulle postazioni lavorative.

Il dettaglio dei server previsti che costituiscono i tre cluster è il seguente:

- N. 6 PowerEdge R640 Server ciascuno con le seguenti caratteristiche:
  Dell PowerEdge R640: 1 x CPU Intel® Xeon® Silver 4110; 64 GB RAM; 2 x HDD 1 TB; 2 Year 2Yr ProSupport and SO VMWare ESXI

Sul virtualizzatore VMWare ESXI installato sui server, saranno create 2 Virtual Machine per la gestione delle componenti dell'applicativo PERSEO:

a) VM PERSEO: SO Ubuntu Server LTS, su cui saranno installati il core dell'applicativo PERSEO e il suo database PostgreSQL;

b) VM PERSEO LAS: SO Microsoft Windows Server, su cui saranno installate le componenti PERSEO LAS, Mirth Connect e il database Microsoft SQL Server.

Ogni Nodo sarà ospitato in apposito rack attrezzato e munito di UPS di nuova fornitura.

Sempre per elevare la resilienza della soluzione saranno previsti dei moduli convertitore Ethernet/Seriale RS232 da installare per quelle apparecchiature strumentali che hanno ancora interfaccia RS232 e collegarli in rete. L'attuale situazione degli apparati strumentali, richiede la fornitura di N° 17 adattatori RS232/Ethernet così suddivisi:

Laboratorio MONALDI Strumentazione Elettromedicale	Q.ta	Tipologia di Collegamento
MenariniDirector	2	LAN-Condivsione
SebiaPhoresisCap	1	LAN-Condivisione
SireTest1	1	Seriale Adattatore (RS232/Lan)
IL_ACL_TOP	1	Seriale Adattatore (RS232/Lan)
Liaison	1	Seriale Adattatore (RS232/Lan)
Kryptor	1	Seriale Adattatore (RS232/Lan)
SiemensInpecoServizi	1	LAN-HL7
BIORADVariant	1	Seriale Adattatore (RS232/Lan)
TOAXSUIT	2	LAN-HL7
MenariniZenIt	1	LAN-HL7
RocheCobas8000	1	LAN-HL7HL7
NaviosFC550	1	LAN-HL7
IL_ACL_ACUSTAR	1	Seriale Adattatore (RS232/Lan)
BeckmanAquios	1	LAN-HL7HL7

Laboratorio COTUGNO Strumentazione Elettromedicale	Q.ta	Tipologia di Collegamento
EpicenterMon	2	Seriale Adattatore (RS232/Lan)
BYKLiaisonXL	2	Seriale Adattatore (RS232/Lan)
RocheAmplilink	1	Seriale Adattatore (RS232/Lan)
CopanWASPLab (su perseo)	1	LAN-HL7HL7
BiomerieuxVitek2	1	Seriale Adattatore (RS232/Lan)
Roche 6800	1	LAN-HL7HL7

Laboratorio CTO Strumentazione Elettromedicale	Q.ta	Tipologia di Collegamento
SireTest1	1	Seriale Adattatore (RS232/Lan)
SebiaPhoresisCap	1	LAN-Condivisione
AbbottArchitect	2	Seriale Adattatore (RS232/Lan)
Dasit-DMS	1	LAN-HL7HL7
IL_ACL_TOP	2	Seriale Adattatore (RS232/Lan)
MindrayBC6800	2	LAN-HL7HL7
Abbott Alinity	1	LAN-HL7HL7

Inoltre, viene prevista una dotazione di scorta pari a 17 unità come apparati di backup, già opportunamente configurati, in modo da sostituire in caso di guasto quelli in produzione.

2. RISORSE DESTINATE ALL'ADEGUAMENTO DEL SITO DI DR

Vengono indicate le risorse HW e SW destinate al sito di DR per il corretto allineamento all'infrastruttura Cloud e funzionamento.

2.1. RISORSE FISICHE DESTINATE ALL'ADEGUAMENTO DEL SITO DI DR

Al fine di allineare il sito di DR, in termini di disponibilità di risorse computazionali, occorre procedere essenzialmente ad un adeguamento delle risorse RAM e di Memoria. Nelle tabelle seguenti si riporta la fornitura prevista

Upgrade RAM		
Codice	**Descrizione**	**Q.tà**
Banchi RAM	HP 8GB (1x8GB) Single Rank x4 PC3-12800R DDR3-1600) Registered CAS-11 Memory Kit	88

Upgrade Dischi 3PAR		
Codice	**Descrizione**	**Q.tà**
BC774AAE	HPE 3PAR 7400 Operating System Software Suite Drive E- LTU	8
E7X49A	HPE M6710 1.2TB 6G SAS 10K 2.5in HDD	8
	HPE Foundation Care NBD SVC – 01.01.2020 – 30.09.2021	1

2.2. SUPPORTO LICENZE VMWARE

La piattaforma di virtualizzazione a servizio dell'Azienda Ospedaliera dei Colli è VMWare. Nell'ambito del progetto è previsto il rinnovo del supporto delle licenze VMWare dal 31/3/2018 fino al 16 settembre 2021 per 22 CPU(s).

Di seguito i codici di licenza attivati per l'Azienda dei Colli.

- MM0AJ-A611J-L8045-081A2-CMTNM 2 CPU(s)
- MJ4C3-A6311-Q8945-081K6-C5LNM 2 CPU(s)
- MJ433-A6343-L8945-0T820-2WVQM 2 CPU(s)
- MJ42L-F63EJ-L804D-0T026-C01QM 2 CPU(s)
- J0421-26KEQ-P804M-0Z122-0XVN0 14 CPU(s)

3. LICENZE COBOL

Nell'ambito della soluzione, è prevista la fornitura delle seguenti licenze software Micro Focus:

- Acucobol GT Runtime
- Acu4GL Oracle

Le licenze sono fornite, con servizio di manutenzione per 24 mesi dalla consegna, per Ambiente di Produzione Primario - 4 core – S.O. LINUX 64 bit, come di seguito dettagliato:

PRODOTTO	U.M.	Q.TÀ
Micro Focus Acucobol GT Runtime (PROD)	core	4
Micro Focus Acucobol GT Runtime (PROD2)	core	4
Micro Focus Acu4GL Oracle (PROD)	core	4
Micro Focus Acu4GL Oracle (PROD 2)	core	4

Le licenze Micro Focus saranno installate ed utilizzate per l'Azienda Ospedaliera dei Colli di Napoli, al fine di eseguire l'applicazione PERSWEB di Engineering. Le licenze saranno installate su una partizione virtuale dedicata in Architettura Cloud di TIM ed a uso esclusivo dell'AORN dei Colli.

4. SOLUZIONE DI SICUREZZA

La soluzione di sicurezza da implementare dovrà essere articolata in diverse componenti.

In particolare, visto la natura delle informazioni presenti sono da prevedere i seguenti servizi/prodotti:

- Web Application Firewall in cloud
- Antivirus con le seguenti feature:
  - Antimalware
  - IPS/IDS
  - Firewall
- Servizio di security monitoring
- Servizio di Vulnerability Assement
- Servizio di Penetration Test infrastrutturale

Di seguito vengono fornite le descrizione dei sopra elencati servizi/prodotti:

4.1. WAF

Host Protection Ready è una delle soluzioni in cloud, in grado di offrire una protezione state of the art per le applicazioni web, con tutti i vantaggi di una soluzione cloud e senza alcun impatto sul codice applicativo.
La soluzione consente di proteggere i siti web e le applicazioni online contro le maggiori minacce informatiche presenti oggi sul web, tra cui:

- SQL injection: è una tecnica di «iniezione di codice» che sfrutta vulnerabilità di sicurezza del database di un'applicazione. Gli aggressori possono sfruttare queste vulnerabilità per eseguire comandi SQL sul database e rubare, corrompere o cancellarne i dati.
- Cross-Site Scripting (XSS): è un attacco che sfruttando le vulnerabilità presenti consente l'inserimento di codice malevole nella applicazione WEB. L'esecuzione di tale codice in maniera incosapevole sulla postazione client/browser ha come obiettivo il furto di dati e/o l'installazione di software dannoso sul computer (postazione di lavoro) dell'utente.
- Illegal Resource Access: è un attacco portato ad una applicazione web allo scopo di ottenere l'accesso alle risorse amministrative del server web e alle pagine/contenuti sensibili del sito web dell'A.O.
- Remote file inclusion: consente a un utente malintenzionato di inserire un file remoto (di solito uno script) sul server web . Gli aggressori utilizzano questo tipo di attacchi per sottrarre informazioni, per mandare in crash il sito web, e per eseguire attacchi di tipo XSS etc.
- Comment Spam: commenti o promozioni commerciali automaticamente postati verso blog, wiki, guestbook, o altre piattaforme di discussione on-line accessibili al pubblico. Qualsiasi applicazione web che accetta e visualizza i collegamenti ipertestuali presentati dai visitatori può essere un obiettivo.
- Suspected Bots (CAPTCHA): in condizioni di richieste anomale il sistema pone una domanda di verifica per confutare che la richiesta non provenga da uno spider o robot o sw di crawling che sta cercando di enumerare o peggio copiare tutte le pagine del sito protetto. E' un primo strumento di difesa contro il phishing perché gli attaccanti non riuscendo a clonare il sito avranno molte più difficoltà nell'organizzazione dell'attività fraudolenta.
- Backdoor Protect: Permette di isolare e disattivare backdoor dannosi eventualmente presenti sul sito dell'A.O..
- Protezione DDoS Applicativo: Gli attacchi DDoS a livello applicativo non sono strettamente legati a tentativi di consumare brutalmente le risorse trasmissive e/o IT dell'A.O., ma colpiscono i singoli servizi applicativi sfruttando vulnerabilità non direttamente causate da errori di implementazione del codice, ma dal modo in cui tali servizi si comportano nativamente.

4.2. ANTIVIRUS

Le aziende riservano oggi uno sguardo critico alla sicurezza degli endpoint di cui dispongono, consapevoli che i soli approcci antivirus tradizionali basati sulle definizioni offrono una debole difesa contro le minacce moderne e gli attacchi mirati.

Per difendersi dalle minacce di oggi, è essenziale implementare una protezione avanzata per endpoint che garantisca la copertura dell'intero ciclo di vita della sicurezza per prevenire, rilevare, analizzare e rispondere alle minacce. Un approccio integrato su tutto il ciclo di vita significa meno console e fornitori, meno spese e una risposta molto più rapida alle minacce. E per proteggerti da un panorama delle minacce in rapida evoluzione, ti serve una piattaforma flessibile di sicurezza degli endpoint che possa adattarsi alle tue esigenze in mutamento con un'architettura ottimizzata per le prestazioni di rete e degli endpoint.

Trend Micro Deep Security assicura una tecnologia completa di sicurezza degli endpoint per il presente e per il futuro, con una protezione per il mondo reale contro le più recenti minacce avanzate. Puoi contare su una moderna protezione per endpoint per antimalware, varianti di packer, controllo di dispositivi, traffico command and control (C&C), exploit del browser, monitoraggio del comportamento, minacce Web, controllo basato sul censo e molto altro ancora. Questa protezione ad ampio spettro viene distribuita tramite un'architettura che utilizza risorse per endpoint in modo più efficace e che, in definitiva, offre prestazioni migliori della concorrenza per utilizzo di CPU e rete.

- **Antimalware**

Deep security, protegge contro virus, cavalli di Troia, worm, spyware, ransomware e nuove varianti nel momento in cui emergono.

- Riduce l'oneroso problema della gestione dei file di pattern e limita l'impatto sulle prestazioni.
- Rileva e rimuove i rootkit e il ransomware attivi e nascosti.
- Protegge le caselle postali negli endpoint effettuando la scansione dei messaggi e-mail POP3 e delle cartelle di Outlook alla ricerca di minacce.
- Identifica e blocca i botnet e le comunicazioni Command and Control (CC) degli attacchi mirati servendosi di informazioni sulle minacce mondiali e locali (sia in entrata che in uscita).
- Protegge gli utenti e i sistemi endpoint contro l'accesso ai contenuti Web dannosi senza affidarsi agli aggiornamenti per garantire la protezione di tipo zero day (protezione contro gli exploit dei browser).
- Rileva in modo proattivo le varianti malware e riduce così il numero di definizioni richieste tramite la protezione anti variante/packer.
- Monitora la presenza di attività di crittografia dei file sospette all'endpoint e termina le attività dannose, per una prevenzione ransomware più ampia.
- Identifica e blocca i botnet e le comunicazioni Command and Control (C&C) degli attacchi mirati servendosi di informazioni unificate sulle minacce fornite dal database globale di reputazione dei domini di Trend Micro.

- **Firewall**

Deep Security Firewall è un firewall estremamente flessibile che è possibile configurare in modo restrittivo o permissivo. Come i moduli di prevenzione delle intrusioni e reputazione Web, il modulo Firewall può anche essere eseguito in due modalità: inline o tap.

- **IPS/IDS**

Il modulo IPS/IDS protegge i computer dagli attacchi da attacchi noti e zero- vulnerabilità, dagli attacchi SQL injection, dagli attacchi cross-site scripting e da altre vulnerabilità delle applicazioni Web. Protegge le vulnerabilità fino a quando le correzioni del codice possono essere completate. Identifica il software dannoso che accede alla rete e aumenta la visibilità o il controllo sulle applicazioni che accedono alla rete.

- **Visibilità e controllo centralizzati**

La gestione centralizzata assicura una visibilità elevata e un controllo maggiore.

- Gestisce per utente su tutti i vettori delle minacce per una visibilità completa della sicurezza dell'ambiente.
- Centralizza la gestione in un'unica console Web.

Il servizio è previsto per le seguenti piattaforme:

DC ACILIA

- 18 macchine virtuali RedHat
- 2 macchine virtuali windows
- 23 Linux
- 2 macchine fisiche per DB con Red Hat

DC POMEZIA

- 18 macchine virtuali RedHat
- 2 macchine virtuali windows
- 23 Linux
- 2 macchine fisiche per DB con Red Hat.

Il servizio di gestione è previsto in orario base e precisamente LU-VE 08:00-18.30 festivi esclusi.

4.3. SECURITY MONITORING

Le soluzioni di Security Information and Event Management (SIEM) sono una combinazione delle due categorie precedentemente distinte di SIM (Security Information Management) e SEM (Security Event Management). La tecnologia SIEM fornisce funzioni di analisi real-time degli alert di sicurezza generati da applicazioni, sistemi ed apparati di network. Le soluzioni SIEM sono usate anche per attività per collezionare i log e generare report per finalità legate alla Compliance.

Caratteristiche essenziali del servizio:

- Data aggregation. Aggregazione dei log raccolti da fonti eterogenee, includendo apparati/sistemi/applicazioni di network, sicurezza, server database, applicazioni e fornire la possibilità di consolidare i dati monitorati per evitare la perdita di eventi cruciali
- Correlazione. Ricerca di attributi comuni a più eventi per connetterli in insiemi significativi. La tecnologia fornisce l'abilità di eseguire una serie di tipologie di correlazioni per integrare fonti eterogenee per trasformare i dati in informazioni utili
- Alerting. Analisi automatizzata di eventi correlati con possibilità di generare alert e notifica delle segnalazioni.

Il SIEM è costituito quindi dall'insieme di attività orientato ad assicurare il mantenimento nel tempo del livello di rischio prefissato, attraverso il monitoraggio costante e l'analisi degli eventi di sicurezza raccolti dall'infrastruttura. Gli eventi di sicurezza rilevati dagli apparati, richiedono infatti una valutazione dell'impatto potenziale sui servizi di business che deve essere necessariamente contestualizzato sul sistema informativo dell'A.O..

Tale valutazione determina il livello di trattamento dell'evento che può arrivare, in alcuni casi, all'apertura di un incidente informatico. Per supportare questo processo complesso e garantirne la massima efficacia, gli specialisti di sicurezza si avvalgono di una piattaforma su cui vengono definite specifiche regole di correlazione degli eventi.

A fronte della rilevazione di evento viene prodotto un SIR (Security Incident Report) dal SOC, il SIR contiene le informazioni necessarie a:

- Classificare l'incidente e riportare le azioni necessarie al contenimento/ripristino/risoluzione della problematica verificatasi;
- supportare le eventuali richieste di intervento.

Di seguito si riporta l'elenco delle informazioni contenute nel SIR:

- categoria di incidente;
- data (AA/MM/GG/HH/MM/SS) del verificarsi dell'incidente come da rilevazione degli strumenti di monitoraggio;
- criticità (molto bassa, bassa, media, alta, critica) dell'incidente;
- descrizione dell'incidente e dei servizi e/o degli apparati coinvolti;

Soluzione

Il servizio è previsto in orario h.24. L'analisi sarà circoscritta per il modulo IPS di deep security presente sui server. In particolare i log saranno inviati al SIEM attraverso la management presente in datacenter.

4.4. VULNERABILITY ASSESSMENT

La gestione della sicurezza informatica per una Azienda si compone di una serie di processi specializzati che affrontano ambiti specifici come la protezione perimetrale, la protezione dai virus e dallo spam, la protezione dai tentativi di intrusione, la protezione delle informazioni di proprietà della Azienda.
L'efficacia delle misure di sicurezza applicate, deve essere continuamente verificata per individuare nuove minacce o mancate conformità dovute sia a nuove esigenze di business, sia ad evoluzioni tecnologiche, sia alle evoluzioni degli strumenti a disposizione di utenti malintenzionati.
Uno dei processi fondamentali che una Azienda deve implementare per la verifica continua dell'efficacia delle misure di sicurezza tecnologiche applicate è quello che permette di gestire le vulnerabilità che ogni sistema informatico avrà nel corso della propria "vita" operativa.
Ogni software presenta delle vulnerabilità:

- alcune sono pubblicamente note così come gli strumenti che ne permettono lo sfruttamento ed i rimedi che le risolvono;
- altre sono pubblicamente note, ma gli strumenti che permettono di sfruttarle ed i rimedi non sono disponibili;
- alcune sono note a pochi e potrebbero essere sfruttate da malintenzionati per l'esecuzione di attacchi informatici a sorpresa, che colgono del tutto impreparati i responsabili di Sicurezza;
- altre infine devono ancora essere scoperte.

Il processo che permette di conoscere le vulnerabilità note presenti sui sistemi, di gestire la continua evoluzione delle vulnerabilità, di valutare gli impatti potenziali di ognuna all'interno di una specifica realtà e di individuare le contromisure necessarie ad eliminarle è comunemente indicato come Vulnerability Assessment.

Tale tipologia di attività rientra, inoltre, tra i requisiti minimi di compliance ai principali standard di sicurezza internazionali nonché alle direttive normative in materia di protezione dei dati personali e sensibili/sanitari.

Soluzione

Per l'Ospedale dei Colli sono stati previste scansioni per 80 indirizzi IP due volte l'anno.

4.5. PENETRATION TEST

Siccome i sistemi target (precisamente per 3 ambienti che saranno esposti su internet) si richiede un servizio di penetration test che vada a identificare le minacce e rendere il tunning del WAF più efficace. In particolare i servizi individuati sono:

1. Penetration Test infrastrutturale
2. PenetrationTest Applicativo

Soluzione

Per l'Ospedale dei COLLI sono previsti:

- Penetration Test infrastrutturale 4 giorni da remoto
- Penetration Test Applicativo 8 giorni da remoto

5. SOLUZIONE DI CONNETTIVITÀ

La soluzione di connettività fa riferimento ai collegamenti in dark fiber ed agli apparati di rete per l'accesso al Cloud TIM, da fornire, installare e configurare presso i Data Center di TIM ed il Centro Stella dell'A.O.

La soluzione da fornire si articola in diverse componenti che di seguito sono illustrate:

a) Rete VDCN: tale rete è una rete intra-CED, che collega esclusivamente i CED di TIM; saranno previsti due collegamenti ad 1 GB per collegare rispettivamente i due data center di Acilia e Pomezia con il DC di Napoli. Si è scelto di predisporre due collegamenti per garantire l'alta affidabilità.

b) Collegamenti Dark Fiber-DF (Fibra ottica Spenta): Tra la sede del Monaldi ed il punto d'ingresso alla rete VDCN di TIM, collocato presso il Centro Direzionale di Napoli, saranno attivati 2 collegamenti DF con istradamento diversificato e ultravailability di apparati: velocità prevista 1 GB x 2, configurati in LAG (Link Aggregation Group);

c) Collegamenti fra la sede del Monaldi ed gli altri Presidi Ospedalieri: Fra il Monaldi ed il CTO, e fra il Monaldi ed il Cotugno verranno attivati dei collegamento DF, sempre con instradamento diversificato con velocità prevista 10 GB x 2 in LAG (Link Aggregation Group)

d) Diversificazione del percorso: per i punti (b) e (c), come 2°Via di accesso al Monaldi

e) Alimentazione di Rete Privilegiata (No Break): gli apparati di rete locale (switch) saranno installati presso i tre ced dei tre presidi, inoltre tali apparati dovranno essere collegati alla rete elettrica privilegiata (No Break).

E' prevista la fornitura degli apparati di terminazione (intesi come apparati di attestazione delle FO ai quali dovranno essere attestati gli apparati di rete), la manutenzione e la gestione guasti.
Gli swtich da fornire installati e configurati sono:

Marca	Modello	Descrizione	Q.tà
Switch - HUAWEI	RL6L1_ S5720-28X-SI-24S-AC-C	Switch 24 porte Gig SFP,8 of which are dual-purpose 10/100/1000 or SFP,4 10 Gig SFP+,AC 10/220V,front access)	8

I livelli di servizio relativi alla sola infrastruttura in dark fiber, e relativamente al singolo collegamento, dovranno essere:

- tempo max di ripristino 12h nell'80% dei casi
- tempo max di ripristino 14h nel 100% dei casi.

6. APPLICAZIONE PERSEO DI DEDALUS PER LABORATORI

Dovrà essere fornita la soluzione di Dedalus che aggiorna il software LIS in esercizio destinato ai laboratori sempre di Dedalus.

La SOLUZIONE PERSEO è una piattaforma "middleware" per il governo della strumentazione medicale di laboratorio che completa le funzioni del LIS e con il quale è strettamente integrata, ponendosi come sistema di connessione tra l'Automazione di Laboratorio e il Laboratory Information System (LIS).

Permette di gestire centralmente tutta la strumentazione preanalitica, analitica, postanalitica e POCT agevolando il controllo totale dei processi e assicurando la massima aderenza alle esigenze di connettività, anche multi-LIS, dei moderni laboratori analisi. La soluzione fornisce una visione completa dell'automazione di laboratorio includendo tutte le piattaforme all'interno della struttura, indipendentemente dalla loro localizzazione. L'interfaccia web permette la gestione centralizzata di dati numerici, grafici, anomalie/flag strumentali", con "La soluzione è strutturata in due componenti applicative integrate tra loro. Il core del prodotto, denominato PERSEO, su Sistema Operativo Ubuntu Server e database PostgreSQL, fornisce una visione completa dell'automazione di laboratorio includendo tutte le piattaforme all'interno della struttura, indipendentemente dalla loro localizzazione, tramite interfaccia web. Il core del prodotto si integra in tempo reale con la seconda componente applicativa, chiamata PERSEO LAS, su Sistema Operativo Microsoft Windows Server e database Microsoft SQL Server, che permette la gestione di tutti i dati numerici e grafici inviati dalle strumentazioni, la produzione e la stampa dei referti.

PERSEO fornisce un completo supporto per le attività di automazione preanalitica, funzionalità dedicate alla fase postanalitica rendono PERSEO una soluzione middleware completa.

7. PATCHING SW E MANUTENZIONE HW

È richiesta la fornitura di patching applicativo e manutenzione hardware come di seguito riportato

7.1. PATCHING SOFTWARE APPLICATIVO

Il servizio patching si realizza attraverso modifiche e miglioramenti tecnici del software applicativo. Il patching dovrà prevedere:

- Patching Correttivo,
- Patching Perfettivo,
- Patching Adattativo,
- Patching Normativo.

L'attività di patching, dovrà avere durata sino al 30/06/2021, è rivolta alle applicazioni oggetto del progetto dei fabbisogni Consip Lotto 1 che vengono di seguito elencate:

- AREAS X-MPI - Anagrafe Centrale Unica
- AREAS Anatomia Patologica
- AREAS Trasfusionale ELIOT
- AREAS Human Resources:
  - Gestione Giuridico Matricolare e Dotazione Organica e dati giuridici da fascicoli dei Dipendenti
  - Economica
  - Gestione Presenze
  - Portale del dipendente
- AREAS Amministrazione e Controllo
- AREAS SIOPE+
- AREAS Direzionale - Data Warehouse e SPAGOBI4AREAS Business Intelligence
- Protocollo informatico

- Software di Document Management System del Sistema di Protocollo Informatico
- Gestione Fascicolo di Liquidazione
- Moduli per la gestione di Delibere, Determine e DLgs33/13 Trasparenza
- AREAS CUP Aziendale
- AREAS DT – Movimentazione Ospedaliera (ADT)
- AREAS PS – Pronto Soccorso
- AREAS Rilevazione Spese Sanitarie
- AREAS PAGO PA + EngPAY Servizio in Cloud
- Moduli Integrazione con SIAC (XMPI, CUP, Paghe, Data Warehouse, Fascicolo di Liquidazione)
- Privacy Manager
- ASAP_sio – Cartella Clinica Generalista, Cartella Clinica Specialistica, Gestione Reparto, Ciclo del Farmaco
- ASAP_sio – Preospedalizzazione, Blocco Operatorio
- ASAP_sio – Gestione Ambulatorio, Day Service
- ASAP_rad – Radiodiagnostica (RIS-PACS)
- Intramoenia allargata
- Intramoenia per attività medico-chirurgiche
- Portale referti
- Modulo di Integrazione del software LIS del SIO con il sistema PARMA GT
- Modulo di Integrazione "Intramoenia allargata" con SIAC
- Piattaforma CALEIDO (LIS)

7.1.1. PATCHING CORRETTIVO

Il servizio di patching correttivo ha l'obiettivo di garantire il mantenimento della operatività e delle funzionalità del software applicativo e si attua attraverso la rimozione degli eventuali malfunzionamenti che possono emergere nel corso dell'esercizio delle soluzioni applicative.

Gli interventi di patching correttivo hanno quindi l'obiettivo di restituire l'applicazione in condizioni operative di perfetto funzionamento. Gli interventi di patching correttivo non includono modifiche di tipo funzionale rispetto a quanto definito nelle specifiche di progetto.

Nel servizio di patching correttivo si intendono comprese quindi tutte le attività connesse con il processo di individuazione dell'errore e della causa che l'ha generato (problem determination) ed i conseguenti interventi finalizzati alla rimozione dell'anomalia ed al ripristino del corretto funzionamento del software applicativo.

Per il servizio di patching correttivo del software applicativo, vengono definiti i seguenti livelli di criticità usati per classificare gli impatti del problema sulle funzionalità del sistema:

- Bloccante: Impatto critico. Il personale dell'Ente perde completamente il servizio ed il lavoro non può ragionevolmente continuare oppure un'essenziale parte del sistema è fuori uso.
- Grave: Impatto medio. Il problema impatta le funzionalità del servizio in termini di continuità, efficacia, sicurezza o qualità, ma il servizio può essere usato.
- Lieve: Impatto minimo. Il personale dell'Ente può aggirare il problema ed utilizzare il servizio con solo un minimo di disagio. Il problema può essere considerato insignificante e non ha alcun effetto importante sull'utilizzabilità del servizio.

In fase di delivery del progetto verranno comunicati gli sla raggruppati per le aree applicative e per i singoli livelli di criticità.

7.1.2. PATCHING PERFETTIVO

Il servizio di patching perfettivo ha lo scopo di assicurare il costante aggiornamento del software applicativo rispetto alle nuove major release e release intermedie (patch/add) del medesimo, che includono evoluzioni delle funzionalità già esistenti piuttosto che aggiunta di nuove funzionalità non richieste direttamente dal Committente ma realizzate in base alla legge quadro nazionale e comunque implementate a discrezione del Fornitore in quanto previste dai propri piani di rilascio.

Il servizio in oggetto include altresì gli interventi di aggiornamento del software applicativo rispetto ad esigenze di miglioramento di prestazioni, robustezza e sicurezza delle applicazioni, che ne lascino tuttavia inalterate le funzionalità.

7.1.3. PATCHING ADATTATIVO

Il servizio di patching adattativo ha lo scopo di assicurare il costante aggiornamento del software applicativo rispetto alla modifica delle versioni dei sistemi software di base della componente server e client (sistemi operativi, data base management system, application server) che costituiscono l'attuale ambiente di installazione delle applicazioni dell'A.O..

Il servizio non prevede l'adeguamento del software applicativo affinché possa essere installato\utilizzato su sistemi software di base della componente server\client che siano differenti rispetto a quelli previsti dalla fornitura originaria dell'A.O., ovvero indicati come requisiti minimi di compatibilità delle applicazioni dell'A.O..

Il servizio mira invece a garantire il funzionamento del software applicativo sulle nuove versioni del software di base della componente server e client rispetto i quali il Fornitore ritiene utile e profittevole effettuare tali adeguamenti.

Il servizio è garantito esclusivamente per le applicazioni web-based.

Il Fornitore inoltre non garantisce il funzionamento delle soluzioni applicative e l'assistenza su quelle versioni del software di base che non sono più mantenute dal relativo Vendor.

Per il servizio di patching adattativo del software applicativo, vengono definiti i seguenti livelli di criticità usati per classificare gli impatti del problema sulle funzionalità del sistema:

- Urgente: Intervento critico che richiede un tempestivo intervento di risoluzione. Tale evento impedisce il funzionamento del servizio.
- Non urgente: Intervento ordinario su componenti/anomalie che non comportano disservizi al servizio. Questo livello di criticità è anche applicato a domande, commenti e richieste di migliorie.

In fase di delivery del progetto verranno comunicati gli sla raggruppati per le aree applicative e per i singoli livelli di criticità

7.1.4. PATCHING NORMATIVO

Il servizio di patching per adeguamenti normativi ha lo scopo di assicurare il costante aggiornamento delle funzionalità del software applicativo rispetto a variazioni normative rilevabili da documenti ufficiali di livello nazionale che comportino interventi di modifica del software medesimo.

Il Fornitore si impegna, nel caso di mutamento di disposizioni di legge, nazionali o regionali che risultano essere vincolanti per l'A.O. e la cui entrata in vigore ricada nel periodo contrattuale, ad apportare le modifiche alle funzionalità già disponibili conseguentemente necessarie. Le modifiche verranno rilasciate dal Fornitore nei tempi utili, sempre che l'A.O. abbia segnalato le nuove eventuali esigenze con sufficiente anticipo.

Per modifiche alle funzionalità si intendono sviluppi di software applicativo finalizzati ad adattare il software in uso alle suddette disposizioni che non prevedano l'inserimento di nuove funzionalità o la riprogettazione sostanziale di funzionalità già presenti. (es: conversione lira->euro)

Nello specifico il servizio di patching per adeguamenti normativi si applica agli interventi che comportano la modifica di elementi funzionali di un modulo applicativo affinché questo risulti aderente alla normativa vigente.

Il servizio di patching normativo, quindi, è caratterizzato da:

- esigenze ed obiettivi già previsti in sede di pianificazione delpresente servizio;
- eventi non prevedibili che danno luogo ad "attività non pianificabili".

Si indicano come "non pianificabili" quelle attività il cui svolgimento dovesse rendersi necessario ed urgente, a seguito di eventi non prevedibili in sede di pianificazione del servizio, quali sono, ad esempio, tutte quelle attività finalizzate a conformare il software applicativo a modifiche e/o integrazioni normative.

Nel caso in cui l'adeguamento normativo del software comporti sostanziali modifiche alla struttura tabellare o la progettazione di nuove funzionalità, il Fornitore si riserva di effettuare una specifica valutazione dell'impegno richiesto ed una relativa proposta economica e di presentarla al Committente. A fronte dell'approvazione della stessa, si procederà allo sviluppo, ai test ed al rilascio della nuova soluzione applicativa.

7.2. MANUTENZIONE INFRASTRUTTURA ESISTENTE

È richiesta la manutenzione delle seguenti componenti già in uso presso l'AORN dei Colli.

La manutenzione dovrà avere durata sino al 30/09/2021.

Dall'attività di manutenzione sono escluse tutte le stazioni video di refertazione (Barco-Apple) presenti all'interno dell'AORN dei Colli.

7.2.1. MANUTENZIONE DELL'ATTUALE HD E SW DEL SIO DELL'A.O. DEI COLLI

Infrastuttura tecnologica presso il CED Monaldi

	Unità Rack	
Part Number	**Descrizione**	**Q.tà**
BW904A	HP 642 1075mm Shock Intelligent Rack	1
H5M57A	HP 3.6kVA 200-240V 20out WW bPDU	2
BW946A	HP 42U Location Discovery Kit	1
BW932A	HP 600mm Rack Stabilizer Kit	1
BW930A	HP Air Flow Optimization Kit	1
BW906A	HP 42U 1075mm Side Panel Kit	1
AF616A	HP 0x2x8 KVM Svr Cnsl G2 SW	1
336047-B21	HP CAT5 KVM USB 1 Pack Interface Adapter	8
263474-B22	HP KVM IP CAT5 Qty-8 6ft/2m Cable	1

252663-B31	HP 40A HV Core Only Corded PDU	2
AF461A	HP R5KVA UPS 3U IEC309-32A HV Intl Kit	2
612371-061	HP KVM Console Itl Kit	1
AF576A	HP 3.6m 16A C19 EU Pwr Cord	1
	San Switch	
Part Number	**Descrizione**	**Q.tà**
AM867B	HP 8/8 (8)-ports Enabled SAN Switch	2
QK734A	HP Premier Flex LC/LC OM4 2f 5m Cbl	16
AJ716B	HP 8Gb Short Wave B-Series SFP+ 1 Pack	16
	Backup Server	
Part Number	**Descrizione**	**Q.tà**
652063-B21	HP ML350pR08 SFF CTO Server	1
660598-L21	HP ML350p Gen8 E5-2620 FIO Kit	1
647893-B21	HP 4GB 1Rx4 PC3L-10600R-9 Kit	1
652745-B21	HP 500GB 6G SAS 7.2K 2.5in SC MDL HDD	4
631679-B21	HP 1GB FBWC for P-Series Smart Array	1
503296-B21	HP 460W CS Gold Ht Plg Pwr Supply Kit	2
701593-A21	MS WS12 Std FIO E/F/I/G/S SW	1
AK344A	HP 81Q PCI-e FC HBA	1
J9583A	HP X410 1U Univ 4-post Rack Mnt Kit	1
	San StorServ 7400	
Part Number	**Descrizione**	**Q.tà**
QR483A	HP 3PAR StoreServ 7400 2-N Storage Base	1
QR492A	HP M6710 300GB 6G SAS 15K 2.5in HDD	24
BC773A	HP 3PAR 7400 OS Suite Base LTU	1
BC774A	HP 3PAR 7400 OS Suite Drive LTU	24
	Jbod aggiuntivo 24 x 3,5" e HDD	
Part Number	**Descrizione**	**Q.tà**
QR491A	HP M6720 3.5in 4U SAS Drive Enclosure	1
QR499A	HP M6720 2TB 6G SAS 7.2K 3.5in NL HDD	14
BC774A	HP 3PAR 7400 OS Suite Drive LTU	14
	Libreria Backup	
Part Number	**Descrizione**	**Q.tà**
C0H22A	HP MSL2024 1 LTO-6 Ult 6250 FC Library	1
C7976A	HP LTO-6 Ultrium 6.25TB MP RW Data Tape	24
	Enclosure Blade	
Part Number	**Descrizione**	**Q.tà**
507019-B21	HP BLc7000 CTO 3 IN LCD ROHS Encl	1
571956-B21	HP BLc VC FlexFabric 10Gb/24-port Opt	2
453154-B21	HP BLc VC 1Gb RJ-45 SFP Opt Kit	2
499243-B21	HP 2400W Gold Ht Plg Pwr Supply Kit	6
413379-B21	HP BLc7000 1 PH FIO Power Module Opt	1
517520-B21	HP BLc 6X Active Cool 200 FIO Fan Opt	1
433718-B21	HP BLc7000 10K Rack Ship Brkt Opt Kit	1

	Database Server Blade	
Part Number	**Descrizione**	**Q.tà**
641016-B21	HP BL460c Gen8 10Gb FLB CTO Blade	2
662065-L21	HP BL460c Gen8 E5-2660 FIO Kit	2
662065-B21	HP BL460c Gen8 E5-2660 Kit	2
669324-B21	HP 8GB 2Rx8 PC3-12800E-11 Kit	16
652605-B21	HP 146GB 6G SAS 15K 2.5in SC HDD	4
684212-B21	HP FlexFabric 10Gb 2P 554FLB FIO Adptr	2
	VMware Server Blade	
Part Number	**Descrizione**	**Q.tà**
641016-B21	HP BL460c Gen8 10Gb FLB CTO Blade	11
662068-L21	HP BL460c Gen8 E5-2630 FIO Kit	11
662068-B21	HP BL460c Gen8 E5-2630 Kit	11
669324-B21	HP 8GB 2Rx8 PC3-12800E-11 Kit	88
652605-B21	HP 146GB 6G SAS 15K 2.5in SC HDD	22
684212-B21	HP FlexFabric 10Gb 2P 554FLB FIO Adptr	11
	Management Server Blade	
Part Number	**Descrizione**	**Q.tà**
641016-B21	HP BL460c Gen8 10Gb FLB CTO Blade	1
662068-L21	HP BL460c Gen8 E5-2630 FIO Kit	1
669324-B21	HP 8GB 2Rx8 PC3-12800E-11 Kit	2
652605-B21	HP 146GB 6G SAS 15K 2.5in SC HDD	2
684212-B21	HP FlexFabric 10Gb 2P 554FLB FIO Adptr	1
	netWorking - moduli HP VirtualConnect FlexFabric 10Gb/24 Porte	
Part Number	**Descrizione**	**Q.tà**
J9145A	HP 2910-24G al Switch	2
J9008A	HP 2-port 10GbE SFP+ al Module	2
J9150A	HP X132 10G SFP+ LC SR Transceiver	4
	DataProtector Software	
Part Number	**Descrizione**	**Q.tà**
B6961BAE	HP Data Prot Stater Pack Windows E-LTU	1
B6963AAE	HP DP drive extn WIN/Netware/Linux E-LTU	1
B6965BAE	HP DP On-line Backup for Windows E-LTU	1
B6966AAE	HP DP Manager of Managers Windows E-LTU	1

AZIENDA OSPEDALIERA DEI COLLI

7.2.2. MANUTENZIONE DELLA DOTAZIONE STRUMENTALE DELLA RADIOLOGIA E UPS RADIOLOGIA

Apparati periferici presso Monaldi

	Armadio rack presso la Radiologia Monaldi	
Part Number	**Descrizione**	**Q.tà**
	Armadio rack	1
210-14399	DELL PowerEdge 180AS a 8 porte analogiche	1
AZ874A	HP TFT7600 KVM Console Itl Kit	1
	Switch Allied Telesyn	1

	Server PACS LTA Radiologia-Medicina Nucleare Monaldi	
Part Number	**Descrizione**	**Q.tà**
661189-B21	HP DL360e Gen8 8SFF CTO Server	2
660650-L21	HP DL360e Gen8 E5-2470 FIO Kit	2
647893-B21	HP 4GB 1Rx4 PC3L-10600R-9 Kit	4
655708-B21	HP 500GB 6G SATA 7.2k 2.5in SC MDL HDD	4
661388-B21	HP DL360eGen8 CPU1 Riser FIO Kit	2
631673-B21	HP Smart Array P421/1GB FBWC Controller	2
631922-B21	HP 512MB 36in FBWC B-Series Smart Array	2
663201-B21	HP 1U SFF BB Gen8 Rail Kit	2
503296-B21	HP 460W CS Gold Ht Plg Pwr Supply Kit	4
AW593B	HP P2000 G3 SAS MSA Dual Cntrl LFF Array	1
QK703A	HP P2000 3TB 3G SATA 7.2K 3.5in MDL HDD	8
407339-B21	HP Ext Mini SAS 2m Cable	4
	UPS da Rack Radiologia Monaldi	
Part Number	**Descrizione**	**Q.tà**
AF461A	HP R5KVA UOS 3U IEC309-32A HV Intl Kit	2

	Server PACS cache Radiologia-Medicina Nucleare Monaldi	
Part Number	**Descrizione**	**Q.tà**
210-39092	PowerEdge R720 4,340.00 SR	1
213-15019	Intel Xeon E5-2640 2.50GHz, 15M Cache, 7.2GT/s QPI, Turbo, 6C, 95W, DDR3-1333MHz	1
330-10238	Risers with up to 6, x8 PCIe Slots + 1, x16 PCIe Slot	1
350-11090	2.5" Chassis with up to 16 Hard Drives	1
370-22140	1333 MHz RDIMMs	1
370-22133	4GB RDIMM, 1333 MHz, Low Volt, Single Rank, x4	4
374-14472	Heat Sink for PowerEdge R720 and R720xd	2
374-14454	DIMM Blanks for Systems with 2 Processors	1
374-14461	Intel Xeon E5-2640 2.50GHz, 15M Cache, 7.2GT/s QPI, Turbo, 6C, 95W, DDR3-1333MHz	1
400-22925	900GB, SAS 6Gbps, 2.5-in, 10K RPM Hard Drive (Hot-plug)	3
405-12070	PERC H710 Integrated RAID Controller, 512MB NV Cache	1
429-14712	16x DVD-ROM unità SATA	1
450-17885	Dual, Hot-plug, Redundant Power Supply (1+1), 750W	1
540-11046	Broadcom 5720 QP 1Gb Network Daughter Card	1
565-10477	8 Pin Phone Connector, Back Cover	1
780-12952	RAID 5 for H710p, H710, H310 Controllers	1
528-10002	iDRAC7 Express	1

	Server per visualizzazione immagini Radiologia-Medicina Nucleare Monaldi (DB_SERVER)	
Part Number	**Descrizione**	**Q.tà**
210-32160	PowerEdge R310 Chassis, Up to 4 Hot Plug HDDs, LCD Diagnostics	1
213-11875	Processore Intel Xeon X3450 (2,66GHz, 4C, cache 8MB, TDP 95W, Turbo, HT), DDR3 1.333MHz	1
370-20358	4GB Memory (1x4GB Dual Rank LV UDIMM) 1333MHz	1
400-21122	500GB SATA 7.2k 3,5" disco rigido hot-plug	2
403-10690	SAS 6iR controller per chassis con disco rigido hot-plug	1
429-15175	16x DVD+/-RW unità SATA con cavo SATA	1
450-12466	2M Rack Power Cord C13/C14 12A	2
450-15103	Redundant Power Supply (2 PSU) 400W	1
565-10294	iDRAC6 Express	1
780-12390	C18 con sostituzione a caldo - R1 per SAS 6iR/PERC H200/H700, esattamente 2 unità hot-plug SAS/SATA/SSD	1
540-10512	Broadcom NetXtreme II 5709 doppia porta 1GbE NIC con offload TOE e iSCSI, PCIe x4	1
565-10240	iDRAC6 Express	1
780-11881	C25 Hot-Swap 8HD - R5 for PERC 6i/H700, Min. 3 Max. 8 Hot Plug Drives	1

	Server PACS Cardiologia Monaldi	
Part Number	**Descrizione**	**Q.tà**
	DELL PowerEdge R620 x8Base	1
213-15015	Intel Xeon E5-2620 (2GHz, 6C, cache 15MB, 7,2GT/s QPI, 95W, Turbo)	1
330-10236	Optional Riser with 1 Additional x8 PCIe Slot for x8, 2 PCIe Chassis with 1 Processor	1
340-27828	PowerEdge R620 Shipping - 4/8 Drive Chassis, EMEA1	1
350-11080	Chassis with up to 4 Hard Drives and 2 PCIe Slots	1
350-10048	No Bezel Option - Rack Chassis	1
370-22145	Performance Optimized	1
370-22140	1333 MHz RDIMMs	1
370-22132	4GB RDIMM, 1333 MHz, Low Volt, Dual Rank, x8	2
374-14451	Heat Sink for PowerEdge R620	1
374-14449	DIMM Blanks for Systems with 1 Processor	1
374-14450	No Additional Processor	1
400-22278	1TB, Near-Line SAS 6Gbps, 2.5-in, 7.2K RPM Hard Drive (Hot-plug)	3
405-12070	PERC H710 Integrated RAID Controller, 512MB NV Cache	1
223-10229	Attivo alimentazione controller BIOS impostazione	1
429-16361	DVD ROM, SATA, Internal	1
450-12466	2M Rack Power Cord C13/C14 12A	2
450-17884	Dual, Hot-plug, Redundant Power Supply (1+1), 495W	1
470-12917	Cable for Mini PERC Cards in Chassis with up to 4 Hard Drives	1
540-11046	Broadcom 5720 QP 1Gb Network Daughter Card	1
565-10477	8 Pin Phone Connector, Back Cover	1

Apparati periferici presso Cotugno

	Armadio rack presso CED 2° piano	
Part Number	**Descrizione**	**Q.tà**
	Armadio rack	1
FOC0904Y253	CISCO CATALYST 2950 SERIES	1

	Server PACS cache Radiologia-Ecointerventistica Cotugno	
Part Number	**Descrizione**	**Q.tà**
210-27063	PowerEdge R710 Rack Chassis for Up to 4x 3.5" Hard Drives	1
213-10168	Intel® Xeon® E5506, 2.13Ghz, 4MB Cache, 4.86 GT/s QPI	1
370-14220	4GB Memory for 1 CPU, DDR3, 1066MHz (2x2GB Dual Ranked UDIMMs)	1
780-11167	C20 - RAID 1/RAID 5 for PERC 6/i Controller, 2 SSD and 3-6 SAS HDDs, Mixed SSD/SAS	1
400-16065	146GB, SAS, 3.5-inch, 15K RPM Hard Drive (Hot Plug)	2
401-11211	1TB, Near Line SAS, 3.5-inch, 7.2K RPM Additional Hard Drive (Hot Plug)	4
330-10106	Riser with 2 PCIe x8 + 2 PCIe x4 Slots	1
429-14712	16x DVD-ROM unità SATA	1
565-10113	iDRAC6 Express	1
	Server PACS LTA Radiologia-Ecointerventistica Cotugno	
Part Number	**Descrizione**	**Q.tà**
210-31979	PowerEdge R510 Rack Chassis for Up to 8x 3.5" Hot Plug HDDs and Intel 55xx/56xx Processors, LCD Diags, Supports Hot Swap PSUs	1
213-11795	Intel Xeon E5503 Processor (2.00GHz, 2C, 4M Cache, 4.80 GT/s QPI, 80W TDP), DDR3-800MHz	1
370-18951	8GB di memoria per 1CPU (2x4GB RDIMM dual rank) 1.333MHz	1
400-20161	1TB Near Line SAS 6Gb/s 7.2k 3,5" disco rigido hot-plug	8
405-11391	PERC H700 controller RAID integrato, cache 512MB, per chassis a 8 dischi rigidi	1
429-14820	16X DVD-ROM Drive SATA (R510/R515)	1
450-14558	Ridondante alimentatore (2 alimentatori) 750W, per chassis a 8 e 12 dischi rigidi hot-plug	1
540-10512	Broadcom NetXtreme II 5709 doppia porta 1GbE NIC con offload TOE e iSCSI, PCIe x4	1
565-10240	iDRAC6 Express	1
780-11881	C25 Hot-Swap 8HD - R5 for PERC 6i/H700, Min. 3 Max. 8 Hot Plug Drives	1
	UPS da Rack Radiologia-Ecointerventistica Cotugno	
Part Number	**Descrizione**	**Q.tà**
DL5000RMI50	APC Smart-UPS 5000VA 230V Rackmount/Tower	1

Apparati periferici presso CTO

	Armadio rack presso locale tecnico 1° piano	
Part Number	**Descrizione**	**Q.tà**
	Armadio rack	1
9Y52LD818	HP Tastiera da rack	1
	Server PACS cache Radiologia CTO	
Part Number	**Descrizione**	**Q.tà**
210-31979	PowerEdge R510 Rack Chassis for Up to 8x 3.5" Hot Plug HDDs and Intel 55xx/56xx Processors, LCD Diags, Supports Hot Swap PSUs	1
213-11795	Intel Xeon E5503 Processor (2.00GHz, 2C, 4M Cache, 4.80 GT/s QPI, 80W TDP), DDR3-800MHz	2
370-18951	8GB di memoria per 1CPU (2x4GB RDIMM dual rank) 1.333MHz	1
400-20161	1TB Near Line SAS 6Gb/s 7.2k 3,5" disco rigido hot-plug	2
405-11391	PERC H700 controller RAID integrato, cache 512MB, per chassis a 8 dischi rigidi	3

405-14920	16X DVD-ROM Drive SATA (R510/R515)	1
450-14558	Ridondante alimentatore (2 alimentatori) 750W, per chassis a 8 e 12 dischi rigidi hot-plug	2
	Server PACS LTA Radiologia CTO	
Part Number	**Descrizione**	**Q.tà**
	PowerEdge R540 Rack Chassis	1
4057039694	Intel® Xeon® Silver 4108 1.8G, 8C/16T, 9.6GT/s 2UPI, 11M Cache, Turbo, HT (85W) DDR4-2400	1
	8GB RDIMM, 2667MT/s, Single Rank	1
	2TB 7.2K RPM NLSAS 12Gbps 512n 2.5in Hot-plug Hard Drive, 3.5in HYB CARR	5
	600GB 10K RPM SAS 12Gbps 512n 2.5in Hot-plug Hard Drive, 3.5in HYB CARR	2
	PERC H330+ RAID Controller, Adapter, Low Profile	1
	Ridondante alimentatore (2 alimentatori) 750W, per chassis a 8 e 12 dischi rigidi hot-plug	1
	UPS da Rack Radiologia CTO	
Part Number	**Descrizione**	**Q.tà**
PS2200RT3-230	UPS EMERSON NETWAORK POWER Liebert PSi XR 2200va 230v Rack/Tower Mountable	1
IS-WEBRT3	Remote Power Management Adapter Liebert LAN	1

7.3. LIVELLI DI SERVIZIO DI MANUTENZIONE APPARATI E CIRCUITI

Di seguito vengono indicati i livelli di servizio di manutenzione da prevedere per gli apparati e per i circuiti:

Dark Fiber

Per tale componente **i livelli di servizio** sono:

- Relativamente alla sola infrastruttura in dark fiber, e relativamente al singolo collegamento, sono i seguenti:
  - copertura de servizio in orario d'ufficio (09:00-17:00 nei giorni feriali)
  - tempo max di ripristino 12h nell'80% dei casi
  - tempo max di ripristino 14h nel 100% dei casi
- Relativamente agli apparati (switch) è NBD (Next Business Day) per singolo apparato

Infrastruttura DB in colocation a Acilia e Pomezia

Per tale componente **i livelli di servizio** sono:

- NBD (Next Business Day)

Infrastruttura server Laboratori c/o Monaldi, CTO, Cotugno

Per tale componente **i livelli di servizio** sono:

- NBD (Next Business Day)

Apparati esistenti all'interno dell'A.O. dei Colli

Per gli apparati esistenti **i livelli di servizio**, per singolo apparato, sono:

- NBD (Next Business Day)

8. FIRMA DIGITALE BASATA SU TOKEN USB

Nell'ambito del progetto è prevista la fornitura del servizio di Firma Digitale basato su token USB. Il servizio dovrà essere erogato da certificatore accreditato e dovrà prevedere la fornitura di 300 kit.

Per quanto riguarda l'attivazione del servizio, occorrerà individuare i titolari. Tale identificazione sarà effettuata da un addetto del certificatore accreditato che identificherà un incaricato dell'A.O., il quale poi identificherà a sua volta tutti gli altri utenti.

L'identificazione dell'incaricato verrà effettuata presso la sede dell'Azienda dei Colli, previo appuntamento con l'addetto del certificatore accreditato che effettuerà il riconoscimento.

Successivamente l'incaricato potrà effettuare in autonomia il riconoscimento dei singoli titolari, il flusso sarà il seguente:

- L'incaricato identifica il titolare e manda i moduli compilati e firmati al gruppo di delivery alla mail indicata dal certificatore accreditato.

Ricevuti i moduli il delivery procede con la creazione dei kit ed effettua la spedizione del token e della busta oscurata a mezzo corriere espresso

9. TEMPI DI CONSEGNA E REALIZZAZIONE DEI SERVIZI

I beni e servizi offerti dovranno essere messi a disposizione dell'Azienda entro 40 giorni lavorativi dall'aggiudicazione della fornitura, per consentire il collaudo e l'attivazione dei servizi.

Sarà a cura dell'aggiudicatario garantire la messa in esercizio dei servizi previsti nel presente avviso, curando in proprio i rapporti con i subfornitori per lo svolgimento delle attività previste, senza quindi vi sia alcun tramite dell'AO, quali autorizzazioni da TIM per l'accesso ai Data center, Sistemi di interfacciamento tra le componenti software offerte ed i sistemi informativi aziendali, etc.).

10. RICONSEGNA

I server, gli switch e quant'altro oggetto di fornitura dovranno essere consegnati alla scadenza contrattuale presso la sede dell'A.O. Ospedali dei Colli o presso altra sede indicata dall'A.O. stessa senza alcun costo aggiuntivo e senza null'altro a pretendere.

11. REQUISITI MINIMI DI PARTECIPAZIONE

Gli operatori economici interessati dovranno dichiarare ai sensi dell'artt. 46 e 47 del D.P.R. n. 445/2000 - consapevoli delle sanzioni penali previste dall'art. 76 del medesimo D.P.R. per le ipotesi di falsità in atti e dichiarazioni mendaci ivi indicate:

- la capacità tecnica allo svolgimento dei servizi di manutenzione correttiva, conservativa e correlati servizi in quanto titolari dei sorgenti del software di cui trattasi o in qualità di fornitori autorizzati dai titolari dei sorgenti a svolgere tali servizi;
- di essere garante nei confronti di questa Azienda per danni provocati imputabili al non effettivo svolgimento dei servizi offerti oltre che al non rispetto dei tempi che saranno eventualmente indicati nella lettera d'invito;
- l'impegno inderogabile a fornire successiva offerta, qualora invitati;
- di essere in possesso, pena esclusione, dei seguenti requisiti:
  a) requisiti di ordine generale, di cui all'art. 80 del D.Lgs 50/2016;
  b) certificazione di sistema di qualità conforme alle norme europee della serie UNI EN ISO 9001: 2015 (EA: 28 - 31 - 34 – 33);
  c) certificazione di sistema di qualità conforme ai requisiti della norma per il Sistema di Gestione Ambientale UNI EN ISO 14001:2015;
  d) certificazione di sistema di qualità conforme ai requisiti della norma per il Sistema di Gestione UNI EN ISO 27001:2013, "Monitoraggio e gestione degli incidenti di sicurezza ICT" (Settore EA:33);
  e) certificazione di sistema di qualità conforme ai requisiti della norma per il Sistema di Gestione UNI EN ISO 27001:2013, "Data Center & Cloud Computing Services in modalità IaaS (Infrastructure as a Service) con l'utilizzo della linea guida ISO/IEC 27018:2014 e con l'utilizzo della linea guida ISO/IEC 27017:2015 per i servizi di self datacenter "vcloud & hypervisor".
  Servizi di ICT Security con l'utilizzo delle linee guida ISO/IEC 27035:2016-1 e ISO/IEC 27035:2016-2. Network Services, Unified Communication & Collaboration Services, Mobile Services; Predisposizione, attivazione ed esercizio di infrastrutture, piattaforme e servizi di Information Communications Technology presso i Data Center e Centri Servizi TIM anche in modalità cloud e virtuale, attraverso: a gestione di facilities e di impianti tecnologici;
  f) certificazione di sistema di qualità conforme ai requisiti della norma per il Sistema di Gestione UNI EN ISO 27001:2017 per la predisposizione, attivazione ed esercizio di infrastrutture, piattaforme e servizi di Information Communications Technology presso i Data Center e Centri Servizi TIM anche in modalità cloud e virtuale, attraverso: la gestione di facilities e di impianti tecnologici; la gestione e assurance di infrastrutture, servizi di rete e firewall; la gestione della sicurezza fisica alle sale sistemi; la predisposizione e configurazione dei siti e sale sistemi; l'attivazione ed esercizio di piattaforme e servizi IT; la gestione di applicazioni a supporto del servizio di Payroll per società del Gruppo TIM (Settore EA: 33);
  g) certificazione di sistema di qualità conforme ai requisiti della norma per il Sistema di Gestione UNI EN ISO 20000-1:2011, "Conformità della sede operativa a Information Technology Service Management System standard";
  h) certificazione di sistema di qualità conforme ai requisiti della norma per il Sistema di Gestione UNI EN ISO 20000-1:2011, "Gestione e monitoraggio degli usi e consumi energetici";
  i) fornitore autorizzato all'accesso ai Data Center TIM per lo svolgimento dei servizi oggetto della fornitura supplementari a quelli previsti nel contratto quadro CONSIP SPC Cloud Lotto 1. Per tale requisito occorre che il fornitore fornisca attestazione/dichiarazione rilasciata da TIM.

Per informazioni tecniche: U.O.C. Sistema Informativo Aziendale (S.I.A.) – Dott. Oreste Califano - (tel. 0817062289 - segreteria tel. 0817062280).