CAV S.p.A.

Concessioni Autostradali Venete

Sede Legale: via Bottenigo, 64 a – 30175 Marghera Venezia
Tel. 041 5497111 – Fax. 041 935181
R.I./C.F./P.IVA 03829590276 – Iscr. R.E.A. VE 0341881
Cap. Sociale € 2.000.000,00

AUTOSTRADE IN CONCESSIONE: Autostrada A4
Autostrada A57 – Tangenziale di Mestre
Raccordo per l'Aeroporto "Marco Polo"

OGGETTO: FORNITURA E MANUTENZIONE DELLA NUOVA STRUTTURA DI NETWORKING A LARGA BANDA DELLA SEDE AZIENDALE

ALLEGATO

D

CAPITOLATO SPECIALE D'APPALTO

- DESCRITTIVO E PRESTAZIONALE -

R.U.P. ing. Sabato Fusco

Progettista: ing. Mario Frara

Redatto da: ing. Mario Frara

EDIZIONE: Anno 2017

Sommario

PREMESSA

Il presente documento costituisce il Capitolato Descrittivo e Prestazionale per la fornitura, la realizzazione, configurazione e manutenzione della rete ad alta velocità per la trasmissione dati (LAN-WAN) ad alte prestazioni di CAV S.p.A. (nel seguito Società). Con questo intervento la Società intende rispondere alle necessità interne di alta velocità dotandosi di un networking con elevate prestazioni in termini di banda di trasmissione, affidabilità, salvaguardia e sicurezza dell'investimento consentendo di supportare, oltre ai dati, applicazioni voce e video, che verranno implementate in un prossimo futuro, integrandole su di un'unica rete IP.

Riassumendo, gli obiettivi principali che si intende perseguire sono cinque:

- aumentare la larghezza di banda a tutta l'infrastruttura di rete, incrementando la velocità sui backbone di Core a 40GBps.
- Incrementare l'availability della rete attraverso un'architettura ridondata, costituita da apparati con elevato MTBF, e con l'adozione di un adeguato piano di manutenzione.
- Implementare un'infrastruttura di rete Wireless, in tutte le sedi della Società, integrandola con la rete Wireless esistente relativa al servizio di telefonia VoIP.
- Implementare un'infrastruttura firewall ridondata con doppi apparati sia nella sede di Mestre sia nella sede di Padova per gestire in alta affidabilità un doppio canale internet.
- Implementare una gestione collaborativa di tutta l'infrastruttura di rete con gestione avanzata dell'autenticazione degli utenti e report settimanali sulle anomalie di funzionamento della rete e dei relativi nodi.

L'investimento connesso alla realizzazione di una nuova infrastruttura di rete costituisce un investimento destinato a condizionare a lungo termine le future scelte nel settore telematico ed informatico della Società.

La Società punta a garantire la massima disponibilità e affidabilità dei servizi che eroga agli utenti interni ed esterni. In particolare, questo progetto è caratterizzato dalla necessaria attenzione richiesta all'Appaltatore sulla fornitura di ciascuno dei servizi richiesti, con massimo focus su entrambi gli aspetti di integrazione e "governo" dell'intera gestione del servizio, allo scopo di ottenere un efficace controllo della qualità raggiunta.

Nel contesto di questo documento, l'indicazione "IT" abbraccia tutte le Infrastrutture e le applicazioni core che l'Appaltatore sosterrà attraverso l'erogazione dei necessari servizi al fine di supportare le "IT Operations" della Società L'obiettivo principale richiesto è di erogare la stabilità dei servizi IT e l'industrializzazione necessaria per consentire il realizzarsi delle aspirazioni di crescita e trasformazione della Società. I fattori abilitanti delle caratteristiche di stabilità ed industrializzazione saranno creati dall'Appaltatore, quando fornirà le adeguate infrastrutture IT, applicazioni, Servizi IT, metodi e strumenti, supportati dalle migliori pratiche e standard internazionali.

La tecnologia di trasporto a cui si fa espressamente riferimento è Ethernet, con tutte le sue evoluzioni. Con riferimento a quanto detto, tra i tanti criteri adottabili, quelli che si ritengono indispensabili sono:

— adozione di tecnologie all'avanguardia e contemporaneamente consolidate e sperimentate;

— semplicità di uso e di gestione;

— affidabilità massima degli apparati;

— aderenza agli standard internazionali;

— robustezza ed espandibilità, oltre alla flessibilità di configurazione del SO degli apparati;

— capacità di supportare tutte le esigenze di comunicazione (dati, fonia, video, audio, etc.);

— assoluta uniformità ed omogeneità degli apparati di networking wired e wireless.

Parte integrante della rete saranno la copertura Wi-Fi e l'implementazione del nuovo firewalling.

La copertura wifi dovrà interessare pressoché tutta l'area della sede di Marghera, sia indoor che outdoor, il casello di Padova Est e gli altri caselli autostradali della Società in itinere tra la barriera di Mestre e di Padova Est e del Passante di Mestre. Lo studio di copertura e la configurazione della rete Wi-Fi dovrà tener conto della futura funzionalità di trasporto VoIP sull'intera rete, dove la parte Wi-Fi merita sicuramente la massima attenzione a riguardo per arginare le

note problematiche di roaming e di handover dovute all'erogazione del servizio in mobility. Per la definizione del posizionamento più opportuno degli Access Point è richiesta un'attività di Site Survey On Site.

Tale servizio, da realizzare indoor ed outdoor con il supporto di idoneo strumento S/W, consentirà di garantire la necessaria copertura radio ed avere una visione d'insieme dell'intera rete Wi-Fi. Agli Art. 5÷8 sono riportati maggiori dettagli.

Gli apparati firewall saranno ridondati nelle 2 sedi e formeranno un unico cluster in grado di garantire la connettività verso il mondo esterno in alta affidabilità.

Verranno distribuite connessioni 10/100/1000 Mb/s Ethernet al desktop a tutte le postazioni esistenti con 20% di possibilità di ampliamento per ogni Rack, con elevate prestazioni in termini di switching e routing, quest'ultimo limitato alle sole macchine di core. La rete sarà in configurazione "Fault Tolerant", come evidenziato in figura 1. La Società è dotata di un'infrastruttura (wired networking) costituita da circa 200 punti rete, collegati tramite cablaggi strutturati di categoria 5E ed alcuni di categoria 6. In ogni caso il cablaggio esistente consente una velocità di 1 GB/s.

Le dorsali esistenti sono realizzate in fibra ottica monomodale G.652D ad eccezione di quelle relative ai piani dell'edificio "Palazzina Tecnica" che rimangono in fibra multimodo. Tutti i gruppi ottici sono terminati con connettori SC-PC. La posa di cavi ottici di dorsale non costituisce oggetto di gara mentre sono oggetto di fornitura tutte le bretelle ottiche necessarie per la connessione degli apparati alle dorsali in Fibra Ottica.

L'attuale rete è costituita da alcuni apparati, che andranno dismessi e smaltiti, e da 3 apparati Extreme Networks di recente acquisto uno da 24Rj45 e due da 48Rj45. Mantenendo l'uniformità dell'offerta, il concorrente potrà prevedere un'integrazione degli apparati Extreme Networks, nel caso proponga lo stesso Brand, oppure il ritiro e la sostituzione dei medesimi nel caso proponga un Brand differente, a beneficio dell'omogeneità di rete.

In ogni caso la manutenzione dovrà includere tutti gli switch della nuova configurazione di rete presente dopo l'intervento.

Sarà onere dell'Appaltatore prevedere lo smaltimento, secondo la normativa vigente, degli apparati dismessi cancellando preventivamente ogni informazione in essi contenuta.

Art. 1 – MODALITÀ DI REALIZZAZIONE

L'Appaltatore dovrà completare la fornitura rispettando il Cronoprogramma riportato in figura 4.

Alla firma del Contratto l'Appaltatore dovrà designare una serie di figure esplicitate al successivo art.21. Tra esse il Projesct Executive si interfaccerà sin da subito con il Direttore dell'esecuzione del contratto. Detta figura parteciperà ai necessari incontri presso la sede della Società con il Servizio Sistemi Informativi (SSI) e il Direttore dell'esecuzione del contratto per definire congiuntamente la configurazione ottimale della rete (prestazioni, sicurezza, livello di servizio, etc..).

La configurazione della rete esistente è attualmente indirizzata in classe A ad uso privato ed in classe A pubblica ad uso privato in via di dismissione. Sarà onere dell'appaltatore prevedere la migrazione di tutte le eventuali utente ancora attestate nella classe in via di dismissione.

La fornitura ed i lavori oggetto dell'appalto avverrà senza creare alcun disagio agli utenti della rete, minimizzando il tempo di intervento da parte dell'Appaltatore e garantendo la buona qualità dell'opera.

Non essendo possibile fermare la rete durante l'orario lavorativo e, per alcuni settori, nemmeno fuori da tale orario, si renderà necessario allestire, configurare e collaudare la rete offline per poi effettuare il passaggio durante un periodo da concordare, verosimilmente durante un fine settimana.

Sarà compito dell'Appaltatore rimuovere gli apparati di rete dismessi, il riassetto e bonifica dei Rack al fine di poter ospitare ordinatamente i nuovi apparati di rete.

Art. 2 – ARCHITETTURA DELLA RETE WIRED

La configurazione della nuova rete, che dovrà sostituire l'esistente, è riportata in figura 1.

Si nota la ridondanza degli apparati in ogni Rack di piano; le 4 macchine di Core dovranno essere configurate come una unica macchina virtuale, permettendo al gruppo di switch di essere gestito e di operare come un singolo switch virtuale.

Inoltre la tecnologia Virtual Stacking dovrà consentire, in caso di guasto ad uno dei rami dell'anello che unisce I 2 Switch, un tempo di recupero e una convergenza di rete inferiore a 50 millisecondi al fine di mantenere attive le eventuali comunicazioni VoIP instaurate.

Tutte le connessioni di rete fra i Core dovranno essere a 40Gigabit/s, le connessioni di rete tra Core e Edge / Firewall / Wireless Controller dovranno essere a 10Gigabit/s.

I link di campus sono in fibra monomodo SMR. Solamente i link indoor di piano nella Palazzina Tecnica e nella sede di Padova rimarranno in fibra Multimodo, come già descritto.

Gli apparati indicati con "PARTE SERVER" non sono da fornire. Anche il Datacenter è in via di sostituzione e i lavori saranno ultimati presumibilmente entro il 2018. Il locale nella sede di Padova Est è stato riprogettato e i lavori saranno terminanti presumibilmente entro il 2018.

Per quanto riguarda il dimensionamento PoE degli switch, è da tener presente che in futuro si prevede di collegare i terminali VoIP esistenti, ovvero Cisco CP8865 (44Watt max) e CP7821. Inoltre Gli apparati di Core proposti dovranno essere dimensionati per supportare traffico VoIP e videochiamate (Skype) per almeno 250 utenze simultanee.

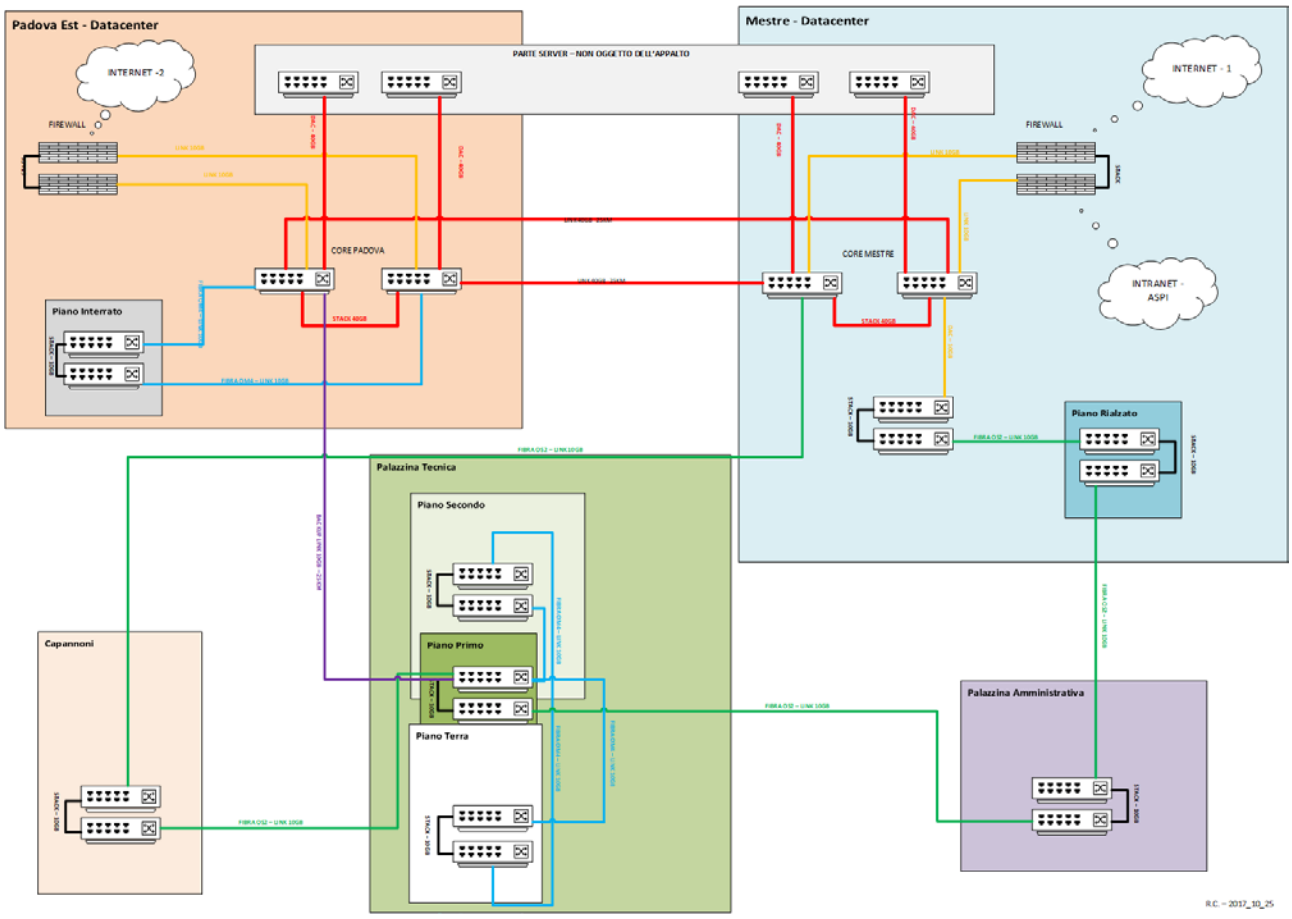

Figura 1 – Configurazione della nuova rete CAV

Art. 3 – CARATTERISTICHE DEGLI APPARATI

Di seguito è riportata la consistenza minima richiesta suddivisa per Core Devices, Edge Devices, Firewall.

Type	Switch di Core	
ITEM	**HARDWARE SPECIFICATIONS**	
1	Tipologia di apparato	Formato Rack

2	Porte disponibili	N°48 porte 1000/10000 SFP+ N°4 Porte QSFP+
3	Funzionalità di Virtual Stacking	Deve essere possibile su connessione WAN fino a 40 Km con fino a 40GBps
4	Alimentazione	Ridondata 100÷240VAC input Potenza almeno 280W

Type	48 Ports Switching for Edge Applications	
ITEM	**HARDWARE SPECIFICATIONS**	
1	Porte disponibili	N°48 porte 10/100/1000BASE-T (RJ-45) PoE+ N° 4 Slot per SFP+ 1000/10G N° 1 x Serial (console port)
2	Alimentazione	Ridondata 100÷240VAC input PoE Budget >300watt

Type	Firewall	
ITEM	**HARDWARE SPECIFICATIONS**	
1	Tipologia di apparato	Formato Rack
2	Porte disponibili	N°16 porte 100/1000 BaseT N°8 Porte SFP+
3	Funzionalità di Clustering	Deve essere possibile su connessione WAN fino a 40 Km con velocità minima 1 GBps
4	Alimentazione	Ridondata 100÷240VAC input Potenza almeno 400W

Art. 4 – REQUISITI TECNICI MINIMI DELL'HARDWARE

Tutti gli apparati proposti devono rispettare i seguenti requisiti:

- Tutte le componenti si intendono nuove di fabbrica e conformi alle normative europee o ad altre disposizioni internazionali riconosciute e, in generale, alle vigenti norme legislative, regolamentari e tecniche disciplinanti i componenti e le modalità di impiego delle apparecchiature medesime ai fini della sicurezza degli utilizzatori;
- Essere sul mercato alla data di pubblicazione della presente bando di gara;
- L'appaltatore deve fornire prodotti hardware originali e licenze software rilasciate appositamente dal costruttore per CAV S.p.A.;
- Gli apparati forniti dovranno essere idonei allo scopo, autentici, nuovi di fabbrica, quindi inclusi nel loro packaging originale e provenienti da fonti autorizzate;
- Il costruttore licenzierà i prodotti specificatamente per la CAV S.p.A., che sarà il primo acquirente per tali prodotti e primo licenziatario di qualsiasi copia del software, compreso quello incluso nei prodotti;
- Onde evitare forniture di licenze software non autorizzate ed apparati non originali, rigenerati, usati o provenienti da canali non autorizzati, la Società potrà richiedere preventivamente opportune verifiche per documentarne l'origine. Tutto ciò affinché siano confermate dal costruttore stesso, attraverso le sue sedi in Italia, le necessarie certificazioni sulla genuinità, provenienza e garanzia.

Si specifica, infine, che nell'ambito dei requisiti espressi di seguito, è richiesta la fornitura di tutte le componenti hardware e software necessarie alla implementazione e all'utilizzo delle funzionalità indicate.

REQUISITI TECNICI E PRESTAZIONALI MINIMI PER GLI SWITCH DI CORE	
ITEM	DESCRIZIONE DEL REQUISITO TECNICO O PRESTAZIONALE
TP01	Omogeneità tecnologica - Tutti i dispositivi switch previsti in fornitura devono essere della stessa tecnologia (stesso vendor).
TP02	La tipologia di soluzione fornita per la componente di Core dovrà essere costituita da apparati a rack, con una composizione ridondata tale da garantire scalabilità, affidabilità, sia hardware che software, con architettura no Single Point of Failure, alimentazione ridondata con capacità di switching minima pari a 1.28 Tbps e un throughput di 960Mpps. L'apparato fornito deve essere uno switch Terabit-Class con funzionalità L2/L3 integrate, ideale per un posizionamento di livello Core/Datacenter dove sono richiesti, connettività, capacità, alta affidabilità (HA) e latenze minime.
TP03	L'apparato richiesto deve supportare almeno fino a 48 porte a 10 Gigabit Ethernet SFP+ almeno 4 porte a 40Gigabit Ethernet QSFP+
TP04	Tutti gli apparati devono essere dotati di gruppi ventole il cui funzionamento sia monitorabile da sistema di gestione dello switch e che possano essere sostituiti a caldo (hot swappable).
TP05	Ogni apparato fornito deve supportare almeno una capacità di switching pari a 1.28 Tbps e un throughput di 960Mpps. La soluzione fornita dovrà realizzare una ridondanza 1+1. I processi di switching, routing e management dovranno essere quindi distribuiti su tutti gli switch presenti in configurazione. Ogni switch dovrà agire come Master per determinati servizi L2/L3 e nel caso di improvvisa indisponibilità di tale switch , questi servizi dovranno essere presi in carico dagli altri switch presenti in maniera trasparente all'utente garantendo così una ridondanza sia L2 che L3.

TP06	Possibilità di unire almeno 2 apparati in modalità Virtual Chassis con condivisione delle tabelle Layer 2 e Layer 3 e di creare sino a 128 aggregazioni di porte LAG (Link Aggregation). La connessione tra gli apparati dovrà basarsi su connessione fibra ottica monomodale prevedendo la distanza massima di 40 Km.
TP07	Supporto sFlow (RFC 3176)
TP08	L'apparato deve poter applicare politiche di traffico (mappare su VLAN, rate limiting, L2/L3, L4 filtering, traffic shaping) sui flussi di traffico identificati come IP sorgente/destinazione e porta TCP/UDP sorgente/destinazione. Deve quindi essere possibile classificare i flussi di traffico ed applicare loro politiche differenziate, questo deve essere possibile sia in una configurazione L2 switching che L3 routing. Le politiche di traffico devono inoltre essere applicabili su base VLAN.
TP09	L'apparato dovrà supportare avanzate funzionalità di QoS e gestione del traffico real-time (VoIP), dovrà quindi essere in grado di classificare il traffico a livello 2/3/4 applicando conseguentemente adeguati livelli di priorità. Devono essere supportate almeno 8 code hardware per porta. Dovranno inoltre esse supportati dei protocolli per il riconoscimento automatico di terminali VoIP connessi allo switch quali LLDP-MED. Traffico dati e voce dovranno poter essere associati a VLAN differenti e vedersi applicati livelli di priorità specifici

FUNZIONALITÀ E CERTIFICAZIONI MINIME RICHIESTE PER GLI SWITCH DI CORE	
ITEM	DESCRIZIONE DELLA FUNZIONALITÀ O CERTIFICAZIONE
FC01	802.1ab LLDP-MED 802.1ad Provider Bridges 802.1ag Connectivity Fault Management (CFM) 802.1ak Multiple VLAN Registration Protocol (MVRP) 802.1ax-2008 / 802.3ad Link Aggregation, up to 64 groups with up to 8 ports in a group
FC02	802.1d MAC Bridges 802.1q VLAN and 4.094 VLAN. 802.1s Multiple Spanning Tree 802.1w Rapid re-convergence of Spanning Tree 802.3ae 10 Gigabit Ethernet (fiber) 802.3x Flow Control
FC03	IP Multicast (IGMPv1, v2, v3) IGMP v1/v2/v3 Snooping and Querier Jumbo Packet with MTU Discovery Support for Gigabit (9216 bytes)

ITEM	DESCRIZIONE DELLA FUNZIONALITÀ O CERTIFICAZIONE
FC04	Static Routes Standard ACLs OSPF with Multipath Support OSPF Passive Interfaces IPv6 Routing Protocol Extended or Advanced ACLs Policy-based Routing
FC05	Virtual Extensible LAN (VXLAN) In-Service Software Upgrade (ISSU) Hitless patch upgrades sFlow® (RFC 3176) Unicast Reverse Path Forwarding (uRPF) RFC 3074 Multiprotocol Label Switching (MPLS) Multiprotocol Label Switching (MPLS) Layer 3 VPN Multiprotocol Label Switching (MPLS) Layer 2 VPN Super VLAN RFC 3069 Multicast Border Gateway Protocol (MBGP) Multicast Source Discovery Protocol (MSDP) MLD IPv6 Snooping and Querier Virtual Stacking trough 40Gb/s ports OpenFlow 1.3
FC06	DHCP Snooping IP Source Guard Arp Attack Protection
FC07	Virtual Routing and Forwarding (IPv6 and IPv4) Border Gateway Routing Protocol - BGPv4 PIM Source Specific Multicast - PIM SSM Generic Route Encapsulation (GRE)
FC08	Multi-user, Multi-method Authentication and Policy per port 802.1X Port-based Authentication Web-based Authentication MAC-based Authentication Multiple Authentication Types per Port Simultaneously
FC09	Broadcast Suppression ARP Storm Prevention or Attack Protection Spanning Tree Protection (BPDU guard) Static Multicast Group Provisioning Multicast Group, Sender and Receiver Policy Control
FC10	Strict Priority Queuing Weighted Fair Queuing with Shaping

	Packet Count or Bandwidth based Rate Limiters IP ToS/DSCP Marking/Remarking 802.1D Priority-to-Transmit Queue Mapping
FC11	SNMP v1/v2c/v3 Web-based Management Interface Industry Common Command Line Interface Multiple Software Image Support with Revision Roll Back Multi-configuration File Support Editable Text-based Configuration File Telnet Server and Client Secure Shell (SSHv2) Server and Client
FC12	Link Layer Discovery Protocol (LLDP) Syslog FTP Client Simple Network Time Protocol (SNTP) RADIUS and RADIUS Accounting TACACS+ for Management Access Control Management VLAN Mirror Many to-One-port, One-to-Many Ports, Remote Port Mirroring
FC13	Safety CAN/CSA 22.2 No. 60950-1; FCC Part 15, Subpart B; RoHS Compliance; IEC 60950-1, Second Edition; EN 60950-1:2006 + A11:2009; IEC 60825-1; UL 60950-1, 2nd Edition; EN60825-2:2004+A1:2007
ITEM	DESCRIZIONE DELLA FUNZIONALITÀ O CERTIFICAZIONE
FC14	Emissions VCCI Class A; EN 55022 Class A; CISPR 22 Class A; IEC/EN 61000-3-2; IEC/EN 61000-3-3; ICES-003 Class A; AS/NZS CISPR 22 Class A; FCC (CFR 47, Part 15) Class A;

REQUISITI TECNICI E PRESTAZIONALI MINIMI PER GLI SWITCH DI EDGE	
ITEM	DESCRIZIONE DEL REQUISITO TECNICO O PRESTAZIONALE
TP01	48 porte gigabit Ethernet 10/100/1000BaseTX PoE+, più 4 porte SFP+ 1/10Gb Modulo opzionale per ulteriori 2 porte SFP+ 1/10Gb Switching capacity mimima di 176 Gbps e throughput di 130 Mpps. Latenza 10GbE <3µs (64-byte). Latenza 1GbE <5µs (64-byte).
TP02	Stacking ad alta velocità (almeno 10Gbps) e alta disponibilità, impilabili almeno sino ad 8 unità, due porte 10Gb SFP+ Gli switch devono poter essere impilati anche con switch di tipologie differenti (es densità porte) della stessa famiglia e dello stesso costruttore per una maggiore elasticità. Alimentazione ridondata
TP03	Supporto del protocollo LACP 802.3ad. Supporto di almeno 14 trunk LACP su singolo device, con 8 porte per trunk. Supporto di almeno 4.094 VLAN. Supporto di almeno 512 ACL in ingresso. Supportare almeno 16k MAC Address. Supportare 8 code di priorità QoS per porta.
TP04	Supporto di Lifetime Warranty con Advanced Hardware Replacement. Supporto tecnico minimo di 5 anni dalla data di fine vita del prodotto
TP05	Supportare una temperatura di esercizio da 0° C a 45° C. Umidità operative relative: dal 10% al 90%, senza condensa.

FUNZIONALITÀ E CERTIFICAZIONI MINIME RICHIESTE PER GLI SWITCH DI EDGE	
ITEM	DESCRIZIONE DELLA FUNZIONALITÀ O CERTIFICAZIONE
FC01	Supporto del protocollo Spanning Tree 802.1D, 802.1s, 802.1w e PVST+. SNMPv1, v2 e v3. SSHv2 client e server. SCP/SFTP client e server. RADIUS e TACACS+. Support HTTPS/SSL per web-based.
FC02	Supporto dei seguenti metodi di autenticazione di rete: Web based; 802.1X;

	MAC-based; Local database per autenticazione MAC/web-based;	
FC03	IGMP snooping Remote mirroring. sFlow® (RFC 3176)	System virtual router L3. Supporto di RIPv1 e v2, RIPng. Policy based routing (PBR) per IPv4.
FC04	UL 60950-1; EN 60825-1 Safety of Laser Products-Part 1; EN 60825-2 Safety of Laser Products-Part 2; IEC 60950-1; EN 60950-1; CAN/CSA-C22.2 No. 60950-1; FDA 21 CFR Subchapter J; ROHS Compliance; GB 4943; EMC Directive 2004/108/EC; FCC (CFR 47, Part 15) Class A; EN 61000-4-11:2004; ANSI C63.4-2009;	EN 61000-3-3:2008; EN 61000-3-2:2006+A1:2009+A2:2009 ; EN 61000-4-3:2006; EN 61000-4-4:2012; EN 61000-4-5:2006; EN 61000-4-6:2009; CISPR 22:2008 Class A; EN 55022:2010 Class A; EN 61000-4-29: 2000; CISPR 24:2010; EN 300 386 V1.6.1; VCCI V-3/2013.04 Class A; EN 55024 EN300 386

REQUISITI TECNICI E PRESTAZIONALI MINIMI PER I FIREWALL
DESCRIZIONE DEL REQUISITO TECNICO O PRESTAZIONALE
Apparati di tipo UTM con funzionalità Next Generation Firewall, ovvero sino a livello 7 applicativo, funzionalità Intrusion Prevention e threat management, protezione da Spam e virus sia via navigazione che via Mail Gli apparati devono avere le seguenti caratteristiche fisiche: 16 porte gigabit Ethernet 100/1000BaseTX, più 8 porte SFP+ 1/10Gb, 2 porte per funzionalità di clustering, 1 porta console Capacità di firewalling mimima per blocchi da 512 byte di 80 Gbps con latenza di 3 us Capacità di throughput firewall di almeno 80 Milioni di pacchetti al secondo Gestione di almeno 12 milioni di sessioni contemporanee Capacità di throughput VPN Ipsec con pacchetti da 512 byte di almeno 50 Gbps Capacità di throughput VPN SSL di almeno 4 Gbps Capacità di ispezione di pacchetti SSL con throughput di almeno 10 Gbps Capacità di ispezione a livello applicativo con throughput di almeno 12 Gbps Capacità di ispezione con analisi threat con throughput di almeno 5 Gbps
Disponibilità di aggiornamenti e patch del Sistema operative Disponibilità di aggiornamenti di impronte virali e liste di siti dannosi Disponibilità di aggiornamenti di per le funzionalità di intrusion prevention Disponibilità di aggiornamenti di impronte virali per spam e antivirus mail
Supportare una temperatura di esercizio da 0° C a 40° C. Umidità operative relative: dal 10% al 90%, senza condensa.

FUNZIONALITÀ E CERTIFICAZIONI MINIME RICHIESTE PER I FIREWALL		
ITEM	DESCRIZIONE DELLA FUNZIONALITÀ O CERTIFICAZIONE	
FC01	Supporto del protocollo Spanning Tree 802.1D SNMPv1, v2 e v3. SSHv2 client e server. Support HTTPS/SSL per manutenzione web-based.	
FC02	Supporto dei seguenti metodi di autenticazione di rete: Web based; 802.1X; Radius	
FC03	Supporto di RIPv1 e v2 Supporto a BGP	
FC04	Certificazioni FCC Part 15 Class A C-Tlck VCCI, CE, UL/cUL CB	Certificazioni ICSA Labs

E' espressamente richiesto che le macchine di Core e di Edge, le cui caratteristiche minime sono sopra elencate, e gli AP Wi-Fi più avanti descritti, proposte dal concorrente, siano di un unico Vendor; in particolare le macchine Core ed Edge devono possedere lo stesso Sistema Operativo che consenta di avere uniformità di CLI (Command Line Interface).

Le macchine firewall devono essere fornite corredate di un analizzatore esterno di traffico in grado di fornire report dettagliati (anche sotto forma di VM) e di un antispam ridondato almeno equivalente a quello in dotazione ad oggi nella Società (VM Fortimail) entrambi totalmente licenziati e per tutta la durata dell'appalto.

Tutte le regole di firewall devono essere riportate nei nuovi apparati ed ogni ulteriore nuova implementazione sarà validata dal direttore dell'esecuzione del contratto e dal Project Executive.

Art. 5 – RETE WIRELESS

La società dispone di due differenti sistemi Wi-Fi. Uno fornisce accesso degli uffici alla rete; è destinato ad essere dismesso e sostituito con il nuovo sistema riutilizzando il cablaggio esistente. Il secondo, di recente realizzazione, fornisce il servizio VoIP. Quest'ultimo dovrà essere integrato con il nuovo sistema. L'attuale Wi-Fi dedicata al VoIP è interfacciato alla centrale telefonica presso la sede di Venezia Mestre. La funzione di centrale telefonica è svolta da una coppia di Call manager Cisco BE6H-M4-K9. Le funzionalità supportate dal servizio Voip, che dovranno essere integrate nella nuova rete Wi-Fi, sono:

- Supporto di almeno 1000 utenti e 2500 device VoIP;
- Utilizzo di telefoni Cisco Unified Wireless IP Phone 7926G (numero massimo 10 unità).

Allo stato la rete WiFI propaga un solo SSID dedicato al servizio VoIP con VLAN Voce.

La copertura attuale dell'area uffici/magazzino/capannoni della sede di Marghera è pressoché totale: sono stati utilizzati 43 AP Cisco Aironet 3700 (utilizzati sia per indoor che per outdoor). Il disegno ottimale di un precedente survey ne prevedeva 49. E' da intendersi che il nuovo sistema dovrà fornire almeno una copertura identica se non migliorativa.

Il nuovo sistema Wi-Fi quindi dovrà dare copertura Wireless alla sede di Marghera indoor e outdoor, alle palazzine Uffici e Data Center al casello Padova Est e agli 8 caselli autostradali della Società in itinere tra la barriera di Mestre e di Padova Est e del Passante di Mestre.

Per quanto riguarda la sede di Marghera, la copertura Wi-Fi outdoor dovrà interessare in particolar modo le aree evidenziate in verde nella Figura 2 e precisamente le 2 "pensiline parcheggi", le aree antistanti la palazzina Direzione Tecnica e Direzione Amministrativa (rispettivamente DA/DG e DT/DE) e il percorso tra il magazzino e la Direzione Tecnica. Tale copertura dovrà garantire l'uso di terminali VoIP nel passaggio tra i vari edifici della sede. La copertura indoor a Marghera riguarda le palazzine Esercizio, Direzione Amministrativa, Direzione Tecnica e le aree uffici dei Capannoni A-B-C.

Al casello di Padova Est la copertura indoor riguarda le due palazzine evidenziate in rosso (uffici) ed in verde (Data Center) in Figura 3. La copertura outdoor si limita alla pensilina auto presente al Data Center

Nei restanti caselli verrà realizzata solamente copertura indoor con un solo AP per ogni fabbricato di stazione (8 in totale).

La Società metterà a disposizione le piante in formato PDF delle aree interessate dalla copertura; l'Appaltatore dovrà fare delle simulazioni utilizzando strumenti S/W come Ekahau Site Survey, Chanalyzer, TamoGraph Pro Site Survey o altri equivalenti. Con tali strumenti, avendo cura di definire dettagliatamente le dimensioni e la natura degli ostacoli quali pareti, soffitti e strutture metalliche, sarà possibile triangolare il segnale di ogni AP e valutare così i parametri fondamentali quali, ad esempio, la potenza del segnale, che non dovrà scendere sotto i -65dBm nelle aree interessate, sia per non ridurre troppo il throughput, sia per favorire il roaming nelle conversazioni VoIP in mobility.

Si ritiene il Site Survey fondamentale per ottenere i seguenti risultati:

- livello segnale adeguato ed uniforme;
- velocità delle connessioni;
- riduzione dei tempi di latenza;
- compatibilità di nuovi apparati con eventuali dispositivi già esistenti;
- corretta posizione degli AP;
- ottimizzazione della copertura delle aree richieste;
- determinare i requisiti di alimentazione, cablaggio, e accessori di montaggio;

- verificare eventuali zone d'interferenza;
- verificare la salute della rete (Network Health, Network Issue, Signal-to-Noise Ratio, Signal Strength).

Figura 2 – Pianta della CAV S.p.A. – in verde le aree di copertura outdoor

Figura 3 – Pianta del casello CAV S.p.A. di Padova Est

Art. 6 – PRESTAZIONI DELLA RETE WI-FI

Il progetto prevede la realizzazione dell'infrastruttura di rete wireless per l'erogazione del Servizio WiFi almeno nelle aree indicate nelle Figure 2 e 3.

Le forniture degli apparati e dei sistemi dovranno essere comprensive di ogni componente accessorio necessario alla loro completa funzionalità. Per quanto riguarda gli uffici di Padova Est si consideri che gli edifici sono lunghi circa 120 metri e consistono in un corridoio con uffici su un solo lato. Si ritiene che siano sufficienti 4 AP per edificio, mentre per la copertura outdoor siano sufficienti 2 AP.

La gestione delle configurazione di tutta l'infrastruttura wireless dovrà essere centralizzata (non sono ammesse soluzioni con AP stand alone senza una gestione centralizzata e non sono ammesse soluzioni dipendenti dal Cloud).

Il Controller di gestione del sistema dovrà essere Hardware, ridondato e installato localmente.

La gestione centralizzata dovrà consentire di prendere in carico gli Access Point e configurare i vari parametri fisici e radio dell'infrastruttura wireless.

La soluzione wireless proposta deve poter supportare le seguenti funzionalità, oltre che essere dello stesso Vendor della soluzione wired descritta al capitolo precedente:

- Supporto standard 802.11 a/b/g/n/ac Wave2 – 5GHz 3x3MIMO (1,300 Mbps max rate) and 2.4GHz 2x2MIMO (400Mbps max rate)
- Tipologia Dual Radio con antenne omnidirezionali integrate;
- Supporto di almeno 10 SSID per radio;
- Controllo dinamico del roaming dei client con standard IEEE 802.11k e IEEE 802.11v;
- Supporto di External AAA/RADIUS per Autenticazione, Autorizzazione ed Accounting;
- Almeno una porta Network Gigabit Ethernet per ciascun AP;
- Supporto di funzionalità di DPI (Deep Packet Inspection) sugli AP;
- Radio Bluetooth Low Energy (BLE) integrata negli AP;
- Supporto di Policy Applicative (L7) configurabili dinamicamente;
- Numero di AP associabili al controller (Virtuale o Fisico) maggiore o uguale a 64;
- Funzionalità di Automatic Controller Failover (elezione del controller con criterio automatico);
- Monitoraggio accessi per utente e WLAN;
- Log di sistema;

Di seguito è riportata la consistenza e le caratteristiche tecniche minime richieste, suddivisa per AP Indoor e Outdoor.

Type	Wireless Controller	Quantità: 2
ITEM	HARDWARE SPECIFICATIONS	
1	Almeno 2 porte 10GBASE-X (SFP+) Almeno 4 porte (1000BASE-X o 10/100/1000BASE-T) Almeno 1 USB 2.0 Console	

Type	Access Point Indoor 802.11ac	Quantità: 40
ITEM	HARDWARE SPECIFICATIONS	
1	Caratteristiche obbligatorie richieste: Access Point (AP) dual radio 2.4 GHz e 5 GHz - 802.11 a/b/g/n/ac Throughput della Radio a 2.4GHz almeno pari a 300Mbps Throughput della Radio a 5GHz almeno pari a 867Mbps Tipologia MIMO minimo 2X2 su 2,4 GHz e almeno 3X3 su 5GHz Bluetooth integrato nativamente per geolocalizzazione	

Type	Access Point Outdoor 802.11ac	Quantità: 20
ITEM	HARDWARE SPECIFICATIONS	
1	Caratteristiche obbligatorie richieste: Access Point (AP) dual radio 2.4 GHz e 5 GHz - 802.11 a/b/g/n/ac Throughput della Radio a 2.4GHz almeno pari a 300Mbps Throughput della Radio a 5GHz almeno pari a 867Mbps Tipologia MIMO minimo 2X2 su 2,4 GHz e almeno 3X3 su 5GHz Certificazione IP66 e/o IP67 Range di temperatura operativa da -30C a +60C senza alcun disservizio	

REQUISITI TECNICI E FUNZIONALITÀ MINIME DEI WIRELESS CONTROLLER
DESCRIZIONE DEL REQUISITO TECNICO O PRESTAZIONALE
Caratteristiche obbligatorie richieste: Numero massimo di AP >= 200 Numero Massimo di RAPs >= 200 Numero di Device Concorrenti >=8000 VLAN >= 4000 Numero di Sessioni IPSec / SSL Concorrenti >= 4000 Throughput >= 12GBps

REQUISITI TECNICI E FUNZIONALITÀ MINIME DEGLI ACCESS POINT	
ITEM	DESCRIZIONE DEL REQUISITO TECNICO O PRESTAZIONALE
AP01	High performance enterprise class AP Numero di schede radio 2 802.11ac – 5GHz 3x3 MIMO (867Mbps max rate) and 2.4GHz 2x2 MIMO (300 Mbps max rate) Numero di spatial streams 3 Deve supportare la modalità Plug and play operation/Zero touch deployment Deve supportare Security e Standards WPA, WPA2 (AES), 802.11i, 802.1x, IPSec, IKEv2, PKCS #10, PKCS #12, X.509
AP02	Servizi WDS per estendere la rete in aree non cablate. Funzionalità di Dynamic Radio Management. Access Point load balancing. Access Point band steering. Funzionalità di QoS e Rate Limiting e filtraggio su AP. Multicast Rate Control
AP03	802.11b: Direct-sequence spread-spectrum (DSSS) 802.11a/g/n/ac: Orthogonal frequency-division multiplexing (OFDM) 802.11b: BPSK, QPSK, CCK 802.11a/g/n/ac: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM
AP04	Supporto funzionalita' DPI direttamente su AP per analisi applicativa realtime Supporto di policy applicative L7 direttamente su AP per poter permettere, limitare o negare l'utilizzo di specifiche applicazioni Supporto funzionalità di Wireless IDS/IPS integrate

ITEM	DESCRIZIONE DEL REQUISITO TECNICO O PRESTAZIONALE
AP05	FCC/Industry of Canada CE Marked R&TTE Directive 1995/5/EC Low Voltage Directive 72/23/EEC EN 300 328 EN 301 489 EN 301 893 UL/IEC/EN 60950 EN 60601-1-1, EN60601-1-2 Wi-Fi Alliance (WFA) certified 802.11a/b/g/n/ac

Per quanto detto in precedenza in previsione del supporto VoIP, gli AP devono supportare il roaming su reti Wi-Fi con gli standard 802.11k, 802.11r (FT) e 802.11v che consentono di ridurre a 50ms il tempo di connessione, senza handover, di un terminale VoIP nel passaggio da un AP ad un altro.

Tutti gli AP devono essere autoinstallanti; una volta connessi in rete devono essere in grado di interconnettersi alla gestione centralizzata senza che sia necessario alcun tipo di configurazione sull'AP.

Deve essere possibile configurare gli AP al fine di non far apparire gli SSID nei messaggi di beacon trasmessi in modo che gli Utenti non vedano alcun SSID ne debbano specificare l'SSID al quale desiderano connettersi.

Art. 7 – SISTEMA DI AUTENTICAZIONE – CAPTIVE PORTAL

Il progetto deve prevedere che tutti gli accessi alla rete, sia wireless che wired, debbano essere controllati attraverso un sistema di controllo accessi (NAC) con autenticazione basata su 802.1X che fungerà da Radius con interfacciamento verso altri eventuali servizi di Active Directory o LDAP.

Oltre ad un sistema per l'autenticazione degli asset aziendali è anche richiesto un sistema di controllo degli accessi alla rete da parte di ospiti, fornitori o personale temporaneo (Guest Users).

Tale strumento Software dovrà consentire un NAC (Network Access Control) su tutti gli accessi alla rete permettendo di verificare, validando oppure negando, i device wired e wireless utilizzati.

Lo strumento software richiesto dovrà consentire di realizzare una piattaforma di autenticazione AAA con funzionalità avanzate di controllo delle politiche di accesso, con la possibilità di profilare l'accesso in base a fattori temporali (orari, giorno della settimana), posizione, appartenenza a gruppi AD specifici, etc.

Lo strumento dovrà essere fornito on-premise, come Hardware fisico oppure come Virtual Machine, in funzione delle necessità e decisioni della Società.

Il software dovrà fornire funzionalità di profiling per identificare e classificare i dispositivi sulla rete, e permettere la creazione di reportistica e analisi degli accessi alla rete integrata nella piattaforma.

Il software di NAC dovrà essere fornito completo di supporto direttamente da parte del vendor, sono in tal modo esplicitamente escluse soluzioni non commerciali.

Sempre nell'ottica di verifica e gestione degli accessi è richiesta la fornitura di una soluzione di Captive Portal Web per un numero ridotto di accessi, con possibilità di espansione futura, che permetta la completa configurazione di un sistema di accesso per le utenze Guest.

La piattaforma dovrà prevedere uno strumento software installato su hardware fisico o virtual machine. Il Captive Portal in questione dovrà supportare le seguenti funzionalità minime richieste:

- Self-registration degli utenti;
- customizzazione delle pagine web con personalizzazione di grafica e form di registrazione;
- possibilità di accesso mediante credenziali social;
- registrazione sponsor-based degli utenti;
- pagine di pre-registrazione massiva delle utenze (random user & password generation, bulk import);
- notifica tramite mail e sms delle registrazioni utente;
- limitazioni di accesso in base a fasce temporali e scadenza predefinite;
- funzionalità di reporting dell'attività dei guest.

REQUISITI TECNICI E FUNZIONALITÀ MINIME DEL SISTEMA DI AUTENTICAZIONE	
ITEM	DESCRIZIONE DEL REQUISITO TECNICO O PRESTAZIONALE
SA01	Interfaccia grafica web based Radius Server per l'accesso di almeno 500 endpoints Supporto AAA/802.1X standard Database Interno utenti/endpoints Supporto integrazione con Active Directory Supporto integrazione LDAP server Supporto integrazione con database SQL ODBC compliant
SA02	Supporto policy di accesso in base a RADIUS Internet Engineering Task Force (IETF) Attributes Supporto policy di accesso time based (orario, giorno della settimana, etc) Supporto policy di accesso in base ad attributi Active Directory (User group, user and machine attributes, etc)
SA03	Password Authentication Protocol (PAP) Protected Extensible Authentication Protocol (PEAP) Microsoft Challenge Handshake Authentication Protocol Version 2 (MS-CHAPv2) Extensible Authentication Protocol-Message Digest 5 (EAP-MD5) Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST) Protected Extensible Authentication Protocol-Transport Layer Security (PEAP-TLS)

Art. 8 – ATTIVITÀ E SERVIZI COMPLEMENTARI

Tutte le attività descritte agli art. precedenti sono inclusive dei servizi di configurazione di tutto l'hardware ed il software forniti, inclusa l'attività di Site Survay con la produzione del Covering Plan indispensabile per la dislocazione degli AP, che dovrà essere fatto sia presso la sede di CAV S.p.A. di Marghera, come illustrato in Figura 2, sia presso il casello di Padova Est, come illustrato in Figura 3. Le attività saranno concordate con il Direttore dell'esecuzione del contratto.

Al termine delle attività l'Appaltatore dovrà predisporre uno schema, in formato Power Point o altro formato da concordare, relativo allo schema architetturale e dei collegamenti telematici con l'esterno dell'intera rete TLC della Società (Wan, Lan, Wireless, Remote Access, ecc.).

Lo schema servirà da base per tutti gli interventi futuri e dovrà essere sempre aggiornato, sia dal punto di vista hardware, sia come configurazione di layer 2 e 3.

Art. 9 – CABLAGGIO UTP BONIFICA RACK E MIGRAZIONE DELLA RETE

Sono incluse nella fornitura le attività di cablaggio dei punti UTP relativi agli Access Point, oltre all'installazione degli stessi, sia in outdoor (20 punti) che indoor (40 punti), per un totale di 60 punti posizionati come descritto al capitolo precedente, ovvero a Marghera, a Padova est e nei 5 caselli caselli.

Ulteriore attività, inclusa nella fornitura, è la bonifica dei Rack interessati ad ospitare le macchine di nuova fornitura. Attività che consiste nel riposizionamento degli switch esistenti in previsione della loro dismissione, organizzazione delle permutazioni con eventuale fornitura di passacavi e Patch di permutazione.

Tutte le Patch cord ed i Patch Panel dovranno essere etichettati secondo la logica che verrà concordata con il Direttore dell'esecuzione del contratto. E' richiesta la sostituzione di tutte le Patch Cord di permutazione degli armadi esistenti, con differenti colorazioni in funzione alle differenti utenze collegate, per una migliore e diretta individuazione della topologia di cablaggio.

A titolo di esempio, anche se non vincolante, potrebbe essere usata la seguente logica:

- GIALLO: utenti;
- VERDE: stampanti;
- BIANCO: access point outdoor;
- BLU: access point indoor;
- ROSSO: server / servizi (solo rack);
- ARANCIO: management;
- VIOLA: apparecchiature IOT.

Dopo aver bonificato tutti gli armadi Rack si procederà alla posa dei nuovi apparati ed alla loro alimentazione. La migrazione completa andrà effettuata molto verosimilmente nel corso di un weekend al fine di non creare disagio all'operatività della Società. Si procederà successivamente allo smontaggio dei vecchi apparati dai Rack.

Art. 10 - CRONOPROGRAMMA

La completa fornitura e configurazione degli apparati, interventi di adeguamento e Site Survay dovranno essere eseguiti in 60 giorni naturali o consecutivi, decorrenti dalla data di avvio dell'esecuzione del contratto.

L'Appaltatore potrà modificare le singole attività del cronoprogramma in figura 4, sia come tipologia che come durata, senza allungare la durata complessiva della fornitura e configurazione.

Si segnala che ad oggi i lavori di predisposizione della sala che ospiterà gli apparati della Sede di Padova non sono terminati. L'Appaltatore dovrà prevedere quindi un collaudo funzionale a 2 step: un primo collaudo per la sola sede di Mestre e un secondo collaudo funzionale definitivo a lavori ultimati (presumibilmente entro i primi mesi del 2019).

FASI DI LAVORAZIONE		Giornate Lavorative
Descrizione dell'Attività	Durata (GG)	1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40
Avvio esecuzione del contratto		
Approvigionamento dei materiali	20	
Site Survay e definzione rete Wi-Fi	10	
Cabling punti di accesso Outdoor	10	
Cabling punti di accesso Indoor	15	
Bonifica dei Rack	8	
Definizione e configurazione Networking	5	
Configurazione apparati ed installazioni S/W	5	
Prove funzionali e test H/W e S/W	3	
Installazione apparati e migrazione	4	PREVEDERE MIGRAZIONE DURANTE FINE SETTIMANA
Collaudo tecnico e funzionale	2	
Training del personale Sistemi Informativi	6	

Figura 4 – Cronoprogramma relativo alla realizzazione della rete

Art. 11 – FORMAZIONE DEL PERSONALE DELLA SOCIETÀ

L'Appaltatore avrà l'onere dell'addestramento del personale IT della Società (n. 3 persone) per raggiungere un sufficiente livello di conoscenza nell'uso delle macchine e dei software, tale da rendere possibile effettuare operazioni di configurazione ordinarie e modifiche successive. Si dovrà prevedere una prima fase "pre-installazione", di introduzione e spiegazione generale dei prodotti e del software seguita da una sessione di "training on the job" durante le fasi di pianificazione e di installazione delle macchine e del software.

Art. 12 – SERVIZIO DI MONITORAGGIO PROATTIVO – REAL TIME E MANUTENZIONE

L'Appaltatore dovrà fornire un servizio di monitoraggio proattivo e real-time dello stato e delle risorse disponibili della rete attraverso una supervisione remota costante ed attiva di tutti gli apparati forniti.

Con "monitoraggio proattivo e real-time dello stato e delle risorse disponibili della rete" si intende l'attivazione di un servizio erogato da specialisti di Networking, in grado di verificare in modo continuo lo stato di funzionamento di tutti gli apparati della rete della Società e di tutti i relativi servizi di rete, inviando messaggistica (email, sms) automaticamente qualora vengano rilevati dei problemi o quando determinati parametri assumono valori anomali o semplicemente raggiungano delle soglie prefissate.

Oltre alla notifica automatica, l'Appaltatore dovrà, previa attività di diagnosi eseguita dal team di specialisti, allertare il personale della Società per aggiornarlo sulle problematiche in corso ed eventuali azioni correttive.

Tale servizio dovrà essere erogato attraverso specialisti di networking e con gli strumenti che l'Appaltatore dovrà mettere a disposizione presso il proprio Network Operation Center (NOC).

Tutte le attività dovranno essere rintracciabili attraverso un numero identificativo.

Sarà cura della Società, prima dell'attivazione del servizio, stabilire le configurazioni e le metriche che l'Appaltatore dovrà implementare nel sistema sulla base dell'offerta presentata.

Eventuali altri oneri derivanti dall'attivazione del servizio di cui al presente articolo (licenze software, connettività etc.) saranno a completo carico dell'Appaltatore.

Tale attività dovrà essere garantita secondo gli SLA indicati all'art 19.

Art. 13 – SERVIZIO ATTIVAZIONE TERZE PARTI, ATTIVITÀ ON-SITE O REMOTE

L'Appaltatore dovrà fornire un servizio di attivazione terze parti in caso di richiesta di attività manutentive on-site o remote in gestione ad altre aziende (ad esempio Carrier,…).

A seguito di eventi critici rilevati dal servizio di monitoraggio proattivo o rilevati dalla Società relativi agli apparati di rete e oggetto dei servizi che richiedano attività in loco o remota, l'Appaltatore dovrà contattare per conto ed a nome della Società il manutentore (Carrier, etc.) secondo gli SLA indicati.

La Società fornirà all'Appaltatore l'elenco dei manutentori (Carrier, etc.) di cui al comma precedente, comprensivo di recapiti, indirizzi per apertura ticket, identificativi, etc.

L'Appaltatore dovrà collaborare con il manutentore per l'eventuale supporto alla risoluzione del problema. Il servizio comprende il monitoraggio delle attività del manutentore fino alla risoluzione del guasto. L'Appaltatore rimarrà in tal modo l'unico punto di contatto per la Società verso il mondo esterno per quanto riguarda le problematiche connesse alle TLC.

L'Appaltatore dovrà attivare il manutentore (Carrier, etc.) autonomamente dandone tempestiva comunicazione alla Società, sulla base degli eventi critici segnalati dai servizi oppure su segnalazione diretta da parte della Società.

L'attivazione di terze parti, effettuate previa diagnosi remota da parte del team di specialisti del NOC dell'Appaltatore, dovrà avvenire definendo correttamente e dettagliatamente l'anomalia riscontrata al fine di ripristinare il corretto funzionamento dei servizi di rete e sicurezza nel più breve tempo possibile.

Tale attività dovrà essere garantita secondo gli SLA indicati all'art 19.

Art. 14 – SERVIZIO DI MONITORAGGIO DELLE RISORSE DISPONIBILI DELLA RETE WIRELESS

L'Appaltatore dovrà fornire un servizio di monitoraggio proattivo e real-time dello stato e delle risorse disponibili anche della rete Wireless attraverso una supervisione remota costante ed attiva di tutti gli apparati descritti negli art. 5,6,7.

Il servizio dovrà prevedere la realizzazione di una mappa di copertura della rete wireless, basata sulle seguenti informazioni:

- Planimetrie;
- Posizionamento Access Point;
- Risultati del Survey wireless.

Eventuali altri oneri derivanti dall'attivazione del servizio di cui al presente articolo (licenze software, connettività etc.) saranno a completo carico dell'Appaltatore.

Tale attività dovrà essere garantita secondo gli SLA indicati all'art 19.

Art. 15 – SERVIZIO CAMBIO DELLE CONFIGURAZIONI / SETUP AVANZATO

L'Appaltatore dovrà fornire un servizio di modifica delle configurazioni/setup avanzato degli apparati esistenti per mutate esigenze o per gestire nuovi contesti di funzionamento.

La Società potrà richiedere direttamente all'Appaltatore la modifica della configurazione di uno o più apparati oggetto del servizio.

Al fine di garantire un corretto funzionamento della rete, l'Appaltatore dovrà suggerire eventuali modifiche da apportare alle configurazioni degli apparati. Tali modifiche dovranno essere approvate dalla Società prima di essere implementate sugli apparati.

E' compito dell'Appaltatore mantenere aggiornato l'elenco degli apparati a fronte di ogni variazione apportata, e renderlo sempre disponibile alla Società.

Dovrà comunque essere possibile da parte della Società poter effettuare tutte le configurazioni che si rendano necessarie ed opportune. Tutte le attività effettuate autonomamente dalla Società o approvate dalla stessa (per esempio modifiche effettuate da terze parti/fornitori esterni) verranno comunicate anticipatamente all'Appaltatore, che dovrà fornire le sue considerazioni in merito al fine di condividere ed acquisire le modifiche apportate.

Tale attività dovrà essere garantita secondo gli SLA indicati all'art 19.

Art. 16 – SERVIZIO DI ASSISTENZA REMOTA

L'Appaltatore dovrà fornire un servizio di assistenza remoto.

Tale servizio dovrà garantire tutte le attività di supporto remoto in grado di assicurare una rapida risposta alle diverse e complesse esigenze tecniche relative a tutta l'infrastruttura di rete.

Tale attività dovrà essere garantita secondo gli SLA indicati all'art 19.

Art. 17 – SERVIZIO DI UPGRADE DEL SOFTWARE / FIRMWARE DEGLI APPARATI DI RETE

L'Appaltatore dovrà fornire un servizio di upgrade alle versioni superiore del software/firmware degli apparati di rete oggetto della gara.

L'installazione di qualsiasi upgrade sopra indicato dovrà essere sempre congiuntamente valutata e pianificata tra la Società e l'Appaltatore.

Sarà comunque cura dell'Appaltatore informare la Società di qualsiasi nuovo upgrade disponibile. Tale attività dovrà essere garantita secondo gli SLA indicati all'art 19.

Art. 18 – SERVIZIO DI BACKUP / RESTORE DELLE CONFIGURAZIONI DEGLI APPARATI DI RETE

L'Appaltatore dovrà fornire un servizio di backup delle configurazioni degli apparati oggetto della gara Tale attività dovrà essere schedulata mensilmente e a seguito delle seguenti attività:

1. prima e dopo il cambio di una configurazione;
2. prima e dopo la sostituzione di un apparato (se l'apparato risulta raggiungibile);
3. prima e dopo l'upgrade o il downgrade di un firmware;
4. su richiesta espressa dalla Società.

Le copie di backup delle configurazioni dovranno essere conservate adeguatamente dall'Appaltatore sulla base di politiche concordate (vedi art. 21) ed inoltre rese disponibili alla Società.

L'Appaltatore sarà responsabile dell'eventuale attività di restore delle configurazioni ogni qualvolta venga richiesto. Tale attività dovrà essere garantita secondo gli SLA indicati all'art 19.

Art. 19 – SERVIZIO DI CONTROLLO DELLA VULNERABILITÀ

Prima di attivare i servizi di monitoraggio sopra descritti, l'Appaltatore dovrà fornire un servizio di controllo delle vulnerabilità attraverso un'attività di Vulnerability Assessment.

Tale attività dovrà essere costante.

Al temine di ogni attività, l'Appaltatore dovrà produrre un report che dovrà essere messo a disposizione dall'Appaltatore stesso.

Nel caso fossero rilevate delle criticità, l'Appaltatore dovrà contattare immediatamente la Società per presentare i risultati dell'analisi ed eventualmente proporre migliorie per risolvere tali criticità.

Art. 20 – SLA SERVIZI, SLA PROACTIVE MONITORING, SLA MANUTENZIONE ONSITE

Come esplicitato nei precedenti articoli il monitoraggio proattivo remoto deve essere costante e l'Appaltatore si dovrà attivare autonomamente ogni qualvolta si renda necessario secondo gli SLA successivamente esplicitati e secondo le regole esplicitate poi all'art 21.

In ogni caso deve essere operante un service desk che operi H24 dal lunedì alla domenica:

Orari di Servizio (orario locale)	
Servizio	**Lunedì-Domenica**
Service Desk	00:00 – 24:00

Dovrà essere possibile aprire un ticket attraverso almeno 3 canali: un canale telefonico, un indirizzo mail dedicato e attraverso l'accesso all'area dedicata sui sistemi informativi dell'Appaltatore.

L'Appaltatore è responsabile di fornire globalmente i servizi alla Società (in local time), secondo i seguenti periodi:

DESCRIZIONE	Service Level Agreement (SLA)
Network Monitoring – General Services	
Proactive Monitoring	H24 x 365
Network Monitoring Presidiato	H24 x 365
Notifica Automatica degli eventi CRITICI	H24 x 365
Intervallo tra il Polling di ogni apparato per lo STATUS Monitoring	30"
Accesso a info e servizi	24x7

Campionatura minima per la generazione Trend Report	10’
Disponibilità dati raccolti (Trend Report)	Secondo indicazioni della Società
Problem Solving	
Analisi in tempo reale di allarmi ed eventi di rete	La presa in carico deve essere congrua con la criticità dell'evento
Evento Critico	Presa in carico entro 15 min - Risoluzione in 4H
Evento Importante	Presa in carico entro 2h – Risoluzione NBD
Evento Pianificabile	Presa in carico entro 6h - Risoluzione NBD
Escalation supporto specialistico	Entro 1 ora dalla presa in carico
Richiesta verifica anomalia	Presa in carico entro 15 min.
Coinvolgimento terze parti (es. manutenzione, ISP, …)	entro 15 min dal termine dell’analisi del problema.
Incident Tracking	Ogni attività è rintracciabile attraverso un ticket
Configuration Management	
Backup configurazioni apparati	Frequenza mensile (salvo eccezioni). Retention delle ultime 4 versioni
Ripristino configurazione apparati	Entro 1 ora dalla richiesta
Remote Technical Support	
Richiesta analisi configurazione	Presa in carico entro 1 giorno dalla richiesta
Richiesta modifica configurazione	Presa in carico entro 4 ore dalla richiesta
Richiesta verifica configurazione	Presa in carico entro 4 ore dalla richiesta
Aggiornamento firmware apparati	Presa in carico entro 1 giorno dalla richiesta
Controllo/verifica di tipo “informativo”	Presa in carico entro 2 giorni dalla richiesta
Modifica elenco oggetti monitorati	Presa in carico entro 2 giorni dalla richiesta
Wireless Monitoring – General Services	
Analisi in tempo reale di allarmi ed eventi di rete	H24 x 356
Accesso Mappa Copertura Wireless	H24 x 356
Status soluzione Wireless / interferenze	H24 x 356

Anche il servizio di manutenzione / interevento On - Site degli apparati dovrà essere garantito 24H su 24H e rispettare i seguenti SLA:

Core Switch	**Pianificabile**	**Importante**	**Critico**
Intervento on-Site riparazione/sostituzione/ripristino	NBD	NBD	4h

Distribution Switch e Apparati Wireless	**Pianificabile**	**Importante**	**Critico**
Intervento on-Site riparazione/sostituzione/ripristino	NBD	NBD	4h

Firewall	**Pianificabile**	**Importante**	**Critico**
Intervento on-Site riparazione/sostituzione/ripristino	NBD	NBD	4h

Qualora i servizi erogati dovessero subire un'interruzione, qui sopra sono previsti e definiti i livelli di servizio (SLA) che la Società intende ricevere dall’appaltatore; gli SLA diverranno ufficialmente operativi a partire dalla fine della fase di transizione.

Di seguito sono dettagliate le definizioni di gravità, da intendersi software (configurazione ad es.) e hardware:

Critico: è un problema bloccante per tutti o per un gruppo di utenti che non sono in grado di usufruire di un servizio per indisponibilità dello stesso o perché le sue prestazioni risultano decisamente degradate.

Importante: qualsiasi evento che non necessita di un intervento urgente in quanto causa un degrado di prestazioni del servizio tollerabile e per periodi limitati;

Pianificabile: qualsiasi evento di bassa priorità la cui risoluzione può essere pianificata.

Come si evince dalle tabelle che si tratti di guasto / problema di livello critico a livello hardware e /o software la risoluzione del problema (che essa avvenga tramite sostituzione dell'apparato o altro intervento) deve avvenire entro 4H dalla presa in carico. Per tutto il resto, data la ridondanza di tutta l'infrastruttura si ritiene che il problema non critico possa essere risolto il giorno lavorativo successivo. Resta facoltà della Società richiedere una escalation del problema da pianificabile / importante a Critico per ripercussioni che solamente il personale della Società può valutare correttamente.

Ogni ritardo sugli SLA deve essere motivato e giustificato in forma scritta, altrimenti la Società attiverà l'eventuale applicazione di penali, come definito nel CSA-NG.

Se durante il periodo di garanzia un materiale o dispositivo dimostra di essere difettoso per motivi di fabbricazione e il difetto risulta non essere correggibile attraverso la consueta manutenzione l'Appaltatore è responsabile della sostituzione dello stesso materiale/dispositivo con un altro con caratteristiche simili, come definito nelle specifiche pertinenti senza alcun costo per la Società.

Inoltre, l'Appaltatore è responsabile dell'integrità di tutti i dati che sono memorizzati sui dispositivi da lui gestiti. In dettaglio l'Appaltatore è indicato come responsabile della corruzione dei dati, quando l'integrità manca a causa di un guasto hardware / software, bug software, manomissioni da parte del personale dell'Appaltatore, cattiva manutenzione, errori a causa di mancata osservanza di procedure, migliori pratiche, indicazioni scritte da parte della Società, etc.); l'hardware gestito rientra nel perimetro di responsabilità.

L'Appaltatore dovrà fornire accesso a tutte le informazioni relative ai servizi sopradescritti in qualsiasi momento e su qualsiasi richiesta della Società. La modalità con cui fornire l'accesso a queste informazioni è lasciata all'Appaltatore. Si dovrà poter accedere specificatamente alle seguenti informazioni/servizi:

1. informazioni in tempo reale dello stato degli apparati di rete e sicurezza;
2. trend-report dei parametri monitorati;
3. visualizzazione in tempo reale e storica degli eventi/log raccolti;
4. copia delle configurazioni;
5. documentazione operative;
6. servizi attivi;
7. rintracciabilità richieste/attività effettuate;
8. apertura richieste.

L'Appaltatore si impegna a stabilire e mantenere adeguato personale qualificato operante presso i vari ambiti secondo il perimetro oggetto del presente documento (cioè, la gestione e il personale di supporto) per fornire i seguenti servizi di gestione dell'infrastruttura per la Società. E' obbligatorio che l'Appaltatore fornisca il servizio basandosi sulla funzione di Service Desk completamente formalizzata e operativa presso la sua sede, che impieghi il concetto di "SPOC" (Single Point of Contact) per tutte le richieste (ticket) aperte dal canale della Società o dal canale del monitoraggio proattivo. L'Appaltatore gestirà per conto della Società ed in coordinamento con il Service Manager della Società i processi necessari per fornire il servizio, compresi, ma non limitati a, quelli elencati qui sotto e che saranno ulteriormente definiti sviluppati e documentati nella fase di start-up:

- Operations (patching)

- Hardware and Facilities Planning
- Configuration Management
- Change Management
- Performance Management
- Capacity Planning
- Problem Management
- Installation and Maintenance Services
- Availability Management
- Data Management & Data Backup
- Data Communication Software Support and Operations
- Identity Management

a) deve dimostrare che, al fine di garantire lo SLA / SLO richiesto, un piano di Disaster Recovery (DRP) è formalmente stabilito e mantenuto, in cui sono documentati i requisiti di backup dei dati, conservazione e ripristino per l'infrastruttura IT oggetto del presente documento;

b) esaminerà e aggiornerà il DRP dopo ogni test periodico o come richiesto dai processi di Business, o a seguito di modifiche tecniche sull'infrastruttura, o cambiamenti sostanziali in ambito Servizi, allo scopo di mantenere allineate le strategie ed i relativi piani di Disaster Recovery della Società e dell'Appaltatore.

c) attivare il piano di DR su dichiarazione di disastro (stato di crisi).

L'Appaltatore manterrà allineati i controlli di sicurezza con le Politiche di Sicurezza definite dalla Società dalla data in cui inizi a prestare i servizi ("Data di Efficacia") concordata in sede di start-up.

Art. 21 – LINGUA

Tutti i servizi verranno forniti nelle seguenti lingue (in ordine di importanza):

- Italiano
- Inglese

Tutta la documentazione necessaria deve essere fornita sia in lingua italiana che inglese.

Art. 22 – CARATTERISTICHE DELL'APPALTATORE, STRUTTURA E MODELLO ORGANIZZATIVO

E' preciso onere e obbligo dell'operatore economico o dell'eventuale subappaltatore dimostrare di usare i processi quotidiani di governo necessarie in materia di gestione dei servizi (ISO/IEC 20000) il cui perimetro e le persone impiegate sono inclusi nell'offerta e di possedere la certificazione ISO 27001 inerente il perimetro oggetto del presente appalto e di applicarla correttamente.

Tali certificazioni sono obbligatorie per la parte di organizzazione e gestione del servizio (monitoraggio, assistenza, gestione collaborativa) non per la parte di fornitura.

Modello Organizzativo Suggerito per la governance del progetto

"L'IT Governance è parte integrante della gestione aziendale e si compone di strutture organizzative e di processi che assicurano che l'IT supporti la strategia dell'Azienda e concorra al raggiungimento degli obiettivi di business".

Questa definizione assume un'importanza ancora maggiore quando una società intraprende il percorso che persegua l'outsourcing strategico.

La Società quindi chiede all'Appaltatore di impegnarsi nella realizzazione di una struttura di governance del progetto basata su:

- Un modello di interazione basato su tre livelli (strategico, tattico e operativo);
- Una serie di processi formalizzati e condivisi;
- Un'organizzazione con ruoli e responsabilità precise e ben definite (vedi matrice RACI).

Governance Team

L'Appaltatore è invitato a fornire almeno i seguenti ruoli (o equivalenti):

- Project Executive:

Lui/lei ha la responsabilità diretta e specifica per verificare il raggiungimento degli obiettivi del contratto. Lui/lei ha il potere di rappresentare l'Appaltatore e assume gli obblighi in relazione a tutti gli aspetti del contratto. Lui/lei fa parte del Comitato Direttivo e partecipa alle riunioni con i rappresentanti della Società.

L'Appaltatore deve presentare una certificazione in ambito Project Management, che sarà utilizzata in questo progetto (persone, perimetro).

- Service Delivery Manager

Lui/lei è responsabile della fornitura di servizi alla Società in funzione della qualità e degli obiettivi di servizio concordati nel contratto. Rappresenta il principale punto di riferimento per tutte le questioni relative al servizio durante l'intera durata del contratto. Ha la responsabilità di identificare i modi per migliorare il servizio e la "soddisfazione del cliente" e di raccomandare al Project Executive le relative iniziative. Funge da interfaccia per la Società per la gestione di tutti i requisiti tecnici, assistenza e supporto. Interfaccia lo staff dedicato al delivery. Autorizza le modifiche dopo averle validate. Sviluppa soluzioni per le richieste di servizio. Svolge un ruolo attivo nello sviluppo di azioni correttive e del loro follow-up, in relazione alle questioni chiave che riguardano le prestazioni del servizio. Fornisce la segnalazione sui livelli di servizio. Analizza i reports e propone ottimizzazioni per migliorare la qualità del servizio. Pianifica e conduce le riunioni di gestione.

- Security Coordinator

Lui/lei è responsabile per l'attivazione dei Controlli di Sicurezza concordati. Analizza le richieste di modifica alle Politiche di Sicurezza. Informa la Società circa la fattibilità del cambiamento e sui possibili effetti connessi e collaterali. Coordina le relazioni e le attività con le terze parti (fornitori, consulenti, etc.) relative ai controlli di sicurezza. Gestisce i possibili problemi di sicurezza e gli incidenti e coordina le attività di soccorso e di bonifica, quando necessario. Lui/lei sarà disponibile in tutte le circostanze di eventuali gravi problemi legati alla sicurezza.

Coordinamento

L'Appaltatore e l'Impresa predisporranno un gruppo di coordinamento, composto da ruoli operativi provenienti da entrambe le società.

Il gruppo di coordinamento è responsabile della preparazione, la gestione e l'organizzazione tecnica dei contenuti del servizio. Il team di Governance organizza incontri periodici per il coordinamento e le esecuzioni del servizio. L'Appaltatore si impegna a proporre fin da subito il calendario delle periodicità.

Documentazione Operativa

Prima dell'inizio formale dell'Appalto, l'Appaltatore produrrà e condividerà un manuale operativo, in modo che:

- Fornisca un elenco di alto livello dei processi che sono inclusi nel servizio (ad esempio, Change Management, Incident Management, Problem Management, ecc.);
- Sia utilizzato dall'Appaltatore per condurre le attività costituenti il servizio;

- Identifichi ogni processo, i ruoli ed i punti di contatto in materia;
- Descriva le interazioni tra la Società, l'Appaltatore e le terze parti durante la prestazione del servizio;
- Contenga i dettagli tecnici dell'architettura hardware e software su cui si basa il servizio.

Il manuale in parola sarà ulteriormente dettagliato ed approvato dalla Società entro un mese dalla data ufficiale di avviamento del servizio, e conterrà tutti i dati necessari che sono considerati utili per gestire con successo reciproco il servizio stesso.

L'Appaltatore si impegna a:

1. creare, aggiornare e gestire i manuali operativi per ogni hardware e software incluso nel servizio, in reciproca collaborazione con il coordinatore del servizio della Società;

2. chiedere l'approvazione della Società prima di aggiungere o modificare qualsiasi clausola nei manuali;

3. verificare che la documentazione relativa alle operazioni sia conforme alle norme e procedure operative;

4. comunicare periodicamente al personale competente della Società tutte le informazioni relative ai compiti e procedure nuove o modificate;

5. aggiornare la documentazione relativa al Service Desk, inserirla nel manuale operativo e distribuirla al proprio personale ed al personale della Società;

6. fornire i manuali nei formati e attraverso il supporto richiesto dalla Società.

Processi di IT Governance

L'Appaltatore erogherà alla Società, e le Parti si accorderanno mutualmente per definire ed utilizzare, i seguenti processi di IT Governance per la gestione dei servizi. I processi di gestione manutenzione e processi di Service Delivery, elencati di seguito, saranno ulteriormente definiti nel Manuale delle Operazioni e saranno comuni per tutto l'IT, comprendente sia le infrastrutture che le applicazioni; qualora dovessero essere necessari requisiti particolari, questi saranno dettagliati solo laddove necessario.

Quindi, saranno definiti e impiegati, tra gli altri, i seguenti processi di gestione di servizio:

- Change Management;
- Incident Management & Escalation Management;
- Problem Management;
- Measurements and Reporting;
- Service Level Management;
- Availability Management (Business Continuity Management);
- Project Management;
- Asset management;
- Configuration Management;
- Capacity Planning;
- Network management - LAN / WAN;
- Database Management;
- IT Security Management Network Management;
- Operations Management;

- Performance Management;
- Technology Strategy and Refresh Management;
- User ID Administration.

Perimetro del Servizio

Il Servizio sarà composto da più livelli di gestione, che idealmente saranno individuati in:

• un Centro di Produzione del Servizio, centralizzato presso l'Appaltatore, da cui lo stesso fornirà il servizio e dove lo stesso ha stabilito e manterrà i suoi sistemi tecnologici operativi.

• un Centro per la Gestione del Servizio, remota e centralizzata presso l'Appaltatore, da dove il personale svolge la sua attività amministrativa, operativa, di coordinamento e di controllo del servizio, utilizzando un insieme integrato di strumenti orientati al controllo dei processi coinvolti.

Gestione della Sicurezza e delle Politiche di Sicurezza

L'Appaltatore lavorerà con la Società per dettagliare i controlli di sicurezza esistenti della Società e, se necessario, svilupperà un documento dettagliato nel quale verranno definiti i controlli di sicurezza stabiliti di comune accordo, e che l'Appaltatore implementerà per la Società. Tale documento prevede, come minimo, la definizione delle responsabilità in ambito sicurezza elencate di seguito. La Società riconosce che per l'erogazione dei Servizi richiesti, l'Appaltatore viene autorizzato all'accesso alle reti della Società.

E' richiesto che venga fornito, e costituisca parte integrale dei servizi richiesti, un servizio di gestione delle identità (Identity Management).

La Società e l'Appaltatore, durante la fase di start-up dei servizi, discuteranno, si accorderanno e documenteranno i dettagli relativi all'ambito Sicurezza (es. Security Policies, controlli sulla sicurezza, ruoli e responsabilità).

E' richiesto all'Appaltatore di:

a) fornire un focal-point con responsabilità sulle Politiche di Sicurezza ed i relativi controlli;

b) con l'assistenza della Società, raccogliere informazioni per documentare i controlli di sicurezza che la stessa ha in essere alla "Data di Efficacia", concordare la Baseline IT Security della Società e definire e documentare le specifiche tecniche per i sistemi gestiti dall'Appaltatore, che saranno oggetto di rivisitazione (audit) periodica;

c) eseguire una gap-analysis tra i controlli di sicurezza che la Società ha in essere alla "Data di Efficacia" e la loro corrispondenza documentale;

d) fornire una sintesi iniziale di identificazione delle minacce rilevata dai risultati della gap-analysis ed aggiornare il report "identificazione delle minacce" ogni dodici (12) mesi. Tale sintesi conterrà:

- le minacce individuate, organizzate secondo la normativa ISO27001:2013;
- le azioni correttive suggerite per ciascuna minaccia individuata;

e) assicurare che tutti gli asset gestiti dall'Appaltatore ed i relativi servizi siano posizionati all'interno del campo di applicazione (scope) della normativa ISO27001:2013.

f) con l'aiuto della Società, sviluppare ed implementare il documento di sicurezza che viene utilizzato per normare/definire le politiche di sicurezza e i controlli tecnici previsti e supportati dalla Security Compliance dell'Appaltatore;

g) attuare, come richiesto dalla Società, tutti i controlli di sicurezza (come indicato nel Documento Informativo Controlli di sicurezza che sarà fornito durante la fase di configurazione), su tutti i sistemi e reti gestite dall'Appaltatore;

h) definire e tracciare nel documento di Information Security Controls, tutti gli ID utente privilegiati insiti nelle piattaforme (hardware e software);

i) attuare una procedura che, in base alle soluzioni tecnologiche adottate, consenta di monitorare correttamente i diritti sui dati della Società;

e) su base periodica e secondo gli intervalli definiti in fase di start-up, rivisitare ed aggiornare, assieme alla Società, il documento dei controlli di sicurezza.

Da parte sua, la Società si impegna a:

a) fornire un focal-point responsabile della Politica di Sicurezza e di Controllo;

b) assistere l'Appaltatore nel documentare i controlli di sicurezza che la Società ha in essere alla "Data di Efficacia";

c) fornire un contatto, le politiche di sicurezza e le informazioni sulle infrastrutture IT e tutti gli aggiornamenti/modifiche che dovessero essere eseguiti;

d) assistere l'Appaltatore nello sviluppo del documento dei controlli di sicurezza;

e) assegnare i ruoli e le responsabilità, come indicato nella documentazione concordata;

f) esaminare il riepilogo individuazione delle minacce e prendere i provvedimenti, a seconda dei casi;

g) su base periodica, rivisitare il documento dei controlli di sicurezza assieme all'Appaltatore, e fornire gli aggiornamenti consigliati, a seconda dei casi.

Gestione dell'IS Audit

L'Appaltatore si impegna a:

a) autorizzare la Società ad effettuare Audit sulle infrastrutture e sui servizi inclusi nel perimetro oggetto della presente;

b) fornire un focal-point con la responsabilità di supportare gli IS Audit;

c) fornire assistenza alle attività di auditing, per un massimo di due Audit all'anno;

d) comunicare e rispondere alle richieste di Audit;

e) facilitare gli Audit e le revisioni periodiche ai sistemi e servizi;

f) fornire attività di supporto ed indirizzo per le attività di audit di prima, seconda e terza parte;

g) coordinare le attività per la risoluzione delle criticità individuate durante il processo di audit della sicurezza e fornire raccomandazioni per la risoluzione;

h) fornire il nome degli strumenti utilizzati per effettuare gli audit;

i) fornire evidenza di qualche caso aziendale (accaduto) e il supporto (documentato) fornito.

Da parte sua, la Società si impegna a:

a) fornire un focal-point responsabile per i controlli di sicurezza;

b) durante il periodo di verifica congiunta, effettuare una revisione delle autorizzazioni di accesso al sistema di ciascun utente, per confermare la necessità di utilizzo degli stessi requisiti di accesso, successivi alla "Data di Efficacia", e allineare l'Appaltatore su qualsiasi modifica effettuata/richiesta;

c) fornire all'appaltatore (se disponibile) lo storico di audit della sicurezza (sia politiche, standard interni ed esterni) e le pratiche in vigore alla "Data di Efficacia" e tutti gli aggiornamenti che si verificano. La Società si riserva a sua discrezione di incaricare un fornitore terzo per eseguire un audit degli standard di sicurezza IT in uso e verificare l'esecuzione / realizzazione degli stessi.

Change Management e Custodia dei Dati

Se le esigenze cambiano nel corso del contratto di servizio, la modifica verrà gestita attraverso il processo di Change Management.

Qualsiasi cambiamento nel dimensionamento (la capacità disponibile) sarà discussa con il focal-point della Società e verrà gestito tramite la procedura di Change Management.

In ogni caso, L'Appaltatore si impegna ad incontrarsi con i referenti del Servizio della Società, con cadenza almeno semestrale, per stabilire un piano e dare seguito alle necessarie attività che risiedono nel processo di Manutenzione Evolutiva.

Inoltre, l'Appaltatore è responsabile dell'integrità di tutti i dati che sono memorizzati sui dispositivi da lui gestiti. In dettaglio, l'Appaltatore è indicato come responsabile della corruzione dei dati, quando l'integrità manca a causa di un guasto hardware / software, bug software, manomissioni da parte del personale dell'Appaltatore, cattiva manutenzione, errori a causa di mancata osservanza di procedure, migliori pratiche, indicazioni scritte da parte della Società etc.); l'hardware gestito rientra nel perimetro di responsabilità.

Licenze

- Licenze: l'Appaltatore sarà responsabile di fornire tutte le eventuali licenze di software che si rendessero necessarie per la corretta fornitura di tutti i servizi richiesti e manutenute per tutta la durata dell'appalto.

L'Appaltatore dovrà garantire che quanto fornito (servizi, infrastrutture, sistemi) sia rispondente alla vigente normativa in ambito Privacy.

Art. 23 – CONSULENZA E GIORNATE SPECIALISTICHE

La Società si è dotata da tempo di un sistema interno in grado di monitorare le risorse hardware e software: sarà onere dell'Appaltatore fornire su richiesta della Società tutto il supporto possibile al fine di inserire i nuovi sistemi (HW e SW) oggetto del presente CSA all'interno di questo sistema di monitoraggio.

Dovranno inoltre essere previste delle giornate di consulenza specialistica, tenute da personale certificato della soluzione proposta per l'intera durata del contratto, da pianificare su richiesta della Società. Il fabbisogno individuato dalla Società è di 30 giornate.

Dal momento della richiesta, l'attività dovrà essere svolta entro 10 giorni lavorativi.