PROGETTO DEFINITIVO

E CAPITOLATO TECNICO

RETE LAN - WLAN

DA REALIZZARE PRESSO

ISTITUTO COMPRENSIVO STATALE
64° "RODARI-MOSCATI"
NAPOLI

AVVISO PUBBLICO 20480 del 20 Luglio 2021
per la realizzazione di reti locali, cablate e wireless nelle scuole
Azione 13.1.1 "Cablaggio Strutturato e sicuro all'interno degli edifici scolastici"

CNP: 13.1.1A-FESRPON-CA-2022-2

CUP: E69J21011800006

CIG: ZE336330FBC

Allegati:
ALLEGATO 1: Piano di installazione degli Access Point con stima della copertura radio.

Data: _____

Ing. Francesco Auriemma

Ing. Francesco Auriemma – P.IVA: 09999911218 - Studio: Via Cupa di Nola, 145 – 80049 – Somma Vesuviana (Na)
cell.: 3382803114 - PEC: francesco.auriemma@ordingna.it – PEO: f.auriemma@isfea.it

SOMMARIO

1. PREMESSA 3
2. TIPOLOGIE DI INTERVENTO 3
3. CARATTERISTICHE DEI BENI E SERVIZI 4
4. DESCRIZIONE DEGLI AMBIENTI 4
5. DESCRIZIONE DELLA RETE ESISTENTE 5
5.1 Plesso Moscati 5
5.2 Plesso Rodari e Plesso Picasso 5
5.3 Plesso Van Gogh e Plesso Chagall 5
6. FORNITURE E SERVIZI RICHIESTI 6
7. DETTAGLIO DELLA FORNITURA 7
7.1 Tracciatura e identificazione dei cablaggi esistenti 7
7.2 Fornitura in opera di nuovi Switch per AP 7
7.3 Switch Ethernet 7
7.4 UPS per protezione Rack 7
7.5 CABLAGGIO IN RAME 8
8. DISTRIBUZIONE CABLAGGI 9
9. NUOVO SISTEMA WIFI 10
9.1 Access Point per interni: Caratteristiche Tecniche 10
9.2 Access Point: Autenticazione 11
9.3 SISTEMA DI GESTIONE WIFI 12
9.4 SISTEMA HARDWARE DI GESTIONE E CONTROLLO A.P. IN CLOUD 12
10. DISTRIBUZIONE ACCESS POINT 13
11. SERVIZI DI SICUREZZA 14
11.1 Sicurezza Perimetrale “Firewall” 14
11.2 Firewall: Specifiche tecniche 15
11.2.1 Specifiche tecniche HW “Firewall” 15
11.2.2 Specifiche tecniche SW di BASE 15
11.3 Licenze e Servizi di Sicurezza 16
11.3.1 Servizio di Monitoring e Log 17
12. RIEPILOGO DELLA FORNITURA 18
12.1 Elenco riepilogativo della fornitura Plesso Moscati 18
12.2 Elenco riepilogativo della fornitura Plesso Rodari 18
12.3 Elenco riepilogativo della fornitura Plesso Picasso 19
12.4 Elenco riepilogativo della fornitura Plesso Van Gogh 19
12.5 Elenco riepilogativo della fornitura Plesso Chagall 20
12.6 Elenco della fornitura alla voce “Servizi Accessori” (per tutti i plessi) 20
13. Servizi accessori (specifiche) 20
14. Glossario 21

1. PREMESSA

Il presente documento integra il progetto definitivo e il capitolato tecnico della rete LAN/WLAN da realizzare presso l'Istituto Comprensivo "Rodari - Moscati" di Napoli. Il progetto ha come obiettivo principale quello di garantire una connettività veloce, stabile e sicura, sia per gli uffici amministrativi che per le aule didattiche e i laboratori.

Gli interventi faranno uso sia di tecnologie Wired (cablaggio) che Wireless (WiFi) e riguarderanno tutti i plessi scolastici, ma saranno diversificati in relazione alle esigenze e allo stato di efficienza della rete attualmente in esercizio.

L'intervento ha lo scopo di promuovere il superamento degli effetti della crisi nel contesto della pandemia di COVID19 e delle sue conseguenze sociali e preparare una ripresa verde, digitale e resiliente dell'economia (REACT-EU), nell'ambito del Programma operativo nazionale "Per la scuola, competenze e ambienti per l'apprendimento" 2014-2020 – Fondo europeo di sviluppo regionale (FESR). L'intervento è, altresì, ricompreso all'interno del complessivo Piano nazionale di ripresa e resilienza (PNRR), di cui al regolamento UE n. 2021/241 del Parlamento europeo e del Consiglio del 12 Febbraio 2021.

2. TIPOLOGIE DI INTERVENTO

Gli interventi ammissibili prevedono la realizzazione o il potenziamento delle reti locali cablate e wireless degli edifici scolastici, utilizzate dalle scuole a fini didattici e amministrativi, comprensivi di fornitura di materiali e strumenti per la realizzazione di cablaggi strutturati, fornitura e installazione di apparati attivi, switch, prodotti per l'accesso wireless, dispositivi per la sicurezza delle reti e servizi, compresi i dispositivi di autenticazione degli utenti (personale scolastico e studenti), fornitura e installazione di gruppi di continuità, posa in opera della fornitura ed eventuali piccoli interventi edilizi strettamente indispensabili e accessori.

Gli interventi devono assicurare il cablaggio degli spazi didattici e amministrativi delle scuole, consentire la connessione alla rete, in modalità wired e/o wireless, dei dispositivi utilizzati dai docenti, dal personale scolastico, dalle studentesse e dagli studenti, anche attraverso la gestione e autenticazione degli accessi, nel rispetto delle norme vigenti in materia di accessibilità ai sistemi informatici e telematici della Pubblica Amministrazione, di tutela della privacy e di sicurezza informatica dei dati, nonché delle norme vigenti in materia di protezione dell'ambiente e di risparmio energetico.

Questo progetto "RETI" ha i seguenti obiettivi:

- Tracciare ed identificare il cablaggio esistente
- Bonificare e sistemare gli armadi rack esistenti
- Ampliare, adeguare e armonizzare la rete cablata esistente
- Migliorare e ampliare la copertura della Rete WiFi
- Installare dispositivi di protezione elettrica per gli apparati di networking
- Irrobustire il sistema di sicurezza, o realizzarne uno nuovo
- Attivare un servizio di monitoraggio e manutenzione della rete

3. CARATTERISTICHE DEI BENI E SERVIZI

Le apparecchiature oggetto della fornitura devono essere in possesso delle certificazioni riconosciute dall'**Unione Europea** ed essere conformi alle norme relative alla compatibilità elettromagnetica. La conformità deve essere estesa alle ultime disposizioni internazionali e norme vigenti ai fini della sicurezza degli utilizzatori. Tra queste si ricorda che gli impianti realizzati devono rispettare le norme sulla sicurezza e affidabilità degli impianti (L. 37/08).

Questo capitolato prevede la fornitura "*chiavi in mano*" e cioè il prezzo offerto deve essere comprensivo di IVA, imballaggio, trasporto, facchinaggio oltre ai servizi descritti in fondo al documento.

Tutte le apparecchiature dovranno essere di primaria marca e devono essere fornite almeno delle caratteristiche tecniche funzionali minime indicate nella tabella che segue e risultare dai datasheet e/o dépliant e certificazioni da allegare all'offerta.

Non verranno prese in considerazioni offerte tecnicamente incongrue o in contrasto con le caratteristiche indicate nel "dettaglio della fornitura" indicate nelle pagine seguenti

4. DESCRIZIONE DEGLI AMBIENTI

Gli ambienti di riferimento e oggetto delle opere per la realizzazione della Rete Wireless e Wired (cablata), opere accessorie e relativa configurazione sono:

Plesso Rodari

- Piano Terra (Uffici, aule e laboratori)
- Piano Primo (Aule e laboratori)
- Secondo Piano (Aule e laboratori)

Plesso Moscati

- Piano Terra (Uffici, aule e laboratori)
- Piano Primo (Aule e laboratori)

Plesso Picasso

- Piano Terra (Uffici, aule e laboratori)
- Piano Primo (Aule e laboratori)
- Secondo Piano (Aule e laboratori)

Plesso Van Gogh

- Piano Terra (Aule e laboratori)

Plesso Chagall

- Piano Terra (Aule e laboratori)

5. DESCRIZIONE DELLA RETE ESISTENTE

A valle del sopralluogo effettuato, in tutti plessi sopra descritti, si rilevano le seguenti situazioni comuni:

- Il cablaggio è privo di mappatura;
- Nonostante sia disponibile una linea in Fibra FTTH, gli apparati (attivi e passivi) non riescono a sfruttare in modo efficace le potenzialità di tale tecnologia

Di seguito si riporta una sintesi sullo stato dei singoli Plessi con lo scopo di descrivere, laddove esistenti la tipologia dell'infrastruttura di rete sia cablata che Wireless.

5.1 Plesso Moscati

- esiste un cablaggio di tipo U/UTP Cat.5 a servizio della sola zona amministrativa posta al piano terra, ma le aule non sono cablate;
- è attiva una rete Wireless realizzata mediante Access Point installati a vista nei corridoi e distribuiti in modo da servire le aule. Infatti, le lezioni della didattica sono svolte mediante la rete WiFi dell'istituto.
- La suddetta rete wireless, attualmente in uso, risulta tecnologicamente datata, poco performante, non idonea alle nuove esigenze operative degli utenti e non garantisce la copertura di alcune aree nevralgiche dell'istituto.
- Gli apparati di attivi di networking sono tecnologicamente datati ed inoltre non esiste un sistema di sicurezza perimetrale.

5.2 Plesso Rodari e Plesso Picasso

- Per entrambi i plessi **non** esiste un cablaggio di tipo U/UTP Cat.5 a servizio della sola zona amministrativa posta al piano terra, ma le aule non sono cablate;
- è attiva una rete Wireless realizzata mediante Access Point installati a vista nei corridoi e distribuiti in modo da servire le aule. Infatti, le lezioni della didattica sono svolte mediante la rete WiFi dell'istituto.
- La suddetta rete wireless, attualmente in uso, risulta tecnologicamente datata, poco performante, non idonea alle nuove esigenze operative degli utenti e non garantisce la copertura di alcune aree nevralgiche dell'istituto.
- Gli apparati di attivi di networking sono tecnologicamente datati ed inoltre non esiste un sistema di sicurezza perimetrale.

5.3 Plesso Van Gogh e Plesso Chagall

Per entrambi i plessi non esiste un cablaggio e non risulta attiva alcuna rete Wireless.

6. FORNITURE E SERVIZI RICHIESTI

L'idea alla base di questo progetto è di utilizzare parte dell'infrastruttura esistente ad esempio le [1]PDL per i devices di tipo fisso (Computer, LIM, Stampanti, etc.) e per i [2]CWF per i devices mobili (Smartphone, Laptop, Tablet, etc.), e di sostituire tutta la parte tecnologica (Switch, Firewall e AP) esistente. Contestualmente, si procederà alla realizzazione del cablaggio per le aule (che ne sono sprovviste) e per gli AP al fine di ampliare la copertura radio rispetto a quella esistente.
Inoltre sarà implementato un nuovo Sistema di Sicurezza Perimetrale "Firewall".
In altre parole, il progetto punta ad ottenere la massima efficienza e copertura dei plessi in termini di connettività, compatibilmente con il piano economico-finanziario approvato.
Di seguito si elencano i punti principali del progetto:

1. Ottimizzazione dei cablaggi esistenti;
2. Tracciatura e identificazione dei cablaggi esistenti;
3. Fornitura di nuovi cablaggi e nuove PDL ove necessario;
4. Fornitura in opera di nuovi Switch per il collegamento dei nuovi AP e delle PDL;
5. Fornitura in opera di un sistema di backup e protezione elettrica dei Rack;
6. Fornitura di nuovi gli Access Point di ultima generazione per ampliare/ottimizzare la copertura WiFi;
7. Fornitura Firewall di ultima generazione provvisti dei Servizi di Security adeguatamente configurati e personalizzati secondo i dettami dell'amministratore di rete o responsabile della scuola.

Nelle pagine che seguono vengono descritti i dettagli della fornitura e le specifiche minime dei prodotti richiesti

[1] Postazione di Lavoro
[2] Cablaggio per Access Point

7. DETTAGLIO DELLA FORNITURA

Si richiede l'eliminazione dei dispositivi in disuso o comunque non più necessari alla funzionalità della rete, è richiesto altresì l'adeguamento dei Rack con ottimizzazione degli spazi e l'adeguamento del cablaggio interno.

7.1 Tracciatura e identificazione dei cablaggi esistenti

Dovranno essere identificati ed etichettati sia i componenti passivi (cavi, patch panel, permute, etc.) che quelli attivi (switch, router, firewall, AP). Il tutto dovrà essere riportato in un'apposita scheda tecnica e le info raccolte digitalizzate e inserite in DB (Excel, PDF) da consegnare in formato elettronico a fine lavoro.

7.2 Fornitura in opera di nuovi Switch per AP

Si richiede la fornitura di Switch L2 a supporto degli AP questi dovranno essere di tipo Managed con 8 o 24 porte Gigabit Ethernet PoE (802.3at/802.3af compliant) con 2 o 4 porte SFP per una connettività veloce con diverse nuove funzioni di commutazione e gestibili via Cloud in modo gratuito. I nuovi AP destinati alla copertura delle Aule dovranno essere collegati a questi Switch che andranno installati nei Rack esistenti o (dove necessario) nei nuovi Rack da fornire. Gli Switch dovranno essere forniti in opera comprensivi di accesso al Cloud di gestione.

7.3 Switch Ethernet

Si richiede la sostituzione degli Switch esistenti di tipo Fast Ethernet (10/100 Mbps), questi dovranno essere sostituiti con apparati di ultima generazione che dovranno essere installati e configurati. Gli Switch previsti a supporto delle LIM o Digital Board o comunque devices che utilizzano il cavo Ethernet dovranno essere L2 di tipo Managed con 8 o 24 porte Gigabit Ethernet con 2 o 4 porte SFP per una connettività veloce con diverse nuove funzioni di commutazione e gestibili via Cloud in modo gratuito. I nuovi Switch destinati alla copertura delle Aule/Laboratori/Uffici dovranno essere installati nei Rack esistenti o (dove necessario) nei nuovi Rack da fornire. Gli Switch dovranno essere forniti in opera comprensivi di accesso al Cloud di gestione.

7.4 UPS per protezione Rack

A bordo di ciascun armadio Rack è richiesto l'installazione di un dispositivo in grado di fornire alimentazione di emergenza e protezione da sovratensioni per gli apparati di networking (switch, firewall). Il dispositivo fornirà l'alimentazione di emergenza tramite batterie durante i black-out e protezione da sovratensioni per evitare i danni causati dai fulmini o dalle fluttuazioni della rete accidentali. I nuovi UPS (comprensivi di ripiano d'appoggio) saranno posizionati nei Rack di Distribuzione. Gli UPS dovranno avere le seguenti caratteristiche minime:
Potenza erogata Watt: 600 VA - Prese: 6 prese tipo Schuko.

7.5 CABLAGGIO IN RAME

Laddove necessario si dovrà realizzare un cablaggio (destinato sia ai devices ethernet che agli Access Point) utilizzando tecnologie moderne con materiali di alta qualità ed elevate prestazioni. Tutti i prodotti per la parte di cablaggio relativa ai componenti passivi, dovranno essere conformi alle normative vigenti per quanto riguarda la sicurezza e le emissioni/compatibilità elettromagnetica e marcatura CE.

Gli elementi di cablaggio orizzontale e verticale dovranno essere certificati e conformi alle indicazioni minime degli standard di riferimento.

Le caratteristiche dovranno rispettare i seguenti requisiti minimi:

- Prestazioni adeguate alle esigenze attuali e possibilità di seguire le evoluzioni tecnologiche;
- Semplicità di gestione, manutenzione ed espansione della rete;
- Conformità alle raccomandazioni nazionali ed internazionali in relazione sia al materiale utilizzato sia delle procedure d'installazione, certificazione e collaudo adottate;
- Supporto di protocolli standard di comunicazione;
- Conformità rispetto alle raccomandazioni fisiche ed elettriche indicate nelle norme Europee ed Internazionali quali CPR (EN 50575), CEI-UNEL 35016, CEI 64-8, EN 50173-1, ISO/IEC 11801 2nd edition ed ANSI/TIA/EIA 568.Il sistema di cablaggio orizzontale dovrà prevedere il collegamento di distribuzione orizzontale che partendo dall'armadio a rack di piano raggiunge in maniera stellare la postazione di lavoro;

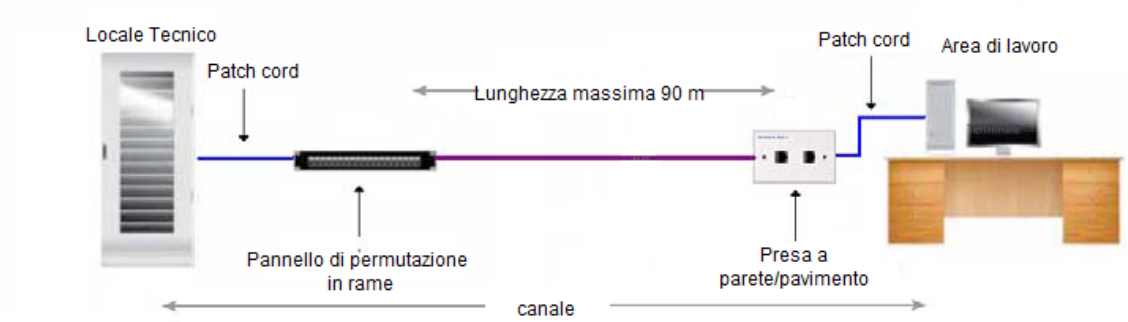
I cablaggi per le PDL o per i CWF dovranno essere realizzati con cavo in rame di tipo non schermato U/UTP Cat.6 costituito da 4 coppie intrecciate con conduttori a filo solido temprati a sezione circolare 24 AWG. I cavi saranno posati in canalizzazione preesistente oppure, dove necessario, tramite canalizzazione realizzata mediante canaline in PVC.

I cavi rame saranno connettorizzati con connettori RJ45 Cat.6.

Ciascuna postazione dovrà essere fornita con la seguente configurazione minima:

- Nr.1 - Cavo U/UTP Cat.6, 100Ohm classe Cca
- Nr.1 - Scatola esterna tipo UNI503;
- Nr.1 - Placca autoportante da almeno 2 posizioni;
- Nr.1 - Tappo per RJ45 con attacco Keystone
- Nr.1 - Presa Keystone tipo U/UTP CAT 6

Nella figura che segue è rappresentato lo schema generale di un cablaggio di distribuzione orizzontale che interconnette un pannello di permutazione alla postazione di lavoro (PdL):



Il cablaggio delle dorsali dovrà collegare gli armadi rack di piano a partire dal rack di centro stella.

8. DISTRIBUZIONE CABLAGGI

Di seguito si riporta la distribuzione dei cablaggi da realizzare nei vari plessi

Plesso Moscati

- Nr.6 – Uffici Amministrativi “Piano Terra”
- Nr.4 – Aule “Piano Terra”
- Nr.1 – Access Point “Piano Terra”
- Nr.8 – Aule “Piano Primo”

Plesso Rodari

- Nr.2 - Uffici Amministrativi “Piano Terra”
- Nr.5 – Aule “Piano Terra”
- Nr.10 – Aule “Primo Piano”
- Nr.4 – Aule “Secondo Piano”
- Nr.3 – Dorsali in rame verso switch

Plesso Picasso

- Nr.2 – Access Point “Piano Terra”

Plesso Van Gogh

- Nr.2 – Access Point “Piano Terra”

Plesso Chagall

- Nr.2 – Access Point “Piano Terra”

9. NUOVO SISTEMA WIFI

Il sistema WIFI sarà realizzato utilizzando Access Point di ultima generazione sicuri, scalabili e gestiti in cloud con funzionalità di gestione avanzate al fine di collegare efficacemente persone, luoghi e oggetti.
Si richiedono Access Point di fascia Enterprise che dovranno fornire piena funzionalità senza bisogno di installare un controller fisico. La soluzione potrebbe essere quella di ricorrere ad una piattaforma in Cloud – gratuita - dalla quale si potranno anche ricavare i log e le statistiche.
Gli access point saranno distribuiti in modo da ottenere una copertura il più possibile omogenea e totale in relazione alla configurazione planimetrica dei plessi.
L'accesso alle SSID (Reti Wireless) create sarà discriminato da un meccanismo di autenticazione e accesso mediante associazione a più fattori, una volta autenticato, all'utente verranno applicate le policy di sicurezza decise dall'amministratore di rete e, in base a queste, l'utente potrà avere accesso ai servizi a lui concessi: tempo di connessione, limitazione in banda, ecc.
Si riporta uno schema logico dell'accesso al web da parte degli utenti WiFi.

9.1 Access Point per interni: Caratteristiche Tecniche

L'access point richiesto è di tipo Wi-Fi 6 progettato per una copertura wireless ad ampio raggio pur mantenendo la capacità complessiva della rete. Offre una velocità radio aggregata fino a 1,77 Gbps con radio a 5 GHz (2x2 MU-MIMO e OFDMA) e 2,4 GHz (2x2 MIMO).
L'AP può essere montato a soffitto per ampliare la copertura del segnale e supportare reti ad alta densità di dispositivi, oppure può essere montato a parete per estenderlo
Questo AP semplifica il processo di portare il WiFi 6 a casa o in ufficio. Può essere configurato in pochi minuti e completamente gestito con l'applicazione web in cloud.

Specifiche tecniche:

- WiFi 6 2x2 ad alta efficienza (802.11ax)
- Banda a 5 GHz (2x2 MU-MIMO e OFDMA) con velocità di trasmissione di 1,2 Gbps
- Banda da 2,4 GHz (2x2 MIMO) con velocità di trasmissione di 570 Mbps
- 1.77 Gbps aggregate data rate
- Alimentato da 802.3at PoE
- Throughput rate a 2.4 GHz 570 Mbps; 5 GHz 1201 Mbps
- Antenna gain 2.4 GHz 4 dBi; 5 GHz 5 dBi.

Come detto, gli AP richiesti sono da interno con antenna omnidirezionale.

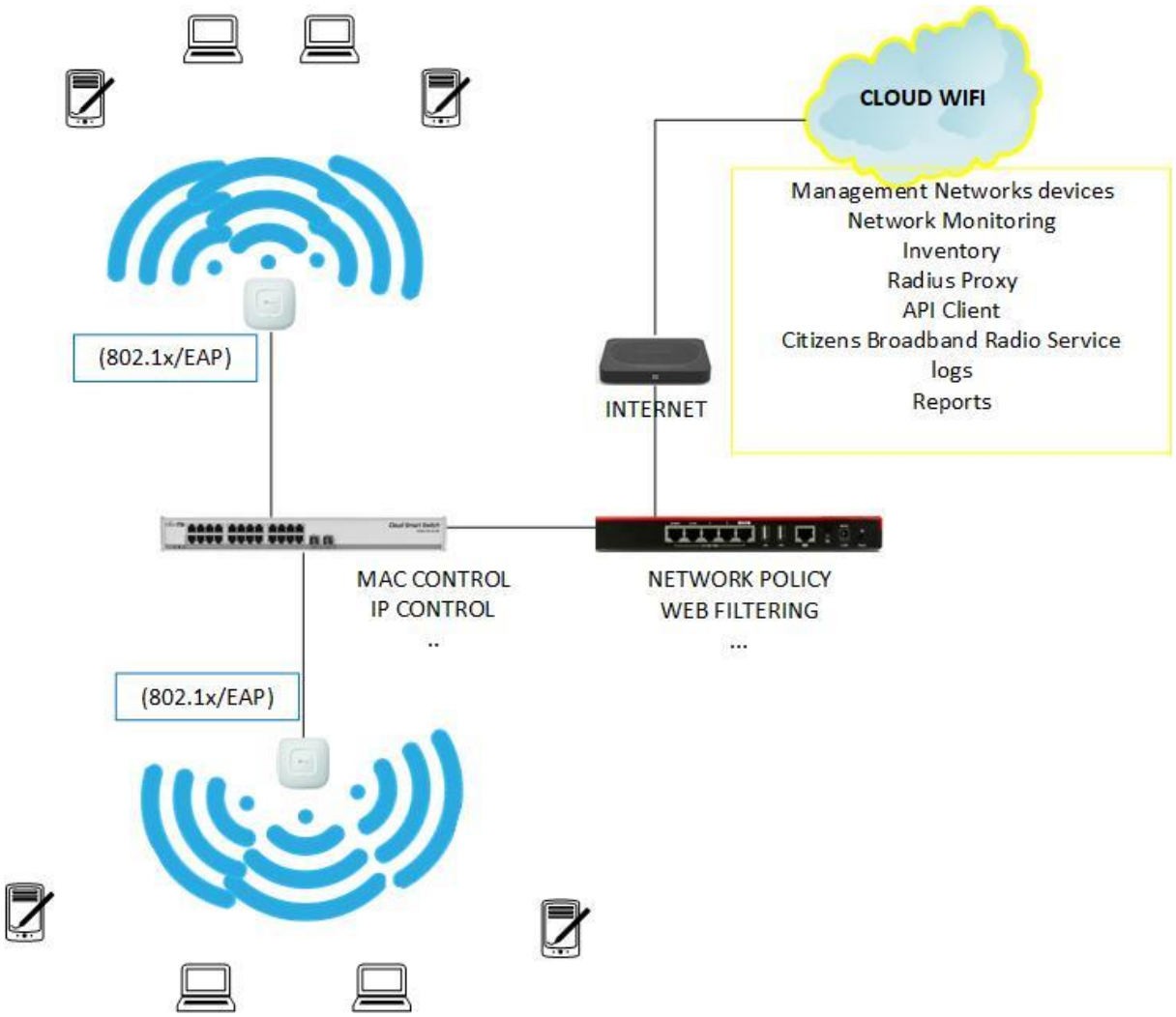
9.2 Access Point: Autenticazione

L'accesso alle SSID (Reti Wireless) create sarà discriminato da un meccanismo di autenticazione e accesso mediante associazione a più fattori, una volta autenticato. all'utente verranno applicate le policy di sicurezza decise dall'amministratore di rete e, in base a queste, l'utente potrà avere accesso ai servizi a lui concessi: tempo di connessione, limitazione in banda, ecc.

Il social login, in combinazione con l'accesso guest (tramite portale dedicato) consente di acquisire maggiori informazioni sugli utenti. È prevista anche la possibilità di registrazione via SMS, sempre nel rispetto del GDPR.

Le funzioni per l'accesso Guest supportano l'hosting di pagine introduttive, il social login, i voucher per l'accesso temporaneo e il gateway di pagamento (se necessario nel tempo). Queste funzionalità possono essere combinate con la possibilità di creare profili di traffico con limitazioni di tempo, velocità e volume.

Si riporta uno schema logico dell'accesso al web da parte degli utenti WiFi.



9.3 SISTEMA DI GESTIONE WIFI

A corredo degli AP dovrà essere configurato e fornito l'accesso ad un tool **in cloud** per il controllo, la gestione, la configurazione e la manutenzione degli AP.
Tale servizio dovrà essere **gratuito per sempre, cioè NON deve prevedere alcun costo di licenza e nessun costo ricorrente**.
Grazie a tale tool SW in cloud si potranno gestire tutti gli AP ubicati nei vari plessi.
Sebbene non verrà installato in fase esecutiva, è richiesta la possibilità di installare analogo tool SW in rete locale e che questo sia gratuito per sempre. In altre parole, gli AP devono essere compatibili con controller on premise e in cloud e questo deve essere gratuito per sempre.

9.4 SISTEMA HARDWARE DI GESTIONE E CONTROLLO A.P. IN CLOUD

Il controller hardware richiesto per gli AP permette di gestire centralmente tramite cloud più reti da un'interfaccia intuitiva ed inoltre consente di:

- Visualizzare le informazioni dettagliate sul dispositivo in tempo reale e le opzioni di configurazione dettagliate
- Aggiornare il firmware del dispositivo da remoto
- Gestire facilmente utenti e ospiti della rete
- Personalizza il design, l'architettura e la privacy degli hotspot degli ospiti
- Configurare rapidamente i dispositivi e gestirli in movimento con una potente app mobile

Offre inoltre la possibilità di implementare in modo semplice e rapido un proprio Captive Portal per l'accesso guest con splash page personalizzabile utilizzando i seguenti metodi di autenticazione:

- per mezzo voucher con limite impostabile di ore di validità
- social login (Facebook)
- tramite password
- server radius

Inoltre è possibile realizzare un accesso free con limitazione per tempo o per quota di traffico.

Specifiche tecniche del sistema
Chip basato su quad core Arm® Cortex®-A53
Metodo di alimentazione: 802.3af/at PoE, 5 V CC, 1 A
Interfaccia di rete: Porta RJ45 GbE

10. DISTRIBUZIONE ACCESS POINT

Di seguito si riporta la distribuzione degli AP per i vari plessi

Plesso Moscati

- Nr.4 – “Piano Terra”
- Nr.5 – “Piano Primo”

Plesso Rodari

- Nr.3 - “Piano Terra”
- Nr.3 – “Primo Piano”
- Nr.3 – “Secondo Piano”

Plesso Picasso

- Nr.2 – “Piano Terra”
- Nr.3 – “Primo Piano”
- Nr.1 – “Secondo Piano”

Plesso Van Gogh

- Nr.2 – “Piano Terra”

Plesso Chagall

- Nr.2 – “Piano Terra”

Nell’allegato “**Allegato 1 al Capitolato”** l’ubicazione degli Access Point riportata nella planimetria è da intendersi ad uso rappresentativo e che il valore del RSSI è una stima della potenza del segnale e pertanto l’esatta posizione dovrà essere determinata in fase esecutiva con l’approvazione della direzione lavori.

11. SERVIZI DI SICUREZZA

Dovranno essere previsti servizi **di sicurezza** che migliorano la protezione nelle aree cruciali di attacco per una gestione completa delle minacce:

- **Controllo Applicazioni:** limita le applicazioni improduttive, inappropriate o pericolose,
- **IPS:** servizio di prevenzione delle intrusioni provenienti da codice malevolo, sovrascrittura malevola di script (ad esempio Java, ASP), attacchi tramite buffer overflow.
- **Antivirus di rete:** scansione del traffico Internet in cerca di virus e di intrusioni.
- **Analisi WEB:** categorizzazione del traffico internet e limitazione di alcune categorie.
- **Riconoscimento SPAM:** combinazione di regole per identificare e bloccare con precisione il messaggio di spam e tenerli lontani dal server di posta elettronica
- **Difesa basata su reputazione**: analisi della reputazione dei siti internet e limitazione di accesso ai siti con cattiva reputazione.
- **Monitoraggio della rete**: consente al firewall di rilevare i dispositivi sulle reti interne e mostrarli su una mappa di rete nell'interfaccia web del firewall.
- **Cloud Management:** Gestione del firewall da cloud con conservazione dei log principali

11.1 Sicurezza Perimetrale "Firewall"

Per garantire un adeguato livello di sicurezza è richiesta l'installazione di Firewall di tipo UTM Next Generation Firewall con capacità di affrontare il traffico di rete di un Istituto Scolastico di medie dimensioni. Tale firewall offre un livello di sicurezza elevatissimo congiunto ad una velocità commisurata con le esigenze espresse anche con le lezioni in videoconferenza. La sicurezza viene assicurata dagli abbonamenti ai servizi di sicurezza inclusi.

La soluzione fornita, in termine di protezione della Rete LAN dell'Istituto, è pienamente conforme alle prescrizioni AGID e al GDPR (regolamento UE 2016/679), permettendo di:

- ridurre il rischio di "data breach",
- aiutare a prevenire incidenti di sicurezza,
- accrescere la visibilità della infrastruttura monitorata.

L'Istituto potrà sfruttare, inoltre, appieno delle caratteristiche e le funzionalità presenti nell'abbonamento dei Servizi UTM. La soluzione permette anche di instaurare connessioni VPN tra diverse sedi e VPN Mobile per gli operatori che hanno necessità di lavorare da remoto in piena sicurezza. La soluzione differisce dai semplici firewall perché, oltre al ruolo di firewall, svolge anche gli altri ruoli di sicurezza perimetrale come: antivirus, antispam, controllo delle applicazioni, prevenzione delle intrusioni, web-blocker, difesa basata sulla reputazione dei siti visitati, ecc. Inoltre, la soluzione unificata per la sicurezza delle reti integra protezione completa e al tempo stesso riduce i tempi e i costi necessari per gestire più prodotti di sicurezza single-point.

Tutte le funzionalità di sicurezza operano congiuntamente per ottenere una completa protezione della rete. Il personale IT ha così più tempo per impegnarsi in altre aree dell'amministrazione della rete e l'Istituto riduce i costi dell'hardware e del supporto.

L'UTM permette anche il pieno controllo dei contenuti HTTPS ed il supporto VoIP. È facile da usare grazie a strumenti di gestione che includono una console centralizzata e/o interfaccia utente Web per avere la massima flessibilità. Tutte le funzionalità in tempo reale per il monitoraggio, reporting semplice ed avanzato, ed il routing dinamico sono inclusi senza costi aggiuntivi.

Il prodotto fornito risulta essere il prodotto ideale per Enti Governativi e Istituti Scolastici ed offre

un livello di sicurezza elevatissimo congiunto ad una velocità commisurata con le esigenze espresse soprattutto in previsione di lezioni in videoconferenza.
Oltre alla fornitura dei prodotti hardware e software, e ai servizi erogati dal produttore il fornitore si occuperà anche dell'installazione, configurazione dell'apparato e formazione di base all'uso del sistema.

11.2 Firewall: Specifiche tecniche

Di seguito si riportano specifiche tecniche del firewall suddivise in:

- Specifiche tecniche Hardware
- Specifiche tecniche Software di base
- licenze servizi di sicurezza

11.2.1 Specifiche tecniche HW "Firewall"

- 8 Porte Ethernet Gigabit attive ed indipendenti, che supportano reti locali ad alta velocità e connessioni Gigabit WAN. Due delle porte sono PoE+.
- Slot di Espansione 1xSFP+ oppure LTE
- Velocità Firewall di 4.7 Gbps.
- Velocità VPN di 1.4 Gbps.
- Velocità aggregata UTM di 631 Mbps anche quando gli abbonamenti di sicurezza sono tutti abilitati.
- 500.000 di connessioni simultanee, 25.000 nuove connessioni al secondo.
- 60 VPN in Branch Office, 60 Mobile VPN in SSL

11.2.2 Specifiche tecniche SW di BASE

- SD-Wan per gestire in maniera dinamica diverse connettività e fruire agevolmente di servizi cloud.
- Gestione di più connettività, utile per la gestione del carico, del bilanciamento e del failover delle connettività Internet disponibili. In pratica, se l'istituto è dotato di più connettività Internet, il dispositivo può bilanciare il carico su queste e trasferire tutto il traffico internet su una di queste in caso di indisponibilità dell'altra (failover).
- Portale di accesso: permette di accedere da remoto alle risorse in maniera sicura anche senza l'uso delle VPN. Ciò viene fatto tramite web a valle della autenticazione sul relativo portale di accesso e gestione delle risorse che si vuole rendere disponibili (RDP, SSH, Web app e Website interni o esterni, Exchange server, ecc).
- Funzione di ispezione del contenuto in base ai livelli applicativi che rileva e blocca minacce non rilevabili dai firewall (*stateful packet inspection)*.
- Protezione proxy ad ampio raggio che offre notevole sicurezza per i protocolli HTTP, HTTPS, FTP, SMTP, POP3, DNS e TCP/UDP.
- Funzionalità interattive di monitoraggio e reporting in tempo reale che permettono di osservare con accuratezza senza precedenti l'attività correlata alla sicurezza della rete, per dare modo di intervenire immediatamente con azioni preventive o correttive.
- Console di gestione centralizza per la gestione di tutte le funzioni di sicurezza. Gestione dell'apparato tramite applicativo, Web o CLI.

- Autenticazione degli utenti tramite Single Sign On (Autenticazione Trasparente) Active Directory, Radius e LDAP.
- Funzionalità di controllo dell'accesso in base ai ruoli che permette all'amministratore di livello più alto di creare ruoli su misura per il controllo granulare.
- Controllo preciso sui privilegi di accesso a Internet per diversi gruppi di utenti.
- VPN multiple (SSL e IPSec) per la flessibilità dell'accesso remoto, compreso il supporto per dispositivi Apple iOS come iPhone e iPad e dispositivi Android
- Connettività remota sicura per quelli che si connettono al di fuori dai sedi periferiche: caso di utenti che lavorano da casa (mobile vpn).
- Altre funzionalità di rete come, ad esempio:
    - Instradamento Statico / Dinamico (BGP4, OSPF, RIP v1/2),
    - Instradamento basato sui criteri,
    - NAT Statica, dinamica, ecc.
    - Link Aggregation
    - Supporto VLAN

11.3 Licenze e Servizi di Sicurezza

La Suite comprende **servizi di sicurezza per 1 anni** che migliorano la protezione nelle aree cruciali di attacco per una gestione completa delle minacce:

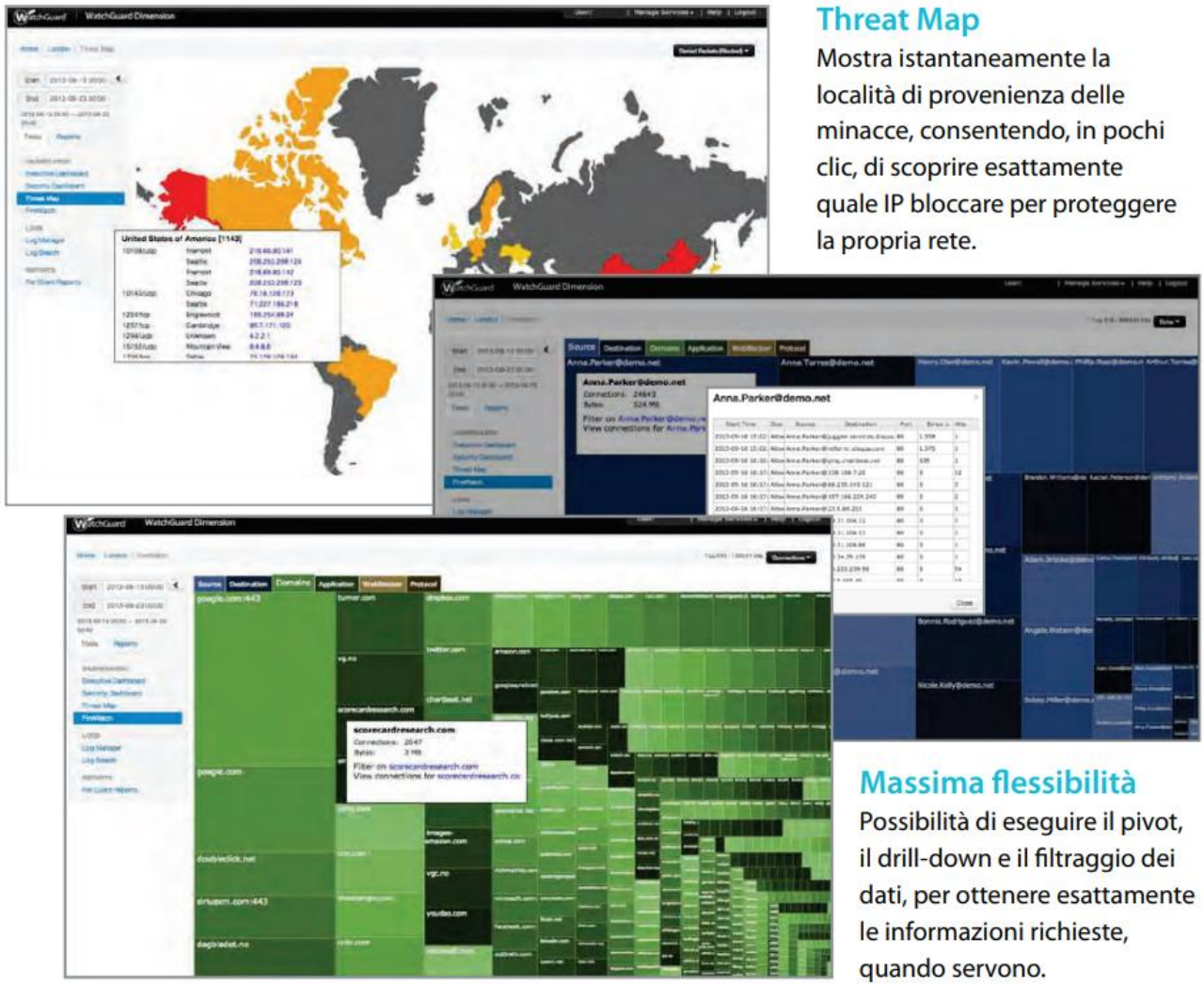
- **Controllo Applicazioni:** limita le applicazioni improduttive, inappropriate o pericolose, con la possibilità di intervenire su più di 1800 applicazioni SW (es. APP di Facebook, TikTok, Instagram, ecc).
- **IPS:** servizio di prevenzione delle intrusioni provenienti da codice SQL malevolo, sovrascrittura malevola di script (ad esempio Java, ASP), attacchi tramite buffer overflow.
- **Antivirus di rete:** scansione del traffico Internet in cerca di virus e di intrusioni.
- **Analisi WEB:** categorizzazione del traffico internet e limitazione di alcune categorie.
- **Riconoscimento SPAM:** combinazione di regole per identificare e bloccare con precisione il messaggio di spam e tenerli lontani dal server di posta elettronica
- **Difesa basata su reputazione**: analisi della reputazione dei siti internet e limitazione di accesso ai siti con cattiva reputazione.
- **Monitoraggio della rete**: consente al firewall di rilevare i dispositivi sulle reti interne e mostrarli su una mappa di rete nell'interfaccia web del firewall.
- **Cloud Management:** Gestione del firewall da cloud con conservazione dei log principali per un giorno.
- Garanzia hardware, assistenza tecnica e aggiornamenti software
- Servizio di "Supporto Standard" del Produttore
- 24 ore su 24 al giorno per 7 giorni su 7 alla settimana da parte del produttore
- Aggiornamenti e perfezionamenti software
- Avvisi tempestivi delle minacce e strumenti online (knowledge base, forum interattivo, pubblicazioni tecniche e training video)
- Sostituzione anticipata dell'hardware: in caso di guasto hardware, il produttore spedirà un'appliance di ricambio con consegna stimata entro il giorno successivo, franco destinatario, prima di ricevere l'appliance guasta.

11.3.1Servizio di Monitoring e Log

È richiesto un tool di reportistica avanzato sull'uso della risorsa Internet.

Questo deve offrire una vista di alto livello dell'attività della rete che mostra i top trend, i top client e le viste correlate degli utenti e delle applicazioni più utilizzate. Dopodiché, con un solo clic, gli utenti autorizzati possono approfondire l'analisi e vedere tutto, fino ai dati dei singoli log per scoprirne i dettagli più rilevanti e, soprattutto, le minacce e coloro (utenti o devices) che intasano la rete.

Questo strumento consente di organizzare le informazioni in base a punti chiari e precisi. Infatti, in assenza di tale tool, un'analisi efficace è impossibile quando la quantità di dati da esaminare è enorme … come accade per i log di accesso ad Internet.



Tale software dovrà essere installato su un computer messo a disposizione della scuola.

12. RIEPILOGO DELLA FORNITURA

12.1 Elenco riepilogativo della fornitura Plesso Moscati

Voce Fornitura	Q.tà
UTM Firewall	**1**
Switch Gigabit 24 porte + 4 SFP Managed	**2**
Switch Gigabit 8 porte PoE + 4 SFP Managed	**1**
UPS Rack 600VA	**3**
Access Point WiFi 6 Indoor	**9**
Sistema di gestione WiFi in Cloud	**1**
Punto PDL completo di accessori	**19**

12.2 Elenco riepilogativo della fornitura Plesso Rodari

Voce Fornitura	Q.tà
UTM Firewall	1
Switch Gigabit 24 porte PoE + 2 SFP Managed	2
Switch Gigabit 8 porte NO PoE + 4 SFP Managed	1
Armadio Rack 19” 9U	2
UPS Rack 600VA	4
Access Point WiFi 6 Indoor	9
Sistema di gestione WiFi in Cloud	1
Punto PDL completo di accessori	24

12.3 Elenco riepilogativo della fornitura Plesso Picasso

Voce Fornitura	Q.tà
UTM Firewall	**1**
Switch Gigabit 8 porte PoE + 4 SFP Managed	**1**
UPS Rack 600VA	**1**
Access Point WiFi 6 Indoor	**6**
Sistema di gestione WiFi in Cloud	**1**
Punto PDL completo di accessori	**2**
Opere accessorie alla fornitura (Piccoli adattamenti edilizi),	**1**
Servizio di monitoraggio e gestione della rete, Bonifica armadi, Mappatura rete esistente, Configurazione, Formazione	**1**
Servizio di Assistenza e Manutenzione	**1**

12.4 Elenco riepilogativo della fornitura Plesso Van Gogh

Voce Fornitura	Q.tà
Switch Gigabit 8 porte PoE + 4 SFP Managed	**1**
Armadio Rack 19” 6U	**1**
UPS Rack 600VA	**1**
Access Point WiFi 6 Indoor	**2**
Sistema di gestione WiFi in Cloud	**1**
Punto PDL completo di accessori	**2**
Servizio di Assistenza e Manutenzione	**1**

12.5 Elenco riepilogativo della fornitura Plesso Chagall

Voce Fornitura	Q.tà
Switch Gigabit 8 porte PoE + 4 SFP Managed	**1**
Armadio Rack 19” 6U	**1**
UPS Rack 600VA	**1**
Access Point WiFi 6 Indoor	**2**
Sistema di gestione WiFi in Cloud	**1**
PDL	**2**

12.6 Elenco della fornitura alla voce “Servizi Accessori” (per tutti i plessi)

Voce Servizi Accessori	Q.tà
Opere accessorie alla fornitura (Piccoli adattamenti edilizi),	**1**
Servizio di monitoraggio e gestione della rete, Bonifica armadi, Mappatura rete esistente, Configurazione, Formazione	**1**
Servizio di Assistenza e Manutenzione	**1**

13. Servizi accessori (specifiche)

Le apparecchiature tecnologiche (Switch, Firewall, Access Point) dovranno essere fornite con i seguenti servizi:

- Installazione e configurazione di tutti i prodotti hardware e software
- Installazione dei cablaggi forniti
- Collaudo e formazione
- La garanzia sui prodotti di cablaggio dovrà essere almeno di 12 mesi;
- La garanzia sui prodotti forniti elettronici e di rete (Switch, UPS, prese elettriche, etc.) dovrà essere almeno di 12 mesi (*salvo diversamente indicato nei paragrafi precedenti*)
- La garanzia sui prodotti WiFi (Access Point) dovrà essere almeno di 5 anni oltre l’anno di fine produzione (EOS).
- La garanzia sui prodotti di sicurezza (Firewall) 12 mesi (*salvo diversamente indicato nei paragrafi precedenti*)
- Servizio di Assistenza e Manutenzione 12 mesi (*salvo diversamente indicato nei paragrafi precedenti*) comprensivo interventi On-Site e da Remoto.

14. Glossario

AP – Access Point
PDL – Postazione di Lavoro, rappresenta l'impianto di cablaggio per le aule, uffici o laboratori
CWF – Cablaggio per la rete Wireless, rappresenta l'impianto di cablaggio per gli Access Point
WiFi – Wireless, rete via radio
PR – Piano Rialzato
PT – Piano Terra
1P – Primo Piano
UPS – "Uninterruptible Power Supply" Gruppo di Continuità
EN – Organismo di Normazione Europea
CEI - Comitato Elettrotecnico Italiano
ISO/IEC - International Standards Organization / International Electrotechnical Commission
ANSI – American National Standard Institute
EIA/TIA - Telecommunications Industry Association / Electronic Industries Association
AWG – American Wire Gauge (standard per misurare sezione e diametro dei conduttori)
Cat.6 – Categoria 6 è il sistema di cablaggio stabilito dalla norma EN-50173

Allegati:
Allegato 1: Piano di installazione Access Point e stima copertura

Il progettista
Ing. Francesco Auriemma

ORDINE DEGLI INGEGNERI DELLA PROVINCIA DI NAPOLI
DOTT. ING. AURIEMMA FRANCESCO
ISCRITTO ALL'ALBO PROFESSIONALE
COL N. 11537