


	<p align="center">Ministero dell'Istruzione ISTITUTO COMPRENSIVO STATALE di via VALLETTA FOGLIANO</p> <p align="center">Via Valletta Fogliano n° 59 - 27029 VIGEVANO (PV) - tel. 038175513 - fax 038170900 PEO pvic830001@istruzione.it - PEC pvic830001@pec.istruzione.it C.M. PVIC830001 - C.F. 94033990188</p> <p align="center">  </p> <p align="center"> <i>Scuole dell'Infanzia "R. Bianchi" - "M. Pistoja Mastronardi"</i> <i>Scuole Primarie "G.B. Ricci" - "A. Negri" - "G. Vidari"</i> <i>Scuola Secondaria di Primo grado "D. Bramante"</i> </p>	
--	--	---

All'Albo
Al sito web d'Istituto
Agli atti

Scheda Tecnica: Affidamento Diretto (ODA) Fondi Strutturali Europei – Programma Operativo Nazionale “Per la scuola, competenze e ambienti per l'apprendimento” 2014-2020. Asse II - Infrastrutture per l'istruzione – Fondo Europeo di Sviluppo Regionale (FESR) – REACT EU. Asse V – Priorità d'investimento: 13i – (FESR) “Promuovere il superamento degli effetti della crisi nel contesto della pandemia di COVID-19 e delle sue conseguenze sociali e preparare una ripresa verde, digitale e resiliente dell'economia” – Obiettivo specifico 13.1: Facilitare una ripresa verde, digitale e resiliente dell'economia - Azione 13.1.1 “Cablaggio strutturato e sicuro all'interno degli edifici scolastici”– Avviso pubblico prot.n. 20480 del 20/07/2021 per la realizzazione di reti locali, cablate e wireless, nelle scuole.

CODICE CUP: J59J21007290006

CODICE IDENTIFICATIVO PROGETTO: 13.1.1A - FESR PON-LO -2021-385

CIG: 923379832A

Al fine di predisporre un'infrastruttura idonea ad attività scolastica da integrare nella struttura esistente ma proiettata verso l'apertura al mondo dell'integrazione con telematica, iot, smart working e linee ultraveloci, si intendono realizzare tutte le linee principali in fibra ottica e di adottare materiali già rivolti verso la prossima tecnologia.

A tal fine, sono riportate di seguito le indicazioni fornite per l'attuazione del progetto dalla Progettista Sig.ra Cristina Cuvillo, la quale ha individuato come prima necessità la realizzazione delle linee di collegamento tra rack in modo da avere 5 apparati collegati tra loro alla velocità della fibra.

Per il collegamento servono 5 linee principali da realizzare con cavo monomodale OM4 che garantisca velocità di trasferimento fino a 10gb/s sulle direttrici principali.

I rack dovranno essere da 19 pollici con anta in vetro per poter controllare anche visivamente il funzionamento degli apparati.

In ogni rack dovrà essere presente uno switch layer3 con 4 porte SFT+ al fine di unire e rimandare il segnale in fibra (transceiver da 10gb/s con attacchi a piacere del fornitore purchè in classe adeguata alla velocità indicata), con tecnologia poe al fine di alimentare direttamente gli access point che dovranno essere installati (switch da almeno 24 porte di cui 8 poe).

In ogni rack dovrà essere creata anche la linea di alimentazione a 220v completa di multiprese da rack 19 pollici e gruppo di continuità al fine di garantire continuità di segnale anche in assenza di rete elettrica o in presenza di sbalzi.

Un firewall dovrà garantire la sicurezza delle connessioni, reti dedicate a didattica e segreteria separate, controllo MacAddress, regole di sicurezza, aggiornamenti costanti, ingresso e uscita in fibra ottica al fine di non creare colli di bottiglia.

Funzioni base apprezzabili in un firewall elencate qui di seguito:

-Filtraggio navigazione: pieno controllo sulla navigazione degli utenti.

-Antivirus centralizzato: verifica le connessioni HTTP, POP3, SMTP per identificare e bloccare software indesiderati.

-Antispam trasparente: contrassegna le mail di SPAM rendendole facilmente identificabili dall'utente.

-Gestore di banda (QOS): riserva la banda disponibile alle attività che ne hanno più bisogno.

-IDS, Bandwidth monitoring: grazie alle tecnologie integrate incrementa il livello di sicurezza della LAN

-Navigazione controllata: permette di ottenere il controllo completo della navigazione aziendale.

-Gestione blocco contenuti: basato su quindici categorie combinate tra loro permette di consentire l'accesso solo a siti con pertinenza al lavoro aziendale (ad esempio blocco pornografia, droghe, gioco d'azzardo ecc.).

-Gestione Whitelist e Blacklist: permette di definire siti ritenuti attendibili che quindi verranno visualizzati oppure che non devono essere concessi (ad esempio bloccare social network, giochi ecc.).

-Log completo: Registra quali siti sono stati visitati, quando e cosa è stato scaricato computer per computer.

-BlackHole DNS: annulla le richieste DNS verso domini specificati in modo da impedirne la connessione a prescindere dal protocollo o dall'app utilizzati. Questa caratteristica è spesso usata per bloccare Facebook, Twitter ecc.

-Gruppi di navigazione: permettono di gestire politiche di filtraggio differenti in base al gruppo di appartenenza.

-Autenticazione: in modalità trasparente non è richiesta nessuna configurazione sui client, il filtraggio avviene per indirizzo IP. Mentre con autenticazione attiva viene richiesto nome utente e password, le credenziali possono essere create direttamente sul server o ereditate da un dominio Active Directory esistente. Le impostazioni di navigazione possono essere rilasciate automaticamente via DHCP.

-Regole orarie: permette di definire regole di navigazione orarie.

-Privacy: E' importante ricordare che il sistema è comunque rispettoso della privacy, non permettendo l'identificazione univoca del computer specifico e/o dell'utente se non esplicitamente impostato, in modo da non violare lo statuto dei lavoratori in materia di controllo sul lavoro (consultare il proprio legale e/o sindacati in tal caso). Tuttavia, consente di tutelarsi in caso di necessità a fronte di problematiche di utilizzo inopportuno dalla rete aziendale verso internet.

-VPN Server: supporto per diverse tipologie di VPN in modo da poter soddisfare ogni esigenza.

-PPTP (GRE), L2TP: con una configurazione semplice e veloce permettono la connessione da qualunque sistema operativo moderno inclusi tablet e smartphone.

-IPSec: garantisce l'interazione con sistemi di altri produttori che utilizzano questo tipo di VPN.

-OpenVPN: permette il collegamento alla rete aziendale, con connessione protetta e criptata, e di lavorare come se foste presenti fisicamente. Ideale per sedi periferiche oppure per lavoratori remoti.

-VPN Lan to Lan immediate: stabilire un tunnel tra due apparati Firegate richiede pochi e semplici passaggi.

-Compatibilità con i principali OS: la connessione in VPN al sistema può essere effettuata dalla maggior parte dei sistemi operativi moderni

-Hotspot: grazie alla versatilità della funzione Hotspot e alla sicurezza del protocollo Radius integrato la serie S viene incontro a tutte le esigenze di controllo sulla navigazione aperta al pubblico. Indicata in tutte quelle realtà come hotel, bar, ristoranti, campeggi ecc.

-Self register: registrazione automatica anche tramite sms (richiede provider sms esterno per funzionare), da parte degli utenti, utile nel caso si voglia fornire la navigazione come servizio gratuito.

La serie Firegate è consigliata in quanto dispone di tutte queste caratteristiche, oltre ad essere fornito già di base con aggiornamento per 36mesi e menù tradotti in italiano.

In base alle esigenze rilevate vi è la necessità di integrare le postazioni filari esistenti con ulteriori 64 punti lan che dovranno essere realizzate almeno in categoria 6. Ogni punto lan dovrà essere corredato a fianco di alimentazione elettrica adeguata all'esigenza per cui verrà realizzato (esempio per postazione lim dovrà avere 2 prese minimo, per postazione pc 3 prese, ecc) .

Si rileva la necessità di integrare 14 access point di tipo professionale (poe, con possibilità di configurazione in mash, controllo geografico tramite ap, almeno certificato per 200 utenti contemporanei)

Si stima che per la realizzazione dei punti rete siano necessari circa 240mt di fibra ottica e 1500 metri di cavi di rete.

Sostituzione dell'attuale tratta di circa 100 metri che corre esternamente all'edificio con una o più tratte realizzate in fibra ottica completa di relativi media converter e tutto quanto occorrente alla realizzazione di un collegamento stabile allo switch dell'aula destinataria (Aula Multimediale).

Ogni punto rete dovrà essere certificato con apparecchiatura certificatrice omologata e certificata (tipo Fluke Wired, per esempio).

Tutti gli apparati dovranno avere una garanzia di almeno 36 mesi.

Inoltre, per il funzionamento, si chiede anche un contratto di assistenza su gestione e configurazione per almeno 12 mesi (meglio 36 mesi)".

Si precisa di seguito altresì quanto da effettuare:

- Posa in opera di 4 dorsali principali in fibra ottica per il collegamento dei rack tra di loro uno in ogni corridoio
- Posa di 5 armadi rack 19inc Intellinet 12U a muro con porta in cristallo completi di impianto elettrico, multipresa e gruppo di continuità per lan, pannello di permutazione lan rj45 e fibra ottica attacchi sc.
- Fornitura di apparati attivi switch layer 3 24 porte + 4 porte sfp+ completi di gbic 10gb/s
- Cablaggio e realizzazione di 64 punti lan armadio/presa completi di elettrificazione nei punti prefissati come da indicazioni
- Fornitura, installazione e configurazione di 20 access point Ubiquiti Ac-Pro 250 utenti e configurazione in mesh
- Fornitura, installazione e configurazione apparato Firegate 2000 completo di aggiornamenti giornalieri per 36 mesi e assistenza tecnica configurazione/manutenzione
- Fornitura cavo in fibra ottica monomodale doppia traccia, OM4 - 500 mt
- Fornitura di 2 media converter
- Fornitura cavo di rete lan utp cat. 6 – 3.000 mt
- Assistenza tecnica all inclusive 36 mesi su impianto e apparati attivi e passivi
- Fornitura di qualsiasi materiale di consumo ulteriore necessario alla finalizzazione dell'opera di infrastruttura di rete al fine di renderla funzionante nel più breve tempo possibile
- Altro: tutti i materiali di consumo atti alla finalizzazione dell'opera
- Certificazione strumentale

il Dirigente Scolastico

dott. Massimo Camola

firmato digitalmente ai sensi del Dlgs. 82/2005 e ss.mm.ii