LICEO STATALE
"FRANCESCO DE SANCTIS"
Liceo Classico – Liceo Scientifico a potenziamento Internazionale

Via Ten. Ugo Stanzione, 3 – 84133 SALERNO - Tel. 089/752094 – C.F 80021870656
www.liceoclassicodesanctis.edu.it - sapc040008@istruzione.it – sapc040008@pec.istruzione.it

Agli atti
Piattaforma MePA
Spett.le Ditta Avr 77
Via Salvator Rosa 138
84091 Battipaglia (SA)

PNRR Missione 4: Istruzione E Ricerca - Componente 1 Potenziamento dell'offerta dei servizi di istruzione: dagli asili nido alle Università Investimento 3.2: Scuola 4.0 - Azione 2 Next Generation Labs -Laboratori per le professioni digitali del futuro , Codice M4C1I3.2-2022-962-P-22204

OGGETTO: Capitolato Tecnico per l'affidamento diretto ai sensi del disposto combinato dell'art. 50 comma 1, lettera b), del D.Lgs n. 36/2023 e delle disposizioni di cui al decreto-legge. N. 77 del 2021, convertito con modificazioni dalla legge n. 108 del 2021, al decreto-legge 24 febbraio 2023 n. 13, mediante Trattativa Diretta sul Mercato elettronico della Pubblica Amministrazione (MePA) per un importo contrattuale di €. 27.908,29 (oltre IVA) pari a €. 34.048,11 (IVATO).

CUP C54D23000300006: CIG: A014C9770B

Codice progetto: M4C1I3.2-2022-962-P-22204
Titolo progetto: Nuovi ambienti per arte, scienze e media communication"

PRESTAZIONI: ACQUISTO DI PRODOTTI E SERVIZI A SUPPORTO DEL PROGETTO IN OGGETTO

CAPITOLATO TECNICO

LOTTO 1 **Massimale lotto – Base Asta € 27.908,29 oltre Iva**

Fornitura e Installazione di n.60 Notebook di primaria marca internazionale avente le seguenti caratteristiche tecniche :

• Processore tipo intel Celeron N4500 o superiore
• Ram 4 Gb DDR4
• Hard Disk Tipo e-MMC 128 Gb
• Scheda Grafica UHD Graphics
• Display 11,6" Lcd Touch Screen (Tipo Convertibile)
• Web Cam e Microfono
• Connettività Bluetooth – Wifi 802.11 AX- Lan RJ45
• Sistema Operativo Windows 11 Pro
• Servizio di installazione e configurazione on site

Software Didattico incluso avente le seguenti caratteristiche :

Avviare
• accendere o spegnere e accedere o disconnettersi da tutti i computer della classe dal PC dell'insegnante.
• NOVITÀ – Gli insegnanti possono scegliere tre modalità utente (Facile, Intermedio e Avanzato) per rendere le funzionalità accessibili in base al loro livello di sicurezza edtech.
• Nascondi gli schermi di tutti gli studenti per attirare l'attenzione e bloccare anche mouse e tastiere.
• Ricollegarsi automaticamente ai PC degli studenti se vengono riavviati.
• Usa il layout degli studenti sugli schermi degli insegnanti per adattarli al layout della classe fisica.
• Utilizza i profili dei singoli insegnanti per fornire le funzionalità richieste da ciascun insegnante.
• Utilizzare l'opzione "Richiedi assistenza" con un clic dalla barra degli strumenti dell'insegnante se è necessario il supporto tecnico.
• Reimpostazione delle password di sistema per gli studenti senza supporto IT.
• Gli insegnanti possono utilizzare Commenti di studenti per valutare come si sentono, la loro fiducia in un argomento e se hanno bisogno di ulteriore supporto.
• Gamma flessibile di metodi di connessione ai dispositivi degli studenti, inclusa l'integrazione SIS tramite ClassLink OneRoster e Google Classroom.

Gestione della stampante e dei dispositivi
• Impedire agli studenti di stampare in classe.
• Limita l'utilizzo della stampante per numero di pagine.
• Richiedi l'autorizzazione del docente prima della stampa.
• Impedire l'utilizzo di singole stampanti.
• Visualizza un indicatore di stampa in tempo reale che identifica lo studente che sta attualmente stampando.
• Mostra il numero di lavori di stampa in pausa che richiedono l'attenzione dell'insegnante.
• Impedire che i dati vengano copiati su o da periferiche di archiviazione USB e CDR / DVD.
• Disattiva la webcam sui dispositivi della classe.

Registro degli studenti
• Richiedi informazioni standard e personalizzate da ogni studente all'inizio della lezione.
• Stampa il registro degli studenti, incluso un totale di eventuali ricompense o lavori di stampa completati durante la lezione.
• Utilizzare icone personalizzate per ciascun gruppo di studenti.

Distribuisci e raccogli file
• Distribuisci file e cartelle dal PC del tutor a più dispositivi studente.
• Trasferisci file da e verso PC selezionati o multipli in un'unica azione.

• Invio e raccolta automatica dei file, con l'inclusione dei dettagli di ogni Studente.
• Il feedback in tempo reale mostra all'insegnante quali file degli studenti sono pronti per la raccolta e quali studenti devono ricordare.
Barra d'informazioni per gli Studenti
• Visualizza obiettivi della lezione e risultati di apprendimento.
• Fornisce informazioni sulle lezioni in tempo reale, ad esempio il titolo della lezione; tempo rimanente; tutti i premi che sono stati dati dall'insegnante.
• Richiedi assistenza dall'insegnante tramite il pulsante di aiuto.
• Accedi al loro diario digitale.
• Accedi alla cartella delle risorse personali dello studente.
• Verifica quali restrizioni sono attualmente presenti, ad esempio Internet, applicazioni, stampa, chiavette USB.
Strumenti dei tecnici
• Il softwareviene inoltre fornito con una Console dei tecnici per aiutare il team IT della scuola a supportare gli utenti e gestire i dispositivi in tutta la scuola. I tecnici IT possono eseguire il potente 1: 1 PC Remote Control su qualsiasi computer selezionato, acquisire schermate, annotare lo schermo e fornire assistenza tecnica diretta a qualsiasi insegnante di classe. E per un controllo completo, possono anche applicare le impostazioni a livello di scuola come Internet e le restrizioni delle applicazioni che sono "sempre attive".
istruzione in Tempo Reale (Modalità Mostra)
• Mostra il desktop del Tutor a tutti o studenti selezionati.
• Mostrare lo schermo di uno studente (modalità Mostra).
• Limitare l'accesso a Internet ai siti approvati solo durante lo spettacolo.
• Mostra un'applicazione specifica agli studenti selezionati.
• Annotate lo schermo di una Presentazione o durante il Controllo Remoto con una serie di strumenti che facilitano la presentazione (come frecce, forme, evidenziatori e testo).
• Mostrate un "Replay file" (precedentemente registrato) agli studenti selezionati.
• Mostrate un file video agli studenti selezionati.
• Lasciate una registrazione della vostra presentazione sui computer degli studenti, per la revisione in un secondo momento.
• Usate la modalità Audio per parlare agli studenti durante una presentazione.
• Inviate le vostre presentazioni ottimizzate per le reti wireless.
Lavagna virtuale
Una lavagna a tutto schermo, integrata direttamente nella Console Tutor, che contiene una gamma completa distrumenti di disegno per migliorare la collaborazione con l'aula.

Leader di gruppo
Ad uno Studente possono essere assegnati certi diritti di tutor in modo che possa agire da leader di gruppo fino alla revocadi tali privilegi. Adesso include un layout visivo dei leader di gruppo e dei relativi membri del gruppo.
Chat
Apri una discussione in chat a cui puoi partecipare tutti gli studenti o solo quelli selezionati, registrati i loro commenti e condivideteli con gli altri membri della classe (adesso disponibile con emoticon!).
Supporto audio
Trasmettete la voce dell'insegnante durante una presentazione. Il supporto audio è incluso in ogni sessione di Presentazione dello schermo e di Controllo Remoto.
Barra degli strumenti dell'insegnante
Quando l'applicazione dell'insegnante è ridotta a icona, Il software dovrà fornire una comoda barra degli strumenti per accedere rapidamente alle sue funzioni chiave. Questa barra degli strumenti è ottimizzata per l'impiego con le lavagne interattive.

Software di sicurezza avente le seguenti caratteristiche

Gestione automatica delle patch

Software Updater è la funzione automatica di gestione delle patch completamente integrata nei client. Non è necessario installare agenti, server di gestione o console separate.

Software Updater è un componente fondamentale della sicurezza. È il primo livello di protezione contro contenuti nocivi che possono raggiungere gli endpoint e previene l'80% degli attacchi semplicemente installando gli aggiornamenti di sicurezza del software non appena sono disponibili.

Software Updater esegue scansioni per rilevare gli aggiornamenti mancanti, crea un rapporto sulla vulnerabilità basato sulle patch mancanti, quindi scarica e implementa gli aggiornamenti, automaticamente o manualmente. Le patch di sicurezza includono aggiornamenti Microsoft e di oltre 2500 applicazioni di terze parti, come Flash, Java, OpenOffice e altre ancora che generalmente vengono usate come vettori per gli attacchi per via della loro diffusione.

Analisi euristica e del comportamento

DeepGuard unisce alcune delle tecnologie più avanzate per la sicurezza. È il livello finale e più importante di difesa contro le nuove minacce, anche quelle che attaccano vulnerabilità precedentemente sconosciute. DeepGuard osserva il comportamento dell'applicazione e in modo proattivo intercetta immediatamente qualsiasi azione potenzialmente nociva prima che causi danni. Spostando l'attenzione dalle caratteristiche di firma agli schemi di comportamento nocivi, DeepGuard può identificare e bloccare il malware ancor prima che un campione venga acquisito ed esaminato.
Al primo avvio di un programma sconosciuto o sospetto, DeepGuard ritarda temporaneamente la sua esecuzione per eseguire un controllo della reputazione del file e del suo tasso di diffusione, lo esegue in un ambiente sandbox e infine lo elabora per produrre un'analisi comportamentale e intercettazione degli exploit.

Intelligence in tempo reale sulle minacce

Sistema Security Cloud ,sistema di analisi delle minacce basato sul cloud. Usa, tra gli altri, Big Data e Machine Learning per aggiornare continuamente la nostra base di conoscenza delle minacce digitali. Security Cloud è sempre in contatto con i sistemi client, identificando le nuove minacce non appena emergono e fornendo protezione nell'arco di pochi minuti.
Un servizio di analisi delle minacce basato sul cloud presenta molti vantaggi rispetto agli approcci tradizionali. L'intelligence per le minacce è il risultato della raccolta di centinaia di migliaia di nodi client, realizzando un'immagine in tempo reale della situazione globale delle minacce. Nell'arco di pochi minuti, usiamo queste informazioni per proteggere i nostri clienti.
Ad esempio, se l'analisi euristica e del comportamento di DeepGuard identifica un attacco zero-day, l'informazione viene condivisa con tutti i dispositivi protetti tramite Security Cloud, rendendo l'attacco inoffensivo pochi minuti dopo la sua individuazione.

Protezione contro i malware

Il componente per la sicurezza dei computer utilizza una piattaforma di protezione a più motori per individuare e bloccare il malware. Fornisce una protezione superiore rispetto alle tradizionali tecnologie basate sulla firma.
Individua una gamma più ampia di funzioni, schemi e trend nocivi, consentendo un rilevamento più affidabile e accurato, anche per varianti precedentemente sconosciute di malware
Sfruttando controlli in tempo reale con Security Cloud, è in grado di individuare più rapidamente minacce

nuove ed emergenti oltre ad assicurare un'impronta ridotta
L'emulazione consente il rilevamento di malware che utilizza tecniche di offuscamento e fornisce un ulteriore livello di sicurezza prima dell'esecuzione di un file

Blocco dell'accesso a siti dannosi

Browsing Protection è un livello di sicurezza fondamentale che impedisce in modo proattivo agli utenti di visitare siti dannosi. Ciò è particolarmente efficace in quanto questo genere di intervento riduce l'esposizione generale a contenuti dannosi e quindi ad attacchi.
Browsing Protection impedisce, ad esempio, agli utenti finali di essere indotti ad accedere a siti di phishing apparentemente normali, a siti dannosi attraverso link e-mail e di venire infettati tramite pubblicità di terze parti su siti normalmente innocui.
Questa funzione controlla la reputazione più recente dei siti web e dei file dal Security Cloud, basandosi su vari dati, quali indirizzi IP, parole chiave dell'URL e comportamento del sito.
Browsing Protection è indipendente dal browser in quanto funziona a livello di rete. Ciò assicura una protezione anche nel caso in cui l'utente non utilizzi i browser raccomandati dall'azienda.

Blocco dei contenuti web dannosi

Web Traffic Protection impedisce che contenuti attivi come Java e Flash, ampiamente usati per gli attacchi online, vengano utilizzati per exploit. Questi componenti vengono bloccati automaticamente su siti sconosciuti e sospetti in base ai dati della reputazione. Gli amministratori possono consentire eccezioni aggiungendo voci a un elenco di siti fidati, per esempio contrassegnando in questo modo i siti dell'intranet dell'azienda, per i quali la soluzione non ha informazioni relative alla reputazione.
Web Traffic Protection analizza il traffico Web HTTP in tempo reale, con più motori di analisi anti-malware complementari e controlli della reputazione. In questo modo malware ed exploit vengono individuati e bloccati durante il traffico Web, prima che i dati vengano scritti sul disco fisso. Si tratta di una protezione aggiuntiva contro il malware più avanzato, come la tipologia che agisce su aree della memoria.

Web Content Control

Web Content Control consente di limitare l'utilizzo improduttivo e inappropriato di Internet. Limita la navigazione Web dei dipendenti, negando l'accesso a destinazioni non collegate all'ambito lavorativo come social media e siti per adulti al fine di sfruttare al meglio il tempo ed evitare siti dannosi.
Web Content Control riduce perdite di produttività, consumo della larghezza di banda e rischi legali causati dall'accesso non autorizzato da parte dei dipendenti a materiale web inappropriato o di svago. Riduce inoltre le possibilità che i dipendenti siano esposti a contenuti nocivi.
Gli amministratori IT possono creare eccezioni locali che ignorano le categorie imposte. Ad esempio, anche in caso di blocco dell'accesso ai social network, si può aggiungere come eccezione Linkedin.com all'elenco di siti fidati.

Alto livello di sicurezza per siti web fondamentali

Connection Control è un livello di sicurezza che aumenta ampiamente la protezione per attività web fondamentali per l'azienda, ad esempio l'utilizzo di intranet o servizi sensibili basati sul cloud come CRM.
Non appena un dipendente accede a un sito web che richiede una protezione aggiuntiva, Connection Control aumenta automaticamente il livello di sicurezza per la sessione. In questo lasso di tempo, Connection Control chiude le connessioni di rete a tutti i siti sconosciuti dall'endpoint. Gli utenti possono continuare a utilizzare i siti che sono stati verificati come sicuri dal sistema antivirus in modo da non ridurre la produttività dei dipendenti.
Tramite il blocco delle connessioni non sicure, trojan bancari e altri malware non sono in grado di inviare a criminali informazioni aziendali riservate come le credenziali utente e le informazioni basate sul cloud. La

sicurezza torna a livello normale quando termina il processo specifico del browser o l'utente conclude la sessione.

Accesso solo per hardware autorizzato

Device Control impedisce che le minacce penetrino nel sistema attraverso dispositivi hardware quali chiavette USB, drive CD-ROM e webcam. Impedisce anche la perdita di dati, consentendo ad esempio un accesso in sola lettura.
Se un dispositivo proibito viene connesso, Device Control lo spegne per evitare ogni possibile accesso. E' possibile impedire l'accesso ai dispositivi impostando regole predefinite, e definire regole per consentire dispositivi specifici, mentre tutti gli altri dispositivi della stessa categoria vengono bloccati. Ad esempio è possibile:
Disabilitare l'esecuzione di programmi da USB/CD/altri drive: disabilita auto run, esecuzione accidentale o lancio di moduli da supporti rimovibili
Bloccare completamente alcune tipologie di device
Impostare un accesso read-only a USB/CD/altri drive
Bloccare alcune tipologie di device con l'eccezione di dispositivi specifici

Firewall

firewall che usa il rule engine Windows di default per eseguire regole firewall. Questo incrementa in modo sensibile la compatibilità con altre applicazioni e appliance. Il sofisticato ruleset , che contiene regole avanzate che combattono rischi quali la propagazione del ransomware e i movimemti laterali, sono aggiunte sul ruleset standard di Windows.
L'amministratore può estendere i set di regole per affrontare minacce specifiche per l'azienda e il contesto. Inoltre, regole di auto-selezione consentono agli amministratori di definire profili sulla base delle necessità di sicurezza di reti differenti.

Sicurezza con i sistemi Windows Anti-malware avanzato
Funzionalità di multi-engine detection, che offrono una sicurezza decisamente superiore.
• DeepGuard
Protezione proattiva da malware zero-day ed exploit grazie ad analisi euristica e comportamentale.
• Patch management
Esegue patch su oltre 2.500 software per server e di terze parti, come Apache, BizTalk, SQL, Flash, ecc.
• Protezione web
Blocca contenuti web pericolosi e impedisce l'accesso a siti malevoli e di phishing.
• Exchange, SharePoint, Citrix, Linux
Componenti di sicurezza dedicate disponibili per piattaforme differenti.

Fornitura e Installazione di n.02 Carrello Mobile di ricarica e conservazione per notebook e tablet avente le seguenti caratteristiche tecniche :
• Anta anteriore apribile a 270°
• porte con chiusura a chiave
• impugnature ergonomiche
• Gruppo di ventilazione forzata dell'aria incluso
• divisori in ABS con passacavi
• Materiale impugnature ABS/Metallo bianco
• 36 alloggiamenti suddivisi in 3 livelli da 12 dispositivi
• ruote con freno per agevolare lo spostamento
• Power Management System incluso per la gestione temporizzata di 3 cicli diversi di ricarica
• Corso di formazione al corretto utilizzo del prodotto

Fornitura e installazione di n.02 Access Point Professionale avente le seguenti caratteristiche minime: • Access Point Wi-Fi 6 (802.11ax) - Velocità Wi-Fi fino a 3550 Mbps (1148 Mbps in2.4 GHz + 2402 Mbps in 5 GHz). • Scenari ad alta densità - Il nuovo standard Wi-Fi 6 introduce le tecnologie 8x8 MU-MIMO (uplink e downlink) e OFDMA che aumentano notevolmente la capacità della rete, fino a 4 volte maggiore rispetto al precedente standard, consentendo di gestire più dispositivi simultaneamente. • Connettività 2.5 GE PoE+ - Connettività cablata dalle alte velocità e alimentazione Power over Ethernet (802.3at). • Piena compatibilità con il sistema di gestione già presente a scuola • Saranno a carico della ditta le operazioni di installazione a soffitto/parete secondo le indicazioni del progettista . • Saranno a carico della ditta le operazioni di configurazione di tipo sistemistica secondo le necessità della nostra amministrazione
Fornitura e Installazione di n.60 Cuffia e Microfono Professionale avente le seguenti caratteristiche minime: CARATTERISTICHE FISICHE • Tipologia Cuffie con filo • Fattore di forma Sovraurali (On-Ear Headphones) • Microfono incorporato Sì CARATTERISTICHE TECNICHE • Sensibilità 120 dB • Impedenza 38 Ohm • Risposta in frequenza 20 - 20.000 • Ascolto musica Sì • Controllo remoto Controllo chiamate • Noise canceling si CONNETTIVITÀ • Alimentazione USB • Tipo di porta USB-A

IL DIRIGENTE SCOLASTICO
Dott.ssa Cinzia Lucia

CINZIA LUCIA GUIDA
25.09.2023 16:57:20 UTC