Istituto Istruzione Superiore
"Italo Calvino"
Via Borzoli,21- Genova 16153
Tel. 010/6504672
e-mail geis01400q@istruzione
www.calvino.ge.it

Capitolato tecnico per la realizzazione della rete wireless

PON WLAN

CUP: C36J15000800007 **CIG: 554638802C**

Oggetto fornitura

Nell'ambito del recepimento del D.L. n.95 del 2012, poi convertito in Legge 135/2012, che rende obbligatorio il registro elettronico in ambito scolastico, l'istituto I.s. I. CALVINO di Via Borzoli 21, 16153 Genova intende realizzare la propria rete wireless, per coprire le strutture didattiche riportate di seguito nel presente documento, allo scopo di offrire la possibilità al personale docente e tecnico-amministrativo di utilizzare il registro informatizzato attraverso un supporto elettronico e le conseguenti comunicazioni con le famiglie e gli alunni. Allo stesso tempo è richiesto di utilizzare la medesima infrastruttura per l'accesso alle risorse messe a disposizione agli studenti iscritti all'anno scolastico (es. connettività a Internet, videoconferenza e materiale didattico).
E' possibile ipotizzare fino ad un massimo stimato di **50** device collegati contemporaneamente in tutta la rete dell'Istituto, con concentrazioni nelle singole aule didattiche.
Per fare ciò si prevede la necessità di adeguare la backbone attuale (rete cablata) in modo da dare pieno supporto a quella di accesso WI-FI, eliminando gli attuali colli di bottiglia.
A tal fine il presente istituto ha predisposto il presente documento riportante le richieste tecnico funzionali che dovranno rispettare l'aggiornamento dell'infrastruttura di rete cablata oltre che quella WI-FI.
Oggetto della presente fornitura è pertanto l'hardware, il software, simulazione software della copertura WI-FI, il site survey WIFI pre-installazione e post- installazione.
La soluzione dovrà sottostare ai parametri di sicurezza dell'istituto e pertanto è richiesto che nessun dato sensibile possa rimanere sugli apparati distribuiti, ma che debba risiedere centralmente.
I nuovi AP WI-FI dovranno essere installati predisponendo nuovi punti wired interconnessi all'attuale infrastruttura di rete cablata degli edifici; la loro attivazione avverrà tramite la configurazione di vlan ad-hoc sugli apparati di switching L2.

Si intende pertanto realizzare il cablaggio strutturato fisico per portare un punto rete su ogni Access Point, ed una rete Wireless d'Istituto che permetta l'accesso a tutti i dispositivi senza fili, il tutto distribuito su 3 plessi distinti.
Si richiede quindi la realizzazione chiavi in mano di un sistema composto da:

- N° 16 access point gestibili centralmente
- N° 01 controller di gestione per gli access point
- N° 03 Switch da 8 porte POE gestibili via web

Planimetrie allegate delle aree dell'edificio.

Servizi integrati nella fornitura

(Installazione, configurazione, startup, manutenzione hardware)

L'azienda che intende partecipare all'offerta dovrà in autonomia provvedere:
- ad un sopralluogo presso i locali e delle aree di raccolta da coprire.

- simulazione software di copertura WI-FI e/o site survey pre-installazione nuovi AP WIFI e/o site survey post-installazione nuovi AP WI-FI.

- alla realizzazione di tutte le opere, sia elettriche che non, per l'installazione e la messa in esercizio dell'infrastruttura di rete, specificando a priori nell'offerta anche eventuali nuovi armadi rack, posizione degli stessi, switch Ethernet L2 e armadi di permutazione;

- alla fornitura, installazione per tutte le nuove tratte realizzate e certificazione di rete cablata in CAT.6A;

- a prevedere un cablaggio, dell'infrastruttura, basato su un centro stella principale
- alla fornitura, installazione di dispositivi WI-FI per il collegamento in Wireless del plesso denominato IIS Italo Calvino

- all'installazione e configurazione della rete WI-FI (AP e centro di controllo marchiati CE) e rilascio funzionale dell'infrastruttura ad un tecnico indicato dall'Istituto Scolastico;

- radio planning WI-FI tenendo conto dei nuovi AP WI-FI e delle fonti di interferenze radio esterne;

Allegato tecnico (sola parte AP WIFI)

Caratteristiche e requisiti della rete Wi-Fi

Il presente capitolo definisce le specifiche tecniche, funzionali e prestazionali per la realizzazione di una rete wireless in tecnologia Wi-Fi IEEE 802.**11 a/b/g/n** nelle bande di frequenza non licenziate 2,4 GHz e 5 GHz per l'istituto I.S. I. CALVINO.
La rete ha lo scopo di garantire l'accesso wireless in tecnologia Wi-Fi ai servizi messi a disposizione dal ministero dell'istruzione per gli utenti forniti di apparati dotati di **connettività IEEE 802.11 a/b/g/n nelle bande di frequenza 2,4 GHz e 5 GHz (definiti in seguito "client")**, quali computer portatili, smartphone e telefoni VoIP, tablet, sistemi wireless presenti negli edifici dell'istituto e rendere fruibili tutti i servizi che la scuola vorrà implementare.
La rete Wi-Fi da realizzare dovrà essere composta dai seguenti elementi:
Centro di Controllo di Rete: WIRELESS CONTROLLER il Centro di Controllo di Rete svolge la funzione di nodo centralizzato di gestione e controllo per tutta la rete Wi-Fi.
Access Point Wi-Fi: un Access Point è un dispositivo che permette al client di collegarsi ad una rete wireless. L'Access Point può essere collegato fisicamente ad una rete cablata (AP Wired); l'Access Point è l'elemento della rete che realizza la copertura radio Wi-Fi in banda 2,4 GHz (standard 802.11 b/g/n). La banda di frequenza 5 GHz (standard 802.11 a/n).
Di seguito si riportano le caratteristiche tecnico-funzionali richieste ai componenti WiFi della rete.

ARCHITETTURA DELLA RETE WI-FI

L'architettura della rete Wi-Fi proposta deve rispondere a requisiti di flessibilità, espandibilità e resilienza. Gli elementi di resilienza del sistema in offerta dovranno basarsi su:

1. La rete Wi-Fi proposta deve essere in grado di adattare dinamicamente ed automaticamente le risorse radio (canali radio e/o livelli di potenza trasmessa) degli Access Point in modo da ottimizzare il segnale a radiofrequenza in presenza di interferenze radio oppure in modo da ripristinare i livelli radio ottimali di una certa area in seguito alla perdita di un Access Point.
2. Gli Access Point dovranno continuare a lavorare anche in assenza del Centro di Controllo. L'architettura della rete Wi-Fi da realizzare prevede che normalmente gli Access Point lavorino sotto il controllo del Centro di Controllo Questa modalità di lavoro viene definita come *dipendente* e costituisce la modalità di funzionamento abituale della rete. Gli Access Point in fornitura devono essere in grado di funzionare anche in assenza del Centro di Controllo, svolgendo localmente le funzioni proprie del Centro di Controllo stesso. Questa modalità di lavoro viene definita come *indipendente* (o stand- alone). Il passaggio da una modalità all'altra (a seconda delle circostanze in cui si venga a trovare la rete) deve avvenire in maniera automatica senza perdita di connettività per i client. Il processo di adozione di un Access Point da parte del Centro di Controllo dovrà essere possibile sia a Layer 2 che a Layer 3. Gli Access Point in offerta dovranno perciò funzionare in modalità adattativa, ovvero adattando automaticamente la loro modalità di funzionamento (dipendente o indipendente) a seconda della situazione.

Dal punto di vista del routing, l'architettura proposta deve essere in grado di eliminare i colli di bottiglia (o "single points of failure") tipici di una rete centralizzata di tipo tradizionale ed essere altamente scalabile: essa deve essere in grado di distribuire l'intelligenza di rete e le funzioni di sicurezza e di instradamento del traffico su tutta la rete pur mantenendo la gestione centralizzata nel Centro di Controllo.

Ogni Access Point deve essere in grado di prendere decisioni in maniera indipendente riguardo la sicurezza o l'instradamento del traffico a livello locale, ottimizzando le risorse di tutta la rete. Il risultato dovrà essere una rete sicura, affidabile e con elevate prestazioni.

Si richiede perciò che il traffico locale venga instradato localmente senza passare dal Centro di Controllo, in maniera dinamica e intelligente. In questo modo si mantengono entrambi i vantaggi di un'architettura distribuita e di un'architettura centralizzata, in quanto gli Access Point vengono comunque gestiti centralmente dal Centro di Controllo.

Questo tipo di architettura diventa fondamentale nel caso di elevate moli di traffico generate dalla rete di accesso Wi-Fi al crescere del numero di Access Point connessi su molteplici siti.

In particolare si evita che il Centro di Controllo diventi rapidamente un collo di bottiglia per tutta la rete, si riducono le problematiche legate alla latenza per le applicazioni voce e al jitter per il traffico video e si offre alla rete maggior flessibilità e maggior capacità. Il Centro di Controllo in fornitura resta comunque il singolo punto di gestione degli Access Point, fornendo funzioni di configurazione, controllo e troubleshooting a livello centralizzato.

1.1 Centro di Controllo di rete

Il Centro di Controllo della rete Wi-Fi dovrà consentire il controllo, la configurazione e la gestione della rete Wi-Fi da un unico punto centralizzato.
Le funzionalità e le capacità del Centro di Controllo della rete richieste sono riassunte di seguito:
1. Gestione centralizzata delle configurazioni iniziali e successive degli Access Point; il Centro di Controllo dovrà avere la capacità di gestire almeno 16 Access Point e messi in cluster fino a 32.
2. Ai fini di sicurezza la macchina dedicata includerà le regole necessarie all'accesso con livelli di restrizione differenti in base agli utenti
3. Ai fini delle sicurezza il centro di controllo deve supportare la funzione di "Content Filtering" Il content filtering è la tecnica tramite la quale è possibile bloccare o consentire un contenuto, sulla base dell'analisi del contenuto stesso.
4. Supporto Autenticazione Captive Portal. Viene richiesta una soluzione basata su autenticazione d'accesso mediante Captive Portal con password, statiche, dinamiche (ticketing) e Radius Server a condizione che i software non abbiano limitazioni di licenza e che siano di facile fruizione (user friendly e basati su interfacce web-based) da parte del personale autorizzato e preposto per l'aggiunta e/o modifica di utenti e/o gruppi di utenti e relative modifiche/creazione delle regole d'accesso.
5. L'interfaccia web-based dovrà essere gestibile da amministratore remoto e senza limitazioni di licenza per l'utilizzo richiesto.
6. Il controller dovrà supportare la funzionalità fast roaming al fine di limitare la perdita di pacchetti nel passaggio tra una cella e l'altra.
7. Il controller dovrà supportare la funzionalità Multi SSID e il protocollo IEE 802.1Q al fine di poter gestire al meglio le varie segmentazioni della rete wireless; proprio per essere più gestibile e performante il Controller deve consentire di indirizzare il traffico utente (data traffic) in locale (Local Forwarding) o verso un punto centralizzato (Centralized Forwarding). La scelta deve essere possibile per singola WLAN.
8. Al fine di essere predisposto a eventuali cambi di esigenza ed espansioni si richiede anche che il controller:
a. Supporti i protocolli Vlan 802.1q, le VPN e NAT/SNAT necessari per collegamenti con altre sedi
b. Debba essere predisposto a gateway di pagamento con possibilità di fare ticketing con emissioni di password uniche con scadenze temporali.
c. Deve poter supportare anche la funzione "Captive Portal" con autenticazione Social network come "facebook"
d. Abbia una garanzia a vita
9. Ai fini della sicurezza della salute dei docenti, alunni, personale della struttura ecc il controller deve gestire Access Point certificati EN 60601-1-2:200 – certificazione in ambito elettromedicale che minimizza le interferenze radio e i concorrenti dovranno allegare tale certificazione
10. Il controller deve supportare Routing Statico con VLan routing per la comunicazione tra le vlan.
11. Gestione delle policy di Quality of Service (QoS) sulle varie WLAN (Wireless LAN) per consentire la prioritizzazione del traffico su WLAN multiple, a seconda del tipo di traffico supportato (navigazione, VoIP, etc.); la QoS di una WLAN dovrà supportare:

a) Protocollo WMM (Wi-Fi Multimedia) con capacità WMM Power Save;

b) b. Classificazione WMM del client wireless, che dovrà includere diversi profili del tipo seguente sulla WLAN:

Traffico Voce.
Traffico Video.
Traffico Normale (best effort).
Traffico Low Priority

12. Supporto dei Multicast Frames per supportare data rate più elevati

13. Supporto del roaming a livello Layer 2 o Layer 3 per la mobilità dei client da un Access Point all'altro

14. Server DHCP integrato

15. Supporto di funzionalità di sicurezza a livello centralizzato:
    a) Supporto della funzionalità di NAT/SNAT
    b) Supporto del protocollo 802.11i
    c) Supporto della cifratura WPA2-CCMP (AES)
    d) Supporto della cifratura WPA2 TKIP
    e) Supporto della cifratura WPA TKIP
    f) Supporto del protocollo RADIUS

16. Supporto di funzionalità di Autenticazione a livello centralizzato:

17. Protocolli 802.1x/EAP:

    EAP-MD5, EAP-TLS, EAP-TTLS, EAP-FAST, EAP-SIM, PEAP-GTC, PEAP-TLS, PEAP-MS-CHAPv2

18. Supporto di protocolli SNMP v1, 2 e 3.

19. Il Centro di Controllo dovrà includere funzioni e strumenti di analisi e risoluzione dei problemi (troubleshooting). Gli strumenti di troubleshooting potranno essere utilizzati per la scoperta l'analisi e la risoluzione proattiva di eventuali problemi.

20. Gli Access Point dovranno essere in grado di generare e gestire i log, le quali potranno essere poi aggregate e inviate al Centro di Controllo oppure gestite direttamente dagli Access Point, in caso di assenza di collegamento con il Centro di Controllo stesso.

1.2 Access Point

Le prestazioni degli Access Point in fornitura devono essere all'avanguardia sia dal punto di vista radio che per quanto riguarda le funzionalità di gestione dei client, del routing e della banda disponibile. Essi devono supportare le seguenti caratteristiche:

1. Gli Access Point in offerta devono essere conformi agli standard IEEE 802.11a, 802.11b, 802.11g, 802.11n. Quest'ultimo standard deve essere supportato sia nella banda 2.4 GHz che 5 GHz.
2. Gli Access Point in offerta devono essere alimentabili in modalità Power-over- Ethernet (PoE) in accordo allo standard IEEE 802.3af, senza perdita significativa di prestazioni
3. Gli Access Point in offerta devono avere una porta Gigabit Ethernet, indicatori LED di diagnostica.
4. Gli Access Point in offerta devono supportare il meccanismo del "VLAN tagging" secondo lo standard 802.1q. Gli AP devono poter essere gestiti su di una "tagged VLAN".
5. Gli Access Point in offerta possono essere aggiornati automaticamente col software appropriato via rete e senza necessità di interventi in campo, a partire dal Centro di Controllo.
6. Gli Access Point in offerta devono essere di tipo Dual Radio (Band Unlocked) / Dual Band, in grado di offrire accesso ai client sia nella banda 2,4 GHz che 5GHz
7. Gli Access Point in offerta devono supportare in standard 802.11n canali da 20MHz e 40MHz e Data Rate fino a 300Mbit/s.
8. Gli Access Point in offerta devono supportare almeno 8 SSID (Service Set Identifiers); per ogni SSID dovrà essere possibile definire delle policy specifiche per la sicurezza e l'autenticazione.
9. Con il fine di avere una copertura ottimale gli Access Point dovranno essere di formato smoke detector e dotati di antenne integrate,
10. Gli Access Point in fornitura devono supportare funzioni RF avanzate quali:
    APFlex Technology
    Intra-BSS Traffic Blocking/Layer-2 Isolation
    Smart Classroom Load Balancing for EDU
    Smart Wi-Fi Management
    Dynamic Channel Selection/Smart Load Balancing/Auto Healing
    Band Select/Client Signal Treeshold/ZyMesh Technology
    Hotspot/QR Code
    Local/Centralized Controller
    Free Live Monitoring & Statistics
    Smart Classroom Load Balancing for EDU
    Centralized & Batch Configuration via Software
11. Gli Access Point devono poter essere gestiti sia a livello di Centro di Controllo che singolarmente, tramite accesso di tipo CLI oppure di tipo GUI.

Ogni Access Point in offerta dovrà includere localmente le seguenti funzionalità di sicurezza:

1. Funzioni anti-intrusione a livello wireless native (ovvero funzioni dette di Wireless Intrusion Detection System o WIDS e di Wireless Intrusion Prevention System o WIPS)
2. Sistemi di criptografia:
    WEP a 64 e 128 bit
    WPA-TKIP
    WPA-PSK TKIP
    WPA-AES
    WPA-PSK-AES WPA-802.11i WPA2- AES WPA2-PSK-AES WPA2-TKIP
    WPA2- PSK-TKIP 802.1X

Ogni Access Point in offerta dovrà includere localmente le seguenti funzionalità di networking:

1. Server DHCP integrato
2. Funzionalità integrata di gestione della Quality of Service (QoS) : WMM,802.1p, Diffserv e TOS

3. Capacità locale (ovvero integrata nell'Access Point) di gestione degli aggiornamenti e delle configurazioni di firmware
4. Protocolli 802.1q/p,DHCP server/client, Load-balancing del traffico con Rate Limiting e Bandwidth Management
5. VLAN estese Wired/Wireless : a livello di VLAN, gli Access Point devono consentire di estendere le VLAN della rete wired alla rete wireless.
6. Gli access point devono avere una garanzia a vita ed essere certificati EN60601-1-2:200- certifica che minimizza le interferenze radio.
7. 6.Gli access point devono supportare il Rouge AP detection per la prevenzione degli apparati non autorizzati presenti in rete
8. Supporto della funzione self configuration cluster che permette in assenza di controller di gestire in modo centralizzato gli access point presenti partendo da un access point master.

1.3 Apparecchiature per collegamenti alla rete internet Switch

Le prestazioni degli Switch in fornitura devono essere in grado di gestire al meglio il traffico dati della rete dell'istituto e per questo devono avere le seguenti caratteristiche:
- Devono avere le dimensioni necessarie per essere montati in rack
- Tecnologia Ethernet su cavi in rame: 1000BASE-T, 100BASE-T, 10BASE-T
- Standard di rete: IEEE 802.1D, IEEE 802.1Q, IEEE 802.1s, IEEE 802.1w, IEEE 802.1x, IEEE 802.3ad, IEEE 802.3af, IEEE 802.3x
- Garanzia : **Limited Life time – a vita.**
- POE: 802.3af; 802.3at
- Quantità di porte: almeno 8 porte POE Gigabit 10/100/1000

Site survey da effettuare a carico della ditta appaltatrice: indipendentemente dalla soluzione e dal numero di AP WIFI offerti, la copertura delle zone richieste deve essere completa:

Si richiede uno studio di pianificazione del posizionamento degli AP WIFI nelle aree interessate al progetto tramite uno strumento software di simulazione di copertura radiofrequenza. Lo strumento software dovrà utilizzare mappe digitali in 2D che modellino accuratamente le aree e gli ostacoli alla propagazione e riportino sulle stesse mappe il livello di segnale RF (RSSI) con aree di colore differenti, allo scopo di predire il comportamento del sistema Wi-Fi proposto dal punto di vista RF.

In fase di offerta, l'offerente dovrà riportare i risultati dello studio di pianificazione radio, riportando un'accurata descrizione degli strumenti e delle metodologie utilizzate e dei risultati ottenuti, compresi i grafici e le mappe di copertura.
E' richiesta anche un site survey WI-FI dopo l'installazione ed attivazione dei nuovi AP in modo da poter evidenziare discrepanze tra la simulazione software inziale e l'effettivo stato di fatto.
In tutti i casi, il site survey dovrà essere obbligatoriamente completo di report e visual mapping per i seguenti parametri:
• posizionamento e copertura degli Access Point;
• distribuzione e potenza del segnale;
•rapporto segnale/rumore;
•interferenze;
• data rate.
L'Istituto garantirà l'accesso alle aree in cui effettuare il sopralluogo e fornirà le planimetrie delle strutture interessate.

In conclusione, a fine lavori l'offerente dovrà aver presentato in ordine temporale i seguenti documenti:

1. Progetto di massima, completo di posizionamento AP WIFI e simulazione di copertura che si intende realizzare (in fase di offerta).
2. Progetto Esecutivo, completo di ogni dettaglio di configurazione che la ditta appaltatrice intende utilizzare (dopo l'aggiudicazione del bando e prima dell'inizio lavori).
3. As-built, completo dei risultati del site survey (a seguito del collaudo dell'impianto).
4. Collaudo a fine lavori
5. Ulteriore test a pieno regime (con docenti e studenti in orario scolastico).
6. L'assistenza per le eventuali riparazioni deve prevedere l'intervento entro le 24 ore lavorative.

Apparati richiesti

QUANTITA'	DESCRIZIONE
16	**ACCESS POINT DUAL RADIO PER RETE WIRELESS GESTIBILI VIA WEB** Access point 802.11AC Gestibile tramite controller Wirelless LAN con formato Smoke detector e antenne integrate Unified Access Point Dual-Radio, Frequenza Radio 2,4 Ghz e 5 Ghz funzionanti contemporaneamente, Banda di Frequenza 2,4Ghz: IEEE 802.11 b/g/n Europe(ETSI): 2.412 - 2.472 GHz, Banda di Frequenza 5 Ghz: IEEE 802.11 a/n Europe(ETSI): 5.15 - 5.35 GHz; 5.470 - 5.725 GHz Antenne Interne 2x2 3dBi / 2dBi GHz. Potenza di trasmissione e gestione canali automatica. Porte LAN 1x 10/100/1000Mbps PoE (Power Over Ethernet), Funzionalità WLAN 802.11 a/g: fino a 54 Mbps 802.11n fino a 300 Mbps in MCS15 (40MHz; GI=400ns) WMM (Wi-Fi certified), WEP, WPA/WPA2-PSK, WPA2 (Wi-Fi certified), WPA/WPA2-Enterprise, VLANs, DHCP client, SSID multipli, APFlex Technology, Intra-BSS Traffic Blocking/Layer-2 Isolation, Smart Classroom Load Balancing for EDU, Smart Wi-Fi Management, Dynamic Channel Selection/Smart Load Balancing/Auto Healing, Band Select/Client Signal Treeshold/ZyMesh Technology, Hotspot/QR Code, Local/Centralized Controller, Free Live Monitoring & Statistics , Smart Classroom Load Balancing for EDU, Centralized & Batch Configuration via Software • **Nessun canone annuale di gestione per il funzionamento del sistema.**
16	**INSTALLAZIONE ACCESS POINT** Installazione access point con realizzazione link di collegamento tra AP ed armadio di piano, con cavo in categoria 6 Gigabit, posato in canalina PVC ispezionabile. **Il collegamento deve essere testato e certificato tramite strumento certificatore per la categoria 6 Gigabit, con certificato di taratura in corso di validità, e rilascio finale della certificazione di ogni punto realizzato.** La posizione dell'access point dovrà essere tale da garantire la massima copertura, e tale copertura dovrà essere certificata, con rilascio obbligatorio della mappa di copertura a fine installazione realizzata tramite software di site survey.
1	**CONTROLLER HARDWARE PER GESTIONE CENTRALIZZATA ACCESS POINT** Unified Access Gateway che integra access gateway e wireless controller in un unico apparato All-in-One con gestione e regolamentazione degli account, la tariffazione, la sicurezza e la conservazione dei dati, WLAN Controller, e funzionalità Firewal. Servizio di Content Filtering (filtra l'accesso alle pagine web che non sono legate al business o che sono malevoli Utilizzando un completo database cloud di oltre 140 miliardi di URL continuamente analizzati e tracciati). Gestione fino a 32 AP, Porte 10/100/1000 Mbps RJ-45: 3 x LAN, 2 x WAN, Porte USB 2, WLAN controller, Numero di Managed AP (default/max.): 16/32, Dual-WAN load balancing, failover and fallback, Universal Plug and Play (UPnP), IP Plug and Play (iPnP), NAT/PAT, Static routing and policy routing, DHCP client/server/relay, HTTP proxy support, SMTP redirection, VPN 1-to-1 mapping, VPN pass-through, WAN client: static, DHCP, PPPoE, PPTP, Tagged VLAN (802.1Q), DDNS, Stateful packet inspection firewall, 10-channel IPSec VPN support (site-to-site), L2 isolation, User-aware security policy, Session limit, IP pass-through (white list)
3	**SWITCH GESTIBILE 8 PORTE GIGABIT POE** 8 Porte a 10/100/1000 BaseTX; gestione VLAN tagged; supporto Link Aggregation; supporto SNMP; interfaccia di gestione via Web. Montaggio a rack.

Il Dirigente Scolastico
Cristina Ighina