



**DIREZIONE SISTEMI INFORMATIVI**

**FORNITURA, GARANZIA E MANUTENZIONE**

**NAC - NETWORK ACCESS CONTROL**



**DOCUMENTO TECNICO E CONTRATTUALE**

## Sommario

|   |    |
|---|----|
| Art. 1 – Premessa .....   | 3  |
| Art. 2 – Stato dell’Arte.....                                       | 4  |
| Art. 3 - Oggetto della fornitura .....                              | 5  |
| Art. 4 – Requisiti minimi .....                                     | 11 |
| Art. 5 - Durata della fornitura e Importo del contratto.....        | 11 |
| Art. 6 - Modalità di conduzione del Progetto.....                   | 12 |
| Art. 7 - Oneri.....   | 14 |
| Art. 8 - Collaudo finale, fatturazione e pagamento.....             | 14 |
| Art. 9 - Risoluzione, recesso e foro competente .....               | 14 |
| 9.1. Risoluzione del contratto .....                                | 15 |
| 9.2. Clausola risolutiva espressa .....                             | 16 |
| 9.3. Modalità ed effetti della risoluzione. Facoltà di recesso..... | 16 |
| 9.4. Controversie.....  | 17 |
| Art 10 - Livelli di Servizio minimi e penali.....                   | 17 |
| 10.1 - Livelli Servizio Minimi .....                                | 17 |
| 10.2 - Penali .....   | 19 |
| 10.3 - Modalità e workflow richiesta interventi.....                | 20 |

## **Art. 1 – Premessa**

Il Comune di Firenze (di seguito denominato Ente e/o Amministrazione) al fine di realizzare una infrastruttura di rete sicura intende individuare e realizzare soluzioni integrabili per evitare accessi non autorizzati alla intranet. Tale soluzione deve essere applicabile sia a connessioni cablate che WiFi, ciò permetterebbe di venire incontro a quanto indicato sia nel piano triennale per l'informatica della P.A. (sicurezza, monitoraggio, WiFi) sia nel progetto di "Lavoro Agile" da poco avviata la sperimentazione del Comune di Firenze.

Nelle sedi dove l'accesso alla rete non è esclusivo di un utente è necessario prevedere un sistema per il controllo di accesso alla rete denominato Network Access Control (di seguito denominato NAC) con il protocollo 802.1x che permette di individuare se l'utente o il dispositivo sia abilitato ad aver l'accesso o meno.

A livello WiFi, si vuole rendere possibile un accesso alla rete Intranet mediante l'attivazione di una politica più forte che sfrutti sempre le caratteristiche del protocollo 802.1x e che in alcuni sistemi è denominata WPA2 Enterprise .

Allo stato pratico si vuole attivare un sistema che preveda l'accesso 802.1x + MAC Authentication sia a livello Wired che Wireless.

Per rendere l'idea di come funzioni si riportano alcuni esempi:

- Nel momento in cui un dispositivo viene collegato ad una qualsiasi porta di rete se lo stesso è correttamente configurato con 802.1x e l'utente inserisce delle credenziali di dominio valide, allora la porta dello switch viene configurata per l'accesso alla Intranet aziendale, in caso contrario viene posizionato in una VLAN di registrazione e nel caso vengano inseriti dei "parametri" validi (registrazione tramite gestione di ticket etc etc.....), viene configurata la porta in una VLAN di sola navigazione su altra connettività non istituzionale; in ultima ipotesi se nessuna delle due condizioni precedenti è soddisfatta la porta viene posta in una VLAN black (Vlan chiusa o di confinamento).
- Un dispositivo che si collega al WIFI, può collegarsi al SSID con attivo l'802.1x solo se è debitamente configurato e venga utilizzata un'utenza di dominio valida.

L'accesso alla rete guest o di sola navigazione internet è già fornita tramite il SSID FirenzeWiFi.

## **Art. 2 – Stato dell'Arte**

Alla luce di ciò, il Comune di Firenze dispone di un'infrastruttura di rete articolata in una Metropolitan Area Network (di seguito anche MAN) proprietaria in fibra ottica, denominata FiNet a cui afferiscono in vari siti della città le varie sedi che fanno capo all'Amministrazione. Le varie sedi sono in Intranet con la sede della Direzione Sistemi Informativi (di seguito anche DSI) di Via Reginaldo Giuliani, mediante una topologia ad anello (o su più anelli in fibra), dove ogni sede è "ruotata" a livello 3 (di seguito denominato L3) rispetto alla sede DSI. All'interno della FiNet vengono altresì veicolate, a livello 3, alcune VLAN per le varie attività (WiFi, Intranet Uffici, Internet, ecc.)

La MAN comunale è dotata di una serie di apparati Cisco della serie 3550, 3750, ME-3600X e ASR-9000, mentre la Intranet delle varie sedi è composta da una serie di apparati switch, con la funzione di accesso per i client, nella maggior parte del produttore Allied Telesys (di seguito denominato ATI) nei modelli 8000s, 8000g, X230, X510 e Centrecom FS980M ed in alcuni casi sono presenti dei Cisco Catalyst (2950, 2960 e 2960X).

Gli apparati ATI montano una versione di firmware del 2012 e nello specifico i modelli 8000s la versione 3.0.0.45, mentre i modelli 8000g la versione "2.0.0.27". La sede della D.S.I (ed alcune sedi remote) è dotata di una serie di apparati ATI della serie X510, X230 e Centrecom FS980M che svolgono la funzione di accesso per le postazioni client e tali apparati sono attualmente alla versione di firmware "AlliedWare Plus 5.4.7". Gli apparati del produttore Cisco hanno, di norma, a bordo la versione di firmware "12.1(22)EA13" per i modelli 2950, mentre i modelli 2960 hanno, di norma, a bordo la versione di firmware "15.2(2)E6" .

A livello di infrastruttura WiFi le sedi più "importanti" sono dotate di installazioni di un numero variabile, a seconda delle esigenze, di Access Point dei seguenti produttori/modelli:

- Piattaforma Cisco (modelli della serie 1600 e 2600 e WLC 5508 firmware 8.0.152.0)
- Piattaforma Ubiquiti (modelli della serie Unifi: AC-Lite, AC-Pro e Mesh, attualmente alla versione firmware 4.0.42.10433 con controller versione 5.10.24)

Entrambe le piattaforme sono controlled-based e permettono quindi configurazioni personalizzate sia a livello di Wireless Local Area Network (di seguito denominata WLAN) che di VLAN per il trasporto dati degli utenti.

Per quanto riguarda il VOIP, attualmente alcune sedi hanno soluzioni con reti a apparati switch fisicamente separati, mentre in altre viene utilizzata una VLAN VOIP dedicata utilizzando switch POE solitamente della serie Cisco 2960X. Inoltre è in atto, da parte della direzione preposta, la migrazione della telefonia "tradizionale" con soluzioni VOIP anche su altre sedi.

A livello di infrastruttura server centralizzata ovverosia dove sarà obbligatorio procedere con il dispiegamento del nuovo sistema (dei nodi, delle vm o delle appliance che lo compongono), si rimanda alla lettura dell'Allegato 3 - Infrastruttura di dispiegamento.

### **Art. 3 - Oggetto della fornitura**

La soluzione Open Source di NAC della presente fornitura è la soluzione NAC OpenSource PacketFence, ultima versione disponibile al momento dell'installazione (anche come versione di sistema operativo). Tale soluzione non deve avere costi di licenza, installabile in ambiente virtuale, scalabile e che abbia caratteristiche e funzionalità idonee al contesto del Comune di Firenze.

A corredo dell'offerta presentata dovrà essere prodotto ed allegato un documento di progetto dove vengono evidenziate le soluzioni alle problematiche indicate nel presente documento di gara. Tale allegato sarà solo oggetto di verifica tra quanto richiesto e quanto offerto e non sarà oggetto di altra valutazione, né di assegnazione di punteggi.

Tale documento allegato dovrà essere redatto obbligatoriamente in lingua italiana e composto da un massimo di **20 (*venti*)** pagine in formato A4. Si precisa che per la stesura del documento richiesto si dovrà impiegare il carattere "Times New Roman", o analogo, a 12 (dodici) punti e interlinea 1 (uno) e che nel computo delle pagine si escluderà la copertina, il frontespizio e l'indice. Inoltre il documento indicato dovrà essere fornito in formato elettronico non-modificabile, preferibilmente anche nello standard internazionale ISO 19005-1:2005 noto come PDF/A, e firmato digitalmente in sede di presentazione dell'offerta stessa.

La piattaforma NAC dovrà prevedere un'installazione clusterizzata di tipo attivo-passivo in ambito geografico (Fig. 1), ovvero sarà necessario che i due nodi funzionanti (vm applicative o anche "appliance autocontenute") siano installati su due diversi cluster di virtualizzazione, dislocati fisicamente in due sedi distinte, ma comunque visibili fra loro a livello 2 del modello ISO/OSI (LAN extension), dove un nodo avrà la funzione di master e l'altro di hot-standby. La soluzione dovrà prevedere un funzionamento di fault-tolerance in alta affidabilità e failover automatico in modo tale che per gli apparati di rete l'eventuale down di un nodo sia del tutto trasparente e tutte le funzioni siano migrate automaticamente dal nodo master al nodo in standby. La soluzione clusterizzata non dovrà prevedere costi di licenza aggiuntivi per l'Amministrazione.

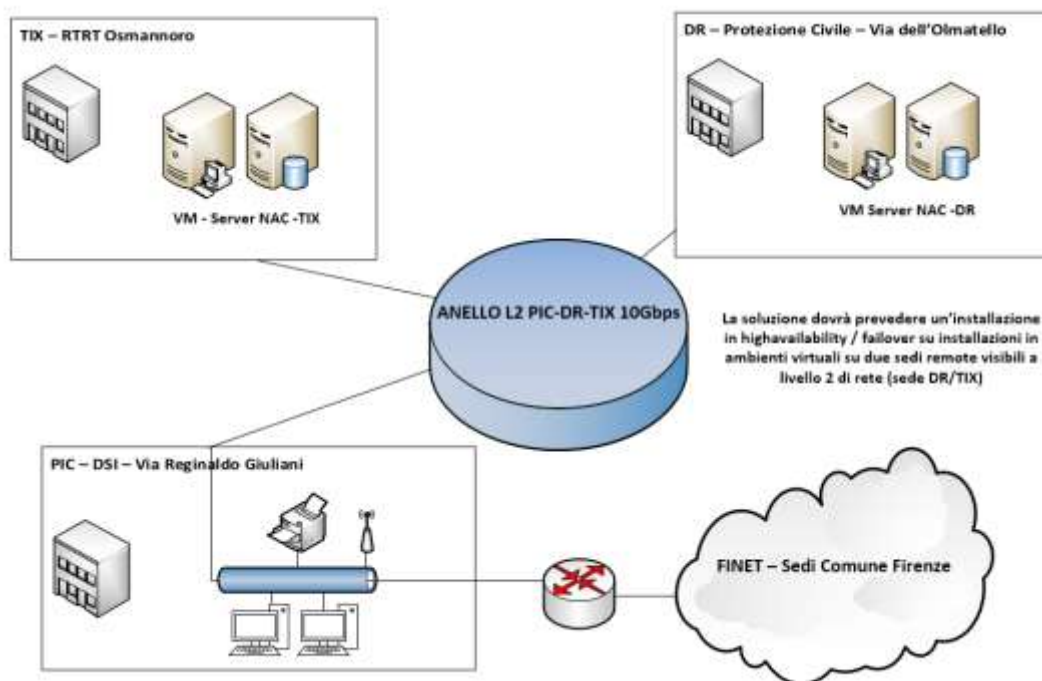


Fig. 1 - Architettura

La piattaforma NAC inoltre deve prevedere l'interfaccia di configurazione sia in modalità grafica (di seguita denominata GUI) che a linea di comando.

Gli apparati delle sedi che saranno oggetto dell'introduzione progressiva di questo nuovo modello di accesso alla rete dell'Amministrazione vedranno la piattaforma NAC a livello 3 del modello ISO/OSI.

La piattaforma NAC dovrà essere configurata per essere supportata da tutti gli apparati indicati nella sezione "stato dell'arte" e allegato 1- "Apparati rete" compatibili con il protocollo 802.1x, in modo da affrontare le eventuali problematiche di configurazione che si potrebbero presentare nel momento dell'introduzione di essa in tutta la rete dell'Ente.

Gli apparati nella sezione "stato dell'arte" e allegato 1- "Apparati rete" se non compatibili, verranno segnalati dall'aggiudicatario per poi provvedere da parte dell'Ente alla sostituzione con apparati compatibili.

La soluzione proposta dovrà tenere conto che una sede remota possa risultare isolata, ovvero gli apparati/switch della sede non siano in grado di dialogare con la piattaforma NAC centrale e quindi la soluzione proposta dovrà permettere o avere una

configurazione tale negli apparati/switch della sede isolata (fatto salvo la compatibilità con gli apparati presenti nella sede) che un funzionamento a livello 2 dei dispositivi della stessa sede sia garantito (es. i PC della sede possano vedere le stampanti di rete ecc. ecc.). Oltre a quanto appena descritto, la soluzione NON dovrà comportare l'installazione di un sistema di controllo NAC remoto in modo da evitare problematiche di idoneità dei locali tecnici delle sedi periferiche oltre che ad eventuali oneri di manutenzione di hardware aggiuntivo.

Ai fini della sicurezza si rende necessario che gli apparati di rete possano prevedere l'utilizzo di almeno due server Radius distinti uno per la gestione dell'apparato (SSH, ...) e uno per l'autenticazione 802.1x. L'aggiudicatrice dovrà comunicare quali apparati indicati nell'allegato 1 - "Apparati rete" consentano tale distinzione e quali no. Nel secondo caso, in cui non sia possibile avere due server Radius distinti tali apparati saranno considerati *"parzialmente idonei"*.

L'analisi e le soluzioni alle problematiche deve seguire un approccio di tipo top-down, andando quindi ad affrontare le possibili soluzioni a seconda delle problematiche che si manifestano in corso d'opera; per questo sono state definite sei Milestone di sviluppo, sotto descritte.

In quest'ottica si delinea un modello in cui si prevede la possibilità di accesso sia in cablato sia in WiFi che permetta di effettuare tre tipi di connessioni dei dispositivi client:

- verso la Intranet aziendale
- verso una rete guest, nelle sedi dove è presente la FirenzeWiFi, la soluzione deve permettere di assegnare all'apparato di rete la VLAN della FirenzeWiFi
- verso una rete isolata bloccante per il client.

L'abilitazione all'accesso ad una delle tre tipologie di rete è soggetta ad una serie di condizioni:

- in base alla tipologia di utente che effettua accesso al sistema (utente dominio, utente ospite, utente non classificato)



- in base al mac-address del dispositivo (apparati tipo stampanti, fotocopiatrici di rete ecc) o tramite tecnologie come DHCP Fingerprint (eventuali licenze non devono comportare un costo aggiuntivo per l'Amministrazione ma sono da considerarsi compresi nella fornitura)

Come sviluppo futuro è immaginabile pensare che l'abilitazione alla rete Intranet sia ulteriormente vincolata secondo una policy di sicurezza che dovrà essere stabilita (es: è presente un'antivirus, quale versione, è aggiornato ecc ecc).

L'accesso alla rete Intranet aziendale deve poter essere consentito almeno a:

- a) agli utenti di dominio Active Directory appartenenti al dominio.
- b) determinati apparati che non hanno la possibilità di avere una configurazione di dialogo con il dominio di Active Directory (esempio abilitando il Mac address dell'apparato, vedi stampanti, telecamere, telefoni VOIP altri sistemi simili)
- c) eventuali altre categorie individuate nel piano di progetto presentato dalla ditta e/o eventuali "situazioni" che si verificano in fase di installazione e avvio della piattaforma

Per la rete guest non deve comunque essere esclusa l'opzione di poter gestire, in futuro, la possibilità con soluzione captive portal permettendo agli ospiti un'auto-registrazione con invio di una password OTP da utilizzare per l'abilitazione della rete. Tale soluzione non dovrà comunque prevedere costi aggiuntivi per l'Amministrazione (es. costi per invio di sms o simili).

Il riconoscimento delle tipologie di utente sarà effettuato in base ad una configurazione specifica della piattaforma NAC la quale identificherà gli utenti di Dominio mediante l'interfacciamento al sistema degli utenti gestito dal Domain Controller Microsoft che gestisce il dominio aziendale, attualmente alla versione Windows server 2012 (e comunque che sia supportato dalla versione indicata e per quelle superiori; si prevede infatti la possibilità di un aggiornamento alla versione Active Directory di Windows 2016 già nel corso dell'anno 2019 o nell'anno successivo).

I PC facenti parte delle policy aziendali e che rientrano nelle sedi in cui si avvia l'introduzione della piattaforma NAC avranno una configurazione di sistema/rete che

supporti le specifiche per l'802.1x tali da permettere il corretto scambio di informazioni fra dispositivo - apparato di rete - piattaforma NAC centralizzato.

In quest'ottica dovrà essere oggetto di fornitura anche una manualistica (o linee guida di tipo how-to) per la corretta configurazione del protocollo 802.1x per PC con S.O.: Windows XP, Vista, Seven, 8, 8.1, 10; Linux: Ubuntu 16 LTS o superiori, CentOS/RedHat 5, 6, 7 o superiori; OSX e più in generale fornitura delle linee guida per l'introduzione nella Intranet di un nuovo dispositivo che sia un nuova Postazione di Lavoro, stampante o qualsiasi dispositivi che necessita l'accesso alla rete.

Nell'ottica di poter estendere in sviluppi futuri le features della piattaforma NAC nella soluzione proposta, dovrà essere indicata l'eventuale fattibilità e relativa possibilità (descrivendo anche eventuali moduli aggiuntivi se necessari):

- di una configurazione per la creazione delle regole di **"Violations"** e quindi il blocco dell'accesso alla risorsa di rete qualora il dispositivo collegato effettui una tipologia di traffico non consentita. A titolo di esempio la piattaforma dovrà potersi collegare con sistemi IDS di tipo OpenSource quali Suricata o suite Linux quali Security Onion e similari .
- dell'integrazione con sistemi di **"Compliance Check"** in uso presso l'ente, qualora ci sia l'esigenza di alzare il livello di policy necessaria per l'accesso alla Intranet aziendale; es: il S.O. client sia aggiornato, sia presente un antivirus aggiornato ecc. ecc.

### **Training on the job**

In tutte le fasi di installazione/attivazione della configurazione sui sistemi interessati si dovrà tenere un approccio di tipo training-on-the-job in modo tale che il personale che dovrà seguire la gestione della nuova piattaforma sia in grado conoscere i vari aspetti di configurazione ed intervenire in caso di problematiche di rete e/o sistemistiche.

A tal riguardo si prevedono almeno 18 ore di attività sul funzionamento della piattaforma da effettuarsi una volta completata la fase due/tre nella sede DSI di via Reginaldo Giuliani.

## **Art. 4 – Requisiti minimi**

L'azienda singola, o all'interno del consorzio di aziende le varie aziende, deve:

- **RM01** aver eseguito negli ultimi 3 anni almeno n.1 fornitura e gestione di sistemi di networking con soluzione di controllo accesso rete a soggetti terzi per almeno € 10.000,00 IVA esclusa
- **RM02** – essere iscritta al MePA ad almeno una sezione tra :
  - SERVIZI - Servizi per l'Information & Communication Technology
  - BENI - Informatica, Elettronica, Telecomunicazioni e Macchine per Ufficio

### **Requisiti professionali e di capacità economica:**

- **RM03** requisiti di idoneità professionale: iscrizione alla CCIAA con oggetto sociale attinente alla prestazione richiesta nel presente avviso;
- **RM04** requisiti di ordine generale: requisiti di cui all'art. 80 del Dlgs 50/2016
- **RM05** requisiti di capacità economia e finanziaria: fatturato minimo annuo pari ad almeno 50.000,00 euro;

### **Requisiti tecnici:**

- **RM06** il NAC Open Source dovrà essere basato su PacketFence ultima versione disponibile al momento dell'installazione
- **RM07** gli aggiornamenti di "major version/release" sono a carico dell'aggiudicatario e quelli "minor release" sono in collaborazione con il personale "P.O. Reti, internet delle Cose e Multimedialità"
- 

## **Art. 5 - Durata della fornitura e Importo del contratto**

Complessivamente la durata della fornitura sarà di 3 anni dal momento dell'affidamento e sarà definita dalle seguenti milestone:

- **Milestone zero:** entro 15 giorni dalla stipula dell'ordine dovrà essere effettuato il kickoff, entro 5 giorni dalla conclusione del kickoff, la ditta aggiudicataria dovrà fornire le specifiche.
- **Milestone uno:** 2 mesi dalla comunicazione della Committente della predisposizione dell'ambiente di virtualizzazione e delle relative VLAN necessarie

- **Milestone due:** 1 mese a conclusione della Milestone precedente
- **Milestone tre:** 1 mese a conclusione della Milestone precedente
- **Milestone quattro:** avvio a fine Milestone precedente, secondo le tempistiche del piano di attivazione.
- **Milestone cinque:** 1 mese dall'avvio della fase e comunque in parallelo con Milestone 4

Ad ogni Milestone verrà redatto un verbale firmato da entrambi le parti con l'indicazione del superamento o meno dei test.

Importo del contratto a base d'asta € 30.000 + IVA così suddivisi:

- €25.000+IVA (Investimenti)
- €5.000+IVA (Servizi):
  - 20% fatturazione anno 2019
  - 40% fatturazione anno 2020
  - 40% fatturazione anno 2021

## **Art. 6 - Modalità di conduzione del Progetto**

Di seguito la descrizione delle sei Milestone (le attività sono da svolgere tutte on-site):

- **Milestone zero:** "kickoff" e predisposizione dell'infrastruttura virtuale e di rete:
  - il primo kickoff presso la sede Direzione Sistemi Informativi Via Reginaldo Giuliani 250 – Firenze con le unità "P.O. Reti, Internet delle Cose e Multimedialità ", "P.O. Data Center, Sistemi e Cloud" e "Postazioni di Lavoro" per illustrare la consistenza della rete, dell'infrastruttura virtuale e delle postazioni di lavoro (di seguito denominate PdL);
  - comunicazione della ditta delle specifiche che dovranno avere le macchine virtuali per una installazione HA previste dal documento
  - creazione macchine virtuali e configurazione dell'infrastruttura di rete esistente da parte delle unità unità "P.O. Reti, Internet delle Cose e Multimedialità ", "P.O. Data Center, Sistemi e Cloud" con il supporto della ditta.

- **Milestone uno:** "startup1", vede l'installazione dei nodi virtuali presso la sede "TIX" e presso "DR" in configurazione di alta-affidabilità secondo le specifiche del documento; successivamente si passerà alla verifica della compatibilità degli apparati switch in uso al Comune con la produzione di un'adeguata reportistica. In questa fase verranno illustrati i test che i tecnici dell'unità "P.O. Reti, Internet delle Cose e Multimedialità" hanno già effettuato col prodotto PacketFence su un campione di apparati, confrontando gli stessi con la soluzione proposta dalla ditta aggiudicatrice dell'appalto.
- **Milestone due:** "startup2", vede la prima sede di attivazione del NAC presso la sala PIC, ovvero tutta la DSI, produzione di reportistica e eventuale manualistica per la corretta configurazione del protocollo 802.1x per PC (S.O.: Windows xp, Vista, Seven, 8, 8.1, 10; Linux; OSX), stampanti e apparati di rete in genere comprensiva dell'analisi per la predisposizione di una configurazione centralizzata tramite Group Policy di Active Directory per i sistemi supportati.
- **Milestone tre:** vede l'estensione del NAC alla sede DR e Protezione Civile di Via dell'Olmattello.
- **Milestone quattro:** si provvederà ad affrontare le problematiche, qualora ce ne fossero, per l'attivazione sempre del modello sopra esposto in una o più sedi remote, collegate quindi a livello 3 con la DSI per poi procedere, secondo un piano di attivazione (che verrà comunicato in fase di installazione della piattaforma e che terrà conto della compatibilità degli apparati switch nelle varie sedi) nelle varie sedi del Comune di Firenze (vedi allegato 2 - "Sedi FiNet") e produzione reportistica.
- **Milestone cinque** (avviabile in contemporanea con la fase quattro): prevede l'introduzione dell'802.1x a livello WIFI sfruttando e configurando le tipologie di sistemi (piattaforme WiFi) installate presso il Comune di Firenze durante tutto il periodo della fornitura.

Per i Milestone 2,3,4 è probabile dover effettuare incontri con altre direzioni per apparati specifici

## **Art. 7 - Oneri**

Sono in carico all'Appaltatore tutte le prestazioni previste nel presente documento oltre ai costi per:

- le licenze software eventualmente necessarie per la durata del progetto, seguendo quanto indicato nei requisiti minimi sopra descritti
- il project management
- le attività necessarie a garantire la sua efficienza per tutto il periodo della fornitura.

## **Art. 8 - Collaudo finale, fatturazione e pagamento**

L'Amministrazione Comunale approverà il piano di test o ne richiederà integrazioni, dopodiché procederà alla esecuzione del collaudo assieme al fornitore.

La fatturazione avviene solo a comunicazione esito positivo del collaudo dell'installazione funzionante secondo le tranche sotto descritte.

Il pagamento in favore della Ditta Aggiudicataria sarà effettuato secondo le norme di legge in vigore. Il Fornitore dovrà sempre indicare nelle fatture le modalità di pagamento e riportare obbligatoriamente gli estremi del contratto, il codice CIG e gli estremi della determinazione dirigenziale che autorizza la spesa.

Il corrispettivo pattuito verrà fatturato successivamente alla data di sottoscrizione del contratto ed erogato in diverse tranche con le modalità di seguito indicate:

- Stipula ordine acconto 50% della parte Investimenti
- Verifica Milestone zero, uno, due, tre, quattro (relativo a 2 sedi definite dal committente di cui una con soluzione VOIP senza separazione fisica della reti dati e fonia) e il test del Milestone cinque, il rimanente 50% della parte Investimenti
- Al 31.12.2019 20% per la Manutenzione
- Al 31.12.2020 40% per la Manutenzione
- Al 31.12.2021 40% per la Manutenzione.

## **Art. 9 - Risoluzione, recesso e foro competente**

Per i casi di risoluzione e recesso si fa rinvio alle norme di cui agli artt. 108 e 109 del D.Lgs. 50/2016 e ss.mm.ii-

### **9.1. Risoluzione del contratto**

L'inadempimento degli obblighi espressamente assoggettati a risoluzione dal presente documento producono un'immediata risoluzione del contratto stesso, di diritto e di fatto, con esclusione di ogni formalità legale o di pronuncia di arbitri o di magistrati.

Le altre inadempienze della Ditta Aggiudicataria saranno contestate per iscritto dall'Amministrazione con fissazione di un termine per la relativa regolarizzazione e daranno luogo alla risoluzione contrattuale in caso di persistente inottemperanza del termine stabilito.

In tutti i casi di risoluzione l'Amministrazione potrà procedere nei confronti della Ditta Aggiudicataria alla determinazione dei danni eventualmente sofferti e rivalendosi con l'incameramento della cauzione e se ciò non bastasse, agendo per il risarcimento completo dei danni subiti.

In caso di cessazione, per la quale sarà dato preavviso di almeno 15 giorni, sarà dovuto il compenso per il servizio svolto fino al momento dell'interruzione.

In ogni caso, pur in presenza di disdetta, la Ditta Aggiudicataria sarà tenuta ad effettuare le prestazioni richieste fino alla data di scadenza naturale dell'appalto medesimo, qualora non possa essere assicurato il subentro di un altro aggiudicatario per l'espletamento del contratto.

L'Amministrazione avrà la facoltà di risolvere il contratto con tutte le conseguenze che tale risoluzione comporta, sia di legge, sia previste dalle disposizioni del presente documento, anche nelle seguenti ipotesi:

- Cessione del contratto, dell'attività, atti di pignoramento e sequestro a carico dell'impresa, fallimento;
- Fallimento o altre cause che possano pregiudicare l'espletamento del servizio, salvo il recupero dei maggiori danni sulla cauzione.

## **9.2. Clausola risolutiva espressa**

Il Comune si impegna ad avvalersi della clausola risolutiva espressa prevista, di cui all'art. 1456 cc, ogni qualvolta nei confronti dell'imprenditore o dei componenti la compagine sociale, o dei dirigenti della Ditta Affidataria, sia stata disposta misura cautelare o sia intervenuto rinvio a giudizio per taluno dei delitti di cui agli art. 317 c.p., 318 c.p., 319-bis c.p., 319-ter c.p., 319-quater c.p., 320 c.p., 322 .p., 322-bis c.p., 346-bis c.p., 353 c.p., 353-bis c.p.

## **9.3. Modalità ed effetti della risoluzione. Facoltà di recesso.**

L'Amministrazione si riserva la facoltà di recedere dal contratto per motivato interesse pubblico.

La risoluzione ed il recesso del contratto vengono disposti con atto dell'organo competente da notificare alla Ditta Aggiudicataria.

L'avvio e la conclusione del procedimento sono comunicati alla Ditta Aggiudicataria con PEC o lettera raccomandata con ricevuta di ritorno, indirizzata al domicilio legale indicato in contratto. Nella comunicazione di avvio viene assegnato il termine per presentare le proprie controdeduzioni. Dell'eventuale mancato accoglimento delle osservazioni è data ragione nella motivazione del provvedimento finale.

Nei soli casi di risoluzione del contratto per fatto dell'Aggiudicatario, l'Amministrazione ha la facoltà di affidare a terzi la parte rimanente del servizio, in danno dell'impresa inadempiente.

All'Aggiudicatario inadempiente sono addebitate le spese sostenute in più dall'Amministrazione rispetto a quelle previste dal contratto risolto, nonché quelle legali. Esse sono prelevate dalla cauzione incamerata e, ove questa non sia sufficiente, da eventuali crediti dell'Aggiudicatario inadempiente.

Nei casi di risoluzione del contratto per inadempimento dell'Aggiudicatario, l'Ente si riserva la facoltà di aggiudicare il servizio all'impresa che segue in graduatoria.



L'affidamento può avvenire con procedura negoziata ad affidamento diretto stante l'esigenza di limitare le conseguenze dei ritardi connessi con la risoluzione del contratto.

#### **9.4. Controversie**

Il Foro di Firenze sarà competente per tutte le controversie che dovessero insorgere in pendenza dell'appalto e del relativo contratto.

Ai sensi dell'art. 209 del D.lgs 50/2016 il contratto non conterrà la clausola compromissoria. E' pertanto escluso il ricorso all'arbitrato per la definizione delle controversie nascenti dal presente appalto. E' vietato in ogni caso il compromesso.

### **Art 10 - Livelli di Servizio minimi e penali**

#### **10.1 - Livelli Servizio Minimi**

**SLA01** - la disponibilità del servizio di garanzia/manutenzione e di assistenza/supporto tecnico (anomalie, problemi software, malfunzionamenti, ecc.) sulla piattaforma NAC e sulla vm a corredo dovrà essere garantito da lunedì a venerdì (giorni feriali) con inizio dalle ore 09:00 fino alle ore 17:00 (nove-diciassette, durata di otto ore) e sabato con orario 9:00-13:00 (nove-tredici);

**SLA02** - si intende per "**tempo presa in carico**" o "**tempo di intervento**" il periodo, espresso in ore lavorative secondo il modello orario sopra richiamato, che intercorre fra la segnalazione del problema da parte del personale dell'Ente e la comunicazione all'Amministrazione almeno della "diagnosi iniziale" e della stima/previsione fatta del tempo necessario a completare l'intervento (ovvero, a risolvere il problema):

- in caso di malfunzionamenti bloccanti, la segnalazione deve essere presa in carico entro 6 (sei) ore dalla richiesta. È opportuno precisare che per "guasto o anomalia bloccante" si intende una indisponibilità del sistema nel suo complesso per erogare i servizi richiesti, quindi trattandosi di una configurazione ridondata in clustering, il disservizio deve in qualche modo coinvolgere contemporaneamente i due apparati in quanto tutte le funzioni devono poter

essere fornite anche da uno solo di essi, come espressamente richiesto dal documento;

- in caso di malfunzionamenti non bloccanti e altre problematiche in genere, la presa in carico deve avvenire entro il giorno lavorativo successivo (NBD) a quello della segnalazione;

**SLA03** - si intende per "**tempo di ripristino**" il periodo, espresso in ore lavorative secondo il modello orario sopra richiamato, che intercorre fra la segnalazione del problema da parte dell'Amministrazione e il ripristino definitivo, o almeno parziale se approvato dal Committente, delle condizioni normali di operatività della piattaforma in manutenzione:

- in caso di problematiche che riducano in modo grave l'uso o compromettano in modo critico le funzionalità del sistema nel suo complesso (malfunzionamenti bloccanti), si deve provvedere al suo ripristino, o a porre in atto un adeguato work-around di natura temporanea e in ogni caso preventivamente concordato e approvato dal Committente, entro il giorno lavorativo successivo (NBD) a quello della segnalazione;
- in caso di problematiche che riducano solo in modo lieve la produttività, le prestazioni o per qualsiasi altra richiesta di assistenza e di supporto riguardante la piattaforma in manutenzione (malfunzionamenti non bloccanti e altre anomalie e problematiche in genere) si deve provvedere al ripristino entro il quinto giorno lavorativo successivo a quello dell'apertura della segnalazione del Committente.

Il livello di servizio base descritto spesso rientra in varianti della nota formula "8x5x4" e sarà in ogni caso la denominazione adottata nel presente documento per fare riferimento agli SLA minimi richiesti.

Nel caso che gli SLA indicati non siano rispettati, l'Ente si riserva di agire nelle sedi più opportune per tutelarsi nei confronti dell'eventuale danno arrecato dall'Aggiudicatario, quindi le penali sotto riportate sono definite sempre salvo risarcimento del maggior danno.

## **10.2 - Penali**

Per il calcolo delle penali, i valori ottenuti saranno arrotondati sempre per difetto al numero intero tralasciando, quindi, i decimali di euro.

Le penali, in conformità a quanto indicato dal Decreto legislativo n. 50 del 18 aprile 2016 e ss.mm.ii., saranno applicate nei seguenti casi:

**P01 - Ritardo nella "presa in carico" o nel "tempo di ripristino"** non imputabile al Committente e imputabile all'Aggiudicataria (salvo prova contraria), in caso di:

- **malfunzionamenti bloccanti** la penale equivale a 1/25.000 (un venticinque millesimo o 0,04‰) dell'importo di aggiudicazione per ogni ora intera (escluse le frazioni) lavorativa di ritardo nell'intervallo indicato, giorni festivi esclusi, della copertura obbligatoria minima richiesta o nella migliorativa offerta dall'Aggiudicataria, quindi per un massimo teorico, considerando di base gli SLA minimi richiesti, almeno pari allo 0,32‰ per ogni giorno lavorativo di ritardo (lun-ven) e 0,16‰ per sabato;
- **altre segnalazioni non bloccanti** la penale equivale a 1/50.000 (un cinquanta millesimo o 0,02‰) dell'importo di aggiudicazione per ogni ora intera (escluse le frazioni) lavorativa di ritardo nell'intervallo indicato, giorni festivi esclusi, della copertura obbligatoria minima richiesta o nella migliorativa offerta dall'Aggiudicataria, quindi per un massimo teorico, considerando di base gli SLA minimi richiesti, almeno pari allo 0,16‰ per ogni giorno lavorativo di ritardo (lun-ven) e 0,08% per sabato;

**P02 - Carenze professionali e/o qualitative nell'espletamento della fornitura;** qualora la formazione erogata, il personale tecnico, le tempistiche previste (ad es. per il collaudo, la formazione, etc.), non risultino adeguati/funzionanti, non rispondano ai livelli di professionalità richiesti o non siano di un livello soddisfacente, il Comune invierà una prima comunicazione formale di richiamo alla ditta Aggiudicataria e al produttore con l'indicazione dettagliata delle carenze rilevate. A tale prima

comunicazione, ditta Aggiudicataria, deve rispondere entro 5 (cinque) giorni lavorativi indicando i comportamenti e le soluzioni poste in essere, entro al massimo 3 (tre) giorni lavorativi a decorrere dalla data della risposta, per risolvere le criticità e le carenze. Qualora si verificassero successivamente i medesimi problemi di qualità e/o di inadeguatezza, il Comune potrà inviare una seconda comunicazione di richiamo e applicare contestualmente una penale di 1/2.000 (un due millesimo o 0,50‰) al giorno lavorativo per ogni episodio contestato. Al perdurare dei problemi l'Ente potrà continuare ad applicare le penali come sopra specificato;

**P03 - Ritardi di intervento durante il periodo di assistenza allo "startup 1 e 2";**

considerato il tempo di intervento fissato estremamente ristretto e la criticità o il disservizio che si potrebbe presentare in queste circostanze per l'Ente, in caso di anomalie o problematiche segnalate dal Committente e in caso di mancata attivazione dei tecnici nei tempi richiesti dal questo documento o in quelli migliorativi offerti dall'Aggiudicataria, verranno contestate immediatamente le mancanze e si inizierà ad applicare le penali. Rimane in tal caso totalmente a carico dell'Aggiudicataria provare la totale estraneità con le cause all'origine del ritardo, entro al massimo 2 (due) giorni solari dall'evento. La penale applicata in questi casi equivale a 1/50.000 (un cinquanta millesimo o 0,02‰) dell'importo di aggiudicazione per ogni ora intera (incluse le frazioni) di ritardo nell'intervallo di copertura indicato ovvero qualsiasi giorno solare dell'anno su 24h, quindi per un massimo teorico, considerando gli SLA richiesti, pari allo 0,48‰ per ogni giorno di ritardo.

**10.3 - Modalità e workflow richiesta interventi**

Una volta conclusa la procedura di affidamento, la ditta aggiudicataria concorderà con l'Ente i canali da utilizzare (FAX, PEC, numero verde, e-mail, web-ticketing, ecc.) e le modalità o il workflow da rispettare per la richiesta degli interventi in garanzia/manutenzione e la relativa presa in carico.

Per quanto non disciplinato dai casi specificati di cui al presente paragrafo, si fa espresso rinvio a quanto previsto dall'art. 113-bis del D.Lgs. 50/2016.

E' fatto salvo il diritto dell'Ente al risarcimento del maggior danno e la facoltà di risoluzione. Eventuali istanze di proroga dovranno essere documentate e quindi provate le cause di forza maggiore non imputabili all'Aggiudicatario.