COMUNE DI FONTE NUOVA

Implementazione e gestione di una Piattaforma d'integrazione per il progetto "Fontenuova.net SIMFO"

Capitolato Tecnico

Avviso

Le informazioni contenute in questo documento sono proprietà del Comune di FONTE NUOVA ("LA STAZIONE APPALTANTE") e sono protette dalla legislazione internazionale sul copyright (c) (Diritti di copia).

Sebbene ogni misura sia stata presa per assicurare che le informazioni contenute in questo documento siano aggiornate e accurate, LA STAZIONE APPALTANTE non potrà essere considerata responsabile per eventuali mancate accuratezze o errori nelle informazioni contenute in questo documento.

LA STAZIONE APPALTANTE non fornisce garanzia di alcun tipo circa le informazioni contenute in questo documento e non potrà essere ritenuta responsabile per danni diretti o indiretti che possano prodursi in relazione con la fornitura, o l'utilizzo delle informazioni contenute all'interno di questo documento.

LA STAZIONE APPALTANTE si riserva il diritto di modificare le informazioni contenute in questo documento e ogni requisito funzionale.

IBM, il logo IBM, sono marchi registrati di International Business Machines Corporation negli Stati Uniti e in altri paesi o in entrambi. Dell è un marchio registrato di Dell Inc. o delle sue consociate negli Stati Uniti e in altri paesi. VMware è un marchio registrato di VMware Inc. sussidiaria della EMC Corporation negli Stati Uniti e in altri paesi o in entrambi. Altri nomi di aziende, prodotti e servizi possono essere marchi registrati di altre aziende. Ogni affermazione riguardante i piani, le direzioni e le intenzioni della STAZIONE APPALTANTE sono suscettibili di cambiamento.

Indice

Glossario

Abbreviazione	Significato
AIPA	Autorità per l'informatica nella pubblica amministrazione
ATP	Advanced Threat Protection
BTS	Base Transceiver Station (Stazione radio base)
CAPWAP	Control And Provisioning of Wireless Access Points
CED	Centro Elaborazione Dati
CPE	Customer Premises Equipment
CSRF	Cross-site request forgery
DLP	Data Loss Prevention
DSS	Data Security Standard
EAP	Extensible Authentication Protocol
EAP-AKA	EAP-Authentication and Key Agreement
EAP-FAST	EAP-Flexible Authentication via Secure Tunneling
EAP-GTC	EAP-Generic Token Card
EAP-MSCHAP	EAP-Microsoft's Challenge Handshake Authentication Protocol
EAP-PEAP	EAP-Protected Extensible Authentication Protocol
EAP-SIM	EAP-Subscriber Identity Module
EAP-TLS	EAP-Transport Layer Security
EAP-TTLS	EAP-Tunneled Transport Layer Security
EMAIL	Electronic Mail (Posta Elettronica)
EN	Standard stabiliti da European Committee for Standardization
FW	Firewall
HA	High Avaliability
HW	Hardware
IEEE	Institute of Electrical and Electronics Engineers
IM	Instant Message
IP	Internet Protocol
IP66	Classe di Protezione
IPS	Intrusion prevention system
IPSEC	IP Security
ISO	International Organization for Standardization
LAN	Local Area Network
MESH	Nelle reti wireless indica un tipo di rete a maglia
NGFW	Next Generation Firewall
OFDM	Orthogonal Frequency-Division Multiplexing
OTP	One Time Password
PA	Pubblica Amministrazione
PBX	Private Branch eXchange
PC	Personal Computer
PCI	Payment Card Industry
PEC	Posta Elettronica Certificata

PSK	Pre Shared Key
PVC	Cloruro di polivinile
RADIUS	Remote Authentication Dial-In User Service
RDBMS	Relational Database Management System
RF	Radiofrequenza
RFC	Request for Comments
RSN	Robust Security Network
SAN	Storage Area Network
SL	Service Level
SLA	Service Level Agreement
SMS	Short Message Service
SQL	Structured Query Language
SSID	Service Set IDentifier
SSL	Secure Sockets Layer
SW	Software
TKIP	Temporal Key Integrity Protocol
UC	Unified Communications
UTM	Unified Threat Management
VOIP	Voice Over IP
VPN	Virtual Private Network
WAI	Web Accessibility Initiative
WAN	Wide Area Network
WCAG	Web Content Accessibility Guidelines
WEP	Wired Equivalent Privacy
WLAN	Wireless LAN
WPA	Wi-Fi Protected Access
WPA2	Wi-Fi Protected Access v2
WSDL	Web Services Description Language
WSS	Web Services Security
XML	eXtensible Markup Language

Preambolo

Questo documento è il capitolato tecnico che descrive i requisiti funzionali e tecnologici del progetto FONTENUOVA.NET SIMFO.

Il committente: La STAZIONE APPALTANTE

Il 15 ottobre 2001, a seguito di una raccolta firma e l'indizione di un referendum popolare, nasce per effetto della L.R. Lazio n. 25 del 5 ottobre 1999, il Comune di Fonte Nuova; una parte del territorio di Mentana (le frazioni di Santa Lucia e Tor Lupara) ed una piccola parte del territorio di Guidonia Montecelio vengono staccati donando un'identità sociale e territoriale ai propri abitanti.

Lo scenario sul quale si erge il Comune di Fonte Nuova è ricco di storia. Sorge sulle rovine dell'antica Nomentum già città della Lega Latina, rinomata per il suo clima e nominata da poeti classici come Ovidio; è stata spettatore dell'incontro tra Carlo, Re dei Franchi ed il Papa, nel 799 per porre le basi del Sacro Romano Impero; ha visto i movimenti di volontari garibaldini, truppe pontificie ed esercito francese nel 1867 per la campagna dell'Agro Romano pe la liberazione di Roma.

Per entrami le frazioni, i primi insediamenti urbani risalgono agli anni 50, quando una discreta immigrazione (soprattutto da Marche, Abruzzo, Umbria e Ciociaria) attratta dall'esiguo costo di terreni, dalla relativa vicinanza alla capitale e dal lavoro offerto dalla fabbrica di laterizi, ha fatto in modo che sorgessero delle abitazioni a S. Lucia lungo la via Palombarese e, soprattutto, in zona Borgo S.Lucia (l'attuale Via S. Lucia) teatro, nel periodo tra la fine del VI e l'inizio del V secolo a.C., di numerose battaglie tra Romani e Sabini ed a Tor Lupara sulla Nomentana, in località Tecla, poi con diramazioni estese fino all'espansione attuale ancora in corso.

Difatti, inizialmente, le uniche costruzioni presenti erano delle torri: Torre San Sebastiano Via della Torre, che diede nome al centro abitato e che poi, successivamente, cambiò la sua denominazione per via delle guardie a difesa della Torre che impugnavano delle lupare ed una torretta d'età moderna poi adibita a casale con osteria situata sulla Via Palombarese al bivio delle Molette, successivamente demolita.

Da allora sono sorte sempre più abitazioni, soprattutto negli anni 70 fino a ricoprire la superficie odierna pari a 20, 20 Km/quadrati.

1 . 1 Obiettivi della Gara Attuale

Per una descrizione generale e una comprensione complessiva e completa degli obiettivi della gara attuale si rimanda all'insieme del presente capitolato tecnico.

L'affermazione precedente è rilevante e accurata poiché questo capitolato tecnico descrive i requisiti funzionali dell'intera infrastruttura tecnologica di supporto a tutti i rilasci informatici di tutti gli interventi e tutte le azioni indicate di seguito sono parte integrante del progetto.

In dettaglio, il sistema specificato in questo documento, DEVE essere progettato in modo tale da consentire di ospitare al suo interno, senza degrado prestazionale, il sistema risultato dei sotto-progetti riguardanti:

- Portale di E-Gov
- Unified Communication
- Gestione Documentale e Dematerializzazione Atti Amministrativi
- Banca dati unificata
- Identity management
- Bus applicativo
- Datacenter comunale
- Hot-Spot pubblici e telecamere di videosorveglianza

Anch'essi oggetto del presente appalto.

1 . 2 Nota terminologica

All'interno di questo capitolato tecnico si adottano le raccomandazioni contenute nelle Linee guida tecniche per i programmi di creazione di sistemi e contenuti digitali e sono quindi prescritti gli standard e le raccomandazioni che DEVONO essere adottate, quelli che DOVREBBERO essere adottati e quelli che possono essere adottati per distinguere con chiarezza i requisiti, le raccomandazioni e i suggerimenti. Nella documentazione sugli standard, le parole "DEVE, DOVREBBE e PUÒ", riprese dalla terminologia usata nella documentazione della Internet Engineering Task Force (IETF), comunicano significati precisi sulla gradazione di requisiti, raccomandazioni, suggerimenti. Esse sono impiegate come parole chiave nel testo di questo documento:

DEVE (must): indica un requisito tecnico assoluto cui il progetto DEVE obbligatoriamente attenersi.

DOVREBBE (should): indica una direttiva che per valide ragioni non ha l'obbligatorietà del requisito, ma, prima di disattenderla, le sue implicazioni dovranno essere comprese appieno e il

caso andrà attentamente valutato. DOVREBBE si usa, ad esempio, in connessione con standard tecnici che probabilmente verranno largamente adottati nel corso del ciclo di vita del progetto, ma che sono ancora in via di diffusione.
PUÒ (may): indica un suggerimento. Il tema merita attenzione, ma i progetti non sono obbligati a seguire tale indicazione.
Il presente capitolato tecnico costituisce parte integrante del contratto finale di aggiudicazione. L'accettazione del contratto da parte del fornitore aggiudicatario (FA) implica da parte sua l'accettazione dei requisiti tecnici o la loro ridefinizione in accordo con LA STAZIONE APPALTANTE. Le funzionalità, non esplicitamente ridisegnate e concordate con LA STAZIONE APPALTANTE, s'intenderanno quindi disponibili e implicitamente accettate.

Introduzione

Partendo da un livello di informatizzazione focalizzato all'automazione dei settori e processi "chiave" (Demografici, Tributi, Ragioneria, Personale, Segreteria Generale), in questi ultimi anni sono stati avviati alcuni progetti di natura infrastrutturale, presupposto per la realizzazione di successive sperimentazioni. L'attenzione si è focalizzata sull'informatizzazione di processi orizzontali che maggiormente impattano sull'utenza finale e sui livelli di efficienza interna della macchina comunale. In particolare, uffici tecnici e l'urbanistica (sistema informativo territoriale), le attività produttive, i servizi scolastici, la gestione documentale, il marketing territoriale.
L'utilizzo della Piattaforma richiesta consentirà di ottimizzare, semplificare e unificare gli strumenti del Comune, fornendo ai dipendenti un alto livello di integrazione degli strumenti, oltre a una serie di servizi utili per il cittadino (richiesta Certificati, pagamenti Remoti, Servizio di teleassistenza, servizi turistici etc.)
Non secondario è poi l'elemento economico: questa nuova gestione delle comunicazioni permette delle economie di scala significative e una sensibile riduzione dei costi di gestione.
Sarà possibile racchiudere tutti i dati provenienti dalle varie amministrazioni del comune e raccoglierli in un'unica applicazione fruibile da qualsiasi postazione.
La piattaforma sarà collegata a una infrastruttura di rete Wireless che permetterà la sua consultazione anche attraverso Hot-spot Pubblici a cui il cittadino potrà collegarsi con terminali mobili per accedere e utilizzare i servizi del comune.

L'azione proposta ha come obiettivi:

- L'incremento dell'efficienza interna alla P.A. e l'erogazione di servizi ai cittadini e alle imprese, tramite un unico punto d'accesso al sistema amministrativo (sportello virtuale unico);

- L'integrazione tra i servizi di diverse Amministrazioni e quindi l'adozione di soluzioni di interoperabilità fra sistemi eterogenei;
- Garantire l'interoperabilità e la cooperazione applicativa tra i sistemi informativi delle Pubbliche Amministrazioni (PA), rendendo fruibili in tal modo servizi e informazioni come requisito di primaria importanza, al fine di realizzare il pieno ed efficace sviluppo dell'e-government mirato alla definizione di una strategia unica e comune nella gestione delle informazioni e servizi.

La necessità di avere un insieme d'informazioni condivise, valide ed effettivamente utili, connessa all'esigenza di promuovere l'erogazione di servizi di qualità per cittadini e imprese, ha portato a sviluppare una proposta progettuale di definizione di una piattaforma tecnologica che, attraverso il completamento e l'integrazione delle componenti di back office in uso presso l'ente, conducano alla realizzazione di una Piattaforma di Servizi di nuova generazione della P.A., inteso come canale unificato di accesso ai servizi on line da parte di cittadini e imprese, conforme con la legislatura vigente (Legge Stanca, Partecipazione Attiva Cittadino, Qualità del web, privacy, comunicazione pubblica) ed in grado di integrare servizi di cooperazione applicativa, servizi di identity management, servizi applicativi e basi informative già presenti all'interno della P.A.

Caratteristiche qualificanti dell'infrastruttura proposta

Nella proposta il Fornitore Aggiudicatario DEVE garantire:

- La presenza di un'infrastruttura tecnologica in grado di eseguire in tempo reale operazioni complesse e l'accesso trasparente ai servizi dei sotto-progetti garantendo al contempo un'adeguata infrastruttura di rete.
- Una comprovata esperienza nella gestione delle infrastrutture per il trattamento e la condivisione di risorse informatiche mediante l'impiego dei principali standard per la gestione.
- L'aderenza agli standard indicati.
- La conformità ai requisiti tecnici di accessibilità e usabilità indicati nel Decreto Ministeriale di attuazione della Legge Stanca (Legge 4/2004 "Disposizioni per favorire l'accesso dei soggetti disabili agli strumenti informatici") e alle linee guida WCAG 1.0 previste dallo standard internazionale WAI Web Accessibility Initative, un'iniziativa del consorzio mondiale W3C che si occupa di standardizzare la progettazione dei siti web.

Soluzione applicativa

1 . 3 Portale di E-Gov

Il componente software richiesto è un portale in grado di offrire informazioni e servizi ai cittadini e alle imprese da presentare in sostituzione del portale esistente. Le aree tematiche, oltre a quanto già presente nel portale attuale, sono l'amministrazione comunale ed i servizi informativi ed interattivi organizzati secondo la metafora degli eventi della vita (studiare, essere cittadino, ecc..), i trasporti, le utilities, la salute, ecc.
Pur nel rispetto delle singole identità istituzionali il portale DEVE essere il più possibile integrato fra le sue componenti e DEVE per questo non solo offrire informazioni univoche e omogenee, ma anche evitare inutili operazioni ripetitive agli utenti e favorire lo scambio di informazioni tra le diverse amministrazioni a partire dall'inserimento delle credenziali di accesso che dovranno essere gestite da una componente di Identity Management, un unico sistema di Utente e Password da assegnare ai cittadini e ai dipendenti del Comune per l'accesso a quelle particolari funzioni del portale che richiedono una identificazione "certa" dell'interlocutore e che permetta in futuro l'uso della Carta di Identità Elettronica e/o di Carte Servizi.

Il Portale DEVE costituire:

- Un Sito istituzionale quale unico punto di accesso personalizzabile per tutti gli utenti;
- Un'infrastruttura operazionale consistente;
- Un'interfaccia utente amichevole e strutturata in modo da agevolare l'accesso, la navigazione ed il recupero delle informazioni;
- Un meccanismo di controllo degli accessi verso tutti i servizi applicativi;
- Offrire modalità di accesso multi-canale (PC e SmartPhone);
- Essere multilingua. La Comunità Europea indica tra le caratteristiche auspicabili della cittadinanza Europea la conoscenza e l'utilizzo per tutti i cittadini di almeno tre lingue della comunità; di conseguenza il sistema DEVE essere fruibile in almeno tre lingue, inizialmente almeno italiano e inglese. E' auspicabile l'aggiunta immediata di francese e/o spagnolo. Il numero delle lingue supportate DEVE essere comunque aperto;
- DEVE essere aderente alle Linee guida dell'Agenzia per l'Italia Digitale.

Il Portale DEVE essere strutturato in:

- Una parte "pubblica": dedicata ai servizi informativi ad accesso libero nei quali saranno reperibili informazioni generali, notizie e documenti non riservati;

- Una parte "riservata": destinata a garantire l'interoperabilità tra gli utenti dell'amministrazione ed utenti abilitati che cooperano nello svolgimento delle loro attività, con accesso alle piattaforma documentale e di Unified Communication;
- Una parte di "gestione": destinata agli amministratori del sistema che vi potranno accedere per le attività di gestione degli utenti, pubblicazione e riorganizzazione dei dati ecc.

Il portale nel suo insieme renderà disponibili diverse tipologie di funzioni integrandole anche con le informazioni provenienti dai portali attualmente in esercizio:

- Informazioni inerenti il rapporto tra cittadini e imprese da un lato e amministrazioni e imprese di utilities dall'altro; le informazioni si riferiranno in genere al "come fare che cosa" e, seguendo le indicazioni del Governo e del Dipartimento della Funzione Pubblica, saranno raggruppate e logicamente organizzate secondo gli eventi della vita;
- Informazioni relative alla città e, più in generale, al territorio di riferimento e riguarderanno diversi aspetti quali:
    - Gli eventi (di qualunque natura siano e quindi business, istituzioni, cultura, spettacolo, ecc.),
    - Le strutture ricettive (ospitalità e ristorazione),
    - I servizi (banche, poste, farmacie, ecc.),
    - La parte architettonica e culturale delle città.

Il portale, integrando il componente software di Unified Communication, si pone anche l'obiettivo di favorire l'avvicinamento alla politica e all'operato delle amministrazioni, di interagire con esse di essere ascoltati; I cittadini e le imprese potranno dialogare a distanza con i diversi enti coinvolti attraverso l'uso di servizi interattivi, risparmiando tempo e migliorando l'efficienza delle amministrazioni. Il portale permetterà a cittadini e imprese di usufruire di servizi interattivi di varia natura consentendo loro di eseguire da casa o dal proprio posto di lavoro le stesse "pratiche" che di norma comportano una presenza fisica presso le amministrazioni.

Usabilità

Nella realizzazione della piattaforma particolare attenzione DEVE essere posta agli aspetti di usabilità delle applicazioni che compongono la soluzione. Tale obiettivo, particolarmente rilevante per una piattaforma a cui accede una tipologia piuttosto variegata di utenti, viene colto curando in modo particolare il progetto dell'interfaccia utente del Portale, il quale è il principale punto di accoglienza delle richieste dell'utilizzatore. Particolare cura, poi, DEVE essere posta

nell'organizzazione dei contenuti in modo da garantire un accesso immediato ed intuitivo alle informazioni di interesse.

- La progettazione e configurazione del Portale DEVE tener conto dei seguenti criteri:
- L'utilità attesa - individuazione delle informazioni e dei servizi più congrui alle aspettative degli utenti;
- La comprensibilità dell'informazione - i contenuti informativi DEVONO essere redatti in un linguaggio semplice e lineare;
- L'efficacia comunicativa - le informazioni e i servizi vengono personalizzati per il singolo utente;
- La navigabilità - la configurazione dinamica (strutturazione delle informazione e accesso ai servizi) coerente con il profilo dell'utente;
- L'attrattiva grafica - occorre raggiungere il giusto bilanciamento tra la piacevolezza visiva, la velocità di caricamento e la garanzia funzionale degli elementi grafici.

L'elemento estetico, il più possibile armonico con il Sito istituzionale, è oltremodo fondamentale giacché contribuirà ad accogliere emotivamente l'utente in un ambiente che spesso presuppone alcuni comportamenti standard quali l'attenzione e la comprensione di ciò che sta accadendo.

Le applicazioni dovranno essere realizzate in modo da garantire massima ergonomia lavorativa e semplicità di utilizzo grazie all'adozione di paradigmi di interazione auto esplicativi e di una sezione di aiuto contestuale.
Il portale DEVE avere una struttura modulare, ben articolata, chiara per le diverse tipologie d'utenti del sistema.

La totale integrazione degli strumenti di sviluppo e gestione richiesta per la realizzazione del portale permetterà all'Amministratore del Portale di sfruttare il profilo definito del singolo utente e la sua appartenenza a gruppi predefiniti: questo permetterà al Portale di riconoscere l'utente senza richiedere ulteriori autenticazioni e di associargli le opportune policy di sicurezza per l'accesso ad aree applicative, contenuti e funzionalità.

1 . 4 Unified Communication

Il componente software richiesto è una Rete Intelligente Multicanale di comunicazione che consenta di agevolare il processo di trasparenza dell'Ente supportando la veicolazione delle informazioni ai cittadini mediante tecniche di "tracciamento informativo" delle procedure in corso. Un sistema in grado di offrire ai cittadini la possibilità di rimanere sempre in contatto con

gli Uffici Comunali con sistemi di comunicazione diretta quali: ISTANT MESSAGE, VOIP, EMAIL, CALENDAR, FILE SHARING, VIDEO SHARING.

La Rete Intelligente di Unified Communication (UC) DEVE fornire i seguenti servizi:

Invio di messaggi tramite diversi canali di comunicazione

Il servizio di invio dei messaggi DEVE essere in grado di effettuare chiamate telefoniche a utenti fissi e mobili, trasmettendo messaggi audio preventivamente registrati. DEVE altresì inviare SMS, e-mail, fax. Inoltre DEVE essere in grado di inviare messaggi a PC connessi ad internet su cui sia stato preventivamente installato il client applicativo.

Collegamento con il Gestore Documentale

La piattaforma UC, direttamente collegata in cooperazione applicativa con i work-flow relativi ai procedimenti, DEVE ricevere degli "eventi" (ovvero passaggi nodali dell'iter) dovrà essere in grado di ospitare in aree riservate i documenti richiesti dagli utenti.

Interfaccia verso gli operatori

La UC DEVE fornire uno strumento veloce e facile da usare, che permetta:

- Funzioni IM Istant Message con protocollo di Presenza
- Gestione di Attività e TASK
- Gestione Video
- Gestione Immagini
- Calendario personale e condiviso
- File Sharing
- Connessione con sistemi Social (gestibili all'interno del sistema UC)
- Sistema VOIP PBX
- Gestione Fax, sms gateway
- Email con multidominio
- Video Conferenza
- Audio Conferenza con re-direzione su PBX o numeri geografici

Interfaccia verso i cittadini e le imprese

La UC DEVE mettere a disposizione dei cittadini e delle imprese una semplice interfaccia web, un'APP Mobile, un'applicazione e un'applicazione fruibile da web browser, a cui si DEVE poter accedere mediante il Portale di e-gov nel caso WEB, tramite la quale, una volta effettuato l'accesso, potranno selezionare i tipi di informazione che intendono ricevere, dialogare con le

istituzioni attraverso i canali di comunicazione e comunque interagire con il Comune nell'ambito dei servizi messi a disposizione. Tutti i dati inseriti dal cittadino dovranno poter essere aggiornati in ogni momento dal cittadino stesso.

Interfaccia terminali di Alert

La piattaforma DEVE essere in grado attivare "Protocolli di Presenza", per gestire l'ingresso nella piattaforma degli utenti loggati.

Conferma della ricezione del messaggio

Nel caso di messaggi inviati ad Enti ed addetti ai lavori, la UC DEVE prevedere la possibilità di ricevere una conferma dal soggetto informato, tramite una accettazione.

Caratteristiche delle linee telefoniche

La UC DEVE essere in grado di effettuare chiamate vocali attraverso l'uso di linee analogiche tradizionali. DEVE, attraverso un singolo server avere la possibilità di interfacciare sistemi PBX.

Modalità invio SMS

La Piattaforma UC DEVE prevedere la possibilità di utilizzare un sistema di "sms gateway" connesso direttamente alla rete per l'invio di SMS in modo autonomo. NON DEVE quindi affidare a Provider di servizi esterni all'Ente l'invio dei messaggi SMS.

Integrazione con sistemi di Digital Signage

La UC DEVE essere predisposta per la eventuale integrazione con terminali dotati di schermi per la diffusione di messaggi video, configurati con opportuni palinsesti e dotati di canali informativi testuali visualizzati in sovraimpressione. Il sistema DEVE essere predisposto per la creazione di un WEBTV con Palinsesto.

Connessione con sistemi SOCIAL

La UC DEVE essere predisposta per la ricezione di informazioni provenienti dai principali canali Social. La gestione del Canale Social DEVE essere possibile all'interno della piattaforma UC.

Interfaccia di Configurazione e multilingua

La UC DEVE essere dotata di apposita interfaccia di configurazione tale da permettere ad un Amministratore del sistema locale di definire la configurazione richiesta e di poter gestire eventuali modifiche in fase di esecuzione del servizio. Viene richiesto un pacchetto esteso di lingue e l'interfaccia DEVE cambiare automaticamente al cambio del settaggio della Lingua. Il pacchetto di lingue DEVE contenere anche l'Italiano e l'Inglese.

Gestione Allarmi

Il servizio di gestione degli allarmi DEVE collezionare tutti gli eventi generati dalla piattaforma. In base alla politica definita nella configurazione dall'Amministratore, si potranno creare allarmi definiti da criteri applicati agli eventi ricevuti secondo una logica di "causa ed effetto".
Gli allarmi dovranno quindi poter essere gestiti tramite meccanismi automatici ovvero tramite l'intervento manuale di un operatore autorizzato.

Gestione Accessi

Il servizio di accesso DEVE essere integrato con la piattaforma di Identity Management. NON DEVE in alcun caso essere necessario inserire le credenziali più di una volta.

1.5 Gestione Documentale e Dematerializzazione Atti Amministrativi

Gestione Documentale

Il componente software richiesto è una piattaforma applicativa per la gestione di Flussi Documentali. I servizi minimi richiesti sono:

- Gestione documentale;
- Work flow di processo;
- Fascicolazione e Ricerca;
- Protocollo Informatico in ingresso e uscita.

Il sistema DEVE consentire l'organizzazione dei documenti in cataloghi, e offrire meccanismi automatici per la gestione documentale e dei procedimenti. Deve offrire una funzionalità di revisione dei documenti, blocco e sblocco di documenti e fascicoli, inserimento e modifica di note e commenti.
Il sistema DEVE favorire le attività di collaborazione tra gli operatori, ad esempio offrendo work flow documentali del tipo Ratifica/Approva, eventualmente anche personalizzabili.
In merito all'interfacciamento con i flussi esistenti, il sistema DEVE dialogare automaticamente con i server di posta normale, PEC e server Fax dello Unified Communication e DEVE disporre di strumenti automatici per il controllo delle firme digitali apposte sui documenti e per l'individuazione di variazioni non controllate sui documenti archiviati.

Le macro funzionalità richieste al minimo sono:

- Gestione dei contenuti di diverso tipo per la catalogazione, organizzazione, condivisione di contenuti;

- Gestione della ricerca, sia essa semplice, avanzata e full-text;
- Gestione dei metadati personalizzabili dall'utente;
- Gestione delle politiche di accesso e di utilizzo dei documenti;
- Gestione dei cicli di lavoro in grado di controllare la revisione e l'approvazione dei contenuti.

Cooperazione applicativa

1 . 6 Banca dati unificata

La necessità di gestire il territorio con sistemi sempre più efficienti è ormai un dato acquisito all'interno della Pubblica Amministrazione.
La complessità e l'articolazione delle problematiche territoriali richiedono che tutte le informazioni siano messe dinamicamente in relazione tra loro.
Una base di dati integrata, unitaria e unica di dati, a partire ove possibile dall'integrazione delle basi di dati esistenti, è lo strumento informatico ritenuto in grado di gestire queste relazioni.
A tale scopo si richiede la realizzazione di una base dati (denominata DBFonte) basata su soluzioni RDBMS open source, con funzione di archivio centrale per tutte le componenti software dell'offerta. La soluzione DEVE poter essere integrata da ulteriori soluzioni software interne ed esterne alla Amministrazione. Si richiede al fornitore anche la creazione del catalogo dei metadati tramite standard opportuno e la creazione di procedure di pubblicazione e controllo dei metadati assicurando i livelli di scoperta, utilizzazione e condivisione.
Il prodotto offerto DEVE essere corredato di licenze d'uso o di attestato di usabilità in caso di soluzioni di tipo open source.

1 . 7 Identity management

Con Identity Management si intende una soluzione applicativa per la completa gestione delle identità digitali di una persona fisica, dal processo di creazione e organizzazione, fino all'eliminazione dell'identità digitale.
Ogni singola persona, dipendente o utente esterno di un servizio, sarà oggetto di un processo di assegnazione di molte identità digitali che possono riguardare l'account di posta o l'accesso ai portali, in maniera coerente con il suo specifico ruolo. Ogni applicazione DEVE adottare l'identity management per l'autenticazione. Nell'Identity Management ciascuna di queste identità digitali va attivata (Provisioning) e disattivata (deProvisioning) in maniera coerente alle politiche amministrative e in modo automatico per evitare errori o ritardi. Ad esempio nel caso di pensionamento di un dipendente comunale l'intero processo di disattivazione dei suoi account DEVE essere eseguito nel modo più rapido ed efficace possibile. Viene inoltre richiesta la possibilità di effettuare auditing e monitoraggio sulle attività di ogni identità digitale,

consentendo una maggior aderenza alle politiche di sicurezza e, quando necessario, un più facile percorso di certificazione.
La soluzione di Identity Management dovrà integrarsi ai sistemi di sicurezza, gestione e monitoraggio dell'infrastruttura wireless e di sicurezza di rete. Inoltre dovrà poter gestire nativamente sistemi di strong autentication basati su Token OTP senza l'ausilio di software terze parti.

1.8 Bus applicativo

La validità di un'architettura è conseguenza degli elementi e degli standard su cui si fonda. In particolare nello sviluppo del Progetto dovranno essere considerati i seguenti aspetti:

- Utilizzo di Standard aperti: per poter operare in ambienti multipiattaforma è necessario, o quantomeno consigliabile, utilizzare esclusivamente standard aperti quali XML, WSDL e WS-Security (WSS).
- Modularità: bisogna trovare il giusto equilibrio tra i servizi erogati da ogni singolo componente, creando un insieme bilanciato di piccoli servizi riutilizzabili per le funzioni comuni e servizi più grandi per processi specifici.
- Utilizzo di contratti di servizio: WSDL (Web Services Description Language) è la specifica standard per la creazione di contratti di Web Services, un contratto definito avrà come conseguenza servizi più flessibili.
- Adozione di un Enterprise Service Bus: La dorsale di pubblicazione dei servizi ed abilitazione delle applicazioni per accedervi. Inoltre include caratteristiche quali adattatori per i sistemi proprietari, capacità di orchestrazione dei servizi, autorizzazione e autenticazione lato sicurezza, trasformazione dei dati, supporto per regole di business e capacità di monitorare i livelli di servizio.

Nell'ambito di un'architettura orientata ai servizi DEVE quindi essere possibile modificare, in maniera relativamente semplice, le modalità di interazione tra i servizi, oppure la combinazione nella quale i servizi vengono utilizzati nel processo, così come DEVE risultare più agevole aggiungere nuovi servizi e modificare i processi per rispondere alle specifiche esigenze di business: il processo NON DEVE più essere vincolato da una specifica piattaforma o da un'applicazione, come attualmente accade con le applicazioni in uso, ma DEVE essere considerato come un componente di un processo più ampio e quindi riutilizzato o modificato.

Infrastruttura

1.9 Datacenter comunale

Nel corso degli ultimi tre anni si è proceduto a virtualizzare tutti i server presenti nel CED di Via Ariosto con la sola eccezione del Centralino. L'infrastruttura virtuale in esercizio (Hypervisor) è VMware ESXi 4.1.0. I server sono ospitati su una SAN Dell PowerVault MD3200i la cui capacità attuale di 2.6TB è totalmente utilizzata. Le macchine Host sono 3: un Dell PowerEdge R510 e due IBM x3650. Su questi host girano un totale di dieci server.
Viene richiesto di valutare la configurazione attuale e proporre un progetto di aggiornamento tecnologico che tenga conto dell'eventuale riuso delle componenti attualmente utilizzate unitamente alle nuove componenti hardware e software del nuovo sistema. Si fa presente che è volontà della scrivente continuare ad adottare soluzioni di virtualizzazione in continuità con quanto già fatto. Tutti i prodotti hardware dovranno poter essere ospitati in armadi Rack da 19". I server offerti dovranno presentare opportune soluzioni di ridondanza. Si richiede inoltre di valutare l'aggiornamento e l'espansione della SAN in produzione o in alternativa l'aggiunta e/o la sostituzione con una nuova SAN più performante. Per quanto riguarda la rete dati, l'infrastruttura di sicurezza e la rete wireless cittadina si chiede di integrare (pena esclusione) con elementi conformi alle caratteristiche minime di seguito indicate:

1.10 Sicurezza applicativa del portale

Tutte le applicazioni web che saranno soggette ad accessi pubblici e/o attraverso rete internet dovranno essere protette da una soluzione Aplliance based di firewall applicativo.

Detto appliance dovrà avere i seguenti requisiti minimi:

- Monitoraggio allargato e protezione specifica per smarrimento carte di credito ed esame delle informazioni sulle applicazioni attraverso un severo controllo del traffico in uscita. Consente ai nostri clienti di creare la propria firma particolare ed i tracciati DLP, insieme con regole predefinite per ogni tipo di evento.
- Capacità di monitoraggio sulle applicazioni protette contro qualsiasi incidente ed abilità a riconfigurare la versione originale in modo automatico e veloce.
- Deve essere in grado di bloccare ogni attacco al protocollo http mantenendo rigorosi standard RFC per prevenire attacchi quali ad esempio encoding, saturazione tamponi ed altri attacchi specifici verso le applicazioni.

- Scansione ed analisi automatiche delle applicazioni web protette, individuando eventuali punti deboli nel sistema di sicurezza e vulnerabilità potenziali conosciute o ignote per rendere complete le soluzioni a livello PCI DSS.
- Deve fornire un firewall XML con validazione dello schema, IPS e capacità di routing.
- Sistema di Protezione esterna dagli attacchi più complessi quali iniezioni SQL, script incrociato, CSRF. Oltre a possedere un sistema di auto apprendimento e varie capacità avanzate, il firewall applicativo DEVE essere in grado di creare criteri di protezione fino al livello dei singoli elementi applicativi.

La protezione delle applicazioni web DEVE prevedere al minino, la prevenzione dei seguenti tipi di attacco:

- Cross Site Scripting
- SQL Injection
- Session Hijacking
- Cookie Tampering / Poisoning
- Cross Site Request Forgery
- Command injection
- Remote File Inclusion
- Forms Tampering
- Hidden Field Manipulation
- Outbound Data Leakage
- HTTP Request Smuggling
- Remote File Inclusion
- Encoding Attacks
- Broken Access Control
- Forceful Browsing
- Directory Traversal
- Site Reconnaissance
- Search Engine Hacking
- Brute Force Login
- Access Rate Control
- Schema Poisoning
- XML Parameter Tampering
- XML Intrusion Prevention
- WSDL Scanning
- Recursive Payload
- External Entity Attack
- Buffer Overflows
- Denial of Service

Caratteristiche HW:

Il sistema dovrà comporsi di due apparati fisici installati in HA. Il trhoughput minimo gestito DEVE essere pari a 500 Mbps. Ogni apparato dovrà essere dotato di minimo 4 interfacce RJ45 10/100/1000, 2 porte USB e minimo 1 TB di storage. Il sistema dovrà garantire una capacità di analisi di minimo 22000 transazioni HTTP per secondo introducendo latenze inferiori al ms.

1.11 Firewall Perimetrale, Controller Wi-Fi, Switch di rete, Sistema di monitoraggio e management, Hot-Spot pubblici e telecamere di videosorveglianza.

Specifiche per la realizzazione di una rete wireless conforme agli standard Wi-Fi per la copertura di alcune aree del comune con particolare interesse alle zone elencate di seguito:

- Via Cuoco Scuola materna ed elementare
- Via Brennero Scuola elementare e media
- Zona

Elenco impianti di Videosorveglianza:

- Via Nomentana/Via I Maggio (centro anziani)
- Via Cuoco (Scuola)
- Via IV Novembre (Piazza Pascoli) di fronte scuola materna comunale
- Via Due Giugno / Via IV Novembre
- Via Due Giugno (Chiesa Bruciata)
- Via Valle dei Corsi/Via Due Giugno (Nomentana Hospital)
- Via Brennero (Scuola)
- Via Monte Circeo/Via Nomentana (rotatoria)
- Via Nomentana – Via Salvatoretto – Via S. Lucia
- Via Selva dei Cavalieri (Impianto Sportivo)

La copertura Wi-Fi DEVE prevedere collegamenti Full Mesh dal comune verso le aree interessate con tecnologie su frequenza di Banda non soggetta a licenza. Le soluzioni di rete Wireless nelle bande non licenziate a 5GHz e 2.4GHz dovranno essere basate su tecnologie Wi-Fi. L'intera rete DEVE essere estesa / terminata attraverso Hotspot Wi-Fi nei punti di interesse sopracitati.

L'offerta tecnica proposta pertanto DEVE, a pena di esclusione, prevedere una soluzione che rispetti tali caratteristiche minime, sia in termini di fornitura sia di servizio.

Caratteristiche richieste per il Sistema WIFI HOTSPOT

La gara prevede la fornitura e l'installazione di un sistema wireless composto, come minimo, dalle seguenti tipologie di prodotti:

1.11.1.1 Scopo

Scopo del presente documento è quello di fornire le specifiche per la realizzazione della copertura Wi-Fi del Comune di Fonte Nuova.
Contestualmente si forniranno le specifiche per la realizzazione dell'infrastruttura di sicurezza a protezione del CED del Comune. In previsione della fornitura del servizio Wi-Fi a cittadini e turisti, si rende infatti necessario un adeguamento dell'infrastruttura di sicurezza del CED.
La rete Wi-Fi sarà messa a disposizione dei Cittadini con l'intento di fornire connettività Internet e connettività sul CED locale, nel quale saranno ospitate applicazioni per la fruizione dei contenuti.
La rete Wi-Fi dovrà fornire anche connettività al personale dipendente, alle forze dell'ordine, e ad eventuali devices, presenti e futuri, che necessitino di connettività IP in zone non coperte dalla rete cablata.

1.11.1.2 Descrizione Generale

La soluzione proposta dovrà prevedere la distribuzione di una serie di reti Wireless ad uso e consumo dei Cittadini e degli operatori del Comune di Fonte Nuova.
Dovrà essere possibile creare ulteriori reti Wireless che forniscano servizi infrastrutturali per la distribuzione di connettività a devices di vario utilizzo, presente e futuro, che necessitino di connettività in zone non coperte dalla rete cablata. (Es. Ampliamento copertura Telecamere Wireless, Totem Informativi, etc.)

L'infrastruttura dovrà fornire contestualmente servizi ai cittadini, al personale operante presso la struttura, alle forze dell'ordine e al CED locale.
Vista l'eterogeneità dell'utenza alla quale verrà fornita connettività, e ai diversi livelli di sicurezza che dovranno essere applicati per ciascuna tipologia di accesso, è indispensabile individuare una soluzione che integri funzionalità di sicurezza e Threat Management delle reti Wireless e Wired, gestibile da un singolo punto e che offra quindi un accurato controllo su tutte le direttrici di traffico.
Su entrambe le reti (Wireless e CED) dovranno essere forniti i medesimi servizi e le medesime protezioni dalle minacce informatiche, con l'intento di proteggere l'infrastruttura a partire dal punto più vicino al device che vi si connette.

La soluzione quindi avrà il compito di proteggere specificamente le reti Wireless dagli attacchi ai quali sono intrinsecamente vulnerabili e di applicare alle stesse un livello di protezione dalle minacce normalmente applicate alle reti Wired (Anti-Virus, Anti-Botnet, AntiDDos, IPS, etc.).

Le reti wireless dovranno essere trattate dal sistema come una qualsiasi interfaccia di accesso alla rete, quindi senza limitazioni rispetto alle contromisure applicabili su una rete tradizionale. Le stesse politiche e gli stessi livelli di sicurezza dovranno essere implementabili in un unico punto e disponibili sulle diverse reti realizzate, siano esse di tipo tradizionale o Wireless.

Questo approccio si rende necessario per fornire un elevato livello di sicurezza e tracciamento dei client, e per semplificare la gestione dell'infrastruttura.

Si ritiene infatti che la possibilità di avere un unico punto di amministrazione e controllo dal quale è possibile gestire completamente le componenti di sicurezza Wireless e Wired porti ad una copertura totale degli aspetti di sicurezza e ad una semplicità di gestione indispensabile per un bacino di utenza così elevato.

Data la natura centralizzata della soluzione, dovrà essere possibile monitorare, individuare ed eliminare qualsiasi tipo di minaccia, indipendentemente dalla rete, dal device o dall'utente dalla quale proviene.

Si rende indispensabile quindi una piattaforma comune di provisioning, logging e reporting unificata tra reti Wireless e Wired, che permetta di monitorare e tracciare le attività e le interazioni tra il CED, la rete Internet e le reti Wireless distribuite sul sito.

1.11.1.3 Wireless Controller e AccessPoint

La soluzione Wireless proposta dovrà essere composta da un Wireless Controller e da Thin AccessPoints.

Tutti gli Access Point dovranno essere gestiti centralmente dal Controller, che avrà il compito di configurare, gestire e monitorare tutte le funzionalità della rete Wireless.

La gestione degli Access Point dovrà essere realizzata tramite protocollo CAPWAP.

Le modalità di forwarding del traffico supportate dovranno essere 2, Tunnel-Mode e Bridge-Mode. Ogni Access Point dovrà poter gestire al minimo 14 (quattordici) SsiD contemporaneamente.

In fase di configurazione dovrà essere possibile specificare, per ciascuna delle reti Wireless (SsiD) distribuite, la modalità di funzionamento (bridge o tunnel).

In entrambe le modalità di funzionamento l'alta affidabilità della piattaforma dovrà essere garantita da funzionamento in HA del Wireless Controller.

Dal Wireless Controller dovranno essere configurate tutte le politiche di sicurezza applicabili all'utenza (IPS/Application Control, Antivirus, Web Content Filtering)

1.11.1.4 WLAN Security

La soluzione proposta dovrà avere come scopo principale quello di fornire un elevato livello di sicurezza e di protezione dalle minacce sulla rete Wireless.
Dovranno essere forniti meccanismi di protezione per attacchi e minacce specifiche delle reti senza fili.
La componente di sicurezza della soluzione avrà il compito di monitorare costantemente i segnali radio presenti sulla rete, rilevare le minacce e porre dei rimedi, ponendo come obbiettivo principale quello di preservare il traffico degli utenti leciti ed impedire un uso fraudolento dell'infrastruttura da parte di utenti malevoli.
La soluzione dovrà inoltre prevedere protocolli e funzionalità di Inspection del traffico fino al Layer7, identificando specifiche applicazioni al fine di applicare delle azioni specifiche (traffic-shaping/drop).

Di seguito una descrizione delle funzionalità di sicurezza richieste, specifiche per le reti Wireless.

1.11.1.4.1 Wireless Intrusion Detection

Dovrà essere costantemente verificata la compliance dei protocolli Wi-Fi e gli eventuali attacchi e vulnerabilità ai quali questo tipo di reti risultano intrinsecamente vulnerabili.
Per sfruttare molte di queste vulnerabilità non è necessario essere connessi alla rete Wireless. E' quindi possibile per un utente malevolo provocare blocchi o malfunzionamenti della rete Wireless pur non avendo credenziali di accesso valide alla rete stessa.
La soluzione dovrà essere in grado quindi di monitorare costantemente tutte queste minacce e di individuare la sorgente malevola, permettendo quindi di applicare le dovute contromisure.

Le principali minacce da monitorare sono:

- Weak WEP Encryption Usage
- Null SSID Probes
- Deauth Broadcasts
- Various Management, EAP, Auth & Beacon floods

Il monitoraggio e la gestione di questi eventi avrà il compito di mettere in sicurezza la rete da possibili tentativi di manomissione dell'infrastruttura Radio da parte di utenti malintenzionati.

1.11.1.4.2 Rogue AP

I rogue access point costituiscono una delle principali falle di sicurezza su reti Wireless. Chiunque con accesso ad uno spazio coperto da rete Wi-Fi può, per ignoranza o maliziosamente, installare

un access point o un router wireless che può potenzialmente dare accesso ad una rete sicura ad utenti non autorizzati.

La soluzione dovrà prevedere dei meccanismi di verifica/controllo delle reti Rouge. Dovrà quindi essere in grado di monitorare lo spettro elettromagnetico alla ricerca di intrusi non autorizzati. Il sistema dovrà rilevare inoltre connessioni in bridge tra i RougeAP e la rete interna. Una volta individuati i segnali dovrà essere possibile localizzarli tramite triangolazione tra i vari AP e sopprimerli.

1.11.1.4.3 Automatic Radio Resource Provisioning

I segnali Wireless trasmessi dai vari AccessPoint dovranno essere costantemente monitorati, in automatico, e adattati automaticamente in termini di potenza di trasmissione, per offrire una copertura adeguata e con la minore interferenza possibile. La soluzione dovrà inoltre prevedere meccanismi di band-auto-provisioning con lo scopo di evitare l'overlapping dei canali in trasmissione e per diminuire la possibilità di interferenze tra i vari AP gestiti.

Sono inoltre richieste le funzionalità di AP-Handoff e Frequency-Handoff, in grado di dirottare i client con poco segnale o connessi su AccessPoint carichi di utenza, su un altro Access-Point o su una banda diversa dello stesso AccessPoint, incrementando così la disponibilità della rete percepita dall'utente.

1.11.1.4.4 Bandwidth Management

Il problema principale delle performance di una rete Wireless è lo sharing della banda disponibile tra tutti i client connessi al medesimo Access-Point.

La soluzione dovrà fornire un interfaccia per la corretta gestione della banda a disposizione degli utenti. In scenari ad alta densità di utenza, è indispensabile avere il controllo delle applicazioni utilizzate per poter definire le opportune politiche di priorizzazione delle applicazioni definite indispensabili e il rate-limiting/blocking delle applicazioni non necessarie o non permesse.

È richiesta quindi l'inspection a livello 7 del traffico passante sugli AP, per fornire un controllo granulare e preciso delle attività degli utenti connessi.

Dovrà essere possibile definire per ciascun utente e per ciascuna applicazione che lo stesso utente utilizza diversi livelli di priority e rate-limiting.

Contestualmente dovrà essere possibile bloccare tutto il traffico proveniente/diretto verso reti/applicazioni dichiarate insicure, come per esempio BotNet.

1.11.1.4.5 Wireless Devices monitoring

In ogni momento DEVE essere possibile monitorare lo stato degli AccessPoint, il numero di Client connessi, le credenziali (device, username) la loro localizzazione e la quantità di banda utilizzata per ciascun utente. Tutte le attività degli utenti dovranno essere opportunamente tracciate.

1.11.1.5 Unified Threat Management

E' richiesta la totale integrazione dei meccanismi di Unified Threat Management sulle reti Wireless.

Tutti i meccanismi di protezione delle minacce normalmente applicate su reti Wired dovranno essere disponibili sulle Reti Radio, senza limitazioni, mantenendo un unico punto di gestione e controllo. Un unico apparato quindi dovrà essere in grado di gestire tutta la componente Radio, agendo come Wireless Controller e come UTM Gateway per i servizi dedicati all'utenza Wi-Fi e al CED.

Oltre alle protezioni specifiche delle reti Radio, descritte nel capitolo 7.3.1.4, è richiesta la possibilità di applicare a tutti i client connessi alla rete Wireless, le seguenti politiche di sicurezza:

1.11.1.5.1 Antivirus

Funzionalità di Antivirus Gateway, disponibile nelle modalità Proxy e Flow. Il motore antivirus dovrà permettere l'ispezione del traffico su base signature e su base euristica, permettendo l'identificazione delle minacce più avanzate (Advanced persistent threath), l'identificazione di BotNet e la possibilità di analizzare i file sospetti attraverso una sandbox.

1.11.1.5.2 Web Content Filtering

E' richiesto un servizio di web content Filtering dinamico è basato sulla categorizzazione dei siti. Tale categorizzazione DEVE essere costantemente aggiornata e manutenuta dal fornitore dei servizi. Deve essere inoltre possibile il blocco di Java Applet, ActiveX, Cookie.

1.11.1.5.3 Application Control

La funzionalità DEVE permettere l'individuazione, la registrazione nei log e l'esecuzione di azioni nei confronti di traffico di rete, sulla base del riconoscimento diretto delle singole applicazioni utilizzate dall'utenza. Come azioni oltre al blocco, al reset e al monitoring dovrà essere possibile effettuare Traffic Shaping per singola applicazione. Il pacchetto di Signature DEVE essere costantemente aggiornato e manutenuto dal fornitore dei servizi.

1.11.1.5.4 Intrusion Prevention

E' richiesta la funzionalità di Intrusion Prevention. Dovrà essere resa disponibile la possibilità di effettuare l'inspection del traffico di rete e identificare tipologie di attacco su base signature e su base anomay detection. Il pacchetto di Signature DEVE essere costantemente aggiornato e manutenuto dal fornitore dei servizi.

Tutti i controlli citati in questo capitolo dovranno essere disponibili per una o per tutte le reti Wireless configurate, contestualmente a tutte le reti di servizio realizzate per la connettività del CED.

1.11.1.6 Firewalling

La soluzione proposta dovrà essere utilizzata, oltre che per la distribuzione e la gestione delle reti wireless, anche per la messa in sicurezza del CED presente presso il sito.
Il FW dovrà essere interconnesso all'infrastruttura CED con link multipli di velocità 1 Gb/s e/o con link 10Gb/s.

Le funzionalità richieste sono:

- *Firewall*
- *VPN IPSEC e SSL*
- *Traffic Shaping*
- *Dos Policy*
- *Proxy e Web Caching*
- *Ipv6*
- *Wan Optimization*
- *HA*
- *SSL Inspection*
- *Server Load balancing*
- *DLP*

Sono richieste inoltre tutte le funzionalità di NGFW e ATP descritte nel capitolo 7.3.1.5.

1.11.1.7 Meccanismi di Autenticazione Wireless

La soluzione dovrà supportare i seguenti meccanismi di autenticazione su rete Wireless:

- Open
- Captive Portal

- WPA/WPA2 PSK
- WPA/WPA2 Enterprise
- EAP-PEAP
- EAP-TLS
- EAP-TTLS/MSCHAPv2
- EAPv0/EAP-MSCHAPv2
- PEAPv1/ EAP-GTC
- EAP-SIM,
- EAP-AKA
- EAP-FAST

Dovrà essere possibile inoltre definire per una o più reti Wireless, dei portali di GuestRegistration o Self Registration, utilizzando come metodo di dispatch delle credenziali, per esempio l'invio, di una e-mail, di un SMS o la stampa cartacea di un Ticket. Sarà l'amministratore a decidere i metodi di SelfRegistration, i metodi di invio delle credenziali e il periodo di validità delle utenze.

1.11.1.8 Sistemi di Autenticazione

Per garantire un elevato livello di sicurezza e di controllo degli accessi sulla rete Wi-Fi verranno implementati vari metodi di autenticazione per ciascuna tipologia di accesso. Allo stesso tempo, per migliorare la fruibilità dell'infrastruttura, verrà implementata per i Visitatori una soluzione di Self Registration che permetterà agli utenti di poter creare il proprio account di accesso alla rete una volta entrati in contatto con la rete stessa all'interno del perimetro del sito.

1.12 I prodotti forniti inoltre DEVONO rispettare le seguenti specifiche:

- Prodotti originali recanti il marchio di fabbrica del costruttore;
- Prodotti nuovi nel loro packaging originale, acquistati e licenziati tramite canali autorizzati dal costruttore;
- Tutti i prodotti forniti per la gestione della rete e della relativa sicurezza, dovranno essere prodotti da un unico costruttore;
- L'Aggiudicatario DEVE fornire licenze software originali rilasciate per il Comune ed apparati idonei allo scopo;
- L'Aggiudicatario non potrà fornire materiali di provenienza illegale, o prodotti usati e rigenerati.
- Tutto il software originale sviluppato nel progetto DEVE essere rilasciato in formato sorgente, compresa la licenza di utilizzo illimitato anche per scopi commerciali.

1.13 Caratteristiche minimali richieste per il Sistema Punto Punto-Multi-Punto

Al minimo 4 (quattro) Access Point da installare presso il Comune;

Al minimo 2 (due) Access Point che garantiscano:

- La completa compatibilità con il firmware OpenWisp e Openwrt;
- Compatibili con lo standard 802.11 a/b/g/n a 2,4 GHz e 5 GHz;
- Annuncio di più reti (Multiple SsiD);

Al minimo 1 (uno) Sistema di controllo e monitoraggio per la rete;

Al minimo 10 (dieci) Access Point Indoor/Outdoor client per la ricezione del segnale con interfaccia WIFI 5GZ/2.4Ghz con una interfaccia per rete Wi-Fi, completi di antenne, alimentazione e fissaggi a muro;

Al minimo 12 (dodici) Alimentatori PoE (Power over Ethernet);

Al minimo 4 (quattro) Device radio mobili Wi-Fi/Wimax/PreWimax usb interfacciabili a pc portatili o desktop;

Al minimo 10 (dieci) Telecamere per videosorveglianza;

Al minimo 4 (quattro) Apparati di rete Switch a 24 porte Gb ethernet che dovranno nativamente essere gestiti dal controller centralizzato del sistema Wi-Fi;

Software di gestione e monitoraggio dell'intero sistema;

Inoltre si richiede:

La fornitura di tutto quanto necessario per collegare tra loro gli Access Point, i controller e gli apparati di rete e per i collegamenti all'infrastruttura esistente, i materiali che verranno impiegati dovranno soddisfare i requisiti più avanti specificati.

Il montaggio a muro o a soffitto o a parete o su palo della antenna BTS (Base Station) e delle CPE/Client nelle posizioni specificate, che verranno concordate con il responsabile del progetto;

L'eventuale configurazione degli apparati CPE;

Il montaggio degli apparati attivi (Switch) negli armadi Rack previsti da progetto;

L'installazione e configurazione degli apparati di controllo;

Il corso di formazione dedicato avente per oggetto la gestione del sistema installato;

Il Sistema di monitoraggio della soluzione wireless installata.

La Base Station (BTS) DEVE essere installata presso le strutture del Comune ed indicato dopo sopralluogo obbligatorio.

Deve essere predisposto inoltre uno studio RF di Radiofrequenza per la copertura dei punti indicati.

La presente attività porterà alla messa in opera di un progetto, la cui realizzazione consentirà di creare un'infrastruttura tecnologica per la realizzazione di una rete WAN per la copertura dell'area di Tor Lupara.

Il sistema DEVE garantire anche:

- Capacità di veicolare servizi di videoconferenza e videostreaming in mobilità;
- Capacità di integrazione ed interconnessione con la rete dati esistente;
- Distribuzione capillare dell'infrastruttura di rete Wireless sul territorio rispondente a criteri di alta affidabilità e sicurezza;
- Scalabilità futura, prevedendo la possibilità di una facile estensione della rete al crescere delle necessità di copertura del Cliente;
- Stretto controllo dell'accesso alla rete al fine di garantire un utilizzo corretto delle risorse di connettività;
- Utilizzo di Bande di frequenza 2,4 Ghz a 5 Ghz WIRELESS
- Velocità minime di collegamento per i client nomadici di 3-4 Mbps, per i client mobile 1Mbps in Uplink per la trasmissione di Video streaming;
- Garanzia del passaggio tra una cella di copertura e l'altra con sistema di hand-over senza perdita di connettività (verifica di ping di connessione);
- Possibilità di facile estensione della connettività anche ad altri soggetti che facciano richiesta successivamente all'entrata in funzione del sistema (i collegamenti saranno in un primo momento riservati ai soli soggetti coinvolti nelle gestioni associate dei servizi);
- L'Accesso alla rete oggetto dell'appalto DEVE poter essere effettuato in modo "controllato" al fine di garantire un utilizzo corretto delle risorse di connettività;
- La connessione integrata di un accesso Wi-Fi per permettere anche un collegamento con terminali mobili e fissi Wi-Fi;
- Dovranno essere previsti Standard di cifratura e sicurezza e protocolli che dovranno essere supportati per il lato Wi-Fi:
- WPA (Wi-Fi Protected Access);
- IEEE 802.11 i. WPA 2 (Wi-Fi Protected Access version 2) e RSN (Robust Security Network);
- Supporto per IEEE 802.1x;
- Supporto per IEEE 802.1x RADIUS guideline;

- Supporto per Extensible Authentication Protocol (EAP);
- Supporto per Web-based authentication;

Gli Access Point dovranno essere in grado di supportare gli standard IEEE 802.11 a/b/g/n e in grado di fornire servizi wireless ad alta capacità trasmissiva. L'uso del supporto hardware per Advanced Encryption Standard (AES) o al Temporal Key Integrity Protocol (TKIP) DEVE garantire l'interoperabilità con il protocollo IEEE 802.11i, WPA o WPA 2.
L'Access Point potrà essere gestito e configurato come dispositivo autonomo oppure, con l'utilizzo di un controller, come parte di un'architettura centralizzata Wi-Fi. Gli Access Point dovranno essere dotati di antenne omnidirezionali integrate nel dispositivo per garantire una facile e immediata installazione. Sarà considerata positivamente la fornitura di AP integrati con MESH.

L'aspetto estetico degli apparati sarà un fattore determinante, in quanto gli stessi saranno posizionati in varie aree espositive e dovranno quindi avere al minimo antenne integrate e cover in PVC.

Specifiche generali richieste per gli AP:

- Certificazione Wi-Fi;
- Collegamento LAN Ethernet almeno 100Mbps;
- Collegamento LAN con supporto al protocollo 802.3af;
- Tecnologie di trasmissione OFDM
- Caratteristiche Radio 802.11 a/b/g/n;
- Possibilità di utilizzo di supporti a muro o a soffitto.
- Cifratura, sicurezza ed autenticazione:
- WPA (Wi-Fi Protected Access);
- EAP- Tunneled TLS (EAP- TTLS);
- EAP-Subscriber Identity Module (EAP-SIM);
- Approvazioni radio:
- EN 300.328
- EN 301.893;

Specifiche generali richieste per gli alimentatori:
Gli alimentatori (power injector) PoE se necessari dovranno rispondere allo standard IEEE 802.3af.
La realizzazione dell'infrastruttura si compone delle seguenti due fasi:
1) installazione e configurazione degli apparati attivi di rete;
2) installazione dell'antenna BTS e degli apparati wireless Client CPE.

L'infrastruttura offerta DEVE basarsi sull'impiego di un sistema di controllo in grado di operare in modo coordinato e centralizzato per garantire il bilanciamento nell'uso della banda e delle risorse hardware e software.
Il sistema, una volta configurato, avrà il compito di garantire la gestione centralizzata di tutti i parametri di funzionamento delle CPE e degli eventuali AP Wi-Fi a terminazione delle CPE. Il sistema di autenticazione utente sarà interfacciato l'Identity Management offerto ma DEVE poter supportare anche un'autenticazione stand-alone.
Il controller centralizzato dovrà necessariamente integrare funzionalità di Firwalling avanzato di tipo UTM e dovrà essere fornito di almeno 2 (due) interfacce 10 Gbps.
Inoltre detto controller dovrà essere adeguatamente ridondato grazie ad una unità gemella. La modalità di funzionamento della alta disponibilità dovrà essere (a scelta dell'ente appaltante) Active Active o Active Stand-By.
Il posizionamento della BTS e delle CPE con i relativi AP Wi-Fi DEVE essere coerente alle risultanze del sopralluogo obbligatorio effettuato.

Specifiche generali richieste per le telecamere:
Grado di protezione IP66
Risoluzione minima 2Megapixel
Interfaccia Ethernet e/o Wi-Fi

Copertura richiesta

L'Aggiudicatario DEVE garantire una copertura radio ottimale dei luoghi oggetto dell'appalto.
Saranno considerati elementi premianti per i sistemi offerti, le tecnologie o la presenza di caratteristiche specifiche degli apparati, per evoluzioni del sistema stesso, che consentano l'impiego di meccanismi analoghi a quelli in uso nei sistemi di telefonia mobile volti a semplificare sensibilmente:

- Il processo di definizione della migliore allocazione delle CPE (site survey);
- Il processo di gestione dell'Infrastruttura;
- Le espansioni future del sistema verso servizi mobili e copertura per l'area Centro Abitato di Tor Lupara.

Cablaggi specifici richiesti

Per il collegamento di tutti gli elementi previsti si richiede la fornitura e posa in opera di un sistema di cablaggio strutturato per il collegamento degli AP alla rete nel caso non esista diversa alternativa per connetterli alle CPE.

L'Aggiudicatario DEVE fornire elaborati grafici esecutivi, indicante il posizionamento di quanto andrà installato.

A conclusione dei lavori, i disegni esecutivi dovranno essere accuratamente aggiornati e includere le esatte locazioni delle postazioni e le indicazioni d'etichettatura degli elementi (as built). In aggiunta DEVE essere consegnato un rapporto sull'esecuzione dei lavori, che includa un'analisi delle attività d'installazione operate dall'installatore stesso.

Modalità di redazione del Progetto Tecnico

Le Ditta partecipante DEVE strutturare l'offerta tecnica organizzando l'esposizione dei contenuti nei seguenti capitoli:

1) Descrizione generale della soluzione offerta
2) Descrizione dettagliata dei requisiti funzionali della soluzione offerta
3) Descrizione dettagliata della soluzione offerta contenente la descrizione dell'architettura e delle componenti del sistema offerto e la descrizione del linguaggio di sviluppo
4) Indicazione di ulteriori caratteristiche ritenute utili alla valutazione dell'offerta
5) Illustrazione dettagliata delle modalità di utilizzo dell'infrastruttura esistente
6) Descrizione del tipo di licenza con cui verranno cedute tutte le componenti software con indicazione precisa dei limiti eventualmente previsti
7) Descrizione delle modalità di realizzazione/personalizzazione, installazione, avviamento del software e del relativo addestramento all'uso
8) Descrizione della documentazione fornita
9) Programma della fornitura con indicazione del tempo di completamento nel formato di diagramma di Gantt.
10) Durata della garanzia e descrizione del servizio di manutenzione

Requisiti Organizzativi richiesti

1.14 Project Plan

Il piano di progetto DOVREBBE essere organizzato per fasi.
Ogni fase DEVE avere dei rilasci documentali e realizzativi chiaramente identificabili e misurabili.

Ogni fase DEVE terminare con un'accettazione formale dei rilasci della fase stessa e DEVE essere prodotta documentazione formale a corredo.
Ogni fase è prerequisito della successiva e l'accettazione di fase ne innesca l'inizio.
Oltre alle fasi già indicate DOVREBBERO essere previste le seguenti fasi:

- Supporto alla produzione
- Manutenzione

1.15 Piano della Qualità e Piano dei Test

La ditta partecipante DEVE predisporre nel Progetto Tecnico un dettagliato Piano della Qualità corredato da relativo Piano dei Test e livelli di servizio, ed in particolare:

- Piano e Risorse di monitoraggio
- Piano di test sistema di autenticazione e politiche per la sicurezza
- Piano di test funzionalità e servizi
- Planning e Cronoprogramma dettagliato delle attività da svolgere
- "Manuale operativo del Servizio Clienti" cioè' il manuale standard del fornitore contenente i SL (Livelli di Servizio) erogati ai propri Clienti

Il Piano di Qualità delle attività sarà redatto dal Fornitore sulla base del proprio manuale di qualità e in conformità a quanto richiesto dalle circolari AIPA/CR/5 del 5 agosto 1994 e AIPA/CR/38 del 28 dicembre 2001, quanto suggerito dalla Deliberazione AIPA n. 49/2000 del 9 novembre 2000 e con quanto previsto dagli standard internazionali ISO:9000:2000

Sia il Piano che il relativo cronoprogramma saranno oggetto di valutazione.
Il fornitore dovrà esprimere anche tutte le Licenze d'uso interessate alla proposta

Durata del Servizio

Il servizio di assistenza e manutenzione preventiva e correttiva DEVE essere garantito e gratuito per un periodo minimo di almeno 24 (ventiquattro) mesi a partire dal giorno del collaudo, periodo dopo il quale inizierà il servizio a pagamento previsto almeno per 3 (tre) anni.

Il Fornitore, in sede d'offerta tecnica DEVE presentare una prima bozza di Piano di Progetto che DEVE contenere anche l'ipotesi proposta per la tempistica delle attività, con particolare riferimento ai rilasci successivi al primo.

Regola di Esecuzione della Fornitura

1.16 Monitoraggio e valutazione del progetto

L'attività di monitoraggio permetterà il controllo e la valutazione in corso d'opera del progetto. Nasce con il progetto e continua anche dopo che lo stesso è diventato operativo, dovendo accertare in ogni momento che il progetto stesso e/o le parti che lo compongono siano in linea con gli obiettivi e le aspettative in termini di pertinenza (condizione di validità funzionale nei confronti di ciò che si persegue), efficacia (attitudine dell'elemento sotto valutazione a produrre risultati), efficienza (uso ottimale delle risorse), tempestività (capacità di produrre risultati in tempo utile rispetto alle esigenze), flessibilità (capacità dell'elemento ad evolvere in funzione del potenziamento dei bisogni dell'utenza).

Le tecniche di controllo che verranno usate sono:

- Controllo di progetto, cioè la verifica dell'attuazione e la rilevazione degli scostamenti tra valori progettati, pertanto il progetto è tenuto in osservazione sotto il profilo del controllo che è teso a valutare se quanto si sta svolgendo sia coerente con quanto è stato previsto nell'elaborato progettuale;
- Valutazione in corso d'opera, nella quale si svolgono funzioni di rilevazione e valutazione, di anticipazione e di previsione sulla base di scenari alternativi, ricerca delle cause di quanto accade e degli effetti che si generano, di individuazione delle responsabilità, di formulazione delle azioni correttive, di determinazione della pertinenza di quanto si sta realizzando rispetto al disegno progettuale, di valutazione dell'efficienza nella condotta dell'attuazione del progetto e di quella dell'efficacia del prodotto ottenuto rispetto al conseguimento degli obiettivi, di stima al completamento;
- Revisione o "audit", attività di accertamento, verifica e valutazione dell'efficacia dei controlli adottati, si esplica tramite l'accertamento del grado di aderenza dei comportamenti alle politiche, ai piani e alle procedure stabilite e l'accertamento del livello di sicurezza e di protezione degli aspetti patrimoniali;

In particolare durante la fase di Analisi e Progettazione la funzione di monitoraggio e valutazione verificherà la rispondenza delle Specifiche Funzionali e Tecniche agli obiettivi ed ai requisiti definiti, per quanto riguarda la pertinenza, l'efficacia, l'efficienza, la tempestività e la flessibilità.

Durante la fase di Realizzazione la funzione di monitoraggio e valutazione verificherà la pertinenza, l'efficacia, l'efficienza, la tempestività, e la flessibilità di quanto si realizza con l'elaborato progettuale.

Durante la fase di primo Esercizio la funzione di monitoraggio e valutazione misurerà gli scostamenti tra le prestazioni previste e quelle operative in termini di facilità di apprendimento di soddisfazione e di utilizzo dell'utenza. Quindi verificherà eventuali modifiche da apportare al Sistema Informativo controllando che esse siano pertinenti, efficaci, efficienti e soprattutto non invalidino l'applicazione originaria.

1.17 Installazione e messa in esercizio

Tutto il Sistema, oggetto della presente gara, dovrà essere fornito e reso PRONTO AL COLLAUDO, entro e non oltre il 30 aprile 2015

1.18 Start-up

La Ditta aggiudicataria, DEVE garantire interventi di manutenzione correttiva almeno fino al collaudo finale dell'intera fornitura.
Il Progetto Tecnico della Ditta partecipante DEVE descrivere dettagliatamente quanto necessario a garantire l'organizzazione del servizio ed i tempi di risposta alle richieste di manutenzione che verranno avanzate.

1.19 Collaudo

L'intera fornitura sarà sottoposta a collaudo dopo l'avvenuta consegna, installazione e messa in funzione, su richiesta della ditta aggiudicataria sarà possibile effettuare anche collaudi parziali della fornitura.
Il collaudo sarà effettuato entro 10 giorni dalla dichiarazione di "Pronti al Collaudo" sulla scorta di un'apposita Lista di Collaudo predisposta dalla ditta ed approvata dal Comune di FONTE NUOVA.
Le prove di collaudo saranno eseguite in contradditorio tra i rappresentanti della STAZIONE APPALTANTE e dall'AGGIUDICATARIO.
In caso di difformità, l'AGGIUDICATARIO si impegna alla loro eliminazione entro il termine massimo di 30 giorni naturali e consecutivi dal momento del rilievo, cui seguirà nuova prova di

collaudo. Tutte le prove daranno luogo ad altrettanti verbali di collaudo che, firmati dalle parti, costituiranno la base dei successivi adempimenti contabili amministrativi.

1.20 Servizi di affiancamento

Il progetto DEVE prevedere un'attività di affiancamento intesa ad addestrare gli amministratori del sistema del Comune di Fonte Nuova che dovranno gestire il sistema integrato. Tutte le attività dovranno essere essenzialmente orientate agli aspetti pratici e dovranno essere corredate da esercitazioni su casi reali.

1.21 Addestramento all'utilizzo

Il Progetto Tecnico DEVE contenere le modalità di addestramento del personale del Comune di FONTE NUOVA nell'utilizzo del Sistema.
Nel Piano di Addestramento si DEVE prevedere tra l'altro, la predisposizione ed il rilascio del materiale tecnico/informativo (sia in formato cartaceo che elettronico) da parte della ditta.

1.22 Manutenzione del Sistema

La Ditta DEVE specificare le modalità e le caratteristiche della dell'assistenza e della manutenzione fornita sull'intero sistema.

Il Fornitore DEVE assicurare il corretto funzionamento dei servizi e la completezza delle informazioni offerti dal sistema e accessibili agli utenti.
A tal fine il Fornitore DEVE illustrare, in fase di offerta, i criteri e le norme tecnico-organizzative che intende mettere in atto per garantire la corretta gestione della fornitura nel suo complesso, e per assicurare la più efficace erogazione dei servizi, nel rispetto dei requisiti di qualità/sicurezza e dei Livelli di servizio previsti.

Le attività che il Fornitore DEVE svolgere sono:

- Le attività di conduzione tecnico/funzionale degli applicativi.
- La manutenzione correttiva.
- La manutenzione evolutiva (aggiornamento alle nuove versioni delle piattaforme).

Conduzione tecnico/funzionale degli applicativi

Il servizio è volto a garantire il funzionamento del parco applicativo che compone il sistema, l'amministrazione delle Basi Dati e la gestione del sistema di monitoraggio.
Tale servizio comprende anche l'attività di trasferimento a fine fornitura del know how relativo all'intera fornitura alla STAZIONE APPALTANTE o ad altro ente/azienda da questa indicata.

La manutenzione correttiva

Il servizio consiste nella manutenzione correttiva del software standard e software realizzato nell'ambito della presente fornitura. Il servizio DEVE essere erogato - in regime di garanzia - dal primo rilascio in esercizio e per tutta la durata della fornitura.
Il servizio prevede la diagnosi e la rimozione delle cause e degli effetti dei malfunzionamenti delle procedure e dei programmi.
L'attivazione del servizio di manutenzione correttiva è innescata, di norma, da una richiesta d'intervento effettuata al servizio di Contact Center, a seguito d'impedimenti all'esecuzione dell'applicazione o differenze riscontrate fra l'effettivo funzionamento dei software applicativi rispetto a quello atteso, desunto dalla documentazione disponibile.
Ogni intervento di manutenzione correttiva DEVE essere registrato dal servizio di Contact Center.
Il Fornitore DEVE indicare come intenda effettuare le attività di supporto di primo e secondo livello a partire da un contact center e come intenda comunque effettuarle.
I Service Level del servizio saranno concordati con la STAZIONE APPALTANTE ad inizio fornitura.
Il fornitore DEVE consegnare il "Manuale operativo del Servizio Clienti" cioè' il manuale standard del fornitore contenente i SL (Livelli di Servizio) erogati ai propri Clienti

1.23 Documentazione

DEVE essere fornita dalla ditta aggiudicataria tutta la documentazione operativa necessaria ed idonea a consentire agli utenti ed agli amministratori l'utilizzo del Sistema nonché tutta la documentazione tecnica necessaria ed idonea ad amministrare il Sistema ovvero:

- Manuale di informazioni generali
- Manuale utente
- Manuale operatore
- Manuale amministratore

- Documentazione tecnica di dettaglio concernente il software applicativo e di sistema sviluppato ad hoc
- Qualsiasi altro documento utile a una migliore comprensione del funzionamento del sistema.

1.24 Riuso

La ditta aggiudicataria DEVE fornire una apposita liberatoria con il relativo trasferimento dei diritti esclusivi di proprietà del sistema realizzato.