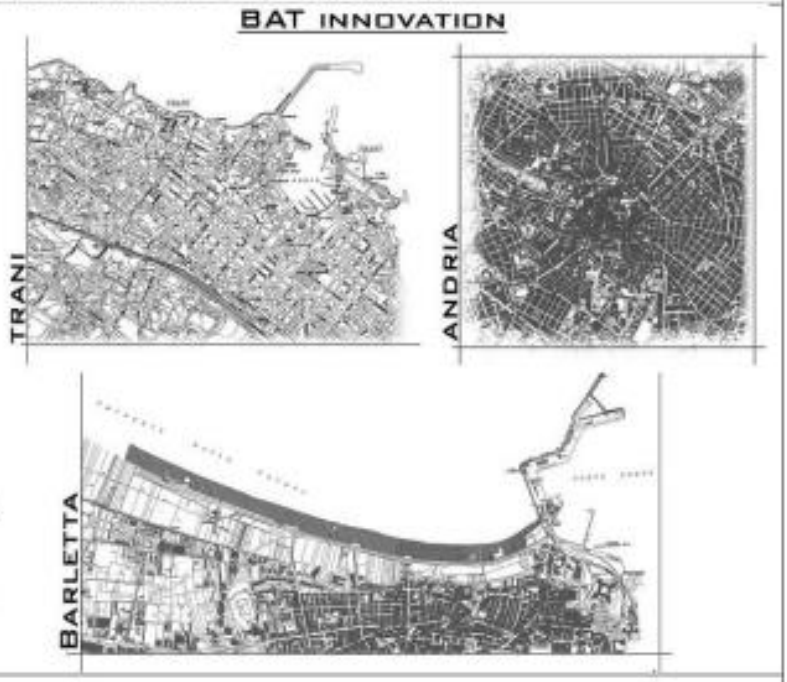
PATTI PER LE CITTA'

PPA PO FESR 2007-2013 - PAC

ASSE I - LINEA D'INTERVENTO 1.5 - AZIONE 1.5.2

"BAT innovation"

Progetto per il Miglioramento della Vivibilità, Sicurezza e Tutela dei Centri Storici dei Comuni di Andria, Barletta e Trani.



COMUNE DI BARLETTA
Città della Disfida

Città di Andria

CITTA' DI TRANI

PROGETTO ESECUTIVO

Il Progettista	Responsabile del Procedimento
RTP (Raggruppamento Temporaneo di Professionisti): **Ing. Giuseppe Perillo** (Mandatario) **Italiantech S.r.l. [D. T. Ing. P. Del Sorbo]** (Mandante) **Ing. Giampietro Massarelli** (Mandante - Giovane Professionista)	**Dott. Savino Filannino**

ELABORATO	DESCRIZIONE	REV.	DATA
A.016	**Disciplinare Tecnico Prestazionale Sistema Cloud**	**1**	**07/08/2020**

1 ESIGENZE DELL'AMMINISTRAZIONE

Si riportano di seguito i requisiti richiesti per i servizi Cloud.

1.1. Descrizione del Contesto di Riferimento dell'Amministrazione

Le tre città co-capoluogo Barletta, Andria e Trani, si sono unite per la valorizzazione dei centri storici in ambito ambientale, di sicurezza del territorio, valorizzazione dei beni culturali, turismo e mobilità sostenibile aderendo all'iniziativa "Patti per le Città", iniziativa compresa nell'azione 1.5.2 del PPA, Periodo 2007–2013, *Asse I – Promozione, valorizzazione e diffusione della ricerca e dell'innovazione per la competitività, Linea 1.5 "Interventi per lo sviluppo dei servizi pubblici digitali"*.

L'iniziativa si propone di individuare una declinazione locale del paradigma delle "smart cities and communities" e, in particolare, sostenere azioni pilota volte allo sviluppo di un insieme di reti funzionali in grado di decodificare i dati che le nuove tecnologie mettono a disposizione per interpretare, in modo condiviso e partecipato, la vocazione di un territorio all'interno del panorama internazionale e di proporre e abilitare nuovi stili di vita più sostenibili, generando nuovi processi di sviluppo dal basso per una effettiva inclusione anche delle fasce di popolazione marginalizzate.

L'azione in questione si muove su due direttrici: la prima è relativa alla costituzione di una rete regionale di servizi, finalizzata allo sviluppo del sistema di e-Government e della Società dell'Informazione nelle Amministrazioni locali; la seconda riguarda la diffusione di contenuti, applicazioni e servizi digitali avanzati inerenti gli ambiti di riferimento delle smart cities and communities, con l'obiettivo di renderli accessibili a tutta la popolazione.

Il progetto "Patti per le Città" prevede la realizzazione del sistema sopra descritto adattato propriamente alle esigenze dei Comuni di Barletta, Andria e Trani con l'obiettivo di gestire la rete di pubblica amministrazione dei centri storici e ridurre così il consumo energetico, contribuendo alla riduzione dell'impatto inquinante dei centri urbani; aumentare il servizio adibito alla sicurezza delle persone e del patrimonio culturale nei centri storici delle tre città attraverso un sistema di videosorveglianza installato sia all'interno delle aree Z.T.L. che in quelle contermini ad esse; estensione della copertura WiFi per consentire la connessione gratuita ad internet; gestire gli stalli dei parcheggi nelle aree del centro cittadino; produrre un sistema digitale di info-localizzazione dei beni storico-architettonico culturali, e delle accessibilità ai centri cittadini.

Il sistema si compone quindi dei seguenti ambiti progettuali:

- OR1 – Sistemi di telegestione della pubblica illuminazione;
- OR3 – Servizi di collegamento ad Internet con WiFi pubblici;
- OR4 – Servizi di telegestione stalli dei parcheggi;
- OR5 – Servizi di prevenzione tramite videosorveglianza;

- OR6 – Info-localizzazione dei servizi.

Lo scopo del presente Disciplinare Tecnico Prestazionale è la specificazione delle caratteristiche tecniche delle risorse Iaas, Baas e Servizi Professionali di Cloud Enabling necessari alla realizzazione degli ambiti OR5 e OR6 per il solo Comune di Barletta. Nello specifico, per il sistema di Videosorveglianza verrà fornita esclusivamente la componente infrastrutturale in Cloud per l’erogazione delle funzionalità di video-server/sistema di registrazione, mentre la componete applicativa, gli apparati video e la connettività degli apparati non sono oggetto della seguente fornitura.

Per l’ambito relativo alla info-localizzazione dei servizi, saranno fornite le risorse Iaas e Baas, mentre la componente applicativa rimane in carico all’Amministrazione.

1.2. Macro Requisiti ed Obiettivi dell’Amministrazione

Per la piattaforma applicativa da erogare in Cloud, l’Amministrazione richiede l’utilizzo delle seguenti risorse virtuali:

ID	Ruolo	vCPU	RAM (GB)	BOOT (GB)	DATA (GB)	SO
VM1	Videosorveglianza	12	96	50	24000	Windows Server 2016
VM2	Infomobilità	12	32	50	8000	Windows Server 2016

1.3. Prerequisiti di Rete

L’impianto di videosorveglianza si compone di 20 telecamere IP con risoluzione da 2Mpx dislocate sul territorio cittadino. Per veicolare il flusso video proveniente dalle telecamere, il sistema deve prevedere una tecnologia wireless, del tipo HIPERLAN 2 (High Performance Radio LAN) che permette di collegare dispositivi dotati di porta ETHERNET (computer, antenne, telecamere, ecc.) in una rete IP virtuale con collegamenti a lunga distanza (decine di chilometri) come se fossero in rete locale.

Tale sistema dovrà sicuramente rispettare i requisiti di seguito riportati:

- capacità di banda necessaria al trasferimento delle immagini in funzione delle caratteristiche delle telecamere e della topologia della rete di trasporto;
- crittografia dei flussi video in accordo a quanto richiesto al paragrafo 3.3.1 comma f) dal “Provvedimento in Materia di Videosorveglianza” del 08/04/10 del Garante per la Privacy (utilizzo di reti pubbliche e connessioni wireless);

Per consentire il trasferimento di immagini di qualità anche su reti con larghezza di banda limitata, le telecamere da impiegare dovranno supportare il formato di compressione H.265, che permette elevati livelli di qualità video pur riducendo le dimensioni del video.

Alla luce di queste informazioni e per la corretta trasmissione dei frames in real-time, è indispensabile avere un collegamento dedicato in fibra GigaBusiness con banda disponibile pari a 100 Mbps in download/upload tra il punto di raccolta dei flussi video localizzato nella sede del Palazzo di Città e l’infrastruttura Spc Cloud che ospiterà la componente applicativa di tale sistema. Questa connessione sarà configurata, tramite un tunnel protetto con protocollo IPSec, con una VPN Site-to-Site tra la sede dell’Amministrazione e il VDC in Cloud.

Il Comando di Polizia Municipale è invece la sede operativa in cui saranno installate le postazioni per gli operatori che monitoreranno le immagini catturate dalle telecamere e che accederanno al software per la videosorveglianza. La connettività tra la rete locale del Comando di Polizia e l’applicativo di video-sorveglianza in Cloud potrà essere realizzata in due modalità: la prima prevede un collegamento dedicato in fibra con banda disponibile pari a 100 Mbps in download/upload, protetto da un tunnel VPN. La seconda opzione prevede la creazione di un link, laddove non fosse già presente, tra la sede del Comando di Polizia Municipale e la sede del Comune, con una idonea banda congrua alla tipologia e quantità di traffico prevista. In questa configurazione la sede Comunale sarebbe il centro stella della rete costituita dagli apparati terminali del sistema (videocamere, postazioni degli operatori e server in Cloud).

Per la creazione del tunnel IPSec saranno installati un Firewall Virtuale nel tenant in Cloud, oggetto della presente fornitura, ed un firewall fisico (si consiglia un Fortigate 200E) di cui l’Amministrazione dovrà dotarsi e che sarà installato presso la sede comunale.

Per il Comando dei Vigili Urbani sarà altresì opportuno dotarsi di un firewall fisico dedicato alla videosorveglianza, indipendentemente dalla tipologia di connessione che si deciderà di implementare tra le due ipotesi progettuali avanzate, essendo, peraltro, l’architettura di rete dell’Amministrazione attualmente non nota.

Pertanto, connettività e apparati fisici di sicurezza non sono oggetto della presente fornitura, ma costituiscono elementi necessari e propedeutici alla messa in esercizio dell’intero sistema di videosorveglianza.

Si evidenzia che saranno altresì predisposti degli accessi in VPN Client-to-LAN per l’accesso al tenant da parte del Cliente/fornitore applicativo della soluzione.

L’applicativo web in ambito info-mobilità sarà invece esposto su Internet, per consentirne la fruizione al maggior numero di utenti possibili.

2 REQUISITI RICHIESTI

Per rispondere ai requisiti indicati dall’Amministrazione nel presente progetto sono previsti i seguenti servizi:

1. **Soluzione IaaS (Infrastructure as a Service):** per l’erogazione delle piattaforme informatiche verrà utilizzata l’infrastruttura Cloud della convenzione SPC;
2. **Soluzione BaaS (Backup as a Service**): onde permettere il pieno ed efficiente Backup & Restore dei sistemi gestiti a livello sistemistico dal Cloud Enabler, l’infrastruttura verrà dotata del servizio Backup as a Service previsto dalla Convenzione SPC Cloud Lotto 1;
3. **Cloud Enabling**: sono previste figure professionali finalizzate a supportare l’Amministrazione.

Oltre alle VM individuate dall’Amministrazione, nel tenant sarà anche previsto il servizio di virtual firewall con la predisposizione della seguente VM che fungerà anche da VPN Concentrator.

ID	Ruolo	vCPU	RAM (GB)	STORAGE (GB)
VM3	vFirewall/VPN Concentrator	4	8	2000

3 PROGETTO DI ATTUAZIONE DEL SERVIZIO L1.S1.2 IAAS - VIRTUAL DATA CENTER

Descrizione

Il servizio “IaaS - Virtual Data Center” permette alle Amministrazioni di creare e gestire uno o più Virtual Data Center (VDC) remoti contenenti risorse virtuali quali server, aree di storage, reti. Tale servizio è reso disponibile alle Amministrazioni a partire dalla acquisizione di uno o più “Pool base” di risorse virtuali in termini di numero di CPU [vCPU], RAM [GB] e spazio Storage [GB/TB], con successiva possibilità di espansione o riduzione delle stesse risorse in autonomia, a seconda delle diverse esigenze. Il servizio consente quindi all’Amministrazione di avere a disposizione e riservare risorse computazionali e di organizzarle autonomamente secondo una logica così definita di Virtual Data Center.
L’aggiornamento delle componenti software presenti nella macchina virtuale (es. patching del sistema operativo) è a carico dell’Amministrazione che fruisce del servizio.

Il Fornitore, nell’ambito del servizio “IaaS - Virtual Data Center” garantisce la disponibilità per l’Amministrazione almeno delle seguenti funzionalità base / strumenti a supporto:

- acquisto di Pool di risorse virtuali “pre-configurate”, comprensivi di una quantità predefinita di CPU [vCPU], RAM [GB] e Storage [GB/TB];

- acquisto di “risorse virtuali extra” a partire da tagli minimi predefiniti ad integrazione del pool base:

  a. CPU [1vCPU]
  b. RAM [1GB]
  c. HD [10GB]

- workflow di installazione e configurazione del VDC e dei suoi elementi costituenti: VM, aree di storage, reti;
- selezione, previo controllo di coerenza con le risorse acquisite, di uno specifico template da installare sulle VM, tra le seguenti tipologie rese disponibili all’Amministrazione:
  - sistemi operativi di tipo Microsoft, Linux/GNU Variants o F/OSS, per configurare lo IaaS base. Il Fornitore garantisce nei limiti di quanto previsto dai contratti di licenza dei singoli produttori, la possibilità per l’Amministrazione di utilizzare sistemi operativi Open Source (ad es. Ubuntu, Debian, CentOS, openSuse, Fedora …), di utilizzare sistemi operativi con proprie Licenze (Bring Your Own License) oppure la possibilità di fornire la Licenza all’Amministrazione, con quotazione economica distinta;
  - solution stack di proprietà dell’Amministrazione possono essere installati sul VDC da parte dell’Amministrazione senza oneri aggiuntivi; qualora le capacità elaborative del VDC non fossero sufficienti a garantire la corretta operatività, l’Amministrazione potrà procedere ad acquisire ulteriori risorse elaborative secondo le modalità di acquisto previste per il servizio di VDC;
  - template originati/prodotti da una singola Amministrazione (ad es. originati dalla virtualizzazione dei propri server e utilizzati quindi per caricare tali server virtualizzati). Il Fornitore infatti potrà prevedere funzionalità di upload in appositi slot di template di macchine virtuali, predisposte in formati basati su standard (ad es. secondo Open Virtualization Format) dalle Amministrazioni anche utilizzando il supporto dei servizi di Cloud Enabling. I template creati dalle Amministrazioni saranno disponibili in fase di creazione di nuove VM;
  - template originati/prodotti da AgID/Consip (es. per sistemi cross-PA) e messi a disposizione in comune tra più Amministrazioni. Il Fornitore prevede appositi slot resi disponibili unicamente ad AgID/Consip per garantire l’upload dei template. AgID/Consip potranno poi definire quali Amministrazioni da quel momento potranno selezionare tali template in fase di configurazione delle VM. Qualsiasi licenza software eventualmente richiesta dal template selezionato sarà a carico dell’Amministrazione che selezionerà il template;

- workflow di gestione e configurazione delle altre risorse base comprese di default nell’acquisto dei pool del VDC e nell’attivazione delle singole VM ad esso afferenti (es. vNetwork e schede di rete per ogni server,vFirewall, vLoadBalancer);
- possibilità di connettere/scollegare in autonomia il VDC e/o le singole VM dalla rete pubblica (internet) edalla rete SPC;
- possibilità di attivare e disattivare il VDC;
- possibilità di effettuare Operazioni Schedulate (singole o ricorrenti), tra cui ad esempio accendere- spegnere forzatamente-arrestare il VDC e/o le singole VM, modificare le risorse computazionali (CPU e/oRAM);
- backup quotidiano delle VM configurate nell’ambito del VDC nella loro interezza al fine di proteggere le stesse da eventi avversi. La soluzione permetterà il ripristino delle VM su richiesta della singola Amministrazione.