Cloud First

la nuova frontiera dell'Amministrazione Digitale

Città metropolitana di Milano

Area Infrastrutture

Indice

Premessa

Il rapido sviluppo delle tecnologie obbliga ad un continuo aggiornamento degli strumenti da utilizzare e delle competenze da sviluppare. La spinta a questo sviluppo è data dal poter offrire servizi sempre più vicini all'utente e concorrenziali dal punto di vista economico.

Per una Pubblica Amministrazione questo significa utilizzare meglio il denaro pubblico per offrire un maggior numero di servizi, qualitativamente migliori, a supporto dello sviluppo economico del proprio territorio e a sostegno delle amministrazioni locali, delle imprese e dei cittadini.

Il cloud computing si inserisce in questa prospettiva: nel mercato dell'ICT è ormai una soluzione affermata e vincente, permettendo economie di scala e livelli qualitativi altrimenti non raggiungibili. Per la Pubblica Amministrazione, il cui core business si discosta da quello del mercato, si tratta di accogliere la sfida e declinare le potenzialità del cloud computing a servizio del territorio.

La sfida per la Città metropolitana di Milano non si ferma all'adeguamento ai sistemi cloud.

Diversi sono gli ambiti del Piano Triennale nei quali la Città metropolitana sta investendo con progetti di innovazione digitale:

- il rinnovo delle postazioni di lavoro,
- la digitalizzazione e la semplificazione dei procedimenti amministrativi legati alla realizzazione delle Opere Pubbliche,
- la semplificazione e digitalizzazione della gestione amministrativa del patrimonio scolastico e degli interventi sugli edifici scolastici dell'area metropolitana,
- l'uso dell'autenticazione SPID nelle piattaforme web,
- il passaggio in cloud,
- la condivisione degli Open Data,
- l'accreditamento al Repertorio Nazionale dei Dati Territoriali (RNTD) per le infrastrutture stradali e le scuole,
- l'apertura al BIM - Building Information Modeling.

Innovare non può limitarsi ad una o più azioni, significa anche attivare processi che costantemente adeguino il modello organizzativo e l'infrastruttura tecnologica, producendo e stimolando una cultura del servizio e del benessere pubblico.

Dal web al cloud: la sfida per la P.A.

La nascita di internet e del web

Nel 1960, il Ministero della Difesa degli Stati Uniti creò il progetto ARPA: si trattava di un'agenzia incaricata di costruire una rete di comunicazione che potesse collegare tra loro anche posti geograficamente lontani e che potesse funzionare anche sotto attacco nucleare. ARPA riuscì a collegare tra loro quattro Università con l'aiuto di un computer e di una linea telefonica: questa piccola rete di comunicazione fu chiamata ARPANET. C'era però bisogno che i dati si spostassero correttamente da un computer all'altro: le informazioni dovevano arrivare in modo corretto e completo e decodificabili nello stesso modo da tutti i computer collegati.

Verso la metà degli anni ’70 nasce quello che oggi chiamiamo **protocollo TCP/IP:** la parte TCP contiene le modalità con cui i dati si spostano fisicamente da una parte all’altra della rete, mentre la parte IP si occupa di come i dati devono essere consegnati ed interpretati dai computer che ne fanno richiesta. Poco dopo fu inventato anche il primo modo con cui due computer connessi potessero scambiarsi dei file: **il protocollo FTP.**

Questa grande Rete connetteva sempre più persone e sempre più Università: è stato quindi necessario creare, ad un certo punto, delle reti di reti. In questo modo più computer venivano collegati tra loro su una piccola rete e tutte le piccole reti venivano connesse su una rete più grande, attraverso una o più dorsali, cioè collegamenti ad alta velocità. Con il tempo sarebbero nate sempre più dorsali in grado di comunicare tra loro sempre più velocemente e di connettere computer sempre più lontani: Internet!

Al CERN di Ginevra alla fine degli anni ‘80 viene inventato il WWW o World Wide Web, che dà la possibilità ai membri del CERN di accedere facilmente, direttamente dalla propria postazione, ai documenti scientifici presenti sui vari computer dell’istituto.

Una importante distinzione:

- per **Internet** si intende l’intera infrastruttura tecnologica, hardware e software, che connette su scala globale miliardi di persone, dispositivi e aziende, permettendo loro di interagire;
- il **WWW** è una componente di Internet, che definisce i protocolli, i linguaggi, le funzionalità che permettono di navigare in rete, come siamo abituati a fare dai nostri computer e smartphone. Il Web è uno dei tanti servizi di Internet, e più precisamente è quello che consente la visualizzazione di dati sotto forma di ipertesto all’interno di un browser.

Così possiamo affermare, ad esempio, che il portale del MEPA (Mercato Economico della Pubblica Amministrazione), Facebook o Instagram, siano applicazioni web (abbreviazione per dire World Wide Web), mentre la posta elettronica, Whatsapp o i cavi transoceanici attraverso cui passano i nostri messaggi in forma di impulsi luminosi non facciano parte del web.

L’unico strumento di cui ha bisogno l’utente per utilizzare il web è un programma gratuito, cioè il browser (ad esempio Chrome, Firefox o Safari).

Lo sviluppo delle Intranet

Fin dagli anni ‘90 le aziende hanno iniziato a sfruttare la semplicità di questo modello, dove il PC posto sulla scrivania degli operatori è stato man mano svuotato delle informazioni e delle applicazioni strategiche, spostando queste ultime sui server e i data center aziendali. Il miglior caso pratico di questa evoluzione è stato lo sviluppo delle Intranet, cioè reti aziendali, basate sui protocolli di internet HTTP e HTML, che necessitano solamente di un browser per accedere ai dati di base per la conoscenza e l’elaborazione aziendale.

I data center aziendali sono diventati quindi il luogo più prezioso e più delicato dell’infrastruttura tecnologica di un’azienda, con un utilizzo di risorse economiche e di competenze sempre più significativo. A titolo di esempio, per garantire la continuità di servizio, la flessibilità alla risposta e la potenza di calcolo necessarie, di solito un server non viene utilizzato oltre il 40% delle sue potenzialità; in aggiunta vanno considerati server aggiuntivi (ridondanti) per prevenire interruzioni

di servizio e garantire risposte a eventuali sovraccarichi (overloading), altri server sono inoltre dedicati al salvataggio e la sicurezza dei dati (sistemi di backup e restore).

Una soluzione che ha reso più efficiente l'uso di queste risorse è stata la virtualizzazione dei server: a fronte di un numero limitato di server fisici particolarmente potenti, i sistemi di virtualizzazione consentono la compresenza di più server virtuali su un singolo server fisico, garantendo bilanciamenti di carico e trasferimento in tempo reale di server virtuali da un server fisico ad un altro, assicurando la continuità del servizio.

Parallelamente a questo sviluppo, da una parte è continuata a crescere la disponibilità di banda e dall'altra la richiesta di continuità di servizio per l'accesso ad Internet da parte delle aziende. Oggi, infatti, la disponibilità di banda è considerato un servizio imprescindibile al pari della fornitura di energia elettrica, telefonica o idrica.

Tutte queste precondizioni hanno permesso la migrazione dei Data Center aziendali su Internet; se si aggiunge a questa un sistema automatico in grado di monitorare, gestire e rendere flessibile la disponibilità di risorse da erogare in tempo reale, si giunge infine a quello che oggi viene chiamato cloud.

Il cloud computing

Letteralmente, cloud computing significa "nuvola informatica" e si riferisce alla tecnologia che permette di elaborare e archiviare dati in rete. Infatti, attraverso internet, il cloud computing consente l'accesso ad applicazioni e dati memorizzati su un hardware remoto invece che sulla postazione di lavoro locale.

Perciò, si intende con cloud computing la distribuzione di servizi di calcolo, come server, risorse di archiviazione, database e software attraverso la rete pubblica, con connessioni private protette. I servizi web sono distribuiti attraverso internet e www.

Il cloud è comunemente utilizzato nella quotidianità da una platea sempre più numerosa ed eterogenea: rappresenta la naturale evoluzione dell'uso del web, con applicazioni di comune utilità come l'uso di social network, la condivisione di foto, documenti e video o l'uso di piattaforme di e-commerce.

È un servizio diventato ormai una commodity, un bene standard ormai consolidato e il sentiero di sviluppo delle tecnologie informatiche sempre più sofisticate, che interagiscono con Internet e permettono agli utenti di soddisfare crescenti esigenze di comunicazione.

Il cloud non rappresenta una nuova tecnologia, ma un modello di condivisione in grado di creare collegamenti tra i diversi livelli di una struttura in modo da stimolare un cambiamento organizzativo.

È quindi un nuovo modo di indirizzare e usare le risorse rese disponibili dall'uso delle infrastrutture ICT basandosi su tecnologie già esistenti. È uno strumento che incrementa e migliora qualitativamente la produttività e la crescita organizzativa, ponendo in discussione il tradizionale ruolo delle risorse IT all'interno del contesto aziendale e non solo.

Si diffonde anche nelle tecnologie il **modello Pay per Use**: l'infrastruttura ICT diventa una risorsa erogabile, la cui potenza può essere aumentata o diminuita a richiesta.

I servizi cloud sono tipicamente suddivisi in tre tipologie:

- **Software-as-a-Service** (SaaS): applicazioni software accessibili tramite Internet, come la posta elettronica, la gestione di documenti, di immagini, sfruttando diverse tipologie di dispositivi (desktop, mobile, ecc …);
- **Platform-as-a-Service** (PaaS): piattaforme per sviluppare, testare e distribuire le applicazioni su internet;
- **Infrastructure-as-a-Service** (IaaS): l'infrastruttura tecnologica fisica e virtuale in grado di fornire risorse di computing, networking e storage da remoto e mediante API (Application Programming Interfaces), senza la necessità di acquistare hardware.

Il cloud a servizio delle nuove esigenze nella P.A.

Visti gli obiettivi della crescita digitale e il continuo incremento nell'uso di documenti digitali, anche la Pubblica Amministrazione non può continuare ad utilizzare un vecchio modello organizzativo nelle proprie infrastrutture IT.

All'AGID - Agenzia per l'Italia Digitale, posta sotto la vigilanza del Presidente del Consiglio, è stato affidato il compito di sostenere le Pubbliche Amministrazioni affinché si raggiungano gli obiettivi prefissati dalla Strategia per la crescita digitale del Paese e con le previsioni del Piano Triennale per l'Informatica nella Pubblica Amministrazione 2019 - 2021, attraverso la qualifica dei servizi e delle infrastrutture cloud, secondo specifici parametri di sicurezza e affidabilità idonei per le esigenze della P.A.

Il Piano Triennale AGID prevede la migrazione dei data center degli enti pubblici in ambiente cloud, per superare i limiti imposti dall'avere proprie dotazioni informatiche, quindi **superare i limiti di logistica e sicurezza propri del modello di gestione in house**.

Il modello cloud della PA si ispira al **principio cloud first** che si prefigge di valutare l'adozione del cloud in fase di definizione di un nuovo progetto o di sviluppo di nuovi servizi, **prima di qualsiasi altra opzione tecnologica tradizionale**. In sinergia con la strategia di cloud enablement (implementazione del cloud) per la migrazione dell'esistente, il principio cloud first nasce con **l'obiettivo di adottare il modello cloud nella P.A. da subito per tutte le nuove iniziative che si intendono avviare**.

Al fine di selezionare la soluzione più idonea nell'ambito del modello cloud, è opportuno applicare la **preferenza SaaS first**, ovvero indirizzare la propria scelta sui servizi SaaS già presenti e attivi nel market-place cloud, se conformi alle necessità dell'amministrazione.

La scelta dei servizi SaaS consente di beneficiare in pieno dei vantaggi offerti dal paradigma cloud e **di ridurre drasticamente costi e sforzi amministrativi,** in quanto non necessita di attività tecnica di gestione e sviluppo dedicato, cosa necessaria invece con l'acquisizione di servizi IaaS e PaaS, che è preferibile prendere in considerazione in seconda istanza.

I vantaggi della migrazione dei dati nel cloud

Rispetto alle tradizionali soluzioni hardware, il modello cloud introduce vantaggi significativi, che consentono di :

1. effettuare in maniera continua gli **aggiornamenti** dell'infrastruttura e delle applicazioni
   Le soluzioni IT commerciali o auto-sviluppate in locale richiedono finanziamenti, impegno e pianificazione per poter essere aggiornate costantemente. Il supporto e gli aggiornamenti sono attività costose e complicate da gestire ed è molto difficile per qualsiasi organizzazione tenere il passo con la costante richiesta di aggiornamenti e patch di sicurezza. Se non si dispone di sufficienti finanziamenti, le infrastrutture della PA non riescono perciò ad essere adeguatamente aggiornate. I servizi di cloud pubblico, invece, vengono generalmente aggiornati, migliorati e mantenuti durante tutto il loro ciclo di vita dal fornitore e il tutto è incluso nei costi del servizio. Chi acquista questi servizi non ha bisogno di aggiornare i sistemi operativi dei server, acquistare hardware, contrattualizzare personale esterno, pianificare le operazioni o spostare i dati per ottenere i benefici della tecnologia più recente.
2. usufruire delle applicazioni **da qualsiasi dispositivo in qualsiasi luogo** tramite l'accesso internet
3. avere **maggiore flessibilità** nel provare nuovi servizi o apportare modifiche con costi minimi
4. ridurre i rischi legati alla **gestione della sicurezza** (fisica e logica) delle infrastrutture IT
   Amministrare le infrastrutture IT comporta responsabilità certamente di tipo economico-amministrativo ma soprattutto di sicurezza e di protezione dei dati personali. Le recenti normative in materia di privacy e di sicurezza informatica impongono infatti anche alle Pubbliche Amministrazioni l'adozione di misure tecniche e organizzative adeguate a garantire la sicurezza del trattamento dei dati. Il modello cloud viene incontro alle esigenze delle P.A. anche sotto questo aspetto, facilitando la separazione delle problematiche di sicurezza per l'infrastruttura fisica, per il software e per la gestione logica delle applicazioni. Il cloud evita alla P.A. i costi legati all'adeguamento dell'impianto anti-incendio, ai sistemi di raffreddamento, alla manutenzione dell'hardware e al presidio fisico dei locali. Inoltre, le applicazioni cloud sono in grado di mettere a disposizione dell'amministratore strumenti di auditing e controllo delle informazioni che consentono interventi puntuali, all'insorgere di eventuali problemi. Certamente non basta dotarsi di soluzioni cloud per assicurare privacy ai propri utenti e sicurezza delle infrastrutture e servizi IT, bensì serve un processo continuo di vigilanza e controllo che, fin dalla prima fase di progettazione dei servizi, agisca trasversalmente su tutte le aree di interesse, e che sia costantemente aggiornato rispetto allo stato dell'arte delle principali misure di sicurezza.
5. avere **importanti economie** nell'utilizzo del software
   È infatti consentito pagare le risorse come servizi in base al consumo ("pay per use"), evitando gli investimenti iniziali nell'infrastruttura e i costi legati alle licenze di utilizzo.
6. **ridurre i costi complessivi** collegati alla location dei data center, come affitti, consumi elettrici e personale non ICT.
   Le applicazioni e le infrastrutture cloud consentono di gestire la crescita e l'aggiornamento tecnologico in maniera dinamica e con costi contenuti. Le applicazioni basate su hardware in locale (data center) richiedono un piano di investimenti che deve tener conto dei prezzi riferiti

al momento della sottoscrizione del contratto e di alcuni anni di manutenzione e supporto. I costi complessivi di questo modello di gestione in house, come le licenze, l'energia elettrica, la potenza di calcolo, la manodopera e così via, raramente diminuiscono nel corso della durata del servizio.

I servizi cloud, invece, tendono ad essere sempre più economici proprio per le dinamiche di mercato. La pressione competitiva, l'hardware migliorato e l'aumento dei tassi di utilizzo stanno riducendo progressivamente i costi delle applicazioni SaaS e delle infrastrutture virtuali (IaaS). Infatti, per una vasta gamma di servizi e sistemi, che vanno dalla sicurezza informatica alla produttività e all'archiviazione, le soluzioni cloud rappresentano spesso la soluzione più vantaggiosa disponibile sul mercato e, in alcuni casi, anche la più utilizzata.

A differenza delle soluzioni on-premise (in sede), i servizi cloud sono davvero elastici: le risorse di calcolo, storage o rete possono essere utilizzate solo quando richiesto e dismesse quando non sono più necessarie, eliminando così tutta la complessità nella pianificazione della capacità dell'infrastruttura IT.

Infine, il modello cloud non richiede alcun investimento a lungo termine e non comporta quello spreco di risorse determinato dal sottoutilizzo della capacità.

Il data center della Città metropolitana di Milano

Attualmente il Sistema Informativo della Città metropolitana è ospitato su un'infrastruttura hardware in locali di proprietà, nelle sedi di viale Piceno e via Soderini, acquistata nel 2012 con il capitolato speciale d'appalto per la fornitura di sistemi storage e di una soluzione di continuità operativa e disaster recovery.

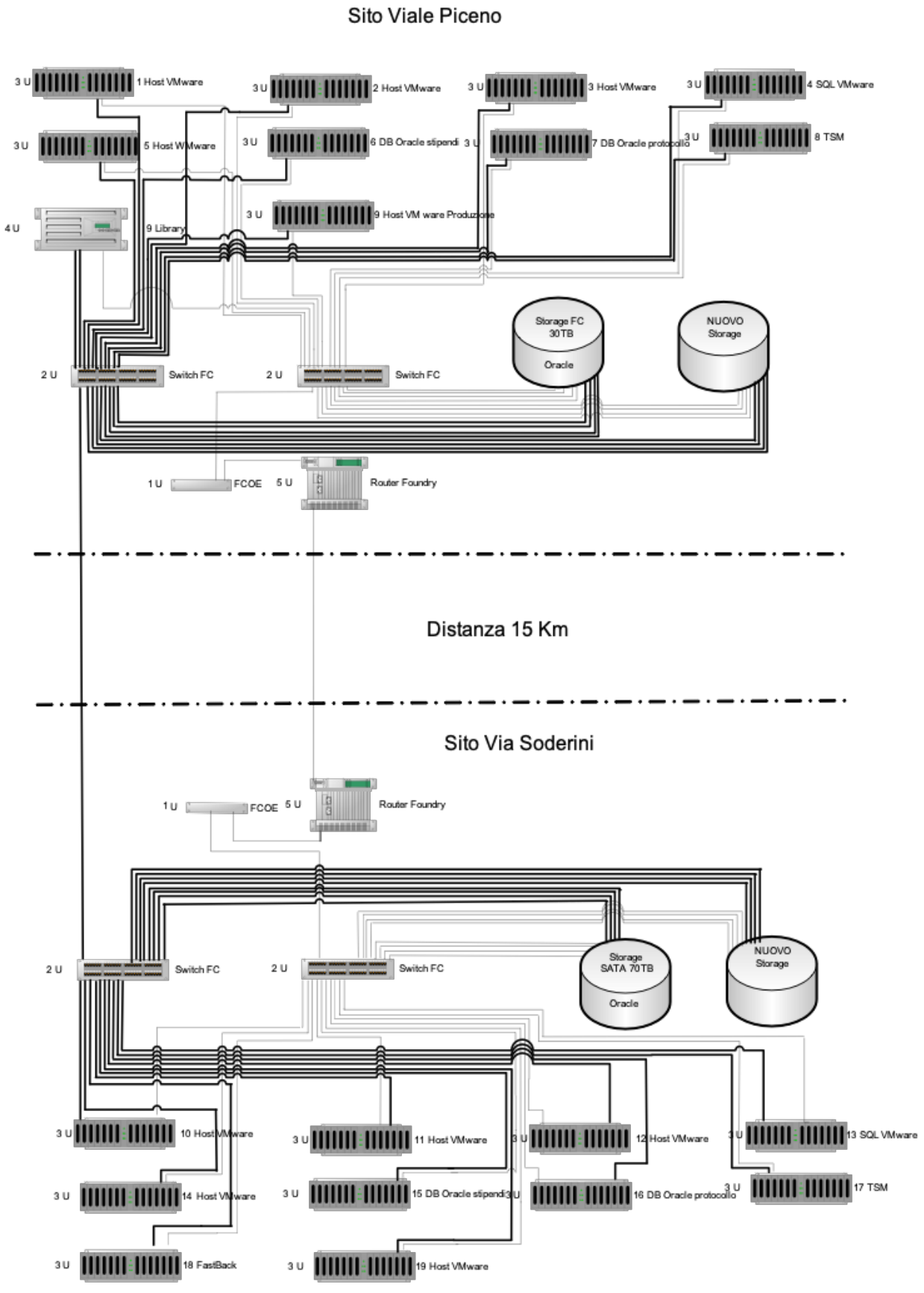
Il data center è strutturato su due siti con una configurazione di disaster recovery: il sito principale si trova in viale Piceno 60 mentre il sito secondario in via Soderini 24, qui sono replicati tutti i servizi erogati dal sito primario ed è presente lo storage del sistema di backup .

L'acquisto dell'infrastruttura tecnologica ha incluso, per una durata di cinque anni, i servizi di manutenzione e supporto da parte di fornitori altamente specializzati, che hanno garantito il pronto intervento in caso di guasti e malfunzionamenti, assicurando la continuità del servizio del patrimonio informativo dell'Ente.

Il data center è composto da un sistema virtuale VMWare operativo su 6 host fisici e un data store di 50 TB dove risiedono 120 server fisici. Gli apparati hardware che ospitano i dati e i sistemi virtuali sono due Storage SUN Oracle dell'età di 10 anni e due di EMC dell'età di 5 anni.

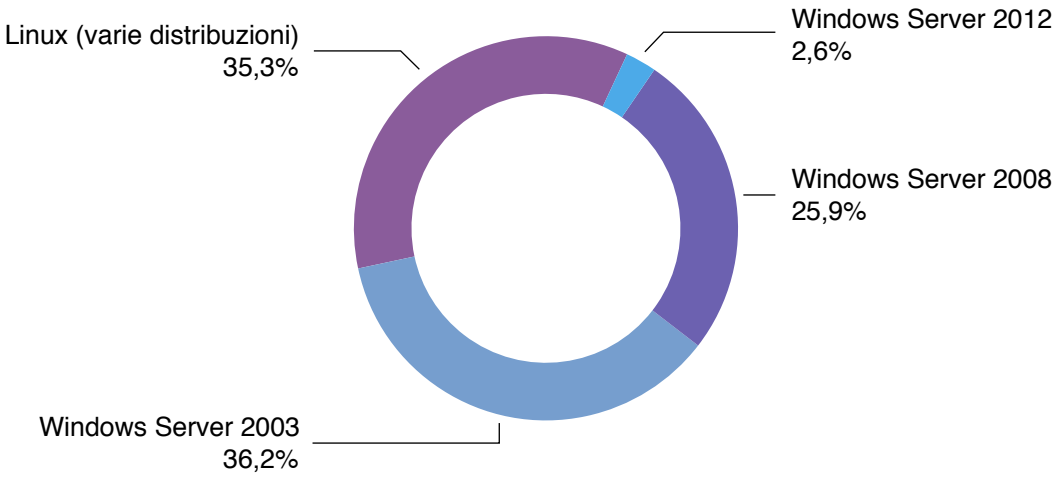
Gli **Storage SUN**, attualmente ancora in funzione, sono nella cosiddetta condizione **"end of life, end of support"**, cioè non sono più coperti dalla garanzia e dal supporto sistemistico da parte del produttore e, a fronte di guasti, non sono garantite le sostituzioni delle componenti di ricambio.

Rappresentazione dell'attuale infrastruttura IT



I sistemi operativi

I sistemi operativi dei server che ospitano i vari ambienti applicativi, cioè la posta elettronica, il protocollo informatico, la contabilità, il trattamento economico, i server web pubblici (Internet), i server web privati (Intranet) e i database server, sono suddivisi come rappresentato nel grafico.



I sistemi operativi Windows Server 2003 sono in condizione di end of life, end of support. Questi sistemi operativi attualmente ospitano la posta elettronica, la totalità dei SQL server e i database Oracle, ad eccezione di quello della contabilità. È perciò urgente l'aggiornamento, per allinearsi alle disposizioni normative in termini di sicurezza.

Il cloud della Città metropolitana di Milano

Considerate le premesse e le indicazioni del Piano Triennale, risulta **inattuabile, oltre che costoso, prevedere un piano di refresh tecnologico** atto alla sostituzione degli Storage, dei server virtuali, dei sistemi di backup e di quelli preposti al disaster recovery.

Il Piano triennale per l'informatica nella PA 2019 - 2019 dice che non possono essere sostenute spese relative alla costituzione o all'evoluzione di data center non eletti a Poli Strategici Nazionali.

In considerazione di tutto ciò, l'Ente ha ritenuto di aderire al **Contratto Quadro SPC Cloud Lotto 1**, stipulato tra Consip ed il Raggruppamento Temporaneo d'Impresa (RTI), rappresentato dalla capogruppo Telecom Italia S.p.A.

Il Contratto Quadro SPC Cloud Lotto 1 ha una **durata di 36 mesi** ed è stata prevista la possibilità di richiedere una proroga temporale del Contratto Esecutivo, al solo fine di consentire la migrazione dei servizi ad un nuovo fornitore al termine del Contratto Quadro, qualora l'aggiudicazione del nuovo fornitore subentrante non sia intervenuta entro i tre mesi antecedenti la scadenza del presente Contratto Quadro.

Il passaggio nel cloud prevede i seguenti step:

- **valutazione iniziale:** assessment infrastrutturale e delle applicazioni utilizzate;
- **progettazione del processo di migrazione:** insieme all'azienda fornitrice del servizio è stato progettato l'intero processo di migrazione secondo un piano di lavoro dettagliato;
- **esecuzione della migrazione:** l'esecuzione della migrazione è la parte operativa di tutto il processo. È stato costituito un centro operativo di comando e controllo della migrazione, in cui devono essere presenti oltre al fornitore anche rappresentanti del personale tecnico della Città metropolitana. Questa è una fase ricorsiva per ogni applicazione e incrementale, di modo che si possa verificare che le applicazioni funzionino correttamente, una volta migrate. Al termine di questa fase l'Ente disporrà di nuovi servizi IT in ambiente cloud;
- **revisione della sicurezza:** le unità di esecuzione effettueranno la revisione della sicurezza applicativa e dell'infrastruttura, indicando le criticità per ogni ambito e avvalendosi di soggetti terzi per una migliore e più indipendente analisi del rischio. La revisione prevede l'applicazione delle misure minime di sicurezza ICT per le Pubbliche Amministrazioni, così come emanate dall'AgID. Nell'ambito della web application security, è necessario applicare i controlli legati alle vulnerabilità più comuni;
- **formazione:** è prevista una fase di formazione ai referenti tecnici dell'amministrazione sui servizi cloud (IaaS, PaaS, SaaS) e sul loro utilizzo.

Il costo del servizio per tre anni di cloud computing e dei servizi di cloud enabling (cioè di sviluppo sul cloud) ammonta a circa €300.000 (IVA inclusa).

Il servizio in cloud di posta elettronica è escluso dal Contratto Quadro SPC Cloud Lotto 1.

La convenzione prevede l'utilizzo di un **Virtual Data Center** che consentirà un maggior grado di flessibilità rispetto a quello fornito da un insieme di virtual machine standard. Il Virtual Data Center dovrà interagire con il dominio di rete dell'Amministrazione e con le macchine virtuali o fisiche non ancora migrate. Il passaggio al cloud sarà graduale, per consentire il contestuale aggiornamento delle piattaforme ormai obsolete, non conforme con gli attuali requisiti di sicurezza.

Il Progetto dei Fabbisogni per la fornitura di servizi di cloud Computing prevede l'utilizzo dei seguenti componenti:

- Infrastructure as a Service (IaaS) per la componente di Virtual Data Center
- Platform as a Service (PaaS Oracle) per la componente dabase Oracle
- Platform as a Service (PaaS Zabbix) per la componente di monitoraggio della rete di server Zabbix
- Backup as a Service (BaaS) per il salvataggio dell'intero patrimonio informativo

L'ambiente virtuale messo a disposizione della Città metropolitana di Milano è predisposto su una infrastruttura hardware (fisica) comune e condivisa tra diverse Amministrazioni Pubbliche: per ogni Amministrazione viene ritagliata una porzione logica delle risorse infrastrutturali (rete, sicurezza, server farm e storage) ed è garantita la separazione logica degli ambienti assegnati a ciascuna.

Per eliminare il rischio di interruzioni del servizio, dovuti a guasti hardware, **la piattaforma di virtualizzazione utilizzata nella Convenzione si chiama OpenStack, una tecnologia open source** completamente diskless. Questo significa che i server non includono alcun disco locale e i

dati sono memorizzati esclusivamente in una Storage Area Network (SAN) ingegnerizzata per i servizi di Storage.

La SAN (Storage Area Network) implementata nei Data Center garantisce l'assenza di Single Point Of Failure, il monitoraggio preventivo degli errori per limitare i guasti di sistema, la possibilità di sostituire e/o aggiungere componenti hardware e aggiornare il firmware minimizzando i fermi del sistema.

La soluzione assicura:

- **separazione fisica** delle infrastrutture;
- **separazione logica** delle risorse;
- **alta affidabilità**, attraverso componenti fisici ridondati, dischi configurati in RAID5 e dischi hot-spare così da garantire continuità anche in caso di problemi hardware;
- **scalabilità**, vale a dire che l'infrastruttura è in grado di supportare richieste di workload addizionale, sia allocando nuove risorse (scalabilità orizzontale) sia incrementando le capacità delle risorse già disponibili (scalabilità verticale).

Servizi e utilità disponibili

1. Virtual Data Center

Un Virtual Data Center è inteso come una struttura personalizzata e flessibile di macchine virtuali, costruite ad hoc a partire da quantità variabili di risorse elementari (CPU, RAM, ecc …). Con un Virtual Data Center si possono creare e gestire in autonomia le proprie macchine virtuali, partendo dalle singole risorse. Questo consente di avere a disposizione e riservare risorse computazionali e di organizzarle autonomamente.

Nel cloud scelto dalla Città metropolitana, sono utilizzate le migliori tecnologie di virtualizzazione attualmente presenti sul mercato che garantiscono una separazione logica dei sistemi operativi, impedendo la visibilità dei dati tra Amministrazioni che utilizzano la stessa piattaforma condivisa. Il sistema di virtualizzazione OpenStack alloca le risorse in maniera intelligente isolando completamente le macchine virtuali dal sottostante layer fisico. Pertanto una singola macchina virtuale non può utilizzare tutte le risorse o causare il crash dell'host fisico. La tecnologia OpenStack fornisce uno strato software che si pone tra l'hardware del sistema ed il sistema operativo, in modo tale da costituire ambienti fisici virtuali completi e separati l'uno dall'altro, definiti "virtual machine". Questi sono a tutti gli effetti visti come 'n' piattaforme x86 coesistenti su un unico sistema fisico, realizzando pertanto una sorta di "partizionamento" logico. La singola applicazione può operare nella "virtual machine" assegnata, in modo completamente indipendente dalle altre, nelle rispettive distinte partizioni. La logica di virtualizzazione consente l'accesso diretto alle risorse hardware.

Il risultato è avere più applicazioni che operano su uno stesso sistema fisico, in ambienti completamente separati, con un utilizzo delle risorse ottimizzato in quanto la condivisione consente di creare combinazioni di applicazioni con profili di carico diversi, tali da massimizzare il tempo di utilizzo della CPU.

La gestione dell'infrastruttura fisica è a totale carico del fornitore (manutenzione hardware e software). La gestione dell'ambiente virtuale, invece, è a carico dei sistemisti della Città metropolitana di Milano che, attraverso strumenti web-based, gestiranno la configurazione, la gestione operativa e il monitoraggio dell'intera infrastruttura.

2. Messa in sicurezza dei sistemi (c.d. hardening)

I sistemi migrati nel cloud, prima di entrare in produzione, sono messi in sicurezza (hardening). L'hardening è l'insieme delle operazioni specifiche di configurazione di un dato sistema informatico (e dei suoi relativi componenti) che mirano a minimizzare l'impatto di possibili attacchi informatici che sfruttano la vulnerabilità. Questo è reso possibile attraverso l'attuazione di tecniche che permettono di "irrobustire" una piattaforma, considerando tutti gli aspetti di sicurezza del sistema informatico, dall'autenticazione degli utenti, fino all'integrità dei dati e dei file system, passando per una configurazione congrua del sistema, allo scopo di eliminare le vulnerabilità comuni.

Al fine di massimizzare la sicurezza delle piattaforme si avvieranno i processi di hardening post-installazione e di hardening periodico.

3. Monitoraggio infrastruttura IT

Attraverso la soluzione open source Zabbix, sarà effettuata la verifica costante del funzionamento e delle prestazioni dei sistemi hardware, del sistema operativo e del software di middleware, con l'intento di rilevare e segnalare, in maniera proattiva, possibili condizioni che potrebbero determinare il degrado o il blocco dei servizi erogati.

La soluzione di monitoraggio Zabbix è in grado di segnalare: il superamento di determinate soglie sull'utilizzo delle risorse di CPU, memoria, spazio disco;

- la presenza, l'assenza e la numerosità di determinati processi running sul sistema;
- la presenza, l'assenza e lo stato di determinati servizi attivi (applicabile per Windows);
- l'analisi dei logfile per determinare situazioni di errore;
- l'analisi degli elementi dell'Event Viewer di Windows.

L'architettura di prodotto prevede una componente manager centralizzata (Zabbix Manager) ed una componente distribuita (Zabbix Agent), attiva sui sistemi target. Nella piattaforma integrata adottata dal RTI il Manager Zabbix inoltra le segnalazioni verso la piattaforma di Event Management centralizzata di back end.

4. Backup as a Service

L'attivazione dei servizi cloud IaaS e PaaS prevede l'implementazione del backup dell'insieme dei sistemi attivi. Le policy di backup applicate per tale servizio prevedono:

- backup incrementale giornaliero;
- backup full settimanale;
- retention massima prevista di 90 giorni.

Il tipo di ripristino assicurato per il ripristino dei dati è il seguente:

- viene effettuato il backup dell'intero filesystem della Macchina Virtuale (VM);
- viene garantito il ripristino della VM all'ultimo backup effettuato, secondo le policy sopra definite;
- viene garantita una consistenza di tipo "crash-consistency";
- è permessa una gestione puntuale per il ripristino di singoli file.

5. Sistema di posta elettronica

Anche il servizio di posta elettronica necessita di un refresh tecnologico che permetterà anche grandi risparmi in termini economici. Dopo un'attenta valutazione economica, si è deciso di escludere l'aggiornamento dell'attuale sistema di posta elettronica on-premise (in locale) optando per il **servizio in cloud tramite l'adesione alla Convenzione Consip PEL** (Posta Elettronica).

Il costo di questa soluzione in cloud è di circa € 30.000 l'anno (IVA inclusa).

Il servizio di Posta Elettronica (PEL) consentirà ai dipendenti dell'Ente di comunicare, tramite messaggi asincroni, sia con l'interno sia con l'esterno dell'Amministrazione. Il servizio sarà erogato attraverso l'infrastruttura centralizzata e resa disponibile dal fornitore presso il proprio centro servizi. Tale infrastruttura sarà condivisa dalle Pubbliche Amministrazioni contraenti.

Il servizio di PEL includerà anche i servizi di sicurezza: anti spam, anti virus, anti phishing, anti malware, anti ransomware, backup/restore dei dati, oltre all'assistenza per l'utente nel normale utilizzo del servizio e nella fase di migrazione.

Il servizio di posta elettronica, inoltre, consentirà di:

- mantenere gli attuali nomi di dominio continuando così ad utilizzare il proprio indirizzo e-mail;
- colloquiare tramite protocolli standard (per esempio POP3S, IMAPS e SMTP) con eventuali altre organizzazioni di posta interne all'Amministrazione su connessione sicura (protocollo TLS);
- gestire centralmente le liste di distribuzione;
- disporre di un servizio di salvataggio dei dati di posta elettronica su un sito diverso da quello dove risiede l'infrastruttura, così da garantire, a fronte di un evento di inagibilità del sito (ad esempio per incendio, allagamento, ecc …) l'integrità dei dati alla ripartenza del servizio, aggiornati almeno alle 24 ore precedenti l'evento;
- accedere ai messaggi (e-mail, rubrica e agenda) tramite dispositivi mobili, come smartphone e tablet con diversi sistemi operativi (Android, IOS, Windows Phone);
- accedere alla propria casella postale, utilizzando l'interfaccia webmail da qualsiasi postazione di lavoro.

Costi e benefici dello spostamento dei sistemi sul cloud

I maggiori costi sostenuti per la gestione di un sistema IT on-premise (in locale) sono:

- spesa in conto capitale necessaria all'aggiornamento tecnologico delle infrastrutture;
- spese per il mantenimento dei Data Center:
  - energia elettrica,
  - manutenzioni degli impianti di condizionamento,
  - manutenzione dei gruppi di continuità e dei gruppi elettrogeni;
- spese per l'occupazione degli spazi fisici dei Data Center;
- spese per il personale per i servizi di presidio notturno e reperibilità;
- spese per il mantenimento della sicurezza fisica del Data Center: impianto anti-intrusione e impianto antincendio.

Con il passaggio al cloud si otterrà progressivamente un innalzamento degli standard di sicurezza e, nel medio/lungo periodo, si avrà un ulteriore significativo risparmio dovuto al recupero degli spazi, alla diminuzione dei consumi elettrici e delle spese di mantenimento dell'infrastruttura fisica. Si potrà rispondere alle esigenze dell'utenza interna ed esterna con il personale esistente, adeguatamente formato nelle nuove competenze.

L'hosting in cloud, infatti, garantisce il costante aggiornamento delle attrezzature e di tutti i supporti, senza costi specifici per il rinnovamento delle infrastrutture, e introduce un ulteriore risparmio perché le policy presenti e future, richieste dalla normativa europea sulla sicurezza logica dei dati, sono implicitamente previste.

Verranno inoltre evitati i costi legati all'adeguamento dell'impianto antincendio, alla sicurezza fisica e al presidio.

Glossario

API (Application Programming Interfaces)
Strumenti di programmazione messi a disposizione degli sviluppatori per facilitare la realizzazione di applicazioni

Anti spam
Software che permette di bloccare l'inoltro indiscriminato di e-mail, spesso a carattere pubblicitario e/o commerciale. Utilizzato dai server di posta elettronica

Anti virus
Software per bloccare, controllare ed eventualmente rimuovere altro software malevolo

Anti phishing
Software per contrastare le frodi telematiche

Anti malware
Abbreviazione per malicious software, generalmente software dannoso per il computer o per le informazioni che si trovano in esso

Anti ransomware
Software per contrastare un tipo di malware che “sequestra” i dati al fine di ottenere un riscatto, in genere i dati sul computer vengono criptati

Backup/Restore
Tecniche informatiche di salvataggio (backup) e ripristino dei dati (restore) solitamente a seguito di un malfunzionamento o ad un attacco informatico

Blog
Pagina internet personale, aperta ai commenti dei lettori

Chat
Scambio di messaggi scritti che si svolge in tempo reale tra due o più utenti di Internet

Data Center o Server Farm
Uno spazio fisico composto da server, storage, apparati di rete, cablaggi, armadi e sistemi di condizionamento

Disaster Recovery
Nell'ambito della sicurezza informatica, si intende l'insieme delle misure tecnologiche e logistico/organizzative atte a ripristinare sistemi, dati e infrastrutture necessarie all'erogazione dei servizi

Firmware
Insieme delle istruzioni e delle applicazioni presenti permanentemente nella memoria di un sistema e che non possono essere modificate dall’utente

Forum
Sistema di comunicazione asincrono dedicato alla discussione su un argomenti specifici

Hardening
Insieme di operazioni specifiche di configurazione di un dato sistema informatico (e dei suoi relativi componenti) che mirano a minimizzare l'impatto di possibili attacchi informatici che sfruttano vulnerabilità

HTTP
HyperText Transfer Protocol, protocollo per il trasferimento di documenti ipertestuali, usato per la navigazione in Internet

HTML
Hyper Text Markup Language linguaggio di markup per ipertesti utilizzato per la creazione di documenti destinati al web

ICT
Le Tecnologie dell'Informazione e della Comunicazione o ICT(acronimo di Information and Communications Technology) sono l'insieme dei metodi e delle tecniche utilizzate nella trasmissione, ricezione ed elaborazione di dati e informazioni (tecnologie digitali comprese)

IoT
Internet of Things insieme di tecnologie che permettono di collegare a Internet qualunque tipo di oggetto

Middleware
Insieme di programmi informatici che fungono da intermediari tra diverse applicazioni e componenti software

Patch
Porzione di software progettata per aggiornare e migliorare un programma

Server
In una rete di computer, è una macchina che fornisce un servizio agli altri elaboratori collegati

Storage
Dispositivi hardware, supporti per la memorizzazione, infrastrutture e software dedicati alla memorizzazione non volatile di grandi quantità di informazioni in formato elettronico

SAN (Storage Area Network)
Rete o parte di una rete ad alta velocità costituita esclusivamente da dispositivi di memorizzazione di massa

Single Point Of Failure
Letteralmente “singolo punto di vulnerabilità”, in un sistema informatico è un aparte del sistema, hardware o software, il cui malfunzionamento può portare ad anomalie o addirittura alla cessazione del servizio da parte del sistema

Software on-premise
in contrapposizione al software come servizio (SaaS), è un software che si installa ed esegue su macchina internet locale

Wiki
Sito internet che permette la creazione e la modifica collaborativa dei contenuti

Virtualizzazione
Creazione di una versione virtuale (software) di una risorsa informatica fisica (computer, apparati ecc …). Il sistema di visualizzazione è composto da tanti server omogenei, collegati ad uno storage in alta affidabilità