#CANTIERI DELLA PA DIGITALE

TRASFORMAZIONE DIGITALE

CLOUD TRANSFORMATION | REPORT 2020

FPA

DIGITAL 360

La redazione del report 2020 del **Cantiere Trasformazione Digitale - Cloud Transformation** è stata curata da un gruppo di lavoro coordinato da Eleonora Bove (FPA) e la supervisione scientifica di Claudio Franzoni (P4I - Partners4Innovation).

Per l'importante e fattivo contributo dato alla redazione del presente report si ringraziano: Anna Sappa (INAIL), Antonio Tommaso (INAIL), Leandro Gelasi (Corte dei conti) e Vito Baglio (CSI Piemonte).

Si ringraziano, inoltre, per il rilevante contributo dato al lavoro del tavolo: Marina Apicella (Samsung Electronics Italia), Massimo Crubellati (Cast), Francesco Lombardo (DXC Technology), Nicola Mangia (DXC Technology), Marco Romoli (Cast), Francesco Seminaroti (Samsung Electronics Italia) e Michele Slocovich (Cast).

Alla redazione del presente report hanno contribuito anche: Martina Leoni (P4I - Partners4Innovation) e Chiara Di Natale (P4I - Partners4Innovation).

I contenuti del report rappresentano il risultato del lavoro di rielaborazione degli spunti emersi nel corso del dibattito tra tutti i protagonisti del Cantiere.

CANTIERI DELLA PA DIGITALE

Cantiere Trasformazione Digitale - Cloud Transformation - Report 2020
Edizioni ForumPA – ISBN 9788897169666

I contenuti sono rilasciati nei termini della licenza

Attribuzione - Non commerciale - Condividi allo stesso modo 3.0 Italia (CC BY-NC-SA 3.0 IT)

in collaborazione con

partnership scientifica

Cloud Transformation

INDICE

1. Il Cantiere Trasformazione Digitale

Il Cantiere Trasformazione Digitale è il nuovo laboratorio di FPA dedicato ai processi di attuazione della strategia italiana sulla PA digitale. Il Cantiere si è articolato in tre focus tematici: cloud, sicurezza informatica e servizi digitali. Partner istituzionale di FPA è la Direzione Centrale Organizzazione Digitale di INAIL (DCOD).

Il Cantiere Trasformazione Digitale si propone di disegnare i percorsi di razionalizzazione ed evoluzione organizzativa e tecnologica dell'amministrazione italiana, alla luce delle previsioni del Piano triennale per l'ICT.

Il Cantiere vuole favorire il mutuo apprendimento tra i partecipanti, attraverso metodologie di lavoro collaborativo improntate all'action learning, che favoriscano lo sviluppo delle persone e delle organizzazioni aderenti attraverso l'analisi di casi concreti, inerenti ai temi individuati.

L'edizione 2020 del Cantiere Trasformazione Digitale è stata realizzata in collaborazione con **Aruba Enterprise, Akamai, Cast, DXC Technology, Samsung Electronics Italia.**

1.1 Cloud Transformation

Nell'ambito del Cantiere Trasformazione Digitale, è il tavolo di lavoro tematico dedicato al percorso di adozione di tecnologie e piattaforme cloud, così come indicato nel Piano Triennale per l'informatica nella Pubblica amministrazione e nei documenti di indirizzo AgID. L'obiettivo del tavolo è stato quello di definire un percorso di Cloud Transformation che ricalcasse le tre fasi principali della trasformazione: **readiness, design e migration**. Partner tecnologici di questo specifico gruppo di lavoro: **Cast, DXC Technology e Samsung Electronics Italia.**

1.2 Nota metodologica

Il tavolo di lavoro dedicato alla Cloud Transformation delle pubbliche amministrazioni si è riunito in occasione di tre workshop digitali, nel corso del 2020, volti al confronto e al lavoro collaborativo. Questi appuntamenti sono stati intervallati da sessioni on line di approfondimento, per cui è stata prevista la partecipazione di un numero ristretto di partecipanti al tavolo.

FPA ha sviluppato una metodologia di lavoro ad hoc per il Cantiere Trasformazione Digitale, secondo i principi dell'action learning.

Ad ogni workshop i partecipanti sono stati divisi in piccoli gruppi, generalmente eterogenei. A ogni gruppo sono stati dati degli obiettivi di lavoro da raggiungere attraverso il confronto e la discussione. Ad agevolare il raggiungimento degli obiettivi, la presenza in ogni gruppo di un facilitatore professionista di FPA.

Ai lavori hanno preso parte più di trenta amministrazioni, nella fattispecie i rappresentanti delle Direzioni IT (CIO) e ai Responsabili per la transizione al digitale (art. 17 CAD) delle grandi amministrazioni centrali (Ministeri, Agenzie fiscali, Istituti di Previdenza sociale, Autorità indipendenti, Organi costituzionali, ecc.) e delle Regioni, nonché i rappresentanti delle grandi aziende ICT del panorama nazionale ed internazionale.

Il presente documento nasce da questo lavoro collaborativo tra i partecipanti e riassume tutti gli spunti, i suggerimenti e le best practices emerse nel corso di questo percorso di lavoro.

1.3 Il Journey della Cloud Transformation

Il documento illustra un possibile percorso di Cloud Transformation per la Pubblica Amministrazione organizzato in tre fasi: strategia, progettazione e piano operativo di migrazione.

1.3.1 Strategia

Definizione della strategia della migrazione attraverso l'assessment dei servizi IT in uso, la creazione del modello di riferimento e della modalità di migrazione, la definizione di un macro-piano di intervento, la trasformazione della governance e la valutazione dei costi e dei benefici economico/organizzativi derivati dalla trasformazione

1.3.2 Progettazione

Costruzione di un progetto e di un capitolato tecnico per la richiesta delle offerte ai fornitori e/o per la definizione del piano dei fabbisogni, comprensivo della trasformazione della governance ICT e della misura dei servizi erogati.

1.3.3 Piano Operativo di Migrazione

Un set completo di Linee Guida per la creazione del piano operativo di migrazione, comprensivo delle tematiche di collaudo, realizzazione della Cybersecurity, monitoraggio dei servizi e formazione del personale.

2. Il Cloud nella PA

2.1 Le Linee guida AgID nella Cloud Transformation

Da diversi anni AgID opera in modo molto attivo per la promozione e l'attivazione della Cloud Transformation per la Pubblica Amministrazione, attraverso modelli, raccomandazioni, circolari e strumenti, che definiscono in modo chiaro la strategia Cloud

La strategia indicata da AgID si può riassumere in tre elementi principali definiti e ripresi direttamente da https://cloud.italia.it

- il principio **Cloud First** secondo il quale le PA devono, in via prioritaria, adottare il paradigma cloud (in particolare i servizi SaaS) prima di qualsiasi altra opzione tecnologica per la definizione di nuovi progetti e per la progettazione dei nuovi servizi nell'ambito di nuove iniziative da avviare;

- il modello **Cloud della PA**, il modello strategico che si compone di infrastrutture e servizi qualificati da AgID sulla base di un insieme di requisiti volti a garantire elevati standard di qualità per la PA;

- Il **programma di abilitazione al cloud** (cloud enablement program), l'insieme di attività, risorse, metodologie da mettere in campo per rendere le pubbliche amministrazioni capaci di migrare e mantenere in efficienza i propri servizi informatici (infrastrutture e applicazioni) all'interno del modello Cloud della PA.

A seguito del Censimento del Patrimonio ICT della PA completato nel 2019 su quasi mille amministrazioni per un totale di un campione altamente significativo di 1252 data center censiti, è stata definita la strategia di razionalizzazione, illustrata nel Capitolo 4 del Piano Triennale per l'Informatica nella Pubblica Amministrazione 2020-2022.

La strategia di razionalizzazione dei data center definita nel Piano Triennale prevede la classificazione in due categorie nominate come segue:

A. Infrastrutture candidabili ad essere utilizzate da parte dei "PSN" e "Gruppo A" (di cui fanno parte 35 candidabili all'utilizzo di PSN e 27 Gruppo A)

B. I restanti data center censiti (1190)

Come si evince dal censimento e dalla successiva classificazione "**molte infrastrutture della PA risultano prive dei requisiti di sicurezza e di affidabilità necessari** e, inoltre, sono carenti sotto il profilo strutturale e organizzativo. Ciò espone il Paese a numerosi rischi tra cui quello di interruzione o indisponibilità dei servizi e quello di attacchi cyber con, conseguente, accesso illegittimo da parte di terzi a dati (o flussi di dati) particolarmente sensibili o perdita e alterazione degli stessi dati" (fonte: Piano Triennale per l'Informatica nella Pubblica Amministrazione 2020-2022)

Il Piano Triennale 2020-2022 indica in modo chiaro il percorso di razionalizzazione per i data center classificati "B", che dovranno migrare i servizi verso una infrastruttura in grado di garantire i requisiti di affidabilità, sicurezza e resilienza, scegliendo fra le infrastrutture del PSN e le infrastrutture ed i servizi Cloud certificati da AgID.

Il principio di razionalizzazione sopra espresso si applica in modo simmetrico alle Amministrazioni Centrali e alle Amministrazioni Locali che potranno quindi migrare i propri data center sia con soluzioni certificate AgID che stringere accordi per consolidare i propri servizi all'interno di data center classificati "A" da AgID.

Per aiutare e facilitare le Amministrazioni nel processo di migrazione dei data center verso il Cloud, AgID ha reso disponibili due importanti strumenti:

2.1 Cloud Marketplace AgID

La piattaforma che espone i servizi e le infrastrutture qualificate da AgID, attraverso un processo che garantisce alle amministrazioni di poter acquisire servizi perfettamente aderenti ai requisiti ed alle normative.

Nel Cloud Marketplace di AgID sono esposti i Servizi IaaS, SaaS e PaaS certificati ed il Registro Pubblico dei Cloud Service Provider Certificati. Il catalogo è in continuo e costante aggiornamento. Alla stesura del presente documento sono certificate 469 soluzioni SaaS, 176 soluzioni PaaS, 115 soluzioni IaaS.
Fornisce inoltre il registro dei Cloud Service Provider di mercato che le Società In House che sono certificate come Cloud Service Provider.

Nelle schede tecniche viene fornito anche il prezzo di riferimento del servizio base a scopo indicativo e per facilitare la ricognizione di mercato che, come si vedrà nei capitoli successivi, è una delle attività previste nella costruzione del piano di migrazione.

Il Cloud Marketplace di AgID non è un metodo di procurement ma un registro di soluzioni e servizi certificati. Come citato dal sito del "Per le modalità di acquisizione da soggetti privati dei servizi Cloud qualificati, occorre fare riferimento alla normativa vigente in tema di *procurement delle pubbliche amministrazioni* (Codice degli appalti) e agli strumenti delle centrali di committenza" indicati in un successivo paragrafo.

Al fine di ulteriormente facilitare le amministrazioni nel procurement dei servizi e delle infrastrutture necessarie alla migrazione, a complemento di quanto sopra indicato è stata pubblicata da Consip la "Gara a procedura aperta per l'affidamento di un Accordo Quadro per la fornitura di servizi cloud IaaS e PaaS in un modello di erogazione pubblico nonché per la prestazione di servizi connessi, servizi professionali di supporto all'adozione del cloud, servizi professionali tecnici per le Pubbliche Amministrazioni" (link) che verrà ulteriormente approfondita nei paragrafi successivi.

2.2 Programma di abilitazione al Cloud

Sviluppato in modo congiunto dal Dipartimento per la Trasformazione Digitale e da AgID, il programma definisce l'insieme delle attività e delle risorse per consentire alle amministrazioni di essere capaci di migrare e gestire i propri servizi IT con il Cloud.

Tutto il materiale indicato nel presente paragrafo è disponibile su https://cloud.italia.it/it/cloud-enablement/

Il programma comprende:

- un kit di metodologie, strumenti, modello, best practices e un percorso adattabile alle proprie esigenze;
- un framework di descrizione delle unità operative che eseguiranno la migrazione al cloud.

Fra i documenti disponibili, si raccomanda una attenta lettura del **Manuale di abilitazione al Cloud e** l'utilizzo dei template raccolta delle informazioni degli applicativi, delle competenze e della strategia di migrazione con i workshop indicati nella metodologia. Il programma viene proposto a tecnici ed esperti del ICT, ai

responsabili della trasformazione digitale e a tutti gli stakeholder della progettazione dei nuovi servizi e della migrazione al Cloud. Il programma è in continua evoluzione sulla base delle esperienze delle amministrazioni.

Quanto illustrato successivamente nel presente documento rappresenta la trasposizione operativa e complementare a quanto indicato dal manuale, insieme alle esperienze di alcune amministrazioni che hanno iniziato o completato il processo di migrazione a Cloud, con specifico riferimento al Programma di Abilitazione al Cloud.

3. La situazione del Cloud nella PA rilevata dai Tavoli di Lavoro

Nei seguenti paragrafi vengono riportati i contributi derivati dal workshop effettuato in data 21 maggio 2020. Dall'edizione 2020, come sopra anticipato, sono stati raccolti attraverso un workshop i contributi dei partecipanti sul tema strategico del Cloud nella PA. Il workshop ha previsto due fasi:

- fase 1 - quattro tavoli di lavoro operativi relativi a:
  - obiettivi, requisiti e vincoli al modello di Cloud Transformation
  - modellazione del percorso attraverso i touchpoint del cloud
  - individuazione delle competenze chiave per il cloud
  - strumenti di procurement e di compliance normativa
- fase 2 – restituzione in plenaria dei risultati e chiusura dei lavori del referente scientifico.

3.1 Obiettivi, requisiti e vincoli della Cloud Transformation rilevati

Nell'ambito della definizione del nuovo modello strategico di Cloud il gruppo di lavoro raccomanda di tenere in considerazione i seguenti elementi:

- **Obiettivi**: quali obiettivi deve avere un percorso ideale di Cloud Transformation per raggiungere il modello desiderato.
- **Target**: a chi si deve rivolgere il percorso di trasformazione.
- **Perimetro**: quale tipologia di servizi sono coinvolti nella trasformazione (es. accessori, marginali, centrali, amministrativi ecc.).

Per quanto riguarda gli **obiettivi**, si riportano di seguito i principali individuati:

- governo del nuovo modello e della trasformazione indotta dalle nuove tecnologie;
- coerenza e governo dei singoli interventi con il paradigma adottato, anche grazie alla definizione di una roadmap realistica sulla realtà interessata, conciliando i limiti dettati dalla natura del dato gestito e i vincoli di connettività;
- miglioramento dei servizi IT in termini di qualità delle prestazioni, inclusività e fruibilità dei servizi offerti;
- abilitazione di nuovi servizi (es. fruibilità in smart working degli applicativi);
- individuazione mirata dei costi di gestione per ciascun nuovo progetto/applicativo/servizio ecc.) e ottimizzazione dei costi ICT complessivi (es. risorse dal datacenter alla connettività centrale e locale, contenimento a tendere della spesa per gli ambienti IT ecc.);
- scalabilità, integrazione, velocità di dispiegamento e flessibilità dell'infrastruttura IT;
- alto livello di sicurezza dell'infrastruttura IT;
- time to market e risposta tempestiva alle esigenze degli stakeholder;
- riutilizzo delle funzionalità e delle risorse cloud già presenti on premises per accelerare la Cloud Transformation e per realizzare un DR sostenibile in tempi brevi;

I **target** a cui si potrebbe rivolgere il percorso di trasformazione sono stakeholder nell'accezione più ampia:

- utenti esterni (cittadini, aziende, amministrazioni), quali ad esempio amministrazioni locali;

- utenti interni (dipendenti e collaboratori), ad esempio dipendenti dei reparti IT, utenti dei tenant come dipendenti regionali, operatori sanitari ecc.

Per quanto riguarda il **perimetro dei servizi** coinvolti, si riporta di seguito quanto rilevato:

- tutti i servizi esistenti erogati dalla PA e individuati a seguito di un assessment organizzativo e tecnologico e per cui è necessaria una reingegnerizzazione secondo delle priorità e prevedendo dei pilota (es. pilota di estensione del processo civile telematico ai giudici di pace);
- tutti i servizi erogati in futuro dalla PA e per cui è necessario realizzare un piano di migrazione.

Inoltre, sono stati rilevati i principali **requisiti organizzativi** e **tecnologici** necessari per avviare un percorso di Cloud Transformation, nonché i **vincoli** alla trasformazione digitale in Cloud.

Requisiti organizzativi

- Dalle gestioni operative al governo delle infrastrutture.
- Ricerca di competenze specifiche a supporto dei processi di governo e di change management.
- Presa di coscienza a livello di tutta organizzazione della necessità di operare un profondo processo di change management e coinvolgimento delle principali figure apicali per favorire il loro commitment.
- Coinvolgimento del top management delle realtà interessate per la definizione degli obiettivi nella definizione del nuovo modello di cloud, la redazione del budget e l'analisi e condivisione degli avanzamenti periodici rispetto agli obiettivi prefissati.
- Strutturazione della direzione IT correttamente dimensionata per far fronte alla complessità delle attività.
- Ricerca di nuove competenze specifiche sulle nuove tecnologie e ampliamento delle competenze dei reparti IT e dei profili tecnici, anche in merito alle skill tradizionali di gestione delle infrastrutture legacy.
- Utilizzo dei fondi strutturali che recepiscono l'agenda nazionale ed europea

Requisiti tecnologici

- Creazione di una roadmap attuabile ottimizzando le risorse e definizione di un programma di analisi partendo dalle best practice, prevedendo un'analisi di servizi per cloud e valutazione della readiness in funzione dei requisiti di business.
- Scurezza, performance e storage.
- Adeguata connettività e penetrazione degli applicativi cloud e alta banda.
- Rinnovamento deli strumenti tecnologici: infrastrutture a microservizi, protocolli leggeri (es. REST, JSON), containers ecc.
- Utilizzo di soluzione infrastrutturali standard.
- Verifica degrado delle performance dei servizi.
- Procurement delle soluzioni già esistenti sul mercato.

Vincoli

- Non sufficiente commitment del vertice, politico e amministrativo, delle realtà interessate dalla trasformazione.
- Non sufficiente comprensione da parte del top management delle realtà interessate dalla trasformazione del cloud come modello di erogazione dei servizi.
- Aspetti di compliance normativa privacy e trust.
- Connettività e sicurezza.
- Situazioni di lock in, causa utilizzo di standard non aperti che non garantiscono la migrazione in modo semplice.
- Gestione del budget e allocazione delle risorse su diversi capitoli di spesa (considerare e gestire la riallocazione delle risorse in tempo utile - es. tipologia di spesa servizi OPEX vs CAPEX).

- Paradigma del modello di gestione (necessario un nuovo paradigma e di operare risk based adottando standard e best practice).

3.2 I servizi Cloud di interesse della PA (*touchpoint*)

La modellazione del percorso di Cloud Transformation effettuato dal gruppo di lavoro attraverso i touchpoint si basa su:

- individuazione AS IS dei principali touchpoint di riferimento, ossia l'individuazione di come viene fornito attualmente il cloud per i servizi IaaS, PaaS e SaaS (Privato - Ibrido - Pubblico);
- individuazione TO BE dei principali touchpoint di riferimento necessari per un percorso di Cloud Transformation e quindi come dovrebbe essere fornito il cloud per i servizi IaaS, PaaS e SaaS (Privato - Ibrido - Pubblico);

Nelle tabelle che seguono si riportano i contributi raccolti durante il workshop, suddivisi per tipologia di servizio.

IaaS (Infrastructure as a service)

Tipo di Cloud	*As is*	*To be*
Privato	• BC e DR • VM per test, collaudo, produzione • Storage e Backup • Sito web e media	Storage e Backup
Ibrido	Supporto definizione strategia di migrazione applicativi in IaaS	n/a
Pubblico	PDL on premises	n/a

PaaS (Platform as a service)

Tipo di Cloud	*As is*	*To be*
Privato	n/a	Big data analytics & Smart City platform
Ibrido	• Supporto definizione strategia di migrazione applicativi in PaaS • Supporto sviluppo cloud first • Gestione vendor del lock in applicativo	n/a
Pubblico	n/a	n/a

SaaS (Software as a service)

Tipo di Cloud	*As is*	*To be*
Privato	• Gestione documentale • Sito web • Posta e PEC • eLearning • Sportello online	Office automation e Posta
Ibrido	n/a	n/a
Pubblico	• Posta e PEC • Collaboration • CRM • Gestionale adempimenti GDPR	Product lifecycle

3.3 Lo stato delle competenze per il Cloud

Si riportano di seguito le competenze individuate da parte dei partecipanti al workshop necessarie per l'avvio di un percorso di Cloud Transformation:

- capacità di visione per individuare il nuovo modello dei servizi e come agire sul parco applicativo per perseguire la realizzazione del nuovo modello;
- capacità di governo della trasformazione e del nuovo modello organizzativo/tecnologico che preveda anche il controllo pubblico sui dati nel rispetto della cornice normativa;
- capacità definizione e di formalizzazione dei requisiti funzionali;
- capacità di semplificazione e di allineamento dei processi organizzativi al modello tecnologico e di adeguamento dei processi anche a scenari di indisponibilità dei servizi cloud;
- capacità di gestione del cambiamento, coinvolgendo gli attori impattati, e di comunicazione verso gli utenti/clienti del percorso di trasformazione da attuare e della cultura dei servizi cloud verso i fruitori del servizio;
- conoscenza del modello cloud da parte degli utilizzatori, in termini di utenti finali e stakeholder;
- capacità di pianificazione economica coerente con il modello agile (opex/servizi a scadenza), anche per evitare interruzioni di servizio pubblico;
- capacità di comprensione delle linee guida dei modelli architetturali e competenze tecniche sulle tecnologie: competenze di enterprise architecture, DevSecOps per sviluppo agile e sicuro, capacità di comprensione dell'infrastruttura as a code e di valutazione della relazione tra architettura logica (applicativa) e pseudo fisica;
- competenze in ambito di gestione della sicurezza informatica (dei dati e infrastrutturale) e miglioramento della security awarness degli utenti/clienti;
- competenze evolute in ambito di data protection (es. chiara definizione di ruoli e responsabilità, data protection by design, anonimization by design, criptazione data lifecylce);
- competenze in materia di procurement e di definizione e misurazione di modelli/contratti agili;
- competenze cross tecnologia e cross cloud per evitare cloud lock in;

- capacità di guidare e coordinare l'ecosistema dei fornitori per riuscire a convergere e a realizzare la roadamap verso il nuovo modello di servizi;

3.4 Strumenti di Procurement

Il Sistema di e-Procurement della Pubblica Amministrazione, realizzato dal MEF tramite Consip in attuazione del Programma per la razionalizzazione degli acquisti nella PA, consente a soggetti aggiudicatori e fornitori di utilizzare gli strumenti di acquisto/negoziazione, nel rispetto della normativa applicabile a ciascun utente operante nel Sistema e rende più efficiente e trasparente l'utilizzo delle risorse pubbliche.

Di seguito vengono illustrati i possibili strumenti di approvvigionamento attuali e futuri a disposizione della PA per il percorso evolutivo dell'ICT pubblico, con particolare riferimento allo scenario Cloud.

- **Accordi quadro (appalto specifico)**: la procedura prevede due fasi. Nella fase 1 Consip pubblica specifici bandi e stipula il contratto con uno o più fornitori, nella fase 2 le amministrazioni indicono e aggiudicano i singoli appalti specifici, negoziando direttamente con i fornitori condizioni contrattuali personalizzate sulla base delle proprie esigenze.
- **Contratti quadro e convenzioni (ordine diretto)**: la procedura prevede due step. Durante il primo step Consip pubblica il bando di gara e stipula il contratto con i fornitori, il secondo step prevede l'emissione da parte delle amministrazioni di ordini diretti, alle condizioni e ai prezzi stabiliti in Convenzione, inviati telematicamente direttamente ai fornitori.
- **Mercato elettronico della PA – MEPA (richiesta di offerta, trattativa e ordine diretto)**: la procedura prevede tre step. Nella fase 1 Consip pubblica i bandi del Mercato elettronico a cui i fornitori possono abilitarsi, se soddisfano le condizioni generali e i requisiti fissati. Nella Fase 2 i fornitori pubblicano le offerte. Nella fase 3 le Amministrazioni emettono ordini diretti o negoziano prezzi e condizioni di fornitura migliorativi, attraverso richieste di offerta o trattative dirette.
- **Sistema dinamico di acquisizione – SDAPA (bando semplificato con appalto specifico)**: la procedura prevede due fasi. Nella fase 1 Consip pubblica un bando per una o più categorie merceologiche a cui i fornitori possono abilitarsi. Nella fase 2 le Amministrazioni pubblicano e aggiudicano gli appalti specifici, a cui possono partecipare i fornitori ammessi a presentare offerta. Per l'aggiudicazione degli appalti, le Amministrazioni seguono le norme della procedura ristretta. Il sistema SDAPA è aperto a tutti gli operatori economici per il periodo di validità del singolo bando di riferimento.
- **Gare su delega/strategiche:** ordine diretto.

Consip, oltre agli strumenti di e-procurement già citati, prevede una serie di iniziative e strumenti atti ad indirizzare fabbisogni specifici. Di seguito si riportano alcuni esempi attualmente disponibili:

- **Gara in aggiudicazione SPC cloud:** divisa nei seguenti lotti:
    - **Lotto 1: servizi di cloud computing**
    - Lotto 2: servizi di identità digitale e sicurezza applicativa
    - Lotto 3: servizi di cooperazione applicativa
    - Lotto 4: open data e big data e ai servizi di realizzazione di portali e servizi on-line.

  La procedura per l'affidamento dei servizi oggetto della fornitura è articolata attraverso la stipula da parte di Consip S.p.A. di un contratto quadro con l'aggiudicatario di ciascun lotto, in modo del tutto disgiunto tra i singoli lotti.

  In relazione al **lotto 1 "Servizi di cloud computing"**, il massimale del contratto quadro è stato stabilito in 500.000.000 di euro e comprende servizi in modalità cloud computing (IaaS, PaaS, SaaS) e servizi di abilitazione al cloud. I servizi possono essere acquistati dalle Amministrazioni con l'obiettivo di

migrare in modalità cloud computing il proprio Data Center, creare servizi pubblici innovativi e cooperabili con altri servizi di altre Amministrazioni, ottemperare agli artt. 43, 44 e 44-bis del CAD sulla conservazione dei documenti informatici. Nello specifico, come indicato da capitolato tecnico, la fornitura del lotto 1 comprende:

- servizi di calcolo e memorizzazione (IaaS) per la fruizione di risorse remote virtuali, rese disponibili per il tramite di risorse fisiche predisposte ad uso esclusivo delle Amministrazioni (Community Cloud) e i servizi sono corredati da strumenti di gestione e configurazione e includono funzionalità di networking;

- servizi di tipo PaaS per l'erogazione alle Pubbliche Amministrazioni di servizi middleware per lo sviluppo, collaudo, manutenzione ed esercizio di applicazioni. I servizi PaaS sono identificati attraverso una o più architetture di servizi software - Solution Stack, diversificate in funzione della tipologia di servizio applicativo che viene erogato, che poggiano su un'infrastruttura di tipo IaaS. Tali servizi sono corredati da strumenti di gestione e di configurazione;

- servizi di tipo SaaS per la erogazione di servizi applicativi alle Pubbliche Amministrazioni tra i quali servizi per la conservazione dei documenti, servizi di collaborazione, servizi di produttività individuale, servizi di comunicazione unificata, servizi di analisi dei dati e reportistica. Tali servizi sono corredati da strumenti di gestione e configurazione;

- servizi di Cloud Enabling, tra cui il supporto alla virtualizzazione di infrastrutture fisiche nell'ambito dei CED privati delle Pubbliche Amministrazioni (migrazione Phisical to Virtual).

- **Sistema dinamico (SDAPA) 3.0 (pubblicato a maggio 2018, durata 3 anni):** nuova categoria merceologica per servizi cloud, con tre schede tecniche dedicate per servizi IaaS, PaaS e SaaS in linea con il piano triennale ICT per le pubbliche amministrazioni e destinato ad acquisti sopra soglia da effettuarsi con Appalti Specifici.
- **Mercato elettronico per la PA (MEPA)**: bando Servizi per l'Information and Communication Technology, sottocategoria Cloud Computing che comprende IaaS e SaaS, destinato ad acquisti sottosoglia.
- **Gare Strategiche (Piano Gare Strategiche ICT 2018)**: Nell'ambito del piano triennale sono state definite alcune gare ad indirizzo strategico, in corso di preparazione, per mettere a disposizione delle PPAA servizi e strumenti abilitanti la trasformazione digitale ed agevolare la transizione dei sistemi informativi verso un modello cloud definito, facilitando in tal modo l'attuazione del Piano Triennale.

Nell'ambito di un modello strategico del Cloud della PA (razionalizzazione delle infrastrutture) e dei servizi ICT, secondo un modello «pubblico» e con specifiche caratteristiche, Consip provvede la messa a disposizione delle PA, tramite i propri strumenti di approvvigionamento, i servizi IaaS, SaaS e PaaS qualificati da AgID.

L'istituzione della **piattaforma Cloud Marketplace di AgID** espone infatti un elenco di fornitori (Cloud Service Provider) e dei servizi Cloud (IaaS, SaaS e PaaS) qualificati. All'interno del marketplace si può visualizzare la scheda tecnica di ogni servizio con informazioni circa le caratteristiche tecniche, il modello di costo e i livelli di servizio dichiarati dal fornitore in sede di qualificazione.

4. Strategia di Digital Transformation

Le indicazioni contenute nel presente capitolo traggono origine dall'esperienza di INAIL e in particolare dal lavoro svolto, a partire dal 2018, dalla Direzione Centrale Organizzazione Digitale per l'ammodernamento dell'infrastruttura digitale dell'Ente. A fine 2020 l'INAIL ha completato il trasferimento dei principali servizi digitali dell'Istituto dal sistema mainframe su una nuova piattaforma, adottando le logiche del paradigma cloud.

Il presente capitolo si prefigge l'obiettivo di **sviluppare operativamente** gli elementi di strategia che concorrono alla definizione e realizzazione di un percorso di Trasformazione Digitale in linea con le indicazioni AgID. Con particolare riferimento al manuale di abilitazione al Cloud gli elementi di seguito riportati derivano dall'esperienza concreta di INAIL che ha seguito l'indirizzo dei Capitoli 3, 4 e 5 (Assessment Servizi e Infrastruttura, Pianificare la migrazione ed Eseguire la migrazione).

Consci delle diversità e delle peculiarità esistenti nel variegato panorama della PA Italiana, traiamo dal percorso intrapreso da INAIL alcune riflessioni in materia di strategia, business, tecnologia e organizzazione, rispetto alla Digital Transformation, che possono essere messe a fattor comune e possano gettare le basi per una comune strategia di Digital Transformation.

Tratto comune, per tutti gli Enti che approcciano la definizione della strategia per la Digital Transformation, deve necessariamente essere la **predisposizione al cambiamento**. Molte sono le iniziative di Change Management in corso nella PA per accompagnare e supportare i progetti di trasformazione e che indirizzano:

- cambiamenti culturali in quanto il Cloud, il provisioning delle risorse, il loro consumo e consuntivazione necessita di un "*mindset*" orientato al pay-per-use e quindi l'idea che, volendo semplificare, alcuni settori possano lavorare a "risorse infinite" non è più applicabile. Il nuovo principio che guida le scelte nella logica "as a Service" deve essere basato su architetture coerenti e correttamente dimensionate in modo che i benefici della trasformazione siano realmente tangibili;
- cambiamenti organizzativi per migliorare la collaborazione tra i gruppi di lavoro e per allineare la strategia all'operatività necessaria ad attuare il cambiamento. La trasformazione digitale all'interno delle amministrazioni deve essere accompagnata da una modalità di ascolto attivo tra i dipartimenti e verso l'utente finale. L'esperienza di fruizione dei servizi nella vita quotidiana ha influenzato le aspettative dell'utente che oggi, più che in passato, cerca la stessa esperienza nell'utilizzo dei servizi da parte delle amministrazioni pubbliche;
- cambiamenti nel modello operativo, definizione di nuovi ruoli, nuove mansioni, nuovi strumenti da utilizzare per l'esecuzione dei servizi;
- cambiamenti nelle tecnologie che vengono acquistate sia dal punto di vista delle infrastrutture che dai "modelli" applicativi che vengono progettati e rilasciati;
- cambiamenti nella modalità di acquisto dei servizi e prodotti, declinare l'approccio Agile & DevOps richiesto ai fornitori all'interno dei framework contrattuali e nella realizzazione degli Appalti Specifici. Utilizzare gli Accordi Quadro che Consip mette a disposizione per la Digital Transformation e il Cloud.

4.1 Tratti specifici contesto di business della PA e delle prospettive di trasformazione digitale (Requisiti di Business)

Il percorso di innovazione verso il Cloud è di fatto unico per ogni Ente. Molti sono i tratti comuni da considerare per l'analisi dell'evoluzione delle Amministrazioni ma, il contesto specifico della singola PA gioca un ruolo determinante e alcuni elementi vanno approfonditi in questa fase in modo da indirizzare correttamente il percorso.

Tra gli elementi maggiormente rilevanti sui quali focalizzare l'attenzione in una fase di approccio alla Digital Transformation riveste un posto di prim'ordine il contesto della **Security**. La sicurezza, secondo i paradigmi attuali di Zero-Trust, merita una trattazione completa, che abbraccia tutti i dipartimenti delle Amministrazioni e che rende i singoli ambiti di security armonizzati con il percorso strategico di evoluzione dei servizi. Si forniscono delle prime basilari indicazioni in materia nel capitolo 6 del presente documento, ma per una trattazione adeguata del tema, si è scelto di indirizzare in maniera compiuta questa declinazione in un allegato successivo al presente lavoro.

- ✓ **Contesto di Business Specifico**
  A seconda del contesto all'interno del quale l'Amministrazione opera è possibile riscontrare elementi che influiscono, supportano o (eventualmente) inibiscono la trasformazione digitale e l'evoluzione verso il Cloud. Basti pensare ad un quadro normativo in frequente evoluzione, ad una pulsione tecnologica e innovativa dettata dall'adeguarsi o, in taluni casi, governare il cambiamento (ad esempio in Enti collegati alla trasformazione del settore fintech).

- ✓ **Rapporto con l'utenza e fruizione dei servizi**
  Gli utenti dei servizi erogati dalla specifica Amministrazione possono essere esterni (cittadini, aziende, amministrazioni) o interni (dipendenti e collaboratori) ed i servizi possono essere fruiti secondo diverse modalità operative più o meno digitali/digitalizzate. I volumi legati al numero di utenti, degli accessi totali e contemporanei ai servizi, le opzioni di multicanalità, i tempi di lavorazione delle

- ✓ **Dati e criticità delle Banche Dati (Interesse Nazionale)**
  Le basi di dati di interesse nazionale sono "basi di dati affidabili, omogenee per tipologia e contenuto, rilevanti per lo svolgimento delle funzioni istituzionali delle Pubbliche amministrazioni e per fini di analisi. Esse costituiscono l'ossatura del patrimonio informativo pubblico, da rendere disponibile a tutte le PA, facilitando lo scambio di dati ed evitando di chiedere più volte la stessa informazione al cittadino o all'impresa".
  I dati sono un elemento imprescindibile di analisi nella scelta di una strategia evolutiva Cloud. La centralità delle banche dati merita di essere collocata, (ancora prima di scendere al dettaglio di analisi su confidenzialità del dato, crittografia, sicurezza e analisi dell'accesso al dato stesso), al livello di strategia e criticità dei dati gestiti dall'Ente per l'interesse Nazionale. In aggiunta alle infrastrutture individuate come critiche per il Paese, esistono una serie di Banche Dati all'interno della Pubblica

Amministrazione che sono oggetto di particolare attenzione. Questo significa che l'evoluzione della componente dati e/o delle applicazioni che con essa interagiscono va analizzata in maniera specifica per non compromettere l'integrità, la sicurezza, la necessità di standardizzazione, la disponibilità, l'accessibilità, la compliance. Le anagrafiche (di cittadini ed aziende) e le banche dati tributarie e giudiziarie sono esempi rappresentativi della tipologia di informazioni di interesse nazionale.

- ✓ **Ruolo e strategicità dell'IT per l'Amministrazione**

  Il peso specifico dell'IT e la sua evoluzione non è lo stesso per tutte le amministrazioni, centrali e locali e, spesso dipende dalla numerosità dei dipendenti, dalla tipologia dei servizi offerti, dal contesto in cui l'Amministrazione opera. Il numero di progetti (sia infrastrutturali che applicativi) che mediamente vengono avviati annualmente è un indicatore che incide sull'approccio da definire per l'evoluzione IT. Se le iniziative progettuali (che nascano all'interno del dipartimento IT o che ne vedono un importante coinvolgimento) sono "relativamente poche" può aver senso impostare una strategia di trasformazione che partendo dall'innovazione di singole applicazioni o servizi o componenti infrastrutturali possa trainare in maniera progressiva altre aree affini verso un percorso coerente di ammodernamento. Laddove l'IT, invece, rivesta un ruolo centrale per il contesto dell'Amministrazione, oppure esistano tematiche di evoluzione strategica di Data Center, loro federazione, realizzazione di un Polo di erogazione servizi Cloud la scelta migliore è impostare una strategia partendo dalla "Big Picture" per poi declinare sui singoli task progettuali.

- ✓ **Evoluzioni dei Servizi, frequenza dei rilasci e creazione di nuove applicazioni**

  Tra gli aspetti importanti da considerare per la definizione della strategia emerge il contesto applicativo. La numerosità delle applicazioni da gestire ed evolvere, la complessità delle architetture, il livello di personalizzazione e di "customizzazione", i *function points* associati allo specifico modulo applicativo, il debito tecnico e l'obsolescenza di versioni, linguaggi e librerie. Questi sono alcuni tra gli elementi "statici" da considerare per pianificare le aree di intervento sulle applicazioni. La componente dinamica è legata a tutto quello che ruota intorno alle applicazioni, la modalità attraverso la quale il Software Lifecycle si articola, le complessità dovute alla corretta implementazione dei requisiti, la difettosità del codice e la gestione/frequenza dei rilasci. Perché la definizione di una strategia di trasformazione verso la digitalizzazione e il Cloud non può prescindere da questi elementi (o una loro parte)? Semplicemente perché il passaggio da una pianificazione teorica all'implementazione pratica deve portare beneficio tangibile anche per chi sviluppa, esercisce e promuove le applicazioni all'interno dell'organizzazione. Il beneficio diventa reale se alla base vengono considerate le specifiche esigenze e peculiarità del parco applicativo, la loro corretta mappatura all'interno di strumenti di Enterprise Architecture e la comunicazione efficace attraverso i dipartimenti/uffici.

- ✓ **Interoperabilità e aspetti di Federazione Cloud**

  A corredo di questi elementi di valutazione è importante definire, in maniera prospettica, il livello di interoperabilità con altri soggetti (enti, ministeri, amministrazioni europee che condividono la stessa missione istituzionale) in modo da definire piattaforme di servizi, protocolli e politiche di sicurezza ed interoperabilità che siano comuni, condivise e standard.

- ✓ **Aspetti di stagionalità dei servizi, periodi di disponibilità, manutenzione e resilienza**

  Esistono specifici contesti di Business e tipologie di servizi verso la cittadinanza che prevedono periodi nei quali l'erogazione, l'attivazione, l'accesso a particolari funzionali non è consentita (si pensi, a titolo di esempio, ad alcune caratteristiche legate alla sottomissione di domande o richieste strettamente collegate a scadenze temporali, servizi di welfare, pratiche concorsuali, campagne fiscali). Alcuni servizi, anche se sempre in numero minore, non sono attivi durante il finesettimana o in fasce orarie notturne. La migrazione del parco applicativo di uno specifico Ente può e deve tenere conto delle caratteristiche legate alla fruizione del servizio, alla sua disponibilità verso l'utente finale, alle finestre di manutenzione programmata all'interno delle quali testare ed effettuare upgrade e migrazioni. Non è da meno la definizione di una strategia per la resilienza dei servizi, anche nella definizione di una roadmap evolutiva,

privilegiano applicazioni, componenti e infrastrutture che emergono all'interno delle analisi di risk management, BIA e compliance.

A supporto dell'approccio strategico sopra individuato può essere utile riportare **un esempio**.

Si pensi ad un Ente *locale* che rivolge i suoi servizi principalmente ad *utenza esterna*, nella fattispecie cittadini attraverso delle piattaforme *multicanale* (portali web, app, social, call center, uffici). Si immagini un contesto all'interno del quale i *dati* – sensibili ma non critici dal punto di vista nazionale - risiedono localmente in *Data Center di proprietà* gestito da fornitori esterni, il *numero di applicazioni* sia circa 20 e con un *elevato debito tecnico* in termini di linguaggi e obsolescenza dei prodotti software. Più che adeguato risulta invece il rispetto delle normative e degli aspetti di *compliance* in termini di mantenimento certificazioni ISO, *Sicurezza*, *Disaster Recovery* e Best Practices per il Service Management e le Operations. L'IT è importante all'interno dell'Ente, ma non è tipicamente il principale driver di innovazione e trasformazione.

Un secondo esempio riguarda un Comune di medio-piccole dimensioni, indicativamente al di sotto dei 20.000 abitanti dotato di una infrastruttura principalmente on premise e con un Sistema Informativo interno composto spesso da un singolo addetto se non da addetti che svolgono anche altre funzioni all'interno dell'Ente. La compliance normativa in termini di sicurezza, certificazioni ISO, Business Continuity è spesso non adeguata se non carente. Si tratta dello scenario numericamente più diffuso per la PA italiana che rappresenta il 93% dei 7.903 comuni italiani (dati Istat 2019).

In un contesto come quello che abbiamo tracciato, in relazioni agli Enti locali, ci sembra utile citare l'esperienza di CSI Piemonte. Il Consorzio piemontese, su incarico di Regione Piemonte e con la collaborazione di AgID, ha avviato un progetto di supporto rivolto a circa 400 Enti piemontesi per supportarli nel processo di migrazione in cloud.

Da qui nascono alcuni semplici suggerimenti per gli Enti locali, affinché affrontino in sicurezza il percorso di adozione del cloud. Il modello è quello proposto da AgID nel suo Manuale di abilitazione al cloud, con l'aggiunta di qualche proposta pratica utile a semplificare il percorso, commisurandolo alla complessità del proprio IT. Nella fase iniziale è determinante come già evidenziato in più punti definire in maniera chiara gli obiettivi, ponendosi alcune semplici domande:

1. l'Ente ha personale IT interno in grado di guidare/coordinare una migrazione in cloud (re-platforming, re-architect) e la volontà di continuare a gestire i servizi in cloud a migrazione ultimata?
2. L'Ente ha la necessità di rivedere o sostituire applicazioni che tecnologicamente potrebbero essere non idonee alla migrazione in cloud (vedi applicazioni client/server)?
3. In merito alla connettività geografica qual è il tipo di connessione in uso e la disponibilità offerta dal mercato nel proprio territorio? L'attuale connessione quanto è utilizzata? Sarebbe in grado di sostenere il traffico derivante da un passaggio in cloud?
4. L'Ente si pone l'obiettivo di migrare solo le componenti applicative o punta a dismettere tutte le infrastrutture locali incluse quelle necessarie al funzionamento delle postazioni di lavoro (autenticazione, condivisione documenti, stampanti)?

Chiarire tali *key points* può tornare molto utile al fine di comprendere meglio la propensione dell'amministrazione ad intraprendere il viaggio verso il cloud e soprattutto individuare quale tipo di percorso intraprendere.

La fase successiva, quella dell'assessment può essere svolta seguendo la traccia proposta da AgID con il supporto dei fornitori applicativi presenti all'interno dell'Ente, con l'obiettivo di creare una mappa di sintesi sullo stato di fatto del proprio sistema informativo e della propria organizzazione. Per comuni sotto i 20.000 abitanti è molto frequente avere meno di 5 fornitori di soluzioni applicative, il che facilita molto questa fase iniziale che punta ad individuare fondamentalmente:

- ✓ quali soluzioni sono pronte per poter essere facilmente migrate in cloud;

- ✓ quali degli attuali fornitori ha già una soluzione in SaaS certificata che permetterebbe all'amministrazione di ridurre i tempi di migrazione e la necessità di formazione del personale;
- ✓ quali richiedono una valutazione più attenta rispetto ai costi/benefici considerando anche l'opportunità di acquisire servizi SaaS certificati da fornitori differenti da quello attuale;
- ✓ Qual è l'impegno economico che l'Ente dovrà affrontare per sostenere il processo di trasformazione.

L'esperienza piemontese ha portato inoltre alla valorizzazione delle forme associate tra Comuni che hanno scelto di sfruttare il momento di passaggio al cloud come la possibilità di rivedere la propria organizzazione ICT ottenendo molteplici benefici tecnici, economici e organizzativi. Vediamone alcuni tra i principali:

- ✓ Semplificazione tramite l'adozione della stessa suite applicativa per l'intera Unione per specifiche coperture funzionali. Rappresenta un passaggio anche culturale che permette una maggiore standardizzazione, una più diffusa conoscenza tra Enti che spesso già si trovano ad erogare servizi in forma associata e la possibilità di trasformazione anche organizzativa facilitando l'interoperabilità.
- ✓ Riduzione del Total Cost of Ownership (TCO): sia i costi relativi al processo di trasformazione che quelli relativi ai costi ricorrenti. In funzione della dimensione della forma associata si possono raggiungere forti economie di scala e un aumentato potere contrattuale nei confronti del mercato che generalmente su questo segmento vede pochi operatori di livello nazionale o moltissime realtà che invece operano localmente.
- ✓ Connettività: in uno scenario di questo tipo sono possibili molteplici soluzioni di connettività geografica che possano portare anche ad architetture *a stella* in cui la massima banda disponibile viene portata verso il Comune con maggiore copertura che può fungere quindi da centro stella per gli altri Comuni che potranno adottare soluzioni con banda ridotta e anche soluzioni wireless per coprire territori non ancora raggiunti dal piano BUL. In un tale scenario gli operatori WISP svolgono sicuramente un ruolo centrale.

4.2 Richiamo alla Strategia Cloud

Con riferimento agli obiettivi salienti della strategia Cloud della PA e a quanto già illustrato nel Capitolo 2, si ritiene importante riprendere e approfondire alcuni aspetti al fine di fornire elementi di contesto, legati alle considerazioni che negli ultimi anni INAIL ha portato avanti, che possono essere utili ad altre amministrazioni.

Internalizzazione vs esternalizzazione delle **competenze informatiche**	In maniera strettamente dipendente dalla capacità, pianificazione e possibilità di intervenire, per la specifica PA, nel processo di reclutamento, selezione e *hiring* di personale interno, è importante valutare il ruolo che si intende far giocare al Dipartimento IT in termini di numero di risorse, formazione e ambito di intervento. L'avvio di un percorso di Trasformazione Digitale è un impegno pluriennale che richiede capacità di governo e competenza sia tecnico/tecnologica che organizzativa. La scelta di potenziamento dell'organico interno, laddove possibile, rappresenta un elemento aggiuntivo significativo per il raggiungimento degli obiettivi sia in termini di consapevolezza e cultura ma soprattutto nell'interesse dell'economicità dei tempi/costi di progetto.
Data Center e considerazioni relative ai Poli Strategici Nazionali	AgID ha avviato e concluso, in conformità con quanto previsto dalla circolare 1/2019 e dal Piano Triennale, il censimento del patrimonio ICT della PA con l'obiettivo di rilevare lo stato delle infrastrutture IT della PA e acquisire informazioni essenziali per dar vita al processo di razionalizzazione dei data center della PA italiana e di adozione del modello Cloud. Il censimento è stato condotto da AgID su quasi mille amministrazioni per un totale di 1252 data center censiti.

	La strategia evolutiva delle Infrastrutture della specifica PA è collegata al posizionamento sia rispetto al censimento, che rispetto alle considerazioni di opportunità, (come il cost-saving, il miglioramento dei servizi e l'innovazione), che possono indirizzare la scelta verso il moving in un PSN o verso la realizzazione (laddove le caratteristiche lo consentono) di un Polo Strategico Nazionale.
Software As a Service	Il Principio del Cloud First potrebbe essere, come anticipato nelle precedenti sezioni, un primo tassello nella definizione della strategia di adozione Cloud. Diverse sono le Amministrazioni che iniziano il percorso dalla Posta Elettronica, dalle integrazioni applicative con Firma Elettronica, adozione di moduli per HR e CRM in SaaS o dall'incapsulamento di servizi di pagamento, chatbot, motori di ricerca esterni erogati attraverso un Software As a Service. Come molte scelte di natura tecnologica e organizzativa esistono dei pro e dei contro. La standardizzazione stessa, che una soluzione SaaS porta con sé, può essere percepita come limitazione alla personalizzazione precedentemente utilizzata o, viceversa, come un passo verso la compliance e l'interoperabilità con altre soluzioni, piattaforme o anche Enti che operano secondo gli standard di riferimento (sia normativi che di mercato). Non è facile individuare i corretti driver di scelta che dipendono dalle caratteristiche della specifica PA ma questo è sicuramente un aspetto che, in questa fase di definizione della Strategia, va affrontato.

Sulla base di questi aspetti è necessario definire un piano con **obiettivi** a breve/medio/lungo termine da inserire nel piano Strategico Triennale in modo da indirizzare gli investimenti secondo una programmazione e un disegno coerente e innovativo.

4.3 Definizione dello stato dei servizi (*Assessment*)

4.3.1 Introduzione all'Assessment

La fase di Assessment consente di valutare i possibili percorsi di innovazione IT che l'Amministrazione può intraprendere fotografando la situazione attuale di infrastrutture, applicazioni, requisiti di business, contratti, sicurezza sulla base della situazione in esercizio.

In un'economia in cui l'innovazione tecnologica è una delle leve principali per la competitività, dove tutte le amministrazioni sono in corsa verso un percorso di trasformazione digitale, è importante avere la capacità di poter prendere delle decisioni strategiche in maniera accurata e veloce, su tematiche riguardanti tecnologie, processi, organizzazione interna e strumenti.

Fare una scelta accurata sulla direzione e approcci da scegliere diviene quindi un punto cruciale, ma che necessita di un supporto di una metodologia e di una modellizzazione, al fine di poter dare delle raccomandazioni sulle future strategie.

Alla base di una metodologia e della creazione di un modello per il processo di trasformazione, ci deve essere una valutazione concisa del livello di conoscenza tecnologica e delle competenze specifiche sia interne che esterne all'amministrazione, assieme ad una chiara vista delle entità tecnologiche in uso e a loro disposizione.

La fase di valutazione del livello di conoscenza tecnologica attraverso un modello pone in rilievo l'attività di assessment, che fotografa, misura e stabilisce lo stato di salute di una organizzazione rispetto ad un tema specifico: tramite queste informazioni è possibile utilizzare dei modelli che possano dare delle indicazioni standardizzate sulle strade da intraprendere.

Creare un assessment verso il cloud racchiude un insieme di attività volte a dare delle indicazioni temporali e strategiche sulla pianificazione delle attività verso un percorso di adozione del cloud e dei paradigmi ad esso legati.

Un assessment può essere suddiviso nelle seguenti sotto attività:

- **Preparazione**, che racchiude l'identificazione dei sistemi di catalogazione delle informazioni, acquisto della consapevolezza sulle informazioni contenute, check su correlazioni fra i differenti sistemi e disegno di un modello dati.
- **Raccolta dati**, dove si iniziano a prendere le informazioni sia tramite le sorgenti dati che attraverso delle interviste a referenti e tecnici.
- **Validazione** fase in cui vengono effettuati dei controlli sui dati per la loro validazione, catalogazione, correlazione e raggruppamento in cluster in base a criteri di similarità di caratteristiche tecniche.
- **Roadmap**, ovvero la fase finale, in cui vengono presentati i risultati strategici e le indicazioni temporali che suggerisce un assessment verso il cloud (ovvero se migrare nel breve, medio o lungo termine).

4.3.2 Assessment tecnologico

Metodologia e modello che consenta valutazioni sia in ambito infrastrutturale, data center, che applicativo ed evolutivo. In questa sezione si farà riferimento al framework AgID & chiaramente all'esperienza INAIL. Sarà sottolineata l'importanza delle analisi delle architetture, delle componenti sia Infrastrutturali che Applicative e della loro predisposizione (sia in termini di roadmap di prodotto, evoluzioni ed EoL, che di protocolli ed integrazioni). L'assessment dovrà tenere certamente conto delle tematiche salienti di Security, di valutazione circa strumenti per il DevOps e dello stato di maturità generale.

Un assessment tecnologico diviene un'attività focale dell'analisi, avente l'obiettivo di individuare gli interventi necessari per un percorso di innovazione digitale sulla base di stato e maturità dei sistemi e processi attualmente in uso all'interno dell'Amministrazione.

Un percorso verso un'innovazione tecnologica si basa su un insieme di cambiamenti da adottare non solo nei sistemi in uso, ma anche nelle tecnologie da utilizzare, processi, governance e skill: avere un processo che possa dare delle indicazioni sullo stato attuale, stabilire un obiettivo target e dare indicazioni sugli step successivi diviene quindi un punto cruciale che viene rappresentata dall'attività di assessment tecnologico.

Una volta definita la mission dell'amministrazione, che vuole intraprendere un percorso di trasformazione e innovazione è necessario fare i seguenti steps:

- creazione, o più verosimilmente, adozione di un **Maturity Model** in cui vengano raccolte le informazioni, tramite una serie di interviste, riguardanti pratiche e processi verso una determinata metodologia.
- Una volta individuate le sotto-aree di analisi si assegna una scala di possibili stati o livelli descrivendo le caratteristiche che concorrono al livello in questione. A titolo di esempio in INAIL è stato utilizzato il seguente ranking per la valutazione circa i processi e l'adozione delle pratiche DevOps con la seguente scala di valori:

    1. **Ad Hoc***:* processi manuali e poco prevedibili/preventivabili.
    2. **Repeatable**: processi definiti esclusivamente su progetti.
    3. **Consistent**: processi in ambito definiti e seguiti a livello organizzativo.
    4. **Optimised**: processi misurabili e controllabili con un sistema di metriche.
    5. **Leading:** processi focalizzati sul miglioramento continuo.

- Per quanto concerne il Cloud, analogamente si stabilisce il grado di Readiness per ogni singola applicazione in base a una serie di indicatori (come indicato nelle linee guida Agid) e si ipotizza un livello (con un indicatore numerico) target che sia raggiungibile per l'Amministrazione.
- In base al grado attuale di risposta a questo Maturity Model, viene stabilito un percorso fatto di passi da sequenzializzare e di dipendenze da costruire per disegnare gli step verso il raggiungimento del grado target.

Per quanto riguarda la migrazione dei sistemi dell'amministrazione verso il cloud, è necessario un assessment che si basi su una valutazione con dati che comprendano diversi livelli di astrazione:

- **Infrastrutturale**, che comprende:
    - dimensionamento delle componenti infrastrutturali: componenti infrastrutturali attualmente in uso nei sistemi (ad es. numero di server, CPU, memoria, sistemi di storage e volumi,) nonché utilizzo di esse;
    - sistemi on-premise con cui il sistema è interconnesso: sistemi on-premise interni ed esterni da cui l'applicativo dipende, ad es. sistemi di autenticazione);
    - rete, comprendendo topologie di rete, connettività, banda disponibile, apparati di rete, policy;
    - stack tecnologico: componenti tecnologiche attualmente in uso (ad es. database usato e rispettiva versione, ambiente di runtime, sistemi di notifica, sistemi di gestione di code, web server);
    - datacenter utilizzati.
- **Tecnologica**, che comprende:
    - tecnologie utilizzate ed architettura;
    - librerie e dipendenze;
    - EOL delle tecnologie utilizzate.
- **Dati**, che comprende:
    - volumi in uso;
    - frequenza di utilizzo e configurazioni.
- **Business**, che comprende:
    - stakeholders del sistema;
    - frequenza di rilascio;
    - criticità del sistema.

L'insieme di queste informazioni permette all'organizzazione di poter pianificare e valutare gli interventi necessari sulla base di riscontri oggettivi, sia che si parli di un software che di infrastruttura o conformità ad uno standard (per maggiori dettagli sulla modellazione, si consulti la scheda di Agid).

4.3.3 Assessment organizzativo

Partendo dalle matrici organizzative, dalla suddivisione delle competenze e delle responsabilità all'interno dell'organizzazione è possibile scendere di livello e mappare i processi, le funzionali aziendali, i partner e i fornitori eventualmente coinvolti.

È utile in questa fase analizzare con un atteggiamento critico il livello di comunicazione presente tra i vari uffici e ipotizzare i possibili referenti, per ogni ufficio, da coinvolgere per le attività inerenti alla

Trasformazione Digitale. In alcuni casi può risultare utile impostare un modello di alto livello che sia direttamente legato agli obiettivi da raggiungere e lavorare ad una mappatura, sulla base delle responsabilità dei diversi dipartimenti ad oggi presenti e delle competenze tematiche maturate, con gli stakeholder che possono agevolare il progetto di trasformazione.

L'organizzazione target potrebbe, in questi casi, emergere a valle dell'analisi del modello attuale lavorando sulle direttrici di ambito.

Direttrici di Ambito	Descrizione
Ecosistema, Utenti e altre PA	✓ L'attuale modalità di lavoro prevede interazione con l'ecosistema di partner, di enti e altre PA? ✓ Come gestisco oggi queste modalità? ✓ Quanto è importante, per le dimensioni, business e ruolo istituzionale, individuare un responsabile per allineare la trasformazione e la sua comunicazione con soggetti terzi esterni all'amministrazione stessa?
Strategia	La relazione con AgID, con Consip, con il Dipartimento per la Trasformazione Digitale è uno dei fattori chiave per il successo della migrazione in Cloud. La revisione dell'organizzazione dovrà tenere conto di questi ambiti di attività e responsabilità al fine di governare in maniera efficace l'evoluzione del programma.
Delivery Prodotti/Servizi	L'esperienza concreta di Istituti come l'INAIL, può consentire di mettere a fattor comune il contributo sulla centralità del prodotto nella visione IT dell'organizzazione. Rivedere i servizi che l'amministrazione eroga e progettare i nuovi, in chiave evolutiva, secondo la "logica a prodotto" può supportare: ✓ la governance delle attività; ✓ definire le responsabilità sia interne che esterne (fornitori); ✓ mappare il budget e le nuove iniziative in maniera meno ambigua; ✓ ottimizzare il ciclo di vita dei prodotti ed evitare ridondanze. Lo stesso modulo applicativo o servizio potrebbe essere stato sviluppato più volte, coprendo requisiti potenzialmente diversi, con tecnologie diverse, semplicemente per la mancanza di questa visione di prodotto; ✓ comunicare in maniera più efficace. A titolo di esempio, il responsabile di prodotto (product owner) dell'applicazione o del servizio IT di "Gestione Pratiche" può interagire con i responsabili funzionali o di business su un perimetro chiaro e condiviso senza dover rintracciare le funzionalità o le applicazioni tra vari referenti e fornitori per valutare l'impatto che un nuovo requisito può avere su un "prodotto".
DevOps & Operations	I dipartimenti/uffici che hanno una responsabilità in termini di Infrastrutture, Operations, Applicazioni e Qualità del software devono facilitare un approccio DevOps per consentire benefici tangibili dal processo di innovazione tecnologica derivante dal Cloud. Per consentire la diffusione di queste Best Practice è possibile definire un riferimento (all'interno dell'organizzazione di ogni ufficio) che giochi il ruolo di DevOps "Ambassador" e supporti la definizione delle linee guida, veicoli le buone pratiche all'interno dell'ufficio e si coordini con gli altri uffici per stabilire tempi, modi, sperimentazioni, per consentire un nuovo modo di lavorare.

	Il comitato costituito dai DevOps Ambassador potrà, grazie alla competenza specifica e al contributo dei singoli, definire le modalità di ingaggio dei fornitori e le caratteristiche delle forniture da richiedere nei capitolati tecnici di gara per consentire che il lavoro, all'interno dell'Amministrazione, possa essere svolto in modalità agile & DevOps.
Gestione dei Costi & Analytics	La trasformazione digitale porta con sé un nuovo modo di concepire il TCO e gestire lo spending IT. Il paradigma **pay-per-use**, tra gli aspetti caratterizzanti del Cloud ✓ comporta il passaggio di alcune voci di spesa da **Capex** in **Opex**; ✓ implica nuove responsabilità sulle architetture dei servizi IT che concorrono in maniera diretta alla **composizione dell'importo** in fattura; ✓ favorisce l'**allocazione rapida di risorse** ed infrastrutture, anche da parte di team di sviluppo; ✓ richiede attenzione sulla gestione di un insieme di risorse virtualmente infinite (si pensi ai servizi di Cloud Pubblico dei principali hyperscaler). Questo rappresenta un cambio di mentalità, rispetto al modello tradizionale, dove l'attivazione di nuove istanze, laddove possibile, sullo stesso hardware, poteva non comportare in maniera diretta e istantanea un aggravio della spesa.
Sicurezza, Technology Management & Centri di Competenza	Il driver tecnologico, seppure non sia il solo elemento, rimane centrale nella trasformazione verso il Cloud. Questo cambiamento porta a rivedere skills e competenze a vari livelli dell'organizzazione e spesso è utile definire dei focus group, dei focal point e dei **Centri di Competenza** che consentano alle varie anime, presenti nell'organizzazione, di procedere in maniera coordinata e sinergica.
Hybrid Cloud Platform & Enabling Technology	La focalizzazione sul Cloud ibrido richiede una "nuova" prossimità tra competenze ed uffici di infrastrutture e applicativi che, si troveranno a confrontarsi quotidianamente su tematiche relative al design, alla progettazione, alle architetture, allo sviluppo, all'esecuzione e all'analisi delle performance di piattaforme Cloud. La necessità di governare in maniera efficace ed efficiente gli ambiti comporta un passo di avvicinamento tra ambiti e responsabilità che, verosimilmente, in passato hanno seguito delle logiche **a silos**.

4.3.4 Gli elementi fondamentali per un progetto di successo

Il completamento della fase di Assessment con esito positivo è fondamentale per approcciare alle successive fasi di progettazione e migrazione.

Il primo elemento di successo, in questa specifica fase, è legato alla qualità delle informazioni disponibili nelle diverse sorgenti e alla **coerenza** tra asset, inventory, cmdb, Enterprise Architecture.

Il secondo elemento di successo è la **disponibilità** di tutti gli stakeholder a fornire le informazioni utili da un punto di vista architetturale, infrastrutturale, applicativo e di business.

Ultimo fattore chiave è rappresentato dalla sponsorship da parte della Direzione. La visione strategica deve essere accompagnata, soprattutto nelle prime fasi, con una forte convinzione, con un piano di comunicazione efficace e con una linea di investimenti adeguata alle necessità e alle diverse fasi attraverso le quali si svilupperà il percorso di Trasformazione Digitale.

Impostare il lavoro, fin dalle prime fasi, con un ecosistema di partner tecnologici di esperienza consente di prevenire gli inciampi che fisiologicamente possono incontrarsi in questo "journey to the cloud".

4.4 Modello di modernizzazione

Una volta definito il quadro e gli obiettivi strategici del viaggio verso il cloud ed effettuato l'assessment organizzativo, tecnologico ed applicativo, un passo importante è effettuare scelte tecnologiche e architetturali coerenti con strategia e vincoli tecnici.

Si è quindi ritenuto utile proporre di affrontare il tema delle scelte tecnologiche, attraverso modelli di modernizzazione e di raccordo tra scelte tecniche e strategiche, e una linea guida sulle opzioni e i criteri di scelta delle architetture di riferimento To-Be in un contesto in generale multicloud.

4.4.1 Le sfide da affrontare

Innanzitutto, si intende brevemente inquadrare il contesto in cui oggi una PA è chiamata fare le scelte tecnologiche di fronte a due spinte correlate l'**evoluzione delle aspettative di cittadini ed imprese**, da un lato, e la r**apida evoluzione tecnologica** dall'altro.

Per quanto riguarda l'**evoluzione delle aspettative di cittadini ed imprese** va fatta la ovvia considerazione sull'esperienza digitale che ciascuno di noi ha nel contesto della "Digital Economy". Questo ha alzato e alza inevitabilmente le aspettative sui servizi digitali delle PA, imponendo una profonda ristrutturazione, in un'ottica di centralità dell'utente e integrazione/interoperabilità dei servizi (network economy). Per comprendere il senso di urgenza e l'inevitabilità di questa trasformazione pensiamo al fenomeno delle segnalazioni dei cittadini sui social dei disservizi e/o malfunzionamenti e dell'ascolto delle amministrazioni di questo canale che diventa spesso più efficace di quello istituzionale.

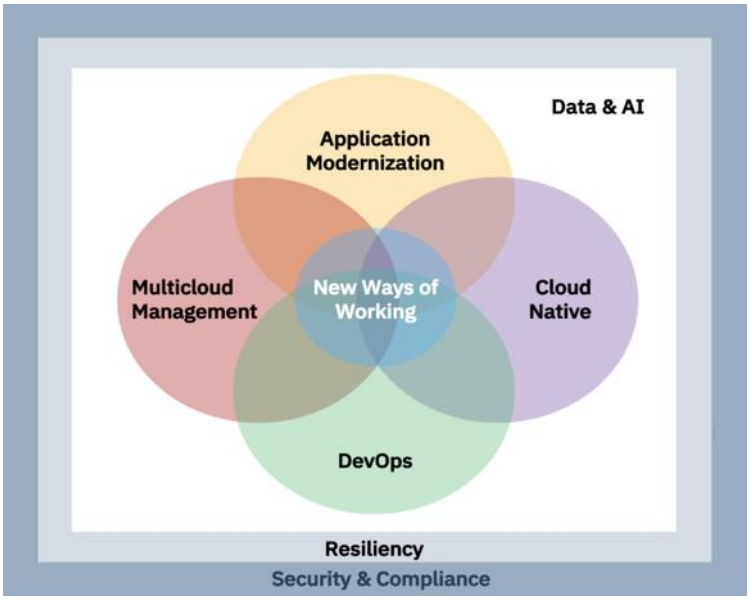
In questo senso si evidenziano alcuni elementi peculiari delle linee guida AgID:

1. il **disegno dei servizi User Centric** utilizzando per esempio i framework inspirati al design thinking di IT.DESIGN ed IT.DEVELOPERS;
2. l'adozione di un modello **API FIRST** nel disegno e nella modernizzazione delle applicazioni, per essere pronti alla **interoperabilità dei servizi** prevista dal modello strategico di evoluzione dei servizi della PA indicato nel piano piano triennale 2020-2022.

In ambito tecnologico le amministrazioni come tutte le organizzazioni subiscono o cavalcano le opportunità e minacce dell'emergere convergente di **tre tecnologie dirompenti: Cloud, Containers e sviluppo a microservizi.** Questo ha **completamente cambiato la traiettoria di sviluppo ed erogazione dei servizi** basati su applicazioni di nuova generazione le cosiddette "applicazioni cloud native".

Nel guardare a questo fenomeno in rapidissima e apparentemente caotica trasformazione tecnologica, le amministrazioni non possono tener conto, in ottica di semplificazione della complessità, che è in atto una forte polarizzazione delle tecnologie su alcuni ecosistemi di sviluppo open-source che possono garantire risparmio e portabilità.

In questo contesto, sicuramente, non mancano per le PA opportunità di mercato e linee guida sullo sviluppo dei nuovi servizi (IT.Designers, IT.Developers,….) secondo i nuovi paradigmi, dall'altro, mentre sicuramente assai più **complesso è gestire in modo olistico la trasformazione dei servizi esistenti ed i relativi processi di gestione.**



Disegnare un quadro coerente in cui si "modernizza" il parco applicativo esistente, si fanno evolvere le infrastrutture verso architetture cloud ready, si cambiano i processi di gestione, si adottano i nuovi pattern architetturali cloud native a microservizi e ci si prepara ad essere multi-cloud evitando lock-in, **è molto complesso.**

Questo percorso richiede, infatti, un insieme di skills e competenze che una PA difficilmente ha al suo interno e che, allo stesso tempo, è rischioso delegare **totalmente** a soggetti esterni.

La prima grande questione e sfida è dunque a **quale team affidare il disegno e l'esecuzione del programma** di trasformazione.

La risposta a questa domanda varia ovviamente da amministrazione ad amministrazione.

Ad esempio, una grande amministrazione come INAIL ha affrontato questo problema costituendo un centro di competenza devops, dove ha messo insieme competenze multidisciplinari, sotto una forte guida e leadership interna, in grado di governare il quadro complessivo. Ha pensato un programma che si articola nel ridisegno e automazione delle toolchain per devops, nella definizione di pattern architetturali standard a microservizi per le nuove applicazioni cloud native, nella costituzione di un layer di interoperabilità per il multi-cloud e di una migration factory per la modernizzazione applicativa.

Una amministrazione più piccola potrebbe affrontare la sfida della complessità in un modo diverso, scegliendo un punto di partenza e un approccio per progetti sequenziali come per esempio adozione pratiche Devops, adozione di architetture Cloud Native per i nuovi sviluppi e modernizzazione delle applicazioni esistenti, oppure al contrario Modernizzazione delle applicazioni, adozione architetture cloud native per i nuovi sviluppi. La scelta del punto di partenza dipende in generale dalla priorità delle attuali criticità.

In un contesto di variabilità di requisiti probabilmente DevOps e l'adozione di architetture cloud native potrebbero essere la priorità, al contrario, in caso di elevati costi di gestione e manutenzione degli attuali ambienti legacy un percorso di modernizzazione applicativa su container potrebbe essere il punto di partenza più opportuno.

Sia che si adotti un approccio di programma o quello di sequenza di progetti, è bene almeno ad alto livello disporre di un quadro complessivo della trasformazione come modello To Be e dei passi necessari per realizzarlo. In tal senso è utile avere un modello di riferimento complessivo come quello descritto nel successivo paragrafo.

4.4.2 Adozione di un modello di riferimento

Molteplici modelli di riferimento sono disponibili e pubblicati da diverse organizzazioni pubbliche e private. In questo contesto si presenta il modello di riferimento utilizzato in INAIL che è frutto di un adattamento dei modelli disponibili.

Il modello prevede che si parta da obiettivi strategici espressi in termini di Key Performance Indicator misurabili analiticamente o qualitativamente, si attui un assessment sulle applicazioni e infrastrutture esistenti in termini di Cloud Readiness (vedi §4.3), si scelgano e si attuino i pattern di modernizzazione applicativa all'interno di una migration factory (vedi §4.6 e 4.7) che è un insieme di competenze, ambienti e tools, si disegnino gli ambienti target in ottica multi-cloud della migrazione o "landing zone" (vedi §4.5) adottando le pratiche e gli strumenti DevOps (vedi §4.7).

Gli obiettivi strategici, in linea anche con quanto espresso al §4.1, ricadono nelle classi di Innovazione, Produttività, Efficienza e Resilienza e sono un fondamentale passo per indirizzare in modo corretto lo scopo della trasformazione, la prioritizzazione del piano di esecuzione dei pattern di migrazione e il disegno degli ambienti della landing zone.

Questo è particolarmente vero per le medie e piccole amministrazioni che attraverso una chiara e puntuale definizione di pochi, ma rilevanti obiettivi, possono focalizzarsi sugli elementi realmente a valore, circoscrivendo e prioritizzando lo scopo della migrazione in termini di portfolio applicativo/servizi, di pattern di migrazione e di ambienti target da utilizzare.

4.5 Scelte architetturali per gli ambienti di deployment (*landing zone*)

I pattern di migrazione come descritto nel modello di riferimento hanno ciascuno una "landing zone", che occorre sia in definita in base a vincoli tecnici, scelte architetturali, strategiche ed economiche.

In questo paragrafo sulla base delle esperienze emerse dal tavolo di lavoro organizzato da FPA, verrà data una guida orientativa, ma necessariamente non esaustiva, alle alternative tecniche e alle scelte architetturali possibili, che consentano di mantenere un quadro di allineamento tecnico, economico e strategico.

Ogni pattern di migrazione ha in realtà una o più zone di atterraggio possibili. Le "Landing Zone" saranno descritte fornendo alcuni approfondimenti allo scopo di supportare le opportune scelte.

Tornando agli esempi riportati nel paragrafo precedente possiamo immaginare un caso di amministrazione che decida che parte del suo portfolio, con le applicazioni custom mission critical, sia riscritto su una piattaforma PaaS di orchestrazione container, che alcune funzioni trasversali come IT Service Management siano in SaaS, che il resto del portfolio è containerizzato su piattaforma di orchestrazione container e/o spostato su ambienti virtuali Software Defined e che infine tutte le applicazioni utilizzano servizi di Intelligenza Artificiale per miglioramento dell'interazione utente (chatbot) e sistemi di discovery e advisor per i processi di back-end.

Questo pone due grandi questioni, tra esse correlate: la prima riguarda la scelta della landing zone tra quelle di seguito descritte, mentre la seconda riguarda il disegno di un'architettura di riferimento di integrazione e interoperabilità tra le diverse landing zone in un contesto multicloud.

4.5.1 Applicazioni as a Service (SaaS)

L'adozione dei servizi SaaS è indicata e favorita dalle linee guida di adozione cloud dell'AgID e nel cloud enablement è esplicitamente suggerito di **valutare prioritariamente la sostituzione in ottica di Replacement** di soluzioni on premise custom e/o basate su package vendor inadeguate con soluzioni SaaS.

In effetti ad oggi nel Cloud Market Place le offerte in SaaS è la categoria più numerosa e copre oltre 400 offerte dei principali vendors, di CSP qualificati e operatori di soluzioni verticali. Questo fa sì che l'offerta copra i principali processi trasversali come office&communication, ERP, IT Service Management e alcuni processi verticali specifici in particolare per sanità, università ed enti locali.

Alcune amministrazioni potrebbero trovare una risposta esaustiva alle proprie esigenze con un'offerta SaaS magari multivendor, molte hanno adottato e/o stanno adottando servizi SaaS per i processi trasversali no-core.

I punti di fondamentale attenzione nella adozione di questa opzione sono:

1. attenta valutazione dell'adeguatezza dell'opzione di configurazione e/o di toolkit di sviluppo rispetto alle proprie esigenze di customizzazione;
2. facilità di integrazione ed interoperabilità che andrà valutata in termini di **API di integrazione**;
3. modalità di uscita dal rapporto di fornitura e switch-off ad altro fornitore con particolare attenzione alla retention ed export dei dati da testare preliminarmente all'avvio del servizio;
4. costi della soluzione che generalmente crescono linearmente con gli utenti ed i dati trattati.

La maggior parte delle **soluzioni SaaS sono in ambienti di Public Cloud** molti vendors offrono una variante di private tenant che garantisce in generale migliori SLA e policy di sicurezza.

4.5.2 Piattaforme tecnologie esponenziali (SaaS-PaaS)

Si definiscono tecnologie esponenziali quelle che consentono, attraverso la loro adozione all'interno dei processi, un salto nei livelli di efficacia ed efficienza attraverso dei cosiddetti "**Intelligent workflow**". In sostanza si sta parlando della possibilità di arricchire i workflow dei processi operativi, con le possibilità di automazione intelligente e strumentata messe a disposizione da queste tecnologie (es. Artificial Intelligence, IoT, Blockchain, Mobile, Robot Process Automation).

Pensiamo, ad esempio, all'apertura di una richiesta supportata da un chatbot. Questo compila per l'utente, direttamente sui sistemi operazionali, la richiesta grazie all'integrazione del workflow gestione richiesta con servizi di Natural Language Processing e Robot Process Automation.

Le tecnologie esponenziali sono messe a disposizione dai principali vendor sotto forma di piattaforme, che possono essere classificate a seconda dei casi come servizi SaaS (invocabili via API) o PaaS verticali (boiler plate pre-integrati di sviluppo con tutte le componenti necessarie).

L'esperienza d'uso di queste piattaforme, indica che **utilizzare queste piattaforme minimizza il codice da sviluppare e di conseguenza il rischio di lock-in sul vendor e abilita una rapida prototipazione.** Questo consente di focalizzare gli sforzi e gli investimenti negli aspetti più critici, quale le modalità di inserimento di queste tecnologie nei processi e la valutazione dei risultati.

Un ulteriore categoria di servizi PaaS-SaaS sono le piattaforme di analisi dati fornite in cloud, che vanno dagli strumenti tipici di Business Intelligence a piattaforme che supportano in modo integrato e semplice le attività tipiche del data scientist: quali ingegnerizzazione e raffinamento delle pipeline dati, di costruzione di modelli di analisi e presentazione dei risultati.

AgID Cloud Market Place offre una moltitudine di offerte dei principali vendors, sia in termini di piattaforma di sviluppo che di dashboard per soluzioni verticali in diversi ambiti. Come esempio si cita il servizio Google Web Analytics, per l'analisi del traffico di un sito web, che è espressamente suggerito dalle linee guida di IT.Developers a supporto della User Centric Design.

Una considerazione finale lo meritano gli ambienti di sviluppo **Serverless** che si sta imponendo come architettura nativa del cloud e che consente di trasferire il più alto livello di responsabilità operative al cloud provider, consentendo all'amministrazione di concentrarsi nella definizione del modello di servizio e nello sviluppo delle relative funzioni. Questa tecnologia consente di sviluppare le funzioni applicative in più linguaggi, di creare ed eseguire applicazioni e servizi senza dover gestire alcun server, eliminando le attività di gestione e manutenzione delle infrastrutture.

Gli scenari applicativi implementabili sono molteplici e particolarmente adatti alla creazione di applicazioni mobile, IoT, integrazione di servizi di back-end esposti via API.

4.5.3 Piattaforme di orchestrazione container (PaaS)

La tecnologia a container è diventata la tecnologia di riferimento nei percorsi di modernizzazione applicativa, in quanto consente semplificazione e consolidamento delle infrastrutture, portabilità su diversi ambienti di deployment e semplificazione della gestione di ambienti eterogenei.

Questo ha determinato l'affermarsi delle piattaforme di orchestrazione dei containers, che consentono di gestire in modo efficace deployment, scalabilità, monitoraggio e connettività di e tra containers.

La piattaforma che più di altre si è affermata in questo contesto è **Kubernetes**: un grande ecosistema di orchestrazione container aperto, che sta garantendo a chi l'utilizza un mainstream continuo di evoluzione e innovazione.

Questa evoluzione alimentata dal vasto ed eterogeneo ecosistema di sviluppo sta rendendo questa piattaforma un ambiente utilizzabile trasversalmente per applicazioni tipicamente cloud native di nuova generazione e quindi idealmente ai "12-factors" (vedi https://12factor.net/), ma anche ad applicazioni che necessitano di funzioni tipiche degli application server e magari sono frutto di una containerizzazione di applicazioni statefull (replatforming).

La sua diffusione fa sì che sia disponibile sia per soluzioni on premise con diverse distribuzioni, sia su cloud pubblico (PaaS managed or unmanaged), questo consente la possibilità di scegliere in modo flessibile gli ambienti di deployment, le modalità operative di gestione e soprattutto evita ogni vendor lock-in.

Nel caso INAIL questa "landing zone" è stata scelta per tutte quelle applicazioni in cui c'è, o c'è stato, un importante investimento in sviluppo, sono mission critical e sono candidate alla modernizzazione secondo i pattern di Re-architect/Re-factor/Re-Platform su container.

4.5.4 Ambienti virtualizzati on demand (IaaS)

Nell'assessment applicativo per alcuni workload potrebbe essere opportuno operare un puro "lift&shift" riducendo al minimo gli interventi applicativi.

Questo richiede una "landing zone" che sia compatibile con quella di partenza e quindi un ambiente IaaS configurabile su tenant private o public, in relazione ai requisiti degli applicativi.

Questa modalità è particolarmente utile quando per alcuni workload e scenari di test e sviluppo si vuole costituire delle capacità addizionali di risorse computazionali on demand sul cloud.

4.5.5 Servizi DR, Backup, Security (RaaS)

Trasversalmente ai diversi pattern di migrazione, è opportuno considerare come affrontare il tema della resiliency in un ambiente multicloud e questo comprende sia le applicazioni migrate verso le diverse landing zone, sia quelle per cui l'opzione scelta è Retain.

I servizi più diffusi in questo ambito sono DRaaS (Disaster Recovery as Service) e BaaS (BackUp as Service) che sono ampiamente presenti nel AgID Cloud Marketplace.

In generale l'adozione di un servizio cloud in questo ambito è vantaggiosa in termini di costi e tempi di setup, ma va disegnata e valutata attentamente rispetto agli obiettivi di resilienza e sicurezza dell'organizzazione.

4.6 Criteri per il disegno di un'architettura integrata e interoperabile

Date le opzioni di landing zone, in relazione ai pattern di migrazione emerge un quadro che spesso conduce a scelte multi-cloud-multiusi, per rispondere alle diverse esigenze e pattern di modernizzazione del portfolio applicativo.

A titolo esemplificativo si riporta il caso di INAIL, in cui la strategia multi-cloud-multiusi è stata rappresentata con una piramide.

Al centro della piramide c'è la scelta di una piattaforma di orchestrazione container basata su Openshift Container Platform (OCP), per tutte le applicazioni mission critical, al fine di valorizzare gli investimenti presenti e futuri. Questa piattaforma è la landing zone, sia per le applicazioni che seguono il pattern di migrazione di Re-Architect, che per quelle che sono quelli di Re-factoring e Re-platforming. La scelta iniziale è di collocare la piattaforma in un private cloud on premise per semplificare l'integrazione con il resto degli ambienti legacy, ma l'architettura scelta consente il paradigma di **runanywhere** delle componenti applicative distribuite.

Alla base della piramide ci sono due elementi fondamentali e complementari alle applicazioni mission critical che sono:

- specifiche applicazioni isolabili e con workload variabile nel tempo che possono essere collocate su specifici tenant con risorse computazionali on demand;
- servizi SaaS ampiamente utilizzati da INAIL nei processi di supporto.

Al vertice della piramide ci sono cloud specializzati sulle diverse piattaforme, per lo sviluppo di soluzioni basate su tecnologie esponenziali come IoT.

La scelta multi-cloud-multiusi ha diversi archetipi di soluzione che ricadono in uno spettro che può essere rappresentato da un lato in "ambienti separati" e dall'altro in "piattaforma ibrida integrata".

Il costruire uno strato di integrazione consistente per gli ambienti on premise e off premise privati e pubblici, offre importanti vantaggi in termini di servizi/prodotti erogabili e della loro gestione consistente ed end to end. Ma è di contro necessario un consistente sforzo di integrazione tecnologico e di processo.

Per questa ragione spesso la partenza è da ambienti operativi separati. Spesso un'architettura ibrida è comunque necessaria per integrare le applicazioni containerizzate (Re-architect e/o Re-platforming), con gli ambienti legacy. In questi casi la raccomandazione è di adottare un'unica piattaforma di orchestrazione container basata su quello che oggi è l'ecosistema opensource di riferimento (Kubernetes) per le ragioni spiegate nel § 4.5.3.

Nel caso di INAIL è in corso di disegno e realizzazione di un layer di interoperabilità che prevede l'erogazione di alcuni servizi trasversali:

- API Management con costituzione di un unico catalogo logico per le Outer API ad uso interno ed esterno.
- Multicloud Management con funzioni di workload e cost management integrate.
- Security e compliance con un unico sistema di accesso e gestione della sicurezza, tracciatura applicativa ed auditing.

4.7 Modalità operative: paradigmi Agile & DevSecOps

La realizzazione dei pattern di migrazione necessita l'utilizzo coordinato di tools, ambienti di sviluppo e collaudo (migration factory), definizione di modalità operative e pianificazione.

Partendo dalle esperienze delle amministrazioni partecipanti al tavolo di lavoro di FPA e, in particolare, di INAIL, è possibile individuare un "*filo rosso*" che collega la necessità di ripensare il software secondo una **logica a prodotto** e le metodologie Agile & DevOps, con i relativi impatti anche a livello di organizzazione aziendale.

La parola prodotto è nata attorno al concetto di product owner scrum, ragionando sull'idea che il software è affidato a qualcuno che se ne prende cura ed è pensato per qualcun altro che, utilizzandolo, ne finanzia in qualche modo i suoi costi.

Il product owner come da metodologia Scrum ha ambiti più tattici: è qualcuno a cui è affidata la gestione del product backlog e, nel framework, ha il compito di aiutare i team a sviluppare software secondo le attese dei suoi clienti. Il prodotto tuttavia ha anche bisogno di una gestione manageriale, di qualcuno che sviluppi una strategia su di esso, definendone le relative politiche di investimento. La figura del capo progetto ha una visione legata a interventi sul prodotto che richiedono coordinamento, se particolarmente complessi. Le sue responsabilità in «agile» sono affidate a più ruoli.

Il concetto di prodotto aiuta a ripensare una organizzazione come una realtà che offre servizi a consumo, secondo modelli di pagamento «pay per use», e lo fa riorganizzandosi internamente, secondo le medesime logiche.

Per esempio, una API in INAIL, come può essere quella che gestisce l'evento infortunistico, è un prodotto il cui consumo può essere monetizzato utilizzando le metriche collezionate da un API Gateway.

Una VM, o un database, è un prodotto on premise che può essere pubblicato a catalogo IaaS o PaaS enterprise con i suoi indicatori di costo, analogamente a quanto accade per le risorse offerte dai cloud provider pubblici. Lo sviluppo di un prodotto X potrà a sua volta utilizzare tali prodotti IaaS o PaaS attingendo a risorse economiche associate al budget del prodotto X stesso.

Quanti «componenti» deve avere una applicazione e quanto devono essere «micro»? Quanti uffici deve avere un'Amministrazione per funzionare meglio? Uno, due o quarantacinque? Avere un solo ufficio molti problemi li risolverebbe, ma può un solo ufficio reggere la complessità dell'intera gestione? A volte tuttavia avere 45 uffici aggiunge una complessità di plastica a una realtà che potrebbe essere più semplice, di suo.

Con le applicazioni a componenti distribuite accade la stessa cosa. Ogni ufficio, così come ogni «componente», è un monolite e quindi esiste una qualche realtà ACID, tuttavia è un lavoro complesso dimensionarlo correttamente in termini di responsabilità e di risorse, ovvero pensandolo come parte di un mondo più vasto (che sia l'Ente o una applicazione, il discorso è analogo).

> *"Any organization that designs a system (defined broadly) will produce a design whose structure is a copy of the organization's communication structure"*
> (Conway's Law, 1967)
>
> *"If you have four groups working on a compiler, you'll get a 4-pass compiler"*
> (Eric S. Raymond, 1996)

A questo punto, la distribuzione di una app in componenti diventa una necessità quando i problemi che questa app deve gestire sono complessi: è qui che l'architettura a (micro)servizi trova la sua ragione d'essere, ma una distribuzione effettuata con poco criterio introduce complessità senza portare vantaggi.

4.8 Definizione degli scenari evolutivi dei Servizi

In un approccio IT Tradizionale, la responsabilità dell'intero stack IT e dei servizi associati è demandata all'organizzazione: suo, infatti, è il compito di gestire il datacenter secondo le normative e gli standard vigenti, coordinare responsabilmente le attività di conduzione di facilities, manutenzione di macchine e apparati, installazione e patch di sistemi operativi e software nonché le attività di gestione dei sistemi applicativi e dei dati annessi.

L'adozione del cloud e l'utilizzo dei suoi servizi porta tuttavia ad un nuovo approccio basato sulla gestione condivisa delle risorse dello stack: a seconda del tipo di servizio richiesto infatti, la responsabilità della corretta fruizione di una parte di componenti e risorse associate al servizio viene affidata al gestore del cloud provider. La tipologia di risorse che viene associata a questo cambio di paradigma, tuttavia, dipende dal servizio richiesto, a seconda che si tratti di IaaS, PaaS o SaaS:

- In un servizio IaaS, il Cloud provider è responsabile della corretta erogazione delle risorse, a partire da quelle infrastrutturali fino all'installazione del sistema operativo: diviene quindi onere del cloud service provider che i Datacenters e le risorse (macchine e apparati) su cui si basano i servizi siano collegati, disponibili, scalabili, sicuri e configurati.
- In un servizio PaaS, oltre alle caratteristiche di un servizio IaaS, vengono gestiti anche gli aspetti relativi al middleware e al runtime dei sistemi: in questo caso, l'organizzazione deve preoccuparsi solo degli aspetti legati allo sviluppo dell'applicazione, del deploy e dei dati, mentre la configurazione del middleware, la sua affidabilità, le configurazioni per garantire affidabilità e scalabilità sono gestite dal Cloud Service Provider.
- In un servizio SaaS, le responsabilità dell'organizzazione si basano sulla corretta configurazione del servizio stesso; la gestione delle applicazioni sottostanti, la disponibilità delle applicazioni sono invece onere dei Cloud Service Provider.

Per quanto riguarda gli aspetti legati alle SLA, la sicurezza e la compliance dei servizi, il nuovo paradigma di gestione condivisa per i servizi cloud porta quindi le organizzazioni ad adottare un "**Modello a responsabilità condivisa**".

Questo modello è volto a garantire la corretta fruizione dei servizi assegnando al provider della piattaforma Cloud pubblica la responsabilità della messa in sicurezza e gestione delle risorse associate ai servizi Cloud utilizzati; tuttavia la gestione degli accessi, il corretto utilizzo di best practices, la loro manutenzione e conformità nell'applicazione delle policy, rispetto a quelle imposte, sarà invece in mano all'organizzazione che ne usufruirà.

Dal punto di vista di erogazione del servizio, è importante sottolineare l'aspetto legato al corretto utilizzo e conformità rispetto agli standard dichiarati dal cloud provider; sebbene tramite l'utilizzo di un certo servizio venga garantito un certo grado di scalabilità e affidabilità, il mancato uso di architetture, pattern e best practices che non rispecchino principi di scalabilità, performance, può incidere in maniera negativa sulle prestazioni del servizio stesso.

4.9 Modello di IT Governance

4.9.1 Il necessario legame con la strategia di Trasformazione Digitale

In un'era caratterizzata dalla **trasformazione digitale** è ormai un dato di fatto come questa porti alla semplificazione e alla creazione di nuove opportunità di business, oltre che ad un maggior valore per gli utenti finali.

In questo contesto, il percorso avviato da alcune PA è perfettamente in linea con la propria roadmap di trasformazione strategica e prevede l'adozione di paradigmi di sviluppo moderni (e.g., metodologia Agile), supportati dall'introduzione di ecosistemi Cloud (sia on-premises, che pubblici), processi self-service e pratiche DevOps.

Tali cambiamenti, in un'organizzazione IT strutturata per offrire servizi erogati da infrastruttura tradizionale, aumentano inevitabilmente la complessità gestionale e operativa (e.g., introduzione di nuove tecnologie, stratificazione delle architetture).

Poiché le maggiori opportunità risiedono nell'efficienza operativa e nello snellimento procedurale, un percorso strategico che abiliti rapidamente il valore e i benefici del Cloud prevede l'*industrializzazione* complessiva dei processi di delivery e operations di applicazioni e servizi.

Per offrire adeguato supporto all'evoluto ecosistema di tecnologie, fornitori e utenti (interni ed esterni), tra gli obiettivi primari del presente documento c'è l'individuazione delle **capability IT** necessarie a rendere il **modello operativo** capace di veicolare iniziative **multi-modali** (Waterfall, Agile, mixed) verso un ecosistema IT altamente ibridizzato ed eterogeneo (infrastrutture, architetture, tecnologie).

Tre pillar alla base della Trasformazione verso un IT Ibrido e Multi-Modale

L'adozione di un **nuovo modello operativo IT** non può prescindere da uno shift verso un **paradigma *service-based***, il quale si riflette su strategie, metodologie, skill-set e governance IT.

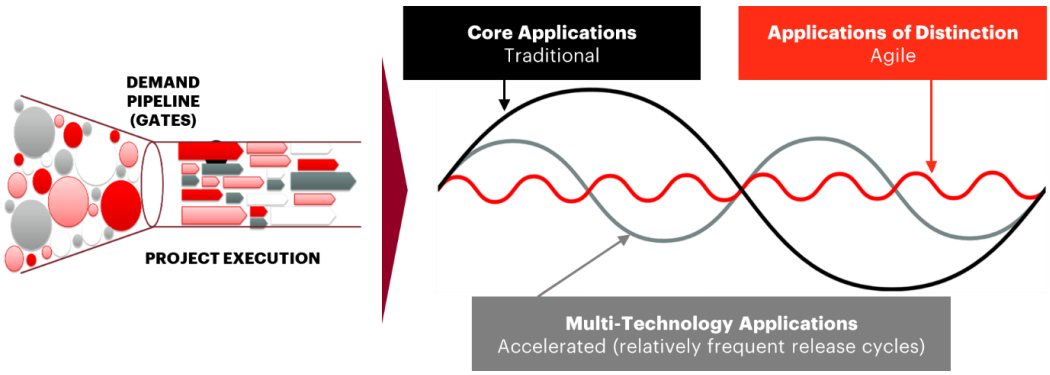
Valutare in aggiunta anche gli adeguamenti organizzativi è un **fattore chiave** per una **trasformazione di successo**, la quale – come è evidente – non è *solo* una trasformazione tecnologica, ma un vero e proprio *shift* culturale, richiede opportuno **supporto organizzativo** per una realizzazione efficace ed armonica.

4.9.2 Modello operativo IT multi-modale

Un modello operativo IT fornisce una rappresentazione astratta di come un'organizzazione opera per eseguire la propria strategia IT a supporto del business. Per fare un esempio, così come accade per le organizzazioni IT solide, il modello operativo IT tradizionale INAIL è ben definito, in quanto è stato sperimentato, testato e migliorato nell'arco di un periodo di tempo considerevole e con il contributo delle diverse aree, interne ed esterne, che operano in questo ambito.

In tale contesto, l'adozione del Cloud, di metodologia Agile e di pratiche DevOps rappresenta una vera e propria trasformazione, la quale chiede di ripensare e adeguare l'approccio tra persone, processi e tecnologie, con l'obiettivo di massimizzare i vantaggi offerti dalla *nuova IT*. Di conseguenza, approcciare il Cloud con il medesimo modello operativo impiegato nel data center tradizionale significa rischiare di fallire o di ottenere pochi benefici.

In presenza di una solida componente di IT tradizionale, per realizzare un'adozione completa, gestita e controllata del paradigma Cloud, è opportuno innanzitutto riconoscere la **necessità (e spesso l'opportunità) del business di consumare l'IT a *diverse velocità***.



Il modello operativo IT deve essere ridisegnato per consentire la coesistenza di diverse tipologie di iniziative

Adeguare il modello operativo ad un business multi-modale è un prerequisito indispensabile per garantire che ciascuna iniziativa sia controllata da team capaci di applicare le proprie competenze, mediante opportune tecnologie e governance solida. Nasce così la necessità di avviare la trasformazione verso un ***modello operativo IT multi-modale***.

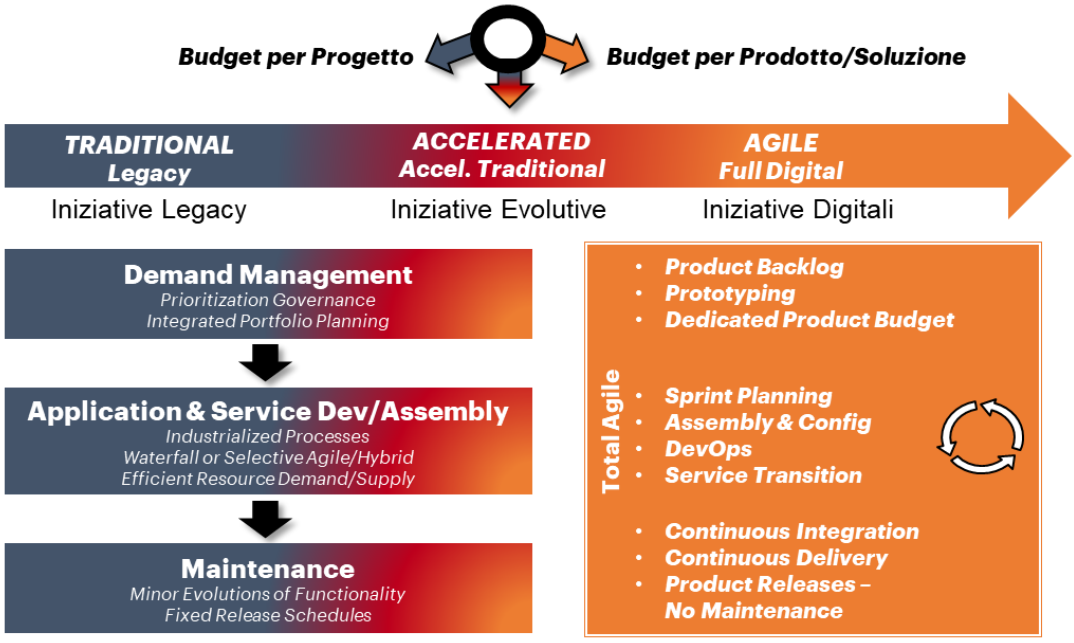
IL FRAMEWORK

Un modello operativo IT in grado di supportare tipologie di iniziativa diverse, implica cambiamenti strutturali alle funzioni IT e richiede che ciascuna iniziativa di business venga indirizzata correttamente.

La coesistenza di ecosistemi così profondamente diversi, e la necessità di supportare sia le iniziative di business di natura più agile, che i progetti più tradizionali, porta di fatto alla creazione di un **Framework** (cfr. figura seguente) a supporto delle diverse modalità/velocità delle varie iniziative di business:

1. **Traditional:** Legacy Business / Core Applications
2. **Accelerated**: Evolving Business / Multi-Technology Applications
3. **Agile**: Digital Business / Application of Distinction

Uno schema di questo tipo si pone l'obiettivo principale di far comprendere la logica evolutiva dal tradizionale/legacy verso i progetti digitali tipicamente sviluppati in modalità Agile. Questo modello deve poter supportare l'Istituto nel cambiamento, introducendo il concetto di accelerazione, partendo dai progetti tradizionali. È importante definire un approccio e una relativa tassonomia che supportino l'Amministrazione nella descrizione di applicazioni, processi e – più in generale – dell'intera IT. Per questo motivo, la "multi-modalità" è un aspetto critico che tutte le aziende coinvolte in processi di ammodernamento devono riuscire a governare in maniera efficace.



Framework Multi-modale

L'intero Software Lifecycle – partendo dalla gestione del Demand e del Portfolio, fino ad arrivare alle strutture di Operations – sarà coinvolto nella revisione della modalità di avanzamento delle iniziative da Tradizionali verso Digitali. La stessa pianificazione degli interventi in un approccio Scrum/Agile sarà un corollario dei Backlog di prodotto che emergeranno a valle dell'esecuzione delle diverse Sprint di esecuzione.

PANORAMICA CAPABILITIES IT

La definizione di un modello operativo IT si fonda sull'identificazione delle aree di competenza che abilitano l'IT ad un efficace supporto del business. Tali aree sono costituite dalla combinazione di processi, governance, organizzazione e tecnologie e costituiscono le **capabilities** che abilitano l'erogazione dei servizi IT.

L'identificazione delle capabilities IT parte dalla consapevolezza che l'IT debba supportare la strategia creando nuova tecnologia, la quale opera al servizio del business, dei clienti (interni o esterni) e degli utilizzatori finali.

Per supportare il contesto IT multi-modale dell'Amministrazione, è opportuno che il nuovo modello operativo IT possieda le seguenti caratteristiche:

- Struttura *service-oriented*, per supportare appieno sia la fornitura di servizi applicativi che tecnologico-infrastrutturali;
- Flusso di lavoro basato sul ciclo di vita del servizio;
- Coesistenza di diverse modalità di delivery (modello multi-modale);
- Responsabilità congiunta del business e dell'IT, per la creazione di valore partendo dalla tecnologia;
- La governance si sposta dal focus sui costi IT al valore e alla trasformazione del business;
- Possibilità di allocazione di budget a livello di prodotto/soluzione, in opposizione al tradizionale finanziamento di progetti;
- Continuous integration e continuous delivery;
- Incremento nell'impiego di analytics nell'ambito di operations e management del rischio e della sicurezza;
- Assottigliamento della separazione tra organizzazione ed ecosistema di partner.

Per garantire le caratteristiche introdotte, nel contesto IT multi-modale sono state identificate 6 capabilities chiave:

1. **Business and Customer Relationships Management**: comprende le priorità del business, supporta il pensiero strategico e innovativo attraverso una chiara articolazione delle capabilities IT, filtra la domanda dei clienti (interni ed esterni) e gestisce le aspettative sullo sviluppo e la delivery di servizi IT.
2. **Service Strategy**: allinea i piani e l'architettura IT con le priorità del business e garantisce che le risorse IT siano distribuite in modo appropriato per soddisfare quanto approvato dal demand in relazione ai servizi IT.
3. **Service Creation**: si focalizza sulle fasi di design, assemblaggio e transition dei servizi IT massimizzando i benefici e minimizzando rischi di rilascio ed esercizio.
4. **Service Management & Operations**: offre servizi IT affidabili e fornisce un punto di integrazione end-to-end, migliorando al contempo la qualità e l'efficienza attraverso una costante attenzione al miglioramento continuo (*Continuous Improvement*).
5. **IT Management**: consente all'IT di adempiere ai propri impegni verso il business modellando le policies, promuovendo le prestazioni, prendendo le decisioni critiche e coordinando le funzioni interne ed esterne.
6. **Ecosystem Management**: si occupa di costruire e mantenere relazioni di fiducia con fornitori e partner, per garantire rapporti lavorativi continuativi e promuovere efficacia dei costi e prestazioni elevate durante l'intero ciclo di vita del contratto.

A supporto del modello delle capabilities IT proposto, possono essere valutate diverse capabilities di secondo livello, ciascuna definita nel contesto di una specifica capabilities di base. Lo schema sintetizza le capabilities di base, indicando per ciascuna le diverse capabilities di secondo livello.

Capability IT Base	Capability IT di Livello 2	Adeguamento per Cloud Adoption e Modello Service-Oriented
Business and Customer Relationship Management	Enterprise Strategy	Formalizza le priorità strategiche del business e gestisce le aspettative su sviluppo e rilascio dei servizi IT. Sviluppa la pianificazione degli interventi strategici.
	Service Requirements	Identifica e raccoglie le necessità del business e dell'IT, e lavora con gli stakeholder per allinearle.
	Service Performance	Verifica gli accordi sul livello di servizio (SLA) con il business, e gestisce aspettative, feedback, osservazioni e reclami dei clienti.
Service Strategy	Technology Strategy	Sviluppa la strategia tecnologica e la cloud adoption, l'evoluzione dei livelli di automazione, la tools strategy ed il piano di investimenti, ed assicura che la roadmap dei servizi sia allineata con le priorità aziendali, le priorità dell'IT e il budget.
	Portfolio Management & Planning	Identifica e sviluppa nuove idee e capabilities.
	Enterprise Architecture	Sviluppa i principi guida e garantisce la conformità architetturale alle policies ed alle blueprint dei componenti di servizio standardizzati.
Service Creation	Program & Project Management	Si occupa della pianificazione (tempi e costi) e della gestione dei progetti di sviluppo di servizi e trasformazione applicativa/tecnologica, assicurando che consegne e rilasci avvengano nel rispetto dei tempi e della qualità.
	Service Design & Assembly	Progetta e realizza servizi su richiesta, sfruttando l'automazione e garantendo che le specifiche siano coperte (da servizi nuovi od esistenti).
	Service Transition	Si focalizza sulla fase di rilascio del servizio, assicurando sia la corretta installazione che la capacità delle operations di erogare e supportare il nuovo servizio.
Service Management & Operations	Service Management	Supporta la manutenzione del catalogo dei servizi e del portale messo a disposizione degli utenti IT per l'accesso ai servizi ed alla descrizione di tutti i componenti Cloud a disposizione.
	Service Operations	Assicura la qualità e la disponibilità del servizio, prediligendo meccanismi basati su automazione ed intervenendo manualmente ove necessario. Include monitoraggio e gestione eventi, capacity e disponibilità.

IT Management	IT Performance & Control	In ambito performance, definisce obiettivi e metriche per l'organizzazione IT, gestisce l'intellectual property, ed assicura che i processi vengano sempre sottoposti a misurazione e continuous improvement. Ottimizza periodicamente i servizi cloud
	Security & Risk Management	Stabilisce ed amministra policy di sicurezza e gestione del rischio per l'organizzazione IT, ivi incluse certificazioni in ambito sicurezza ed accesso ai dati, mantenendo allineamento con la funzione di sicurezza IT.
	IT Financial Management	Garantisce la misura della consumption degli utenti interni, basata sui servizi effettivamente fruiti e sulle condizioni concordate.
	IT Talent Management	Si occupa della valutazione e dello sviluppo delle competenze. Gestisce la formazione ed il rapporto con gli stakeholder.
Ecosystem Management	Vendor & Partner Management	Instaura e mantiene relazioni di fiducia con fornitori e partner, con l'obiettivo di garantire rapporti lavorativi continuativi e prestazioni adeguate. Concorda i livelli di servizio con i fornitori rivedendo le prestazioni dei fornitori rispetto agli SLA e agli OLA, ed innalzando il livello di servizio ove ritenuto opportuno. Ingaggia opportune verifiche nel caso in cui i termini di servizio non vengano rispettati e si occupa di seguire l'eventuale applicazione di penali o riconoscimento di crediti.

LINEE DI INDIRIZZO

Per accelerare l'adozione di soluzioni cloud, che siano native o ibride, può essere utile l'istituzione di un **Centro di Eccellenza Cloud** (Cloud COE), il quale affianca specialisti e **Cloud Architect** agli **stakeholder**, con l'obiettivo di costituire un **team interfunzionale** a supporto della transizione verso il nuovo modello operativo IT.

Il Centro di Eccellenza Cloud viene avviato con il focus sullo sviluppo della strategia per un'implementazione responsabile del nuovo modello IT su larga scala, e si affianca al potenziamento di funzioni di **Cloud Monitoring**, **Triage** e **Cloud Operations**. E' possibile prevedere un progressivo ampliamento delle responsabilità del team Cloud COE, con l'obiettivo di posizionarlo come un hub per le best practice dell'intera organizzazione IT:

- fornire supporto alla strategia, all'interazione con CSP/fornitori, alla definizione delle blueprint e del catalogo di servizi;
- definire, realizzare/trasformare ed esercire i primi servizi nel nuovo modello;
- supportare l'incremento della pervasività delle pratiche DevOps;
- supportare la transizione della gestione dell'infrastruttura tradizionale verso un approccio service-based.

Il Centro di Eccellenza Cloud può quindi dare un forte contributo nell'**indirizzare la complessità** aggiuntiva derivante dall'adozione di servizi Cloud, basato su un consolidato modello tradizionale, ma sottoposto a sperimentazioni e trasformazioni recentemente avviate (e.g., PaaS on-premises, architetture a microservizi, metodologia Agile/Scrum, pratiche DevOps).

In conclusione, l'adozione armonica di un'**architettura IT ibrida e multi-modale** permette all'Amministrazione di trasformare il proprio IT ed abilitare la trasformazione digitale del business:

- maggiore flessibilità nell'adozione della metodologia e dei servizi da impiegare per ciascuna **tipologia di iniziativa** (Waterfall, Agile, mixed);
- nuovi workload (Cloud-native) ed eventuali applicativi migrati su ambienti Cloud (sia Private, che Public) guidano la **modernizzazione del processo di sviluppo applicativo**, potendosi avvalere pienamente delle tecnologie Cloud (Cloud First);
- l'effort attualmente dedicato al consolidamento e all'ammodernamento dell'infrastruttura legacy esistente, potrà essere convogliato nell'incremento dell'**agilità** di sviluppo applicativo e nell'integrazione ed automazione dei nuovi servizi Cloud;
- la **modernizzazione degli strumenti** in uso dovrebbe essere "**prioritizzata"**, nell'ottica di potenziare le funzioni del nuovo modello operativo IT (ITSM, CMDB, billing, etc.), di renderlo più maturo, e di massimizzare la sinergia con i nuovi servizi Cloud.

4.10 Ricognizione di mercato

Come già ricordato nel presente lavoro, per quanto concerne l'ambito di ricognizione del mercato, la PA adotta il modello Cloud individuato da AgID che consente di mitigare il rischio di scostamenti significativi rispetto a standard di sicurezza, garanzie operative e affidabilità definiti a livello internazionale.
Il Cloud Marketplace, in continuo aggiornamento, rappresenta il luogo attendibile attraverso il quale scegliere i servizi Cloud qualificati per la PA.
Il mercato dei CSP Pubblici è in continua crescita in termini di servizi e capabilities aggiunti dai principali vendor. La stessa dinamicità nel trasferire continuamente questa innovazione all'interno dei servizi offerti dagli hyperscaler si riflette sulle tecnologie erogate/erogabili attraverso piattaforme di private Cloud o di Data Center tradizionali.
Effettuare una valutazione dei servizi e un mapping rispetto ai requisiti specifici della singola Amministrazione rientra nelle prime fasi di assessment descritte nel presente documento ed esula dai fini di questo paragrafo.
Vale la pena indicare che il ricorso a report, articoli e analisi degli analisti internazionali (come IDC, Gartner, Forrester) è fortemente raccomandato per avere una panoramica dei servizi e una prima valutazione sulla base di metriche e aspetti standard da un punto di vista internazionale.

4.11 Stima budget intervento, comparazione con TCO attuale e definizione dei benefici

Nel presente paragrafo viene illustrata la metodologia e gli strumenti per presentare al Management il progetto di trasformazione digitale.

L'analisi dei benefici diretti e indiretti, tangibili e intangibili, richiede una maturità che si basa sulla conoscenza profonda del contesto, sui driver di efficientamento e di costo e sul continuo aggiornamento circa le pubblicazioni, gli studi, le linee guida e i report che, in maniera attendibile, trattano l'argomento. La trasformazione digitale può agire, sostanzialmente, su due aree principali: quella che potremmo definire "**del miglioramento**" e quella della "**riduzione**".

L'area del miglioramento prevede un vantaggio nell'aumento di fattori quali, a titolo di esempio:

- prestazioni;
- affidabilità
- disponibilità dei servizi;
- ridondanza;
- scalabilità;
- time-to-market;
- semplicità nelle configurazioni;
- competenze digitali.

L'area della riduzione, nell'ottica della semplificazione, su:

- riduzione dei rischi (es. disservizio, obsolescenza, attacchi di sicurezza, sistemi non più aggiornabili, competenze non più rintracciabili sul mercato, ecc.);
- riduzione dei costi ed ottimizzazione della spesa.

Con questo schema in mente è ora possibile parlare di benefici e analisi dei costi. La mera monetizzazione dei servizi, analisi dell'attuale baseline dei costi IT e forecast per la spesa futura, rischia di essere poco utile se non integrata in un contesto più ampio che recepisce le corrette direttrici di valore e di beneficio nell'approcciare questa Digital Transformation.

L'analisi del TCO e le valutazioni basate sui principali indicatori finanziari (che per esigenze di sintesi non dettaglieremo) può essere condotta una volta che:

- sia completata un'analisi dei costi attuali, per ogni applicazione e componente infrastrutturale dei servizi attualmente attivi organizzando le voci di spesa in CAPEX ed OPEX, collezionando le linee di investimento che, ad esempio nel triennio, sono in approvazione, valutando i costi di esercizio, di sicurezza, di facilities, di progettualità e forniture di sviluppo software;
- si sia scelta la piattaforma target di migrazione (CSP, PSN, SPC Cloud, Private Cloud);
- si sia definita l'architettura di riferimento e i servizi che la compongono;
- si sia ipotizzato un macro-piano di migrazione e, di conseguenza, di attivazione di servizi Cloud, nel caso del CSP;
- si sia valutato, per ogni applicazione o componente infrastrutturale trasversale, il profilo di utilizzo, le ore di disponibilità, la geografia attraverso la quale i servizi vengono erogati, la rete disponibile e quella necessaria;
- si sia ottenuta una quotazione, con le condizioni di maggior favore disponibili sul mercato, per i servizi Cloud, per le professionalità necessarie al disegno, progettazione, analisi, migrazione, collaudo e rilascio delle infrastrutture e delle applicazioni;
- si sia considerata una componente, legata alle persone all'interno dell'organizzazione, declinando le esigenze di formazione, i servizi di supporto e di affiancamento al Change Management e la necessità di una comunicazione, eventualmente con l'avvio di progettualità specifiche, che accompagni questa transizione fondamentale;
- si sia definito il modello per stimare l'impatto e il valore economico a tendere della trasformazione sui processi di business.

Vale la pena sottolineare che l'analisi del trend storico degli ultimi anni, indica un decremento dei costi dei servizi Cloud, seppur a fronte di un arricchimento dell'offerta e del catalogo servizi. Questa indicazione può aiutare a valutare una eventuale percentuale di "rebate" per i costi del Cloud in un mercato che sta assistendo ad un processo di "*commodization*" per i servizi tipicamente IaaS.

5. Progettazione

Le indicazioni contenute nel presente capitolo traggono origine dall'esperienza della Corte dei conti che, da oltre dieci anni, ha ripensato in un'ottica cloud first i propri sistemi informativi, puntando sul modello di erogazione del cloud pubblico. Da dicembre 2016 la Corte dei conti non ha più datacenter di proprietà.

Questo capitolo descrive le attività preliminari di definizione del progetto di migrazione in cloud dell'organizzazione. Lo scopo è quello di individuare i punti principali, così da stilare nel modo più efficace possibile il capitolato tecnico e/o il piano dei fabbisogni del progetto di migrazione.

Appare ovvio che la complessità del progetto esecutivo di migrazione è legata strettamente alle dimensioni dell'organizzazione, alla sua complessità tecnologica e al livello di maturità. Questi sono aspetti che vanno indagati nella fase di assessment, ma che pensiamo sia utile riprendere anche in questa sezione, dato che trascurarne anche solo uno porterebbe a rischi non correttamente gestiti e che potrebbero compromettere il successo dell'iniziativa.

La corretta gestione del rischio, durante questo tipo di progetti, è peraltro di per sé essenziale e condizione necessaria per ottenere i risultati attesi.

Nel seguito si assumerà di dover mettere in condizione uno o più fornitori di produrre un'offerta tecnica realmente rispondente alle necessità di migrazione, anche se non fossero nelle condizioni di conoscere l'Amministrazione.

Ciascuna delle sottosezioni che segue descrive il contenuto dei capitoli del documento da consegnare ai fornitori candidati perché dettaglino la propria offerta e la proposizione progettuale.

5.1 Contesto

La definizione del contesto tecnologico e organizzativo dell'Amministrazione è cruciale per inquadrare il progetto, sia in termini dimensionali che di complessità tecnica. Partendo dai risultati della fase di assessment, nel progetto di migrazione è opportuno descrivere, in linee generali, ma senza dare per scontate conoscenze pregresse:

a. l'Amministrazione e la sua organizzazione, dettagliando sulla struttura IT e su eventuali altre strutture coinvolte nel progetto (ad esempio gli Affari Generali o le Risorse Umane);
b. eventuali altri stakeholder primari in ambito IT, ad esempio outsourcer o consulenti di particolare rilievo;
c. l'obiettivo generale della migrazione verso il cloud, le sue motivazioni principali, la strategia di trasformazione;
d. il commitment dell'Amministrazione sul progetto, esplicitando gli atti formali adottati dai vertici per autorizzarlo, finanziarlo e pianificarlo;
e. le principali linee tecnologiche seguite dall'Amministrazione fino a oggi, rimandando ai documenti di assessment per i dettagli;
f. le aspettative in termini di ritorno economico, tecnico, gestionale e d'immagine del progetto.

È opportuno che, negli ambienti più complessi, alla descrizione del contesto vengano allegati tutti i documenti tecnico-descrittivi ritenuti importanti ai fini della comprensione, quindi schemi di rete, architetture applicative, configurazione delle postazioni di lavoro fisse e mobili (inclusi gli smartphone), documenti sintetici sugli asset informatici.

5.2 Visione del progetto

L'Amministrazione deve descrivere il più precisamente possibile la propria visione del progetto di migrazione, in termini di risultati attesi, tempi, qualità, tolleranze. È un passaggio fondamentale per evitare fraintendimenti più avanti nel corso del progetto. Nel descrivere la visione dell'Amministrazione va esplicitato:

a) l'arco temporale in cui ci si attende l'inizio e la fine del progetto;

b) qual è il risultato complessivo atteso dal progetto e le tolleranze in termini di prodotti progettuali, tempi costi e qualità;

c) i vincoli di budget del progetto stesso;

d) la necessità, per chi avrà in mano l'execution, di seguire le più moderne tecniche o gli standard di project management (ad esempio Prince2);

e) la necessità di avere un project manager dedicato e di livello adeguato;

f) chi sono i referenti dell'Amministrazione che seguiranno in prima persona il progetto;

g) chi avrà, nell'Amministrazione, la responsabilità di definire il successo o meno del progetto, non limitandosi ai meri "collaudi" formali.

5.3 Specifiche tecniche

La definizione delle specifiche tecniche discende direttamente dall'attività di assessment portata avanti prima della fase progettuale. In questa sezione dovranno trovare spazio:

a) lo *scope* del progetto, intendendo il perimetro delle attività progettuali, con il massimo livello di precisione possibile in fase pre-progettuale. Va anche prevista esplicitamente la possibilità di rivedere in corso d'opera il perimetro di intervento. La corretta definizione del perimetro è fattore critico di successo per il progetto e abbassa i rischi connessi;

b) il modello tecnologico di riferimento e i pattern di migrazione (come definiti nella fase di assessment);

c) le scelte già effettuate e quelle da effettuare nell'ambito del modello di migrazione (refactoring, lift-and-shift, ecc.);

d) l'architettura di riferimento *as-is* ed eventualmente quella *to-be*, se già definita e non deliverable di progetto anch'essa;

e) Il modello di sicurezza *as-is* ed eventualmente quello *to-be*, se già definito e non deliverable di progetto anch'esso;

f) tutti i vincoli organizzativi in essere;

g) tutti i vincoli tecnologici rilevati allo stato attuale;

h) le metodologie di project management da utilizzare (che idealmente devono coincidere con quelle in essere nell'Amministrazione);

i) la richiesta della definizione puntuale di un piano di gestione del rischio completo ed esaustivo;

j) i deliverable attesi in ogni fase del progetto, in termini generali.

5.4 Requisiti dei Servizi di Migrazione

È importante indicare cosa si attende dal servizio di migrazione, in particolare in termini di composizione del team di progetto e di comunicazione. Si ritiene essenziale che il capitolato/piano dei fabbisogni contenga la definizione:

a) dei soggetti coinvolti nel processo di migrazione, in particolare se chi condurrà il progetto intenda o meno avvalersi di terzi o di servizi messi a disposizione dal cloud service provider (con eventuali costi associati);

b) della figura del project manager, che dovrà avere esperienza specifica documentata su progetti di migrazione in cloud di pari livello di complessità;

c) del team di progetto, a livello di figure professionali coinvolte;

d) delle garanzie di continuità del team di progetto, dato che questa tipologia di progetti è spesso soggetta a rischi relativi alla durata complessiva e alla perdita di membri importanti della squadra con il passare del tempo;

e) dei canali di comunicazione e degli strumenti di collaborazione (ed eventualmente di sviluppo) da usare durante il progetto.

5.5 Definizione del confine di competenza cliente/fornitore

Definire i confini di competenza fra fornitore e cliente nell'ambito dei progetti di migrazione è critico per la riuscita dei progetti stessi. Questo a maggior ragione se sono presenti uno o più outsourcer o comunque una pluralità di soggetti operanti nell'ambito del change management.

Un esempio calzante può essere quello di un'Amministrazione i cui sistemi/servizi sono gestiti, in via ordinaria, da un fornitore di servizi di conduzione sistemistica, che non coincide normalmente con chi progetterà ed eseguirà la migrazione in cloud. Il "chi-fa-cosa" dovrà essere inizialmente definito in fase contrattuale e poi rivisto e vincolato in avvio di progetto.

L'ipotesi classica è che saranno coinvolti nella migrazione il team di conduzione (già presente stabilmente presso l'Amministrazione) e un team di progetto (definito ad hoc e che si scioglierà al termine del progetto).

In particolare, dovranno essere chiari a tutti gli stakeholder:

a. la baseline della configurazione di partenza in termini di sistemi, servizi, networking, sicurezza;

b. ruolo e compiti del team di conduzione dei sistemi nell'ambito del progetto, che in linea di massima dovrebbero essere di natura puramente operativa e non progettuale o di disegno;

c. ruolo e compiti del team di progetto e sua integrazione nei processi di change management attualmente in essere nell'Amministrazione. Non va dimenticato che il progetto avrà tempi medio-lunghi (6/12 mesi, salvo realtà molto piccole) e che non è pensabile bloccare la naturale evoluzione dei sistemi per tutto il periodo;

d. modalità di ingaggio del team di conduzione da parte di quello di progetto e relativi tempi di risposta ed esecuzione dei task;

e. i responsabili del coordinamento progettuale lato Amministrazione e le figure cardine dei due team;

f. modalità e destinatari delle escalation durante le fasi progettuali;

g. modalità e tempi di presa in carico da parte del team di conduzione della nuova baseline post-migrazione.

h. strumenti e regole di ingaggio per gli incident e le richieste di cange, dashboard di Service Management, NOC, SOC, et

5.6 Requisiti tecnici e normativi

I requisiti di tipo normativo e tecnico dipendono strettamente dall'output della fase di assessment. In linea generale dovranno essere dichiarati i vincoli esistenti nei seguenti ambiti:

- privacy e data Protection, con riferimento al GDPR e ad eventuali normative settoriali per la singola amministrazione (ad esempio in ambito sanitario);
- proprietà intellettuale (se applicabile);
- IT Security;
- posizionamento geografico dei datacenter coinvolti nella migrazione, comprensivi di eventuali peculiarità settoriali e della gestione del disaster recovery;
- licensing del software collegato alla migrazione;
- normativa relativa alla gestione del personale coinvolto nel progetto, ad esempio sulla sicurezza dei luoghi di lavoro;
- definizione della possibilità o dell'opportunità di svolgere le attività progettuali da remoto o in generale in modalità smart-working.

In alcuni casi (si pensi agli Organi Costituzionali o a rilevanza costituzionale) dovranno essere esplicitati anche i vincoli tecnico-normativi derivanti da normativa secondaria o previsti dall'autonomia regolamentare dell'Amministrazione.

5.7 Requisiti di Service Level Agreement per il Progetto

Nello stilare il capitolato o il piano dei fabbisogni vanno definiti in modo il più possibile puntuale i livelli di servizio che ci attendiamo vengano rispettati da tutti i fornitori coinvolti nel progetto stesso. Si tratta principalmente di SLA sul processo di project management e non riguardano gli SLA dei servizi di conduzione che saranno erogati a partire dal termine della fase progettuale.

Il livello di formalismo con cui gli SLA dovranno essere definiti varia con la complessità del progetto e la capacità del committente di misurarli. A tal riguardo vale la pena ricordare che è inopportuno definire degli SLA contrattuali se non si è in grado di misurarli in maniera affidabile e/o non si è in grado di definire una metrica coerente per farlo. In generale, sono necessari degli SLA riguardo:

- tolleranze sulle date di consegna per i singoli prodotti di progetto, sui tempi, sulla qualità;
- tempi di risposta alle comunicazioni o alle sollecitazioni da parte dell'Amministrazione;
- tempi di risposta a fronte di richieste di modifica del progetto, dei deliverable, dei tempi;
- dimensione massima delle finestre di disservizio totale o semi-totale in cui effettuare le migrazioni e relativi tempi di preavviso;
- dimensione massima delle finestre di disservizio per singoli servizi oggetto di migrazione;
- tempistiche sulla fatturazione a seguito dell'accettazione dei deliverable di progetto da parte dei responsabili dell'Amministrazione.

5.8 Requisiti di Service Level Agreement (SLA) per l'esercizio

Qualora non definiti da precedenti accordi istituzionali potrebbe essere utile la definizione nel capitolato dei Service Level Agreement di esercizio.

Questi SLA possono variare in funzione delle tipologie di servizi cloud forniti e dal livello di criticità delle applicazioni.

Le penali relative al mancato raggiungimento dei livelli di servizio saranno definite, dove possibile ed applicabile, nel capitolato in modo da semplificare la successiva stesura del contratto che regolerà il rapporto fra il Fornitore ed il committente

6. Struttura del programma di migrazione

6.1 Introduzione

Il programma di Cloud Transformation è definito attraverso una serie di progetti sinergici e collegati tra di loro, da eseguirsi mediante una pianificazione coordinata centralmente al fine di raggiungere gli obiettivi complessivamente preposti.

La natura diversa delle attività, la molteplicità degli attori coinvolti (Uffici dell'Amministrazione, referenti, fornitori, eventuali altre PA), la dipendenza da vincoli esterni (Linee guida ministeriali, gare e procedure di procurement) possono essere governate solo attraverso una forte accountability su un programma di innovazione condiviso ed una industrializzazione dei percorsi di migrazione

L'industrializzazione del processo di migrazione passa attraverso la creazione e il consolidamento di una *migration factory*, ovvero un team che, tramite skills, tool e processi che permettano il corretto svolgimento delle attività necessarie al programma di migrazione in cloud.

Questo team allestito per la *migration factory*, sarà un team formato da risorse con competenze eterogenee per poter effettuare attività rivolte non solo al delivery e alla migrazione dei sistemi, ma anche al consolidamento del percorso strategico, supporto per la realizzazione di roadmap e gap analysis per la realizzazione di iniziative volte a migliorare il percorso o proseguirlo, nonché il supporto nell'adozione cloud in termini di processi e conduzione.

Per le attività di delivery il team deve essere sicuramente dotato di esperti della tecnologia del cloud (o differenti) che si è scelto di adottare, che possano lavorare con i gruppi di sviluppo e di conduzione dei differenti sistemi, nonché con i gruppi trasversali di sicurezza, infrastruttura e middleware per essere in linea con le policies dell'organizzazione.

Dal momento che il passaggio verso il cloud è un percorso come detto caratterizzato da differenti fasi, sarà importante avere anche esperti delle tecnologie già esistenti, in modo da poter sostenere la fase in cui entrambi i sistemi coesisteranno, in modo da poter mantenere entrambi i sistemi e decidere in maniera corretta, a seconda del sistema e di una serie di aspetti tecnici, la strategia di cutover necessaria.

Si ritiene quindi utile presentare le linee guida per la strutturazione in chiave "industriale" dei progetti di realizzazione della migrazione al cloud che potrebbero essere integrati in un programma esecutivo specifico, in riferimento a quanto definito dalla strategia di migrazione

6.2 Organizzazione per WBS

La struttura di organizzazione del progetto di migrazione potrebbe essere suddivisa in componenti elementari, definibili in WBS, come di seguito indicato:

Nome	Descrizione
Planning	Pianificazione delle attività di progetto, assessment e definizione della strategia di migrazione
Processi IT Governace	Identificazione attraverso una gap analysis del modello dei processi di governance IT da utilizzare
Tecnologie	Piano tecnico della migrazione
Servizi	Pianificazione della migrazione per ogni servizio, eventualmente raggruppando più servizi in waves

Dati	Pianificazione della migrazione dei dati
Indirizzamento IP	Struttura del nuovo indirizzamento IP, della modalità di migrazione e definizione delle modalità di switch al Disaster Recovery
Sicurezza	Definizione delle componenti tecniche di sicurezza logica e piano di implementazione
Test & Collaudo	Definizione delle metodologie di test e collaudo post migrazione
Service Management	Pianificazione della realizzazione del nuovo modello di service management e programma di attivazione degli strumenti di monitor
Organizzazione	Definizione dei ruoli e responsabilità della struttura ICT, dei servizi aziendali si supporto e programma di formazione
Facilities	Identificazione delle facilities necessarie a realizzare il piano

6.3 Planning

6.3.1 Terminologia dei Metodi di Migrazione

I metodi di migrazione verso cloud, come già precedentemente indicato, sono classificati in sei modalità che influenzano in modo sostanziale il piano operativo. Di seguito ricordiamo le definizioni da tenere in considerazione:

- Rehosting (IaaS): approccio “lift and shift”, nella pratica una copia del contesto esistente. Basato sull’immagine del server senza modifica della versione software. Può essere un import diretto del sistema sorgente con o senza tool, oppure re-installazione dei sistemi target mantenendo stessa versione applicativa e di sistema operativo;

- Replatform (IaaS avanzato): modifica/aggiornamento delle versioni del sistema operativo, database ed applicativo attraverso una nuova installazione nativa sul sistema Cloud target;
- Refactoring (IaaS/PaaS): modifica dell’applicazione e degli strumenti di middleware in modo da utilizzare alcuni servizi PaaS nativi del Cloud provider;
- Redesign (PaaS): revisione dell’architettura degli applicativi in modo da utilizzare in forma nativa ed estensiva i servizi Cloud del provider;
- Rebuilding (PaaS/SaaS): revisione delle applicazioni per un utilizzo intensivo dei servizi PaaS e SaaS del Cloud provider. Richiede la scomposizione delle applicazioni in moduli;
- Replacing (SaaS): sostituzione dell’applicazione con la stessa ma fornita in modalità Cloud dal provider.

6.3.2 Metodi di Migrazione per Servizio (criteri operativi di dettaglio)

Nella pianificazione del percorso di migrazione, le pubbliche amministrazioni dovranno descrivere i componenti da migrare organizzati per servizi e con la classificazione della strategia di migrazione e della priorità, in modo da poter organizzare le attività di deployment per waves.

6.3.3 Organizzazione della Migrazione per Waves di realizzazione

Per un'efficace organizzazione della migrazione si dovranno descrivere in dettaglio i percorsi di migrazione per waves con l'indicazione dei servizi da migrare per ogni fase.

6.3.4 Pianificazione Migrazione

Per un'efficace pianificazione è opportuno sviluppare il masterplan del progetto ed il GANTT di dettaglio.

6.3.5 Responsabilità e ruoli nel progetto di migrazione

E' inoltre opportuno inserire nel documento di migrazione un indicazione relativa a:

- il metodo per l'assegnazione delle responsabilità di gestione e realizzazione delle attività da effettuare;
- le tipologie di contratti concordati con i fornitori dei servizi Cloud e con i fornitori degli applicativi;
- la tabella RACI complessiva per tutte le attività di tutte le WBS con la chiara definizione, anche descrittiva delle responsabilità assegnate.

6.4 Processi ICT Governance

E' utile illustrare le attività raccomandate per la definizione dei processi di ICT Governance da adottare con la trasformazione al cloud.

6.4.1 Gap Analysis

Nel contesto di servizi con il Cloud Provider in "shared responsibility" è indispensabile in fase di pianificazione individuare quali sono i processi e le procedure codificate in uso (documenti), quelle che sono necessarie per il governo dei servizi con il Provider, in modo da ottenere la mappa delle attività che dovranno essere sviluppate prima o durante la migrazione.

La seguente tabella rappresenta un esempio per la valutazione della situazione *as is* e identifica le azioni che devono essere intraprese durante l'esecuzione del presente piano.

Nome Processo	AS-IS	Documentazione	Priorità	Azione
Service Desk				
Escalation				
Change Management				
Event Management				
Incident Management				
Data Breach Management				
Ticket Management				
Security Management				
Service Monitoring				

6.4.2 Modello dei Processi di ICT Governance

Il modello dei processi da realizzare per la Governance dei Servizi ICT in "shared responsibility" da personalizzare per lo specifico contesto dovrà considerare il come suddividere le attività di governo fra le risorse interne e i fornitori attraverso un modello specifico.

Gli ambiti di Governance ICT saranno quindi un mix fra il controllo di servizi erogati e la gestione diretta di servizi e componenti tecnologiche.

Da questo modello e dallo stato AS-IS deriva che nella realizzazione del progetto dovranno essere definiti i processi e le procedure almeno da best practices ITIL.

6.5 Migrazione Servizi

Il piano di migrazione deve contenere un'indicazione su come progettare in dettaglio la migrazione dei servizi, secondo le specifiche definite nei documenti prodotti dai fornitori delle aree applicative in collaborazione con i Cloud Provider e con la strategia di Migrazione.

6.6 Migrazione Dati

La migrazione dei dati è un aspetto importante da non trascurare e va dettagliato nel piano di migrazione. Si suggerisce di trattare i seguenti argomenti:

- Validazione dei dati al punto di arrivo.
- Verifica della compatibilità applicativa.
- Misure per la sicurezza dei dati nella migrazione.

6.7 Connettività e Networking

Il Piano dovrà prevedere anche le implicazioni di networking da considerare con la trasformazione al cloud. Si suggerisce di trattare i seguenti argomenti:

- Definizione del contesto di networking.
- Approccio dell'intervento di migrazione del netwoking.
- Piano di adeguamento di indirizzamento e routing interno e dei provider.
- Configurazione Disaster Recovery (se applicabile).

6.8 Sicurezza

6.8.1 Ruoli e responsabilità

Devono essere preventivamente identificati, all'interno dei diversi attori (Amministrazione, cloud provider, ecc.) i soggetti che hanno la responsabilità di garantire la sicurezza dei dati e dei sistemi nel corso delle attività di migrazione, con particolare riferimento a quanto indicato in questa sezione, assicurandone un adeguato coinvolgimento nelle attività di migrazione e nei processi decisionali.

6.8.2 Identity & Access Management

Devono essere identificate le persone incaricate delle diverse attività, assegnando loro dei profili di accesso coerenti con i compiti previsti.

Tutti i profili degli utenti con qualunque livello di autorizzazione coinvolti nei servizi cloud, compreso il processo di migrazione, devono essere configurati almeno su sistemi di Active Directory. La creazione, modifica e cancellazione delle utenze su Active Directory devono essere effettuate assicurando un adeguato processo autorizzativo e il tracciamento delle operazioni. Le utenze devono essere personali, limitando al minimo necessario l'utilizzo di account di gruppo.

Le utenze definite per le attività di migrazione devono avere una scadenza coerente con i tempi dell'attività, e devono comunque essere disabilitate al termine delle attività di migrazione, assicurando che al termine della stessa siano definite solo le utenze effettivamente previste a regime per l'utilizzo e l'esercizio dei sistemi.

Nell'ambito dell'attività di migrazione, dove possibile, la gestione delle utenze deve essere integrata con i servizi di IAM centralizzati, evitando di definire utenze locali per sistemi e applicazioni.

Dove disponibili, devono essere utilizzati strumenti di Privileged Access Management che consentano di mediare e tracciare gli accessi privilegiati ai sistemi.

6.8.3 Sicurezza di rete e delle connessioni

La connessione punto-punto fra i due datacenter deve essere cifrata o, qualora non fosse possibile, deve fornire adeguate garanzie di isolamento logico e di protezione del traffico (es. MPLS), purché sia stata adeguatamente valutato il rischio di accesso non legittimo da parte del fornitore di connettività.

L'ambiente di destinazione dei sistemi e degli applicativi migrati deve essere preventivamente configurato in modo da assicurare un'adeguata protezione di rete, ad esempio attraverso la configurazione dei meccanismi di segregazione, filtraggio (es. firewall) e monitoraggio. La migrazione non deve avvenire in ambienti di cui non sia stata preventivamente predisposta una protezione equivalente almeno a quella del datacenter di origine, e comunque preferibilmente quella prevista come finale nell'ambiente di destinazione.

6.8.4 Protezione dei dati

I dati, compresi i database e le configurazioni, devono essere trasferiti in maniera protetta, cifrati o attraverso connessioni cifrate. In nessun caso devono essere create copie non cifrate al di fuori degli ambienti finali di produzione in cui i dati saranno utilizzati. Eventuali copie cifrate devono essere tracciate e cancellate al termine dell'esigenza che ha portato alla loro creazione.

6.8.5 Ambienti di test

Gli ambienti di test, qualora prevedano l'utilizzo dei dati reali, devono offrire le stesse protezioni, anche in termini di controllo accessi, degli ambienti finali di produzione. I dati portati in ambiente di test devono essere tracciati e cancellati al termine dell'esigenza.

6.8.6 Verifica di integrità

Per i diversi sistemi e servizi, devono essere identificati gli opportuni controlli che consentano di verificare l'integrità dei dati migrati, con particolare riferimento ai database e alle configurazioni. Dove la migrazione preveda il rehosting, la verifica potrà ad esempio consistere in checksum crittografiche (hash) delle immagini

migrate. Negli altri casi, dovranno essere tracciate le modifiche alle configurazioni resesi necessarie in conseguenza del diverso ambiente di produzione.

6.8.7 Monitoraggio e gestione incidenti

I processi di monitoraggio e gestione incidenti devono essere attivati nell'ambiente di destinazione prima dell'inizio delle attività di migrazione di sistemi e servizi, fatti salvi quelli eventualmente necessari per l'implementazione dei processi stessi.

6.8.8 Documentazione

Le attività devono essere adeguatamente supervisionate e documentate, anche per assicurare la rispondenza di quanto effettuato alla normativa applicabile (GDPR, D.lgs. 231 ecc.).

6.8.9 Sicurezza Logica Servizi Cloud, connettività e networking

Strutturare una matrice di controlli di sicurezza con le seguenti informazioni:

- dominio di controllo: l'area di controllo cui facciamo riferimento (es. Accessi, sicurezza delle reti, ecc.);
- livello di sicurezza strutturato a livello 1 per quelli ritenuti fondamentali, mentre quelli a livelli superiori, 2 o 3, potrebbero essere attivabili per specifici ambiti definiti dal cliente, a seconda della criticità di dati/processi gestiti tramite la soluzione cloud;
- stato del controllo: dovrebbe essere indicato lo stato del controllo sulla base delle specifiche risposte ottenute dal fornitore.

Il risultato sarà così una scheda di valutazione dove la componente sicurezza (definita con la matrice dei controlli) è una delle componenti da prendere in considerazione per la valutazione della sicurezza dei servizi e delle azioni di adeguamento necessarie prima di andare in produzione.

6.8.10 Privacy

Ad integrazione delle condizioni contrattuali sottoscritte con il fornitore, è necessario che nel piano siano definite le condizioni cui deve sottostare un responsabile (o sub-responsabile) di trattamento come indicate nell'art. 28 del GDPR, fra cui:

- Descrizione delle misure di sicurezza;
- Piano di adeguamento dei servizi cloud rispetto al registro dei trattamenti;
- Modalità di supporto al titolare in caso di violazione dei dati (data breach);
- Modalità di supporto al al titolare nel rispondere alle richieste dei soggetti interessati;
- Compilazione di un registro di trattamento per ognuno dei titolari per cui svolge un trattamento;
- Metodo di esecuzione del diritto di audit;
- Metodo di valutazione dell'efficacia delle misure di sicurezza;
- DPIA specifica da fare approvare al CdA e da comunicare al DPO.
- ….

6.9 Test e collaudo

6.9.1 Strategia di test

La strategia di test dovrà contenere precise indicazioni relativamente alle attività da svolgere per ciascun servizio oggetto di migrazione e dipenderà, oltre che dalle tecnologie coinvolte, dalla strategia di migrazione adottata a cui dovrà adattarsi per mitigare eventuali rischi.

Sarà opportuno definire un "responsabile delle attività di test", costui sarà responsabile della pianificazione degli stessi e della corretta comunicazione tra i differenti attori che saranno chiamati a collaborare durante le fasi del test (Progettazione, esecuzione, fixing delle anomalie rilevate). Particolare enfasi va posta al coordinamento dei differenti fornitori.

6.9.2 Staging (Definizione degli ambienti di collaudo)

Per ciascun servizio dovranno essere individuate le componenti oggetto della migrazione e le componenti ad esse collegate ma non trasferite. Tale attività si rende necessaria per pianificare la replica degli ambienti necessari per il test funzionale integrato.

In merito alle applicazioni oggetto di migrazione, considerando l'eccezionalità dell'operazione, è possibile decidere di utilizzare gli stessi ambienti destinati ad ospitare in futuro la produzione come ambienti di test delle attività di migrazione. Questa scelta garantisce l'assoluta rispondenza dei sistemi di test ai requisiti di replicabilità e scalabilità, permettendo di verificare ogni configurazione direttamente sull'ambiente destinazione. Sarà in ogni caso buona pratica tracciare puntualmente ogni modifica apportata alle configurazioni. Si potrà inoltre concordare con il fornitore di servizio una differente disponibilità di risorse durante i test, via via che ci si approssima alla effettiva migrazione del servizio.

Gli ambienti allestiti per il test dovranno in ogni caso essere confrontabili con l'ambiente di produzione anche in termini di performance per quanto riguarda la verifica del Workload. Nel caso in cui il server di test non sia il medesimo destinato ad ospitare il servizio in produzione (o una sua identica copia) sarà necessario concordare con il provider una scala proporzionale con cui valutare i risultati dei test di carico.

Come precedentemente indicato per le modifiche alle configurazioni, sarà pratica integrante nelle attività di progettazione della migrazione il tracciamento puntuale e preciso di ogni passo da eseguire per ottenere la stessa in modo corretto. Se da un lato questa pratica è indispensabile al fine di realizzare un sicuro piano per la messa in produzione della stessa, dall'altro garantisce la possibilità di testare correttamente ogni singolo passo di migrazione.

Va peraltro evidenziato che, poiché si procederà per migrazioni successive (waves), la struttura andrà compartimentata al fine di consentire la coesistenza di sistemi di produzione con sistemi di test (che diverranno di produzione al completamento del deploy).

I dataset esportati per consentire i test dovranno essere sottoposti alle medesime misure di sicurezza degli ambienti di produzione, questo per rispettare le norme di sicurezza dei dati in essi contenuti. Ciò non rappresenta un costo se si considera il fatto che tali norme dovrebbero essere in ogni caso applicate al trasferimento dei sistemi in produzione. Si tratta pertanto di "anticipare" tali configurazioni e integrazioni con i sistemi a salvaguardia della sicurezza alla fase di test, coerentemente con le regole in essere e le norme di security definite per la migrazione in cloud. Ciò consentirà al dipartimento preposto alla sicurezza di verificare opportunamente le configurazioni adottate in collaborazione con il provider selezionato.

Per quanto riguarda le piattaforme ed i servizi non oggetto di migrazione, ma richiamati o integrati con essi dovrà essere valutata individualmente l'esigenza di avere tali ambienti a disposizione durante i test. Si potrà altresì valutare di simulare le componenti esterne non oggetto di migrazione con stub o tool idonei. Tale scelta dipenderà in larga parte dalla strategia di test adottata per lo specifico servizio e sarà frutto di

valutazioni legate al rischio. Tale rischio sarà tanto maggiore quanto più importanti saranno le attività di refactoring adottate durante la migrazione.

Nel caso in cui il servizio esterno richiamato sia interrogato senza impatti sul patrimonio di dati contenuto, per esempio una semplice anagrafica di esami clinici a solo scopo di consultazione, si potrà valutare l'opportunità di utilizzare direttamente l'ambiente di produzione per evitare di allestire una replica dello stesso.

Si suggerisce come regola di carattere generale la simulazione dei sistemi collegati nel caso di Rehosting di un servizio e la replica dell'intera applicazione in presenza di Replatforming.

A scopo puramente esemplificativo: l'applicazione "A" oggetto di migrazione e soggetta a Replatforming, necessita di un servizio esposto dall'applicazione "B" per poter essere testata. In tal caso, se non può essere integrato direttamente il servizio in produzione per completare i test, l'applicazione "B" dovrà essere replicata per consentire i test.

6.9.3 Verifica workload

Dovranno essere espressi i requisiti minimi che dovranno essere sostenuti dai sistemi oggetto di migrazione e, qualora non sia possibile disporre dell'intera base dati, individuate le anagrafiche di interesse per gli specifici test in termini di Data set da estrarre o produrre durante le sessioni di test funzionale e di carico.

Il fornitore di ciascun servizio dovrà formalizzare le suddette informazioni con un tempo adeguato alla loro preparazione.

Sulla base dei requisiti di performance espressi dal fornitore del servizio e validati dal cliente (utilizzatore o responsabile finale dei servizi) potranno essere preparati i data set necessari alla somministrazione dei test di carico. In base alle tecnologie adottate saranno individuati i tools o le procedure atte a simulare il carico corrispondente alle indicazioni ed ai requisiti collezionati. Ogni requisito dovrà essere verificato da uno o più test (copertura). Per ogni associazione requisito/test (presumibilmente uno a molti) dovranno essere indicate le modalità di esecuzione e gli eventuali tool da adottare. Sarà cura del responsabile di progetto e del responsabile dei test verificare l'opportunità di adottare differenti tool rispetto a quelli identificati al fine di ridurre il parco software necessario, rivolgendosi eventualmente a specialisti del settore.

Durante il disegno dei test dovranno essere individuati i corretti misuratori volti a verificare la sostenibilità dei carichi (es. utilizzo di memoria, CPU, spazio disco) in aggiunta alle consuete misurazioni dei tempi di risposta. Tali KPI saranno espresse dal fornitore del servizio e validate ed integrate dal provider selezionato. Questo consentirà di prevenire eventuali collassi del sistema oggetto di test. Al fine di evitare risultati inspiegabili e/o difficoltà nella diagnostica post carico, dovranno essere eseguiti in modo separato i test di carico sui singoli sistemi rispetto ai test integrati.

È importante ricordare che le eventuali connessioni ad anagrafiche di produzione utilizzate per i test funzionali andranno opportunamente rimosse nel caso di test di performance (qualora questi vengano eseguiti durante il normale orario di lavoro).

6.9.4 Metodo di test

I test si suddivideranno principalmente in due categorie: verifica dei dati e verifica funzionale. Per entrambe le categorie di test dovranno essere effettuati approfondimenti legati alle tecnologie utilizzate in cui si selezioneranno gli strumenti più adatti all'esecuzione degli stessi ed all'analisi dei risultati. I fornitori delle differenti aree applicative forniranno documentazione relativa all'elenco delle verifiche da effettuare sui dati acceduti dai propri applicativi.

Tale elenco sarà parte integrante della documentazione di analisi del processo di migrazione e un sottoinsieme di tale elenco di verifiche sarà indicato per la successiva fase di verifica post installazione.

Si suggerisce un approccio rivolto al rischio. Perciò durante la progettazione dei test andrà verificata la copertura totale dei rischi individuati in fase di analisi, in presenza di rischi privi di copertura dovrà essere giustificata l'assenza di test volti a controllarli ed eventualmente nuovi test dovranno essere inseriti.

Test dei dati

La verifica dei dati si baserà su una analisi statica di quanto migrato attraverso l'analisi delle basi dati e su una successiva analisi dinamica verificata attraverso l'accesso applicativo ai dati migrati. Le due fasi andranno separate con attenzione in quanto l'analisi dinamica, per sua stessa natura, modifica i dati e rende pertanto inefficace l'analisi statica. Nel caso in cui si intenda procedere in parallelo con le due attività si dovrà quindi operare due basi dati distinte. Tate verifica sarà resa più complessa nel caso in cui il software che accederà ai dati richieda la modifica degli stessi durante la migrazione, per esempio in conseguenza di un cambio RDBMS durante la migrazione. La verifica dei dati potrebbe influenzare ampiamente il check funzionale descritto nel seguito.

Tutti i test di consistenza dati sono considerati ad alto rischio.

Test funzionale

La modalità di verifica (test) funzionale adottata sarà Black Box e sarà volta a coprire i requisiti funzionali e di processo precedentemente espressi dal cliente (o responsabile del servizio).

La capillarità dei test funzionali sarà direttamente proporzionale all'invasività in termini di sostituzione del codice sorgente delle piattaforme migrate, quindi dipendente dalla strategia di migrazione adottata e potrebbe ridursi alla semplice esecuzione di operatività basilari senza particolare enfasi sulle casistiche funzionali nel caso in cui il processo venga trasferito da un server su un altro senza alcun intervento in ambito di sviluppo (vd. Rehosting).

Tanto più saranno standard ed immutati gli applicativi sulla nuova piattaforma destinazione, tanto meno approfondita dovrà essere la verifica delle funzionalità migrate, ci si aspetta infatti che le funzionalità trasferite non cambino il proprio comportamento su di un server equivalente.

Verranno univocamente individuati i responsabili della progettazione dei test e verrà loro richiesto di esprimere per ogni caso di test i passi necessari al loro svolgimento, le casistiche (data set) oggetto di test e i risultati attesi al fine di poter considerare superati i suddetti test. Benché si tratti di test "funzionali" volti cioè a verificare l'assenza di regressione nelle funzionalità offerte dall'applicativo oggetto di migrazione, tali test possono presentare caratteristiche più o meno tecniche e pertanto richiedere per il loro disegno ed esecuzione il supporto di personale con competenze informatiche più o meno approfondite. Talvolta gli attori con conoscenze più spiccatamente tecniche dovranno alternarsi agli esperti funzionali durante il disegno e l'esecuzione dei test.

Per tutti i test progettati andrà valorizzata la priorità al fine di poter agevolmente monitorare lo stato di esecuzione e dare la giusta sequenza ai differenti test, Tali scenari di verifica verranno archiviati prima della loro esecuzione in maniera che sia possibile la loro revisione da parte dei differenti attori coinvolti (anche al solo scopo di preparare gli esecutori ad una più efficace esecuzione degli stessi). Verranno quindi individuati gli attori incaricati di eseguire ciascun test pianificato, non necessariamente chi ha disegnato il test sarà responsabile della sua esecuzione. Ciò fatto verrà resa disponibile la struttura (anche un semplice template) con cui saranno documentati gli esiti dei test in modo che sia possibile inequivocabilmente risalire a chi e quando abbia eseguito la prova ed alle condizioni di contorno in cui la stessa sia stata eseguita. In tale template dovranno essere tracciate chiaramente tutte le informazioni indicate dal fornitore come necessarie alla chiusura del bug o alla risoluzione dell'incidente durante le prove effettuate (es. ambiente di test su cui si è eseguita la prova, timestamp, dataset, utenza, versione del S.O.).

Dovrà essere definito un periodo di tempo adeguato affinché le persone coinvolte nelle prove possano prepararsi, i responsabili della realizzazione degli ambienti di test possano allestire gli stessi e i data set

(comprensivi di tutti i prerequisiti riportati negli scenari di test) possano essere preparati per l'esecuzione. Tra gli attori coinvolti nell'esecuzione dei test sarà importante coinvolgere gli utilizzatori finali dei servizi (es. CUP, PACS) al fine di evitare che siano sottovalutati dettagli operativi di importanza vitale per l'esercizio delle funzioni.

Al termine delle attività di test sarà previsto un periodo che consenta ai differenti fornitori di risolvere le anomalie riscontrate e verificarne puntualmente la risoluzione sul campo. A discrezione del responsabile di progetto potranno essere rieseguite una serie di prove minime volte a garantire che non siano subentrate regressioni durante il fixing delle anomalie.

Tale piano di dettaglio verrà quindi esportato e condiviso verso tutti gli attori.

Test Tecnici dei Cloud Provider

Parallelamente ai test precedentemente esposti dovranno essere disegnati da parte del provider selezionato e resi disponibili al progetto i test tecnici volti a verificare il corretto funzionamento della infrastruttura informatica.

Raggiungimento dei differenti nodi da ciascun server migrato e reciproca raggiungibilità. Corretta attivazione di tutti meccanismi di protezione previsti sulle componenti hardware o virtualizzate (es. riavvio automatico dei server quando previsto, mirroring delle schede di rete e degli alimentatori ove previsto, reindirizzamento su tratte di backup in caso di rottura di una tratta tra i differenti servizi).

Tracciamento dei difetti

Dovrà essere definita la modalità con cui ogni anomalia riscontrata durante l'esecuzione dei test debba essere tracciata. Parimenti dovrà essere chiaro prima della esecuzione quale debba essere il ciclo di vita dei difetti e chi ne sia responsabile.

La reportistica relativa ai difetti riscontrati ed al loro stato dovrà essere accessibile ai responsabili delle attività di Test, al responsabile dell'intero progetto di migrazione, a tutti i manager che abbiano un ruolo di coordinamento volto a raggiungere un esito positivo del progetto di migrazione.

6.9.5 Verifica post migrazione

Verranno indicati tra tutti i test progettati per la verifica funzionale i test che possano verificare la corretta configurazione ed installazione dei sistemi, nonché la corretta migrazione dei dati. Tali verifiche non sono eseguite al fine di verificare la corretta implementazione del processo di migrazione o il corretto comportamento degli applicativi, fasi già abbondantemente testate in precedenza, ma sono selezionate al fine di controllare che non siano stati trascurati passi durante l'installazione (siano essi di configurazione o di compilazione dei sorgenti sul nuovo ambiente operativo) e che tutte le componenti facenti parte della intera struttura informatica siano correttamente collegate tra loro.

Al termine della selezione il responsabile dell'installazione insieme al provider del servizio procederanno a integrare gli scenari con il numero adeguato delle verifiche necessarie a garantire la corretta installazione.

6.10 Service Management

6.10.1 Modello dei processi di ICT Governance

Sulla base del risultato dell'assessment e del modello di migrazione al cloud costruito potrebbe essere necessario progettare o modificare almeno i seguenti componenti di Governance ICT.

- Creazione del Service Desk per raccogliere tutti i ticket aperti dagli utenti o dal Servizio ICT per l'escalation verso il service provider. Attraverso il Service Desk sarà possibile instradare il ticket verso la struttura di supporto adeguata.
- Processi, procedure e strumenti di Incident Management che comprendono:
    - processi, procedure e strumenti di escalation;
    - processi, procedure e strumenti di event management;
    - processi, procedure e strumenti di verifica dello stato dei ticket.
- Processi, procedure e strumenti di apertura dei ticket verso i Cloud Provider.
- Processi, procedure e strumenti di Change Management.
- Processi, procedure e strumenti di Service Management che comprendono:
    - processi, procedure e strumenti di SLA Management;
    - processi, procedure e strumenti di verifica dei consumi delle risorse.
- Processi, procedure e strumenti di Data Breach Management.

Ad integrazione delle attività di design dei processi di Service Management potrebbe essere necessario definire:

- perimetro e del livello di supporto/intervento per ogni componente infrastrutturale ed applicativo attraverso un documento concordato fra Amministrazione e i Cloud Provider;
- ruoli e responsabilità del Service Manager e Demand Manager dell'Amministrazione e del Cloud Provider;
- tabelle RACI dei processi di ICT Governance codificati.

6.10.2 Creazione della Control Room attraverso Monitor servizi, Dashboard,SOC, NOC, Billing, etc

Definire con i Cloud Provider il piano di installazione e di configurazione di tutti gli strumenti di monitoring del servizio previsti dal contratto, comprensivo di configurazione delle credenziali per tipologia di utenti, formazione al personale dell'Amministrazione, test e collaudo. Il piano è parte integrante delle linee guida.

La control room è una funzione che può risiedere in una workstation e che non necessita di un ambiente dedicato. È invece importante che nello strumento siano integrate tutte le informazioni necessarie al Service Management.

6.10.3 Identificazione dei punti di prelievo delle performance per le metriche SLA

I Cloud Provider producono un documento di specifiche funzionali e di integrazione che definisca per ogni SLA concordato dove sono collocate le informazioni (mappa) per la valutazione delle performance ed il metodo di trasferimento delle informazioni ai sistemi di reporting e di dashboard concordati nel contratto. Questo è un documento è parte integrante del presente documento.

6.11 Organizzazione

6.11.1 Ruoli e responsabilità

Durante la realizzazione de progetto di migrazione a Cloud è utile prevedere una revisione dell'organizzazione ICT in modo da poter governare il diverso metodo di delivery dei servizi, dove sussiste la potenziale interdipendenza con il Cloud Provider. I nuovi ruoli da inserire nell'organizzazione si suggerisce siano almeno i seguenti:

- **Service Manager**: ha la responsabilità del dialogo e della collaborazione con il Cloud Provider, verifica l'aderenza ed rispetto dei termini contrattuali e degli SLA concordati. Gestisce gli incident e le relative procedure di escalation anche con l'eventuale supporto del **Operation Manager**. Collabora con il Change Manager per procurare le risorse, E' responsabile della **Control Room** uno strumento che dovrà essere però governato da una risorsa specifica del servizio ICT.
- **Demand Manager**: ha la responsabilità di valutare, approvare e programmare le richieste di evoluzione dei servizi ICT (change) forniti. Collabora con il Service Manager e le altre funzioni ICT per concordare le modalità e le tempistiche di realizzazione delle change.
- **Security Manager**: ha la responsabilità di garantire la realizzazione tecnica delle delle policy di ICT Governance, Security ed Availability Management. Trasforma i processi e le procedure esistenti in Security Policies. Supporta le altre funzioni ICT e l'azienda della definizione degli Standard, coordinandosi con gli altri ruoli aziendali per assegnare le responsabilità all'interno dell'organizzazione. Garantisce il livello di sicurezza dei servizi del Cloud Provider, delle nuove applicazioni e/o tecnologie prima della applicazione in produzione. Si coordina con il DPO e con gli altri ruoli aziendali per definire le azioni da applicare in caso di violazione.
- **Service Desk**: ha la responsabilità di fornire un Single Point Of Contact (SPOC) con gli utenti. Gestisce i rapporti con il Contact Center del Cloud Provider. Organizza il flusso di richieste, le smista al servizio operativo di pertinenza e misura i tempi di risposta (quindi di fermo operativo).

Al fine di identificare le risorse all'interno dell'organizzazione si consiglia di utilizzare la seguente checklist:

Ruolo	Ruolo attuale	Ownership Processi	Responsabilità	Gap Conoscenze
Service Manager		Incident Management Service Management	Erogazione dei servizi secondo gli SLA concordati	
Demand Manager		Change Management	Evoluzione servizi secondo planning e budget	
Security Manager		Data Breach	Rispetto delle norme aziendali di sicurezza e privacy	
Service Desk		Service Desk	Tempistica e qualità della risposta	
Control Room		Monitor Servizi	Controllo dei servizi	

6.11.2 Formazione

In relazione alla Gap Analysis sopra descritta, relativa alle conoscenze delle risorse, potrà essere definito un piano di formazione e coaching secondo le seguenti direttrici:

Formazione delle competenze tecniche

- Formazione degli strumenti forniti dai Cloud Provider
- Metodi e strumenti di gestione delle risorse in Cloud
- Formazione degli strumenti di monitor (NOC, SOC, etc,)
- Formazione sugli strumenti di accounting e billing dei Cloud Provider
- altro indicato dal cloud provider

Formazione delle competenze di ICT Governance

- Formazione generale ITIL a tutto il team ICT
- Formazione individuale riferita al ruolo sui processi da governare
- Formazione sulla Cybersecurity
- Contract Management

Il piano completo di formazione potrà essere completato dopo la sottoscrizione del contratto con i Cloud Provider ed erogato nei dodici mesi successivi.

6.12 Facilities

Questa sezione più che essere un WP rappresenta una checklist indicativa e non esaustiva, relativa alle facilities e ai vincoli di natura logistica che potrebbero essere identificati per completare il piano esecutivo dettagliato.

Codice	Owner	Descrizione
		Definizione orari per le attività operative presso le sedi dell'Amministrazione
		Definizione degli orari di possibile sospensione del servizio
		Definizione degli orari per il trasferimento dei dati in rete
		Regolamenti di sicurezza da applicare (multipli)
		Norme relative alla privacy da rispettare (multipli)
		Metodi di accesso ai locali dell'Amministrazione
		Metodi di accesso ai locali del Cloud Provider
		Spazi richiesti presso l'Amministrazione
		Contatti (Mobile, email) del team di progetto
		Area condivisa per la documentazione di progetto
		……

I PROTAGONISTI DEL CANTIERE

Hanno preso parte ai lavori del Cantiere Trasformazione Digitale – "Cloud Transformation":

- Diego **Antonini**, Presidente - **Insiel SpA**
- Marina **Apicella,** B2B Public Sector Account Manager – **Samsung Electronics Italia**
- Francesco **Appratto**, Ufficio Programmazione e Sviluppo delle Banche Dati, Piattaforma Digitale e Servizi IT - **ANAC**
- Vito **Baglio**, Responsabile Centro di Eccellenza Cloud - **CSI Piemonte**
- Domenico **Barbieri,** Dirigente U.O.S. Sistema informativo e statistico - **INMP**
- Giovanni **Bartolomeo**, Responsabile Sistema Informativo DAP – Datawarehouse - **Ministero della Giustizia**
- Luca **Bertelli**, Responsabile Data Center, Sistemi e Cloud - **Comune di Firenze**
- Massimo **Bisogno**, Dirigente Ufficio Università, Ricerca e Innovazione - **Regione Campania**
- Francesco **Castano**, Direttore Direzione Sistemi Informativi e Agenda Digitale - **ACI Informatica**
- Giuseppe **Ceglie**, Technology Innovation and Cloud services Director - **Aria SpA**
- Massimo **Crubellati**, Country Manager Italia - **CAST**
- Gemma **De Angelis**, Responsabile Tecnologie e ICT e Innovazione - **Agenzia del Demanio**
- Mauro **Fioroni**, Direttore Servizio Informatica - **Senato della Repubblica**
- Giacomo **Fioroni**, Responsabile Ufficio Progetto Smart City - **Comune di Trento**
- Leandro **Gelasi**, Dirigente Settore IT Operations - **Corte dei conti**
- Alessandro **Landi**, Responsabile area infrastrutture per Cloud Transformation - **Regione Emilia-Romagna**
- Barbara **Leoni**, Responsabile UOC Gestione dei sistemi informativi - **Comune di Reggio Emilia**
- Francesco **Lombardo,** Sales Executive - **DXC Technology**
- Nicola **Mangia,** Italy Public Sector General Manager - **DXC Technology**
- Doriano **Maranzana**, Direttore Divisione Servizio Clienti- **Insiel SpA**
- Enrico **Mattioni**, Responsabile Servizio Sistemi Informativi - **COVIP**
- Mattia **Menghi**, Servizio Agenda digitale, Smart City, Sistemi, Settore Sistemi Informatici Associati - **Unione Vallesavio**
- Diego **Mezzina**, Responsabile IT Security - **Insiel SpA**
- Marco **Romoli**, Senior Account Executive - **CAST**
- Fabrizio **Ronci**, Responsabile Ufficio VI Direzione Sistema Informativo della Fiscalità - **Ministero dell'Economia e delle Finanze**
- Ettore **Sala**, Responsabile Sicurezza Informatica ed Architetture Infrastrutturali - **LAZIOcrea SpA**
- Anna **Sappa**, Dirigente Ufficio esercizio infrastrutture ICT - **INAIL- DCOD**
- Francesco Paolo **Schiavo**, Direttore dei Sistemi Informativi e dell'Innovazione - **Ministero Economia e Finanze**
- Francesco **Seminaroti,** Head of Enterprise and Public Sector, IM B2B – **Samsung Electronics Italia**
- Michele **Slocovich**, Solution Design Director - **CAST**
- Leonardo **Tininini**, Responsabile Servizio Gestione infrastruttura IT - **ISTAT**
- Stefano **Tomasini**, Direttore Centrale Organizzazione Digitale - **INAIL- DCOD**
- Loredana **Vajano**, Direttore Servizio Programmazione, Bilancio e Digitalizzazione - **Agcom**
- Raffaele **Visciano**, Referente per la sicurezza del Dipartimento delle Finanze - Laboratorio Infrastrutture e Servizi di Rete - **Ministero dell'Economia e delle Finanze**

CAST
Software Intelligence for Digital Leaders

DXC.technology

SAMSUNG