



Città metropolitana
di Roma Capitale



PIANO STRATEGICO ICT

METROPOLITANO

2024 – 2026

AGGIORNAMENTO 2025

VERSIONE 2.0

Indice dei contenuti

INTRODUZIONE.....	2
Componenti strategiche per la trasformazione digitale.....	3
1. Organizzazione e Gestione del Cambiamento.....	4
Analisi della maturità digitale	8
Azioni Strategiche	9
2. Le principali iniziative	15
2.1. Potenziamento del Datacenter.....	15
2.2. Revisione del Portafoglio Applicativo	16
2.3. Gli Sportelli Telematici e Il Sistema Integrato Metropolitan.....	18
2.4. Lo sviluppo del Portale del Cittadino.....	23
3. Linee di Finanziamento ulteriori rispetto a quelle previste dal Piano Esecutivo di Gestione dell'Ente.	27

INTRODUZIONE

Il **Piano Strategico ICT della Città metropolitana di Roma Capitale** (di seguito "**Piano Triennale CmRC**") presenta la visione strategica IT dell'Ente metropolitano per gli sviluppi futuri del territorio metropolitano, andando a delineare, in coerenza con il quadro definito a livello nazionale e internazionale, e in filiera con il Piano Strategico Metropolitan, i primi obiettivi e le relative strategie prioritarie per la Città metropolitana di Roma Capitale e per l'intero territorio metropolitano, riservandosi di aggiornare ed integrare i contenuti attraverso un processo continuo di revisione e adeguandoli alle esigenze sopravvenute.

Il **Piano Triennale CmRC** intende la transizione digitale come un processo di trasformazione radicale e sistemica dell'organizzazione del lavoro e delle modalità di erogazione di taluni servizi al cittadino fondato sul paradigma dell'*open innovation*, in riferimento al quale si ritengono centrali i temi tra loro complementari della *condivisione* delle risorse, della conoscenza, delle competenze digitali diffuse, e della *cooperazione* verticale e orizzontale.

In quest'ottica, Città metropolitana di Roma Capitale intende sostenere e dare piena attuazione a un proprio percorso di trasformazione digitale che sia coerente con la strategia nazionale per il Digitale e al tempo stesso si caratterizzi per una spiccata originalità operativa imperniata sulla concretezza, l'efficacia e sulle peculiarità della nostra organizzazione e del territorio di riferimento.

A tal fine il **Piano Triennale CmRC** articola la sua azione e i suoi obiettivi su due piani fondamentali:

- l'efficacia dell'azione amministrativa in modo commisurato alla rilevanza del territorio amministrato e coerente con il profilo della propria mission istituzionale;
- lo sviluppo di strumenti e processi con funzione abilitante per innescare meccanismi virtuosi e partecipativi di promozione sociale ed economica del territorio agendo come **Hub di Servizio** per Comuni, Enti Locali, Cittadini e Imprese.

Componenti strategiche per la trasformazione digitale

La Digitalizzazione della Pubblica Amministrazione rappresenta oggi, nell'era post pandemica, una rinnovata opportunità di trasformazione sociale ed economica del Paese e dei territori. Modelli operativi, processi partecipativi e di governance che sino a poco tempo fa si pensavano fossero di difficile adozione, si sono tuttavia rivelati essere non solo sostenibili in termini attuativi ma anche rapidamente implementabili sia grazie a tecnologie innovative, mature ed effettivamente disponibili per una loro immediata adozione (Piattaforme Cloud, Strumenti di collaborazione, ecc.), sia grazie a una più compiuta maturità della collettività e di tutti gli stakeholders (*Citizen Digital Dexterity, Digital Citizenship Awareness*) che oggi, con maggiore consapevolezza del potenziale offerto dal Digitale, ne rivendicano un pieno sfruttamento.

In questo contesto, **il Piano Triennale CmRC** approccia la questione della transizione digitale dell'area metropolitana ispirandosi e allineandosi alle indicazioni e ai principi formulati nel Piano Triennale per l'Informatica nella PA 2024-2026, elaborato da AgID, sottolineando l'importanza di costruire un ecosistema digitale amministrativo capace di erogare servizi di qualità in modo proattivo e trasparente, riducendo al contempo la complessità burocratica.

Un elemento chiave di questo processo è la collaborazione istituzionale. La sinergia tra vari livelli di governo (centrale, regionale, locale) e la partecipazione attiva di cittadini e imprese sono essenziali per una trasformazione digitale efficace e sostenibile. È necessario promuovere piani condivisi e scambi di buone pratiche, garantendo che tutte le iniziative siano allineate con gli obiettivi strategici comuni.

Il ruolo del Responsabile per la Transizione al Digitale (RTD) è centrale in questo contesto. Questa figura deve guidare il cambiamento, coordinando le iniziative digitali e assicurando l'integrazione delle tecnologie nei processi amministrativi. La sua leadership È cruciale per sviluppare strategie digitali coerenti e monitorare l'efficacia delle implementazioni.

La diffusione delle competenze digitali tra il personale delle PA è un altro pilastro fondamentale. La formazione continua e l'acquisizione di competenze avanzate in ambiti tecnologici sono indispensabili per supportare la digitalizzazione. Collaborare con il settore educativo per sviluppare programmi formativi specifici e implementare sistemi di certificazione delle competenze contribuisce a creare una forza lavoro capace di affrontare le sfide digitali.

il Piano Triennale CmRC è ispirato anche al piano di azioni definito dal Ministero per l'Innovazione tecnologica e la Transizione Digitale (MITD) nella **Strategia Italia digitale 2026 (in seguito "Strategia 2026")** e nella **Strategia Nazionale per le Competenze Digitali**, nonché alle direttive del **Programma Digital Europe** e del **Digital Compass** formulato dalla Commissione europea a supporto delle sfide di digitalizzazione definite dalla Ue per la "decade digitale" 2020-2030, in risposta alla crisi del Covid-19. La specifica strategia del Piano Triennale CmRC sul digitale è stata formulata in correlazione con l'articolazione della Misura 1, e dei relativi Ambiti di intervento, del **Piano Nazionale di Ripresa e Resilienza (PNRR)**.

Inoltre, tutte le attività sono coerenti con quanto definito dall'**Autorità per la Cybersicurezza Nazionale**.

Città metropolitana di Roma Capitale intende perciò favorire una piena attuazione e valorizzazione della strategia digitale del Paese, garantendone l'efficacia per tutti gli stakeholders e per tutti i cittadini, raccordandola alle altre strategie e piani del territorio.

1. Organizzazione e Gestione del Cambiamento

Il **Responsabile per la Transizione al Digitale (RTD)** si impegna a promuovere la collaborazione tra i diversi servizi dell'organizzazione, favorendo l'integrazione di soluzioni tecnologiche innovative e la diffusione di una cultura digitale trasversale. La sua principale responsabilità è quella di guidare l'Amministrazione nel percorso di digitalizzazione, individuando le opportunità offerte dalle nuove tecnologie e sviluppando strategie mirate per implementarle in modo coerente con gli obiettivi organizzativi. A tal proposito, la Città metropolitana di Roma Capitale ha designato il Responsabile della Transizione Digitale, come figura di coordinamento all'interno dei Dipartimenti dell'Amministrazione (Atto di nomina del Sindaco n. 107 del 13.10.2022). Questa nomina ha l'obiettivo di guidare e supervisionare strategicamente la trasformazione digitale dell'Amministrazione, ottimizzando le operazioni e migliorando l'efficienza nella fornitura dei servizi pubblici. Inoltre, la Città metropolitana di Roma Capitale ha istituito il Dipartimento Transizione Digitale, una struttura specificamente dedicata alla digitalizzazione, che collabora strettamente con il RTD per garantire un approccio integrato e coordinato.

L'obiettivo di digitalizzazione dell'Ente non può prescindere da una piena sinergia con gli obiettivi nazionali richiamati nel Piano Triennale per l'Informatica; pertanto, anche i principi guida ivi richiamati sono pienamente applicabili al contesto metropolitano. CmRC è attenta a tutte le evoluzioni in atto in modo da adeguare tutti i servizi erogati ed in corso di erogazione verso l'interno e verso i Comuni.

- **digital & mobile first** (digitale e mobile come prima opzione): realizzare servizi primariamente digitali;
- **digital identity only** (accesso esclusivo mediante identità digitale): adottare in via esclusiva sistemi di identità digitale definiti dalla normativa;
- **cloud first** (*cloud* come prima opzione): valutare e adottare primariamente il paradigma cloud;
- **servizi inclusivi e accessibili**: progettare servizi pubblici digitali che siano inclusivi e che vengano incontro alle diverse esigenze delle persone e dei singoli territori;
- **dati pubblici un bene comune**: valorizzare il patrimonio informativo della pubblica amministrazione quale bene fondamentale per lo sviluppo del Paese; deve essere valorizzato e reso disponibile ai cittadini e alle imprese, in forma aperta e interoperabile;
- **interoperabile by design**: progettare servizi pubblici digitali in modo da funzionare in modalità integrata e senza interruzioni in tutto il mercato unico esponendo le opportune API;
- **sicurezza e privacy by design**: i servizi digitali devono essere progettati ed erogati in modo sicuro e garantire la protezione dei dati personali;
- **user-centric, data driven e agile**: sviluppare i servizi digitali, prevedendo modalità agili di miglioramento continuo, partendo dall'esperienza dell'utente e basandosi sulla continua misurazione di prestazioni e utilizzo;
- **once only**: evitare di chiedere ai cittadini e alle imprese informazioni già fornite.

Tutte le Pubbliche Amministrazioni mondiali sono impegnate nella Trasformazione Digitale che si pone i seguenti obiettivi:

- avvicinare la PA ai cittadini e alle imprese, intervenendo proattivamente nei momenti in cui i singoli cittadini hanno bisogno di servizi e/o indicazioni;
- semplificare i servizi ed i loro canali di accesso fornendo ad ogni persona il canale che trova più comodo (canale fisico, digitale via computer, app via telefono, ...);
- ridurre gli impatti ambientali della propria attività, riducendo il consumo della carta e favorendo un corretto utilizzo dei dati forniti dai cittadini e dalle imprese;

-
- integrarsi con le altre PA in modo da fornire un servizio complessivo a cittadini ed imprese evitando l'interfacciamento con più enti.

Si profila, quindi, un modello di digitalizzazione della società che il Piano Triennale per l'informatica nella Pubblica Amministrazione - a complemento del consolidato paradigma della Smart City -, ha voluto sintetizzare nel concetto di "Smart community", fortemente orientato all'inclusione digitale, alla formazione dei cittadini e alla innovazione del tessuto imprenditoriale diffuso.

In questo quadro il Piano considera cruciale la funzione di "indirizzo dell'innovazione" che "Comuni e città" devono svolgere al fine di:

- migliorare la qualità della vita dei cittadini;
- innovare il contesto imprenditoriale del territorio nazionale;
- generare un impatto rilevante sull'efficienza della Pubblica Amministrazione secondo criteri generali di accessibilità e innovazione.

In linea con la programmazione centrale, si può dunque parlare per le Pubbliche Amministrazioni Locali (PAL) di una triplice mission in riferimento alla transizione digitale: in primis c'è una funzione abilitante verso dipendenti, cittadini e imprese, fondata da un lato sulla promozione di competenze digitali (upskilling e reskilling), dall'altro sulla condivisione di asset strategici e sull'innescare di processi innovativi (open innovation, Intelligent Metropolitan Framework, appalti d'innovazione); in secondo luogo vi è l'esigenza di veicolare e sviluppare misure e politiche che favoriscano una digitalizzazione diffusa e inclusiva dei territori (solidarietà digitale, interoperabilità, piattaforme locali, connettività ultraveloce); infine vi è il proposito di orientare la governance verso criteri di efficienza, inclusione, collaborazione.

Nell'ambito di questa articolata mission relativa alla transizione digitale, la CmRC costituisce un decisivo anello di congiunzione tra le diverse scale di governo, e con il **Piano Triennale CmRC** può svolgere un ruolo di "messa a terra" di principi e linee strategiche generali, in un'ottica di integrazione tra le sfide che riguardano i processi di digitalizzazione "interna" con quelle che riguardano il governo dei processi di digitalizzazione "esterna" della società e dei territori. CmRC intende perciò assumere un ruolo di coordinamento dei comuni metropolitani finalizzato all'attuazione delle strategie e iniziative europee e nazionali per la transizione digitale della società e dei sistemi produttivi, favorendo l'incontro e l'armonizzazione delle strategie con i processi spontanei, le progettualità, le risorse e i bisogni espressi dal territorio.

Il **Piano Triennale CmRC**, con riferimento alla sua mission "esterna", definisce 6 obiettivi fondamentali:

1. promuovere le competenze e i diritti digitali;

2. rilevare i bisogni digitali;
3. favorire collaborazione e Open Innovation;
4. promuovere interoperabilità e infrastrutture locali e decentrate;
5. promuovere la consapevolezza del valore dei dati e il loro riuso;
6. garantire e supportare la solidarietà digitale.

Dal punto di vista pratico, il Dipartimento per la Transizione Digitale, in costante collaborazione con Capitale lavoro e con altre realtà private ha già attivato le seguenti attività:

- stesura degli accordi per i Comuni che consentono agli stessi di ottenere i finanziamenti stanziati dal PNRR tramite fornitura diretta dei servizi richiesti (quali PagoPA, AppIO, CIE, SPID, ...) che comprende anche **l'assistenza manutentiva** da parte di CMRC dei medesimi servizi
- rilevazione dei fabbisogni dei Comuni.

Nel corso del 2025 verranno portate avanti queste ulteriori attività:

- rilevazione dei fabbisogni dei Dipartimenti dell'ente;
- avanzamento dello stato di attuazione definito negli accordi con i Comuni interessati;
- ristrutturazione del processo digitale interno degli altri Dipartimenti al fine di soddisfare le esigenze di tutti evitando duplicazioni;
- ottenimento di ulteriore personale per il supporto tecnico e amministrativo;
- erogazione di ulteriori servizi rispetto al progetto "smart metro" e agli altri servizi previsti dal PNRR;
- gestione tecnica e amministrativa del WiFi metropolitano (eventualmente includendo anche il wifi all'interno delle sedi istituzionali dell'Ente);
- supporto nella redazione di piani formativi per la diffusione di cultura digitale presso i Comuni interessati;
- erogazione da parte di CmRC e dei suoi partner di alcuni specifici interventi formativi sul tema della cybersecurity.
- creazione di specifici Tech Lab (da articolare in tematici e territoriali) capaci di innescare processi di open innovation sul territorio.
- Aumento della resilienza dell'Ente tramite interventi tecnici/organizzativi legati al mondo della Cybersecurity, in un'ottica di adesione/allineamento ai dettami della NIS2

La sfida della digitalizzazione dell'Ente a supporto del più ampio **Piano Strategico Metropolitan** non sarà limitata ad un "semplice" rinnovamento tecnologico ma

dovrà necessariamente prevedere una profonda e progressiva revisione dei sistemi IT, del modello organizzativo e operativo, dando altresì corso a quel processo di trasformazione culturale e di servizio che interpreta il digitale come un volano effettivo di cambiamento nelle organizzazioni.

Per perseguire gli obiettivi attesi da un tale percorso programmato ed ottenere i più ampi benefici, non si potrà prescindere dal coinvolgimento e supporto di tutte le Istituzioni pubbliche sia a livello centrale che locale, non solo al fine di favorire le più ampie sinergie operative ma anche al fine di poter contare sulla disponibilità di adeguate e necessarie risorse economiche e strumentali.

In questo scenario, anche grazie ad una preliminare attività di analisi sullo stato di digitalizzazione dell'Ente, ovvero sulla capacità di sfruttare le nuove tecnologie a beneficio di un'Amministrazione maggiormente efficace, trasparente e sempre più in grado di rispondere ai nuovi fabbisogni di tutti gli stakeholders pubblici e privati, sono state evidenziate le linee di azione che troveranno attuazione nei prossimi programmi di indirizzo e operativi, consapevoli sin d'ora che la loro implementazione possa effettivamente contribuire alla trasformazione dell'Ente sempre più al servizio della collettività, del territorio e del Paese.

Il Dipartimento intende avere un approccio molto concreto che parte da una logica consulenziale verso i Comuni e verso gli altri Dipartimenti al fine di erogare le informazioni e gli strumenti richiesti.

Analisi della maturità digitale

L'analisi dello stato di digitalizzazione dell'Ente verrà monitorato tramite una correlazione tra le **Priorità Strategiche Digitali** dell'Ente con gli **Abilitatori Digitali**, per meglio comprenderne i fattori critici di successo e, dall'altra, di **misurare la maturità della postura digitale** dell'Ente, comparando l'attuale livello di maturità con quello del settore pubblico di riferimento, al fine di definire quelle azioni strategiche di intervento che consentiranno di raggiungere gli obiettivi attesi.

Il digitale, infatti, richiede la capacità di scalare il modello operativo dell'Organizzazione, far crescere i talenti, stabilire la giusta mentalità e dotarsi delle necessarie capacità a livello di piattaforma tecnologica. Gli abilitatori alla base della digital strategy mirano quindi a:

Costruire una Piattaforma Tecnologica Digitale: creare una piattaforma tecnologica che sia adatta al digitale, che include AI/Data Analytics, Piattaforme per i Clienti interni, integrazione nell'ecosistema, IoT (Internet of Things), abilitata da un'infrastruttura sicura, elastica e flessibile.

Adottare un Modello Operativo Digitale: migliorare l'abilità di sviluppare le capacità digitali, su scala, in modo predicibile e ripetuto, abbracciando nuovi modi di lavorare, promuovendo una cultura *digital-ready*, allineando la struttura organizzativa e decisionale, implementando pratiche di gestione finanziaria e di approvvigionamento appropriate.

Si prevede l'esecuzione periodica di questo tipo di rilevazione a supporto della misurazione dei progressi dell'esecuzione del piano per la componente di transizione digitale.

Azioni Strategiche

Sulla base delle risultanze dell'assessment preliminare effettuato e degli obiettivi di trasformazione digitali delineati dal Piano Triennale AgID, il focus prioritario, attualmente in corso ed in parte già realizzato, è quello della **revisione e innovazione dei sistemi informativi, dei modelli organizzativi e operativi dell'Ente**.

Obiettivo principale di questa azione è l'adeguamento e lo sviluppo dei sistemi informatici dell'Ente, attraverso un **progressivo programma di revisione, razionalizzazione ed innovazione delle componenti tecnologiche ed informative attuali** che tenga conto dell'obsolescenza delle tecnologie esistenti e dei relativi oneri di manutenibilità, della valorizzazione degli *asset* infrastrutturali già acquisiti e del loro sviluppo futuro e, infine, dei nuovi fabbisogni informativi a supporto di una più efficace azione di governo dell'Ente in coerenza con lo sviluppo del PSM (Piano Strategico Metropolitan) e dell'azione politica sul territorio.

Non si potrà prescindere, pertanto, dalla progressiva valutazione e adozione di tecnologie innovative quali il **Cloud Computing**, l'**Internet of Things** e l'**Intelligenza Artificiale** nonché dell'impatto di altre tecnologie abilitanti quale il **5G**, in particolare in ambito mobilità, sicurezza e ambiente.

Il **modello a piattaforma**, dove le funzionalità fondamentali, trasversali e riusabili sono sviluppate centralmente e messe a disposizione dei diversi sistemi informativi, dovrà continuare ad essere il modello di riferimento per lo sviluppo dei

nuovi sistemi IT secondo un paradigma infrastrutturale più agile in ottica di *componibilità* dei servizi, non solo facendo leva sulla disponibilità di piattaforme tecnologiche già sviluppate a livello centrale come PagoPa, SPID, Fatturazione Elettronica, ecc. o, previste in prospettiva dalla strategia nazionale sul digitale come il **CLOUD per la Pubblica Amministrazione**, ma anche sviluppandone di nuove mirando, tra l'altro, a facilitare l'integrazione con i sistemi interni, come conseguenza del processo di razionalizzazione degli attuali sistemi o integrandole dall'esterno attraverso l'ecosistema pubblico e privato tra quelle già disponibili e/o riutilizzabili. Tale modello, consentirà di sollevare l'Amministrazione dalla necessità di dover realizzare e/o acquistare funzionalità comuni a più sistemi software, semplificando la progettazione, riducendo i tempi e i costi di realizzazione di nuovi servizi e garantendo maggiore sicurezza informatica.

Parimenti, particolare attenzione sarà posta sulla **progettazione degli applicativi e dei servizi digitali interni ed esterni promuovendo la *Total Experience*** dell'utente, ovvero una esperienza digitale totale per tutti gli utenti dei servizi digitali che coniughi da una parte la soddisfazione degli utenti interni nell'utilizzo e sviluppo dei servizi metropolitani e, dall'altra, quella degli stakeholders esterni secondo una logica di maggior coinvolgimento e propensione nell'utilizzo dei servizi digitali stessi.

Si terrà in considerazione, inoltre, l'adozione di **nuovi paradigmi di servizio virtuali e/o in mobilità**, come ad esempio la digitalizzazione delle procedure amministrative e la collaborazione a distanza, già sperimentati con successo in alcuni ambiti che consentono di garantire quell'equità digitale di fruizione a distanza dei servizi amministrativi di cui ciascun utente del territorio dovrebbe beneficiare.

Tra gli interventi già effettuati, è di particolare rilievo **la revisione dell'organizzazione IT e dei processi di governance** in coerenza con la trasformazione del sistema informatico e delle nuove esigenze di governo dell'Amministrazione digitale, favorendo lo sviluppo, la diffusione e il consolidamento di competenze e skills tecnologici necessari a tutti i livelli dell'amministrazione, investendo in formazione specialistica e stimolando quel cambiamento culturale che pone il digitale al centro dell'azione amministrativa quale elemento di supporto e non sussidiario alle competenze e capacità delle risorse umane che costituiscono e restano l'asset principale dell'Ente anche e soprattutto per continuare a mantenere vivo questo processo virtuoso di innovazione continua ormai imprescindibile per una PA capace di modellare e indirizzare rapidamente le esigenze del territorio e contribuirne fattivamente allo sviluppo socio-economico.

Si riportano, di seguito, i punti qualificanti di questa nuova organizzazione:

1. Valorizzazione del patrimonio informativo

La capacità di sapere estrarre valore dai dati gestiti, traducendoli in informazioni utili all'azione governativa e all'erogazione di servizi a valore aggiunto per la collettività costituisce un'azione fondamentale e imprescindibile della strategia IT metropolitana. L'esigenza di raccogliere, strutturare e condividere opportunamente i dati secondo criteri e metodologie appropriate, garantendo al contempo adeguati standard di sicurezza, costituisce una direttrice di intervento prioritaria alla trasformazione digitale dell'Ente. Tale azione si rende necessaria non solo per favorire una piena fruizione delle tecnologie innovative, alla base delle quali la capacità di elaborare dati ben strutturati risulta condizione indispensabile di applicazione ma, soprattutto, per garantire una gestione qualitativamente più rigorosa e certificata delle fonti informative tale da poter sviluppare servizi e politiche d'intervento maggiormente accurate e mirate per il territorio e i cittadini.

A tale scopo, si intende:

- **sfruttare le basi di dati di interesse nazionale**, ovvero basi di dati affidabili, omogenee per tipologia e contenuto, rilevanti per lo svolgimento delle funzioni istituzionali e per fini di analisi che costituiscono l'ossatura del patrimonio informativo pubblico e che possono effettivamente contribuire a completare le informazioni di interesse per l'azione amministrativa sia centrale che locale grazie ad un meccanismo di reciproca condivisione verso gli stakeholders dell'Ente ed evitare, ad esempio, di chiedere al cittadino o all'impresa più volte la stessa informazione - *principio once only*;
- **condividere i dati di pubblico interesse in modo aperto secondo il modello *open data***, ovvero promuovendo la pubblicazione dei dati dell'Ente, secondo opportune modalità e standard di formattazione, consentendo in tal modo il libero utilizzo da parte di chiunque e per qualunque scopo, anche commerciale, purché non soggetti a particolari restrizioni;
- **adottare vocabolari controllati e modelli dei dati** che costituiscono un modo comune e condiviso per organizzare codici e nomenclature ricorrenti in maniera standardizzata e normalizzata (vocabolari controllati) e una concettualizzazione esaustiva e rigorosa nell'ambito di un dato dominio (ontologia o modello dei dati condiviso).

L'obiettivo dell'iniziativa si concretizza, dunque, nel **potenziamento della DATA Governance** dell'Amministrazione in modo tale da sfruttare pienamente l'ampio

capitale informativo ad oggi gestito e abilitare altresì sia l'accesso e la fruizione di informazioni già disponibili presso altre banche dati e sistemi pubblici sia la raccolta ed elaborazione di nuove informazioni da fonti alternative di prossimità e mobilità che grazie alle nuove tecnologie di nuova generazione quali sensori RFID, IoT, e 5G sarà possibile acquisire con maggiore immediatezza ed accuratezza.

2. Potenziamento continuo della Sicurezza Informatica

Con la propensione ad una maggiore spinta di digitalizzazione dell'Ente ed il conseguente sviluppo di sistemi di gestione dei servizi ICT (Information and Communication Technologies), sempre più complessi e accessibili remotamente, la sicurezza informatica continua ad essere una priorità del Piano Strategico Metropolitan per l'Information Technology che si intende sviluppare e potenziare sotto ogni dimensione, tecnologica e culturale. L'obiettivo è quello di **rivedere in modo organico e strategico tutte le componenti della funzione di sicurezza**, come organizzazione, processi e tecnologie in modo tale da adeguarle tempestivamente alle *best practices* internazionali e agli standard nazionali, a maggior tutela dei dati e della privacy.

Ci si prefiggono i seguenti obiettivi:

- ✓ Effettuare una "fotografia" dello stato attuale dell'Ente rispetto alle principali norme e direttive italiane ed europee riguardanti la sicurezza informatica;
- ✓ Delineare una roadmap per l'implementazione delle misure correttive, miglioramenti e mitigazioni emerse dalla fase precedente in modo da far convergere la postura di sicurezza dell'Ente in conformità delle leggi e delle *best practices* locali e internazionali;
- ✓ Diminuire il fattore di rischio riferito agli attacchi informatici aumentando la resilienza operativa attraverso l'implementazione di soluzioni, prodotti, processi e procedure che riescano ad orchestrare in maniera efficace ed efficiente la gestione della crisi. Si inizierà con un'attività di Cybersecurity Maturity Assessment, erogata con l'ausilio di Framework, procedure e analisi tecniche su tutto il perimetro dell'Ente, che si baserà principalmente (ma non solo) sui 3 pilastri che rappresentano i riferimenti pratici e normativi per la sicurezza ICT delle Pubbliche Amministrazioni:

1. Le misure minime di sicurezza ICT emanate dall'AgID;

2. La direttiva europea NIS2 (Network and Information Security Directive);

3. Legge L. 90/2024 “Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici” (c.d. “Legge sulla Cybersicurezza”).

Il valore aggiunto che si vuole perseguire in questa fase non si limita esclusivamente alla competenza e alla padronanza delle tematiche elencate ma comprende anche la capacità di estendere l'efficacia della misurazione del livello di sicurezza, e le relative raccomandazioni per sanare il divario che vi è tra la conformità e i risultati attesi, includendo nell'analisi Framework internazionalmente riconosciuti come, per esempio, il Cybersecurity Framework del NIST (CSF 2.0) e il CIS Critical Security Controls v8, L'attività permetterà di avere una visione completa dell'organizzazione utile sia per le valutazioni nell'immediato sia per eventuali modifiche organizzativo/tecnologiche future. A valle di questa prima raccolta informativa, verrà eseguita una verifica della conformità delle misure e dei processi di sicurezza informatica in essere rispetto ai requisiti menzionati precedentemente tramite un'analisi generale e comprensiva di tutti gli aspetti relativi agli ambiti di sicurezza (tecnologici, organizzativi, normativi e procedurali).

Per la conduzione dell'attività si procederà alla raccolta delle informazioni, attraverso la tecnica mista dell'intervista ai Responsabili di processo, integrata con l'analisi della documentazione in uso presso l'Ente. A conclusione delle attività di conduzione delle interviste e di studio della documentazione raccolta, verrà eseguita un'analisi globale e la normalizzazione delle informazioni raccolte al fine di valutare il gap, sia a livello organizzativo che tecnologico, rispetto ai requisiti dell'AgID, della NIS2, della Legge L90/2024 e agli altri Framework succitati. Il principale risultato dell'attività di Gap Analysis sarà la produzione di un Report Generale di Assessment e Gap Analysis con la descrizione dei principali interventi evolutivi (di natura tecnologico-organizzativa) necessari per colmare eventuali gap rispetto alla normativa e migliorare il livello di maturità ed efficacia delle attuali misure di sicurezza adottate dall'Ente. A seguito delle interviste condotte con gli stakeholder di riferimento e i test operativi eseguiti sul perimetro dell'Ente, verranno prodotti dei documenti che riporteranno i risultati dell'analisi effettuata, in cui verranno evidenziate eventuali scoperture con associato un indice di criticità, e una roadmap di interventi da compiere, di breve, medio e lungo termine, per mitigare l'esposizione al rischio. La lista di priorità degli interventi verrà definita in base all'indice di rischio associato alla scoperta, precedentemente menzionato, e alla complessità dell'intervento stesso.

Le tematiche che verranno affrontate saranno:

-
- Misure minime di sicurezza ICT per le Pubbliche Amministrazioni Agid
L'adeguamento alle misure minime è a cura del responsabile della struttura per l'organizzazione, l'innovazione e le tecnologie, come indicato nel CAD (art. 17) o, in sua assenza, del dirigente designato. Il dirigente responsabile dell'attuazione deve compilare e firmare digitalmente il "Modulo di implementazione" allegato alla Circolare 18 aprile 2017, n. 2/2017. Secondo la circolare, le misure minime di sicurezza devono essere adottate da parte di tutte le Pubbliche Amministrazioni entro il 31 dicembre 2017. Le misure consistono in controlli e messa in atto di natura tecnologica, organizzativa e procedurale e permettono alle Amministrazioni di valutare il proprio livello di sicurezza informatica e di adeguarsi ad esso. A seconda della complessità del sistema informativo a cui si riferiscono e della realtà organizzativa dell'Amministrazione, le misure minime possono essere implementate in modo graduale seguendo tre livelli di attuazione:
 - Minimo: è quello al quale ogni Pubblica Amministrazione, indipendentemente dalla sua natura e dimensione, deve necessariamente essere o rendersi conforme;
 - Standard: è il livello, superiore al livello minimo, che ogni amministrazione deve considerare come base di riferimento in termini di sicurezza e rappresenta la maggior parte delle realtà della PA italiana;
 - Alto: deve essere adottato dalle organizzazioni maggiormente esposte a rischi (ad esempio per la criticità delle informazioni trattate o dei servizi erogati), ma anche visto come obiettivo di miglioramento da parte di tutte le altre organizzazioni.
 - Direttiva Europea NIS2 La NIS2 (Network and Information Security Directive) è una direttiva europea che punta a rafforzare la sicurezza informatica nell'UE. Entrata in vigore il 17 gennaio 2023, la direttiva dovrà essere recepita dai singoli Stati membri entro il 17 ottobre 2024. Per rispettare la Direttiva NIS2 a livello tecnico in ambito cybersecurity, le organizzazioni devono implementare una serie di misure e pratiche per garantire la sicurezza delle proprie reti e sistemi informativi. Le attività possono essere suddivise in macroaree che coprono l'intero ciclo di vita della gestione della sicurezza, dalla prevenzione alla risposta agli incidenti.
 - Legge L90/2024 (c.d. "Legge sulla Cybersicurezza") La legge 90/2024. sulla cybersecurity "Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici" rappresenta un passo cruciale per il rafforzamento della cybersicurezza nazionale in Italia in quanto ha come obiettivo quello di introdurre e armonizzare un ventaglio

molto ampio e variegato di temi legati al mondo della cybersecurity: dalla governance agli obblighi di notifica degli incidenti, dai requisiti di cybersicurezza nei contratti pubblici alle preclusioni per l'assunzione di alcune tipologie di professionalità provenienti dal mondo della cybersecurity pubblica e della sicurezza nazionale, dalla normativa che riguarda la responsabilità amministrativa degli enti fino all'estensione dei reati informatici. Il provvedimento, che ha visto una partecipazione attiva e diversificata delle forze politiche, pone l'accento sulla protezione delle infrastrutture digitali critiche e sulla prevenzione dei reati informatici. La nuova legge mira a rafforzare la cybersicurezza nazionale e contrastare i reati informatici attraverso una serie di misure innovative. Introduce, infatti, obblighi di notifica degli incidenti per PA ed enti strategici, inasprisce le pene per reati come l'accesso abusivo e il danneggiamento di sistemi informatici e, infine, potenzia le funzioni dell'Agenzia per la Cybersicurezza Nazionale – inclusa la creazione di un Centro Nazionale di Crittografia. La legge 90/2024 affronta anche la resilienza operativa digitale nel settore finanziario, estende l'uso di strumenti investigativi speciali per reati informatici gravi e migliora il coordinamento tra autorità in caso di attacchi. Introduce, inoltre, criteri di cybersicurezza negli appalti pubblici IT, prevede referenti per la cybersicurezza nelle PA e nuove misure per la sicurezza delle banche dati giudiziarie. La legge introduce anche il reato di "estorsione mediante attacco informatico", promuove la collaborazione pubblico-privato e programmi di formazione specialistica, con l'obiettivo di rafforzare l'autonomia tecnologica e industriale dell'Italia nel settore della cybersicurezza.

2. Le principali iniziative

2.1. Potenziamento del Datacenter

Al fine di poter garantire continuità nell'erogazione dei servizi interni all'Ente e di quelli erogati ai Comuni, ai cittadini ed alle imprese del territorio metropolitano, si sta effettuando un'analisi dello stato attuale dell'infrastruttura del Datacenter sia a livello fisico, sia a livello di sistemi di sicurezza e di procedure da seguire in caso di fault o cyber attack.

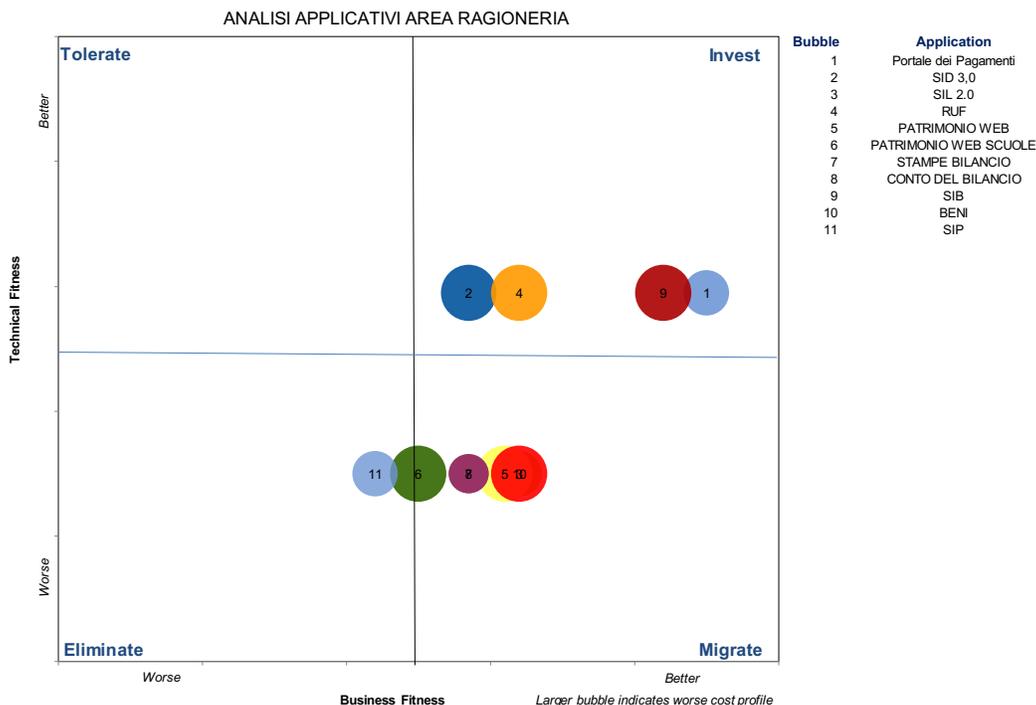
2.2. Revisione del Portafoglio Applicativo

La Città metropolitana di Roma Capitale ha avviato un processo di revisione di tutto il portafoglio applicativo attualmente in uso.

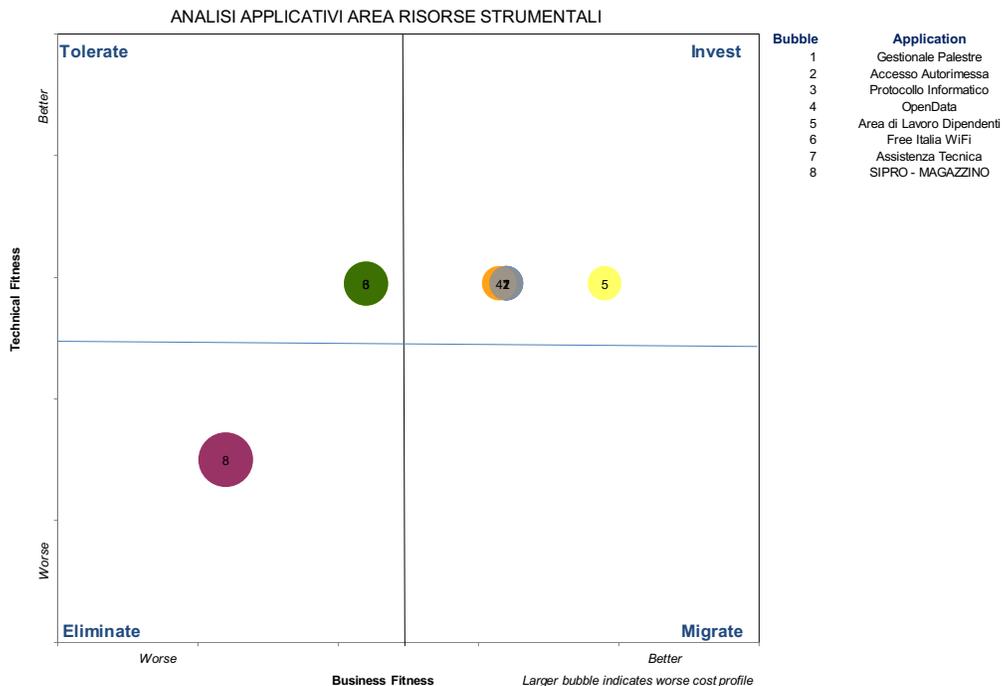
La scelta degli applicativi da esaminare è partita dall'analisi delle funzioni interne e ha riguardato un numero congruo di applicativi, includendo tutti quelli fondamentali ai processi/procedimenti cardine dell'Ente. Utilizzando i tool metodologici forniti, è stato possibile sintetizzare in una lettura quantitativa vari elementi utili a definire le priorità e i punti di intervento sia in ambito generale di indirizzo, sia nel dettaglio delle tecnologie utilizzate grazie all'analisi specifica dei punti di forza e di debolezza del singolo applicativo.

In particolare, l'assessment è stato finalizzato a valutare lo stato di "salute" degli applicativi in termini di utilizzo, costo di gestione e tecnologie utilizzate con l'obiettivo di definire le opportune priorità di intervento per il rinnovo e ammodernamento degli stessi.

Si riportano di seguito i risultati dell'assessment per gli applicativi delle aree funzionali principali.



Classe di utilizzo	Tipologia	Nome	Efficacia di Business	Costo di esercizio	Qualità Tecnica	Priorità intervento
System of Innovation	CUSTOM	Portale dei Pagamenti	5,0	3	3,5	1,7
System of Record	CUSTOM	SID 3,0	3,4	2	3,5	2,5
System of Record	CUSTOM	SIL 2.0	3,7	3	2,0	1,7
System of Record	CUSTOM	RUF	3,7	2	3,5	2,5
System of Record	CUSTOM	PATRIMONIO WEB	3,6	2	2,0	2,5
System of Record	CUSTOM	PATRIMONIO WEB SCUOLE	3,0	2	2,0	2,5
System of Record	CUSTOM	STAMPE BILANCIO	3,4	4	2,0	1,3
System of Record	CUSTOM	CONTO DEL BILANCIO	3,4	4	2,0	1,3
System of Record	CUSTOM	SIB	4,7	2	3,5	2,5
System of Record	CUSTOM	BENI	3,7	2	2,0	2,5
System of Record	CUSTOM	SIP	2,7	3	2,0	1,7



Classe di utilizzo	Tipologia	Nome	Efficacia di Business	Costo di esercizio	Qualità Tecnica	Priorità intervento
System of Differentiation	CUSTOM	Gestionale Palestre	3,7	5	3,5	1,0
System of Record	CUSTOM	Accesso Autorimessa	3,7	5	3,5	1,0
System of Differentiation	ALFRESCO/CUSTOM	Protocollo Informatico	2,7	3	3,5	1,7
System of Differentiation	DKAN/CUSTOM	OpenData	3,7	5	3,5	1,0
System of Record	CUSTOM	Area di Lavoro Dipendenti	4,4	5	3,5	1,0
System of Record	DRUPAL	Free Italia WiFi	2,7	3	3,5	1,7
System of Record	OSTICKET/CUSTOM	Assistenza Tecnica	3,7	5	3,5	1,0
System of Record	CUSTOM	SIPRO - MAGAZZINO	1,7	2	2,0	2,5

Il risultato dell'assessment ha permesso di definire in dettaglio il processo di revisione e sviluppo del parco applicativo dell'Ente.

Il processo prevede tra l'altro, lo sviluppo di nuovi software "cloud-native" caratterizzati da una struttura a silos. Tali caratteristiche permetteranno una maggiore flessibilità ed una maggiore semplicità di sviluppo anche in ottica di eventuale riuso da parte di altri Enti.

I primi applicativi sui quali si è iniziato a lavorare sono quelli in uso presso la Ragioneria Generale. La fase di sviluppo e test ha portato al rilascio, nell'anno scorso, dell'aggiornamento della piattaforma SID (Sistema delle Determinazioni Dirigenziali) e dell'Albo Pretorio, l'introduzione di un nuovo Protocollo Informatico di proprietà dell'Ente e, a seguire, si procederà all'aggiornamento delle altre piattaforme.

Al fine di completare il processo di digitalizzazione all'interno dell'Ente, sarà avviata un'analisi sistematica dei processi dell'Ente ad oggi non integrati al fine, in linea con le direttive AgID, di ottemperare al processo di semplificazione con il conseguente miglioramento dell'efficacia ed efficienza della gestione dei processi interni. A valle dell'individuazione di questi processi sarà avviata una prima fase di analisi dei requisiti e di fattibilità tecnica per poi poter essere integrati in maniera funzionale all'interno del Sistema Integrato Metropolitan.

2.3. Gli Sportelli Telematici e Il Sistema Integrato Metropolitan

Il processo di digitalizzazione dei servizi al cittadino e alle imprese porta come prima conseguenza un'attenta riorganizzazione e sviluppo degli strumenti informatici presenti nel nostro Ente.

Tale azione deve essere necessariamente affiancata da una incisiva e costante trasformazione degli attuali modelli organizzativi utilizzati dai vari Uffici.

Questo cambiamento organizzativo, insieme a quello tecnologico, rappresentano le due direttrici fondamentali su cui operare per il raggiungimento della trasformazione dei servizi della Città metropolitana di Roma Capitale come previsto della transizione digitale.

Con la realizzazione degli sportelli telematici, diventa essenziale la costituzione di un frame work che permetta di utilizzare tutta una serie di servizi di base centralizzati in modo da rendere i dati trattati omogenei a favore dell'intero frame work e facilitare in questo modo la governance e l'utilizzo di Business Intelligence.

2.3.1. Sportelli Telematici e processi amministrativi

Gli sportelli telematici consentono l'invio di istanze, dichiarazioni, documenti e ogni altro atto trasmesso dall'utente in via telematica e sono integrati con i servizi erogati in rete dalle pubbliche amministrazioni, inoltre devono garantire l'interoperabilità anche con sistemi esterni.

Diventa quindi necessario, in fase di progettazione, individuare i singoli procedimenti amministrativi condivisibili tra i diversi Uffici, uniformarli per quanto possibile, in modo da sviluppare singole funzioni comuni da condividere tra più servizi. Questo processo, se svolto correttamente, permetterà di uniformare e compattare le istanze amministrative, producendo una riduzione dei procedimenti e una semplificazione degli adempimenti richiesti ai cittadini.

Classificazione delle tipologie di sportello telematico

Possiamo catalogare in tre diversi modelli gli sportelli che dovranno essere realizzati dalla Città metropolitana di Roma Capitale:

Tipologia Sportello	Descrizione
Modello Semplice (one shot)	Questo modello di base gestisce una richiesta da parte del cittadino o dell'impresa, rilasciando una autorizzazione e/o un servizio a fronte di un eventuale pagamento se dovuto. (accesso agli atti, spese di segreteria, ecc.)
Modello Medio (one time)	Questo modello gestisce una richiesta fatta dal cittadino o dall'impresa, rilasciando una autorizzazione e/o un servizio a fronte di una istruttoria basata su una serie di documenti richiesti e di un pagamento. (autorizzazione agli scavi, occupazione temporanea suolo pubblico, ecc.)
Modello Complesso (more time)	Questo modello gestisce una richiesta fatta dal cittadino o dall'impresa, rilasciando una autorizzazione e/o un servizio a fronte di una istruttoria basata su una serie di documenti richiesti e di un pagamento iniziale. Inoltre, gestisce tutta una serie di procedimenti derivati (subentri, ispezioni, modifiche tecniche, ecc.) e di cicli di pagamento nel corso degli anni (autorizzazioni passi carrabili, concessioni scarico emissioni, ecc.)

2.3.2. Il Sistema Integrato Metropolitan

Il Sistema Integrato Metropolitan (SIM) è il nome del frame work specifico della Città metropolitana di Roma capitale. È costituito una serie di moduli che forniscono servizi di base agli sportelli telematici, da una serie di applicazioni base e da una serie di piattaforme web dell'ente.

Moduli di servizi di infrastruttura	
MySIR	Sistema Integrato di Rendicontazione interconnesso al sistema PagoPA per la gestione delle entrate e delle voci d'incasso e la gestione del contenzioso e del coattivo. Mette a disposizione sevizi di cooperazione per la gestione della anagrafica unica dei contribuenti, la gestione degli accertamenti, gestione dei ruoli e la creazione massiva degli avvisi di pagamento. Il modulo permette allo sportello telematico di pubblicare e gestire le richieste di pagamento attraverso il portale dei pagamenti MySIR e di ricevere le notifiche dei pagamenti ricevuti. MySIR attualmente utilizza base dati esterne e servizi tramite cooperazione applicativa con Siatel, Inipec, ANPR e Agenzia delle Entrate.
MyGateway	Il modulo fornisce servizi di infrastruttura per l'invio di notifiche, avvisi di pagamento, raccomandate RR, documenti, SMS, OTP, Posta Elettronica e PEC, utilizzando in cooperazione applicativa App IO, l'Ufficio Digitale di Poste Italiane e interfacciandosi con il sistema di posta e PEC dell'Ente.
MyID	Sistema di autenticazione per l'accesso ai servizi applicativi e alle piattaforme dell'Ente.
Sistema delle Gestioni delle Deleghe (SDG)	Il modulo permette di gestire le deleghe per quanto riguarda l'accesso ai servizi e allo sportello dell'Ente da parte dei cittadini e delle imprese.
Applicazione base	

Contabilità	Programma di Contabilità dell'Ente attualmente in evoluzione per l'introduzione della interoperabilità con MySIR per la gestione dei ruoli.
Sistema Documentale	Il sistema documentale è predisposto per l'interoperabilità e raccoglie tutta la documentazione richiesta dall'Ente per le istanze di servizio. Lo stesso sistema raccoglie tutti gli atti formali inviati ai cittadini e imprese a seguito della richiesta di un servizio. Dialoga inoltre con lo sportello del Cittadino per gestire la visibilità, all'interno della zona personale dopo l'autenticazione, di tutta la documentazione inviata e ricevuta.
SID	Il Sistema Informatico delle determine dirigenziali fornisce l'iter per la firma e l'ufficializzazione degli atti da inviare ai cittadini e imprese in caso di rilascio di licenze e concessioni, inoltre dal SID inizia il procedimento degli accertamenti di entrata dei dovuti scaturiti dalla erogazione dei servizi dell'Ente.
Protocollo	Sistema di Protocollo necessario per la formalizzazione in entrata ed in uscita dei documenti ricevuti o inviati durante l'iter della istanza trattata dallo sportello.
Piattaforme	
MyPay	Piattaforma dei Pagamenti verso la Pubblica Amministrazione conforme alle linee guida previste da AGID per PagoPA.
Open Data	Sito istituzione della Città metropolitana di Roma Capitale per l'esposizione pubblica delle informazioni trattate in formato open.
Sistema Informativo Geografico	Piattaforma cartografica e portale di consultazione della Città metropolitana di Roma Capitale

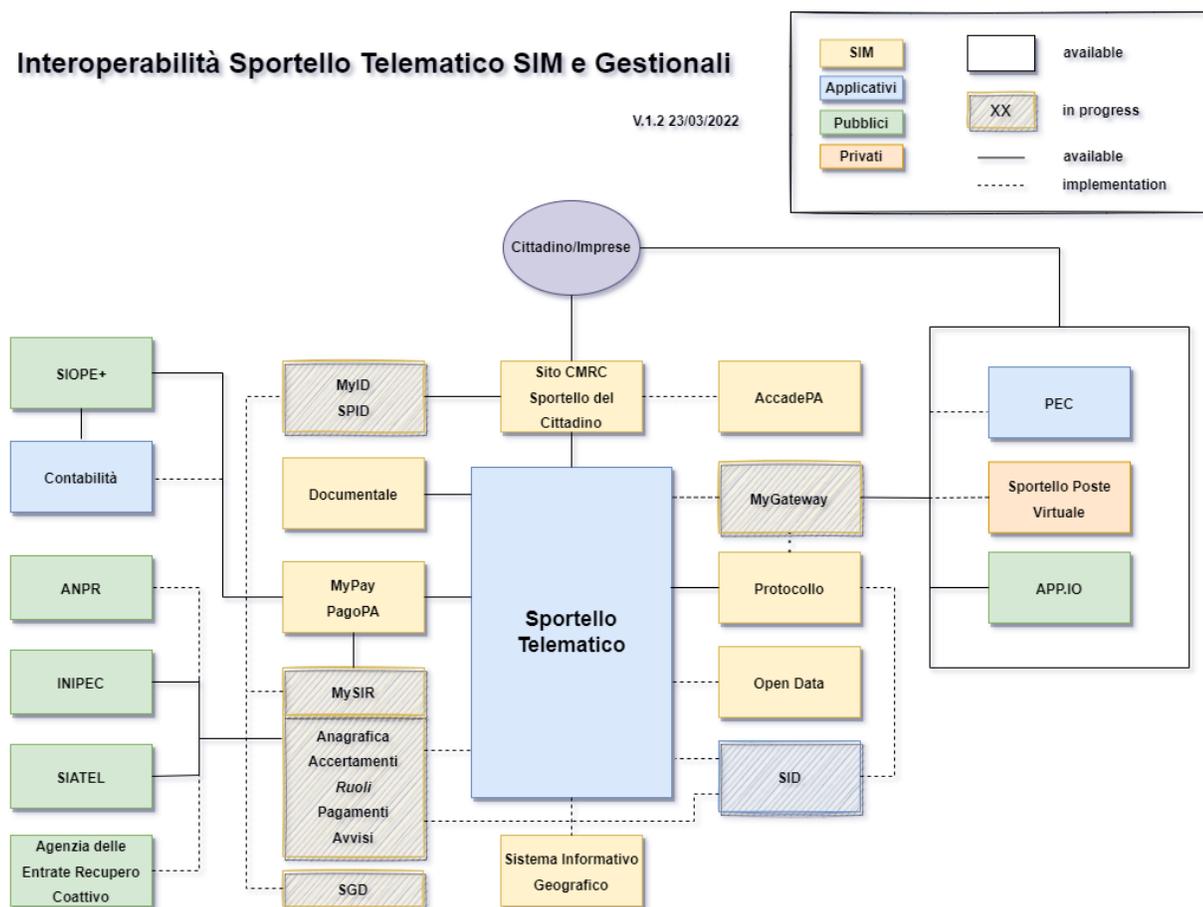
2.3.3. Servizio di sportelli Telematici per i Comune dell'area metropolitana e condivisione della SIM

La realizzazione dei servizi degli sportelli telematici dovrebbe essere estesa anche nei confronti dei procedimenti delle istanze previste dai Comuni condividendo implicitamente in questo modo anche i servizi offerti dalla Struttura Integrata Metropolitana (SIM). Grazie al servizio in cloud, i Comuni dell'area metropolitana potrebbero essere immediatamente operativi, evitando così costi ed investimenti locali. Si otterrebbe così una standardizzazione dei procedimenti comunali e la possibilità di fornire ai cittadini un unico ingresso ai servizi attraverso un unico portale federato del cittadino metropolitano.

Di seguito si riporta lo schema funzionale della SIM dove vengono indicate tramite linee i principali le cooperazioni applicative previste.

Interoperabilità Sportello Telematico SIM e Gestionali

V.1.2 23/03/2022



2.4. Lo sviluppo del Portale del Cittadino

Il modello di Portale del Cittadino che, grazie all'adozione di modelli standard per i siti e servizi della PA predisposte dal progetto Designers Italia, renderà più semplici, coerenti e fruibili i servizi agli utenti della Città metropolitana di Roma Capitale.

Il modello costituirà il punto unico di accesso ai servizi dell'Ente, di fatto un hub di tutti i servizi al pubblico dell'Ente, promuovendo la Total Experience dell'utente per l'erogazione dei servizi digitali attraverso la presentazione di interfacce coerenti e ricorrenti che permettano una più facile fruizione dei servizi digitali stessi.

Attraverso il Portale del Cittadino potrà essere erogato un numero indefinito di servizi che corrispondono ciascuno ad una delle seguenti macro-tipologie individuate:

1. **Permessi e autorizzazioni:** Istanze presentate dal cittadino che prevedono il rilascio di un contestuale permesso o autorizzazione, determinato dall'amministrazione;
2. **Domande con graduatoria:** Istanze presentate dal cittadino che prevedono una erogazione contestuale di una prestazione, vincolata a una graduatoria di precedenza redatta dall'amministrazione;
3. **Servizi a pagamento:** Istanze presentate dal cittadino che prevedono una erogazione contestuale di una prestazione, vincolata esclusivamente al pagamento della stessa;
4. **Vantaggi economici:** Istanze presentate dal cittadino che prevedono l'erogazione contestuale di un vantaggio economico, vincolato unicamente alla presenza di determinate caratteristiche;
5. **Pagamenti dovuti:** Istanze presentate dal cittadino che prevedono il pagamento di un onere, senza l'erogazione un servizio contestuale.

Il cittadino, riconosciuto attraverso SPID/CIE potrà presentare un'istanza che, in base alla configurazione del singolo servizio, determinerà l'erogazione completa e contestuale dello stesso oppure l'avvio di un iter all'interno degli uffici dell'Ente. Pertanto, il Portale del Cittadino avrà due interfacce: una pubblica dedicata ai cittadini e una privata riservata all'accesso dei dipendenti di Città metropolitana di Roma Capitale.

L'interfaccia del cittadino raccoglierà in modo sintetico tutti i servizi disponibili per l'utente riconosciuto, darà evidenza dello stato di avanzamento delle pratiche presentate, conterrà lo storico dei documenti scambiati con l'Ente e dei pagamenti effettuati. L'interfaccia sarà disponibile almeno in lingua inglese oltre che in italiano e i servizi individuati di livello europeo verranno resi disponibili anche sul portale Your Europe (<https://european-union.europa.eu>).

Il Portale del Cittadino costituirà lo strumento di lavoro per i dipendenti dell'Ente, sovrintendendo ai flussi di lavoro definiti dai singoli uffici per ciascun servizio, disciplinando l'accesso alle informazioni e fornendo ai dipendenti un'esperienza senza soluzione di continuità grazie all'integrazione e all'interoperabilità API con i sistemi software in dotazione all'Ente e con le basi dati nazionali.

L'ottimizzazione dei flussi di lavoro determinerà, nel tempo, un miglioramento dei servizi digitali offerti dall'Ente che aumenteranno la soddisfazione e la propensione nell'utilizzo degli stessi da parte degli stakeholders.

L'attivazione dei servizi sul Portale del Cittadino avverrà gradualmente in base ai livelli di interoperabilità disponibili per ciascun sportello telematico dell'Ente. Particolare attenzione dovrà pertanto essere posta sulla progettazione e sull'evoluzione degli sportelli in un'ottica di erogazione di servizi digitali al cittadino.

Il Portale del Cittadino costituirà uno strumento indispensabile per la governance del territorio e l'indirizzamento della strategia IT metropolitana; permetterà di raccogliere, strutturare e condividere i dati secondo criteri e metodologie atte a fornire indispensabili indicazioni sia sulla trasformazione digitale dell'Ente sia sulle dinamiche rappresentative delle esigenze del territorio metropolitano.

A tale scopo si pone l'esigenza di valutare la creazione di un modello di Portale del Cittadino della Città metropolitana di Roma Capitale di tipo confederato che permetta al cittadino di fruire, a partire da un unico punto, di tutti i servizi offerti dagli Enti dell'area metropolitana di Roma.

Il modello confederato costituirebbe il punto di accesso a tutti i servizi della CmRC e a tutti i servizi dei Comuni aderenti. Un punto di ingresso unico per i cittadini metropolitani che, a fronte di una sola autenticazione SPID/CIE, potrebbero usufruire di una moltitudine di servizi digitali distinti per ente ma coerenti per interfaccia, linguaggio utilizzato e modulistica presentata.

Un simile approccio contribuirebbe in maniera concreta a colmare il divario digitale nel quale versano le comunità locali più esigue impossibilitate ad effettuare investimenti tecnologici rilevanti e, allo stesso tempo, consentirebbe un immediato meccanismo di condivisione delle informazioni tra la Città metropolitana di Roma Capitale e gli Enti del proprio territorio, interagendo come hub di servizio per Comuni, cittadini ed imprese.

Legenda degli acronimi e delle sigle

1. **SIM** – *La Struttura Integrata Metropolitana è composta da una serie di applicazioni e di servizi di infrastruttura che facilitano l'integrazione e l'inserimento dei gestionali dell'Ente all'interno di un sistema omogeneo ed interoperabile.*
2. **MyID** – *Sistema di autenticazione per l'accesso ai servizi applicativi e alle piattaforme dell'Ente.*
3. **SPID** – *Sistema Pubblico di Identità Digitale. La PA ha l'obbligo di utilizzarlo per l'accesso del cittadino/impresa ai propri servizi. In alternativa oltre a SPID deve essere disponibile l'accesso ai servizi anche tramite la CIE (Carta d'Identità Elettronica) e il sistema europeo di identificazione eIDAS (electronic IDentification Authentication and Signature).*
4. **SID** – *Sistema Informativo Determinazione Dirigenziali*
5. **MyPay** – *Piattaforma dei Pagamenti verso la Pubblica Amministrazione conforme alle linee guida previste da AGID per PagoPA*
6. **MyGateway** – *Fornisce servizi di infrastruttura per l'invio di notifiche, avvisi di pagamento, raccomandate RR e documenti attraverso App.IO, l'ufficio virtuale di Poste Italiane e PEC.*

7. **MYSIR** – *Sistema Integrato di Rendicontazione interconnesso al sistema PagoPA per la gestione delle entrate e delle voci d'incasso. Mette a disposizione servizi di cooperazione per la gestione della anagrafica unica dei contribuenti, la gestione degli accertamenti, gestione dei ruoli e la creazione massiva degli avvisi di pagamento.*
8. **AccadePA** – *Piattaforma collaborativa di e-learning per l'acquisizione delle competenze digitali dedicata alla Pubblica Amministrazione e utilizzata anche per fornire formazione e supporto ai cittadini e alle imprese per il corretto utilizzo dei servizi digitali forniti dall'Ente.*
9. **SIOPE+** – *Infrastruttura della Banca d'Italia che intermedia il colloquio tra pubbliche amministrazioni e banche tesoriere con l'obiettivo di migliorare la qualità dei dati per il monitoraggio della spesa pubblica e per rilevare i tempi di **pagamento delle Pubbliche Amministrazioni nei confronti delle imprese fornitrici.***
10. **ANPR** – *L'Anagrafe Nazionale della Popolazione Residente è la banca dati nazionale che semplifica i servizi demografici per favorire la digitalizzazione e il miglioramento dei servizi a Cittadini, Imprese ed Enti.*
11. **SGD** – *Modulo che permette di gestire le deleghe per quanto riguarda l'accesso ai servizi e allo sportello dell'Ente da parte dei cittadini e delle imprese.*
12. **INIPEC** – *è l'Indice Nazionale degli Indirizzi di PEC istituito dal Ministero dello Sviluppo Economico, raccoglie tutti gli indirizzi di PEC delle Imprese e dei Professionisti presenti sul territorio italiano.*
13. **SIATEL** – *è un servizio dell'Agenzia delle Entrate che consente ai Comuni, alle Regioni, alle Agenzie Socio Sanitarie Territoriali (ASST) e ad altri Enti di accedere via web gratuitamente, previa stipula di apposita Convenzione, ai dati anagrafici, alle dichiarazioni dei redditi e agli atti del registro dei contribuenti.*

3. Linee di Finanziamento ulteriori rispetto a quelle previste dal Piano Esecutivo di Gestione dell'Ente.

Per il finanziamento delle spese di investimento, le scelte elettive ricadono su **PNRR** e fondi della **politica di coesione**, resi disponibili principalmente tramite il POR FESR della Regione Lazio. Ulteriori fondi della politica di coesione potranno poi provenire dal PON Metro del periodo 2021-2027, la cui proposta prevede la diffusione dei servizi di Agenda Digitale e una maggiore integrazione tra comune capoluogo ed il nostro Ente.

Nel caso in cui gli interventi presentassero un valore aggiunto europeo sarebbe anche possibile il ricorso ai fondi del programma **Digital Europe**, gestiti direttamente dalla Commissione europea. Sarà in ogni caso necessario monitorare periodicamente le fonti di finanziamento a disposizione per aggiornare i seguenti dati ed individuare nuove proposte percorribili per finanziare le strategie dell'Ente metropolitano.

PNRR

Il sito [PA digitale 2026](#) costituisce il punto di accesso unico alle risorse per la transizione digitale della PA e consentirà di richiedere i fondi del PNRR dedicati al digitale, rendicontare i progetti e ricevere assistenza. Le città metropolitane potranno concorrere sui fondi dei seguenti investimenti:

1.3.1/2 – Piattaforma Digitale Nazionale Dati e Sportello Digitale Unico (646mIn €)

I due investimenti, tra loro correlati, si propongono di garantire l'interoperabilità dei principali dati e servizi tra le pubbliche amministrazioni centrali e locali e l'armonizzazione a livello comunitario delle procedure prioritarie (Allegato 2 del regolamento UE 2018/1724). Grazie alla realizzazione di una **Piattaforma Digitale Nazionale Dati** che garantirà l'interoperabilità dei *dataset* e un catalogo centralizzato di API le informazioni saranno immediatamente a disposizione delle amministrazioni centrali e locali in modo semplice ed efficace. Sarà inoltre realizzato uno **Sportello Digitale Unico** che renderà disponibili online le 21 procedure prioritarie permettendo così di attuare il principio del *once-only*.

Sarà possibile accedere alla misura mediante la presentazione di un progetto.

1.4.2 – Migliorare l'accessibilità

Migliorare l'accessibilità dei servizi pubblici digitali attraverso la diffusione di strumenti e strategie condivise quali test di usabilità, attività di comunicazione e disseminazione, sviluppo di kit dedicati, ecc.

Sara accedere alla misura mediante la presentazione di un progetto.

1.4.4 – Adozione identità digitale

Questa misura permette alle amministrazioni pubbliche di favorire l'adozione di soluzioni quali SPID, CIE e ANPR.

La misura prevede che siano messe a disposizione dei richiedenti soluzioni standard.

1.5 "Cybersecurity"

Questa misura permette la realizzazione di interventi di potenziamento della resilienza cyber per la Pubblica Amministrazione, realizzando un percorso virtuoso di gestione del rischio cyber. In particolare, si prevede:

- la realizzazione di un censimento dei livelli di maturità della postura di sicurezza dei servizi e delle infrastrutture digitali delle PA;
- la realizzazione di un piano programmatico di potenziamento, sia a breve che a medio-lungo termine, delle capacità cyber, volto a supportare il percorso di trasformazione digitale sicura della PA; la realizzazione di interventi di potenziamento cyber a breve-medio termine dei servizi e delle infrastrutture in essere della PA.

POR FESR Regione Lazio

La proposta di POR FESR approvata con delibera di Giunta della Regione Lazio n. 996 del 30 dicembre 2021 prevede interventi per la P.A. finalizzati a incrementare il numero, la qualità, la sicurezza e l'accessibilità dei servizi digitali nel rispetto dell'interoperabilità dei sistemi per favorire lo scambio dei dati tra pubblico e privato. Sono previsti sia interventi diretti per la digitalizzazione delle procedure amministrative regionali e dei servizi offerti dalla Regione alla pubblica utenza, sia azioni volte a favorire la digitalizzazione dei piccoli comuni del Lazio. All'azione sono stati riservati 46 milioni di euro: gli investimenti si riferiscono alla programmazione POR FESR 2021-2027 e saranno ammissibili fino al 31 dicembre 2029.

Digital Europe

Il regolamento (UE) 2021/694 istituisce il programma Digital Europe e prevede che le azioni dell'Obiettivo specifico 4 – Competenze digitali avanzate (art. 7) – e

dell'Obiettivo specifico 5 – Implementazione e impiego ottimale delle capacità digitali e interoperabilità (art. 8) – vengano attuate principalmente attraverso la gestione diretta.