Città metropolitana di Milano

DECRETO DEL SINDACO METROPOLITANO

In Pubblicazione:	dal 24/09/2024 al 08/10/2024
Repertorio Generale:	230/2024 del 24/09/2024
Protocollo:	157530/2024
Titolario/Anno/Fascicolo:	3.2/2024/3
Proponente:	CONSIGLIERE DELEGATO FRANCESCO VASSALLO
Materia:	CAMPUS DIGITALE
Oggetto:	APPROVAZIONE DEL PIANO TRIENNALE PER LA TRANSIZIONE DIGITALE 2024-2026 DELLA CITTÀ METROPOLITANA DI MILANO, DEL PIANO DELL'INNOVAZIONE E DEL DISCIPLINARE PER L'UTILIZZO DEI SERVIZI INFORMATICI E DI COMUNICAZIONE TELEMATICA

DOCUMENTI CON IMPRONTE:

Documento 1 *1989_13594^DecretoFirmato.pdf*

89b83535bd65a1b6d1a78ff95079f167af1723fd096fe6d26686a4ab95530978

Città metropolitana di Milano

DECRETO DEL SINDACO METROPOLITANO

Fascicolo 3.2/2024/3

Oggetto: Approvazione del Piano Triennale per la Transizione digitale 2024-2026 della città metropolitana di Milano, del Piano dell'Innovazione e del disciplinare per l'utilizzo dei servizi informatici e di comunicazione telematica

IL SINDACO METROPOLITANO

Assistito dal Segretario Generale

VISTA la proposta di decreto redatta all'interno;
VALUTATI i presupposti di fatto e le ragioni giuridiche a fondamento dell'adozione del presente atto in relazione alle risultanze dell'istruttoria;
VISTA la Legge n. 56/2014;
VISTE le disposizioni recate dal T.U. in materia di Comuni, approvate con D.Lvo 267/2000, per quanto compatibili con la Legge n. 56/2014;
VISTO lo Statuto della Città metropolitana ed in particolare l'art. 19 comma 2;
ACQUISITI i pareri di regolarità tecnica e di regolarità contabile espressi dai Dirigenti competenti, ai sensi dell'art. 49 del T.U. approvato con D.Lvo 267/2000;

DECRETA

1) di approvare la proposta di provvedimento redatta all'interno, dichiarandola parte integrante del presente atto;
2) di incaricare i competenti Uffici di provvedere agli atti consequenziali;
3) di incaricare il Segretario Generale dell'esecuzione del presente decreto.

Letto, approvato e sottoscritto

IL SINDACO	IL SEGRETARIO GENERALE

Documento informatico firmato digitalmente ai sensi del T.U. 445/2000 e del D.Lgs 82/2005 e rispettive norme collegate.

Città
metropolitana
di Milano

PROPOSTA
di decreto del Sindaco Metropolitano

Fascicolo 3.2\2024\3

DIREZIONE PROPONENTE : DIPARTIMENTO TRANSIZIONE DIGITALE
Oggetto: Approvazione del Piano Triennale per la Transizione digitale 2024 – 2026 della Città Metropolitana di Milano, del Piano dell'innovazione e del Disciplinare per l'utilizzo dei servizi informatici e di comunicazione telematica

IL SINDACO METROPOLITANO

Visto il Decreto n. 148/2023 atti. n. 91650/1.9\2023\1 con il quale è stata conferita al Consigliere Francesco Vassallo la delega alla materia " Campus digitale";

PREMESSO che con l'art. 14 bis del D. Lgs. 82/2005 "Codice dell'amministrazione digitale", vengono definite le attribuzione dell'Agenzia per l'Italia Digitale tra cui, oltre alla promozione dell'innovazione digitale nel Paese e l'utilizzo delle tecnologie digitali nell'organizzazione della pubblica amministrazione e nel rapporto tra questa, i cittadini e le imprese e l'emanazione di Linee guida contenenti regole, standard e guide tecniche, viene prevista la redazione con cadenza annuale del Piano triennale per l'informatica nella pubblica amministrazione, contenente la fissazione degli obiettivi e l'individuazione dei principali interventi di sviluppo e gestione dei sistemi informativi delle amministrazioni pubbliche;

PRESO ATTO che con Decreto del Presidente del Consiglio dei ministri del 12 gennaio 2024 si è proceduto all'approvazione del Piano triennale per l'informatica nella pubblica amministrazione 2024-2026;

RILEVATO che il suddetto Piano 2024-2026 si inserisce nel più ampio contesto di riferimento definito dal programma strategico "Decennio Digitale 2030", istituito dalla Decisione (UE) 2022/2481 del Parlamento Europeo e del Consiglio del 14 dicembre 2022, i cui obiettivi sono articolati in quattro dimensioni: competenze digitali, servizi pubblici digitali, digitalizzazione delle imprese e infrastrutture digitali sicure e sostenibili;

RICHIAMATO l'art. 35 comma 1 ter del DL 76/2020, convertito con modifiche in legge n. 120/2020, che dispone che l'Agid definisce nel Piano triennale per l'informatica nella pubblica amministrazione la strategia di sviluppo delle infrastrutture digitali delle amministrazioni pubbliche e la strategia di adozione del modello cloud per la pubblica amministrazione, alle quali le amministrazioni si attengono;

VISTA la circolare n. 3 del primo ottobre 2018 del Ministro per la pubblica amministrazione, ad oggetto “Responsabile per la transizione digitale - art. 17 decreto legislativo 7 marzo 2005, n. 82 Codice dell’amministrazione digitale” in cui, tra le competenze dell’ RTD, viene indicata quella inerente “la predisposizione del Piano triennale per l’informatica della singola amministrazione, nelle forme e secondo le modalità definite dall’Agenzia per l’Italia digitale”;

VISTO il decreto sindacale RG 30/2023 del 31 gennaio 2023 con cui viene individuato quale RTD della Città metropolitana di Milano il dott. Luciano Schiavone, responsabile del dipartimento transizione digitale dell’Ente;

CONSIDERATO che:

Nell’ambito degli obiettivi di diffusione della cultura digitale, ogni Pubblica Amministrazione ha il mandato di adeguare le proprie strutture, procedure e servizi al massimo dell’utilizzo delle tecnologie informatiche al fine di semplificare le proprie modalità organizzative e la vita quotidiana dei cittadini ed imprese del proprio territorio;

In tal senso, la Città Metropolitana di Milano è impegnata in un processo di trasformazione digitale con l'obiettivo di migliorare i servizi offerti a cittadini, alle imprese e agli Enti locali del proprio territorio;

ATTESO che attraverso l'implementazione di soluzioni digitali innovative, l’Ente mira a rendere le interazioni più semplici e accessibili, rispondendo efficacemente ai bisogni della comunità di riferimento e migliorando la qualità dei servizi e che la trasformazione digitale della Città Metropolitana di Milano è caratterizzata da un approccio strutturato e completo, in cui il digitale diventa parte integrante dell'organizzazione e dei processi di lavoro e che tale impegno si manifesta nello sviluppo delle competenze digitali del personale e nella valutazione approfondita delle esigenze di transizione digitale.

PRECISATO che questo processo di profonda trasformazione non può essere realizzato senza una politica di sviluppo tecnico, organizzativo e culturale e relativo investimento economico, nonché senza un adeguato ed esplicito pensiero strategico, attraverso il quale la singola P.A. dovrà conseguire risultati secondo priorità predefinite.

RITENUTO pertanto necessario, seguendo le indicazioni esplicitate dal Piano Triennale di AGID, di elaborare un proprio specifico Piano per la Transizione digitale, con valenza triennale, coerente non solo con le linee guida AGID quanto con le politiche dell’ente sul territorio e nei limiti degli stanziamenti previsti dal proprio bilancio di previsione;

EVIDENZIATO che la Città Metropolitana di Milano si è impegnata a raggiungere diversi obiettivi strategici in tema di transizione al digitale, come dettagliati nel Piano strategico triennale del territorio metropolitano 2022-2024, tra cui il miglioramento dei servizi di e-government e la digitalizzazione delle pratiche per rendere più efficiente l'amministrazione pubblica, puntando inoltre alla valorizzazione del patrimonio archivistico e documentale e al sostegno dell’innovazione del sistema produttivo;

PRECISATO altresì che:

- si ritiene cruciale anche la promozione di percorsi di alfabetizzazione digitale per i cittadini, con l’obiettivo di superare il digital divide e di estendere i collegamenti 5G;
- viene posto un forte accento sul potenziamento delle competenze digitali del personale;
- attraverso il Piano si delineano le future strategie di completamento dei propri sistemi sulle tecnologie in cloud e si inseriscono le prime fasi di creazione di un’agenzia digitale, partecipata dalla

Città Metropolitana, le cui finalità saranno quelle di uniformare i processi di transizione digitale degli enti locali dell'area metropolitana, assicurando anche la possibilità di divenire il referente privilegiato degli enti in materia di acquisti di tecnologie e di produzione di servizi e applicazioni;

RITENUTO opportuno che, In affiancamento al Piano Triennale per la transizione digitale, sia opportuno che l'Ente si doti anche di un "Piano di Innovazione", con il quale definire le migliori strategie possibili, finalizzate allo sviluppo di soluzioni innovative, all'interno dell'Ente e nei rapporti con gli stakeholders esterni, nella costante ottica di miglioramento della qualità dei servizi offerti ai cittadini e per rendere l'azione amministrativa maggiormente efficace;

VALUTATO inoltre che nell'elaborare il Piano Triennale ed il Piano dell'innovazione, si ritiene opportuno riformulare la documentazione interna in termini di Policy in materia di ICT, per promuovere un uso responsabile, efficace e sicuro della tecnologia informatica all'interno dell'Ente, regolamentando l'utilizzo dei dispositivi e delle soluzioni informatiche utilizzate dal personale dipendente e da tutti i collaboratori e amministratori che a vario titolo interagiscono, adeguando, se non rielaborando ex novo, le precedenti regole ad un contesto digitale in continuo mutamento e profondamente modificato rispetto al decennio precedente;

RICHIAMATI gli atti di programmazione finanziaria dell'Ente (DUP e Bilancio di Previsione) e di gestione (PEG e PIAO);

VISTI i documenti in allegato, parte integrante e sostanziale del presente atto, denominati "Piano Triennale per la transizione digitale 2024-2026 della Città Metropolitana di Milano", "Piano di innovazione" e "Disciplinare per l'utilizzo dei servizi informatici e di comunicazione telematica";

VISTO che i suddetti documenti rappresentano strumenti di programmazione e, per la parte relativa al Disciplinare, di regolamentazione, considerata l'interconnessione tra gli stessi e l'attività di revisione complessiva del disciplinare, se ne propone l'approvazione con un unico atto;

VISTI altresì:
- la Legge 56/2014;
- le disposizioni recate dal T.U. in materia di Comuni, approvate con Decreto Lgs.18.08.2000 n. 267 "Testo Unico delle leggi sull'ordinamento degli Enti Locali", per quanto compatibili con la Legge n.56/2014;
- lo Statuto della Città metropolitana di Milano;

D E C R E T A

1) di approvare il Piano Triennale per la Transizione digitale 2024 – 2026 della Città Metropolitana di Milano, il Piano dell'innovazione e il Disciplinare per l'utilizzo dei servizi informatici e di comunicazione telematica, allegati parte integrante dell'atto;
2) di demandare al Direttore competente tutti i successivi adempimenti per l'esecuzione del presente Decreto, ivi compresa la pubblicazione del presente provvedimento in Amministrazione Trasparente ai sensi dell'art. 12 del D.Lgs. 33/2013;
3) di dare atto che il presente decreto non comporta riflessi diretti o indiretti sulla situazione economico-finanziaria o sul patrimonio dell'Ente e pertanto non e' dovuto il parere di regolarità contabile;
4) di dare atto che il presente procedimento, con riferimento all'Area funzionale di appartenenza, non è classificato a rischio

PARERE DI REGOLARITÀ TECNICA/AMMINISTRATIVA
(inserito nell'atto ai sensi dell'art. 49 del TUEL approvato con D.lgs. n. 267/00)

☒ Favorevole
☐ Contrario

SI DICHIARA CHE L'ATTO NON COMPORTA RIFLESSI DIRETTI O INDIRETTI SULLA SITUAZIONE ECONOMICO-FINANZIARIA O SUL PATRIMONIO DELL'ENTE E PERTANTO NON È DOVUTO IL PARERE DI REGOLARITÀ CONTABILE

☒
(inserito nell'atto ai sensi dell'art. 49 del TUEL approvato con D.Lgs. 267/00
e dell'art. 11 del Regolamento sul Sistema dei Controlli Interni)

IL DIRETTORE

Luciano Schiavone

Documento informatico firmato digitalmente ai sensi del T.U. 445/2000 e del D.Lgs 82/2005 e rispettive norme collegate.

Città metropolitana di Milano

Piano Triennale per la transizione digitale 2024-2026 della Città Metropolitana di Milano

Riferimento al Piano Triennale per l'informatica 2024-2026 pubblicato da AGID

Milano, settembre 2024

Sommario

PARTE I - IL PIANO TRIENNALE

Introduzione

La Città Metropolitana di Milano svolge un ruolo cruciale nel coordinamento e nella pianificazione strategica dell'area metropolitana, che comprende Milano e altri 133 Comuni. La sua istituzione risponde all'esigenza di creare un livello di governo intermedio tra i Comuni e la Regione, con funzioni specifiche che includono la pianificazione territoriale, la gestione dei servizi pubblici e la promozione dello sviluppo economico e sociale.

Il territorio della Città Metropolitana di Milano è uno dei più rilevanti a livello europeo, sia per dimensioni che per importanza economica. Questa area rappresenta un hub strategico per lo sviluppo nazionale ed internazionale, capace di attrarre risorse e generare innovazione. L'importanza della digitalizzazione è centrale nelle politiche della Città Metropolitana di Milano, che si impegna a promuovere e coordinare i sistemi di informatizzazione e digitalizzazione.

In questo contesto, la Città Metropolitana di Milano ha espresso la necessità di redigere un Piano Triennale per la Transizione Digitale al fine di definire la propria strategia IT complessiva e verificare la conformità alle normative nazionali ed europee di riferimento. Questo piano mira a delineare le linee strategiche di sviluppo per i prossimi tre anni, seguendo le linee guida del Piano Triennale per l'Informatica nella Pubblica Amministrazione redatto da AgID, e allineandole alla realtà specifica dell'Ente.

Il Piano Triennale della Città Metropolitana di Milano adotta le indicazioni strategiche e i principi guida del Piano Triennale per l'Informatica nella Pubblica Amministrazione (edizione 2024-2026), assicurando coerenza con le politiche nazionali e garantendo un approccio integrato e coordinato alla digitalizzazione.

La Città Metropolitana di Milano si impegna a raggiungere diversi obiettivi strategici in tema di transizione al digitale, come dettagliato nel Piano strategico triennale del territorio metropolitano 2022-2024. Questi includono il miglioramento dei servizi di e-government e la digitalizzazione delle pratiche per rendere più efficiente l'amministrazione pubblica. Si punta inoltre a valorizzare il patrimonio archivistico e documentale e a sostenere l'innovazione del sistema produttivo. È cruciale anche la promozione di percorsi di alfabetizzazione digitale per i cittadini, con l'obiettivo di superare il digital divide ed estendere i collegamenti 5G. Il piano pone, inoltre, un forte accento sul potenziamento delle competenze digitali del personale.

Ruolo del Responsabile per la Transizione al Digitale

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 questo proposito, la Città Metropolitana di Milano ha designato il Responsabile per la Transizione Digitale per creare una figura di coordinamento all'interno delle Aree dell'Amministrazione (decreto sindacale RG 30/2023 del 31 gennaio 2023). Tale nomina mira a 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 Milano ha istituito il Dipartimento Transizione Digitale, una struttura dedicata al tema della digitalizzazione che lavora a stretto contatto con il RTD per assicurare un approccio integrato e coordinato.

Contesto Strategico

La Città Metropolitana di Milano è impegnata in un processo di trasformazione digitale con l'obiettivo di migliorare i servizi offerti a cittadini, imprese e altri Enti. Attraverso l'implementazione di soluzioni digitali innovative, l'Ente mira a rendere le interazioni più semplici e accessibili, rispondendo efficacemente ai bisogni della comunità di riferimento e migliorando la qualità dei servizi.

La trasformazione digitale della Città Metropolitana di Milano è caratterizzata da un approccio strutturato e completo, in cui il digitale diventa parte integrante dell'organizzazione e dei processi di lavoro. Questo impegno si manifesta nello sviluppo delle competenze digitali del personale e nella valutazione approfondita delle esigenze di transizione digitale, analizzando tutti i servizi offerti.

Tra le recenti iniziative di rilievo, spicca la partecipazione alla misura 1.4.4 del PNRR, che ha permesso l'adozione di SPID e CIE come sistemi unici per l'autenticazione dei servizi online. Questa misura ha semplificato l'accesso ai servizi per i cittadini, garantendo maggiore sicurezza e praticità. Inoltre, l'amministrazione ha organizzato workshop seguiti da una survey rivolta a tutti i dipendenti per identificare i fabbisogni in termini di innovazione e le necessità di miglioramento dei processi interni. Questi workshop hanno permesso di raccogliere preziosi feedback e dati per guidare le future iniziative digitali. Un altro progetto significativo è la partecipazione al Syllabus, un'iniziativa del Dipartimento della Funzione Pubblica volta a fornire formazione sulle competenze digitali e trasversali ai dipendenti pubblici. Questa formazione è fondamentale per rafforzare la capacità dell'ente di affrontare le sfide della digitalizzazione, garantendo che il personale sia adeguatamente preparato a utilizzare e gestire le nuove tecnologie.

PARTE IIa – LE COMPONENTI STRATEGICHE

CAPITOLO 1 – Organizzazione e gestione del cambiamento

Questo capitolo affronta le sfide e le strategie relative alla trasformazione digitale della Pubblica Amministrazione. Il focus principale è la creazione di un ecosistema digitale amministrativo che possa erogare servizi di alta qualità in modo proattivo e trasparente, riducendo al contempo la complessità burocratica. Viene enfatizzata l'importanza della collaborazione istituzionale tra vari livelli di governo e la partecipazione attiva di cittadini e imprese per garantire una trasformazione digitale efficace e sostenibile.

La Città Metropolitana di Milano si propone di migliorare i processi di trasformazione digitale, promuovendo la diffusione delle competenze digitali e facilitando la collaborazione istituzionale. Per il futuro, la Città Metropolitana di Milano punta a rafforzare il coordinamento delle iniziative digitali attraverso il ruolo chiave del Responsabile per la Transizione al Digitale e a investire nella formazione continua del personale per acquisire competenze avanzate in ambiti tecnologici.

Contesto nazionale

La trasformazione digitale rappresenta una sfida cruciale per la Pubblica Amministrazione, richiedendo un cambiamento radicale nelle modalità di gestione e organizzazione delle attività amministrative. Il Piano Triennale per l'Informatica nella PA 2024-2026, elaborato da AgID, sottolinea 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.

Obiettivi e risultati attesi

Obiettivo 1.1 - Migliorare i processi di trasformazione digitale della PA

- Target 2025 – Eventuale proposta ad AgID in merito all'attivazione di una comunità digitale tematica su retedigitale.gov.it sulla base delle esigenze emerse durante la consultazione.

Obiettivo 1.2 - Diffusione competenze digitali nel Paese e nella PA

- Target 2024
  - Partecipazione dei dipendenti a corsi di formazione base su Office 365 (in particolare su Teams, OneDrive e Sharepoint), con riferimento alle tempistiche possibili sulla base di possibili affidamenti ad aziende esterne.
  - Candidatura dell'Amministrazione alla misura 1.4.2 del PNRR (Accessibilità).
- Target 2025:
  - Partecipazione di almeno 100 dipendenti dell'Amministrazione e dei comuni del territorio a corsi di formazione sull'accessibilità.
  - Partecipazione 100 dipendenti a corsi di formazione intermedi su Office 365 (in particolare su Teams, OneDrive e Sharepoint).

Cosa deve fare l'Amministrazione

Fornitura della firma digitale ai dipendenti

Attività Operative: la Città Metropolitana di Milano si è impegnata negli anni a dotare i propri dipendenti di firme digitali, iniziando con l'acquisto di un numero considerevole di firme remote. Questa soluzione innovativa permette ai dipendenti di firmare documenti elettronici in modo sicuro e legalmente vincolante. L'Amministrazione si impegna a fornire la firma digitale a tutti i dipendenti che ne facciano richiesta.

Deadline: continuativa.

Strutture interne interessate: Dipartimento Transizione Digitale.

Capitolo di spesa/fonti di finanziamento: fondi dell'Amministrazione.

Dematerializzazione archivi

Attività Operative: Città Metropolitana di Milano ha avviato un progetto di dematerializzazione degli archivi cartacei per modernizzare e rendere più efficiente l'amministrazione. Finora, l'Amministrazione ha digitalizzato con successo il materiale archiviato dal 1940 al 1990, trasformando migliaia di documenti cartacei in formato digitale.

Questo processo ha migliorato l'accessibilità e la gestione dei documenti, riducendo tempi e costi di ricerca e utilizzo. La Città Metropolitana di Milano si impegna a proseguire con la digitalizzazione dei documenti restanti, con l'obiettivo di raggiungere una completa dematerializzazione.

Deadline: dicembre 2026.

Strutture interne interessate: Dipartimento Transizione Digitale e Direzione Generale.

Capitolo di spesa/fonti di finanziamento: fondi dell'Amministrazione.

Attivazione di una comunità digitale telematica per retedigitale.gov.it

Attività Operative: la Città Metropolitana di Milano intende coinvolgere i Responsabili per la transizione al digitale del territorio per condurre una serie di consultazioni incentrate sull'Intelligenza Artificiale. L'obiettivo è raccogliere feedback e identificare temi ed esigenze specifiche legate all'IA che potranno essere oggetto di una proposta ad AgID finalizzata all'attivazione di una comunità digitale tematica su retedigitale.gov.it per affrontare e sviluppare tali tematiche.

Deadline: dicembre 2025.

Strutture interne interessate: Dipartimento Transizione Digitale.

Capitolo di spesa/fonti di finanziamento: fondi dell'Amministrazione.

Attivazione di iniziative di formazione base per il personale

Attività Operative: per potenziare la produttività, la Città Metropolitana di Milano organizzerà corsi formativi su Office 365, lo strumento adottato a supporto dei compiti d'ufficio. Questi corsi saranno progettati per migliorare l'utilizzo degli strumenti digitali, seguendo le seguenti attività:

- Analisi delle esigenze: identificazione delle competenze attuali e delle aree di miglioramento per personalizzare la formazione.
- Pianificazione dei corsi: sviluppo di un piano formativo flessibile, adattabile alle diverse competenze dei partecipanti.
- Organizzazione e promozione: programmazione di sessioni formative accessibili e promozione attiva attraverso canali interni.
- Esecuzione dei corsi: conduzione delle sessioni formative da parte di esperti (interni o esterni), focalizzate sull'apprendimento pratico e coinvolgente.
- Valutazione dei risultati: rilevamento dell'efficacia dei corsi tramite feedback dei partecipanti e monitoraggio dell'applicazione pratica delle competenze acquisite.

Deadline: dicembre 2025.

Strutture interne interessate: Dipartimento Transizione Digitale.

Capitolo di spesa/fonti di finanziamento: fondi dell'Amministrazione.

Attivazione di iniziative di formazione specialistiche per il personale

Attività Operative: la Città Metropolitana di Milano intende promuovere la partecipazione dei suoi dipendenti alle iniziative formative sull'accessibilità. Questa iniziativa è parte della partecipazione al bando PNRR 1.4.2, che prevede l'erogazione di corsi di formazione sull'accessibilità per i dipendenti della Città Metropolitana e dei comuni del territorio. Il progetto prevede le seguenti attività:

- Analisi dei fabbisogni: valutare le esigenze formative dei dipendenti di Città Metropolitana e dei comuni del territorio per identificare le competenze di base e le lacune nell'accessibilità.
- Pianificazione dei corsi: creare un piano formativo mirato per soddisfare i fabbisogni individuati.

- Implementazione dei corsi: organizzare e condurre i corsi seguendo il piano stabilito, assicurandosi che siano efficaci e adeguatamente strutturati.
- Valutazione dei risultati: valutare l'impatto dei corsi sulla partecipazione e sulle competenze acquisite, utilizzando i feedback per migliorare i programmi formativi futuri.

Deadline: dicembre 2025.

Strutture interne interessate: Dipartimento Transizione Digitale.

Capitolo di spesa/fonti di finanziamento: fonte di finanziamento nazionale (misura 1.4.2 del PNRR).

Centro Servizi Territoriale (CST)

Attività Operative: la Città Metropolitana di Milano intende avviare un progetto per la costituzione di un Centro Servizi Territoriale (CST), altrimenti definito come Agenzia Digitale della Città Metropolitana di Milano, con l'obiettivo di supportare i comuni del territorio nella gestione delle loro funzioni ICT attraverso la condivisione di risorse e competenze. Questo progetto è in linea con lo "Strumento 2 - Gestione associata dell'ICT" del Piano Triennale per l'Informatica nella Pubblica Amministrazione (edizione 2024-2026) e ne segue i principi guida. Le attività operative saranno articolate come segue:

- Ricognizione: analisi del fabbisogno di trasformazione digitale degli enti locali, inclusi digitalizzazione dei servizi, applicativi utilizzati, interoperabilità dei dati, competenze digitali del personale, piattaforme, infrastrutture, connettività e processi organizzativi.
- Progettazione: definizione del processo di associazione della funzione ICT e progettazione della gestione associata, con valutazione delle azioni di adeguamento tecnologico, stipula degli accordi con gli enti locali, e progettazione della migrazione della funzione ICT verso un ufficio centralizzato.
- Implementazione: attuazione del processo di associazione della funzione ICT secondo la pianificazione, adozione dei nuovi regolamenti, conferimento degli incarichi e individuazione dei referenti di ciascun ente.
- Gestione: esecuzione delle strategie e delle azioni di trasformazione digitale degli enti, monitoraggio e aggiornamento delle attività in base al loro svolgimento congiunto con gli enti associati.
- Espansione: estensione della collaborazione ad altre attività, funzioni potenzialmente associabili e nuovi enti, sviluppo trasversale della funzione digitale nei servizi comunali e ampliamento della collaborazione a nuovi enti tramite Convenzioni e Consorzi.

Deadline: dicembre 2026.

Strutture interne interessate: Dipartimento Transizione Digitale.

Capitolo di spesa/fonti di finanziamento: fondi dell'Amministrazione.

Esperienze acquisite

Nel corso del 2023, l'Amministrazione ha aderito al Syllabus, la piattaforma messa a disposizione dal Dipartimento della Funzione Pubblica con l'obiettivo di fare un assessment e

di erogare formazione sulle competenze digitali e trasversali ai dipendenti pubblici. Hanno aderito oltre il 50% dei dipendenti e, di questi, un ulteriore 50% ha completato l'intero percorso, composto da 11 moduli.

Inoltre, diversi dipendenti dell'Amministrazione hanno partecipato ad un percorso formativo intensivo di cinque giornate sul tema dell'Intelligenza Artificiale erogato dall'INPS, denominato "Valore PA". Questo percorso ha rappresentato un'opportunità per i dipendenti di acquisire competenze avanzate in un campo in continua evoluzione, preparandoli per sfide future e opportunità di sviluppo professionale.

Queste esperienze confermano l'impegno costante dell'Amministrazione nella promozione della formazione e dello sviluppo professionale dei propri dipendenti. Guardando al futuro, l'Amministrazione continuerà su questa traiettoria, implementando ulteriori iniziative volte a potenziare le competenze del personale e garantire un servizio pubblico all'avanguardia.

CAPITOLO 2 – Procurement

Questo capitolo esplora le strategie e le azioni necessarie per modernizzare il processo di procurement nella Pubblica Amministrazione, con l'obiettivo di migliorare l'efficienza operativa, la trasparenza e la conformità alle normative vigenti. Si evidenzia l'importanza dell'adozione di soluzioni digitali per gestire tutte le fasi del ciclo di procurement, dalla pianificazione delle gare alla gestione dei contratti, e la necessità di garantire l'interoperabilità delle piattaforme digitali. Inoltre, viene sottolineata l'importanza della formazione continua del personale per utilizzare efficacemente questi strumenti e mantenere aggiornate le competenze.

La Città Metropolitana di Milano ha già adottato piattaforme digitali come MEPA, Sintel e Consip per il procurement, e si impegna a tenere costantemente aggiornati i propri dipendenti sull'utilizzo delle stesse.

Contesto nazionale

Il procurement rappresenta una componente essenziale per il funzionamento efficiente della Pubblica Amministrazione. La modernizzazione di questo processo, attraverso l'adozione di strumenti e piattaforme digitali, è fondamentale per garantire trasparenza, efficienza e conformità alle normative vigenti.

L'adozione di soluzioni digitali consente di gestire in modo ottimale tutte le fasi del ciclo di procurement, dalla pianificazione delle gare alla gestione dei contratti. Questo approccio non solo migliora l'efficienza operativa riducendo i tempi di esecuzione, ma assicura anche la massima trasparenza nelle procedure di gara. Le piattaforme di e-procurement facilitano la partecipazione delle imprese, promuovendo la competitività e l'equità dei processi di selezione.

Un aspetto cruciale è l'interoperabilità delle piattaforme digitali, che deve essere garantita per permettere una comunicazione efficace tra le Amministrazioni e i fornitori. L'interoperabilità facilita anche l'adozione di standard comuni, che migliorano la gestione dei contratti e permettono una valutazione più precisa delle performance dei fornitori.

La formazione continua del personale è un altro elemento chiave per il successo della digitalizzazione del procurement. I dipendenti pubblici devono essere costantemente aggiornati sulle nuove tecnologie e procedure, per poter utilizzare efficacemente gli strumenti disponibili e gestire in modo ottimale i processi di approvvigionamento.

Obiettivi e risultati attesi

Obiettivo 2.3 - Favorire e monitorare l'utilizzo dei servizi previsti dalle Gare strategiche

- Target 2025 – Redazione, all'interno del piano acquisti, di una sezione dedicata alla programmazione dei fabbisogni di adesione alle iniziative strategiche disponibili.
- Target 2026 – Redazione, all'interno del piano acquisti, di una sezione dedicata alla programmazione dei fabbisogni di adesione alle iniziative strategiche disponibili.

Cosa deve fare l'Amministrazione

Programmazione dei fabbisogni di adesione alle iniziative strategiche

Attività Operative: l'Amministrazione inserirà, nel proprio piano acquisti, la programmazione dei fabbisogni di adesione alle iniziative strategiche per perseguire gli obiettivi del Piano Triennale, come suggerito dalle linee guida di AgID.

Deadline: continuativo (si ripete ogni anno).

Strutture interne interessate: Dipartimento Transizione Digitale.

Capitolo di spesa/fonti di finanziamento: fondi dell'Amministrazione.

Esperienze acquisite

La Città Metropolitana di Milano ha adottato estesamente le piattaforme digitali per il procurement, utilizzando da tempo strumenti come il MEPA, Sintel e Consip. Oltre all'adozione di queste piattaforme, la Città Metropolitana di Milano si impegna a tenere costantemente aggiornati i propri dipendenti sull'utilizzo delle stesse e sulle novità in termini di procurement digitale.

PARTE IIb – LE COMPONENTI TECNOLOGICHE

CAPITOLO 3 – Servizi

Il terzo capitolo si concentra sull'ottimizzazione dei servizi pubblici offerti ai cittadini e alle imprese attraverso la digitalizzazione. Viene trattata l'importanza di garantire l'interoperabilità tra le Amministrazioni, migliorare la qualità e l'accessibilità dei servizi e adottare standard di design inclusivi. Inoltre, si sottolinea la necessità di una gestione efficiente dei documenti informatici e della formazione continua del personale per assicurare una transizione digitale efficace e sostenibile.

In questo contesto, la Città Metropolitana di Milano mira a migliorare la qualità e l'accessibilità dei servizi digitali, garantendo l'interoperabilità tra le amministrazioni e adottando standard di design inclusivi. Per il futuro, la Città Metropolitana intende sviluppare e registrare nuove API e mantenere una forte attenzione al tema dell'accessibilità dei propri portali istituzionali.

Contesto nazionale

La Città Metropolitana di Milano si trova al centro di un processo di trasformazione digitale, con l'obiettivo primario di ottimizzare i servizi pubblici offerti ai cittadini e alle imprese. Questa trasformazione si basa sulle linee guida fornite da AgID che sottolineano l'importanza dell'interoperabilità, dell'accessibilità e del design dei servizi, nonché della formazione, gestione e conservazione dei documenti informatici.

L'interoperabilità è fondamentale per facilitare l'interazione digitale tra le Pubbliche Amministrazioni, i cittadini e le imprese. Su queste premesse è nata la Piattaforma Digitale Nazionale Dati (PDND) per garantire la completa interoperabilità dei dataset e dei servizi tra le Amministrazioni centrali e locali. Questa piattaforma semplifica gli accordi di interoperabilità e consente agli Enti di pubblicare e-service conformi alle Linee Guida attraverso l'implementazione di API, garantendo un approccio armonizzato alla digitalizzazione dei servizi.

La progettazione dei servizi si concentra sull'accessibilità e sul design, riconoscendo che il miglioramento della qualità e dell'inclusività dei servizi pubblici digitali è essenziale per aumentarne l'utilizzo da parte degli utenti. La Città Metropolitana di Milano adotta un approccio multidisciplinare alla progettazione dei servizi, garantendo la massima qualità e l'accessibilità per tutti gli utenti.

La formazione, gestione e conservazione dei documenti informatici rappresentano un'altra area cruciale nella digitalizzazione dei servizi pubblici. La Città Metropolitana di Milano si è allineata alle nuove Linee Guida dell'Agenzia per l'Italia Digitale, che mirano a semplificare e rendere più accessibile la gestione documentale. Si impegna ad adeguare i propri sistemi di gestione informatica dei documenti per garantire effetti giuridici conformi e assicurare servizi di alta qualità ai cittadini e alle imprese, rispettando gli obblighi del CAD e garantendo la sicurezza e la protezione dei dati personali.

Obiettivi e risultati attesi

Obiettivo 3.1 - Migliorare la capacità di erogare e-service

- Target 2024 – Analisi e programmazione dell'integrazione API da eseguire nel biennio 2025/2026
- Target 2025 – Registrazione di API come da analisi e programmazione svolte del 2024.
- Target 2026 – Registrazione di API come da analisi e programmazione svolte del 2024.

Obiettivo 3.2 - Migliorare la capacità di generare ed erogare servizi digitali

- Target 2024 – Completamento del test automatico di accessibilità sul portale istituzionale, pubblicazione degli obiettivi di accessibilità e compilazione della dichiarazione di accessibilità.
- Target 2025 – Completamento del test automatico di accessibilità sul portale istituzionale, pubblicazione degli obiettivi di accessibilità e compilazione della dichiarazione di accessibilità.
- Target 2026 – Completamento del test automatico di accessibilità sul portale istituzionale, pubblicazione degli obiettivi di accessibilità e compilazione della dichiarazione di accessibilità.

Cosa deve fare l'Amministrazione

Popolamento del Catalogo delle API della Piattaforma Digitale Nazionale Dati con le API conformi alle "Linee guida sull'interoperabilità tecnica delle Pubbliche Amministrazioni"

Attività Operative: la Città Metropolitana di Milano è già accreditata presso la PDND, tuttavia, è necessario avviare attività concrete per il popolamento del Catalogo delle API conformi alle Linee Guida sull'interoperabilità tecnica delle Pubbliche Amministrazioni. Pertanto, si renderà necessario sviluppare un piano d'azione specifico per questo scopo. Le attività previste includono:

- Analisi dello stato attuale: valutare la situazione corrente dell'ente in termini di disponibilità di servizi e dati da esporre.
- Pianificazione delle attivazioni: definire un piano dettagliato per l'attivazione dei servizi e dei dati nel Catalogo, includendo tempistiche, risorse necessarie e responsabilità.
- Implementazione delle attivazioni: procedere con l'attivazione delle API nel Catalogo, seguendo le procedure stabilite e garantendo la conformità alle Linee Guida sull'interoperabilità tecnica.
- Monitoraggio e valutazione: monitorare costantemente il processo di attivazione delle API, valutando il grado di adempimento rispetto agli obiettivi prefissati e apportando eventuali correzioni o miglioramenti necessari.

Deadline: dicembre 2024 (pianificazione); continuativo (pubblicazione API).

Strutture interne interessate: Dipartimento Transizione Digitale.

Capitolo di spesa/fonti di finanziamento: fondi dell'Amministrazione.

Utilizzo delle API presenti sul Catalogo della Piattaforma Digitale Nazionale Dati

Attività Operative: in parallelo al processo di esposizione delle API nel Catalogo della PDND, la Città Metropolitana di Milano si impegna ad utilizzare attivamente le API già presenti nel Catalogo per migliorare l'efficienza e l'interoperabilità dei propri servizi digitali.

Deadline: continuativo.

Strutture interne interessate: Dipartimento Transizione Digitale.

Capitolo di spesa/fonti di finanziamento: fondi dell'Amministrazione.

Test automatico di accessibilità sul sito istituzionale

Attività Operative: ogni anno, l'Amministrazione si impegna a effettuare il test di automatico di accessibilità del proprio portale istituzionale utilizzando la piattaforma Mauve++.

Deadline: annuale (entro il mese di dicembre di ogni anno).

Strutture interne interessate: Dipartimento Transizione Digitale.

Capitolo di spesa/fonti di finanziamento: fondi dell'Amministrazione.

Pubblicazione degli obiettivi di accessibilità

Attività Operative:

- Individuazione degli obiettivi di accessibilità per l'anno in corso.
- Aggiornamento degli obiettivi di accessibilità sul sito web dell'Amministrazione.

Deadline: annuale (entro il mese di marzo di ogni anno).

Strutture interne interessate: Servizio Comunicazione.

Capitolo di spesa/fonti di finanziamento: fondi dell'Amministrazione.

Pubblicazione della dichiarazione di accessibilità

Attività Operative:

- Contatto con il fornitore del sito istituzionale e verifica del modello utilizzato.
- Compilazione, tramite form AGID, della dichiarazione di accessibilità.

Deadline: annuale (entro il 23 settembre di ogni anno).

Strutture interne interessate: Dipartimento Transizione Digitale.

Capitolo di spesa/fonti di finanziamento: fondi dell'Amministrazione.

Interoperabilità tra i sistemi di protocollazione delle PA

L'allegato 6 delle "Linee Guida sulla formazione, gestione e conservazione dei documenti informatici", emanato da AgID, definisce le modalità tecniche di comunicazione tra i sistemi di protocollo delle Pubbliche Amministrazioni.

Si tratta della definizione delle interfacce applicative che consentono alle PA di far dialogare tra loro i propri sistemi di protocollo informatico in maniera diretta, scambiando documenti in modo veloce ed efficiente.

La Città metropolitana di Milano si adopererà affinché tutti i Comuni dell'Area metropolitana possano adottare le tecnologie necessarie per il funzionamento dell'interoperabilità tra i sistemi di gestione documentale, agevolando lo scambio di documenti tra le varie Aree Organizzative Omogenee (AOO).

Attività Operative:

- Analisi dello stato attuale: effettuare un censimento dei sistemi di protocollo informatico e gestione documentale in uso presso i Comuni della Città metropolitana per identificare quali sono le Amministrazioni già allineate alle linee guida AgID e quali invece devono ancora allinearsi;
- Supporto e interfacciamento con gli enti comunali e le software house interessate per agevolarne il necessario adeguamento affinché si raggiunga una convergenza generale.

Deadline: 2026.

Strutture interne interessate: Dipartimento Transizione Digitale.

Capitolo di spesa/fonti di finanziamento: fondi dell'Amministrazione.

Esperienze acquisite

La Città Metropolitana di Milano ha maturato significative esperienze nel campo della gestione documentale e della conservazione, avendo già implementato diverse azioni volte a garantire la trasparenza e l'efficienza nei processi amministrativi. In particolare, l'ente ha assicurato la pubblicazione del manuale di gestione documentale e del manuale di conservazione all'interno della sezione "Amministrazione trasparente" del proprio sito web. Inoltre, ha provveduto alla nomina del responsabile della gestione documentale, garantendo così la corretta gestione e conservazione dei documenti.

La Città Metropolitana di Milano ha adottato a marzo 2023 Web Analytics Italia, la piattaforma di analytics sviluppata da AgID per le Pubbliche Amministrazioni. Questo strumento fornisce statistiche in tempo reale sui visitatori del sito istituzionale, offrendo agli operatori dei report dettagliati. L'integrazione di questa soluzione ha permesso all'ente di migliorare la comprensione del comportamento degli utenti online e di ottimizzare le proprie risorse digitali per garantire un'esperienza più efficiente e soddisfacente ai cittadini e alle imprese.

Queste azioni hanno consentito all'ente di adempiere agli obblighi normativi e di assicurare la corretta gestione dei documenti, favorendo la trasparenza, l'accessibilità e la tracciabilità delle informazioni.

CAPITOLO 4 – Piattaforme

Nel capitolo quattro si analizza il ruolo delle piattaforme digitali nella trasformazione dei processi e dei servizi pubblici. L'obiettivo principale è migliorare l'efficienza e l'accessibilità dei servizi offerti a cittadini e imprese attraverso l'adozione di piattaforme digitali nazionali come SPID, CIE, SUAP e SUE. Il capitolo sottolinea l'importanza di una gestione integrata e coordinata delle piattaforme per garantire una pubblica amministrazione moderna e inclusiva, capace di rispondere efficacemente alle esigenze di una società sempre più digitale.

A tal proposito, la Città Metropolitana di Milano ha già adottato SPID e CIE come modalità di autenticazione per i servizi offerti, garantendo un accesso sicuro ed efficiente. Per il futuro, la Città Metropolitana di Milano intende continuare a migliorare i servizi erogati attraverso le piattaforme nazionali, promuovendo l'interoperabilità e l'integrazione delle nuove tecnologie. Inoltre, la Città Metropolitana sta lavorando per adottare la migliore soluzione per i procedimenti SUAP/SUE, assicurando una gestione efficiente e una transizione fluida verso le nuove piattaforme.

Contesto nazionale

Il contesto della digitalizzazione nella Pubblica Amministrazione italiana è caratterizzato dall'evoluzione di piattaforme digitali fondamentali per la trasformazione dei processi e dei servizi pubblici. Queste piattaforme offrono servizi essenziali a cittadini, imprese e PA, migliorando l'efficienza e l'accessibilità dei servizi pubblici. Le piattaforme nazionali implementate mirano a ottimizzare la gestione delle interazioni tra la Pubblica Amministrazione e i suoi utenti, favorendo un'esperienza più fluida e intuitiva.

L'adozione di queste soluzioni tecnologiche rappresenta un passo significativo verso una Pubblica Amministrazione più moderna e inclusiva, in grado di rispondere efficacemente alle esigenze di una società sempre più digitale. Tali piattaforme contribuiscono a ridurre la burocrazia, a migliorare la trasparenza e a favorire l'innovazione nei servizi pubblici, rendendo più semplice per i cittadini e le imprese accedere alle informazioni e ai servizi di cui hanno bisogno.

Tra le principali soluzioni adottate, l'identità digitale SPID (Sistema Pubblico di Identità Digitale) e la CIE (Carta d'Identità Elettronica) consentono ai cittadini di accedere ai servizi online della Pubblica Amministrazione con credenziali sicure e certificate. Inoltre, gli Sportelli Unici per le Attività Produttive (SUAP) e per l'Edilizia (SUE) facilitano gli adempimenti necessari per le attività produttive e gli interventi edilizi, promuovendo la digitalizzazione come leva strategica per la competitività e la crescita economica del Paese.

Obiettivi e risultati attesi

Obiettivo 4.1 - Migliorare i servizi erogati da piattaforme nazionali a cittadini/imprese o ad altre PA

- Target 2024 – Verifica del contesto esterno al fine di comprendere quali soluzioni adottare per i procedimenti SUAP/SUE
- Target 2025

- Adozione della piattaforma identificata per i procedimenti SUAP/SUE, a seguito della verifica al punto sopra.
- Attivazione di PagoPA su tutti i servizi di pagamento.
- Analisi e programmazione di eventuali altri servizi da attivare su AppIO

Cosa deve fare l'Amministrazione

Identificazione della migliore soluzione da adottare nei procedimenti SUAP/SUE

Attività Operative: Città Metropolitana di Milano si è avvalsa in passato della piattaforma procedimenti di Regione Lombardia per i procedimenti SUAP/SUE. Recentemente, ha effettuato un passaggio al catalogo della Camera di Commercio, sfruttando le funzionalità offerte da questa nuova piattaforma. Attualmente, sta organizzato incontri con le istituzioni regionali, tra cui la Regione, per comprendere meglio le dinamiche del territorio e le esigenze degli utenti finali. L'obiettivo di questo sforzo è lo studio delle modalità di interoperabilità con le nuove piattaforme, garantendo una transizione fluida e una gestione efficiente dei procedimenti SUAP/SUE.

Infine, dopo l'attenta analisi, Città Metropolitana di Milano procederà con l'adozione della piattaforma identificata, garantendo una transizione fluida e una gestione efficiente dei procedimenti SUAP/SUE.

Deadline: dicembre 2025.

Strutture interne interessate: Aree Ambiente, Pianificazione e Sviluppo Economico e Infrastrutture

Capitolo di spesa/fonti di finanziamento: fondi dell'Amministrazione.

Attivazione nuovi servizi PagoPA e AppIO

Attività Operative: l'Amministrazione ha aderito alle piattaforme abilitanti PagoPA e AppIO con l'obiettivo di arricchire la propria offerta di servizi disponibili su mobile e di servizi di pagamento attivi con il nodo PagoPA. In particolare, le attività che l'Amministrazione svolgerà sono:

- Mappatura dei servizi offerti dall'Amministrazione e non ancora attivati sulle piattaforme (PagoPA e AppIO).
- Elaborazione di una roadmap con l'obiettivo di attivare PagoPA per tutti i servizi di pagamento e aumentare i servizi disponibili su AppIO.
- Monitoraggio dei risultati ottenuti.

Deadline: dicembre 2025.

Strutture interne interessate: Dipartimento Transizione Digitale, Dipartimento Ragioneria Generale

Capitolo di spesa/fonti di finanziamento: fondi dell'Amministrazione.

Esperienze acquisite

La Città Metropolitana di Milano ha completato l'adozione di SPID e CIE come modalità di autenticazione per tutti i servizi offerti. Questa decisione è stata guidata dall'obiettivo di garantire un'esperienza utente più sicura, efficiente e uniforme per cittadini e imprese che accedono ai servizi online dell'ente metropolitano. In linea con l'evoluzione del panorama digitale, la Città Metropolitana di Milano ha posto particolare attenzione sull'approccio "SPID e CIE-only" per le nuove applicazioni. Questo significa che le nuove soluzioni digitali sviluppate dall'ente metropolitano sono progettate e implementate per consentire l'accesso esclusivamente tramite SPID e CIE, a meno che non vi siano vincoli normativi o tecnologici che richiedano una diversa modalità di autenticazione.

Infine, la Città Metropolitana di Milano è impegnata nell'adeguamento ai nuovi standard e alle evoluzioni dell'ecosistema digitale. Su questo fronte, è stato organizzato e concluso un corso di formazione per il personale dell'Ente sul nuovo protocollo OpenID Connect nell'ambito della misura 1.4.4 del PNRR.

CAPITOLO 5 – Dati e AI

In questo capitolo si esplora il valore strategico del patrimonio informativo pubblico e l'adozione delle tecnologie di Intelligenza Artificiale (AI) per migliorare l'efficienza e l'efficacia dei servizi pubblici. Viene trattata l'importanza di garantire la qualità e l'interoperabilità dei dati, promuovere la condivisione dei dati tra le Amministrazioni e sviluppare soluzioni di AI che possano modernizzare significativamente il settore pubblico.

Su questi temi, la Città Metropolitana di Milano si è impegnata, negli ultimi anni, a valorizzare il proprio patrimonio informativo attraverso la pubblicazione di dataset in formato Open Data, contribuendo alla piattaforma nazionale dati.gov.it. Per il futuro, la Città punta ad aumentare la consapevolezza e l'adozione delle tecnologie di AI nella Pubblica Amministrazione, organizzando sessioni formative e adottando linee guida specifiche.

Contesto nazionale

La valorizzazione del patrimonio informativo pubblico e l'adozione dell'Intelligenza Artificiale sono due pilastri fondamentali per la trasformazione digitale della Pubblica Amministrazione. Questi temi sono supportati da un quadro normativo europeo e nazionale che promuove la trasparenza, l'accessibilità e l'interoperabilità dei dati, e l'uso etico e responsabile delle tecnologie AI. In questo contesto, la gestione dei dati e l'implementazione delle soluzioni di AI sono viste come strumenti chiave per migliorare la qualità e l'efficienza dei servizi pubblici.

La valorizzazione del patrimonio informativo pubblico è un obiettivo strategico per la Pubblica Amministrazione, volto ad affrontare le nuove sfide dell'economia basata sui dati e garantire la creazione di servizi digitali a valore aggiunto per cittadini e imprese. La Strategia europea dei dati ha introdotto la creazione di spazi di dati comuni e interoperabili per superare le barriere legali e tecniche alla condivisione dei dati, sfruttando il potenziale dell'innovazione guidata dai dati. In Italia, il recepimento della Direttiva Europea 2019/1024 sull'apertura dei dati e il riutilizzo dell'informazione del settore pubblico, attuato con il Decreto Legislativo n. 200/2021, sostiene questo obiettivo attraverso l'implementazione delle Linee guida sui dati aperti.

La disponibilità di dati di alta qualità è essenziale per sviluppare e implementare soluzioni di intelligenza artificiale efficaci. L'IA può modernizzare significativamente il settore pubblico, migliorando l'efficienza e l'efficacia nella gestione e nell'erogazione dei servizi. Può automatizzare attività ripetitive, migliorare il processo decisionale basato sui dati e supportare la personalizzazione dei servizi. La Commissione Europea, con il "Piano Coordinato sull'Intelligenza Artificiale" e la proposta di regolamento sull'IA (AI Act), mira a fare dell'Europa un leader nell'uso dell'IA nel settore pubblico, promuovendo un uso sicuro e affidabile dell'IA. Questo quadro normativo è fondamentale per costruire un'infrastruttura di dati solida e per promuovere l'adozione di soluzioni di IA che migliorino la qualità dei servizi pubblici.

Obiettivi e risultati attesi

Obiettivo 5.4 - Aumento della consapevolezza della Pubblica Amministrazione nell'adozione delle tecnologie di intelligenza artificiale

- Target 2024 –
    - Organizzazione di almeno una consultazione, sul tema dell'IA, con i comuni del territorio.
    - Organizzazione di almeno 1 sessione formative sul tema dell'IA per i dipendenti dei Comuni dell'Area Metropolitana.
- Target 2025 – Adozione delle linee guida in tema di Intelligenza Artificiale nella PA.

Cosa deve fare l'Amministrazione

Adozione delle linee guida per l'adozione dell'IA nella Pubblica Amministrazione

Attività Operative: Città Metropolitana di Milano si impegna ad analizzare attentamente le Linee guida in tema di Intelligenza Artificiale nella PA non appena saranno pubblicate. Successivamente, adotterà tutte le indicazioni contenute nel documento, aggiornando le proprie procedure di procurement per assicurare che l'acquisizione di soluzioni IA avvenga in modo trasparente, sicuro e in conformità con i migliori standard di qualità e rispetto dei diritti fondamentali.

Parallelamente, Città Metropolitana di Milano sta partendo un progetto che prevede la convocazione dei Responsabili per la Transizione Digitale dei Comuni dell'Area Metropolitana sul tema dell'Intelligenza Artificiale. L'obiettivo è la creazione di una consulta degli RTD dell'area metropolitana, che possa discutere e delineare le modalità per seguire le linee definite da AgID (si veda il capitolo 1 di questo documento). La prima iniziativa di questo progetto è stata l'avvio di una serie di sessioni formative sul tema dell'IA, di cui si è già tenuto il primo incontro, per valutare le competenze già presenti e identificare i fabbisogni specifici.

Deadline: dicembre 2025.

Strutture interne interessate: Dipartimento Transizione Digitale e Direzione Generale.

Capitolo di spesa/fonti di finanziamento: fondi dell'Amministrazione.

Esperienze acquisite

La Città Metropolitana di Milano ha intrapreso un percorso significativo nella valorizzazione del proprio patrimonio informativo pubblico, allineandosi agli obiettivi strategici nazionali ed europei in materia di dati. Questo impegno si è concretizzato nella pubblicazione di oltre 200 dataset in formato Open Data, disponibili sul portale Open Data della Regione Lombardia, che a sua volta contribuisce alla piattaforma nazionale dati.gov.it. Tutti i dataset pubblicati rispettano le Linee guida Open Data sia in termini di qualità del dato che di metadatazione, assicurando che le informazioni siano facilmente reperibili e comprensibili, facilitando l'accesso e l'utilizzo da parte degli utenti finali.

CAPITOLO 6 – Infrastrutture

Nel sesto capitolo si affronta l'importanza delle infrastrutture digitali per supportare la trasformazione digitale della Pubblica Amministrazione. Viene analizzato il ruolo delle infrastrutture tecnologiche nella promozione dell'efficienza operativa, della sicurezza e della resilienza dei servizi pubblici. Un focus particolare è dedicato alla migrazione verso il cloud, riconosciuta come uno dei pilastri fondamentali per l'ammodernamento della Pubblica Amministrazione. Questo processo è stato sostenuto sia da importanti risorse stanziate attraverso il PNRR che dalla creazione del Polo Strategico Nazionale (PSN), con l'obiettivo di consolidare e ottimizzare le infrastrutture IT pubbliche.

La Città Metropolitana di Milano ha già migrato la maggior parte delle sue infrastrutture digitali verso il cloud e si impegna a completare questa migrazione. Adottando il piano "Cloud Italia", la Città punta a consolidare e ottimizzare le proprie risorse IT, riducendo i costi e migliorando l'efficienza operativa.

Contesto nazionale

La strategia "Cloud Italia", pubblicata a settembre 2021 dal Dipartimento per la Trasformazione Digitale e dall'Agenzia per la Cybersicurezza Nazionale, rappresenta un elemento cruciale per la riorganizzazione delle Pubbliche Amministrazioni italiane. Questo approccio mira a trasformare profondamente il modo in cui le amministrazioni operano e forniscono servizi, affrontando le sfide dell'autonomia tecnologica, del controllo sui dati e della resilienza dei servizi digitali.

In linea con gli obiettivi del PNRR, la strategia guida le PA italiane nella migrazione di dati e applicativi verso un ambiente cloud sicuro, adottando il principio "cloud first". Questo principio richiede alle PA di considerare prioritariamente il cloud per nuovi progetti e servizi, giustificando eventuali scelte diverse.

L'adozione del cloud permette di ridurre il debito tecnologico, mitigare il rischio di lock-in con i fornitori, abbattere i costi di manutenzione dei data center obsoleti e migliorare la sicurezza delle infrastrutture pubbliche. La modernizzazione dei sistemi informativi attraverso il cloud non solo aumenta l'efficienza, ma garantisce anche una maggiore resilienza contro le minacce informatiche.

Obiettivi e risultati attesi

L'Amministrazione ha già raggiunto gli obiettivi relativi a questo capitolo.

Cosa deve fare l'Amministrazione

L'Amministrazione ha già concluso le attività relative a questo capitolo.

Esperienze acquisite

La Città Metropolitana di Milano ha adottato la strategia "Cloud Italia" trasferendo quasi la totalità delle proprie infrastrutture al cloud gestito da CSI Piemonte. Questa migrazione ha

permesso di modernizzare e ottimizzare i sistemi informativi, migliorando l'efficienza operativa e riducendo i costi di manutenzione.

La transizione al cloud di CSI Piemonte ha coinvolto quasi tutte i server della Città Metropolitana, consentendo di sfruttare appieno i vantaggi offerti dal cloud, quali la scalabilità, la flessibilità e la sicurezza avanzata. Questo passaggio ha anche aumentato la resilienza delle infrastrutture, garantendo una maggiore continuità operativa e protezione contro le minacce informatiche. Le poche infrastrutture rimaste fuori dal cloud saranno dismesse a breve, completando così il processo di migrazione.

Sarà da valutare, nel proseguimento del triennio, l'eventuale adesione al Polo Strategico Nazionale, anche in forma graduale. Ciò, in funzione anche di valutare, da una parte, le diverse esperienze dei Comuni dell'area metropolitana e le loro forme di gestione della transizione digitale e, dall'altra, in riferimento a quelle che potrebbero essere le scelte della futura Agenzia Digitale, come accennato al capitolo 1.

Dal 2005, la Città Metropolitana di Milano ha realizzato un'estesa infrastruttura ultra-broadband di proprietà, attualmente lunga 6.000 km lineari e in espansione fino a 7.200 km entro il 2024. Questa rete in fibra ottica, sviluppata anche grazie a brevetti di proprietà e in collaborazione con enti come il CERN di Ginevra, ha permesso di abbandonare il vecchio sistema di posare i cavi nelle fognature. L'infrastruttura garantisce connettività veloce e affidabile favorendo una navigazione internet ultrarapida e un'efficiente trasmissione di grandi quantità di dati. Essendo di proprietà, assicura un controllo diretto sulla gestione e sullo sviluppo della rete, permettendo una maggiore autonomia e la capacità di rispondere in modo più efficace alle esigenze del territorio.

CAPITOLO 7 – Sicurezza informatica

Il Capitolo sette si concentra sulla sicurezza informatica come elemento cruciale per la trasformazione digitale della Pubblica Amministrazione. L'evoluzione delle moderne tecnologie e la digitalizzazione dei procedimenti amministrativi hanno esposto imprese e servizi pubblici a nuovi rischi cyber. Per garantire la sicurezza del Paese e il benessere dei cittadini, è fondamentale migliorare la resilienza delle reti e dei sistemi. La recente istituzione dell'Agenzia per la Cybersicurezza Nazionale (ACN) e l'adozione della Strategia nazionale di cybersicurezza sottolineano l'importanza di un indirizzo istituzionale unico e coerente. Significative risorse del Piano Nazionale di Ripresa e Resilienza sono state destinate a migliorare la postura di sicurezza del sistema Paese e della Pubblica Amministrazione.

La Città Metropolitana di Milano ha già compiuto passi importanti, come l'implementazione dell'autenticazione a più fattori per l'accesso alla suite Office 365. In futuro, la Città si impegna a estendere l'MFA anche per l'accesso alla VPN, adottare un modello di governance della cybersicurezza con la nomina di un responsabile dedicato, definire e approvare requisiti di sicurezza per i processi di approvvigionamento IT e promuovere attività di formazione continua sulla cybersicurezza per i dipendenti. Questi progetti sono fondamentali per rafforzare la sicurezza informatica e proteggere le risorse digitali dell'amministrazione.

Inoltre, l'Amministrazione si è candidata all'avviso n. 8/2024 di ACN dedicato al rafforzamento delle infrastrutture e dei servizi digitali e al miglioramento delle competenze specialistiche necessarie a garantire adeguati livelli di cyber resilienza.

Contesto nazionale

L'evoluzione delle moderne tecnologie e la conseguente possibilità di ottimizzare i procedimenti amministrativi per rendere l'azione amministrativa più efficace, efficiente ed economica, ha reso necessaria la "migrazione" verso il digitale. Tuttavia, questa trasformazione ha anche portato alla luce nuovi rischi, esponendo imprese e servizi pubblici a possibili attacchi cyber. In questo scenario, la sicurezza e la resilienza delle reti e dei sistemi su cui poggiano queste tecnologie sono fondamentali per garantire la sicurezza del Paese e, in prospettiva, lo sviluppo e il benessere dello Stato e dei cittadini.

La recente riforma dell'architettura nazionale cyber, attuata attraverso il decreto-legge 14 giugno 2021, n. 82, ha istituito l'Agenzia per la Cybersicurezza Nazionale (ACN). Uno degli obiettivi principali dell'ACN è sviluppare e rafforzare le capacità cyber nazionali, garantendo un indirizzo istituzionale unico e coerente, anche attraverso la redazione e l'implementazione della Strategia nazionale di cybersicurezza. Questa strategia considera cruciale la sicurezza dell'ecosistema digitale alla base dei servizi erogati dalla Pubblica Amministrazione, con specifica attenzione ai beni ICT, che supportano le funzioni e i servizi essenziali dello Stato e sono spesso bersaglio di attacchi cyber.

Per garantire lo sviluppo e il rafforzamento delle capacità cyber nazionali, significative risorse sono state destinate alla sicurezza cibernetica attraverso il Piano Nazionale di Ripresa e Resilienza (PNRR) e i Fondi per l'attuazione e la gestione della Strategia nazionale di cybersicurezza. Questi investimenti mirano a migliorare la postura di sicurezza del sistema Paese nel suo insieme e, in particolare, della Pubblica Amministrazione.

Obiettivi e risultati attesi

I seguenti obiettivi sono funzionali all'esito del Bando ACN al quale la Città metropolitana ha risposto.

Obiettivo 7.1 - Adottare una governance della cybersicurezza diffusa nella PA

- Target 2025 –
  - Estensione dell'autenticazione a più fattori (MFA) all'accesso alla rete privata virtuale (VPN).
  - Adozione di un modello di governance della cybersicurezza e nomina del responsabile della cybersicurezza.

Obiettivo 7.2 - Gestire i processi di approvvigionamento IT coerentemente con i requisiti di sicurezza definiti

- Target 2025 – Approvazione dei requisiti di sicurezza relativi ai processi di approvvigionamento IT.

Obiettivo 7.5 - Implementare attività strutturate di sensibilizzazione cyber del personale

- Target 2024 – Indagine di mercato per l'acquisto di corsi di formazione su temi legati alla cybersicurezza.
- Target 2025 – Partecipazioni di ulteriori 100 dipendenti a corsi di formazione su temi legati alla cybersicurezza.
- Target 2026 – Partecipazioni di ulteriori 100 dipendenti a corsi di formazione su temi legati alla cybersicurezza.

Cosa deve fare l'Amministrazione

Adozione di un modello di governance della cybersicurezza e nomina del responsabile della cybersicurezza

Attività Operative: l'Amministrazione ha intenzione di adottare un modello di governance della cybersicurezza che definisca chiaramente ruoli e responsabilità, nominando un Responsabile della Cybersicurezza e creando una struttura organizzativa di supporto. Il progetto seguirà le seguenti attività:

- Nominare il responsabile della cybersicurezza: identificare e selezionare un candidato qualificato con esperienza in sicurezza informatica, formalizzare la nomina e assicurare l'accesso alle risorse necessarie.
- Definire ruoli e responsabilità: creare una struttura organizzativa che stabilisca chiaramente i compiti e le responsabilità in materia di sicurezza informatica.
- Stabilire procedure operative standard: sviluppare e implementare delle procedure per la gestione quotidiana della sicurezza informatica.
- Pianificare riunioni periodiche: organizzare incontri regolari tra il responsabile e il team di sicurezza per valutare e migliorare continuamente le strategie di sicurezza.
- Implementare un sistema di monitoraggio continuo: utilizzare strumenti di monitoraggio per rilevare e rispondere tempestivamente alle minacce informatiche.

- Creare un piano di risposta agli incidenti: definire un piano dettagliato per rispondere rapidamente ed efficacemente agli incidenti di sicurezza informatica.
- Assicurare la conformità normativa: verificare che tutte le pratiche di sicurezza siano conformi alle normative nazionali e internazionali.

Deadline: dicembre 2025.

Strutture interne interessate: Dipartimento Transizione Digitale

Capitolo di spesa/fonti di finanziamento: fondi dell'Amministrazione e PNRR misura 1.5

Adozione dell'autenticazione a più fattori per l'accesso alla VPN

Attività Operative: l'Amministrazione intende estendere l'autenticazione a più fattori all'accesso alla rete privata virtuale utilizzata dai dipendenti per accedere in remoto alle risorse aziendali. Questo rafforzerà ulteriormente la sicurezza degli accessi e proteggerà i dati sensibili da potenziali minacce.

Deadline: dicembre 2025.

Strutture interne interessate: Dipartimento Transizione Digitale.

Capitolo di spesa/fonti di finanziamento: fondi dell'Amministrazione.

Definizione e approvazione dei requisiti di sicurezza relativi al processo di approvvigionamento IT

Attività Operative: l'Amministrazione provvede a definire e ad approvare i requisiti di sicurezza relativi ai processi di approvvigionamento IT, garantendo che tutti i beni e servizi acquisiti rispettino gli standard di sicurezza necessari per proteggere le risorse digitali.

Deadline: dicembre 2025.

Strutture interne interessate: Dipartimento Transizione Digitale.

Capitolo di spesa/fonti di finanziamento: fondi dell'Amministrazione.

Promozione dell'accesso e dell'utilizzo di attività strutturate di sensibilizzazione e formazione in ambito cybersicurezza

Attività Operative: la città Metropolitana di Milano intende promuovere una cultura della sicurezza informatica attraverso la formazione continua dei dipendenti su temi di cybersicurezza, aumentando la consapevolezza e le competenze per prevenire e gestire le minacce cyber. In questo senso, l'Amministrazione lavorerà su due fronti:

- Organizzare sessioni di formazione periodiche su tematiche di cybersicurezza.
- Fornire materiali didattici e risorse online per l'autoapprendimento dei dipendenti.

Deadline: dicembre 2025.

Strutture interne interessate: Dipartimento Transizione Digitale.

Capitolo di spesa/fonti di finanziamento: fondi dell'Amministrazione.

Esperienze acquisite

La Città Metropolitana di Milano ha implementato l'autenticazione a più fattori per l'accesso alla suite Office 365 per tutti i dipendenti. Questo avanzamento nella sicurezza informatica richiede agli utenti di fornire due o più verifiche indipendenti prima di concedere l'accesso ai servizi e ai dati sensibili. L'introduzione dell'MFA è stata accompagnata da una campagna di formazione per sensibilizzare i dipendenti sull'importanza della sicurezza informatica e sulle best practice per la gestione delle credenziali di accesso. Questa misura ha contribuito a ridurre il rischio di accessi non autorizzati, migliorando la protezione delle informazioni critiche e garantendo una maggiore sicurezza operativa per l'amministrazione.

APPENDICE 1 – Cronoprogramma

2024		
CAPITOLO DEL PT	**OBIETTIVO DEL PT**	**RISULTATO ATTESO**
1 – Organizzazione e gestione del cambiamento	1.2 - Diffusione competenze digitali nel Paese e nella PA	Partecipazione dei dipendenti a corsi di formazione base su Office 365 (in particolare su Teams, OneDrive e Sharepoint)
		Candidatura dell'Amministrazione alla misura 1.4.2 del PNRR (Accessibilità)
2 – Procurement	-	-
3 – Servizi	3.1 - Migliorare la capacità di erogare e-service	Analisi e programmazione delle API da registrare su PDND
	3.2 - Migliorare la capacità di generare ed erogare servizi digitali	Completamento del test automatico di accessibilità sul portale istituzionale
		Pubblicazione degli obiettivi di accessibilità
		Compilazione della dichiarazione di accessibilità
4 – Piattaforme	4.1 - Migliorare i servizi erogati da piattaforme nazionali a cittadini/imprese o ad altre PA	Identificazione della soluzione da adottare per i procedimenti SUAP/SUE
5 - Dati e AI	5.4 - Aumento della consapevolezza della Pubblica Amministrazione nell'adozione delle tecnologie di intelligenza artificiale	Organizzazione di almeno una consultazione, sul tema dell'IA, con i comuni del territorio
		Organizzazione di almeno 1 sessione formative sul tema dell'IA per i dipendenti dei Comuni dell'Area Metropolitana
6 – Infrastrutture	-	-
7 – Sicurezza informatica	7.5 - Implementare attività strutturate di sensibilizzazione cyber del personale	Indagine di mercato per l'acquisto di corsi di formazione su temi legati alla cybersicurezza
2025		
CAPITOLO DEL PT	**OBIETTIVO DEL PT**	**RISULTATO ATTESO**
1 – Organizzazione e gestione del cambiamento	1.1 - Migliorare i processi di trasformazione digitale della PA	Eventuale proposta ad AgID in merito all'attivazione di una comunità digitale tematica su retedigitale.gov.it sulla base delle esigenze emerse durante la consultazione
	1.2 - Diffusione competenze digitali nel Paese e nella PA	Partecipazione di almeno 100 dipendenti dell'Amministrazione e dei comuni del territorio a corsi di formazione sull'accessibilità

		Partecipazione 100 dipendenti a corsi di formazione intermedi su Office 365 (in particolare su Teams, OneDrive e Sharepoint).
2 – Procurement	2.3 - Favorire e monitorare l'utilizzo dei servizi previsti dalle Gare strategiche	Redazione, all'interno del piano acquisti, di una sezione dedicata alla programmazione dei fabbisogni di adesione alle iniziative strategiche disponibili
3 – Servizi	3.1 - Migliorare la capacità di erogare e-service	Registrazione di API come da analisi e programmazione svolte del 2024.
	3.2 - Migliorare la capacità di generare ed erogare servizi digitali	Completamento del test automatico di accessibilità sul portale istituzionale
		Pubblicazione degli obiettivi di accessibilità
		Compilazione della dichiarazione di accessibilità
4 – Piattaforme	4.1 - Migliorare i servizi erogati da piattaforme nazionali a cittadini/imprese o ad altre PA	Adozione della piattaforma identificata per i procedimenti SUAP/SUE
		Attivazione di PagoPA su tutti i servizi di pagamento
		Analisi e programmazione di eventuali altri servizi da attivare su AppIO
5 - Dati e AI	5.4 - Aumento della consapevolezza della Pubblica Amministrazione nell'adozione delle tecnologie di intelligenza artificiale	Adozione delle linee guida in tema di Intelligenza Artificiale nella PA
6 – Infrastrutture	-	-
7 – Sicurezza informatica	7.1 - Adottare una governance della cybersicurezza diffusa nella PA	Estensione dell'autenticazione a più fattori (MFA) all'accesso alla rete privata virtuale (VPN)
		Adozione di un modello di governance della cybersicurezza e nomina del responsabile della cybersicurezza
	7.2 - Gestire i processi di approvvigionamento IT coerentemente con i requisiti di sicurezza definiti	Approvazione dei requisiti di sicurezza relativi ai processi di approvvigionamento IT
	7.5 - Implementare attività strutturate di sensibilizzazione cyber del personale	Partecipazioni di almeno 100 dipendenti a corsi di formazione su temi legati alla cybersicurezza
2026		
CAPITOLO DEL PT	**OBIETTIVO DEL PT**	**RISULTATO ATTESO**
1 – Organizzazione e gestione del cambiamento	-	-
2 – Procurement	2.3 - Favorire e monitorare l'utilizzo dei servizi previsti dalle Gare strategiche	Redazione, all'interno del piano acquisti, di una sezione dedicata alla programmazione dei fabbisogni di adesione alle iniziative strategiche disponibili

3 – Servizi	3.1 - Migliorare la capacità di erogare e-service	Registrazione di API come da analisi e programmazione svolte del 2024.
	3.2 - Migliorare la capacità di generare ed erogare servizi digitali	Completamento del test automatico di accessibilità sul portale istituzionale
		Pubblicazione degli obiettivi di accessibilità
		Compilazione della dichiarazione di accessibilità
4 – Piattaforme	-	-
5 - Dati e AI	-	-
6 – Infrastrutture	-	-
7 – Sicurezza informatica	7.5 - Implementare attività strutturate di sensibilizzazione cyber del personale	Partecipazioni di ulteriori 100 dipendenti a corsi di formazione su temi legati alla cybersicurezza

APPENDICE 2 - Acronimi

Acronimo	Definizione
ACN	Agenzia per la Cybersicurezza Nazionale
AGID	Agenzia per l'Italia Digitale
AI/IA	Artificial Intelligence/ Intelligenza artificiale
ANPR	Anagrafe nazionale popolazione residente
API	Application Programming Interface
BDNCP	Banca Dati Nazionale dei Contratti Pubblici
CAD	Codice dell'amministrazione digitale
CIE	Carta d'Identità Elettronica
MFA	Multi-Factor Authentication/Autenticazione a più fattori
PDND	Piattaforma Digitale Nazionale Dati
PSN	Polo Strategico Nazionale
RTD	Responsabile per la Transizione al Digitale
SPID	Sistema Pubblico di Identità Digitale
SUAP	Sportello Unico per le Attività Produttive
SUE	Sportello Unico per l'Edilizia
VPN	Virtual Private Network/Rete Privata Virtuale

Città metropolitana di Milano

easygov
INNOVARE, SEMPLICEMENTE

CITTÀ METROPOLITANA DI MILANO

PIANO DI INNOVAZIONE

Milano, 17 settembre 2024

Indice

Il Piano di Innovazione

Il Piano di Innovazione

L’obiettivo del documento

Insieme al Piano Triennale per la Transizione Digitale e al Documento di Policy ICT,
che rappresentano gli altri strumenti di programmazione e indirizzo della strategia digitale dell’Ente,
il Piano di Innovazione è il **documento che mira a definire le azioni utili per diffondere l'innovazione**
all'interno dell'Ente e nei rapporti con gli stakeholder esterni, al fine di migliorare i servizi offerti agli
utenti e di aumentare l'efficienza dell'azione amministrativa.

Il contesto europeo e nazionale

Il contesto europeo e nazionale

I principali documenti normativo-strategici di riferimento in tema di trasformazione digitale

Il Piano di Innovazione della Città Metropolitana di Milano si inquadra in un **contesto nazionale ed europeo che pone vincoli ed obiettivi ambiziosi in tema di trasformazione digitale per la PA.** Pertanto, è necessario **assicurare coerenza** tra gli elementi del Piano di Innovazione e i target nazionali ed europei previsti.

European Digital Compass 2030

Ambiziosi obiettivi in tema di **competenze digitali, digitalizzazione dei servizi pubblici, infrastrutture telematiche**

Strategia «Italia Digitale 2026»

Visione, prospettive e target che accompagnano l'importante programma di investimenti e riforme del PNRR

Piano Triennale di AgID

Indicazioni operative, obiettivi e risultati per l'attuazione della strategia nazionale per la trasformazione digitale delle PA

Altri documenti normativo-strategici che guidano la strategia digitale della Città Metropolitana di Milano sono:

- **Livello nazionale**: Agenda per la semplificazione 2020-2026, Strategia Nazionale di Cybersicurezza 2022-2026
- **Livello europeo**: EU Data Act, Interoperable Europe Act, European Skills Agenda, EU AI Act.

Il progetto

Il progetto

Il processo di elaborazione del Piano di Innovazione

Le attività che hanno portato all'elaborazione della strategia digitale hanno seguito un processo strutturato in **quattro fasi**.

Fase 1: Analisi dello stato dell'arte e dei fabbisogni

- **Analisi della configurazione** dell'Ente dal punto di vista **organizzativo** e **tecnologico**
- **Analisi dei fabbisogni** attraverso **interviste** con il Direttore Generale, il Consigliere Delegato alla Digitalizzazione e il Dipartimento Transizione digitale, oltre a **workshop** con gli altri attori dell'Ente (Direttori di Dipartimento e Responsabili di Area).

Fase 2: Analisi dello scenario normativo

- Analisi del **posizionamento dell'Ente rispetto allo scenario normativo** di riferimento, al fine di valutare il grado di conformità dell'Ente e definire le azioni future utili per garantire il costante rispetto delle prescrizioni.

Fase 3: Analisi di trend e buone pratiche

- Analisi dei **trend tecnologici** in atto e delle **buone pratiche** di Enti simili a Città Metropolitana di Milano, al fine di valutare opportunità di innovazione.

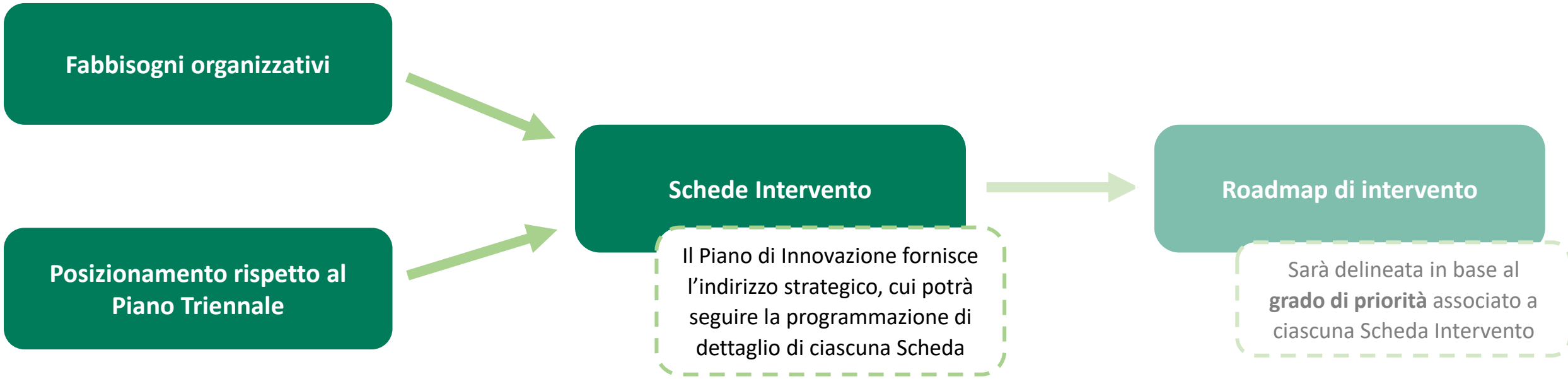
Fase 4: Definizione della strategia

- Definizione della strategia digitale che delinea il **percorso concreto e sostenibile** per il **raggiungimento degli obiettivi di transizione digitale dell'Ente**.

Il progetto

Definizione delle Schede Intervento

Sulla base dei fabbisogni raccolti e del posizionamento dell'Ente rispetto al PT di AgID, sono state identificate **24 Schede Intervento** che rappresentano le azioni che Città Metropolitana di Milano sarebbe utile si impegnasse ad implementare nel prossimo triennio per raggiungere gli obiettivi previsti dalla strategia digitale dell'Ente.



Il progetto

Template della Scheda Intervento

Criticità o adempimento rilevato	*[criticità rilevata durante la Fase 1: Analisi dei fabbisogni]*				
Intervento proposto	*[descrizione dell'intervento proposto]*				
Owner intervento	*[Servizi responsabili della coordinazione dell'intervento]*		**Soggetti beneficiari**	*[soggetti target dell'intervento, sia internamente che esternamente all'Ente]*	
Complessità	Vincoli	*[possibili vincoli all'implementazione]*	**Benefici**	Benefici diretti	*[capacità dell'intervento di risolvere la criticità e di sfruttare le opportunità di innovazione su una scala alto-medio-basso]*
	Soggetti esterni	*[altri Enti, fornitori, utenti, etc. da coinvolgere per l'implementazione]*		Benefici indiretti	*[impatti dell'intervento su altri uffici o soggetti esterni su una scala alto-medio-basso]*
	Servizi coinvolti	*[altri Servizi da coinvolgere per l'implementazione]*	**Costi**	Investimento iniziale	*[investimento richiesto per l'implementazione su una scala alto-medio-basso]*
	Competenze richieste	*[elenco delle competenze critiche richieste]*		Mantenimento a regime	*[investimento per il mantenimento una volta implementato su una scala alto-medio-basso]*
	Sforzo del personale	*[effort del personale in una scala alto-medio-basso]*	**Finanziamenti**	*[presenza di fonti di finanziamento da cui attingere]*	

Il progetto

Obiettivi strategici e macro-categorie di intervento

Sono stati identificati **5 obiettivi strategici**, raggiungibili attraverso specifici interventi raggruppati in **17 macro-categorie.**

Semplificazione dei processi della PA

- Utilizzo di strumenti abilitanti
- Digitalizzazione processi di supporto
- Digitalizzazione dei processi interni
- Interoperabilità tra applicativi interni
- Governance interna
- Rinnovamento hardware ad uso personale

Miglioramento dei servizi offerti

- Utilizzo di piattaforme nazionali
- Digitalizzazione dei servizi
- Utilizzo dell'Intelligenza Artificiale

Aumento delle competenze digitali

- Gestione della conoscenza
- Potenziamento delle competenze

Miglioramento della gestione e conservazione dei dati

- Interscambio di dati
- Open Data
- Dematerializzazione degli archivi

Sviluppo della *governance* metropolitana

- Centro Servizi Territoriali
- Valorizzazione dell'infrastruttura di rete metropolitana
- Community con altre Città Metropolitane

Il progetto

Schede Intervento per macro-categoria (1/2)

Di seguito è riportato l'elenco degli interventi previsti dal Piano di Innovazione, per ciascuno dei quali è indicata la **macro-categoria** di riferimento e, laddove presente, il **riferimento agli obiettivi del Piano Triennale** di AgID che ogni Scheda Intervento contribuisce a raggiungere.

ID	Scheda Intervento	Macro-categoria	Riferimento al PT AgID
1	Favorire l'interoperabilità con sistemi esterni di altre PA	Interscambio di dati	-
2	Favorire lo scambio di dati con soggetti privati		-
3	Condividere i dati aperti prodotti da CMM	Open Data	Capitolo 5, Obiettivi 5.1, 5.2, 5.3
4	Aumentare l'utilizzo di pagoPA	Utilizzo di piattaforme nazionali	Capitolo 4, Obiettivo 4.1
5	Prevedere l'invio di notifiche digitali		Capitolo 4, Obiettivo 4.1
6	Aumentare le collaborazioni con altri Enti	Community con altri Enti	Capitolo 1, Obiettivo 1.1
7	CMM come Centro Servizi Territoriali	Centro Servizi Territoriali	Capitolo 1, Obiettivo 1.1
8	Valorizzazione dell'infrastruttura di rete metropolitana	Valorizzazione dell'infrastruttura di rete metropolitana	Capitolo 6. Infrastrutture
9	Favorire la condivisione documentale con gli utenti esterni	Digitalizzazione dei servizi	Capitolo 3, Obiettivo 3.3
10	Customer satisfaction		Capitolo 3, Obiettivo 3.2
11	Migliorare l'usabilità del sito web di CMM		Capitolo 3, Obiettivo 3.2
12	Promuovere la co-progettazione dei servizi digitali		Capitolo 3, Obiettivo 3.2

Il progetto

Schede Intervento per macro-categoria (2/2)

ID	Scheda Intervento	Macro-categoria	Riferimento al PT AgID
13	Interoperabilità tra applicativi interni	Interoperabilità tra applicativi interni	-
14	Dotare di firma digitale i dipendenti di CMM	Utilizzo di strumenti abilitanti	-
15	Garantire l'accesso tramite SPID		-
16	Definire un modello di governance del digitale all'interno dell'Ente	Governance interna	-
17	Digitalizzare i processi di supporto	Digitalizzazione processi di supporto	-
18	Acquisire nuovi software/gestionali	Digitalizzazione dei processi interni	-
19	Migliorare gli applicativi gestionali a supporto di processi interni		-
20	Dematerializzare gli archivi	Dematerializzazione degli archivi	Capitolo 3, Obiettivo 3.3
21	Dotare i dipendenti di CMM di strumenti idonei	Rinnovamento hardware ad uso personale	-
22	Migliorare la condivisione di informazioni all'interno dell'Ente	Gestione della conoscenza	-
23	Formazione sugli strumenti in uso presso l'Ente	Potenziamento delle competenze	Capitolo 1, Obiettivo 1.2
24	Utilizzare strumenti innovativi	Utilizzo dell'Intelligenza Artificiale	Capitolo 5, Obiettivi 5.4, 5.5

Schede Intervento

Interscambio di dati

1. Favorire l'interoperabilità con sistemi esterni di altre PA

Criticità o adempimento rilevato	I dipendenti della Città Metropolitana di Milano possono riscontrare difficoltà nel recuperare dati utili allo svolgimento delle loro attività da banche dati o software esterni di titolarità di altre Pubbliche Amministrazioni.
Intervento proposto	Identificare le specifiche necessità di integrazione, così da aumentare l'interoperabilità tra gli applicativi interni di Città Metropolitana di Milano e sistemi esterni. L'intervento prevede: (i) una mappatura dei software e delle banche dati dell'Ente che devono configurarsi come interoperabili con sistemi esterni; (ii) valutazione in via prioritaria delle possibilità e modalità di integrazione attraverso la PDND; (iii) in caso di impossibilità di integrazione tramite PDND, valutazione di altre modalità di integrazione sempre tramite API; (iv) in caso di indisponibilità di API, valutazione di modalità di integrazione alternative; (v) implementazione dell'integrazione e definizione di un sistema di monitoraggio per valutare la corretta implementazione delle attività. In particolare, è stata segnalata la necessità di integrare: • l'applicativo del personale con i sistemi dell'INPS, per gestire tutti i dati relativi ai dipendenti di Città Metropolitana che contribuiscono al popolamento del fascicolo del dipendente • la piattaforma *Inlinea* di CMM con l'applicativo *Procedimenti* di Regione Lombardia, anche per assicurare il principio once-only.
Owner intervento	Tutte le U.O. dell'Ente, con supporto del Dipartimento Transizione digitale
Soggetti beneficiari	Personale interno, cittadini

Complessità	Vincoli	Tecnologico (disponibilità API, sviluppo API, configurazione applicativo di CMM da integrare) Disponibilità delle altre PA
	Soggetti esterni	Altre PA
	U.O. coinvolte	U.O. che hanno necessità di integrare software/banche dati, tra cui Dipartimento Risorse Umane e Organizzazione e Area Ambiente
	Competenze richieste	Informatiche Giuridico/amministrative (DPO, privacy, GDPR)
	Sforzo del personale	Medio

Benefici	Benefici diretti	Alti
	Benefici indiretti	Medi
Costi	Investimento iniziale	Laddove è possibile utilizzare API, costo medio per integrazione 2.500€ – 5.000€
	Mantenimento a regime	Se richieste manutenzione e supporto esterno, da valutare in base al numero e alla tipologia di API integrate
Finanziamenti	-	

Interscambio di dati

2. Favorire lo scambio di dati con soggetti privati

Criticità o adempimento rilevato	I dipendenti della Città Metropolitana di Milano possono riscontrare difficoltà nel recuperare dati dai software/database dei soggetti privati con cui l'Amministrazione collabora quotidianamente.
Intervento proposto	Valutare le modalità di integrazione tra i sistemi dell'Ente e i database dei soggetti con cui CMM collabora (es. gestori di strutture come l'Idroscalo, gestori di mezzi di mobilità sostenibile) così da facilitare l'interscambio di dati che CMM potrebbe utilizzare per realizzare politiche *data driven,* nonché a supporto delle attività di programmazione e monitoraggio. L'intervento prevede: (i) ricognizione dei fabbisogni attraverso una mappatura dei software e delle banche dati dell'Ente che si vogliono rendere interoperabili con sistemi esterni; (ii) valutazione in via prioritaria delle possibilità e modalità di integrazione tramite API; (iii) valutazione di modalità di integrazione alternative all'utilizzo di API; (iv) implementazione dell'integrazione e definizione di un sistema di monitoraggio per valutare la corretta implementazione delle attività.
Owner intervento	Tutte le U.O. dell'Ente, con supporto del Dipartimento Transizione digitale
Soggetti beneficiari	Personale interno

Complessità	Vincoli	Tecnologico (disponibilità API, configurazione applicativo di CMM da integrare) Disponibilità dei soggetti privati a fornire/vendere dati
	Soggetti esterni	Fornitori software Proprietari banche dati
	U.O. coinvolte	Strutture dell'Ente che hanno necessità di integrare software/banche dati
	Competenze richieste	Informatiche Giuridico/amministrative (DPO, privacy, GDPR)
	Sforzo del personale	Medio

Benefici	Benefici diretti	Alti
	Benefici indiretti	Medi
Costi	Investimento iniziale	Laddove è possibile utilizzare API, costo medio per integrazione 2.500€ – 5.000€
	Mantenimento a regime	Dati non acquistati: 10.000€/anno per manutenzione e supporto esterno Dati acquistati: molto variabile
Finanziamenti	-	

Open Data

3. Condividere i dati aperti prodotti da CMM

Criticità o adempimento rilevato	Necessità di proseguire il percorso di pubblicazione di open data coerenti con i modelli di riferimento di dati nazionali ed europei (es. Piano Triennale 2024-2026, Linee guida nazionali per la valorizzazione del patrimonio informativo pubblico).		
Intervento proposto	Aggiornare i dati aperti di CMM già pubblicati sul sito di Regione Lombardia, oltre a valutare la possibilità di condividere nuovi dati aperti, compresi quelli di elevato valore. Nello specifico, l'intervento prevede: (i) una fase inziale di individuazione dei dataset più rilevanti per gli stakeholder dell'Ente (cittadini, imprese, altre PA) da aggiornare e/o pubblicare; (ii) una fase di bonifica dei dati con la finalità di rendere i dataset conformi alle linee guida AgID (formato del dato, presenza di metadati ed ontologie di riferimento); (iii) una fase di effettiva pubblicazione sul portale di Regione Lombardia; (iv) una fase finale di comunicazione finalizzata ad informare la comunità della presenza dei dataset pubblicati e di monitoraggio dei risultati ottenuti dalla pubblicazione.		
Owner intervento	Tutte le U.O. dell'Ente, con supporto del Dipartimento Transizione digitale	**Soggetti beneficiari**	Cittadini, imprese, altre PA

Complessità	Vincoli	-	**Benefici**	Benefici diretti	Bassi
	Soggetti esterni	Fornitori software		Benefici indiretti	Medi
	U.O. coinvolte	U.O. che trattano dataset rilevanti (da definire nella fase – individuazione dataset)	**Costi**	Investimento iniziale	10.000€ - 20.000€
	Competenze richieste	Informatiche Organizzative/gestionali Giuridico/amministrative		Mantenimento a regime	Basso
	Sforzo del personale	Medio	**Finanziamenti**	-	

Utilizzo di piattaforme nazionali

4. Aumentare l'utilizzo di pagoPA

Criticità o adempimento rilevato	L'utilizzo della piattaforma pagoPA per i pagamenti digitali da parte di cittadini e imprese verso la Città Metropolitana di Milano è attualmente limitato. In particolare, per l'Area Ambiente, questa modalità è disponibile solo per quattro procedimenti.
Intervento proposto	Aumentare il numero di procedimenti per cui è possibile effettuare pagamenti tramite pagoPA, così da aumentare l'efficienza e la semplificazione nella gestione dei pagamenti dei servizi pubblici. Nello specifico, l'intervento prevede (i) l'individuazione dei servizi per i quali si può utilizzare pagoPA, e (ii) la pubblicazione del servizio su pagoPA.

Owner intervento	Dipartimento Ragioneria Generale, con supporto del Dipartimento Transizione digitale	**Soggetti beneficiari**	Cittadini, imprese

Complessità	Vincoli	-	**Benefici**	Benefici diretti: Medi
	Soggetti esterni	-		Benefici indiretti: Medi
	U.O. coinvolte	U.O. che devono pubblicare su pagoPA i servizi di propria competenza	**Costi**	Investimento iniziale: 4.000€/servizio
	Competenze richieste	Informatiche Organizzative/gestionali		Mantenimento a regime: L'investimento iniziale includerebbe anche un canone di 5 anni
	Sforzo del personale	Basso	**Finanziamenti**	-

Utilizzo di piattaforme nazionali

5. Prevedere l'invio di notifiche digitali

Criticità o adempimento rilevato	Necessità di aggiornare le modalità di notifica ed inoltro Atti agli utenti. Attualmente, a conclusione dei procedimenti digitalizzati sulla piattaforma *Inlinea,* viene inoltrata una notifica all'utente in cui si segnala soltanto che il procedimento è concluso e che un nuovo Atto è disponibile, senza condividere contestualmente il relativo Atto.
Intervento proposto	Aggiornare le modalità di notifica ed inoltro Atti agli utenti adottando nuove piattaforme definite a livello nazionale, nell'ottica di rendere più veloce, economico e sicuro l'invio e la ricezione delle notifiche a valore legale. Pertanto, si vuole valutare la possibilità di utilizzare strumenti alternativi, come l'AppIO e la piattaforma SEND, per procedere con l'invio di notifiche, e contestualmente degli Atti correlati, relative a procedimenti conclusi per cui nuova documentazione è disponibile per il cittadino/impresa. L'intervento prevedere l'identificazione di un primo gruppo di servizi che potranno essere integrati con l'AppIO e la piattaforma SEND per testare la funzionalità e l'efficacia di queste ultime rispetto alle esigenze specifiche dell'Ente. In caso la fase di test abbia esito positivo, si valuterà di ampliare tale modalità ad un numero maggiore di procedimenti.
Owner intervento	Tutte le U.O. dell'Ente, con supporto del Dipartimento Transizione digitale
Soggetti beneficiari	Cittadini, imprese

Complessità	Vincoli	Tecnologici
	Soggetti esterni	Fornitori gestionali
	U.O. coinvolte	U.O. che vogliono utilizzare l'AppIO e la piattaforma SEND per i servizi di propria competenza
	Competenze richieste	Informatiche Organizzative/gestionali
	Sforzo del personale	Basso

Benefici	Benefici diretti	Alti
	Benefici indiretti	Medi
Costi	Investimento iniziale	Sviluppo middleware: circa 15.000€ (invio manuale notifiche) Integrazione singoli servizi: da definire con il fornitore (invio automatico notifiche)
	Mantenimento a regime	L'investimento iniziale includerebbe anche un canone di 5 anni
Finanziamenti	-	

Community con altri Enti

6. Aumentare le collaborazioni con altri Enti

Criticità o adempimento rilevato	Volontà di aumentare la collaborazione con altri Enti, incluse altre Città Metropolitane, visti i riscontri positivi di precedenti collaborazioni (es. Città Metropolitana di Venezia – scambio di best practices inerenti la georeferenziazione dei dati).
Intervento proposto	Vista l'importanza di instaurare rapporti stabili e continuativi con altri Enti, si propone la creazione di una community e/o la partecipazione a community già esistenti con altri Enti con un duplice obiettivo: da un lato, effettuare analisi di benchmark tra Enti simili, al fine di identificare punti di forza di CMM, nonché miglioramenti che potrebbero essere raggiunti grazie alla condivisione di best practices; dall'altro, implementare progettualità che portino beneficio a una maggiore platea di utenti, ma che sarebbero di difficile realizzazione se portate avanti singolarmente.

Owner intervento	Tutte le U.O. dell'Ente	**Soggetti beneficiari**	Amministrazione, altri Enti

Complessità	Vincoli	Disponibilità alla collaborazione di altri Enti	**Benefici**	Benefici diretti: Medi Benefici indiretti: Medi
	Soggetti esterni	Altri Enti		
	U.O. coinvolte	Tutte le U.O. dell'Ente	**Costi**	Investimento iniziale: - Mantenimento a regime: Basso
	Competenze richieste	Organizzative/gestionali Giuridico/amministrative		
	Sforzo del personale	Medio	**Finanziamenti**	-

Centro Servizi Territoriali

7. CMM come Centro Servizi Territoriali

Criticità o adempimento rilevato	Necessità di definire ed instaurare una *governance* comune che supporti gli Enti del territorio, soprattutto i più piccoli, nel fornire servizi omogenei e di qualità agli utenti, nonché a rispondere ad adempimenti specifici del Piano Triennale di AgID (es. Intelligenza Artificiale, creazione di Community).
Intervento proposto	Costituzione di un CST per supportare i comuni del territorio nella gestione delle loro funzioni ICT attraverso la condivisione di risorse e competenze. Le fasi del progetto prevedono: (i) **Ricognizione**: analisi del fabbisogno di trasformazione digitale degli Enti, inclusi digitalizzazione dei servizi, applicativi utilizzati, interoperabilità dei dati, competenze digitali del personale, piattaforme, infrastrutture, connettività e processi organizzativi; (ii) **Progettazione**: definizione del processo di associazione della funzione ICT e progettazione della gestione associata, con valutazione delle azioni di adeguamento tecnologico, stipula degli accordi con gli Enti, e progettazione della migrazione della funzione ICT verso un ufficio centralizzato; (iii) **Implementazione**: attuazione del processo di associazione della funzione ICT secondo la pianificazione, adozione dei nuovi regolamenti, conferimento degli incarichi e individuazione dei referenti di ciascun Ente; (iv) **Gestione**: esecuzione delle strategie e delle azioni di trasformazione digitale degli Enti, monitoraggio e aggiornamento delle attività in base al loro svolgimento congiunto con gli enti associati; (v) **Espansione**: estensione della collaborazione ad altre attività, funzioni potenzialmente associabili e nuovi Enti. A titolo esemplificativo, alcuni servizi che potranno essere erogati dal CST sono: supporto alle attività di programmazione, creazione di una community RTD, utilizzo di piattaforme di *democracy* utili a favorire anche la costruzione dei documenti di programmazione condivisa, strumenti di *collaboration,* fibra ottica, servizi di fonia.
Owner intervento	Direzione Generale, con supporto del Dipartimento Transizione digitale
Soggetti beneficiari	Cittadini, imprese, altre PA

Complessità	Vincoli	Interesse/disponibilità degli Enti del territorio
	Soggetti esterni	Altre PA del territorio metropolitano
	U.O. coinvolte	Dipartimento Transizione digitale
	Competenze richieste	Organizzative/gestionali Giuridico/amministrative Informatiche
	Sforzo del personale	Alto

Benefici	Benefici diretti	Alti
	Benefici indiretti	Alti
Costi	Investimento iniziale	Costi definiti a seguito di uno studio di fattibilità dell'intervento
	Mantenimento a regime	
Finanziamenti	-	

Valorizzazione dell'infrastruttura di rete metropolitana

8. Valorizzazione dell'infrastruttura di rete metropolitana

Criticità o adempimento rilevato	Città Metropolitana offre al territorio un importante patrimonio infrastrutturale, composto da: • più di 7000km di fibra ottica di proprietà di Città Metropolitana disponibili entro dicembre 2024 • oltre agli attuali 80 tralicci dedicati al 5G, a cui potranno aggiungersene ulteriori 40, su cui Città Metropolitana può installare anche infrastruttura specifica da mettere a disposizione della Protezione Civile e ai Comuni del territorio • servizi di fonia, attualmente utilizzati soltanto da 7 Comuni Il numero di Enti utilizzatori di tale infrastruttura e i servizi ad essa correlati potrebbero essere aumentati.
Intervento proposto	Valorizzare e promuovere nei confronti degli Enti del territorio/altri soggetti interessati, eventualmente nell'ambito del nuovo CST (*cfr. Scheda «Centro Servizi Territoriali»*), il patrimonio infrastrutturale di CMM, nonché la creazione e/o diffusione di nuovi servizi a valere su tale infrastruttura.

Owner intervento	Direzione Generale	**Soggetti beneficiari**	Altre PA, cittadini, imprese

Complessità	Vincoli	-	**Benefici**	Benefici diretti: Medio
	Soggetti esterni	Altre PA del territorio metropolitano		Benefici indiretti: Alti
	U.O. coinvolte	-	**Costi**	Investimento iniziale: -
	Competenze richieste	Organizzative/gestionali Giuridico/amministrative Informatiche		Mantenimento a regime: -
	Sforzo del personale	Basso	**Finanziamenti**	-

Digitalizzazione dei servizi

9. Favorire la condivisione documentale con gli utenti esterni

Criticità o adempimento rilevato	Difficoltà a condividere con gli utenti esterni documenti, soprattutto di elevate dimensioni.
Intervento proposto	Si suggerisce di individuare uno strumento di gestione documentale a disposizione di tutte le strutture dell'Ente che permetta la condivisione di file di grandi dimensioni, spesso correlata anche all'ambito procedimentale, con gli utenti esterni a CMM. Per raggiungere tale obiettivo, l'intervento si divide in due fasi: 1. **Analisi preliminari**: (i) identificazione delle U.O. che manifestano la necessità, (ii) analisi dell'utenza per comprendere quali utenti utilizzeranno le nuove modalità di condivisione documentale, (iii) valutazione della possibilità di utilizzare gli attuali applicativi in uso per rispondere a tale criticità. 2. **Analisi e adozione di nuove soluzioni**: nel caso in cui gli attuali applicativi non rispondano alle esigenze, (i) sarà svolto un *assessment* delle diverse soluzioni presenti sul mercato, (ii) verranno individuate le modalità di acquisizione del nuovo strumento e infine (iii) verrà dispiegato il nuovo strumento, a disposizione di cittadini/imprese/liberi professionisti oltre che ai dipendenti dell'Ente. Nel caso in cui tali documenti si riferiscano ad un procedimento, verranno valutate le modalità di integrazione tra questo strumento e altri applicativi dell'Ente, a seconda della necessità (es. Protocollo).
Owner intervento	Tutte le U.O. dell'Ente, con supporto del Dipartimento Transizione digitale
Soggetti beneficiari	Utenti esterni all'Ente

Complessità	Vincoli	Tecnologici
	Soggetti esterni	Fornitore della piattaforma
	U.O. coinvolte	Tutte le U.O. dell'Ente
	Competenze richieste	Organizzative/gestionali Informatiche
	Sforzo del personale	Medio

Benefici	Benefici diretti	Medi
	Benefici indiretti	Bassi
Costi	Investimento iniziale	5.000€ - 20.000€
	Mantenimento a regime	Basso
Finanziamenti	-	

Digitalizzazione dei servizi

10. Customer satisfaction

Criticità o adempimento rilevato	Per molti dei servizi digitali messi a disposizione non è previsto un meccanismo per valutare il grado di soddisfazione da parte degli utenti fruitori.
Intervento proposto	Revisione e aggiornamento degli strumenti utili a rilevare i livelli di *customer satisfaction* degli utenti che utilizzano i servizi digitali messi a disposizione da CMM, come i questionari di *feedback* presenti sulla piattaforma *Inlinea - Servizi online per la cittadinanza e le imprese*.

Owner intervento	Tutte le U.O. dell'Ente, con supporto del Dipartimento Transizione digitale	**Soggetti beneficiari**	Fruitori dei servizi digitali

Complessità	Vincoli	-
	Soggetti esterni	Fornitore della piattaforma Altri fornitori con competenze specifiche
	U.O. coinvolte	-
	Competenze richieste	Informatiche
	Sforzo del personale	Basso

Benefici	Benefici diretti	Medi
	Benefici indiretti	Bassi
Costi	Investimento iniziale	5.000€ - 10.000€
	Mantenimento a regime	Basso
Finanziamenti	-	

Digitalizzazione dei servizi

11. Migliorare l'usabilità del sito web di CMM

Criticità o adempimento rilevato	La consultazione del sito web istituzionale di CMM potrebbe essere migliorata. Attualmente, le modalità di comunicazione con gli utenti esterni sono eterogenee all'interno dell'Ente poiché ogni sotto-sito tematico viene gestito dalla struttura responsabile: ciò porta a disomogeneità di linguaggio utilizzato, contenuto condiviso, tempistiche di esposizione delle informazioni.
Intervento proposto	Utilizzando come riferimento le Linee Guida di design per i siti internet disponibili su Designers Italia, l'intervento si propone di: (i) **ridefinire l'architettura dell'informazione**, identificando un insieme di standard/linee guida che permettano di uniformare la comunicazione con gli utenti tramite sito web dell'Ente, (ii) **uniformare la *user interface*** del sito web; (iii) **creare collegamenti diretti tra i diversi sotto-siti tematici** presenti, ponendo particolare attenzione alla sezione «Amministrazione Trasparente»; (iv) **inserire uno strumento di ricerca** informazioni all'interno del portale istituzionale; (v) **implementare test di usabilità** semplificati (utilizzando anche le linee guida fornite da AgID) per valutare l'usabilità del sito web dell'Amministrazione.

Owner intervento	Direzione Generale, Ufficio Relazioni con il Pubblico (URP)	**Soggetti beneficiari**	Cittadini, imprese, altre PA, personale interno

Complessità	Vincoli	-	**Benefici**	Benefici diretti: Medi Benefici indiretti: Medi
	Soggetti esterni	Fornitore del sito web Altri fornitori con competenze specifiche		
	U.O. coinvolte	Tutte le U.O. dell'Ente	**Costi**	Investimento iniziale: 50.000 – 100.000 € Mantenimento a regime: Basso
	Competenze richieste	Organizzative/gestionali Informatiche		
	Sforzo del personale	Medio	**Finanziamenti**	-

Digitalizzazione dei servizi

12. Promuovere la co-progettazione dei servizi digitali

Criticità o adempimento rilevato	I servizi digitali trasversali a più strutture, se non co-progettati dai diversi attori coinvolti nello specifico servizio, non rispondono a pieno alle necessità delle singole U.O. coinvolte, né alle esigenze dei fruitori finali.
Intervento proposto	L'intervento è volto a identificare le modalità di co-progettazione dei servizi che coinvolgono diverse U.O. dell'Ente. In particolare, il Dipartimento Transizione digitale è identificato come l'U.O. responsabile delle attività di co-progettazione di servizi digitali. A tal fine, il Dipartimento Transizione digitale svolgerà diverse azioni: 1. **Acquisizione dei fabbisogni di co-progettazione** di un sistema digitale, facilitata dalle interazioni tra il Dipartimento e i referenti IT di ciascuna U.O. (*cfr. scheda «Definire un modello di governance del digitale all'interno dell'Ente»);* 2. **Analisi del contesto** per definire l'obiettivo del sistema che si vuole co-progettare; 3. **Organizzazione di uno o più workshop** con gli attori dell'Ente interessati per co-progettare, da un lato l'esperienza utente del servizio, dall'altro i contenuti del sistema: a) Workshop per l'esperienza utente: (i) si identificano le diverse tipologie di utenti coinvolti nel servizio, che andranno raggruppati in base a caratteristiche simili; (ii) si valutano tutte le fasi dell'esperienza attuale di interazione con il sistema, per ogni categoria di utente; (iii) partendo dalle criticità riscontrate, si identificano possibili soluzioni fino ad arrivare a soluzioni solide b) Workshop per i contenuti del sistema: (i) mappando le fasi del servizio, si valutano i bisogni informativi dell'utente; (ii) si valuta se i contenuti del sistema devono esser progettati, ri-progettati, revisionati, oppure ottimizzati; (iii) a seconda della fase in cui ci si trova, possono essere utilizzati i template di AgID per supportare e indirizzare il lavoro sui contenuti. Una volta terminata la fase di co-progettazione, se possibile, si potrà realizzare un prototipo del sistema e procedere con le attività di test con gli utenti utilizzatori. Se la fase di test dovesse dare esito negativo, si potranno prevedere ulteriori momenti di co-progettazione per adattare il prototipo e quindi il servizio alle effettive esigenze degli utenti.
Owner intervento	Tutte le U.O. dell'Ente, con supporto del Dipartimento Transizione digitale
Soggetti beneficiari	Amministrazione, utenti fruitori dei servizi

Complessità	Vincoli	-
	Soggetti esterni	Fornitori coinvolti
	U.O. coinvolte	Tutte le U.O. dell'Ente, a seconda del servizio da progettare/ri-progettare
	Competenze richieste	Informatiche Organizzative/gestionali
	Sforzo del personale	Medio

Benefici	Benefici diretti	Medi
	Benefici indiretti	Medi
Costi	Investimento iniziale	-
	Mantenimento a regime	Basso
Finanziamenti	-	

Interoperabilità tra applicativi interni

13. Interoperabilità tra applicativi interni

Criticità o adempimento rilevato	La mancata integrazione tra alcuni pacchetti applicativi esistenti ed in uso presso l'Ente può rendere inefficiente l'attività delle U.O., che si trovano a dover replicare più volte la stessa attività, spesso copiando i dati da un applicativo ad un altro, con un margine di errore molto alto.
Intervento proposto	Individuare le criticità specifiche inerenti alla mancata integrazione tra i diversi applicativi esistenti ed in uso presso l'Ente e le modalità per integrare tali applicativi, così da garantire una maggiore interoperabilità e aumenterebbe notevolmente l'efficacia delle attività. Un primo caso potrebbe riguardare l'integrazione di alcuni applicativi esistenti con l'applicativo *CiviliaNext Contabilità*. In particolare, verranno valutate le criticità e sviluppate le necessarie integrazioni, rispetto a: • programma Atti • applicativo del personale • gestionale a supporto della redazione del Piano esecutivo di gestione (PEG)

Owner intervento	Dipartimento di Trasformazione Digitale, con coinvolgimento delle U.O. dell'Ente interessate	**Soggetti beneficiari**	Personale interno

Complessità	Vincoli	Tecnologici
	Soggetti esterni	Fornitori degli applicativi
	U.O. coinvolte	U.O. dell'Ente di cui si vogliono integrare gli applicativi
	Competenze richieste	Informatiche
	Sforzo del personale	Medio

Benefici	Benefici diretti	Alti
	Benefici indiretti	Medi
Costi	Investimento iniziale	5.000 – 10.000 €/applicativo da integrare (verificare con fornitore)
	Mantenimento a regime	Basso
Finanziamenti	-	

Utilizzo di strumenti abilitanti

14. Dotare di firma digitale i dipendenti di CMM

Criticità o adempimento rilevato	Necessità di dotare i dipendenti di firma digitale per garantire loro la possibilità di firmare documenti elettronici in modo sicuro e legalmente vincolante.
Intervento proposto	L'intervento è volto ad acquistare firme digitali remote per i dipendenti che ne manifestano la necessità. L'obiettivo è inoltre quello di dotare anche i nuovi dipendenti di firma digitale, già dal momento di firma del contratto, in modo tale che anche questo documento sia nativo digitale.

Owner intervento	Dipartimento Transizione digitale		**Soggetti beneficiari**	Personale interno	
Complessità	Vincoli	-	**Benefici**	Benefici diretti	Medi
	Soggetti esterni	Fornitori del servizio		Benefici indiretti	Medi
	U.O. coinvolte	Tutte le U.O. dell'Ente	**Costi**	Investimento iniziale	30€ - 50€ cad, che garantisce una durata di 3 anni (stima)
	Competenze richieste	Organizzativo/gestionali		Mantenimento a regime	Costo di rinnovo
	Sforzo del personale	Basso	**Finanziamenti**	-	

Utilizzo di strumenti abilitanti

15. Garantire l'accesso tramite SPID

Criticità o adempimento rilevato	Spesso i dipendenti di Città Metropolitana si trovano ad utilizzare il proprio SPID personale per accedere a servizi messi a disposizione da altri Enti. Tale modalità può creare problemi legati alla raccolta e condivisione di informazioni, non permettendo di rintracciare le interazioni tra Enti diversi nell'ambito delle proprie attività professionali, né tantomeno la possibilità di identificare i dipendenti di CMM come tali.
Intervento proposto	L'intervento è volto a sviluppare, attraverso policy interne, la corretta gestione delle credenziali per l'accesso ai portali messi a disposizione da altri Enti. In particolare, si propone l'introduzione di appositi meccanismi di delega interni in merito alla gestione dello SPID all'interno dei servizi maggiormente coinvolti dalla criticità evidenziata al fine di poter svolgere le attività o controlli di dominio interessate. Tale intervento potrà ovviare alle criticità sopra presentate, permettendo ai dipendenti di gestire correttamente ed autonomamente i controlli necessari al completamento delle attività in oggetto.

Owner intervento	Dipartimento Transizione digitale		**Soggetti beneficiari**	Personale interno	
Complessità	Vincoli	-	**Benefici**	Benefici diretti	Medi
	Soggetti esterni	-		Benefici indiretti	Bassi
	U.O. coinvolte	Tutte le U.O. dell'Ente	**Costi**	Investimento iniziale	Basso
	Competenze richieste	Organizzativo/gestionali		Mantenimento a regime	Basso
	Sforzo del personale	Basso	**Finanziamenti**	-	

Governance interna

16. Definire un modello di governance del digitale all'interno dell'Ente

Criticità o adempimento rilevato	I meccanismi di coordinamento che garantiscono la governance del digitale all'interno dell'Ente non sono pienamente formalizzati.
Intervento proposto	Formalizzare il ruolo del Dipartimento Transizione digitale e i meccanismi di coordinamento con le altre U.O. dell'Ente. A tal fine verrà individuato un referente IT all'interno di ciascuna U.O. dell'Ente che rappresenterà il punto di contatto tra l'U.O. e il Dipartimento Transizione digitale. Queste figure potranno supportare ricognizioni preliminari dei fabbisogni puntali per ciascuna U.O., i cui esiti verranno comunicati al Dipartimento Transizione digitale che fornirà linee di indirizzo per procedere con le relative attività. Per supportare il lavoro dei referenti IT, il Dipartimento Transizione digitale elaborerà inoltre delle Linee Guida per indirizzare le attività di ricognizione dei fabbisogni svolte dai referenti IT delle U.O. e la successiva fase di acquisto di nuove soluzioni, promuovendo in prima istanza il riuso di soluzioni già predisposte da altre PA. I referenti IT delle U.O. potranno, inoltre, supportare il dispiegamento di nuove soluzioni, facilitando la comunicazione e attivando logiche di formazione peer to peer. Inoltre, si promuoverà la collaborazione tra esperti di dominio applicativo del Dipartimento Transizione digitale e le diverse U.O. per uno sviluppo diffuso delle competenze specialistiche con l'obiettivo di valorizzare a pieno le potenzialità delle soluzioni adottate e la consapevolezza sulle prospettive evolutive.
Owner intervento	Dipartimento Transizione digitale
Soggetti beneficiari	Amministrazione

Complessità	Vincoli	-
	Soggetti esterni	-
	U.O. coinvolte	Tutte le U.O. dell'Ente
	Competenze richieste	Organizzative/gestionali
	Sforzo del personale	Medio

Benefici	Benefici diretti	Medi
	Benefici indiretti	Medi
Costi	Investimento iniziale	-
	Mantenimento a regime	-
Finanziamenti	-	

Digitalizzazione dei processi di supporto

17. Digitalizzare i processi di supporto

Criticità o adempimento rilevato	I processi di supporto dell'Ente (es. richiesta permessi, gestione orario, richiesta/approvazione smartworking, trasferte, prenotazione sale) non sono sempre gestiti attraverso strumenti digitali interoperabili. Spesso vengono utilizzate comunicazioni via email o strumenti Office (es. moduli Excel) rendendo la gestione del processo meno efficiente.
Intervento proposto	L'intervento si propone di (i) svolgere un'attività di analisi degli strumenti attualmente in uso presso l'Ente per valutare se questi possono rispondere alla criticità, (ii) svolgere un'attività di *assessment* delle soluzioni tecnologiche messe a disposizione da altre PA oppure a disposizione sul mercato, (iii) definire le modalità di acquisizione della soluzione prescelta (riuso/acquisto) nonché (iv) implementare la soluzione prescelta che permetterà di digitalizzare i processi di supporto.

Owner intervento	Tutte le U.O. dell'Ente, con supporto del Dipartimento Transizione digitale	**Soggetti beneficiari**	Personale interno

Complessità	Vincoli	-
	Soggetti esterni	Fornitori del software Altro fornitore con competenze specifiche
	U.O. coinvolte	Tutte le U.O. dell'Ente
	Competenze richieste	Informatiche
	Sforzo del personale	Basso

Benefici	Benefici diretti	Alti
	Benefici indiretti	Alti
Costi	Investimento iniziale	15.000€, in caso di acquisto di una nuova soluzione tecnologica
	Mantenimento a regime	1.500€/mese
Finanziamenti	-	

Digitalizzazione dei processi interni

18. Acquisire nuovi software/gestionali

Criticità o adempimento rilevato	Qualora migliorie a software in uso presso l'Ente non siano sufficienti, è necessario acquisire nuovi software/gestionali a supporto dei processi interni, compresi quelli attualmente non digitalizzati.
Intervento proposto	Prima di procedere con l'acquisizione dei nuovi software/gestionali, sarà fondamentale effettuare un assessment degli attuali applicativi in uso per valutare le esigenze e le carenze tecnologiche e organizzative. Questo processo includerà: (i) un'**analisi dettagliata dei flussi di lavoro esistenti** e delle interazioni tra i vari dipartimenti per identificare le aree che necessitano di miglioramenti; (ii) la **raccolta di feedback dal personale** per comprendere le difficoltà attuali e le necessità future; (iii) la **definizione di obiettivi chiari e misurabili** per l'implementazione dei nuovi strumenti, assicurando che essi siano allineati con la strategia complessiva dell'Ente. In via prioritaria, verranno acquisiti nuovi software/gestionali per digitalizzare i processi relativi a: • gestione delle opere, così che venga costantemente assicurato un allineamento tra l'avanzamento tecnico e finanziario delle opere, nonché sia permessa un'eventuale riprogrammazione • redazione del Piano di utilizzo degli edifici scolastici, il quale prevede la mappatura delle strutture scolastiche e assegnazione spazi per la didattica. Attualmente la mappatura viene fatta raccogliendo le planimetrie delle scuole in formato PDF • concorsi pubblici indetti da CMM. L'Amministrazione sta attualmente valutando alcune esperienze nazionali, tra cui la possibilità di utilizzare inPA, così da trovare un applicativo che permetta lo svolgimento interamente digitale del concorso stesso.
Owner intervento	Dipartimento Appalti e Contratti
Soggetti beneficiari	Personale interno

Complessità	Vincoli	-
	Soggetti esterni	Fornitori software/gestionali
	U.O. coinvolte	Dipartimento Transizione digitale Tutte le U.O. dell'Ente che necessitano di acquisire nuovi software/gestionali
	Competenze richieste	Informatiche Giuridico/amministrative (gestione dati, DPO, privacy, GDPR)
	Sforzo del personale	Medio

Benefici	Benefici diretti	Medi
	Benefici indiretti	Medi
Costi	Investimento iniziale	Molto variabile a seconda dei software acquisiti
	Mantenimento a regime	Molto variabile a seconda dei software acquisiti
Finanziamenti	-	

Digitalizzazione dei processi interni

19. Migliorare gli applicativi gestionali a supporto di processi interni

Criticità o adempimento rilevato	Necessità di aggiornare alcuni applicativi a supporto dei processi interni all'Ente per efficientarne l'utilizzo.
Intervento proposto	Valutare le criticità inerenti i diversi applicativi e le relative necessità di miglioramento. A tal fine: (i) verranno **raccolte le esigenze specifiche** delle singole U.O. tramite una ricognizione interna, (ii) sarà svolto un ***assessment* degli applicativi** che, nella prima fase, sono risultati necessitanti di upgrade, (iii) in base all'esito dell'*assessment*, saranno **valutate le modalità con cui implementare le migliorie**, (iv) infine, verranno **realizzati gli upgrade** previsti. Prime applicazioni specifiche di questo intervento, potranno essere realizzate per i software utilizzati per: • la costruzione di documenti di programmazione e controllo, nonché di valutazione della performance che richiedono, inoltre, l'interoperabilità con diversi applicativi dell'Ente. Si sta valutando inoltre di creare un cruscotto di *business intelligence* per il monitoraggio • attività di redazione Atti, attraverso la creazione di modelli di atto (determinazioni, decreti, delibere, liquidazioni) che siano davvero digitali e che guidino la compilazione, soprattutto in riferimento alla parte finanziaria che è oggi ancora compilata come testo libero
Owner intervento	Dipartimento di Trasformazione Digitale, con coinvolgimento delle U.O. dell'Ente interessate
Soggetti beneficiari	Personale interno

Complessità	Vincoli	Tecnologici
	Soggetti esterni	Fornitori degli applicativi
	U.O. coinvolte	U.O. dell'Ente che hanno necessità di aggiornare i propri applicativi gestionali
	Competenze richieste	Organizzativo/gestionali Informatiche
	Sforzo del personale	Medio

Benefici	Benefici diretti	Medi
	Benefici indiretti	-
Costi	Investimento iniziale	Variabile, a seconda dell'applicativo per cui è necessario l'upgrade
	Mantenimento a regime	Basso
Finanziamenti	-	

Dematerializzazione degli archivi

20. Dematerializzare gli archivi

Criticità o adempimento rilevato	Necessità di digitalizzare i documenti di proprietà di Città Metropolitana ancora attualmente in forma cartacea con l'obiettivo di meglio rispondere alle esigenze di personale interno, di professionisti e singoli cittadini, i quali chiedono di poter entrare in possesso dei documenti e delle informazioni necessarie allo svolgimento delle loro attività e alla tutela dei loro interessi in tempi sempre più rapidi.
Intervento proposto	L'Ente ha avviato da qualche anno un progetto di carattere generale per il riordino e la valorizzazione del proprio patrimonio documentale Dopo aver progressivamente riordinato i fondi archivistici sarà possibile elaborare dei progetti di digitalizzazione di particolari fondi o tipologie documentarie. La selezione delle porzioni di archivio da digitalizzare sarà effettuata sulla base di un confronto con gli uffici in relazione alle esigenze specifiche di ciascuno. La pianificazione e la redazione del progetto di digitalizzazione sarà preceduta da un'attività di ricognizione e analisi: 1. degli obiettivi che si intendono raggiungere; 2. del fondo archivistico oggetto del progetto e degli strumenti di recupero dell'informazione; 3. dell'intervento di digitalizzazione (scansione, metadatazione, gestione e conservazione delle immagini); 4. individuazione del/i soggetto/i incaricato/i.
Owner intervento	Dipartimento Transizione digitale
Soggetti beneficiari	Amministrazione

Complessità	Vincoli	Proattività uffici Gestore documentale
	Soggetti esterni	Fornitori software/gestionali
	U.O. coinvolte	U.O. dell'Ente
	Competenze richieste	Informatiche Organizzative/gestionali Archivistiche
	Sforzo del personale	Medio

Benefici	Benefici diretti	Medi
	Benefici indiretti	Medi
Costi	Investimento iniziale	Variabile, in relazione al tipo di documento da digitalizzare ed alla consistenza della serie oggetto di intervento
	Mantenimento a regime	Basso
Finanziamenti	-	

Rinnovamento hardware ad uso personale

21. Dotare i dipendenti di CMM di strumenti idonei

Criticità o adempimento rilevato	Alcuni dipendenti dell'Ente non dispongono ancora degli strumenti per svolgere al meglio l'attività lavorativa, soprattutto quando operano in modalità smartworking.
Intervento proposto	L'intervento prevede l'acquisto degli strumenti hardware, principalmente pc, ad uso personale per i dipendenti della Città Metropolitana che ancora non ne dispongono.

Owner intervento	Dipartimento Transizione digitale		**Soggetti beneficiari**	Personale interno	
Complessità	Vincoli	-	**Benefici**	Benefici diretti	Alti
	Soggetti esterni	Fornitori degli strumenti		Benefici indiretti	Bassi
	U.O. coinvolte	Tutte le U.O. dell'Ente	**Costi**	Investimento iniziale	Variabile, a seconda del numero di strumenti acquistati
	Competenze richieste	Organizzativo/gestionali		Mantenimento a regime	Basso
	Sforzo del personale	Basso	**Finanziamenti**	-	

Gestione della conoscenza

22. Migliorare la condivisione di informazioni all'interno dell'Ente

Criticità o adempimento rilevato	Attualmente, i dipendenti possono trovarsi nella situazione di dover richiedere a utenti esterni e/o ad altre Unità Organizzative informazioni o documenti già disponibili all'interno dell'Ente. Questo può essere dovuto a una circolazione non ottimale delle informazioni all'interno dell'Amministrazione, con possibili impatti sull'efficienza.
Intervento proposto	Per garantire una migliore circolazione delle informazioni all'interno dell'Ente, si propone di adottare logiche e una piattaforma di *collaboration* che permetta l'interazione costante tra le diverse strutture dell'Ente e la condivisione di dati. Prima di implementare la soluzione tecnologica, sarà fondamentale identificare le procedure e i processi che richiedono uno scambio di dati frequente e critico attraverso un'analisi dettagliata dei flussi informativi attuali, con l'obiettivo di individuare le aree che beneficeranno maggiormente dall'integrazione della nuova piattaforma. Saranno quindi definite le priorità e sviluppate linee guida operative per la gestione delle informazioni, includendo la definizione di ruoli e responsabilità specifiche per la gestione dei dati e l'interazione tramite la piattaforma. Inoltre, verranno stabilite procedure di monitoraggio e valutazione dell'efficacia della piattaforma. Si valuterà la possibilità di utilizzare lo stesso strumento previsto dalla Scheda Intervento *«Favorire la condivisione documentale con gli utenti esterni»,* per ottimizzare i costi, in cui verrà predisposta un'area riservata al personale di Città Metropolitana.

Owner intervento	Tutte le U.O. dell'Ente	**Soggetti beneficiari**	Personale interno

Complessità	Vincoli	-
	Soggetti esterni	Fornitore della piattaforma
	U.O. coinvolte	Tutte le U.O. dell'Ente
	Competenze richieste	Organizzativo/gestionali Informatiche
	Sforzo del personale	Medio

Benefici	Benefici diretti	Medi
	Benefici indiretti	Medi
Costi	Investimento iniziale	5.000€ - 20.000€ (costo già indicato nella Scheda Intervento *«Favorire la condivisione documentale con gli utenti esterni»)*
	Mantenimento a regime	Basso
Finanziamenti	-	

Potenziamento delle competenze dei dipendenti di CMM

23. Formazione sugli strumenti in uso presso l'Ente

Criticità o adempimento rilevato	Generale bisogno di formazione in ambito digitale, con specifico riferimento a strumenti Office 365 (in uso dalla fine del 2023) e ad applicativi in uso presso l'Ente.
Intervento proposto	Aumentare la conoscenza e le competenze dei dipendenti di Città Metropolitana di Milano sui nuovi strumenti di Office 365 e sugli applicativi in uso. In particolare, l'intervento prevederà due fasi: 1. **Progettazione ed erogazione di formazione su specifiche soluzioni**. A tal fine, (i) verrà svolta una ricognizione per identificare i bisogni formativi specifici, (ii) saranno valutati i livelli di competenze di partenza e conseguente definizione dei gap da colmare, (iii) verranno progettate ed erogate sessioni formative; 2. **Identificazione di un modello di supporto utilizzabile in situazione di regime**. Per fare ciò, saranno previste attività di *peer-to-peer education* volte a favorire la condivisione di conoscenze, esperienze, informazioni e competenze tra dipendenti dell'Ente.
Owner intervento	Dipartimento Risorse Umane e Organizzazione, Dipartimento Transizione Digitale
Soggetti beneficiari	Personale interno

Complessità	Vincoli	-
	Soggetti esterni	Esperti tematici
	U.O. coinvolte	Tutte le U.O. dell'Ente
	Competenze richieste	Organizzative/gestionali
	Sforzo del personale	Medio

Benefici	Benefici diretti	Medi
	Benefici indiretti	Medi
Costi	Investimento iniziale	10.000 – 30.000 € (variabile in base alla quantità di formazione erogata)
	Mantenimento a regime	Basso
Finanziamenti	-	

Utilizzo dell'Intelligenza Artificiale

24. Utilizzare strumenti innovativi

Criticità o adempimento rilevato	In linea con l'obiettivo 5.4 del Piano Triennale, CMM mira ad aumentare «la consapevolezza della Pubblica Amministrazione nell'adozione delle tecnologie di intelligenza artificiale»
Intervento proposto	Valutare l'utilizzo di strumenti innovativi per semplificare le azioni da parte dei cittadini, nonché l'attività dei dipendenti di CMM. In particolare, l'intervento è volto a (i) valutare le attività e i processi dove si possono utilizzare soluzioni di AI e, successivamente, (ii) identificare le tecnologie che potrebbero essere utilizzate. Ad esempio, si potrebbero utilizzare chatbot per lo smistamento delle richieste interne di assistenza all'help desk, per la consultazione delle informazioni sul sito web, per la raccolta delle informazioni dislocate tra i diversi sotto-siti tematici.

Owner intervento	Dipartimento di Transizione Digitale		**Soggetti beneficiari**	Dipendenti dell'Ente, cittadini	
Complessità	Vincoli	Tecnologici Normativi	**Benefici**	Benefici diretti	Medi
	Soggetti esterni	Fornitore sito web, fornitore help desk		Benefici indiretti	Medi
	Servizi coinvolti	-	**Costi**	Investimento iniziale	Basso
	Competenze richieste	Informatiche		Mantenimento a regime	Variabile, a seconda della soluzione scelta
	Sforzo del personale	Basso	**Finanziamenti**	-	

Città
metropolitana
di Milano

easygov
INNOVARE, SEMPLICEMENTE

Città
metropolitana
di Milano

Disciplinare per l'utilizzo dei servizi informatici e di comunicazione telematica

Milano, 17 Settembre 2024

PREMESSA

Il Sistema Informativo rappresenta una componente vitale per l'operatività della Città Metropolitana di Milano, che promuove attivamente tutti gli interventi tecnologici, procedurali e organizzativi atti a mantenere un adeguato livello di sicurezza dell'infrastruttura e dei servizi nel costante rispetto delle normative in materia.

Le complesse attività volte al raggiungimento di tale obiettivo richiedono una continua evoluzione tecnologica e la collaborazione di tutti i soggetti coinvolti.

Un utilizzo consapevole degli strumenti informatici rappresenta una condizione imprescindibile e un obiettivo prioritario da perseguire.

A tal fine, viene individuato l'insieme di regole atte a definire il corretto comportamento da tenere nell'utilizzo dei dispositivi e dei servizi messi a disposizione degli utenti dalla Città Metropolitana di Milano, garantendo la conformità dei sistemi informativi ai requisiti di sicurezza ed alle vigenti normative sulla tutela della privacy.

Art. 1 - Oggetto

Il presente disciplinare ha per oggetto i criteri e le modalità operative di accesso e di utilizzo dei servizi informatici e telematici (servizio Intranet, Internet e posta elettronica) da parte degli utenti che utilizzano tali servizi.

Destinatari del presente disciplinare sono i dipendenti, collaboratori e tutti gli utilizzatori che, a vario titolo, nello svolgimento della propria attività, ricorrono ai servizi informatici e telematici forniti dalla Città Metropolitana di Milano.

Il presente disciplinare non disciplina strumenti e servizi che la Città Metropolitana di Milano mette a disposizione dell'utenza esterna. In tali casi il settore richiedente è responsabile dell'osservanza delle norme di legge in materia.

Art. 2 - Riferimenti normativi, adozione e pubblicità

Il presente disciplinare è adottato ai sensi del:

- D.lgs. 196 del 30 giugno 2003 (Codice in materia di protezione dei dati personali - Allegato B);
- D.lgs. 82 del 7 marzo 2005 (Codice dell'amministrazione digitale);
- Provvedimento 1° marzo 2007 del Garante per la protezione dei dati personali (Linee Guida sull'uso di posta elettronica e internet nei rapporti di lavoro). In particolare, questo Provvedimento costituisce il disciplinare d'uso di internet e della posta elettronica nei rapporti di lavoro ed è adottato dalla Città Metropolitana con le modalità prescritte per i regolamenti sull'ordinamento degli uffici e dei servizi;
- Regolamento (UE) 2016/679 (*General Data Protection Regulation*)
- Circolare n. 1 del 17 marzo 2017 (Misure minime di sicurezza ICT per le pubbliche amministrazioni; Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015);

- D.lgs. 101 del 10 agosto 2018 (Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679);
- DPR nr. 81 del 13.06.2023 (Codice di comportamento dei dipendenti della Pubblica Amministrazione, con specifico riferimento alle nuove norme riguardanti l'utilizzo delle tecnologie informatiche, dei mezzi di informazione e dei social media).
- L. 90 del 28 giugno 2024 (Legge sulla Cybersicurezza)
- Piano Triennale per l'informatica nella Pubblica Amministrazione 2024-2026;

L'allegato tecnico al presente disciplinare, limitandosi a descrivere aspetti tecnici relativi ai sistemi informatici e di comunicazione telematica, viene aggiornato dal Dipartimento Transizione digitale mediante atto dirigenziale.

Di tale disciplinare, dell'allegato tecnico e relativi aggiornamenti si dà adeguata diffusione tra i destinatari, anche attraverso la rete intranet.

Art. 3 - Uso degli strumenti e dei servizi informatici - modalità di accesso e norme di comportamento

L'uso degli strumenti e dei servizi informatici è indispensabile per assicurare l'efficienza e l'efficacia della Pubblica Amministrazione.

Gli utenti sono tenuti a mantenere in buono stato gli strumenti e ad osservare le seguenti norme di utilizzo dei servizi. Il Dipartimento Transizione digitale, al fine di garantire la sicurezza del sistema, si riserva di sospendere temporaneamente i servizi informatici per effettuare accertamenti e controlli.

Per accedere ai servizi informatici da una postazione di lavoro viene utilizzato il meccanismo di Multi-Factor Authentication (MFA). L'utente è infatti tenuto ad autenticarsi utilizzando un codice identificativo (userid) e una parola chiave segreta (password) che sono rilasciati dal Dipartimento Transizione digitale e successivamente procedere con l'autenticazione utilizzando gli strumenti messi a disposizione dall'Amministrazione.

Poiché la conoscenza della password può consentire indebitamente a terzi l'accesso alla rete della Città Metropolitana in nome dell'utente titolare e l'accesso ai dati cui il medesimo è abilitato (ad es. visualizzazione di informazioni riservate, distruzione o modifica dei dati, lettura della posta elettronica, ecc.), ogni utente è tenuto ad attenersi alle seguenti indicazioni:

- Conservare la propria password con riservatezza e diligenza non cedendola a terzi;
- Cambiare con periodicità la propria password (ogni sei mesi o tre mesi nel caso si gestiscano dati sensibili e/o giudiziari);
- Non utilizzare credenziali (userid e password) di altri utenti, nemmeno se fornite volontariamente o di cui si ha casualmente conoscenza;
- Non cedere, una volta superata la fase di autenticazione, l'uso della propria postazione ad altre persone senza la propria supervisione;

- Non lasciare incustodita ed accessibile la propria postazione una volta connesso al sistema con le proprie credenziali di autenticazione;
- Utilizzare per il proprio lavoro soltanto componenti hardware e software autorizzati dall'Ente e/o di proprietà dell'Ente;
- Prendere tutte le precauzioni necessarie a prevenire l'accesso ai dati salvati in locale sulla postazione di lavoro da parte di persone non autorizzate. L'utente è infatti responsabile di tali dati;
- Salvare periodicamente i dati importanti residenti sul proprio personal computer per evitare spiacevoli inconvenienti, come la perdita dei file causata da guasti hardware o da cancellazione involontaria. Il dipendente dovrà posizionare i file di lavoro nella cartella "Documenti" del proprio computer che dovrà essere sincronizzata su un sistema condiviso di archiviazione messo a disposizione dall'Ente (OneDrive). Inoltre, nel caso di dati estremamente sensibili, sarà necessario cifrare i documenti contenenti tali dati utilizzando gli strumenti di criptazione già in uso presso l'Ente.
- Procedere con la protocollazione di documentazione a valore legale secondo le regole previste dal Manuale di Gestione dell'Ente.
- Non è consentito l'utilizzo degli strumenti e dei servizi informatici per attività non connesse allo svolgimento delle mansioni lavorative assegnate;
- Non è consentito dalla propria postazione di lavoro disinstallare o disattivare sistemi di protezione o aggirare politiche di sicurezza distribuite dal Dipartimento Transizione digitale.

Art. 4 - Uso dei servizi di comunicazione telematica

Città Metropolitana di Milano provvede a dotare tutti i dipendenti di un'utenza per l'accesso ai servizi di posta elettronica ed alla intranet.

L'accesso alla rete Internet deve invece essere richiesto dal direttore al quale l'utente è assegnato. Lo stesso direttore è tenuto a comunicare il trasferimento o la cessazione del rapporto dell'utente con la Città Metropolitana di Milano. Tale comunicazione determina la disabilitazione dai servizi.

L'accesso alla rete Internet è attivato automaticamente ai direttori.

L'accesso ai servizi di comunicazione telematica è revocato su richiesta – *motivata ed inviata per conoscenza al lavoratore, che entro 3 giorni può presentare le sue controdeduzioni al Direttore del Personale* - del direttore di riferimento o in caso di accertate violazioni della legge o del presente disciplinare.

Art 4.1 - Posta elettronica

L'uso della posta elettronica, strumento fondamentale nello svolgimento dell'attività lavorativa, deve essere adottato per quanto possibile in sostituzione delle comunicazioni cartacee per tutte le comunicazioni interne al fine di rendere più efficienti le procedure e realizzare consistenti risparmi di risorse.

L'utilizzo dell'indirizzo di posta elettronica fornito dall'Ente a ciascun dipendente deve essere utilizzato esclusivamente per attività lavorative e non per scopi personali.

Responsabilità

L'uso dell'indirizzo di posta elettronica assegnato dalla Città Metropolitana di Milano comporta la spendita del nome dell'Ente. Il materiale e i contenuti inviati sono diretta responsabilità dell'utente che deve evitare che propri comportamenti in rete possano ledere l'immagine esterna dell'Ente o ne possano comportare la responsabilità.

Occorre inoltre osservare alcune precauzioni per evitare che le mail scambiate arrechino rischi ai servizi informativi della Città Metropolitana o contribuiscano a diffondere informazioni riservate. A tale scopo ogni utente è tenuto ad attenersi alle seguenti norme:

- Controllare con attenzione le mail ricevute: l'ambiente di posta è in grado di identificare ed eliminare i principali virus nascosti negli allegati. Tuttavia, è possibile che qualche virus non venga intercettato ed è compito di ogni utente vigilare e cancellare ogni e-mail con mittenti, link o allegati sospetti specialmente se non se ne conosce la provenienza;
- Effettuare la manutenzione della casella di posta eliminando i messaggi non più attuali e contenenti allegati di grandi dimensioni e archiviando i messaggi di posta dalla casella alla propria postazione di lavoro; ciò eviterà rischi di sovraccarichi che limitano le prestazioni del sistema di posta elettronica;
- In caso di assenze prolungate attivare un messaggio automatico che indichi il periodo di assenza ed eventualmente un altro riferimento al quale inviare i messaggi di lavoro urgenti;
- L'utente evita che, nei messaggi inviati a destinatari esterni all'Ente, siano visibili in chiaro liste di indirizzi mail di utenti della Città Metropolitana di Milano;
- Impostare la firma delle mail, utilizzando format di firma e disclaimer standard definiti dall'Ente;
- Sono vietate pratiche di "spamming", cioè di invio e diffusione di grandi quantità di messaggi indesiderati (messaggi a catena, inserimento di utente e password nei messaggi, ecc.). L'inoltro di messaggi non sollecitati (ad esempio informazioni, avvisi, notizie etc.) deve essere attentamente valutato;
- È vietato l'invio di e-mail con allegati di grosse dimensioni o a un numero elevato di destinatari perché ciò può compromettere il corretto funzionamento del servizio.

Art. 4.2 - Internet

La Città Metropolitana di Milano fornisce accesso alla rete Internet per lo svolgimento dell'attività lavorativa. L'accesso è fornito dal Dipartimento Transizione digitale previa richiesta del direttore di riferimento di ogni utente ed è subordinato all'autenticazione dell'utente presso la rete della Città Metropolitana di Milano.

La navigazione in Internet comporta numerosi rischi che possono minacciare la sicurezza della rete della Città Metropolitana, dei dati e della postazione di lavoro. Per evitare tali rischi, l'accesso ad Internet è filtrato e controllato da adeguati apparati di sicurezza, che si

aggiornano automaticamente con liste di indirizzi di siti considerati pericolosi o non correlati con la prestazione lavorativa.

Modalità di conservazione dei dati

I dati di log del servizio internet, specificati nell'allegato tecnico, sono conservati per ragioni connesse alla gestione del servizio e alla sicurezza del sistema per sei mesi.

Un eventuale prolungamento dei tempi di conservazione è limitato ai seguenti casi:

- Per indispensabilità del dato rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria. In questo caso il Dipartimento Transizione digitale si atterrà alle indicazioni della Direzione Generale;
- Per ottemperare ad una specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria;
- Per eccezionali esigenze tecniche e di sicurezza che il Dipartimento Transizione digitale documenterà indicando nello specifico le ragioni del prolungamento e la sua durata.

Responsabilità

L'uso di internet, sia rispetto alla navigazione che all'utilizzo dei servizi disponibili in rete, rientra nella piena responsabilità dell'utente che, a propria tutela, tiene rigorosamente riservate le sue credenziali di accesso.

Tenendo conto che l'uso di internet è consentito per lo svolgimento della propria attività lavorativa, l'utente è tenuto al rispetto delle seguenti norme di comportamento:

- Per evitare problemi di efficienza e sicurezza della rete, verificare le dimensioni e la provenienza degli eventuali file (immagini, video, documenti etc.) che si intendano scaricare;
- Valutare con attenzione l'opportunità di compilare, fornendo dati personali propri e della Città Metropolitana, form o moduli disponibili in rete;
- Valutare con attenzione l'opportunità di partecipare a forum, aree di dibattito, *virtual community* presenti in rete;
- Valutare con attenzione l'opportunità di effettuare l'upload o comunque la condivisione in rete di materiale di cui si disponga per l'esercizio della propria attività lavorativa.
- Non è consentito scaricare e installare programmi non autorizzati che potrebbero danneggiare il sistema ricevente o carpire informazioni riservate;
- Non è consentito l'accesso e la navigazione se non a mezzo della rete della Città Metropolitana. È pertanto vietato l'utilizzo di modem personali e di Internet provider diversi, salvo i casi autorizzati dal direttore di riferimento;
- Non è consentita l'effettuazione di transazioni finanziarie (remote Banking, acquisti on-line, ecc.), salvo i casi autorizzati dal direttore di riferimento;
- Non è consentito scaricare/scambiare materiale informatico privo di licenza o in violazione del diritto d'autore o altri diritti tutelati dalla normativa vigente;

- È inoltre vietato compiere qualsiasi azione tesa ad aggirare o compromettere i meccanismi di protezione dei sistemi informatici (ad esempio effettuare operazioni non autorizzate di scansione di porte e protocolli dall'interno della rete dell'Ente, falsificare la propria identità, falsificare il contenuto degli *header* dei protocolli di comunicazione, trasmettere software che alteri il normale funzionamento del sistema informatico del destinatario).

Art. 4.3 Wi-Fi

Rete Wi-Fi pubblica

All'interno delle sedi di Città Metropolitana di Milano è disponibile una rete Wi-Fi pubblica per consentire la navigazione internet agli utenti esterni all'Ente (ospiti, cittadini, turisti etc.). Per accedere a tale rete, sarà necessario registrarsi inserendo il proprio numero di cellulare.

Rete Wi-Fi privata

In alcune zone delle sedi principali della Città Metropolitana di Milano è presente una rete WiFi privata destinata agli utenti dell'Amministrazione. Tale rete consente ai dispositivi portatili forniti dall'Ente ed opportunamente configurati dal Dipartimento Transizione digitale, di accedere alle risorse della rete come se fossero connessi via cavo.

Tale rete Wi-Fi è protetta ed è ad uso esclusivo dei dispositivi forniti dall'Ente. Non è pertanto consentito collegare qualsiasi dispositivo, diverso da quelli assegnati, alla rete Wi-Fi dell'Ente.

Art. 4.4 Intranet

Il portale Intranet è un portale web interno alla rete di Città Metropolitana di Milano ed è utilizzato da tutti i dipendenti dell'Ente. Dal portale Intranet è possibile accedere ai software istituzionali e ai link dei principali portali informativi dell'Ente.

Il portale intranet inoltre è utilizzato come bacheca elettronica per le comunicazioni interne ai dipendenti e per la diffusione di informazioni e documenti di interesse generale dell'ente.

Art. 5 – Smartworking

I dipendenti di Città Metropolitana di Milano che usufruiscono dello smart working, devono disporre di una dotazione informatica minima adeguata alle mansioni svolte, che comprende un personal computer e una connessione ad Internet.

Dispositivi di proprietà dell'Ente

Il dipendente potrà essere dotato dall'Amministrazione di un personal computer portatile ed eventualmente di un cellulare, da utilizzarsi nel totale rispetto delle regole determinate dalla regolamentazione e in conformità con le indicazioni che gli saranno fornite, nonché con quanto trattato nell'Allegato tecnico a questo documento.

Gli strumenti di lavoro affidati al dipendente devono essere usati esclusivamente per lo svolgimento dell'attività lavorativa, nel rispetto di quanto previsto dai regolamenti dell'Amministrazione, e non per scopi personali o non connessi all'attività lavorativa. Il dipendente ha l'obbligo di utilizzare e custodire gli strumenti di lavoro affidatigli con la massima cura e diligenza.

I dispositivi mobili di proprietà dell'Amministrazione, utilizzati dai dipendenti per svolgere

attività lavorativa da remoto, sono utilizzati anche durante l'espletamento dell'attività lavorativa presso l'ordinaria sede di servizio.

Dispositivi di proprietà del dipendente

L'utente potrà utilizzare, nel caso in cui non possa disporre di strumentazione fornita dall'Ente, apparecchiature di proprietà per svolgere attività lavorativa in smartworking. L'uso di strumentazione propria dovrà essere autorizzato dal personale del Dipartimento Transizione digitale, che ne valuterà la compatibilità con i sistemi utilizzati dall'Ente e verificherà che dispongano dei requisiti di sicurezza necessari. In questo caso verrà richiesto all'utente, che confermerà di svolgere l'attività con una autodichiarazione, di installare alcuni programmi necessari per accedere ai servizi informatici e di mantenere i sistemi e l'antivirus aggiornati. In particolare, il dipendente deve seguire le Linee Guida fornite dal Dipartimento transizione digitale per installare il software di Remote Desktop, che garantisce il collegamento remoto al dispositivo presente presso l'ordinaria sede di servizio.

Nel caso di utilizzo di sistemi di proprietà del dipendente verrà fornita assistenza solo sulle componenti software che saranno fornite dall'Ente. In particolare, si richiama la necessità di verificare la presenza e il regolare funzionamento del software antivirus e anti-malware installato sul proprio computer.

Per minimizzare il rischio potenziale di danni, il dipendente che si avvale di strumenti propri per effettuare le attività di smartworking, almeno durante l'esercizio di tali attività, deve tenere i comportamenti descritti nel presente disciplinare anche durante l'utilizzo di dispositivi personali.

Norme di utilizzo degli strumenti laptop, desktop e mobili

I dipendenti che usufruiscono dello smartworking devono rispettare le seguenti indicazioni:

- sia che vengano utilizzati dispositivi personali oppure di proprietà dell'Ente, accedere alla rete dell'Ente utilizzando la VPN e nel caso di dispositivi personali è necessario collegarsi tramite Accesso Remoto (Remote Desktop) al computer presente nella propria sede di lavoro e operare come se si fosse davanti allo stesso: il monitor della postazione in sede risulterà disattivato in modalità CTRL-ALT-CANC e non sarà possibile visualizzare l'attività dell'utente;
- nel caso di dispositivi di proprietà del dipendente, creare un account separato per le attività lavorative, le cui credenziali siano note unicamente al dipendente medesimo (è esclusa pertanto la condivisione di tali credenziali con i familiari);
- nel caso di dispositivi forniti dall'Amministrazione, utilizzare solo l'account creato per il dipendente dal Dipartimento Transizione digitale e solo per scopi di lavoro; è vietata la creazione di ulteriori account, se non su specifica e motivata autorizzazione del responsabile della struttura di appartenenza; è altresì vietata la condivisione delle credenziali, anche con i familiari;
- i dati trattati durante l'attività lavorativa devono essere accessibili unicamente al dipendente;
- una volta terminato il servizio, utilizzare le funzioni di gestione degli appunti di Windows per eliminare la cronologia appunti, evitando così di mantenere anche solo

temporaneamente salvate password o dati sensibili;

- configurare la modalità di blocco automatico dell'accesso al sistema dopo un breve periodo di inattività o bloccare manualmente l'accesso al sistema quando il dispositivo non è in uso;
- custodire adeguatamente le credenziali di accesso e non condividerle con terzi;
- effettuare sempre il logout dai servizi Web, programmi e piattaforme di lavoro una volta terminata la sessione lavorativa;
- custodire con le debite cautele i dispositivi in uso;
- utilizzare esclusivamente dispositivi removibili (chiavette usb, hard-disk esterni, ecc.) di cui si conosce la provenienza ed effettuare sempre la scansione di tali dispositivi provenienti dall'esterno;
- utilizzare, sia nel caso di attività lavorativa in sede sia durante lo smart working, la funzione di stampa riservata per evitare di lasciare a lungo nel vassoio della stampante documenti. Utilizzare tale funzione soprattutto nel caso di stampa di documenti contenenti dati sensibili;
- non tentare di aggirare i meccanismi di controllo degli accessi di qualsiasi risorsa informatica protetta;
- comunicare tempestivamente al Dipartimento Transizione digitale qualsiasi incidente da cui potrebbe derivare una violazione di dati personali.

Tutte le indicazioni contenute nel presente Disciplinare (es. gestione della posta elettronica, creazione e conservazione di password etc.), valide per l'attività in presenza, sono da considerarsi valide e applicabili anche nel caso di attività svolta da remoto.

Norme di utilizzo di smartphone e router Wi-Fi

I dispositivi smartphone e router Wi-Fi (con SIM dati) assegnati dall'Amministrazione sono strumenti di lavoro utilizzabili unicamente a tale scopo. Non possono essere ceduti, condivisi con terzi o utilizzati per scopi personali.

Entrambe le tipologie di dispositivo possono essere utilizzate per la connessione ad Internet in mobilità. Il relativo traffico dati può essere consumato solo per finalità connesse con l'attività lavorativa. Il dipendente è responsabile dell'uso corretto e lecito della connessione ad Internet.

Connessione ad Internet

Il dipendente che effettua attività di smartworking potrà utilizzare la propria rete Wi-Fi, e quindi connettere a tale rete i dispositivi forniti dall'Ente, per finalità istituzionali connesse alle attività lavorative svolte e nel rispetto del presente Disciplinare.

Nel caso in cui ci sia necessità di connettersi a rete wireless diverse da quella della propria abitazione si raccomanda, al fine di prevenire l'esposizione a cyber attacchi, di evitare il collegamento a reti non sicure o sulle quali non si siano presenti adeguati sistemi di protezione e sicurezza.

Art. 6 - Monitoraggi e controlli

Al fine di garantire la sicurezza degli strumenti e dei servizi informatici e di comunicazione telematica, per effettuare statistiche e prevenire usi impropri, il Dipartimento Transizione digitale si avvale di sistemi di monitoraggio e controllo, nel rispetto dei principi di pertinenza e non eccedenza.

Il Dipartimento Transizione Digitale imposta la propria azione di monitoraggio e controllo sui sistemi informatici dell'Ente messi a disposizione per lo svolgimento dell'attività lavorativa nel rispetto della normativa vigente e sul presupposto di un utilizzo responsabile degli stessi da parte degli Utenti, adottando in ogni caso le soluzioni tecnologiche idonee a garantire i profili di sicurezza dei sistemi informativi e dei dati gestiti.

Tutte le attività sotto riportate sono svolte nel rispetto dei principi di gradualità, pertinenza e non eccedenza stabiliti dal Garante per la protezione dei dati personali nonché dei diritti e delle libertà fondamentali dei lavoratori, sempre mediante funzionalità consentite dalla normativa vigente.

Postazione di lavoro

Il Dipartimento Transizione digitale verifica che le postazioni di lavoro mantengano lo standard di sicurezza definito. Il riscontro di eventuali anomalie consente al Dipartimento Transizione digitale di adottare tutte le misure necessarie, compreso l'isolamento della postazione di lavoro dalla rete della Città Metropolitana. Nel perdurare di tali anomalie il comportamento verrà segnalato al responsabile della struttura di appartenenza del dipendente e al Direttore del Personale.

L'amministratore di sistema, nel caso in cui rilevi anomalie o configurazioni non corrette delle PdL, può provvedere a isolare immediatamente l'origine dell'anomalia o del malfunzionamento anche senza preavvisare l'Utente, per salvaguardare la sicurezza e l'integrità dei sistemi informativi dell'Ente. In tal caso, verrà data successiva informativa all'Utente sui motivi dell'avvenuto intervento sulla PdL da parte dell'amministratore di sistema. Nel caso l'utilizzo anomalo sia riconducibile ad un utente non dipendente, il comportamento andrà segnalato alla Direzione Generale per l'adozione degli atti di competenza.

Internet

Il Dipartimento Transizione digitale verifica il corretto utilizzo della rete ai fini della sicurezza e l'attività sull'uso della rete Internet.

Su richiesta esplicita dell'utente, per lo svolgimento di attività diagnostica, può essere temporaneamente memorizzato e controllato il contenuto di una pagina consultata. Una volta effettuata la verifica, la pagina viene cancellata.

Il Dipartimento utilizza sistemi automatizzati per la gestione centralizzata dei cosiddetti "file di log", che consentono di tracciare eventuali anomalie o minacce informatiche che potrebbero colpire i sistemi, compromettendo la funzionalità e la sicurezza degli apparati informatici dell'Ente e delle informazioni ivi contenute.

I file di log relativi alla navigazione in Internet sono registrati e conservati per le suddette finalità di funzionalità e sicurezza, in conformità alla normativa vigente. Nel caso di eventi anomali e/o pregiudizievoli per la sicurezza informatica, i file di log relativi alla navigazione possono essere

esaminati dagli amministratori di sistema per l'individuazione del problema tecnico e l'adozione delle necessarie misure conseguenziali. In ogni caso, tutti i controlli di funzionalità e monitoraggio avvengono nel rispetto di quanto previsto dal CAD, dalle norme in materia di tutela della libertà e dignità dei lavoratori, della normativa unionale e nazionale in materia di protezione dei dati personali.

La conservazione dei log di navigazione Internet è di sei mesi.

I controlli vengono effettuati su dati aggregati anche relativi a singole direzioni o settori. Qualora il controllo anonimo rilevi un utilizzo anomalo degli strumenti informatici, il Dipartimento Transizione digitale effettuerà un avviso generalizzato inerente all'utilizzo anomalo rilevato, con l'invito ad attenersi scrupolosamente alle istruzioni impartite. Nel perdurare delle anomalie si procederà a controlli su base individuale o per postazioni di lavoro segnalando il comportamento al responsabile della struttura di appartenenza del dipendente e al Direttore del Personale il quale, se necessario, attiverà il procedimento disciplinare nelle forme e con le modalità previste dal C.C.N.L.

Nel caso l'utilizzo anomalo sia riconducibile ad un utente non dipendente, il comportamento andrà segnalato alla Direzione Generale per l'adozione degli atti di competenza.

Posta elettronica

I contenuti dei messaggi di posta elettronica, compresi i file allegati, sono riservati. L'accesso ai messaggi e ai file allegati è ammesso solo per eccezionali e documentati problemi di sicurezza del sistema su richiesta dell'utente o previa comunicazione all'utente stesso.

Il Dipartimento Transizione digitale utilizza strumenti di tracking e monitoraggio che consentono di rilevare minacce per la sicurezza dell'Ente e analizzare il flusso di traffico o di carico dei sistemi di posta elettronica.

Tali strumenti hanno l'esclusiva finalità di garantire la piena funzionalità, la sicurezza e l'efficienza del sistema di posta e sono utilizzati esclusivamente da personale autorizzato del Dipartimento.

Art. 7 - Modifica o cessazione del rapporto di lavoro

Di norma l'assegnazione della strumentazione che costituisce la postazione di lavoro non decade in caso di spostamento ad altro settore dell'Ente.

In caso di cessazione del rapporto di lavoro con l'Ente o pensionamento, prima della restituzione della postazione di lavoro si è tenuti a:

- comunicare tutte le informazioni relative all'ubicazione nei sistemi centralizzati di tutti i dati concernenti l'attività lavorativa al proprio responsabile o al soggetto che, in accordo alla normativa, è deputato a trattarli, cancellando le eventuali copie presenti nella postazione stessa;
- cancellare eventuali altri dati personali propri o di terzi e non personali che dovessero risultare ancora presenti.

In assenza di richieste specifiche, il Dipartimento provvederà al ritiro della postazione di lavoro e alla formattazione/cancellazione dei dati presenti per procedere alla riassegnazione.

In caso di decesso, è possibile da parte degli eredi inoltrare richiesta di copia delle comunicazioni email al Dipartimento Transizione digitale al fine di raccogliere eventuale documentazione personale ancora presente sui dispositivi di proprietà dell'Ente.

In tutti i casi in cui si verifichi un trasferimento interno alla struttura o cessazione del rapporto con l'Ente, il Dipartimento Risorse Umane e Organizzazione, lo comunica formalmente al Dipartimento Transizione digitale secondo le modalità stabilite.

Il Dipartimento Transizione digitale procede, quindi, secondo le seguenti modalità:

- nel caso di assegnazione ad altro Settore verranno disattivate tutte le abilitazioni dell'utente relative ai servizi utilizzati dal Settore di provenienza, comprese quelle relative ai portali e alle banche dati esterne. Resteranno valide le abilitazioni ai "servizi orizzontali" (es. utente di dominio e posta elettronica). Nel caso di assegnazione ad altro settore sarà competenza e responsabilità del Dirigente, di una P.O. o del Responsabile di Settore di procedere alla richiesta delle specifiche abilitazioni necessarie per lo svolgimento dell'attività lavorativa ovvero per gli ulteriori "servizi orizzontali" (es. navigazione internet, cloud, ecc.) e i necessari "servizi verticali" (es. protocollo, gestione atti, finanziaria, risorse condivise ecc.);
- nel caso di cessazione del rapporto tutti gli account relativi all'utente verranno disabilitati e/o eliminati.

Resta in capo al Responsabile del proprio Settore di ogni cartella di rete o risorsa condivisa, a cui l'utente per il quale è sopraggiunta la modifica o la cessazione del rapporto è abilitato, richiedere la modifica o eliminazione dei permessi di accesso.

Allegato tecnico

Standard di sicurezza e principali misure di protezione

Dotazione informatica

Gli strumenti forniti sono di proprietà dell'Ente e devono essere utilizzati esclusivamente per svolgere la propria attività lavorativa.

Il computer assegnato contiene tutti i software necessari a svolgere le attività. Per evitare rischi di sicurezza o danni accidentali non è consentita l'installazione di programmi o la modifica di configurazioni (software e hardware) che non siano state preventivamente richieste e autorizzate dal Dipartimento transizione digitale.

Per evitare problemi durante la migrazione dei dati, utilizzare esclusivamente la cartella "Documenti", da sincronizzare in OneDrive laddove possibile, per salvare e organizzare i file in sottocartelle, evitare d'immagazzinare documenti personali come foto/video/musica ed effettuare pulizie periodiche eliminando file non più necessari.

Aggiornamenti e patch di sicurezza

Una delle principali cause che rendono i sistemi informatici vulnerabili agli attacchi è la mancanza di aggiornamenti che correggono importanti falle di sicurezza.

Le Postazioni di Lavoro prevedono un sistema centralizzato e automatico per la distribuzione degli aggiornamenti del sistema operativo e dei software installati.

Gli aggiornamenti del sistema operativo sono distribuiti mensilmente tramite Windows Update:

- sui **pc portatili** l'installazione è programmata in settimana in pausa pranzo. L'utente è tenuto a riavviare il pc per completare l'aggiornamento dopo che appare la notifica di riavvio, oppure scegliere "Aggiorna e arresta" al termine dell'attività lavorativa (attenzione che in quest'ultimo caso il pc impiegherà un po' più tempo a spegnersi).
- sui **pc fissi** gli aggiornamenti sono programmati nel fine settimana, in modo completamente automatico. Per i pc spenti in tale orario l'utente è tenuto ad avviare manualmente l'installazione cliccando sulla notifica che indica la disponibilità di aggiornamenti e a riavviare poi il pc per completare l'aggiornamento una volta che appare la notifica di riavvio.

Interventi di assistenza

Ogni malfunzionamento hardware o software della dotazione informatica assegnata deve essere segnalato al servizio di Helpdesk attraverso il sistema di ticketing e l'indicazione dettagliata del problema riscontrato, attraverso l'apertura di un ticket all'indirizzo: https://assistenza.cittametropolitana.mi.it

Gli interventi di assistenza possono richiedere l'accesso da remoto alla postazione di lavoro. Tale accesso può avvenire unicamente con il consenso dell'assegnatario che sta utilizzando la postazione.

Password

Indicazioni per creare una password più sicura

- Utilizzare **minimo 8 caratteri**
- Utilizzare almeno una lettera **maiuscola**, un **numero** e un **carattere speciale** ($!@&?.-#)
- Più la password è **lunga** e **complessa**, più è sicura.
- Evitare l'uso di **parole ovvie e banali** o **facilmente indovinabili** (es. il proprio nome)
- Evitare l'uso d'**informazioni personali** facilmente rintracciabili (data di nascita, nomi dei figli, nome dell'animale domestico, etc.)
- Sostituire alcune lettere di una parola con numeri o caratteri speciali graficamente riconducibili alla lettera sostituita (ad esempio la "**a**" con "**4**" o "**@**", la "**e**" con "**3**" o "**&**", la "**s**" con "**5**" o "**$**", la "**i**" con "**1**" o "**!**", la "**o**" con "**0**", etc.)

  Es. CittàMetropolitana ► *C1tt4M3tr0p0l!t4n@*
- Usare una frase facile da ricordare (come un motto, un titolo di una canzone, etc.)

  Es. LavoroInCittàMetropolitanaDiMilano
- Oppure usare in alternativa solo le iniziali della frase, seguita da numeri e caratteri speciali, in modo da avere una password non troppo lunga, ma comunque sicura perché non forma una parola di senso compiuto

  Es. Licmdm97!

Indicazioni per gestire al meglio la propria password

- **Non condividere** mai la propria password per e-mail.
- Negare eventuali richieste di **salvataggio password** dell'utenza di Città Metropolitana (ad esempio nel browser).
- Non inserirla mai in portali che non siano quelli **ufficiali** dell'ente o tramite collegamenti contenuti in mail di dubbia provenienza (phishing).
- **Non riutilizzare** la password dell'utenza di Città Metropolitana per altri servizi e portali (es. corsi online, servizi di storage, etc.), o per account privati (es. posta personale, banca, etc.); usare sempre **password diverse** per **utenze diverse**.
- Effettuare sempre il **logout** da servizi e portali dopo aver concluso l'attività.
- **Bloccare** sempre il pc quando ci si allontana dalla postazione (CTRL+ALT+CANC ► Blocca)
- **Non scrivere** mai la propria password su foglietti, agende o in file sul pc.
- Per ricordarsi le varie password si può ricorrere a un **gestore delle password** gratuito come **KeePass**, che permette di salvare e categorizzare le proprie password tramite una sola password di accesso.
- Registrarsi sul portale **Cambio Password** per poter facilmente cambiare la propria password in caso di scadenza o dimenticanza, seguendo la semplice guida passo per passo sul portale E-learning.

Posta elettronica

Controlli automatici sullo spam

Il servizio di posta elettronica prevede specifiche misure di protezione, che, attraverso l'analisi automatica del contenuto della e-mail, identificano e-mail malevole (che contengono virus o altre tipologie di minacce). Le e-mail riconosciute dal sistema di posta come pericolose vengono automaticamente spostate nella casella "Posta indesiderata" dell'utente o vengono bloccate prima dell'ingresso in casella.

Qualsiasi sistema di posta non è però in grado di riconoscere tutte le e-mail malevole che, talvolta, vengono recapitate all'utente.

È fondamentale che ogni utente controlli con attenzione le e-mail ricevute, esaminando il mittente e allertandosi nel caso una e-mail abbia contenuti dubbi e chiedendo eventualmente supporto all'assistenza informatica.

Di seguito alcuni elementi che caratterizzano mail malevole:

1. Il mittente è un indirizzo di posta elettronica pubblico

Guardare l'indirizzo del mittente aiuta a capire se la persona che ha inviato l'e-mail è veramente colei che afferma di essere. Spesso, i criminali informatici usano un indirizzo di posta elettronica pubblico, come @gmail.com. Se si hanno dubbi sulla veridicità del messaggio, prima di aprire la e-mail o cliccare su qualsiasi link in essa contenuto, è meglio contattare direttamente il destinatario e chiedere informazioni sulla e-mail ricevuta.

2. Allegati o link sospetti

In caso di e-mail inaspettate o derivanti da qualcuno di non conosciuto, in cui si è invitati ad aprire e/o scaricare allegati o a cliccare su link apparentemente non sicuri, non aprire e/o scaricare mai l'allegato né cliccare sul link sospetto. Questo potrebbe contenere malware che infetteranno il computer, o peggio ancora, ransomware che bloccheranno il computer e i dati, prendendoli in ostaggio.

Nel caso in cui siano stati aperti/scaricati allegati o sia stato cliccato un link non sicuro, il dipendente dovrà seguire i seguenti passaggi:

- scollegare immediatamente il dispositivo da Internet e da qualsiasi altra rete interna, scollegando sia Wi-Fi che i cavi Ethernet utilizzati per una connessione di rete interna o esterna;
- avvisare il servizio di Helpdesk per richiedere un controllo accurato del dispositivo;
- effettuare tempestivamente una scansione antivirus e ripetere tale procedura anche qualche giorno dopo;
- eliminare il messaggio e qualsiasi eventuale copia scaricata dell'allegato;
- modificare le credenziali di accesso degli account salvati sul dispositivo;
- cancellare tutti i dati del browser, inclusi cookie e cronologia.

Inoltre, il dipendente dovrà contattare il Dipartimento Transizione digitale, e nello specifico il DPO dell'Ente, per ricevere supporto nella gestione delle situazioni di possibili compromissioni del proprio computer. Nello specifico, il dipendente dovrà:

- comunicare al Direttore del Dipartimento Transizione Digitale la situazione di compromissione del proprio computer;
- se ritenuto necessario, procedere con la denuncia alle Autorità;
- valutare, insieme al Dipartimento Transizione digitale e DPO, se inoltrare una comunicazione ufficiale anche al Garante per la protezione dei dati personali.

3. Senso di urgenza

Le e-mail di phishing spesso creano un falso senso di urgenza e pericolo che spinge l'ignara vittima a seguire le indicazioni contenute nel messaggio. Controllare attentamente la veridicità del messaggio prima di cliccare sui link invitati che, in caso di e-mail di phishing, non rimandano al sito autentico, ma ad uno creato ad-hoc per la truffa.

4. Errori di ortografia in un dominio conosciuto

Senza cliccare, passare il mouse sopra il link per visualizzare il vero URL nascosto. Spesso, le truffe replicano siti web famosi in tutto e per tutto. Non potendo però duplicare il dominio, cercano di crearne uno il più simile possibile all'originale: se si riceve una e-mail che invita a cliccare un link che cita siti web famosi (es. amazon.it o intessasanpaolo.it), probabilmente l'e-mail ricevuta è fraudolenta; pertanto, si invita a non cliccare sul link contenuto nell'e-mail.

5. Messaggio sgrammaticato

Spesso è possibile capire che si tratta di una e-mail di phishing dal modo in cui è scritto il messaggio. Lo stile potrebbe essere diverso da quello che ci si aspetta di solito dal mittente, oppure il messaggio potrebbe contenere errori grammaticali e ortografici.

Limiti di spazio delle caselle

Ogni provider di posta definisce un limite massimo di spazio per casella di posta. Lo spazio è vincolante e non può essere incrementato. Per questo motivo ogni utente deve provvedere alla cancellazione di mail non necessarie per non portare la casella a saturazione.

Template di firme e disclaimer

Per garantire la coerenza della comunicazione, i dipendenti sono tenuti ad utilizzare un template per le firme e i disclaimer inseriti nei messaggi di posta elettronica. In particolare, il template della firma deve contenere, nell'ordine riportato, le seguenti informazioni:

- Nome e Cognome
- Ruolo all'interno dell'Ente
- Nome dell'Ente [Città Metropolitana di Milano]
- Dipartimento/Settore/Area
- Indirizzo [Via/Viale …, numero civico (Milano)]
- Numero di telefono

La firma dovrà essere impostata secondo le direttive definite dall'Ente.

Sistema Antivirus

Tutte le postazioni di lavoro che hanno accesso alla rete (dominio “provmi”) sono dotate di sistema antivirus per il rilevamento, segnalazione, blocco e rimozione di virus, worm, Trojan, malware e altre applicazioni pericolose o indesiderate.

La distribuzione degli aggiornamenti avviene quotidianamente ed è gestita centralmente da un server.

Una consolle centralizzata permette di monitorare tutte le attività di aggiornamento in atto e verificarne il completamento e raccoglie le segnalazioni di infezione permettendo di identificare particolari tendenze di crescita ed intervenire eventualmente in maniera remota su interi rami di rete.

Ogni utente deve comunque tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico dell’Ente, evitando di compiere navigazione su siti non sicuri, download di software e file non autorizzati, etc.

Crittografia dei dati

Così come descritto all’Art. 3 del presente disciplinare, sarà necessario crittografare i dati estremamente sensibili utilizzando gli strumenti di criptazione in uso presso l’Ente. In particolare, i dipendenti potranno utilizzare la funzionalità “Cifra” di GoSign Desktop per proteggere i dati con una password di accesso, scegliendo tra diverse tipologie di “chiavi” per criptare il documento contenente i dati sensibili.

Internet

Filtri

L’accesso ad Internet è regolamentato da un sistema di controllo delle pagine web visitate che permette di bloccare l’accesso a siti Web e ai file potenzialmente pericolosi e specificati mediante appositi filtri.

Accertarsi comunque sempre dell’affidabilità di qualsiasi sito prima di visitarlo e della genuinità di qualsiasi file prima di eseguirlo.

Registrazione dei dati

I sistemi di controllo e filtraggio dei siti navigati, registrano le seguenti informazioni (Log) che possono essere utilizzate dal personale IT per attività di monitoraggio:

- Nome account dell’utente
- Indirizzo IP della stazione di lavoro
- URL richiesta
- Indirizzo IP del server remoto
- Quantità dei dati trasferiti

Browser

La Città metropolitana, al fine di non avere vincoli tecnologici, promuove lo sviluppo e l'acquisto di prodotti applicativi multi browser. A seguito dell'adozione di M365 da parte dell'Ente, Il browser che si consiglia di utilizzare è Microsoft Edge che, oltre ad essere un browser moderno e sicuro con aggiornamenti automatici regolari, contiene nei preferiti una cartella "Città Metropolitana" con i siti più utili dell'Ente.

Edge permette l'uso di applicativi progettati per Internet Explorer, residuali presso l'Ente, grazie alla modalità di compatibilità già configurata.

Utilizzo delle condivisioni di rete

L'utente può accedere alle cartelle di rete del proprio settore di appartenenza, per le quali ha ricevuto le opportune **autorizzazioni**.

La **richiesta** di accesso a cartelle già esistenti o la creazione di nuove avviene tramite un **modulo** di richiesta presente sulla Intranet, firmato digitalmente dal proprio responsabile.

Tutte le cartelle di rete servono per immagazzinare esclusivamente documenti inerenti l'attività **lavorativa** in condivisione con i colleghi; pertanto, non è consentito il salvataggio di documenti personali come foto/video/musica.

Ogni cartella ha uno **spazio limitato**: è quindi importante porre attenzione all'uso dello spazio, evitando sprechi e organizzando una manutenzione periodica, eliminando dati duplicati o non più necessari.

Tutte le cartelle di rete sono soggette a salvataggi giornalieri.

Nominare file e cartelle

Non creare file e cartelle con nomi **troppo lunghi** o con caratteri particolari, per evitare poi problemi nella gestione dei percorsi e nella compatibilità tra i vari sistemi e applicazioni.

Usare piuttosto nomi **corti e semplificati**, usare eventuali parole solo in forma abbreviata, evitare articoli, preposizioni, accenti, apostrofi e spazi, utilizzare il trattino "-" o il trattino basso "_" per distanziare le parole.

Utilizzo dei portatili

Il portatile assegnato è di proprietà dell'Ente e fa parte della dotazione informatica messa a disposizione esclusivamente per l'attività lavorativa, nel rispetto delle seguenti regole e nel divieto di utilizzo per scopi personali non connessi all'attività lavorativa.

Un portatile va maneggiato con cura poiché è molto più delicato di una postazione fissa e necessita di maggiore attenzione nel suo utilizzo quotidiano.

I danni causati da incuria non sono coperti dalla garanzia del fornitore e gli interventi fuori garanzia danno luogo ad addebiti extra, a carico di chi ha causato il danno.

Per evitare che si verifichino la maggior parte dei guasti e/o incidenti occorre seguire alcune semplici regole:

Prevenire i possibili incidenti

- Evitare di mangiare o bere mentre si lavora al computer per evitare danni irreversibili (ad esempio nel rovesciare bevande sul pc);
- Usare il portatile solo in condizioni sicure, al riparo da luce del sole e altri fonti di calore, liquidi, polveri e altro materiale dannoso;
- Posizionare il computer in punti non raggiungibili dai bambini o dagli animali domestici;
- Evitare di appoggiare oggetti sopra il portatile: la pressione eccessiva sullo schermo LCD e sulla tastiera potrebbe danneggiarli;
- Impugnare e sollevare il computer solo dalla base, non afferrandolo dallo schermo per evitare di danneggiare il display o i connettori che lo collegano alla scheda madre inserita nella base del portatile;
- Prima di richiudere lo schermo del portatile assicurarsi sempre che non ci sia nulla tra la tastiera e lo schermo;
- Non smontare per nessun motivo il coperchio posteriore del portatile, per non invalidare la garanzia e per evitare danni accidentali alle parti interne.

Custodia

- Quando non in uso, il PC dev'essere custodito in luogo sicuro, adottando tutte le opportune precauzioni contro furti e danneggiamenti accidentali;
- Durante il trasporto, utilizzare la custodia assegnata assicurandosi che non vi siano all'interno alimenti o sostanze che possano danneggiarlo;
- Posizionare il portatile nel vano interno della borsa, isolandolo da altri materiali;
- Prestare attenzione agli urti durante il trasporto o lo spostamento;
- Non lasciare il pc in sospensione per lungo tempo, piuttosto usare l'ibernazione o meglio ancora spegnerlo quando in custodia;
- Quando è spento, non lasciare l'alimentatore collegato se la batteria è già carica al 100%.

Usare il portatile in condizioni ideali

- Assicurarsi di avere le mani pulite prima di usare il portatile;
- Posizionare il portatile su una superficie piana, pulita e priva di polvere;
- Usare il portatile in una posizione areata in modo tale che ci sia spazio attorno al dispositivo per favorirne l'aerazione e prevenirne il surriscaldamento;
- Non appoggiare fogli di carta o altro materiale sul portatile acceso che ne impedirebbe la dissipazione del calore.

Pulizia

- Spegnere il computer e scollegarlo dall'alimentazione elettrica prima di procedere alla pulizia;
- Mantenere pulito il portatile rimuovendo i residui di polvere e sporcizia con un panno in microfibra;

- Per non danneggiarlo, pulire lo schermo delicatamente senza fare troppa pressione;
- Non spruzzare mai dell'acqua o altre soluzioni detergenti direttamente sul portatile e sullo schermo, ma su un panno morbido;
- Non utilizzare fazzoletti o simili tipi di carta per non graffiare le superfici lucide;
- Non applicare adesivi, calamite o altre "personalizzazioni "sul telaio del portatile.

Collegamento delle periferiche (chiavette usb, cuffie, adattatori di rete e cavo di alimentazione)

- Prestare attenzione all'inserimento di prese USB e di rete: gli ingressi sono molto delicati e vanno maneggiati con cura;
- Fare attenzione alle dimensioni e alla forma dei relativi connettori prima di stabilire il collegamento in modo da individuare la porta corretta;
- Non forzare l'inserimento della periferica: se si sente resistenza nell'inserimento controllare bene e non forzare.

Non abbandonare il portatile in macchina

- Le alte temperature raggiunte nell'abitacolo dell'auto potrebbero causare danni molto gravi;
- Inoltre, rappresenterebbe un invitante obiettivo per malintenzionati di passaggio.

In caso di qualsiasi problema hardware o software, si è pregati di darne comunicazione al servizio competente o all'assistenza tecnica di Città Metropolitana.

Utilizzo dei dispositivi di telefonia mobile e smartphone

I dispositivi di telefonia mobile o smartphone e relativa SIM sono di proprietà dell'Ente e fanno parte della dotazione informatica messa a disposizione esclusivamente per l'attività lavorativa, nel rispetto delle seguenti regole.

Il dipendente assegnatario di tali dispositivi è responsabile di tenere con cura il dispositivo e di intraprendere ogni azione in suo potere per impedire deterioramenti o danneggiamenti dello stesso.

I dispositivi mobili assegnati non possono essere ceduti a terzi a nessun titolo.

Tutte le attività non espressamente previste nei relativi contratti di fornitura di beni e servizi (es. aggiornamento software, backup, ripresa dati, configurazioni varie ecc.) sono a carico e sotto la responsabilità dell'assegnatario.

Gli assegnatari possono utilizzare il telefono di servizio per telefonate personali solo avvalendosi della fatturazione separata a proprio carico delle telefonate private (Dual billing) da parte dell'operatore di telefonia mobile. Il servizio Dual billing è attivabile mediante la sottoscrizione di un apposito contratto contenente i dati necessari per la fatturazione delle telefonate private.

L'assegnazione, la consegna iniziale e la restituzione, in caso di modifica o cessazione del rapporto con l'amministrazione, dei dispositivi avverrà secondo le modalità stabilita dal Dipartimento Transizione Digitale.

Utilizzo della firma digitale

La firma digitale è il risultato di una procedura informatica che, applicata a un documento elettronico, ne garantisce l'autenticità. La firma digitale è l'equivalente elettronico della firma autografa su carta e ha valore legale in quanto è strettamente legata al suo titolare.

Città Metropolitana di Milano ha acquistato un numero considerevole di firme digitali InfoCert con l'obiettivo di distribuirle a tutti i dipendenti dell'Ente.

Il Dipartimento Transizione digitale gestisce il registro delle firme digitali concesse e provvede al rinnovo di quelle in scadenza ove ne sussistano le condizioni. Il Dipartimento, a seguito di comunicazione dell'organo competente, provvede alla revoca della firma nei casi previsti dalla legge o qualora non sussistano più i presupposti di fatto e di diritto che ne hanno determinato il rilascio.

La firma digitale è utilizzata per la sottoscrizione di documenti nel rispetto dei poteri di firma derivanti dalla legge o dai regolamenti interni dell'Amministrazione.

Per procedere con la firma digitale, il dipendente deve scaricare uno dei software messo a disposizione dai distributori di firme digitali certificati AgID (es. Go Sign Desktop) attraverso cui confermare la propria identità, utilizzando il codice OTP ricevuto tramite SMS o notifica tramite app. Al termine del processo, si suggerisce di controllare puntualmente che la firma sia stata correttamente apposta attraverso l'utilizzo della componente "Verifica" disponibile sul software scaricato.

In futuro, si prevede di dismettere l'utilizzo di app/software specifici, per utilizzare invece le versioni web di tali strumenti.

Identità digitale

L'identità digitale è oggi necessaria per accedere a moltissimi servizi online. I dipendenti di Città Metropolitana devono rispettare alcune indicazioni di utilizzo dell'identità digitale al fine di non ledere all'immagine dell'Ente, soprattutto nel caso in cui accedano ai servizi digitali con delega ad operare per conto dell'Amministrazione.

Tale delega, rilasciata dall'Amministrazione, prova infatti l'appartenenza del dipendente all'Ente Città Metropolitana. Pertanto, l'accesso ai servizi digitali con delega ad operare per conto di Città Metropolitana di Milano deve essere effettuato soltanto per scopi correlati all'attività lavorativa.

Nel caso in cui un dipendente non sia stato precedentemente delegato ad operare per conto dell'Ente, ma si trova comunque ad accedere a servizi digitali che permettono al dipendente di raccoglie dati e informazioni inerenti all'attività lavorativa, questo è tenuto ad utilizzare tali informazioni soltanto nell'ambito dell'attività professionale, senza divulgare informazioni sensibili.

Social media policy

Sulla base delle Linee Guida del Vademecum "Pubblica Amministrazione e Social Media" realizzato dal Formez, sono qui definite le principali regole e le modalità di gestione dei profili dell'Ente sui social media (LinkedIn, Facebook, Instagram, X, YouTube).

Utilizzo degli account istituzionali dell'Ente

Se il dipendente accede ai social network dell'Ente con un account istituzionale, egli agisce in nome e per conto dell'Ente, pertanto dovrà utilizzare un linguaggio consono e in nessun modo pubblicare contenuti che possano ledere l'immagine dell'Ente.

Abilitato a gestire i vari social network è l'Ufficio Stampa. In particolare, l'Ufficio Stampa si occupa del monitoraggio, dell'aggiornamento e del corretto funzionamento del social network.

Ogni argomento ed il contenuto delle varie tematiche che si vuole pubblicare su un profilo social istituzionale deve essere, a seconda della complessità, discusso e condiviso con il vertice politico-istituzionale di riferimento, il relativo dirigente per competenza e il dirigente dell'Ufficio Stampa. Nel caso in cui il contenuto da pubblicare fosse inerente a richieste derivanti dagli utenti tramite commenti, le risposte devono essere preventivamente verificate con gli uffici di competenza, se necessitano di integrazioni con contenuti tecnici.

Il linguaggio da usare sui social network deve essere semplice e diretto, non confidenziale né burocratico, valorizzando, per tipologia di contenuti e stili comunicativi, le potenzialità del canale e del mezzo utilizzato (ad esempio audio video, visual, etc.). Inoltre, il dipendente che pubblica contenuti sui profili social istituzionali deve sempre mantenere un tono adeguato al contesto di comunicazione pubblica e istituzionale dell'Ente verso il cittadino.

I dipendenti possono utilizzare gli account istituzionali dell'Ente per:

- comunicare attività istituzionali;
- promuovere iniziative di vario genere (progetti, informazioni sui bandi, servizi, eventi e messaggi di pubblica utilità…). Si precisa che Si precisa che la pubblicazione di atti o avvisi pubblici sui profili social ha validità di pubblicità-notizia e non di pubblicità legale.
- rilanciare e condividere contenuti e messaggi di pubblico interesse ed utilità provenienti da terzi, enti pubblici, associazioni e gruppi presenti nel territorio.

I dipendenti non possono utilizzare i profili social istituzionali per finalità politiche di parte, per scopi personali e commerciali.

Utilizzo degli account personali

Anche nel caso in cui il dipendente acceda ai social network con account personali, egli è sempre considerato un dipendente pubblico anche fuori dal luogo e dall'orario di lavoro. Pertanto, anche in questo caso, il suo comportamento deve essere decoroso, dignitoso e improntato alla correttezza verso l'Amministrazione.

Ai dipendenti è severamente vietato trattare sui social media argomenti di lavoro o condividere informazioni riservate relative all'Amministrazione, nonché pubblicare contenuti che possano ledere l'immagine dell'Ente. È però consentito condividere liberamente sui propri profili privati i contenuti diffusi dai canali social della Città Metropolitana.

I dipendenti non possono trasmettere e/o diffondere messaggi minatori ovvero ingiuriosi, commenti e dichiarazioni pubbliche offensive nei confronti dell'Amministrazione, riferiti alle attività istituzionali dell'Ente e, più in generale, al suo operato, che per le forme e i contenuti possano comunque nuocere all'Amministrazione, ledendone l'immagine o il prestigio o compromettendone l'efficienza.

Ad eccezione di eventi pubblici che si svolgono presso la sede di lavoro i dipendenti non possono divulgare foto, video o altro materiale multimediale, che riprenda locali e personale dell'Ente senza l'esplicita autorizzazione delle strutture e delle persone coinvolte.

I dipendenti non possono aprire canali social a nome della Città Metropolitana di Milano o che trattino argomenti riferiti all'attività istituzionale dell'Ente, senza preventiva autorizzazione.

L'utilizzo improprio dei social network dell'Amministrazione e la diffusione di notizie e comunicazioni varie inerenti all'attività lavorativa, costituisce violazione del Codice di Comportamento nazionale e della Città Metropolitana e determina l'applicazione delle sanzioni disciplinari previste dalla normativa vigente e dal Contratto collettivo nazionale e decentrato di Lavoro.

Microsoft Office 365

Dal 2023, Città Metropolitana di Milano fornisce ai propri dipendenti gli strumenti di Microsoft Office 365 per lo svolgimento delle loro attività lavorative. Gli strumenti di Microsoft Office 365 rappresentano oggi gli strumenti ufficiali utilizzati dall'Amministrazione.

L'Ente fornisce licenze che permettono l'utilizzo degli strumenti di Microsoft 365 anche in locale. I dipendenti che non dispongono di tali licenze sono tenuti ad accedervi tramite web utilizzando il proprio account Microsoft.

Tutti gli strumenti devono essere utilizzati nel rispetto delle indicazioni contenute in questo Disciplinare e soltanto ai fini delle attività lavorative.

Microsoft Teams

Messaggistica istantanea

Il dipendente può utilizzare le chat di **messaggistica istantanea** di Microsoft Teams per comunicare sia con i colleghi dell'Amministrazione sia con utenti esterni all'Ente tramite chat disponibile per le videoconferenze.

La messaggistica istantanea è consigliata per comunicazioni brevi e immediate inerenti all'attività lavorativa che richiedono risposte rapide. Si consiglia infatti di non utilizzare questo strumento per discutere di temi personali. La messaggistica istantanea non è adatta per discussioni complesse o per condividere qualsiasi comunicazione che richiede una validazione ufficiale o la condivisione di informazioni e/o documenti altamente riservate o sensibili, che vanno invece trasmessi tramite canali ufficiali e che garantiscano il rispetto delle norme GDPR.

Videoconferenze

Il dipendente utilizza Microsoft Teams anche per organizzare videoconferenze sia con gli altri dipendenti dell'Ente, sia con utenti esterni all'Amministrazione. I sistemi di videoconferenza sono strumenti di lavoro da utilizzare in alternativa a riunioni in presenza o come alternativa alla chiamata telefonica.

Sono riportati di seguito alcuni accorgimenti per la buona riuscita di una videoconferenza:

- Assicurarsi che la connessione internet sia stabile. Utilizzare cuffie con microfono per migliorare la qualità dell'audio e ridurre il rumore di fondo;

- Spegnere il proprio microfono quando non utilizzato per evitare di introdurre rumori, brusii o interferenze e utilizzare la funzione "alzare la mano" di Teams per segnalare la volontà di intervenire;
- Verificare che la webcam sia posizionata correttamente per catturare un'immagine chiara e centrata del viso e assicurarsi che l'illuminazione sia adeguata, preferibilmente con luce frontale;
- Nel caso ci si connetta dalla propria abitazione è bene utilizzare uno sfondo neutro o le funzioni di sfondo sfocato o sfondi virtuali di Teams nel caso in cui non si disponga di una zona riservata e per minimizzare le distrazioni visive;
- Nel caso in cui non si disponga di banda sufficiente a garantire un adeguato segnale audio-video è conveniente spegnere la videocamera;
- Condividere lo schermo solo quando necessario e chiudere tutte le altre applicazioni o schede che non sono pertinenti alla riunione per evitare condivisioni accidentali;
- Qualora sia necessario registrare la videoconferenza, informare i partecipanti e ottenere il loro consenso prima di registrare qualsiasi sessione al fine di rispettare la privacy e la conformità alle normative vigenti;
- Scollegarsi sempre al termine della videoconferenza, soprattutto se si utilizzano stanze virtuali condivide che potrebbero essere utilizzate successivamente per altre riunioni.

Outlook

Per accedere ad Outlook Web, il dipendente deve collegarsi al sito Outlook.com ed effettuare l'accesso al proprio account Microsoft. Tramite Outlook web, il dipendente dell'Ente avrà accesso alla propria casella di posta elettronica, nonché al riquadro di navigazione con il calendario, i contatti e le attività.

Per un utilizzo corretto e sicuro di Outlook web il dipendente è tenuto a rispettare tutte le indicazioni inerenti alla posta elettronica riportate in questo Disciplinare.

OneDrive

OneDrive è utilizzato dai dipendenti come soluzione di archiviazione cloud dei propri file inerenti l'attività lavorativa. Il dipendente è infatti tenuto a salvare i propri file su OneDrive e non in locale sui propri dispositivi così da evitare perdite di dati e documenti.

In particolare, tale strumento viene utilizzato per effettuare backup periodici, così come indicato all'Art. 3 del presente disciplinare.

È vietato al dipendente l'utilizzo di OneDrive per salvare documentazione di carattere personale.

Integrazione tra OneDrive e SharePoint

Per permettere la collaborazione sui file all'interno dell'Ente, il Dipartimento Transizione digitale sta valutando la possibilità di integrare lo strumento di OneDrive con quello di SharePoint, utilizzato come piattaforma per siti di team collaborativi e intranet dell'Ente dove i documenti e i file sono destinati alla condivisione e alla collaborazione di gruppo.

I file memorizzati in SharePoint potranno essere sincronizzati sul computer locale di un utente tramite il client di sincronizzazione di OneDrive. Questo permetterà agli utenti di lavorare offline sui file e poi sincronizzarli automaticamente con SharePoint.

I file creati o modificati in OneDrive potranno essere automaticamente trasferiti o sincronizzati con SharePoint per iniziare processi di workflow, come approvazioni o revisioni, che sono configurati su SharePoint.

Le impostazioni di sicurezza e i permessi assegnati ai file in SharePoint influenzano come i file sono accessibili e gestiti quando vengono sincronizzati o aperti tramite OneDrive.

Per garantire l'accesso a documentazione lavorativa anche a seguito di pensionamento oppure cambio del datore di lavoro, il dipendente dovrà condividere l'accesso a tutti i documenti salvati su SharePoint al Direttore/Responsabile del proprio Settore e ad almeno un altro collega, individuato in accordo con il Direttore/Responsabile del proprio Settore stesso.

Città metropolitana di Milano

PARERE DEL SEGRETARIO GENERALE
sulla proposta di decreto del Sindaco Metropolitano

Fascicolo 3.2\2024\3

Oggetto della proposta di decreto:

Approvazione del Piano Triennale per la Transizione digitale 2024-2026 della città metropolitana di Milano, del Piano dell'Innovazione e del disciplinare per l'utilizzo dei servizi informatici e di comunicazione telematica

PARERE DEL SEGRETARIO GENERALE
(inserito nell'atto ai sensi del Regolamento sul sistema dei controlli interni)

[X] Favorevole

[ ] Contrario

IL SEGRETARIO GENERALE

Documento informatico firmato digitalmente ai sensi del T.U. 445/2000 e del D.Lgs 82/2005 e rispettive norme collegate.