

Piano triennale per l'informatica nel comune di Lamezia Terme 2021-2023

Sommario

Normativa di riferimento.....	2
Definizioni e acronimi:.....	4
Premessa.....	8
Finalità.....	9
Capitolo 1 – servizi.....	10
Capitolo 2 - dati.....	10
Capitolo 3: piattaforme.....	10
Capitolo 4: infrastrutture.....	10
Capitolo 5: interoperabilità.....	10
Capitolo 6: sicurezza informatica.....	10
Strumenti e modelli per l'innovazione.....	11
Governare la trasformazione digitale.....	11
Ricognizione dell'esistente:.....	12
Obiettivi del triennio 2021- 2023.....	13
Capitolo 1a – servizi.....	13
Capitolo 2 b- dati.....	13
Capitolo 3c: piattaforme.....	13
Capitolo 4d: infrastrutture.....	13
Capitolo 5e: interoperabilità.....	14
Capitolo 6f: sicurezza informatica.....	14
Conclusioni.....	14
Riferimenti siti web.....	15

Normativa di riferimento

- a) **Decreto Legislativo 7 marzo 2005, n.82** «Codice dell'Amministrazione Digitale» e successive modifiche.
- b) **DPCM 1° Aprile 2008** «Regole tecniche e di sicurezza per il funzionamento del Sistema Pubblico di Connettività» previste dall'art. 71 c.1 bis del D.Lgs. 7 marzo 2005, n.82, recante il Codice dell'Amministrazione Digitale.
- c) **DPCM 24 gennaio 2013** «Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale».
- d) **DPCM 3 dicembre 2013** «Regole tecniche per il protocollo informatico ai sensi degli articoli 40-bis, 41, 47, 57-bis e 71, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005».
- e) **DPCM 3 dicembre 2013** «Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44, 44-bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005».
- f) **DL 24 giugno 2014, n.90** «Misure urgenti per la semplificazione e la trasparenza amministrativa e per l'efficienza degli uffici giudiziari», convertito nella legge 11 agosto 2014, n.114.
- g) **DPCM 24 ottobre 2014** «Definizione delle caratteristiche del Sistema Pubblico per la gestione dell'Identità Digitale (SPID) nonché dei tempi e delle modalità di adozione del sistema SPID da parte della Pubblica Amministrazione e delle imprese».
- h) **DPCM 13 novembre 2014** «Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonché di formazione e conservazione dei documenti informatici delle pubbliche amministrazioni ai sensi degli articoli 20, 22, 23-bis, 23-ter, 40, comma 1, 41, e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005».
- i) **DPR 28 dicembre 2000, n. 445** «disposizioni legislative in materia di documentazione amministrativa, di seguito «Testo unico», e la gestione informatica dei documenti»
- j) **Regolamento UE n° 910/2014** – eIDAS (electronic IDentification Authentication and Signature)
- k) **Legge n. 124 del 07/08/2015** (Riforma Madia) «Deleghe al Governo in materia di riorganizzazione delle amministrazioni pubbliche» recante norme relative alla cittadinanza digitale
- l) **D.lgs. 97/2016** (FOIA) Revisione e semplificazione delle disposizioni in materia di prevenzione della corruzione, pubblicità e trasparenza, correttivo della legge 6 novembre 2012, n. 190 e del decreto legislativo 14 marzo 2013, n. 33, ai sensi dell'articolo 7 della legge 7 agosto 2015, n. 124, in materia di riorganizzazione delle amministrazioni pubbliche
- m) **Regolamento UE 679/2016** (trattamento e circolazione dei dati personali)
- n) **decreto legislativo n. 179 del 2016** «Modifiche e integrazioni al Codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82, ai sensi dell'articolo 1 della legge 7 agosto 2015, n. 124, in materia di riorganizzazione delle amministrazioni pubbliche» (CAD 3.0)
- o) **DPCM 31 maggio 2017** «Piano Triennale 2017-2019 per l'informatica nella Pubblica Amministrazione»
- p) [Linee Guida per il Disaster Recovery \(DR\) delle PA](#) in data 23/03/2018.
- q) [Caratterizzazione dei sistemi cloud per la pubblica amministrazione](#) in data 23/03/2018
- r) **Circolare n. 3 del 9 aprile 2018** «Criteri per la qualificazione di servizi SaaS per il Cloud della PA»
- s) [Linee guida di design per i servizi digitali della PA](#) in data 13/06/2018.
- t) **Circolare n. 3 del 1° ottobre 2018** «Responsabile per la transazione al digitale»

- u) **12 febbraio 2019** “Piano triennale 2019 – 2021 per l'informatica nella Pubblica Amministrazione”
- v) **03 febbraio 2020** Ultimo aggiornamento del “Piano triennale 2019 – 2021 per l'informatica nella Pubblica Amministrazione”
- w) **DCPM dell'8 marzo 2020** “Ulteriori disposizioni attuative del decreto-legge 23 febbraio 2020, n. 6, recante misure urgenti in materia di contenimento e gestione dell'emergenza epidemiologica da COVID-19” all'art. 2 comma r) la modalità di lavoro agile disciplinata dagli articoli da 18 a 23 della legge 22 maggio 2017, n. 81.

Definizioni e acronimi:

Ai fini del presente piano s'intende per:

- **ACCOUNTABILITY:** criterio guida del Regolamento per la protezione dei dati personali, entrato in vigore nell'area Ue lo scorso 25 maggio. In italiano è stato tradotto con il termine "responsabilizzazione" ma il concetto non è chiaramente interpretabile solo come "responsabilità". Il concetto di "accountability" è legato al rendere conto dell'azione fatta o fatta fare.
- **AGID:** è l'agenzia tecnica della Presidenza del Consiglio che ha il compito di garantire la realizzazione degli obiettivi dell'Agenda digitale italiana e contribuire alla diffusione dell'utilizzo delle tecnologie dell'informazione e della comunicazione, favorendo l'innovazione e la crescita economica
- **API:** un insieme di [procedure](#) (in genere raggruppate per strumenti specifici) atte all'espletamento di un dato compito
- **Amministratori di sistema:** soggetti deputati a intervenire per garantire l'efficienza e la funzionalità di un determinato sistema informatico, aventi la possibilità di accedere a dati personali qualora l'accesso sia assolutamente necessario per raggiungere le finalità proprie del ruolo ricoperto; secondo le misure minime di sicurezza gli amministratori di sistema devono accedere con le proprie utenze amministrative e solo in casi particolari e documentati possono accedere con l'utenza Administrator generica;
- **ANPR:** Anagrafe nazionale della popolazione residente, è il registro anagrafico centrale del Ministero dell'interno della Repubblica Italiana.
- **Antivirus:** Programma in grado di riconoscere un virus presente in un file e di eliminarlo o di renderlo inoffensivo
- **Apparati attivi:** apparecchiature hardware collegate alla rete che ne permettono il funzionamento;
- **Aree condivise:** spazi di memorizzazione messi a disposizione degli utenti sui sistemi centralizzati per la condivisione e lo scambio di files;
- **Attachment:** (attaccamento) File allegato: può essere un allegato alla posta elettronica o a qualsiasi software di gestione dei file
- **Backup:** procedura per la duplicazione dei dati su un supporto esterno o distinto da quello sul quale sono memorizzati, in modo da garantirne una copia di riserva;
- **Banda:** Quantità di dati per unità di tempo che può viaggiare su una connessione. Nella banda ampia la velocità varia da 64 Kbps a 1,544 Mbps. Nella banda larga la comunicazione avviene a velocità superiori a 1,544 Mbps.
- **CAD:** Codice dell'amministrazione digitale: norma che riunisce in sé diverse norme emanate tra il 1997 e il 2005 riguardanti l'informatizzazione della pubblica amministrazione, ed in particolare il documento informatico, la firma elettronica e la firma digitale, delle quali stabilisce l'equivalenza con il documento cartaceo e con la firma autografa.
- **CERT_PA:** Computer Emergency Readiness/Response Team. In sostanza, si tratta di una speciale squadra attiva per dare subito risposta in caso di emergenze informatiche all'interno della pubblica amministrazione. CERT-PA opera all'interno dell'AgID, l'Agenzia per l'Italia Digitale
- **CONSIP:** è la centrale acquisti della pubblica amministrazione italiana; è una società per azioni il cui unico azionista è il Ministero dell'economia e delle finanze del governo italiano ed opera nell'esclusivo interesse dello Stato
- **Cookie:** Tradotto letteralmente significa biscotto. E' un file memorizzato sul proprio computer che identifica il computer quando è collegato ad alcuni siti Internet.
- **Classificazione Data Center:**
Gruppo A - Data center di qualità che non sono stati eletti a Polo strategico nazionale, oppure con carenze strutturali o organizzative considerate minori. Come indicato in seguito, queste strutture potranno continuare ad operare ma non potranno essere effettuati investimenti per l'ampliamento o l'evoluzione. Dovranno comunque garantire continuità dei servizi e Disaster recovery, fino alla completa migrazione, avvalendosi dei servizi disponibili con il Contratto quadro SPC Cloud lotto 1 o messi a disposizione dai Poli strategici nazionali.

Gruppo B - Data center che non garantiscono requisiti minimi di affidabilità e sicurezza dal punto di vista infrastrutturale e/o organizzativo, o non garantiscono la continuità dei servizi. Queste infrastrutture dovranno essere rapidamente consolidate verso uno dei Poli strategici nazionali o verso il cloud tramite i servizi disponibili con il Contratto quadro SPC Cloud lotto 1.

- **Cloud:** indica un paradigma di erogazione di servizi offerti on demand da un fornitore ad un cliente finale attraverso la rete Internet. Il cloud è un modello che consente di disporre, tramite internet, di un insieme di risorse di calcolo (ad es. reti, server, storage, applicazioni e servizi) che possono essere erogate come un servizio.
- **CIE:** La carta d'identità elettronica italiana è un documento di riconoscimento previsto in Italia dalla legge. Ha sostituito la carta d'identità in formato cartaceo nella Repubblica Italiana. La carta di identità elettronica attesta l'identità del cittadino
- **CSIRT:** (Computer security incident response team) Il CSIRT Italiano è stato istituito presso il Dipartimento delle informazioni per la Sicurezza della Presidenza del Consiglio dei Ministri (DIS) con l'obiettivo di ottimizzare l'efficacia della prevenzione e della risposta del Paese a fronte di eventi di natura cibernetica a danno di soggetti pubblici e privati.
- **CSP:** Cloud Service Provider – Fornitori di servizi in cloud
- **Data breach:** incidente di sicurezza in cui dati sensibili, riservati, protetti vengono consultati, copiati, trasmessi, rubati o utilizzati da soggetti non autorizzati
- **Dati personali:** dati identificativi: cognome e nome, residenza, domicilio, nascita, identificativo online (username, password, customer ID, altro), situazione familiare, immagini, elementi caratteristici della identità fisica, fisiologica, genetica, psichica, economica, culturale, sociale, dati inerenti lo stile di vita la situazione economica, finanziaria, patrimoniale, fiscale, dati di connessione: indirizzo IP, login, altro, dati di localizzazione: ubicazione, GPS, GSM, altro.
- **DNS (Domain Name System):** Sistema che gestisce gli indirizzi dei domini Internet.
- **DPIA - Data Protection Impact Assessment**” - “**Valutazione d’impatto sulla protezione dei dati**”: è una procedura finalizzata a descrivere il trattamento, valutarne necessità e proporzionalità, e facilitare la gestione dei rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento dei loro dati personali.
- **Ente:** il Comune di Lamezia Terme
- **Firewall:** apparato di rete hardware o software che filtra tutto il traffico informatico in entrata e in uscita e che di fatto evidenzia un perimetro all’interno della rete informatica comunale e contribuisce alla sicurezza della rete stessa.
- **Garante Privacy:** il Garante per la protezione dei dati personali istituito dalla Legge 31 dicembre 1996 n. 765, quale autorità amministrativa pubblica di controllo indipendente.
- **Indirizzamento:** attività di assegnazione di indirizzi logici ad apparati attivi;
- **Integrità:** la protezione contro la perdita, la modifica, la creazione o la replica non autorizzata delle informazioni ovvero la conferma che i dati trattati siano completi;
- **IP:** Indirizzo che permette di identificare in modo univoco un computer collegato in rete. Si suddivide in due parti, la prima individua la rete dove si trova il computer, la seconda individua il computer all’interno di quella rete.
- **Interoperabilità:** caratteristica di un sistema informativo, le cui interfacce sono pubbliche e aperte, di interagire in maniera automatica con altri sistemi informativi per lo scambio di informazioni e l'erogazione di servizi;
- **IPSEC Internet Protocol Security:** è una collezione di protocolli implementati che fornisce un metodo per garantire la sicurezza del protocollo IP, sia esso versione 4 sia 6, e dei protocolli di livello superiore (come, ad esempio, UDP e TCP), proteggendo i pacchetti che viaggiano tra due sistemi host, tra due security gateway (ad esempio router o firewall) oppure tra un sistema host e una security gateway.
- **Linee guida o policy:** regole operative tecniche e/o organizzative atte a guidare i processi lavorativi, decisionali e attuativi;
- **Log:** file che registra attività di base quali l’accesso ai computer e che è presente sui server della rete informatica
- **Logging:** attività di acquisizione cronologica di informazioni attinenti all’attività effettuata sui sistemi siano essi semplici apparati o servizi informatici;

- **Misure minime di sicurezza:** le misure minime di sicurezza ICT emanate dall'AgID, sono un riferimento pratico per valutare e migliorare il livello di sicurezza informatica delle amministrazioni, al fine di contrastare le minacce informatiche più frequenti
- **NAS: Network Attached Storage** è un dispositivo collegato alla [rete](#) la cui funzione è quella di consentire agli utenti di accedere e condividere una [memoria di massa](#), in pratica costituita da uno o più [dischi rigidi](#), all'interno della propria rete. In ambiente NetApp tale dispositivo prende il nome di FAS.
- **Office automation:** software di produttività, si intendono gli applicativi a corredo delle mansioni lavorative.
- **Open data:** formato aperto: un formato di dati reso pubblico, documentato esaustivamente e neutro rispetto agli strumenti tecnologici necessari per la fruizione dei dati stessi
- **PagoPa:** è un sistema di pagamenti elettronici realizzato per rendere più semplice, sicuro e trasparente qualsiasi pagamento verso la Pubblica Amministrazione.
- **Policy:** modello di configurazione e adattamenti da riferirsi a gruppi di utenti o a uso del software.
- **Policy di riferimento:** documento tecnico che descrive lo stato attuale delle policy in uso, aggiornato periodicamente in funzione dell'evoluzione tecnologica/organizzativa;
- **Postazione di lavoro:** dispositivo (personal computer, notebook, thin/fat client, ecc.) che consente l'accesso al proprio ambiente di lavoro informatico;
- **Protocollo:** insieme di regole che definisce il formato dei messaggi scambiati tra due unità informatiche e che consente loro di comunicare nonché di comprendere la comunicazione;
- **PSN:** Poli strategici nazionali: il soggetto titolare dell'insieme di infrastrutture IT (centralizzate o distribuite), ad alta disponibilità, di proprietà pubblica, eletto a Polo Strategico Nazionale dalla Presidenza del Consiglio dei Ministri e qualificato da Agid ad erogare, in maniera continuativa e sistematica, ad altre amministrazioni:
- **Responsabile del trattamento:** il Dirigente/Responsabile P.O., oppure il soggetto pubblico o privato, che tratta dati personali per conto del Titolare del trattamento.
- **RDP (Remote Desktop Protocol):** è un protocollo di rete proprietario sviluppato da Microsoft, che permette la connessione remota da un computer a un altro in maniera grafica
- **Responsabile per la protezione dati – RPD o DPO:** il dipendente della struttura organizzativa del Comune, il professionista privato o impresa esterna, incaricati dal Titolare o dal Responsabile del trattamento.
- **Registri delle attività di trattamento:** elenchi dei trattamenti in forma cartacea o telematica tenuti dal Titolare e dal Responsabile del trattamento secondo le rispettive competenze.
- **Rete dati:** insieme dell'infrastruttura passiva (cavi, prese, ecc.) e degli apparati attivi (modem, router, ecc.) necessari alla interconnessione di apparati informatici;
- **Sandbox:** è un processo di rete che consente di inviare i file a un dispositivo separato, da ispezionare senza rischiare la sicurezza della rete. Ciò consente il rilevamento di minacce che potrebbero aggirare altre misure di sicurezza, comprese le minacce zero-day.
- **SIOPE+:** è la nuova infrastruttura che intermedierà il colloquio tra pubbliche amministrazioni e banche tesoriere con l'obiettivo di migliorare la qualità dei dati per il monitoraggio della spesa pubblica e per rilevare i tempi di pagamento delle Pubbliche Amministrazioni nei confronti delle imprese fornitrici.
- **Software web-based:** ha interfaccia web e non ha prerequisiti e dipendenze obbligatorie (ad esempio plug-in sul dispositivo) ed è mobile first.
- **SPC:** Sistema Pubblico di Connettività e cooperazione (SPC) è una cornice nazionale di interoperabilità: definisce, cioè, le modalità preferenziali che i sistemi informativi delle pubbliche amministrazioni devono adottare per essere tra loro interoperabili
- **SPC2:** Sistema pubblico di connettività e cooperazione fase 2
- **SPC Cloud:** Sistema pubblico di connettività e cooperazione in cloud per l'erogazione di servizi a favore della Pubblica amministrazione
- **SPID:** Sistema Pubblico di Identità Digitale, è la soluzione che ti permette di accedere ai servizi online della Pubblica Amministrazione e dei soggetti privati aderenti con un'unica Identità Digitale (username e password) utilizzabile da computer, tablet e smartphone.
- **SSL: Secure Sockets Layer:** protocollo [crittografico](#) usato nel campo delle [telecomunicazioni](#) e dell'[informatica](#) che permette una comunicazione [sicura](#) dalla sorgente al destinatario (end-to-end) su reti [TCP/IP](#) (come ad esempio [Internet](#)) fornendo [autenticazione](#), integrità dei [dati](#) e [confidenzialità](#) operando al di sopra del [livello di trasporto](#).

- **Titolare del trattamento:** l'autorità pubblica (il Comune o altro ente locale) che singolarmente o insieme ad altri determina finalità e mezzi del trattamento di dati personali
- **URL (Uniform Resource Locator):** Identifica in modo univoco le informazioni presenti su Internet, un indirizzo dal quale si richiamano le informazioni.
- **Utente:** persona fisica autorizzata ad accedere ai servizi informatici dell'Ente.
- **VOIP:** (Voice over IP) tecnologia che rende possibile effettuare una comunicazione telefonica sfruttando il protocollo IP della rete dati
- **VPN:** Virtual Private Network, è una [rete di telecomunicazioni](#) privata, instaurata tra soggetti che utilizzano, come tecnologia di trasporto, un protocollo di [trasmissione](#) pubblico, condiviso e sicuro attraverso la rete internet

Premessa

Con la pubblicazione ad agosto del Piano triennale per la Pubblica Amministrazione 2020 – 2022 da parte di Agid e con il D.L. n. 76 del 16 luglio 2020 (convertito con Legge 11 settembre 2020 n.120) il cosiddetto decreto “*semplificazioni*” è doveroso aggiornare il piano triennale per l’informatica nel Comune di Lamezia Terme.

Le due sopracitate pubblicazioni hanno evidenziato in maniera significativa i passi metodologici da affrontare con un preciso scadenziario delle attività. Inoltre, l’emergenza COVID 19 ha imposto alle Amministrazioni di procedere con celerità all’attivazione delle procedure per lo smart working diffuso con approcci digitali basati sulla sicurezza e su metodologie quanto più possibile in cloud.

In particolare, il primo *switch off* determinato dal decreto semplificazioni è relativo al 28 febbraio 2021 ha obbligato le Pubbliche amministrazioni a rilasciare servizi in modalità digitale, utilizzare come strumento di pagamenti per la PA la piattaforma PagoPa, non rilasciare credenziali per collegarsi ai servizi comunali che dovranno essere accessibili solo tramite CIE e SPID e attivare servizi dell’app IO.

Il presente documento è adeguato alle scadenze temporali delle macro-operazioni da effettuare.

L’amministrazione non perde di vista il rispetto delle normative che regolano i nuovi processi, prevedendo la possibilità di avere all’interno dell’ente, un responsabile per la transizione digitale, prevedendo in tal senso, nel fabbisogno del personale, una figura dotata di profilo idoneo per ricoprire tale ruolo.

Finalità

Il Piano triennale 2020-2022 e gli adeguamenti al PNRR, emanato da Agid, rappresenta la naturale evoluzione dei due Piani precedenti e introduce un'importante innovazione con riferimento ai destinatari degli obiettivi individuati per ciascuna delle tematiche affrontate.

Si tratta di obiettivi di ampio respiro declinati tuttavia in risultati molto concreti.

L'elemento innovativo del Piano sta proprio nel forte accento posto sulla misurazione di tali risultati, introducendo così uno spunto di riflessione e una guida operativa per tutte le amministrazioni: la cultura della misurazione e conseguentemente della qualità dei dati che diventa uno dei motivi portanti di questo approccio.

La rappresentazione semplificata del modello strategico consente di descrivere in maniera funzionale la *trasformazione digitale*. Tale rappresentazione è costituita da due livelli trasversali: *l'interoperabilità* e la *sicurezza dei sistemi informativi* e dei livelli verticali di servizi, dati, piattaforme ed infrastrutture.



Sulla base di questo modello operativo e di concetti già espressi precedentemente, nel piano 2020 – 2022, si delinea una *road map* operativa, che relativamente a quanto deve fare la pubblica amministrazione (nel piano Agid ogni componente ha dei compiti precisi), le tappe su possono elencare come segue:

Capitolo 1 – servizi

L'obiettivo è migliorare la capacità di generare ed erogare servizi digitali attraverso l'utilizzo di soluzioni SaaS (software as a service) certificati Agid, anche già esistenti e riusare e condividere i software tra le pubbliche amministrazioni; è necessario adottare modelli e strumenti validi che siano a disposizione di tutti e monitorare costantemente i servizi online che devono necessariamente incrementare il livello di accessibilità dei servizi digitali della PA secondo le Linee guida sull'accessibilità degli strumenti informatici.

Capitolo 2 - dati

La valorizzazione del patrimonio informativo pubblico è un obiettivo strategico per la pubblica amministrazione che, in piena adesione al contesto europeo, ha il compito di adottare una *data governance* che consenta non solo di erogare servizi digitali di alto valore per i cittadini ma anche di permettere la piena condivisione dei dati tra le pubbliche amministrazioni.

Capitolo 3: piattaforme

Le piattaforme tecnologiche offrono funzionalità fondamentali, trasversali, abilitanti e riusabili nella digitalizzazione dei processi e dei servizi della PA; consentono di ridurre il carico di lavoro delle pubbliche amministrazioni, sollevandole dalla necessità di dover realizzare ex novo funzionalità, riducendo i tempi e i costi di attuazione dei servizi, garantendo maggiore sicurezza informatica. Il Piano triennale proseguendo nel percorso di evoluzione delle piattaforme esistenti (es. SPID, PagoPa, ANPR, CIE, ecc.) promuove l'utilizzo di piattaforme che consentano di razionalizzare i servizi sia per le amministrazioni sia per i cittadini., quali quella di IO; INAD (piattaforma che gestisce l'Indice nazionale dei domicili digitali); piattaforma del Sistema museale nazionale; piattaforma digitale nazionale dati (PDND).

Capitolo 4: infrastrutture

Lo scenario sulle infrastrutture, ben evidenziato nel censimento dei Ced, pone l'esigenza immediata di attuare un percorso di razionalizzazione delle infrastrutture per garantire la sicurezza dei servizi erogati e mediante la migrazione verso data center più sicuri e verso infrastrutture e servizi cloud qualificati da AGID secondo il modello Cloud della PA e evitare che le amministrazioni costruiscano nuovi data center al fine di ridurre la frammentazione delle risorse e la proliferazione incontrollata di infrastrutture con conseguente moltiplicazione dei costi.

Capitolo 5: interoperabilità

L'interoperabilità permette la collaborazione e l'interazione telematica tra pubbliche amministrazioni, cittadini e imprese, favorendo l'attuazione del principio "once only" e recependo le indicazioni dell'European Interoperability Framework attraverso la diffusione e l'utilizzo di API.

Capitolo 6: sicurezza informatica

La minaccia cibernetica cresce continuamente in quantità e qualità. L'esigenza per la PA di contrastare tali minacce diventa fondamentale in quanto garantisce non solo la disponibilità, l'integrità e la riservatezza delle informazioni proprie del Sistema informativo della Pubblica Amministrazione, ma è il presupposto per la protezione del dato che ha come conseguenza diretta l'aumento della fiducia nei servizi digitali erogati dalla PA e questo può essere attuato con la formazione e la prevenzione e con un incremento del livello di Cyber Security Awareness misurato tramite questionari di self-assessment ai RTD, con portali istituzionali che utilizzano il protocollo HTTPS only e adeguando le misure minime di sicurezza emanate da cert-Pa.

Strumenti e modelli per l'innovazione

In questo capitolo tutte le azioni da intraprendere devono essere finalizzate, in ultima istanza, al miglioramento della qualità della vita dei cittadini e cioè

- Lo sviluppo delle smart city e dei borghi del futuro
- La realizzazione di poli di innovazione che diventino catalizzatori e acceleratori della innovazione nella PA
- Il considerare l'innovazione come un bene comune.

Governare la trasformazione digitale

I punti salienti di questo capitolo sono:

- Il coinvolgimento attivo delle amministrazioni e dei territori;
- Consolidamento del ruolo del [responsabile della transizione al digitale](#);
- La domanda pubblica come leva per l'innovazione del Paese;
- Modelli e regole per l'erogazione integrata di servizi interoperabili;
- Le competenze digitali per la PA e per il Paese e l'inclusione digitale;
- Il monitoraggio del Piano triennale.

Ricognizione dell'esistente

Allo stato attuale, il patrimonio informatico dell'ente dispone sulle seguenti implementazioni:

1. Miglioramento della connettività dell'ente passando da una linea internet da 40 Mbit ad una a 200 Mbit.
2. Affidamento dei vari software gestionali tecnico/amministrativi ad un'unica A.T.I., composta da due software house, per la durata contrattuale di 5 anni.
Questa scelta ha comportato un allineamento delle piattaforme, il coordinamento tra le stesse che consente un'interoperabilità settoriale.
È stato intrapreso un percorso di migrazione delle banche dati dai vecchi gestionali verso i nuovi, garantendo in questo modo la consultazione agli utenti.
3. Attivazione dei servizi tramite app *municipium*, che consente un canale diretto di comunicazione con i portable device dei cittadini;
4. Attivazione dei servizi di pagamento su PagoPa con accesso tramite SPID;
5. Pianificazione per il passaggio in cloud certificato Agid di una parte significativa dei servizi comunali con conseguente dismissione di server locali;
A tal proposito sono stati attivati dei servizi di *IaaS* e *BaaS* per consentire l'estensione dell'infrastruttura on-premise e per garantire meccanismi di backup e ridondanza degli stessi dati.
6. Adesione alla convenzione Consip per la gestione di tutti i servizi Cloud & on Premise, con il riordino degli stessi sui server fisici e virtuali.
7. Censimento del servizio di *posta elettronica*, al fine di dismettere le caselle non più in uso con contestuale backup dei dati in esse contenuto.
8. Adozione di una suite di sicurezza endpoint cloud based distribuita in ambiente sia client che server. Tale soluzione prevede la scansione in tempo reale delle minacce informatiche, sfruttando motori
9. Adesione all'APP IO con programmatico inserimento dei vari servizi (attualmente *Anagrafe* e *Elettorale*);
10. Attivazione di sportelli virtuali con agenda delle prenotazioni per colloquiare con il personale comunale e rilasciare informazioni in maniera esclusivamente digitale.
11. Implementazione di meccanismi di sicurezza perimetrale della rete mediante implementazione e conduzione di Firewall fisici per gestione del traffico da/verso la rete internet. La gestione del traffico viene garantita tramite meccanismi che permettono un livello di granularità elevata (a livello utente o macchina) del traffico.
12. Adeguamento della connettività SPC alle reali esigenze dell'Ente, con l'adesione a servizio affidabile e che consenta l'operabilità continua senza cali di potenziale;
13. Adeguamento dei sistemi operativi di pc comunali con svecchiamento del parco macchine, con contestuale miglioramento della performance e della sicurezza.
14. Adesione all'ANPR
15. Predisposizione di un'infrastruttura di backup per prevedere la ridondanza di dati e metadati. I backup vengono effettuati quotidianamente sia on-premise che in cloud. I backup vengono effettuati su diversi repository così da garantire strategie robuste di *disaster recovery*.
16. Implementazione, tramite migrazione da precedenti prodotti, di software antivirus basato su una suite di sicurezza avanzata per postazioni client e server.

Le attività e operazioni effettuate nell'annualità in corso sono state realizzate con personale interno.

Obiettivi del triennio 2021- 2023

L'obiettivo del triennio vede nella prima parte del 2021 una fase di consolidamento delle procedure avviate nel 2020. Inoltre

Entro la data indicata dal decreto semplificazioni (31/12/2021) l'amministrazione intende procedere all'inserimento nell'app IO di tutti i servizi e all'aumento di servizi per PagoPa e SPID.

Nel medio lungo termine, secondo il piano triennale di Agid si cercherà di adottare il modello strategico e la metodologia precedentemente indicata.

In particolare:

Capitolo 1a – servizi

Publicare e compilare i form di accessibilità dei siti web, delle app nonché l'uso dei modelli per lo sviluppo web per i propri siti istituzionali e in generale migliorare la capacità di generare ed erogare servizi digitali con l'adesione a Web analytics secondo i principi Cloud First - SaaS First e ad acquisire servizi cloud solo se qualificati da AGID.

Capitolo 2b - dati

Avviare l'adeguamento dei sistemi che si interfacciano verso tutte le banche dati di interesse nazionale secondo le linee guida del modello di interoperabilità comprese le banche dati territoriali per favorire la condivisione e il riutilizzo dei dati tra le PA e il riutilizzo da parte di cittadini e imprese, aumentare la qualità dei dati e dei metadati e la consapevolezza sulle politiche di valorizzazione del patrimonio informativo pubblico e su una moderna economia dei dati

Capitolo 3c: piattaforme

Proseguire il percorso di adesione a SPID e PagoPa e dismettere le altre modalità di autenticazione e pagamento associate ai propri servizi online con l'obiettivo di incrementare il numero di piattaforme per le amministrazioni ed i cittadini

Capitolo 4d: infrastrutture

L'ente, essendo proprietario di un CED ed essendo fornito di rete intranet, si impegnerà al rinnovo dell'intera infrastruttura di rete.

È stato previsto un piano per la fornitura di apparati di rete (switch, firewall) di ultima generazione che mira ad ottenere performance di sicurezza e di fruibilità per i servizi interni all'ente.

Verranno sostituiti gli UPS dei rack di piano e quelli della sala CED con conseguente adeguamento della rete elettrica.

La struttura logica e fisica della rete comunale verrà re-ingegnerizzata e verrà attuata una segmentazione della stessa con sistemi per il controllo degli accessi basati sul principio del "privilegio minimo".

Per gli anni seguenti, l'aggregazione e la migrazione su infrastrutture sicure ed affidabili consentirà il miglioramento dell'offerta di servizi di connettività per le PA e si provvederà ad acquistare nuovi servizi disponibili nel listino SPC.

È previsto un piano di rinnovo delle licenze Server per adeguamento agli standard vigenti con conseguente upgrade dell'intero dominio Active Directory ad un livello di funzionalità supportato dal fornitore.

L'upgrade prevede anche la dismissione dell'attuale File Server che verrà migrato su infrastruttura aggiornata. Ciò garantisce un aumento delle misure di sicurezza e controllo degli accessi.

Capitolo 5e: interoperabilità

Favorire l'applicazione della Linea guida sul Modello di Interoperabilità da parte degli erogatori di API conformi al Modello di Interoperabilità.

Capitolo 6f: sicurezza informatica

Agid deve produrre gli aggiornamenti alle misure minime di sicurezza previste per giugno 2021 e dei tool di sicurezza. Inoltre, deve uscire il decreto attuativo della legge sul perimetro di sicurezza nazionale cibernetica e le linee guida per lo sviluppo e la definizione del modello di riferimento per i CERT di prossimità e di conseguenza il comune si adeguerà a tutte le normative mantenendo alto il livello di sicurezza e aggiornando il regolamento interno informatico anche alla luce dei passaggi al cloud di molte procedure.

In generale deve aumentare il livello di consapevolezza del dato prodotto e gestito dalla pubblica amministrazione secondo un principio di accountability, principio cardine del GDPR, favorendo al contempo la diffusione di formati aperti e sicuri.

Conclusioni

Molte delle operazioni indicate come obiettivi sono in fase di realizzazione o sono stati realizzati e si è posta una base solida e un traguardo che, a piccoli passi, sposta i servizi digitali dell'ente verso obiettivi condivisi e indicati da Agid.

Riferimenti siti web

AGID <https://www.agid.gov.it/>

CERT-PA <https://www.cert-pa.it/>

CSIRT <https://csirt.gov.it/home>

PagoPA <https://www.pagopa.gov.it/>

SPID <https://www.spid.gov.it/>

IO <https://io.italia.it/>

Grante privacy <https://www.garanteprivacy.it/>