COMUNE DI CAVALLERMAGGIORE

(Provincia di Cuneo)

Piano Triennale per la transizione digitale 2021-2023

Riferimento al Piano Triennale per l'informatica 2021-2023 pubblicato da AGID

Cavallermaggiore, dicembre 2022

Sommario

PARTE Iª - IL PIANO TRIENNALE

Introduzione

Redigere un piano per l'attuazione della transizione al digitale e per l'implementazione informatica per il Comune di Cavallermaggiore comporta da una parte comprendere le linee guida del Piano Triennale della Pubblica Amministrazione redatto da AGID (Agenzia per l'Italia Digitale) e dall'altra calarsi nella realtà dell'informatica dell'Ente Locale per adeguare l'esistente e ciò che è stata fatto nella direzione indicata da AGID.

Si riprende, per meglio comprenderne le finalità, la definizione iniziale del Piano Triennale AGID nella sua guida dinamica: "Il Piano Triennale, nel proseguire il percorso intrapreso col Piano precedente, prevede un importante coinvolgimento delle Pubbliche Amministrazioni che dovranno recepire ed utilizzare le indicazioni e gli strumenti messi a disposizione da AGID. Le Pubbliche Amministrazioni sono al centro del processo di trasformazione digitale del Paese in quanto costituiscono lo snodo principale in grado di abilitare la cultura dell'innovazione tra imprese e cittadini. In quest'ottica, il Piano detta indirizzi su temi specifici che le Amministrazioni potranno utilizzare per costruire i loro piani di trasformazione digitale all'interno di una cornice condivisa, definita da AGID".

Il piano vuole essere anche una guida operativa, una strada da seguire per ottemperare all'evoluzione informatica in atto e per condurre, di concerto con il piano politico dell'Amministrazione Comunale, ad una strategia di sviluppo allargato in campo digitale.

Il piano infine vuole essere uno strumento aperto, suscettibile di continui miglioramenti ed adeguamenti finalizzato a far crescere la qualità dei servizi all'interno dell'Amministrazione e di conseguenza di quelli forniti alla cittadinanza e alle imprese, promuovendo e sollecitando la partecipazione allargata ed attiva dei cittadini.

Il Piano Triennale per l'Informatica della Pubblica Amministrazione dell'Agenzia per l'Italia Digitale (AgID), di seguito Piano Triennale o Piano di Transizione Digitale, è lo strumento principale di pianificazione della trasformazione digitale della Pubblica Amministrazione italiana. Esso tiene conto:

- dei principi dell'eGovernment Action Plan 2016-2020;

- delle azioni previste dalla eGovernment Declaration di Tallinn (2017-2021);

- delle indicazioni della nuova programmazione europea 2021-2027;

- dei target al 2030 del Digital Compass, i cui indicatori misurano il livello di digitalizzazione in tutta l'UE e rilevano l'effettiva presenza e l'uso dei servizi digitali da parte dei cittadini e imprese. In quest'ottica la Commissione UE nella Comunicazione "Progettare il futuro digitale dell'Europa" ha disposto che almeno il venti per cento della spesa complessiva del PNRR sia rivolta a investimenti e riforme nel digitale, con l'obiettivo di migliorare le prestazioni digitali sintetizzate dall'Indice di digitalizzazione dell'economia e della società (DESI).

Il PNRR ha fra i propri assi strategici, condivisi a livello europeo, quello della digitalizzazione e innovazione. Prevede nella componente denominata "Digitalizzazione, innovazione e sicurezza nella PA" investimenti pari a 9,75 Mld, di cui 6,14 Mld destinati alla misura "Digitalizzazione PA". Quest'ultima dovrà essere attuata secondo le linee tracciate dal Piano Triennale, nel pieno rispetto delle disposizioni del CAD e di tutte le altre normative e Linee Guida pubblicate.

In campo normativo il Decreto Semplificazioni “bis” (D.L. 31 maggio 2021 n. 77 come convertito con la Legge n. 108 del 29 luglio 2021) ha recentemente introdotto l’art. 18-bis del CAD (Violazione degli obblighi di transizione digitale).

Il presente documento rappresenta il Piano Triennale per l’Informatica della Pubblica Amministrazione del Comune di Cavallermaggiore, ovvero lo stato dell’arte dell’esecuzione delle misure previste dal Piano Triennale della Pubblica Amministrazione AgID presso l’Ente e gli intenti formulati nei vari progetti oggetto di finanziamento del PNRR.

Tutti i principali obiettivi del Piano nazionale, la diffusione dell’identità digitale, la riduzione del gap di competenze digitali, l’incremento dell’uso dei servizi in cloud da parte della PA, la crescita dell’erogazione dei servizi digitali essenziali online, il completamento delle reti a banda ultra-larga, sono recepiti, condivisi ed attuati con il contributo ed il supporto dell’Ufficio del Responsabile della Transizione Digitale e più in generale della Giunta e della Struttura Tecnica ed Amministrativa dell’Ente.

Ruolo del Responsabile per la Transizione al Digitale

Il Responsabile per la Transizione al Digitale (RTD) è la figura dirigenziale, dotata di alte competenze in ambito tecnologico, manageriale e di informatica giuridica, che, all’interno della PA, ha il compito di attuare e coordinare la trasformazione digitale dell’Amministrazione, lo sviluppo dei servizi pubblici digitali, il rispetto degli standard e l’adozione dei nuovi modelli di design, accessibilità, riuso ed open data. L’RTD risponde, con riferimento ai compiti relativi alla transizione alla modalità digitale, direttamente all’organo di vertice politico.

L’RTD del Comune di Cavallermaggiore è la dott.ssa Laura MENTONE.

Obiettivi e spesa complessiva prevista

Di seguito si elencano le azioni principali:

▪ Sviluppo di progetti di transizione/trasformazione digitale legati a bandi europei e nazionali o a specifici progetti regionali, a cui il Comune di Cavallermaggiore partecipa;

▪ Candidature a bandi europei e PNRR, affidamenti di servizi complessi e strategici;

▪ Piano Triennale per l'Informatica nella PA del Comune di Cavallermaggiore (adozione nuovo Piano Triennale per l'informatica del Comune di Cavallermaggiore, aggiornamento delle Misure di Sicurezza ICT per le PA, analisi della compliance al "Regolamento Cloud della PA", Digitalizzazione dei processi e dei documenti);

▪ Aggiornamenti/consolidamenti dei sistemi informativi per garantire la compatibilità con gli obiettivi di attuazione dell’agenda digitale e, in particolare, con quelli stabiliti nel piano triennale;

▪ Attivazione di nuovi servizi o integrazione su servizi già pubblicati sulla piattaforma IO Italia;

▪ Consolidamento di strumenti innovativi per la dematerializzazione, in particolare delle pratiche edilizie, potenziamento PagoPA nell'Ente;

▪ Potenziamento dell'integrazione e interoperabilità tra i sistemi e servizi dell'Amministrazione e dei servizi in rete e rinnovamento tecnologico dei sistemi informativi;

▪ Infrastrutture tecnologiche: potenziamento e razionalizzazione;

▪ Sviluppo dei servizi decentrati sul territorio – sportelli virtuali.

P.N.R.R.

Progetto	Importo finanziato	Termini
Avviso Misura 1.2 "Abilitazione al cloud per le PA locali Comuni"	€ 115.064,00	04.03.2023 – 27.05.2024
Avviso Misura 1.4.1 "Esperienza del Cittadino nei servizi pubblici" Comuni	€ 155.234,00	16.05.2023 – 10.05.2024
Avviso Misura 1.4.3 "Adozione AppIO"	€ 4.802,00	08.02.2023 – 06.10.2023
Avviso Misura 1.4.3 "PagoPA" Comuni	€ 18.854,00	30.01.2023 -26.09.2023
Avviso Misura 1.4.4 "SpID CIE" Comuni	€ 14.000,00	28.07.2023 - 23.05.2024
Avviso Misura 1.4.5 "Piattaforma notifiche digitali" Comuni	€ 32.589,00	In attesa decreto di finanziamento

Ricognizione dell'esistente

Per la transizione al digitale, si è provveduto alla individuazione dei settori dell'Ente, con provvedimento decreto n. 6 in data 01.06.2022, con cui è stato deciso tra l'altro:

- di disporre che l'ufficio della transizione al digitale ex art. 17 del D.Lgs. n. 82/2005, come modificato dal D.Lgs. n. 217/2017, coerentemente agli obiettivi strategici e all'assetto organizzativo dell'Ente è da ritenersi composto da tutti i settori dell'Ente, in staff;

- di stabilire che i compiti attribuiti al servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, descritti all'art. 61 del D.P.R. n. 445/2000 e del DPCM 3.12.2013 recante le regole tecniche per il protocollo informatico (s.m.i.) siano svolte dal settore nell'ambito del quale è incaricato il protocollo archivio, tempo per tempo;

- di stabilire che la gestione documentale e la conservazione siano svolti in staff dagli uffici di tale settore deputati alla gestione del protocollo e dell'archivio, unitamente al servizio di staff centro elaborazione dati, e con il supporto del DPO, data protection officer.

Il responsabile della transizione digitale è l'esecutore del servizio per la transizione al digitale coadiuvato dal personale interno, nonché dall'Amministratore di sistema, e da supporto tecnico esterno, in particolare per le attività manutentive. Sono inoltre attivi contratti di assistenza sistemistica di ulteriore livello.

Il DPO ha prodotto il "disciplinare interno per l'utilizzo dei sistemi, dati e strumenti informatici all'interno del Comune di Cavallermaggiore con contestuale informativa. Il Comune di Cavallermaggiore è adeguato alle misure minime di sicurezza redatte da Agid poste come base per la

sicurezza dell'Ente. Esegue scansioni di vulnerabilità in maniera programmata ed è dotata di un software per la gestione dell'inventario.

La struttura prevede circa 22 computer e tre macchine server tutte gestite in maniera virtuale. Sia il backup che lo spazio condiviso sono interni alla struttura. In cloud c'è la Conservazione Sostitutiva, delegata all'Istituto per i Beni Artistici, Culturali e Naturali della Regione Emilia-Romagna (IBACN), qualificato come fornitore di servizi SAAS in qualità di CSP per i servizi offerti dal Polo archivistico regionale (ParER), in seguito ad accordo sottoscritto il 4 dicembre 2022.

Dal punto di vista normativo la struttura è stata classificata data center classificati nel gruppo B idonea per quanto riguarda la fase minima di continuità operativa avendo un secondo datacenter collegato con fibra ottica privata presso una sede secondaria del comune mentre la classificazione finale da parte di Agid al data center comunale è risultata essere di tipo nodo1 - Gruppo B server domain controller secondario - Gruppo B con comunicazione da parte di Agid del 10.02.2020.

Tale classificazione impone al Comune di Cavallermaggiore l'impossibilità di investire in hardware (al netto di esigenze bloccanti) e di continuare il processo di trasformazione verso il Cloud per la completa eliminazione del data center.

La struttura informatica utilizza per la maggior parte una serie di software web based che ne permettono la fruizione anche dall'esterno favorendo il cosiddetto "lavoro agile" o il telelavoro che avviene in maniera sicura tramite client installato sul personal computer e collegamento protetto. La posta elettronica è gestita per in maniera web based.

Per quel che riguarda le piattaforme abilitanti il Comune di Cavallermaggiore ha due postazioni di carta d'identità elettroniche ed è collegata ad ANPR. Gestisce i flussi con il SIOPE+ ed ha all'attivo alcuni servizi di PagoPa con altri servizi già in fase di attivazione. Anche l'app IO ha già alcune funzionalità attive.

Il sito internet comunale è adeguato alle normative del settore sulla grafica Agid e l'accessibilità e all'interno della sezione servizi online fornisce diverse procedure online. Infine l'Amministrazione Comunale è attiva sui canali youtube, facebook.

La gestione della telefonia fissa utilizza di un sistema centralino digitale, di cui si prevede l'implementazione. E' affidata alla ditta ESSEPI TELEFONIA.

PARTE IIa – LE COMPONENTI TECNOLOGICHE

CAPITOLO 1. Data Center e Cloud

L'utilizzo del cloud è rafforzato e indirizzato sia alla razionalizzazione delle risorse ICT, sia a nuove modalità di erogazione dei servizi digitali. In questo senso trova collocazione l'attività di AgID per qualifica dei servizi cloud forniti alla PA. Dal 1 aprile 2019 le PA utilizzano gli specifici servizi del contratto quadro Consip (SPC Cloud Lotto 1) o i Poli Strategici Nazionali (PSN) o esclusivamente servizi cloud qualificati

Obiettivi e risultati attesi

Si ritiene prioritario il passaggio al cloud del maggior fornitore di procedure per quanto esposto nei capitoli precedenti. I server saranno oggetto di una trattativa con tempistiche più allungate.

Cosa deve fare l'Amministrazione

Stante la comunicazione di Agid sulla nostra infrastruttura è impossibile aggiornare o acquistare dei macchinari o rinnovare dei server in uso e l'obiettivo a medio lungo termine è trasferire i dati in cloud.

Per comprendere meglio le tipologie di cloud disponibili sono necessarie due precisazioni:

Il cloud prevede quattro tipologie di servizio:

• Infrastructure as a Service (IaaS): Modello di servizio cloud. La facoltà fornita al consumatore è quella di acquisire elaborazione, memoria, rete e altre risorse fondamentali di calcolo, inclusi sistemi operativi e applicazioni. Il consumatore non gestisce né controlla l'infrastruttura cloud sottostante, ma controlla sistemi operativi, memoria, applicazioni ed eventualmente, in modo limitato, alcuni componenti di rete (esempio firewall).

• Platform as a Service (Paas): Modello di servizio cloud. La facoltà fornita al consumatore è quella di distribuire sull'infrastruttura cloud applicazioni create in proprio oppure acquisite da terzi, utilizzando linguaggi di programmazione, librerie, servizi e strumenti supportati dal fornitore. Il consumatore non gestisce né controlla l'infrastruttura cloud sottostante, compresi rete, server, sistemi operativi, memoria, ma ha il controllo sulle applicazioni ed eventualmente sulle configurazioni dell'ambiente che le ospita.

• Public cloud (cloud pubblico): Modello di deployment su infrastruttura che eroga servizi cloud destinati ad un portafoglio di clienti generico (non predefinito).

• SaaS (Software as a Service): Tra i modelli di servizio offerti dalle piattaforme di cloud computing, il Software as a Service (SaaS) identifica la classe di servizi fully-managed in cui il gestore del servizio (CSP) si occupa della predisposizione, configurazione, messa in esercizio e manutenzione dello stesso (utilizzando un'infrastruttura cloud propria o di terzi), lasciando al fruitore del servizio (PA) il solo ruolo di utilizzatore delle funzionalità offerte.

L'altra precisazione è che la Pubblica Amministrazione è obbligata a fruire solo di fornitori (CSP) che si sono certificati Agid nel marketplace appositamente creato. Il vantaggio della piattaforma cloud è la delega al fornitore della gestione dell'infrastruttura e quindi agli aggiornamenti di sistema, al

mantenimento delle macchine e all'aggiornamento del software. La Pubblica Amministrazione oltre al risparmio delle spese di raffreddamento e di elettricità una volta affidato il servizio al cloud è svincolata dall'obbligo di mantenimento delle infrastrutture sia hardware che software, della fase della continuità operativa e dell'obbligo di backup.

Per fare questa manovra di passaggio in cloud è necessario suddividere ulteriormente le fasi delle operazioni ponendo l'attenzione sui seguenti segmenti interni alla rete informatica comunale:

• Area della posta elettronica

• Area del software operativo gestionale

• Area dei server di gestione del dominio e attività similari

• Area dello spazio condiviso o dati utenti.

• La gestione del software gestionale è più complessa perché abbiamo diversi fornitori di software. La parte software è gestita da server virtuali con licenza HYPER-V su server Microsoft. Tranne rare eccezioni (ad esempio la conservazione sostitutiva che è già in cloud Saas) tutte le altre sono residenti sui server comunali. Obiettivo del dell'Amministrazione è di ridurre se non eliminare la parte residente per spostare su cloud gli applicativi. L'impegno sarà rivolto ai fornitori di software installato che, tra l'altro, distribuiscono già un cloud certificato Agid. Nel capitolo successivo delle tempistiche si proporrà un piano di intervento mentre per i software rimasti si cercherà di traslare in cloud oppure di inseguire una strategia di comparazione con altre piattaforme se il fornitore stesso non sarà in grado di spostare gli applicativi in modalità Saas anche perché la norma impone di non fare più rinnovi con procedure non in cloud.

• Gli accessi utenti, i controller di rete, i backup e la parte relative alle policy aziendali risiedono su server virtuali all'interno dell'Ente. In questo caso si valuterà lo spostamento dei server con tempistiche più graduali e si valuterà caso per caso la convenienza delle operazioni da effettuare.

• Gli utenti comunali usufruiscono di un ambiente condiviso e protetto da policy di gruppo per il deposito e la condivisone di files. Tale repertorio, che è destinato ad aumentare di spazio con il passare del tempo, sarà oggetto di uno spostamento in cloud. Per tale operazione è necessario avvalersi di una struttura certificata Iaas.

CAPITOLO 2. Connettività

In raccordo con il Piano Nazionale Banda Ultra Larga e con la strategia di razionalizzazione delle risorse ICT della PA, è necessario che le PA incrementino la loro connettività alla rete e razionalizzino le spese per la connettività attraverso l'utilizzo delle gare SPC. Va inoltre garantita l'interconnessione dei territori a SPC e la connettività per le sedi estere della PA.

Obiettivi e risultati attesi

Aumento banda internet e vpn: 2023

Videosorveglianza: secondo specifici piani operativi in relazione alle esigenze di sicurezza. Completato nel 2020 il sistema di videosorveglianza agli accessi della Città.

La connettività è la base per fornire un adeguata struttura per il passaggio al cloud e va gestita in priorità.

Cosa deve fare l'Amministrazione

L'infrastruttura comunale gestita con una modalità denominata "rete a stella" per quel che riguarda gli uffici con centro stella al piano superiore dell'Ente. La connessione ad internet è a 100Mbit bilanciata.

I recenti sviluppi di emergenza sanitaria, che hanno portato molti utenti ad utilizzare lo smart working e il relativo e prossimo passaggio al cloud delle procedure informatiche spingono ad una ridondanza delle linee all'interno della sede informatica comunale. Questa configurazione garantisce il passaggio al cloud e sfrutterà in maniera ottimale le connessioni in entrata ed uscita dal comune per una fruizione ottimale delle richieste digitali.

CAPITOLO 3. Modello di interoperabilità

Continuano ad essere proposti i temi dell'interoperabilità e della cooperazione tra sistemi informativi. Con a disposizione adeguate infrastrutture di rete (indispensabili per utilizzare il cloud) è possibile sviluppare una nuova interoperabilità per il colloquio tra sistemi, per esempio tra la protocollazione di pratiche e applicativi gestionali di sportello al cittadino (SUE, SUAP), per assicurare una completa circolazione dei dati nel rispetto della protezione dei dati personali.

È evidente che un adeguato sviluppo di un sistema di interoperabilità a livello nazionale è la base per l'efficienza delle procedure digitali e per il raggiungimento dello scopo già indicato in precedenza di once only.

Obiettivi e risultati attesi

integrazione API altre procedure o cloud come da candidatura PNRR nella misura 1.3.1

Il passaggio delle altre procedure software è un problema che verrà affrontato dopo un collaudo e una formazione operativa sul cloud. Solo allora si potrà ragionare su integrazione con l'esistente attraverso web services o API o passaggio diretto al cloud. Allo stesso tempo occorre lavorare sulla interoperabilità tra programmi all'interno dell'Ente; tra le priorità, con previsione entro l'anno 2022:

- automatismo di invio al SUAP/SUE istanze pervenute al protocollo informatico;

- revisione strutturazione web Amministrazione Trasparente

- definizione standard dimensionale di invio istanze digitali

- condivisione d'utilizzo applicativo gestione cimiteriale

--sportello del cittadino.

Cosa deve fare l'Amministrazione

In una prospettiva di pianificazione a medio lungo termine è fondamentale impegnarsi in un'ottica di interoperabilità tra applicazioni. Come accennato nel capitolo dell'esistente, il Comune di Cavallermaggiore ha la maggior parte delle procedure acquistate a titolo di licenza. Alcune procedure sono slegate le une dalle altre salvo rare eccezioni di collegamento.

Il modello operativo indicato da AGID è quello delle API (Application Programming Interface) e dei web services intesi quest'ultimi come una particolare modalità con cui realizzare API. I modelli di interazione di Agid possono essere ti tipo human-to-machine o machine-to-machine con varie declinazioni. Per fare un esempio concreto, l'invio degli Ordinativi di Pagamento Informatici (OPI) al gateway Siope+ di Banca d'Italia è una interazione A2A (Amministrazione verso Amministrazione) in modalità human-to-machine, perché l'Ufficio Finanziario ha a disposizione un software per controllare, firmare e inviare gli ordinativi mentre un esempio di concatenazione funzionale di interoperabilità machine-to-machine è rappresentato dal ciclo della fatturazione elettronica passiva.

L'applicazione concreta del modello di interoperabilità e del corretto approccio Api first troverà il suo naturale ambito nella progressiva acquisizione di servizi SaaS dal Cloud Marketplace AgID in sostituzione delle installazioni software on premise e in futuro lo scambio di informazioni dovrà avvenire su logiche aperte e standard pubblici che garantiscano ad altri attori, pubblici e privati, accessibilità e massima interoperabilità di dati e servizi, evitando integrazioni ad hoc.

CAPITOLO 4. Piattaforme

Attraverso l'utilizzo delle Piattaforme si favorisce l'attuazione di un modello uniforme di interazione per i servizi realizzati dalla PA per i cittadini e le imprese. Le piattaforme abilitanti sollevano le Amministrazioni dalla necessità di dover acquistare e/o realizzare funzionalità comuni a più sistemi software, semplificando la progettazione, riducendo i tempi e i costi di realizzazione di nuovi servizi e garantendo maggiore sicurezza informatica. Le piattaforme abilitanti consentono alle PA di gestire i procedimenti in modo più efficace e veloce e di dialogare in maniera più efficiente tra di loro, con minore richiesta di informazioni a cittadini ed imprese (principio once only). Fra le piattaforme citiamo ad esempio CIE, SPID, l'app IO, ANPR, PagoPA.

Obiettivi e risultati attesi

IO, PAGO PA, accesso tramite CIE, SPID: secondo disposizioni normative.

Naturalmente PagoPa e accessi tramite SPID, nonché l'utilizzo di IO, costituiscono la priorità. Sono già stati fatti investimenti a riguardo L'attivazione di IO sarà valutata in corso d'opera e a seconda degli aspetti normativi e di settore.

Piattaforma PND

Piattaforma PDND.

Cosa deve fare l'Amministrazione

Il Comune di Cavallermaggiore non intende aggiungere postazioni per la carta di identità elettronica, ritenendo le tre postazioni idonee al momento alle richieste.

Avendo già aderito ad ANPR ad ottobre del 2018 ed essendo già attivo il SIOPE+ l'obiettivo si sposta sull'attivazione dello SPID / IO e su altri servizi di pagamento con PAgoPa.

L'attivazione dello SPID su alcuni nostri servizi è in realtà attivo tramite applicazioni di terze parti, l'obiettivo è quello di uniformare le richieste e fornire un accesso ai servizi tramite SPID.

Per quel che riguarda i servizi da attivare su PagoPa sono in implementazione le tipologie di servizio da rendere fruibili. Analogamente è stato predisposto il servizio di pagamento delle multe del codice della strada che avverrà tramite una piattaforma on line

E' in programma di attuare l'interoperabilità con le piattaforme PDN/PDND.

CAPITOLO 5. Sicurezza informatica

La sicurezza ha un'importanza fondamentale in quanto garantisce la disponibilità, l'integrità, la riservatezza delle informazioni proprie del Sistema informativo della PA e la resilienza della complessa macchina amministrativa. Inoltre la sicurezza informatica è direttamente collegata ai principi di privacy previsti dall'ordinamento giuridico. Le misure minime di sicurezza forniscono alle PA indicazioni puntuali su come raggiungere livelli di sicurezza prefissati a partire da quello minimo ed è obbligatorio per tutti.

Obiettivi e risultati attesi

- sicurezza in cloud

- miglioramento Firewall e VPN

Sulla sicurezza informatica si è investito negli anni passati, e quindi l'obiettivo, in attesa di nuovi sviluppi (vedi aggiornamento alle misure standard), è quello di traslare in cloud il software utilizzato per il monitoraggio e la ricerca delle vulnerabilità. È implicito un miglioramento della sicurezza dell'ente spostando le procedure e quindi i server obsoleti (che ridiventerebbero attuali spostando il sevizio) in cloud. Se il lavoro agile o smart working dovesse continuare con numeri importanti vale la pena considerare un miglioramento prestativo dei firewall di rete, dei collegamenti in vpn anche con doppia autenticità e di una "sandbox" o di dispositivi di sicurezza per il controllo sul cloud delle operazioni.

Cosa deve fare l'Amministrazione

Il regolamento informatico ha posto le basi per definire una guida operativa per l'utilizzo delle attrezzature informatiche. Dal punto di vista della sicurezza è basata sulle misure minime di sicurezza emanate da Agid sotto l'egida di Cert-Pa recentemente raggruppato in CSIRT (Computer security incident response team).

L'Ente si avvale di un software antivirus centralizzato su cloud che monitora e controlla e programma gli aggiornamenti dei singoli pc e dei server che avviene in maniera silente su tutte le macchine del

dominio comunale e che si occupa della gestione dell'inventario dei beni informatici, e per il monitoraggio delle infrastrutture.

Obiettivo a medio lungo termine dell'ufficio è migliorare la gestione del software di gestione della sicurezza per razionalizzare la spesa e trasferire in cloud l'applicazione che adesso è gestita in locale.

Altro obiettivo è la gestione dello smart working è stata implementata con dei portatili comunali in collegamento vpn SSL con un client installato sul portatile e collegamento in RDP sul pc dell'infrastruttura comunale. Potrebbe essere una valutazione da fare, se il metodo di lavoro da casa dovesse continuare anche successivamente all'emergenza epidemiologica in atto, di potenziare la sicurezza con autenticazione a due fattori.

CAPITOLO 6. Strumenti per la generazione e la diffusione dei servizi digitali

Cittadini e imprese accedono preferenzialmente attraverso interfacce digitali ai servizi online, interoperabili e decentralizzati, messi a disposizione dalla PA. A tal proposito è stata sviluppata la piattaforma Designers Italia che è dedicata all'aggiornamento di linee guida, strumenti e kit di sviluppo front-end per siti web della PA per avere un'unica struttura ed è attiva l'app chiamata "IO" per la gestione unificata dei servizi online delle PA.

Obiettivi e risultati attesi

Caricamento elenco pratiche edilizie (ove occorra attraverso esternalizzazione) pregresse, avvio digitalizzazione archivio pratiche edilizie mediante investimenti annuali (avvio nel 2023);

Informatizzazione procedure elettorali

Sportello digitale.

Cosa deve fare l'Amministrazione

Il piano, nel breve periodo, prevede la valutazione del nuovo servizio di sportello virtuale che permetterebbe al cittadino o all'azienda di interagire con l'Amministrazione direttamente dalla propria sede ed ottenere i certificati richiesti in formato digitale.

Il personale del servizio informatico vuole apprendere, tramite formazione, la creazione di istanze per i servizi on line in modo da essere autonomo alla creazione di qualsiasi servizio di richiesta online o di modificare quelli già presenti.

Anche per altre procedure potrebbero essere necessari momenti di incontro formativo, per elevare il livello di conoscenza dello strumento informatico.

PARTE IIIa - La governance

CAPITOLO 7. Governance

I processi di transizione digitale in cui sono coinvolte le Amministrazioni richiedono visione strategica, capacità realizzativa ed efficacia della governance. Con il Piano Triennale per l'Informatica nella PA, nel corso di questi ultimi anni, visione e metodo sono stati declinati in azioni concrete e condivise, in raccordo con le Amministrazioni Centrali e Locali e attraverso il coinvolgimento dei Responsabili della Transizione al Digitale che rappresentano l'interfaccia tra AGID e le Pubbliche Amministrazioni. I cambiamenti che hanno investito il nostro Paese negli ultimi due anni, anche a causa della crisi pandemica, sono stati accompagnati da una serie di novità normative e da nuove opportunità che hanno l'obiettivo di dare un'ulteriore spinta al processo di trasformazione digitale già iniziata. Il Piano Triennale, in questo contesto, si pone come strumento di sintesi tra le differenti linee di trasformazione digitale della Pubblica Amministrazione. Tra queste va data rilevanza a quella rappresentata dal Piano Nazionale di Ripresa e Resilienza (PNRR), inserita nel programma Next Generation EU (NGEU). In particolare, la Missione 1 del PNRR si pone l'obiettivo di dare un impulso decisivo al rilancio della competitività e della produttività del Sistema Paese affidando alla trasformazione digitale un ruolo centrale. Lo sforzo di digitalizzazione e innovazione è centrale in questa Missione, ma riguarda trasversalmente anche tutte le altre. In questo mutato contesto obiettivi e azioni del Piano triennale, dunque, non possono che essere definiti e individuati in accordo con le indicazioni del PNRR. Da questo punto di vista, è importante evidenziare che il Decreto-Legge 31 maggio 2021 n. 77 c.d. "Semplificazioni" (come convertito con la Legge n. 108/2021) contiene disposizioni in ordine all'organizzazione della gestione del Piano Nazionale di Ripresa e Resilienza, definendo i ruoli ricoperti dalle diverse Amministrazioni coinvolte nonché le modalità di monitoraggio del Piano e del dialogo con le autorità europee.

La prima parte del decreto-legge, in particolare, ha definito, con un'articolazione a più livelli, la governance del Piano Nazionale di Ripresa e Resilienza (PNRR). La responsabilità di indirizzo del Piano è assegnata alla Presidenza del Consiglio dei Ministri. Viene istituita una Cabina di regia, presieduta dal Presidente del Consiglio dei Ministri, alla quale partecipano di volta in volta i Ministri e i Sottosegretari competenti in ragione delle tematiche affrontate in ciascuna seduta. La Cabina di regia esercita poteri di indirizzo, impulso e coordinamento generale sull'attuazione degli interventi del PNRR. Va sottolineato, inoltre, che lo stesso decreto-legge con l'articolo 41 - che introduce l'articolo 18-bis del Codice dell'Amministrazione Digitale - prevede un articolato procedimento sanzionatorio per le Pubbliche Amministrazioni per le violazioni degli obblighi in materia di transizione digitale.

In particolare, l'articolo prevede che AGID eserciti poteri di vigilanza, verifica, controllo e monitoraggio sul rispetto delle disposizioni del Codice dell'Amministrazione Digitale e di ogni altra norma in materia di innovazione tecnologica e digitalizzazione della Pubblica Amministrazione, comprese quelle contenute nelle Linee guida e nel Piano triennale per l'Informatica nella Pubblica Amministrazione. Al riguardo, l'Agenzia con un apposito Regolamento, disciplinerà le procedure di "contestazione, accertamento, segnalazione e irrogazione delle sanzioni" in caso di violazioni della norma.

Consolidamento del ruolo del Responsabile per la Transizione al digitale

Anche per la realizzazione delle azioni del Piano triennale 2021-2023 la figura del RTD ha un ruolo centrale non solo come interfaccia tra AGID, Dipartimento per la Trasformazione Digitale e Amministrazioni, ma all'interno dell'Amministrazione stessa come motore dei processi di cambiamento e innovazione. Continua ed è rafforzato anche il processo di collaborazione tra gli RTD attraverso un modello di rete che possa stimolare il confronto, valorizzare le migliori esperienze, la condivisione di conoscenze e di progettualità e la promozione di azioni di coordinamento tra le Pubbliche Amministrazioni, sia nell'ambito dei progetti e delle azioni del Piano Triennale per l'Informatica nella PA, sia nell'ambito di nuove iniziative che maturino dai territori.

Il monitoraggio del Piano triennale

Il monitoraggio del Piano triennale si compone delle seguenti attività:

● misurazione dei risultati (R.A.) conseguiti dal sistema PA per ciascuna componente tecnologica e non tecnologica del Piano;

● verifica dello stato di avanzamento dell'attuazione delle linee d'azione (L.A.) da parte delle PA centrali e locali componenti il panel di riferimento del Piano stesso;

● analisi della spesa e degli investimenti pubblici in ICT delle PA centrali e locali componenti il panel.

Con la finalità di ottenere una visione delle attività svolte dalle Amministrazioni in relazione alla loro coerenza con il Piano triennale con la possibilità di introdurre azioni correttive necessarie per il raggiungimento degli obiettivi previsti.

I target 2020 rappresentano le baseline del sistema di monitoraggio rispetto alle quali verificare gli avanzamenti successivi.

I dati e le informazioni raccolti come baseline del sistema di monitoraggio permettono, abbinati alla logica di aggiornamento (rolling) annuale del Piano triennale, di intervenire tempestivamente per inserire correttivi sia sulla catena Obiettivo Risultato Atteso-Target sia sulle relative roadmap di Linee di Azione. Allo stesso tempo, tali azioni di monitoraggio e verifica hanno l'obiettivo di supportare l'attuazione fisica, finanziaria e procedurale del Piano triennale nel suo complesso.

La prossima edizione del Piano triennale, anche in previsione dell'attuazione delle linee progettuali del PNNR, prevede un maggiore allineamento tra gli indicatori e gli obiettivi del Piano stesso e gli strumenti di misurazione e monitoraggio adottati dalla Commissione Europea ovvero oltre al Digital Economy and Society Index (DESI) e l'eGovernment Benchmark Action Plan, i più recenti Digital Compass 2030 e il Berlin Declaration Monitoring Mechanism.

Format Piano Triennale

Le Pubbliche Amministrazioni, secondo la roadmap definita dalle Linee d'Azione nel Piano triennale e le modalità operative fornite da AGID, saranno chiamate a compilare il "Format PT" per le PA così da rendere possibile la costruzione e l'alimentazione della base dati informativa. Tale Format ricalca la struttura obiettivi-azioni del Piano triennale ed è stato definito al fine di:

● rendere uniforme i Piani triennali ICT dei diversi enti;

● semplificare le attività di redazione di ciascuna Amministrazione;

● comprendere e monitorare con maggiore efficacia come sono state recepite dalle PA le azioni previste all'interno del Piano triennale;

● approfondire quali altre azioni sono state individuate localmente per il conseguimento dei singoli obiettivi previsti nel Piano triennale.

Contesto normativo e strategico

Decreto Legislativo 7 marzo 2005, n. 82: «Codice dell'Amministrazione Digitale» e s.m.i..

• 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.

• DPCM 24 gennaio 2013: «Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale».

• 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 D.Lgs. n. 82/2005».

• 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 D.Lgs.n. 82/2005».

• 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.

• 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».

• 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 D.Lgs. n. 82/2005».

• DPR 28 dicembre 2000, n. 445: "Disposizioni legislative in materia di documentazione amministrativa, di seguito «Testo unico», e la gestione informatica dei documenti".

• Regolamento UE n° 910/2014 – eIDAS (electronic IDentification Authentication and Signature).

• 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.

• D.Lgs. n. 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 D.Lgs. 14 marzo 2013, n. 33, ai sensi dell'art. 7 della Legge 7 agosto 2015, n. 124, in materia di riorganizzazione delle Amministrazioni Pubbliche".

• Regolamento UE 679/2016 (trattamento e circolazione dei dati personali).

• D.Lgs.n. 179/2016: “Modifiche e integrazioni al Codice dell'Amministrazione Digitale, di cui al D.Lgs. 7 marzo 2005, n. 82, ai sensi dell'art. 1 della Legge 7 agosto 2015, n. 124, in materia di riorganizzazione delle Amministrazioni Pubbliche" (CAD 3.0).

• DPCM 31 maggio 2017: “Piano Triennale 2017-2019 per l'informatica nella Pubblica Amministrazione”.

• D.Lgs.13 dicembre 2017, n. 217: “Disposizioni integrative e correttive al D.Lgs. 26 agosto 2016, n. 179, concernente modifiche ed integrazioni al Codice dell'Amministrazione Digitale, di cui al D.Lgs. 7 marzo 2005, n. 82, ai sensi dell'art. 1 della Legge 7 agosto 2015, n. 124, in materia di riorganizzazione delle Amministrazioni Pubbliche.

• Linee Guida per il Disaster Recovery (DR) delle PA HYPERLINK "http://www.agid.gov.it/sites/default/files/repository_files/linee_guida/linee-guida-dr.pdf" in data 23/03/2018.

• Caratterizzazione dei sistemi cloud per la Pubblica Amministrazione HYPERLINK "http://www.agid.gov.it/sites/default/files/repository_files/linee_guida/sistemi_cloud_pa.pdf" in data 23/03/2018.

• Circolare N. 2 del 9 aprile 2018: “Criteri per la qualificazione dei Cloud Service Provider per la PA”.

• Circolare n. 3 del 9 aprile 2018: “Criteri per la qualificazione di servizi SaaS per il Cloud della PA”

• Determinazione AgID n. 419/2020 del 22 settembre 2020 - Chiarimenti applicativi in merito alle Circolari AgID nn. 2 e 3 del 9 aprile 2018, recanti i criteri per la qualificazione dei Cloud Service Provider per la PA e dei servizi SaaS per il Cloud della PA.

• Linee guida di design per i servizi digitali della PA HYPERLINK "http://www.agid.gov.it/sites/default/files/repository_files/design-italia.pdf" in data 13/06/2018.

• Circolare n. 3 del 1 ottobre 2018: “Responsabile per la Transizione al Digitale”;

• 12 febbraio 2019 “Piano triennale 2019 – 2021 per l'informatica nella Pubblica Amministrazione”.

• 03 febbraio 2020 Ultimo aggiornamento del “Piano triennale 2019 – 2021 per l'informatica nella Pubblica Amministrazione”.

• DCPM dell’8 marzo 2020: “Ulteriori disposizioni attuative del D.L. 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.

• Determinazione AgID. 157/2020: Emanazione delle Linee Guida per la sottoscrizione elettronica di documenti ai sensi dell’art. 20 del CAD (Linee Guida SPID 23 marzo 2020).

• 19 maggio 2020 - Linee guida sulla sicurezza nel procurement ICT.

• Determinazione AgID 404 del 9 settembre 2020 - Linee Guida sulla formazione, gestione e conservazione dei documenti informatici, in vigore dal 10 settembre 2020.

• D.L. n. 76/2020 convertito in Legge n. 120/2020: “Misure urgenti per la semplificazione e l'innovazione digitale”, che recepiscono le nuove linee guida.

• Decreto Ministeriale 21 luglio 2020: *«Strategia nazionale per le competenze digitali».*

- 20 luglio 2020 – Linee guida sull'accessibilità degli strumenti informatici.
- 14 agosto 2020: «Piano Triennale dell'Informatica 2020/2022».
- Decreto Legge 31 maggio 2021, n. 77: «Governance del Piano Nazionale di Ripresa e Resilienza e prime misure di rafforzamento delle strutture amministrative e di accelerazione e snellimento delle procedure».
- Maggio 2021 – Linee guida sulla formazione, gestione e conservazione dei documenti informatici.

Obiettivi e risultati attesi

Il piano Agid nella sua declinazione per gli Enti Locali individua delle macro aree di intervento che in maniera sintetica e non esaustiva si possono elencare nelle seguenti:

• Data Center e Cloud

• Connettività

• Modello di interoperabilità

• Piattaforme

• Sicurezza informatica

• Strumenti per la generazione e la diffusione dei servizi digitali.

Il piano Agid deve essere attuato dal Responsabile per la Transizione al Digitale, dagli uffici preposti, compresi gli uffici di parte finanziaria e dal DPO e si basa su due principi fondanti: digital by default e once only ovvero le Amministrazioni forniscono servizi digitali come opzione predefinita e le PA dovrebbero evitare di chiedere informazioni già in loro possesso a cittadini e imprese. Quest'ultimo principio viene reiterato per l'ennesima volta e quindi come tale è certamente il più sfidante.

Cosa deve fare l'Amministrazione

Con la stesura di questo piano l'Ente ha pensato ad un percorso per quella che ritiene la direzione da seguire, secondo le indicazioni Agid, per migliorare i servizi rivolti agli utenti e per garantire sicurezza nel trattamento dei dati secondo le normative GDPR e di transazione delle stesse. Il piano è una base che può essere migliorato, cambiato e ridefinito a seconda delle opportunità, delle normative e delle necessità che nel corso del triennio verranno ad affrontarsi ma la strada da seguire è tracciata e definitiva.

Nel piano non sono state considerate le eccezioni o le richieste particolari che dovranno essere vagliate opportunamente. Ad esempio il Comune sta ancora attrezzando la ripresa e del consiglio comunale e in tal caso sono stati necessari investimenti hardware (videocamere, registratori, ecc.) per una fruizione ottimale del consiglio. L'effettiva quantificazione dei software, hardware e attivazioni da intraprendere, costituiranno oggetto di specifica condivisione e confronto tra Amministrazione e servizi finanziari unitamente all'Amministratore di Sistema, secondo le priorità indicate dall'Amministrazione.

APPENDICE 1. Definizioni e acronimi

Ai fini del presente piano s'intende per:

• 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 funzioni (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. È 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 Cavallermaggiore.

• 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 della mansione lavorativa.

- 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.

• SPCCloud: 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 HYPERLINK 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.

APPENDICE 2. 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/

Garante privacy https://www.garanteprivacy.it/

Regione Piemonte https://www.regione.piemonte.it/web/

Guida_Rapida_SPID_Dipartimento_Trasformazione_digitale;

Guida_Rapida_pagoPA_Dipartimento_Trasformazione_digitale;

Guida_Rapida_CIE_Dipartimento_Trasformazione_digitale;

Guida_Rapida_App_IO_Dipartimento_Trasformazione_digitale)