LA TRANSIZIONE DIGITALE TRA PNRR, PIANO TRIENNALE DELL'INFORMATICA E RIFORMA DEL CAD

Le principali azioni in carico alle amministrazioni locali

CLAPp s.r.l.
FINANZA AGEVOLATA E CONSULENZA PER IMPRESE E P.A.

Normativa di riferimento

- decreto legislativo 7 marzo 2005, n. 82 Codice dell'Amministrazione Digitale **(CAD)**
- **Piano triennale** per l'informatica nella Pubblica Amministrazione 2020-2022;
- **Linee Guida** dell'Agenzia per l'Italia Digitale regole tecniche di cui all'art. 71 CAD («Formazione, gestione e conservazione dei documenti informatici» approvate con determina dirigenziale n. 404/2020 e pubblicate il 10 settembre 2020);
- **PNRR** (Piano Nazionale di Ripresa e Resilienza) **Componente 1 "Digitalizzazione, innovazione e sicurezza nella PA**" compresa nella Missione 1 "Digitalizzazione, innovazione, competitività, cultura e turismo"

Gli obiettivi nel Piano Triennale 2020 – 2022

Previsto dal **CAD** (art. 14-bis, lettera b)

Per attuare la strategia nazionale, come previsto dal Piano triennale per l'informatica nella PA e ribadito dalla circolare del Ministero della pubblica amministrazione n. 3 del 2018, ogni **amministrazione deve predisporre** un proprio documento strategico: **il Piano triennale ICT**.

Oltre ad essere un obbligo, la redazione del piano triennale per l'informatica dell'ente è fondamentale per organizzare tutte le attività relative all'attuazione della transizione digitale dell'ente; è **adottato dall'organo di vertice dell'ente su proposta del dirigente dell'Ufficio responsabile per la transizione al digitale**.

La programmazione del Piano Triennale per l'Informatica deve essere resa **coerente** con la specifica allocazione di azioni nelle Missioni e Programmi del Documento Unico di Programmazione (DUP).

Deve individuare le possibili azioni di reingegnerizzazione volte alla digitalizzazione dei servizi e dei processi e coordinarsi con il **Piano organizzativo per il lavoro agile** (POLA) e con il **Piano della Performance (ora con il PIAO)**.

Il Piano 2020-2022, approvato con Dpcm del 17 luglio 2020, introduce un'importante innovazione rispetto ai piani precedenti con riferimento ai destinatari degli obiettivi individuati per ciascuna delle tematiche affrontate. Saranno infatti le singole amministrazioni a dover **realizzare gli obiettivi** elencati. Altro elemento innovativo è il forte accento posto sulla **misurazione dei risultati**: sono state introdotte specifiche attività di monitoraggio.

I principi guida del Piano

- digital & mobile first (digitale e mobile come prima opzione)
- digital identity only (accesso esclusivo mediante identità digitale)
- cloud first (cloud come prima opzione)
- Servizi pubblici digitali inclusivi e accessibili
- dati pubblici un bene comune
- interoperabile by design: i servizi pubblici devono essere progettati in modo da funzionare in modalità integrata e senza interruzioni in tutto il mercato unico esponendo le opportune API;
- sicurezza e privacy by design: i servizi digitali devono essere progettati ed erogati in modo sicuro e garantire la protezione dei dati personali;
- user-centric, data driven e agile: le PA sviluppano i servizi digitali, prevedendo modalità agili di miglioramento continuo, partendo dall'esperienza dell'utente e basandosi sulla continua misurazione di prestazioni e utilizzo;
- once only: le PA devono evitare di chiedere ai cittadini e alle imprese informazioni già fornite;
- transfrontaliero by design (concepito come transfrontaliero): le PA devono rendere disponibili a livello transfrontaliero i servizi pubblici digitali rilevanti;
- codice aperto: le pubbliche amministrazioni devono prediligere l'utilizzo di software con codice aperto e, nel caso di software sviluppato per loro conto, deve essere reso disponibile il codice sorgente

Il ruolo del responsabile per la transizione al digitale (RTD)
Le funzioni previste dall'art. 17 del CAD

coordinamento strategico dello sviluppo dei sistemi informativi di telecomunicazione e fonia

indirizzo, pianificazione, coordinamento e monitoraggio della sicurezza informatica relativamente ai dati, ai sistemi e alle infrastrutture anche in relazione al sistema pubblico di connettività, nel rispetto delle regole tecniche

accesso dei soggetti disabili agli strumenti informatici e promozione dell'accessibilità anche in attuazione di quanto previsto dalla legge 9 gennaio 2004, n. 4

analisi periodica della coerenza tra l'organizzazione dell'amministrazione e l'utilizzo delle tecnologie dell'informazione, al fine di migliorare la soddisfazione dell'utenza e la qualità dei servizi nonché di ridurre i tempi e i costi dell'azione amministrativa

Il ruolo del responsabile per la transizione al digitale (RTD)
Le funzioni previste dall'art. 17 del CAD

progettazione e coordinamento delle iniziative rilevanti ai fini di una più efficace erogazione di servizi in rete a cittadini e imprese mediante gli strumenti della cooperazione applicativa tra pubbliche amministrazioni ivi inclusa la predisposizione e l'attuazione di accordi di servizio

promozione delle iniziative attinenti l'attuazione delle direttive impartite dal Presidente del Consiglio dei Ministri o dal Ministro delegato per l'innovazione e le tecnologie

pianificazione e coordinamento del processo di diffusione dei sistemi di identità e domicilio digitale, posta elettronica, protocollo informatico, firma digitale o firma elettronica qualificata e mandato informatico, e delle norme in materia di accessibilità e fruibilità nonché del processo di integrazione e interoperabilità tra i sistemi e servizi dell'amministrazione e quello di cui all'articolo 64-bis (App IO)

pianificazione e coordinamento degli acquisti di soluzioni e sistemi informatici, telematici e di telecomunicazione al fine di garantirne la compatibilità con gli obiettivi di attuazione dell'agenda digitale e, in particolare, con quelli stabiliti nel piano triennale

Il ruolo del responsabile per la transizione al digitale (RTD)
Gli ulteriori “poteri” previsti dalla Circolare n. 3/2018

Costituire gruppi tematici per singole attività e/o adempimenti (attivazione servizi App IO, gestione documentale…)

Proporre atti di indirizzo nelle materie di propria competenza (in materia di approvvigionamento di beni e servizi ICT…)

predisporre il Piano triennale per l’informatica della singola amministrazione, nelle forme e secondo le modalità definite dall’Agenzia per l’Italia digitale, nonché la relazione annuale sull’attività svolta dall’Ufficio da trasmettere al vertice politico o amministrativo che ha nominato il RTD

Strumenti di raccordo e consultazione tra il RTD e soggetti interni all'amministrazione

il **Responsabile della gestione documentale** (**DPR 28 dicembre 2000, n. 445** art. 61 co. 2; DPCM 3 dicembre 2013, art. 4 – figura chiave per la dematerializzazione dei processi cui spetta predisporre il Manuale di gestione documentale

il **Responsabile per la protezione dei dati personali** (art. 37 del **Regolamento (UE) 2016/679**): figura chiamata ad assolvere funzioni di supporto e controllo, consultive, formative e informative relativamente all'applicazione della **normativa in materia di protezione dei dati personali**. Il coordinamento con il RTD è fondamentale per lo sviluppo di sistemi informativi e servizi online conformi ai principi *data protection by default* e *by design*

il **Responsabile della prevenzione della corruzione e della trasparenza** (**legge 190/2012**, art. 1, co. 7 come modificato dal **d.lgs. 97/2016**): la collaborazione tra le due figure è in questo caso essenziale per garantire che l'applicazione delle tecnologie ai processi di riorganizzazione dell'ente rispondano ad adeguate caratteristiche di **trasparenza** e ai principi dell'amministrazione aperta

Le responsabilità dirigenziali e disciplinari

Art. 12 comma 1 ter CAD

I dirigenti rispondono **dell'osservanza ed attuazione delle disposizioni di cui al presente Codice** ai sensi e nei limiti degli articoli 21 e 55 del decreto legislativo 30 marzo 2001, n. 165, ferme restando le eventuali responsabilità penali, civili e contabili previste dalle norme vigenti. L'attuazione delle disposizioni del presente Codice è comunque rilevante ai fini della misurazione e valutazione della performance organizzativa ed individuale dei dirigenti

Art. 18-*bis* ***(Violazione degli obblighi di transizione digitale)***

inserito nel decreto decreto-legge 31 maggio 2021 n. 77 (art. 41), che introduce il tema della necessità di sanzioni al fine di assicurare l'attuazione dell'Agenda digitale italiana ed europea, la digitalizzazione dei cittadini, delle pubbliche amministrazioni e delle imprese, con specifico riferimento alla realizzazione degli obiettivi fissati dal Piano nazionale di ripresa o di resilienza

Le responsabilità dirigenziali e disciplinari

- **Responsabilità civile e penale**

Nel caso in cui, a causa della mancata nomina del RTD, della scorretta gestione documentale, della mancata adozione di adeguate misure di sicurezza, mancata attivazione dello SPID ecc., sia stato prodotto un danno a terzi;

- responsabilità amministrativo-contabile per il danno erariale arrecato alla PA

In tutti i casi in cui il rispetto delle previsioni di legge consentirebbe notevoli risparmi (acquisto di strumenti informatici non conformi, ricorso alle comunicazioni analogiche…)

- responsabilità disciplinare per violazione degli obblighi previsti dalla legge (così, ad es., in caso di inosservanza delle disposizioni in materia di accessibilità), dal codice di comportamento o dalle direttive impartite

- responsabilità dirigenziale per il solo personale dirigenziale che non raggiunga i risultati posti o si discosti dalle direttive impartite

Le sanzioni

È prevista una **riduzione del 30 per cento** della retribuzione di risultato e del trattamento accessorio collegato alla *performance* e il divieto di attribuire premi e incentivi, ai dirigenti responsabili, in caso di:

- violazione delle disposizioni di cui agli artt. 64, comma 3-bis e 64-bis del CAD in materia di accesso telematico ai servizi online (SPID, CIE e appIO);

- Violazione dell'obbligo di adottare i pagamenti online con il nodo nazionale dei pagamenti – PagoPA;

- progettazione, realizzazione e sviluppo di servizi digitali e sistemi informatici in violazione del codice di condotta tecnologica di cui all'art. 13-bis del CAD;

- inadempimento dell'obbligo di rendere disponibili i dati di cui all'art. 50 del CAD;

- inadempimento dell'obbligo di accreditarsi presso la Piattaforma Digitale Nazionale Dati (PDND) di cui all'art. 50 ter del CAD

Le responsabilità dirigenziali e disciplinari. Il ruolo dell'AgID

AgID vigila sul rispetto delle norme in materia di innovazione e digitalizzazione della p.a., ivi comprese quelle contenute nelle Linee guida e nel Piano triennale per l'informatica, e procede, d'ufficio ovvero su segnalazione del difensore civico digitale, **all'accertamento delle relative violazioni** da parte degli enti locali.

Nell'esercizio dei poteri di vigilanza, verifica, controllo e monitoraggio, l'AgID richiede e acquisisce dati, documenti e ogni altra informazione strumentale e necessaria. La mancata ottemperanza alla richiesta di dati, documenti o informazioni o la trasmissione di informazioni o dati parziali o non veritieri è punita con applicazione della sanzione amministrativa pecuniaria nel minimo di euro 10.000 e nel massimo di euro 100.000

AgID, ove accerti la sussistenza delle violazioni contestate, assegna al trasgressore un congruo termine perentorio, proporzionato rispetto al tipo e alla gravità della violazione, per conformare la condotta agli obblighi previsti dalla normativa vigente, segnalando le violazioni all'ufficio competente per i procedimenti disciplinari di ciascuna amministrazione, nonché ai competenti organismi indipendenti di valutazione

Le violazioni accertate dall'AgID rilevano ai fini della misurazione e della valutazione della performance individuale dei dirigenti responsabili e comportano responsabilità dirigenziale e disciplinare

Le responsabilità dirigenziali e disciplinari. Il ruolo del difensore civico digitale

Articolo 17, comma 1-*quater* del CAD

Chiunque può presentare al difensore civico per il digitale (attraverso apposita area presente sul sito istituzionale dell'AgID) segnalazioni relative a presunte violazioni del Codice e di ogni altra norma in materia di digitalizzazione ed innovazione della pubblica amministrazione da parte di pubbliche amministrazioni.

Ricevuta la segnalazione, il difensore civico, se la ritiene fondata, invita il soggetto responsabile della violazione ad avviare, tempestivamente e comunque non oltre trenta giorni, le attività necessarie a porvi rimedio e a concluderle entro un termine perentorio indicato tenendo conto della complessità tecnologica delle attività richieste.

Le decisioni del difensore civico sono pubblicate in un'apposita area del sito Internet istituzionale. Il difensore segnala le inadempienze all'ufficio competente per i procedimenti disciplinari di ciascuna amministrazione. Il mancato avvio delle attività necessarie a porre rimedio e il mancato rispetto del termine perentorio per la loro conclusione rileva ai fini della misurazione e della valutazione della performance individuale dei dirigenti responsabili e comporta responsabilità dirigenziale e disciplinare.

Gli obiettivi nel Piano Triennale 2020 – 2022

Servizi

- Migliorare la capacità di generare ed erogare servizi digitali
- Migliorare l'esperienza d'uso e l'accessibilità dei servizi

Dati

- 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
- Aumentare la consapevolezza sulle politiche di valorizzazione del patrimonio informativo pubblico e su una moderna economia dei dati

Piattaforme

- Favorire l'evoluzione delle piattaforme esistenti per migliorare i servizi offerti a cittadini ed imprese semplificando l'azione amministrativa
- Aumentare il grado di adozione ed utilizzo delle piattaforme abilitanti esistenti da parte delle pubbliche amministrazioni
- Incrementare e razionalizzare il numero di piattaforme per le amministrazioni al fine di semplificare i servizi ai cittadini

Infrastrutture

- Migliorare la qualità e la sicurezza dei servizi digitali erogati dalle amministrazioni locali favorendone l'aggregazione e la migrazione sul territorio
- Migliorare la qualità e la sicurezza dei servizi digitali erogati dalle amministrazioni centrali favorendone l'aggregazione e la migrazione su infrastrutture sicure ed affidabili
- Migliorare la fruizione dei servizi digitali per cittadini ed imprese tramite il potenziamento della connettività per le PA

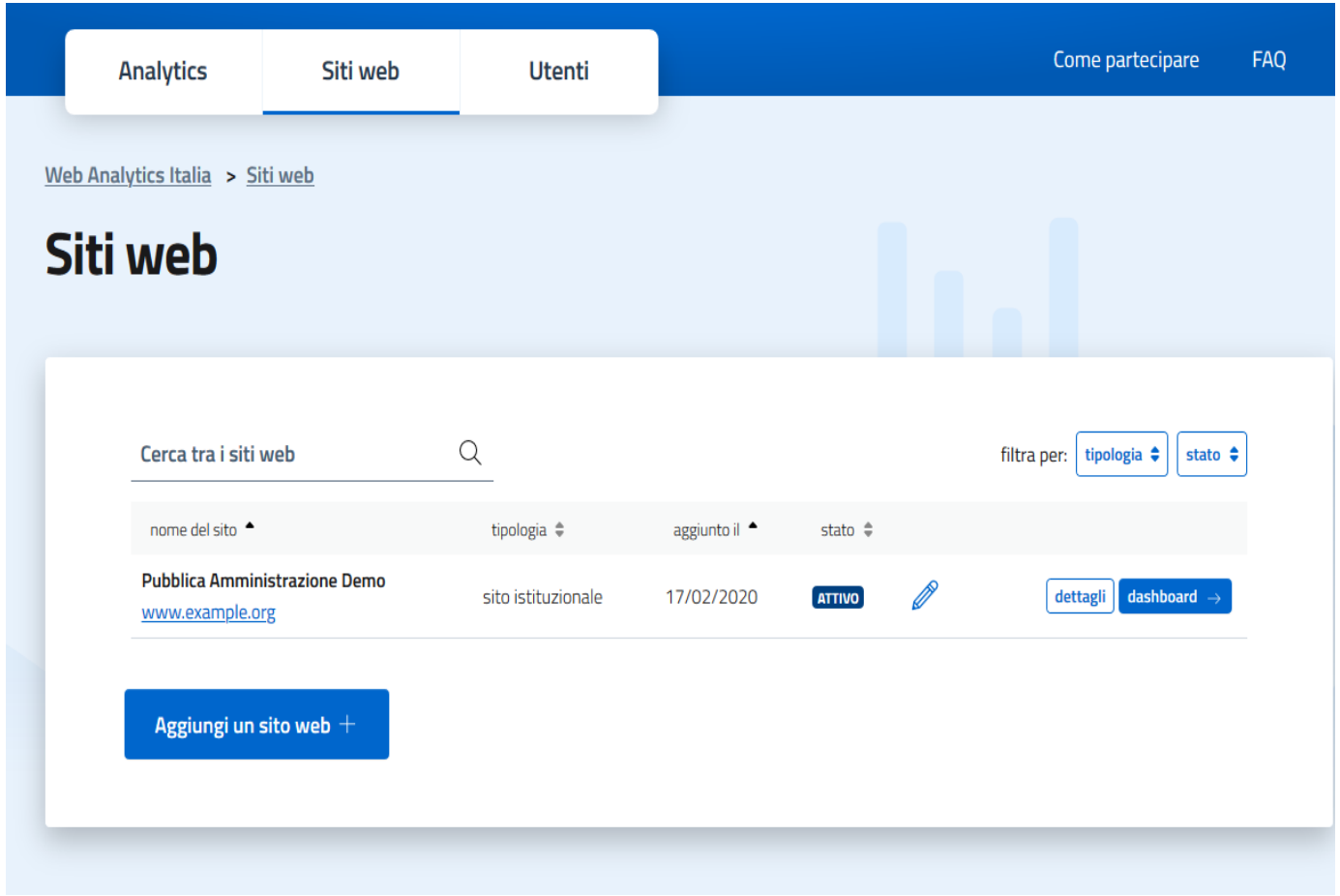
Interoperabilità

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

Sicurezza

- Aumentare la consapevolezza del rischio cyber (Cyber Security Awareness) nelle PA
- Aumentare il livello di sicurezza informatica dei servizi digitali

Finalizzazione dell’adesione a Web Analytics Italia per migliorare il processo evolutivo dei servizi on line



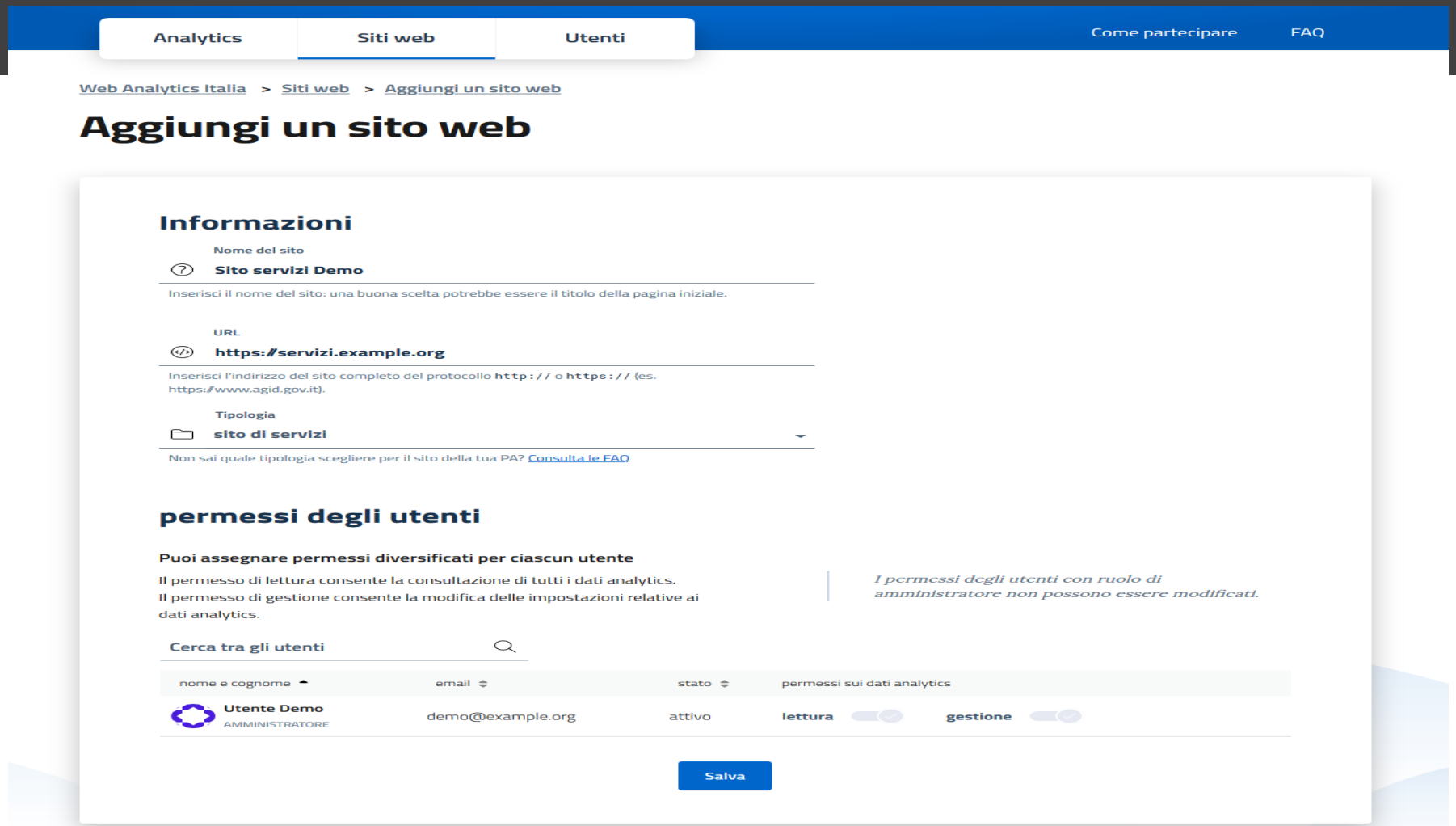
Web Analytics Italia (WAI) è una piattaforma che offre le statistiche in tempo reale dei visitatori dei siti della Pubblica Amministrazione, fornendo agli operatori dei report dettagliati. WAI aiuta le amministrazioni a comprendere il comportamento degli utenti online.

Per accedere alla piattaforma WAI è necessario usare un'identità SPID. Dopo l'autenticazione, va inserito l'indirizzo del sito web istituzionale, cioè quello indicato su IndicePA. Solo in un secondo momento sarà possibile aggiungere, eventualmente, anche altri siti web. WAI invierà per e-mail il codice di tracciamento relativo al sito web, che andrà inserito all'interno della struttura del sito; il codice consente al sistema di tracciare le visite e numerosi altri dati relativi al comportamento dei visitatori

Guida utente Web Analytics

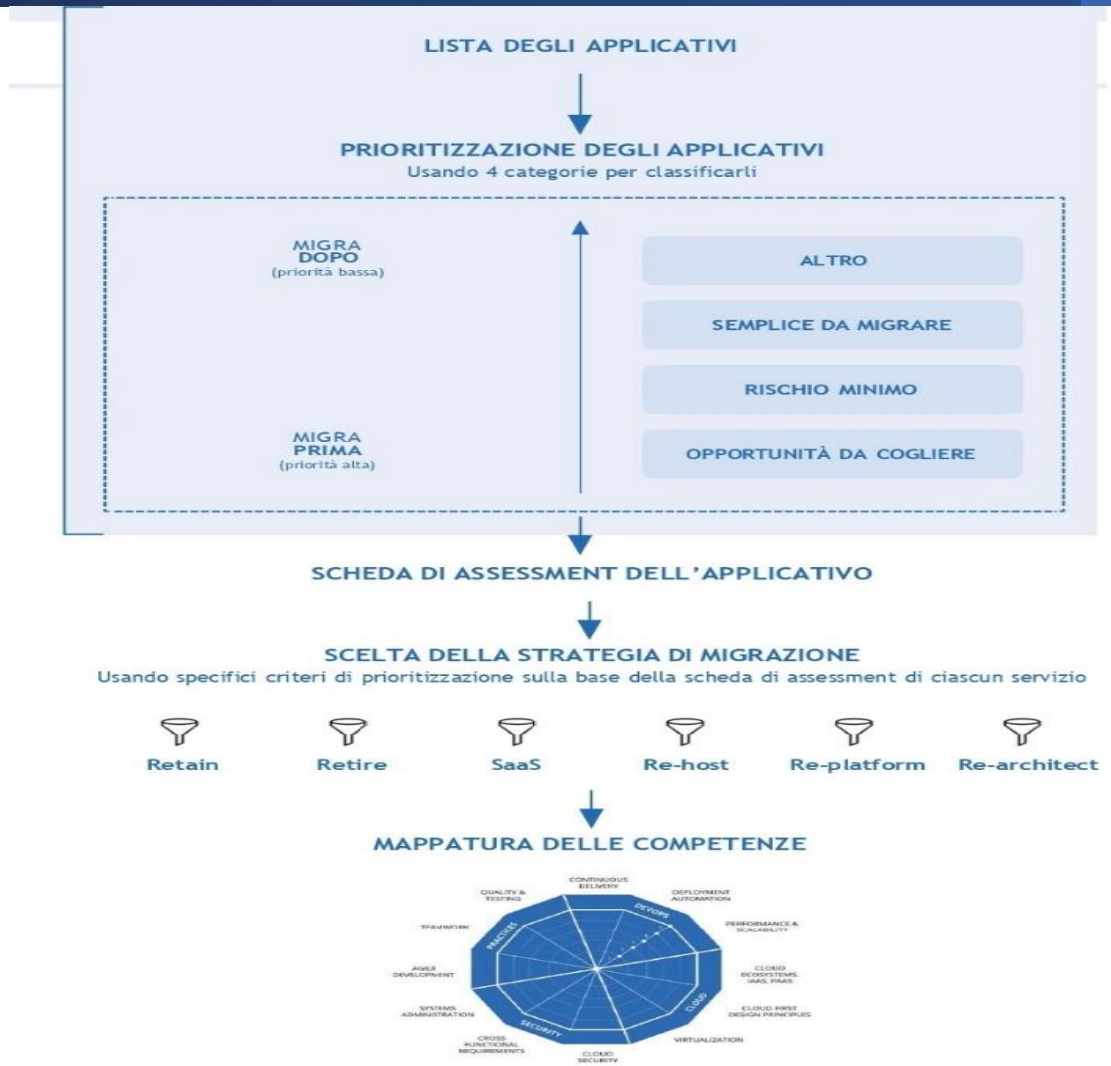
https://docs.italia.it/AgID/wai/wai-user-guide-docs/it/stabile/index.html

Finalizzazione dell’adesione a Web Analytics Italia per migliorare il processo evolutivo dei servizi on line



Applicazione dei principi Cloud First - SaaS First

Adesione al programma di abilitazione al cloud e trasmissione ad Agid degli elaborati previsti dalla fase di assessment e avvio fasi successive



Adeguamento delle procedure di procurement al CAD (artt. 68 e 69) e alle Linee Guida AGID sull'acquisizione e il riuso del software per la Pubblica Amministrazione

Fase 1.1: Analisi del fabbisogno

Fase 1.2: Individuazione dei vincoli economici (disponibilità di bilancio) e temporali (tempi per la messa in esercizio)

Fase 1.3: Redazione del documento descrittivo delle esigenze

Fase 2.1: Ricerca soluzioni riusabili per la PA presenti all'interno della piattaforma Developers Italia (https://developers.italia.it)

Fase 2.2: Valutazione soluzioni riusabili per la PA

Fase 2.3: Approvvigionamento della soluzione riusabile per la PA

Fase 2.4: Ricerca soluzioni Open Source

Fase 2.5: Valutazione soluzioni Open Source

Fase 2.6: Approvvigionamento della soluzione Open Source

Fase 2.7: Accertamento impossibilità

Fase 3.1: Ricerca soluzioni proprietarie

Fase 3.2: Studio realizzazione ex novo

Fase 3.3: Comparazione soluzioni proprietarie e realizzazione ex novo

Fase 3.4: Approvvigionamento soluzione proprietaria o realizzazione ex novo

Catalogo

developers.italia.it/it/search?type=software_reuse&sort_by=relevance&page=0#717d52059a3592611ae1954fb106409316da0e65

Piattaforme | Software | API

Come lo uso | Come partecipo | News | Contatti

Catalogo software

Cerca

TIPOLOGIA 1

- (○) Tutto
- (○) Software Open Source
- (●) Software A Riuso

CATEGORIE

- [ ] Accounting
- [ ] Agile Project Management
- [ ] Applicant Tracking
- [ ] Application Development
- [ ] Appointment Scheduling

AMBITO DI APPLICAZIONE

- [ ] Agriculture
- [ ] Culture
- [ ] Defence
- [ ] Education
- [ ] Emergency Services

STATO DI SVILUPPO

- [ ] Concept

187 risultati

Ordina per Rilevanza

SOFTWARE A RIUSO

COMUNWEB Sito web comunale

Comunweb

Il sito web comunale

SOFTWARE A RIUSO

GasPlanetService

Calcolo una tantum e ricerca del gestore per comune

SOFTWARE A RIUSO

Portale delle valutazioni ambientali VAS-VIA-AIA

Portale delle valutazioni

SOFTWARE A RIUSO

REGIONE DEL VENETO

Sistema documentale di gestione dell'Educazione Continua in Medicina (ECM)

Nei procedimenti di acquisizione di beni e servizi ICT, le PA devono far riferimento alle Linee guida di *design*

I servizi pubblici digitali devono rispettare i principi elencati all'art. 53 del CAD: Le pubbliche amministrazioni realizzano siti istituzionali su reti telematiche che rispettano i principi di accessibilità, nonché di elevata usabilità e reperibilità

- inserire nei **contratti di gara** per lo sviluppo dei siti web l'indicazione di aderenza alle linee guida sull'accessibilità degli strumenti informatici emanate da AGID
- garantire la **protezione dei dati personali**, nello sviluppo di un sito web o di un servizio digitale, fin dalla progettazione
- rispettare almeno il **livello base di sicurezza** stabilito dalle «Misure minime di sicurezza ICT per le pubbliche amministrazioni
- pubblicare, sul singolo sito, **l'informativa sul trattamento** dei dati personali e chiedere il consenso laddove necessario, anche con riferimento all'uso dei cookie
- provvedere a inserire i trattamenti di dati personali nel **Registro dei trattamenti** e nominare Responsabili del trattamento ai sensi dell'art. 28 del GDPR gli eventuali fornitori dei servizi web che trattano dati personali per conto del soggetto titolare
- **mappare le funzioni** (user stories) del servizio e creare un prototipo da testare per validare la soluzione progettuale e la sua usabilità
- condurre interviste e **test di usabilità** per comprendere se i servizi digitali esistenti corrispondono alle esigenze degli utenti

Comunicazione ad AGID, tramite apposito form *online*, dell'esito dei test di usabilità del proprio sito istituzionale

I test di usabilità sono delle sessioni di osservazione diretta dell'interazione tra un utente e un servizio digitale. I test vengono svolti individualmente, assegnando all'utente uno o più task da svolgere, e analizzando il suo comportamento nel portarli a termine.

Vedi https://designers.italia.it/kit/usability-test/ - il portale mette a disposizione il seguente materiale:

a) Guida alla conduzione dei test di usabilità. Protocollo che contiene le istruzioni e le domande aperte da chiedere durante l'intervista - Vai alla risorsa

b) Liberatoria per la conduzione di un test di usabilità. Modello di liberatoria per richiedere il consenso dei partecipanti alla registrazione - Vai alla risorsa

c) Template per il calcolo delle valutazioni dei test basato sul Net Promoter Score - Vai alla risorsa

d) Questionario SUS. Template dedicato alla compilazione di un questionario SUS (System Usability Scale) - Vai alla risorsa

e) Domande UMUX Lite. **Modello di valutazione** alternativo al questionario SUS - Vai alla risorsa

Comunicazione ad AGID, tramite apposito form *online*, dell’esito dei test di usabilità del proprio sito istituzionale

Sintetizzare le conclusioni in maniera strutturata per presentarle agli altri stakeholder di progetto e produrre una relazione ad-hoc.

- Relativamente a questa fase, il portale mette a disposizione il seguente materiale:

a) Tabella dei risultati. Template dove riportare gli esiti dei task dei partecipanti al test di usabilità - **Vai alla risorsa**

b) Report dei risultati. Indicazioni operative sulla costruzione di un report relativo ai risultati dei test - **Vai alla risorsa**

c) Comunicazione degli esiti dei test di usabilità. Il form ufficiale dell'Agenzia per l'Italia Digitale dedicato alla comunicazione degli esiti dei test - **Vai alla risorsa**

Pubblicazione, tramite l'applicazione form.agid.gov.it, della dichiarazione di accessibilità per i siti web e per le APP mobili Linee Guida sull'accessibilità degli strumenti informatici – AGID

Il documento aggiorna tutta la parte regolamentare in materia di accessibilità dalla prima emanazione della Legge Stanca L.4/2004 recependo anche i dettami della **Direttiva Europea n. 2016/2102** in materia di accessibilità dei siti web e delle applicazioni (APP).

Le principali novità del documento riguardano:

- i **requisiti tecnici** di accessibilità;
- le **metodologie tecniche per la verifica** dell'accessibilità dei siti web e delle applicazioni mobili;
- il modello della **dichiarazione di accessibilità**;
- le particolari circostanze che possono consentire l'invocazione **dell'onere sproporzionato**;
- la metodologia di **monitoraggio e valutazione** della conformità dei siti e delle APP.

Linee Guida sull'accessibilità degli strumenti informatici – AGID

Secondo le nuove disposizioni **le PA dovranno:**

- effettuare le **verifiche dell'accessibilità degli strumenti informatici** (siti web e APP), al fine di valutarne lo stato di conformità;
- compilare e pubblicare, a cura del Responsabile della Transizione al Digitale, una **dichiarazione di accessibilità**;
- predisporre un **meccanismo di feedback** per ricevere le segnalazioni dagli utenti del sito.

La Dichiarazione di accessibilità è lo strumento attraverso il quale le Amministrazioni rendono pubblico lo stato di accessibilità di ogni sito web e applicazione mobile di cui sono titolari.

La dichiarazione viene redatta e pubblicata utilizzando l'applicazione online https://form.agid.gov.it, realizzata da AGID nel rispetto del modello stabilito dalla Direttiva UE 2016/2102 (Allegato 1 delle Linee Guida). L'applicazione si compone di due macro-sezioni.

La prima sezione presenta i contenuti in ottemperanza alla Decisione di esecuzione UE 2018/1523:

- Stato di conformità;
- Dichiarazione di contenuti, sezioni e funzioni non accessibili, in caso di non conformità parziale o totale;
- Indicazione del Meccanismo di feedback e recapiti dell'amministrazione;
- Procedura di attuazione (Difensore Civico Digitale).

Linee Guida sull’accessibilità degli strumenti informatici – AGID

La seconda sezione invece è composta da:

- Informazioni sul sito / applicazione mobile;
- Informazioni sull’amministrazione.

La prima Dichiarazione di accessibilità per i siti web doveva essere pubblicata dalle Amministrazioni entro il 23 settembre 2020, mentre per le applicazioni mobili la scadenza è il 23 giugno 2021.

Entro il 23 settembre di ogni anno il soggetto erogatore riesamina e valida l'esattezza delle affermazioni contenute nella dichiarazione di accessibilità, avvalendosi esclusivamente dell’applicazione online https://form.agid.gov.it.

Pertanto, la validità di ogni dichiarazione ricopre un periodo temporale che va dal 24 settembre al 23 settembre dell’anno successivo.

La mancata pubblicazione della "dichiarazione" determina un inadempimento normativo, con la responsabilità prevista dall'art. 9 della Legge n. 4/2004.

Pubblicazione degli obiettivi di accessibilità sul proprio sito istituzionale

Le pubbliche amministrazioni hanno l'obbligo di presentare, entro il 31 marzo di ogni anno, gli obiettivi di accessibilità relativi all'anno corrente, come ribadito anche nelle Linee Guida sull'accessibilità degli strumenti informatici.

Sul sito dell'Agenzia per l'Italia digitale è disponibile un'apposita applicazione on-line "Obiettivi di accessibilità" che facilita la redazione e la pubblicazione o degli Obiettivi e consente ad AgID di effettuare il monitoraggio dello stato di attuazione degli Obiettivi.

La procedura prevede i seguenti passaggi:

1. registrazione al sito

2. compilazione degli Obiettivi di accessibilità

3. generazione del link degli Obiettivi (da pubblicare sul sito dell'amministrazione come previsto dalla delibera ANAC 50/2013)

Comunicazione ad AGID, tramite apposito *form online*, dell'uso dei modelli per lo sviluppo web per i propri siti istituzionali

Il modello viene messo a disposizione gratuitamente sulla piattaforma di Designers Italia sotto forma di prototipi hi-fi e template che rappresentano l'esperienza di navigazione del sito nelle versioni desktop e mobile, basati sulle linee guida e sui kit di Designers Italia.

Tutti i comuni, o più in generale la comunità open source e le software house che realizzano le soluzioni web per i comuni, possono usare il kit per i Comuni, comprensivo di architettura dell'informazione e template html, per sviluppare la propria offerta digitale in modo rapido e a basso costo.

L'utilizzo del kit per il design dei siti comunali, che è bene inserire all'interno dei capitolati tecnici in caso di affidamento all'esterno di attività di sviluppo web, permette di attuare le linee guida di design dei siti web della Pubblica Amministrazione.

La comunicazione viene redatta utilizzando l'applicazione online https://form.agid.gov.it.

Le PA uniformano i propri sistemi di metadati e documentano i propri dataset nel catalogo nazionale dati.gov.it
Le PA adottano la licenza aperta di riferimento nazionale, documentandola esplicitamente come metadato

La disponibilità dei dati della pubblica amministrazione è regolata dall'art. 50 del CAD che prevede anche sanzioni per l'inadempimento dell'obbligo di renderli disponibili. Altre normative di riferimento sono l'art. 50 ter CAD che regola il funzionamento della Piattaforma Digitale Nazionale Dati, le Linee guida nazionali per la valorizzazione del patrimonio informativo pubblico e per i cataloghi dati e la Direttiva UE 2013/37 (Direttiva PSI 2.0)

Le Linee guida nazionali per la valorizzazione del patrimonio informativo pubblico propongono una serie di azioni :

- **Verificare la conformità al modello qualitativo per i dati aperti** sul web

Tipologia dati:

livello 1: Dati disponibili tramite una licenza aperta e inclusi in documenti leggibili e interpretabili solo grazie a un significativo intervento umano (e.g., PDF);

livello 2: Dati disponibili in forma strutturata e con licenza aperta. Tuttavia, i formati sono proprietari (e.g., Excel) e un intervento umano è fortemente necessario per un'elaborazione dei dati;

livello 3: Dati con caratteristiche del livello precedente ma in un formato non proprietario (e.g., CSV, JSON, geoJSON). I dati sono leggibili da un programma ma l'intervento umano è necessario per una qualche elaborazione degli stessi;

livello 4: Dati con caratteristiche del livello precedente ma esposti usando standard W3C quali RDF e SPARQL I dati sono descritti semanticamente tramite metadati e ontologie;

livello 5: Dati con caratteristiche del livello precedente ma collegati a quelli esposti da altre persone e organizzazioni (i.e., Linked Open Data). I dati sono detti "linked" per la possibilità di referenziarsi (i.e., "collegarsi") tra loro. Nel referenziarsi, si usano relazioni ("link") che hanno un preciso significato e spiegano il tipo di legame che intercorre tra le due entità coinvolte nel collegamento

Le PA uniformano i propri sistemi di metadati e documentano i propri dataset nel catalogo nazionale dati.gov.it
Le PA adottano la licenza aperta di riferimento nazionale, documentandola esplicitamente come metadato

Corredare i dati con i relativi metadati: La metadatazione ricopre un ruolo essenziale laddove i dati sono esposti a utenti terzi e a software. I metadati, infatti, consentono una maggiore comprensione e rappresentano la chiave attraverso cui abilitare più agevolmente la ricerca, la scoperta, l'accesso e quindi il riuso dei dati stessi.

Livello 1: i dati non sono accompagnati da un'opportuna metadatazione;

Livello 2: i dati sono accompagnati da metadati esterni, (e.g., inclusi nella pagina di download del dataset o in file separati);

Livello 3: i dati incorporano i metadati che li descrivono (I metadati forniscono informazioni relative a un dataset);

Livello 4: dati incorporano i metadati che li descrivono (informazioni relative al singolo dato, quindi col massimo grado di dettaglio possibile).

Rispettare il profilo di metadatazione DCAT-AP_IT : Nel caso di dati geografici, siano essi aperti o non aperti, il profilo di metadatazione da adottare è quello del Repertorio Nazionale dei Dati Territoriali (RNDT), conforme alla direttiva INSPIRE, banca dati di interessa nazionale

Individuare una data governance: Definire una chiara data governance interna con l'individuazione di ruoli e relative responsabilità e assicurarsi che i processi integrino il rilascio di dati aperti e il coinvolgimento degli utenti. All'interno del gruppo di lavoro Open Data è nominato un responsabile o Data Manager

Le PA definiscono al proprio interno una “squadra per i dati” *(data team)*

Il gruppo che promuove l’uso e la diffusione degli Open Data riporta all’interno dell’amministrazione le novità inerenti al mondo dell’Open Government, media e valuta le esigenze di pubblicazione dati in base alle normative di riferimento, e ne cura la razionalizzazione rispetto agli altri processi di apertura del dato. Ha la responsabilità di pianificare e coordinare l’evoluzione continua dell’apertura dei dati nell’amministrazione, nonché dell’infrastruttura IT a supporto.

Si ritiene importante che il responsabile dell’ufficio per la Transizione digitale faccia parte del gruppo di lavoro open data. All’interno del team Open Data è nominato un responsabile. Il responsabile Open Data deve possedere sia le capacità operative di controllo di tale sistema, sia quelle amministrative di coordinamento con i processi già esistenti.

Le PA di piccole dimensioni, come i comuni al di sotto di 5.000 abitanti, possono sfruttare meccanismi di sussidiarietà (ad esempio attraverso le Regioni)

Le Amministrazioni gestori di pubblici servizi adottano le linee guida per l'aggiornamento dei dati in IPA

L'Indice dei domicili digitali delle Pubbliche Amministrazioni e dei gestori di pubblici servizi (art. 6-ter del CAD), indicato con l'acronimo IPA, è l'elenco pubblico contenente i domicili digitali da utilizzare per le comunicazioni e per lo scambio di informazioni e per l'invio di documenti validi a tutti gli effetti di legge tra le pubbliche amministrazioni, i gestori di pubblici servizi e i privati.

Le Linee Guida dell'Indice dei domicili digitali delle Pubbliche Amministrazioni e dei gestori di pubblici servizi prevedono che i soggetti deputati devono:

- istituire almeno una Area Organizzativa Omogenea, associata al proprio registro di protocollo (art. 40-bis del CAD, articoli 50 e 61 del D.P.R. n. 445/2000);

- assegnare ad ogni Area Organizzativa Omogenea almeno un domicilio digitale, che corrisponde all'indirizzo di PEC che deve essere pubblicato su IPA per ciascun registro di protocollo (comma 3 dell'art. 47 del CAD);

- istituire almeno un ufficio di fatturazione elettronica.

Le informazioni da inserire in IPA per facilitare l'individuazione del domicilio digitale e il suo corretto utilizzo, sono strutturate in sezioni: informazioni caratterizzanti l'Ente; informazioni relative al Registro di protocollo; informazioni relative agli uffici, tra i quali quelli istituiti per obbligo di legge.

Le modalità operative per l'utilizzo delle funzionalità rese disponibili dall'IPA sono riportate nelle Guide Operative pubblicate sul sito www.indicepa.gov.it

Le piattaforme abilitanti

Le amministrazioni pubbliche hanno dunque l'obbligo di rendere fruibili tutti i loro servizi anche in modalità digitale e avviare **i progetti di trasformazione digitale entro il 28 febbraio 2021**- e salvo impedimenti, tale fruibilità deve essere pertanto assicurata mediante la applicazione su dispositivi mobili.

La violazione delle disposizioni così dettate comporta una **valutazione negativa della *performance* dirigenziale** (non già responsabilità dirigenziale e disciplinare ai sensi degli articoli 21 e 55 del decreto legislativo n. 165 del 2001), con la conseguente 'sanzione' di una **riduzione non inferiore al 30 per cento** della retribuzione di risultato e del trattamento accessorio collegato alla performance individuale. Si aggiunge il **divieto di attribuire premi** o incentivi nelle medesime strutture.

Si segnala che, in sede di conversione del decreto, è stato introdotto l’art. 23-bis ai sensi del quale le nuove disposizioni in materia di cittadinanza digitale e accesso ai servizi digitali (artt. da 24 a 30 del decreto) sono efficaci nei confronti dei comuni con popolazione inferiore a 5.000 abitanti solo a partire dalla data prevista per la cessazione dello stato di emergenza legato al Covid-19.

Nodo dei pagamenti-SPC o Sistema pagoPA

Tra i diritti di cittadinanza digitale rientra l'art. 5 CAD "**Effettuazione di pagamenti con modalità informatiche**" che **obbliga la pubblica amministrazione** ad accettare, tramite una piattaforma tecnologica per l'interconnessione e l'interoperabilità tra le pubbliche amministrazioni e i prestatori di servizi di pagamento abilitati, messa a disposizione da AGID attraverso il Sistema pubblico di connettività, al fine di assicurare l'autenticazione dei soggetti interessati, **i pagamenti spettanti a qualsiasi titolo attraverso sistemi di pagamento elettronico** senza discriminazione in relazione allo schema di pagamento abilitato per ciascuna tipologia di strumento di pagamento elettronico.

Modalità di adesione Enti Creditori

Modalità di Adesione Enti Creditori

Modalità diretta

L'EC richiede di aderire a pagoPA, indicando i propri dati e nominando il proprio Referente Pagamenti (RP).

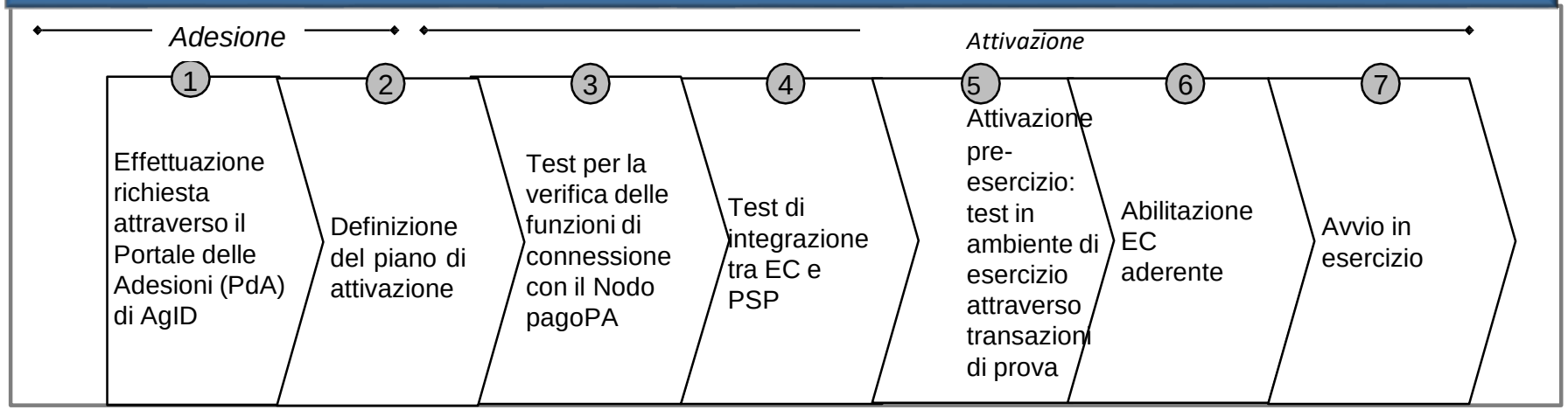
E' lo stesso EC ad avere l'intera responsabilità del progetto ed è titolare dell'interconnessione al Nodo pagoPA, pur potendo utilizzare anche contributi tecnici esterni per la realizzazione del progetto.

Opzionalmente l'EC può nominare anche un proprio Referente Tecnico, se diverso dal RP.

Modalità intermediata

- L'EC richiede di aderire a pagoPA, indicando i propri dati e nominando sia il proprio Referente Pagamenti (RP) sia l'intermediario o partner tecnologico prescelto.
- La responsabilità del progetto viene condivisa tra EC e intermediario/partner titolare dell'interconnessione al Nodo pagoPA.
- L'intermediario/partner deve essere censito da AgID con Referente Tecnico (RT) univoco.

Principali fasi progettuali



SPID (Sistema pubblico per la gestione delle identità digitali e modalità di accesso ai servizi erogati in rete dalle pubbliche amministrazioni)

Le PA e i gestori di pubblici servizi proseguono il percorso di adesione a SPID e PagoPA e dismettono le altre modalità di autenticazione e pagamento associate ai propri servizi *online*

Le PA e i gestori di pubblici servizi interessati adottano lo SPID *by default*

Fondamento della trasformazione digitale è la progettazione di servizi on-line della PA focalizzata sui bisogni dei cittadini/imprese (in un'ottica **digital first**); è per questo che sono state istituite piattaforme abilitanti concepite con al centro l'esperienza utente.
SPID rappresenta, tra le infrastrutture immateriali del Piano triennale per l'informatica nella pubblica amministrazione, la principale piattaforma abilitante per lo sviluppo di servizi digitali innovativi.

SPID è anche uno strumento per la **presentazione di istanze e dichiarazioni** valide alle pubbliche amministrazioni.
Il titolare dell'ufficio competente, che ha ricevuto un'istanza telematica da un soggetto identificato mediante SPID, è tenuto ad avviare il procedimento relativo all'istanza altrimenti questo comporta responsabilità dirigenziale e responsabilità disciplinare.
Le istanze e le dichiarazioni presentate per via telematica da un soggetto identificato tramite SPID hanno lo stesso valore legale di quelle sottoscritte con firma autografa, apposta in presenza del dipendente addetto al procedimento (rif. articolo 65 del CAD, comma 2).

SPID (Sistema pubblico per la gestione delle identità digitali e modalità di accesso ai servizi erogati in rete dalle pubbliche amministrazioni)

SPID altra modalità di sottoscrizione digitale

Nel marzo 2020 AgID ha emanato le Linee Guida che consentono di firmare documenti on-line con SPID, in conformità **all'art. 20 del CAD**
Lo SPID e gli altri strumenti di autenticazione (come la CIE e la CNS) si prestano ad essere utilizzati anche **per creare documenti informatici validi e rilevanti a tutti gli effetti di legge** dando luogo ad un'ulteriore modalità di sottoscrizione digitale. Si tratta di una nuova **tipologia di firma apposta attraverso l'utilizzo dell'identità digitale.** Il processo attraverso il quale si firma tramite SPID deve avvenire con modalità tali da garantire *la sicurezza, l'immodificabilità e l'integrità* del documento stesso oltre *la sua riconducibilità all'autore.*

Anagrafe Nazionale della Popolazione Residente (ANPR)

Tutti i Comuni, progressivamente, potranno utilizzare l’archivio nazionale dei registri dello stato civile contenuto nell’ANPR e verranno integrate nell’ANPR anche le liste elettorali comunali (con dati eventualmente anche divisi per sezione elettorale).

La certificazione telematica, inoltre, sarà esente da imposta di bollo e diritti di segreteria e, in ogni caso, senza oneri per il richiedente.
La certificazione dei dati anagrafici in modalità telematica è assicurata dal Ministero dell'Interno tramite l’ANPR mediante l'emissione di **documenti digitali muniti di sigillo elettronico qualificato**, ai sensi del Regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014.

Anagrafe Nazionale della Popolazione Residente (ANPR) modalità di accesso

- **Web Application (WA)**

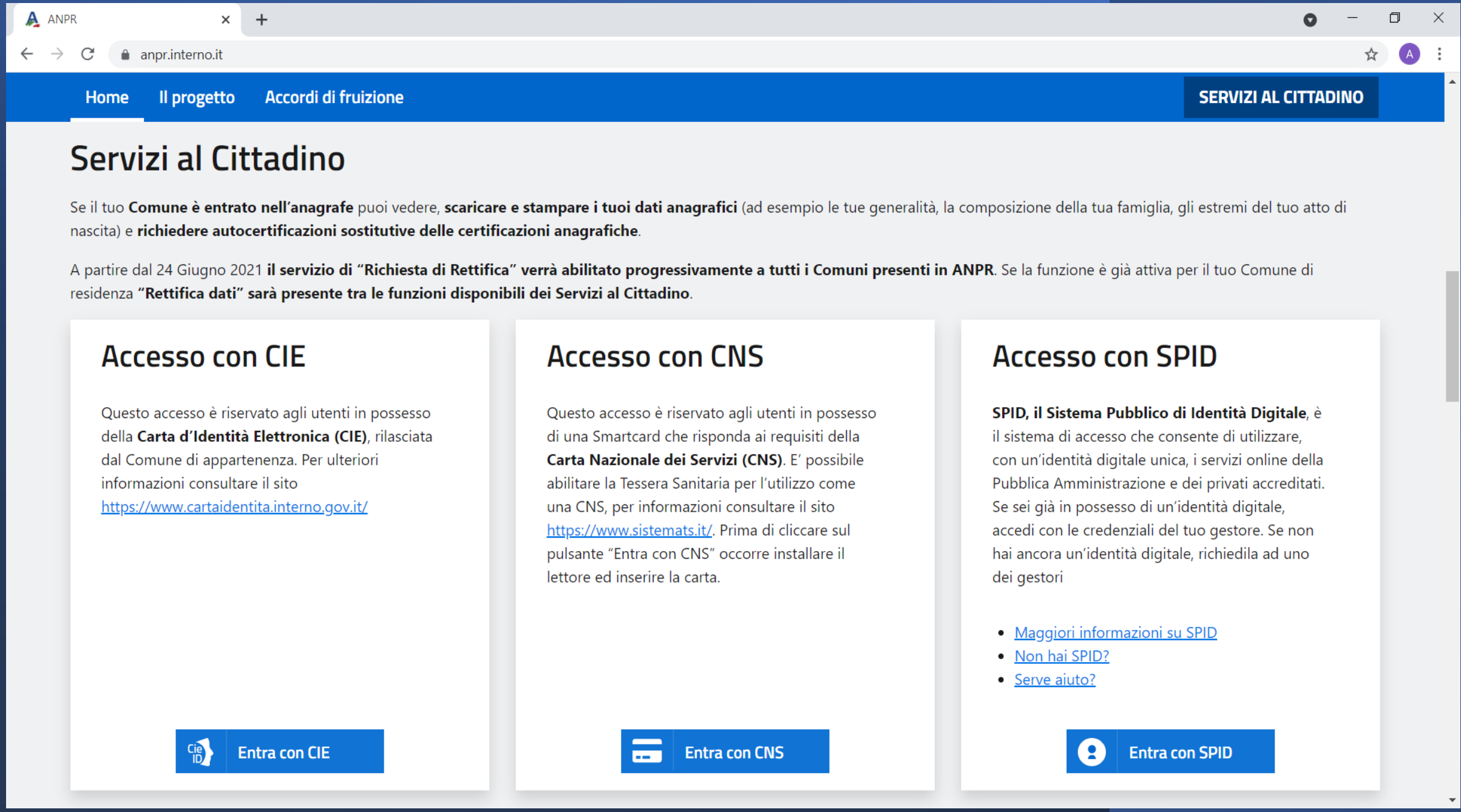
- In questa modalità il Comune non dovrà apportare modifiche al proprio sistema gestionale, in quanto accederà ad una applicazione Web realizzata da Sogei utilizzando le *smart card* nominative ed i certificati di postazione distribuiti prima del subentro definitivo.

- I Comuni potranno allineare le banche dati locali attraverso procedure *batch* (di aggiornamento automatico), messe a disposizione da ANPR, che permettono l'acquisizione periodica delle posizioni anagrafiche di interesse.

Web Service (WS)

In questo caso il Comune deve modificare, prima di dare seguito al subentro definitivo in ANPR, il proprio sistema di gestione anagrafica implementando l'integrazione con ANPR tramite i Web services.

In tale modalità le azioni di allineamento delle banche dati locali sono a carico dei sistema di gestione anagrafica in uso che, comunque, deve assicurare il ruolo di master al database centralizzato di ANPR.


ANPR
anpr.interno.it
Home
Il progetto
Accordi di fruizione
SERVIZI AL CITTADINO
Servizi al Cittadino
Se il tuo Comune è entrato nell'anagrafe puoi vedere, scaricare e stampare i tuoi dati anagrafici (ad esempio le tue generalità, la composizione della tua famiglia, gli estremi del tuo atto di nascita) e richiedere autocertificazioni sostitutive delle certificazioni anagrafiche.
A partire dal 24 Giugno 2021 il servizio di "Richiesta di Rettifica" verrà abilitato progressivamente a tutti i Comuni presenti in ANPR. Se la funzione è già attiva per il tuo Comune di residenza "Rettifica dati" sarà presente tra le funzioni disponibili dei Servizi al Cittadino.
Accesso con CIE
Questo accesso è riservato agli utenti in possesso della Carta d'Identità Elettronica (CIE), rilasciata dal Comune di appartenenza. Per ulteriori informazioni consultare il sito https://www.cartaidentita.interno.gov.it/
Entra con CIE
Accesso con CNS
Questo accesso è riservato agli utenti in possesso di una Smartcard che risponda ai requisiti della Carta Nazionale dei Servizi (CNS). E' possibile abilitare la Tessera Sanitaria per l'utilizzo come una CNS, per informazioni consultare il sito https://www.sistemats.it/. Prima di cliccare sul pulsante "Entra con CNS" occorre installare il lettore ed inserire la carta.
Entra con CNS
Accesso con SPID
SPID, il Sistema Pubblico di Identità Digitale, è il sistema di accesso che consente di utilizzare, con un'identità digitale unica, i servizi online della Pubblica Amministrazione e dei privati accreditati. Se sei già in possesso di un'identità digitale, accedi con le credenziali del tuo gestore. Se non hai ancora un'identità digitale, richiedila ad uno dei gestori
Maggiori informazioni su SPID
Non hai SPID?
Serve aiuto?
Entra con SPID

Le PA si predispongono per interagire con INAD per l’acquisizione dei domicili digitali dei soggetti in essa presenti

L’INAD è l’elenco pubblico contenente i domicili digitali eletti ai sensi dell’articolo 3-bis, commi 1-bis e 1-ter, del CAD destinati alle comunicazioni aventi valore legale effettuate dai soggetti privati o dai soggetti di cui all’articolo 2, comma 2, del CAD e, con riferimento a questi ultimi, altresì alle comunicazioni connesse al conseguimento di finalità istituzionali

Alla data di completamento dell’ANPR, i domicili digitali eletti dalle persone fisiche e iscritti nell’INAD sono trasferiti al Ministero competente, come previsto dal comma 3 del CAD, unitamente a tutti i dati oggetto di tracciamento, al fine di consentire l’accesso alle informazioni relative all’elezione, alla modifica o alla cessazione di ciascun domicilio digitale

Linee Guida – versione 1.0. del 15 settembre 2021, predisposte da AgID (Agenzia Italia digitale) e pubblicate il 20 settembre, con determinazione dirigenziale n. 529/2021

L’APP IO quale strumento di riferimento nei rapporti tra cittadini e PA

Art. 64-bis. Accesso telematico ai servizi della pubblica amministrazione
Le amministrazioni pubbliche hanno l'**obbligo** di rendere fruibili i propri servizi in rete tramite applicazione **su dispositivi mobili** anche attraverso il punto di accesso telematico.

Possono esentare da tale obbligo solo **impedimenti** di natura tecnologica, i quali debbono essere attestati dalla società gestrice della piattaforma tecnologica per l'interconnessione per i pagamenti elettronici, la quale ha assunto il nome "**PagoPA**".

IO è un canale che qualsiasi ente pubblico può utilizzare per inviare comunicazioni ai propri utenti:

- avvisi di pagamento (con possibilità di pagare contestualmente tramite l’app);
- promemoria di scadenze;
- notifiche e aggiornamenti vari

01

Identificazione dei servizi

Identifica **quali** servizi vuoi erogare attraverso IO e prepara i relativi **messaggi**.

TEMPLATE SERVIZI E MESSAGGI

02

Integrazione tecnologica

Registrati al back-office **https://developer.io.italia.it,** e usa le API di IO per sviluppare l'integrazione.

BACK-OFFICE SVILUPPATORI

03

Adempimenti legali

Identifica un **legale rappresentante** dell'ente per gestire adesione al progetto, privacy e security.

BACK-OFFICE ENTI PRESTO DISPONIBILE

04

Comunicazione ai cittadini

Definisci come comunicare ai cittadini che potranno ricevere i tuoi servizi anche tramite l'**app IO**.

KIT COMUNICAZIONE

FASE 2: Predisporre l’integrazione tecnologica

Le comunicazioni di un servizio digitale passano attraverso un’integrazione software (*application to application*).

Significa che l’applicazione con cui il tuo ente gestisce quel servizio deve “parlare” con l’applicazione che gestisce le comunicazioni su IO.

Per integrarsi a IO è necessario:
- associare ad ogni specifico servizio **una *API key***;

- integrare il software con IO, utilizzando le API che consentono l’invio dei messaggi.

FASE 3: Compiere gli adempimenti legali necessari

- fare un ***assessment* dei dati personali** che vengono trattati per ciascun servizio;

- pubblicare **un'informativa privacy** (tipicamente, sul sito web istituzionale dell'ente), che, per ciascun servizio, spieghi al cittadino in modo chiaro che tipo di dati personali vengono trattati da ciascun canale con cui il servizio è erogato, incluso IO;

- sottoscrivere un **accordo** per aderire a IO, che include la definizione del rapporto tra il Team per la Trasformazione Digitale, responsabile dello sviluppo di IO, e l'ente, nonché le modalità di gestione di sicurezza e privacy previste da IO;

- registrarsi all'interno del *back-office* indicando **una o più figure delegate alla gestione dei servizi** del tuo ente su IO e una figura incaricata come **legale rappresentante** dell'ente. Sarà loro compito creare il profilo dell'ente all'interno del sistema di gestione dell'app IO, approvare i servizi predisposti da sviluppatori e partner tecnologici e firmare i documenti legali per l'adesione a IO.

FASE 4: Comunicare la disponibilità dei servizio

Comunicare ai tuoi utenti l’adesione a IO

sezione dedicata ai giornalisti sul sito io.italia.it
Kit di comunicazione per gli enti

Le amministrazioni pubbliche hanno dunque l'obbligo di rendere fruibili tutti i loro servizi anche in modalità digitale e avviare **i progetti di trasformazione digitale entro il 28 febbraio 2021**- e salvo impedimenti, tale fruibilità deve essere pertanto assicurata mediante la applicazione su dispositivi mobili

	**Istruzioni:** 1)Definisci l'elenco dei servizi che vuoi gestire attraverso IO, completando la lista qui sotto. 2)Per ogni servizio, prepara i messaggi usando il Template Messaggi che trovi in questo documento. 3)Prendi spunto dagli Esempi Messaggi.

Elenco Servizi	Messaggi da inviare
Servizio 1 (Es. pass mobilità)	Messaggio 1 (es. avviso scadenza)
	Messaggio 2 (es. notifica di ingresso in area ZTL)
	Messaggio 3
	...
Servizio 2 (Es. TARI)	Messaggio 1 (es. promemoria di pagamento TARI)
	Messaggio 2 (es. avviso di accertamento TARI)
	Messaggio 3
	...
Servizio 3 (Es. Fascicolo previdenziale)	Messaggio 1 (es. stato di avanzamento di una domanda)
	Messaggio 2 (es. riepilogo situazione contributiva
	Messaggio 3
	...

Infrastrutture

Le PA proprietarie di *data center* di gruppo B richiedono **l'autorizzazione ad AGID per le spese** in materia di *data center e* **trasmettono ad AGID i piani di migrazione** verso i servizi *cloud* qualificati da AGID –

- Manuale di abilitazione al Cloud
- Per accompagnare la migrazione della PA al cloud centrale fornito dal PSN, è previsto nel PNRR anche un programma di supporto e incentivo per trasferire basi dati e applicazioni, in particolare rivolto alle amministrazioni locali (Investimento 1.2: Abilitazione e facilitazione migrazione al Cloud). Le amministrazioni potranno scegliere all'interno di una lista predefinita di provider certificati secondo criteri di adeguatezza rispetto sia a requisiti di sicurezza e protezione, sia a standard di performance. Il supporto sarà realizzato con "pacchetti" completi che includeranno competenze tecniche e risorse finanziarie.
- team MITD, incaricato di censire e certificare i fornitori idonei per ogni attività della trasformazione e, successivamente, di predisporre pacchetti/moduli standard di supporto
- Per le PA locali minori verrà resa obbligatoria l'aggregazione in raggruppamenti ad hoc per l'esecuzione dell'attività di trasformazione/migrazione

Governare la trasformazione digitale

Adesione alla piattaforma di community dei RTD

Le PAL procedono – anche in forma aggregata - alla nomina formale del RTD.

Le PA che hanno nominato il RTD aderiscono alla piattaforma di *community e* partecipano all'interscambio di esperienze anche fornendo contributi per l'individuazione di *best practices*

rafforzare il processo di collaborazione tra i RTD attraverso un modello di rete che possa stimolare il confronto, valorizzare le migliori esperienze e la condivisione di conoscenze e di progettualità

Le PA, attraverso i propri RTD, partecipano alle *survey* periodiche sui fabbisogni di formazione del personale, in tema di trasformazione digitale

Le PA aggiornano i piani di azione secondo quanto previsto nel Piano strategico nazionale per le competenze digitali "Competenze digitali per la PA" Dipartimento della Funzione Pubblica che mette a disposizione una piattaforma e contenuti formativi rivolti ad amministrazioni differenziate per dimensioni e tipo di attività svolta

Home / Syllabus

Competenze digitali

Il Syllabus

Dati, informazioni e documenti informatici

Il Syllabus

Il Syllabus "Competenze digitali per la PA" è il documento che descrive l'insieme

Tipo di test

Il test è di tipo adattivo in funzione del livello di padronanza rilevato (**base, intermedio, avanzato**)

Domande

Il test contiene da un minimo di **5** ad un massimo di **15** domande.

Ogni domanda presenta 4 risposte alternative di cui una sola è corretta.

Durata

Il test ha una durata variabile fino a un massimo di **15 minuti**.

Il tempo massimo per ogni domanda è di **60** secondi.

Le competenze digitali

Dati, informazioni e documenti informatici

Comunicazione e condivisione

Sicurezza

Le PA partecipano alle attività di monitoraggio predisponendosi per la misurazione delle baseline dei Risultati Attesi del Piano secondo le modalità definite da AGID e Dipartimento per la Trasformazione Digitale

Il monitoraggio del PT prevede e integra 3 livelli che complessivamente concorrono al raggiungimento dell'obiettivo sopra indicato:

• monitoraggio della realizzazione delle Linee di Azione in capo ai singoli *owner* identificati: misurato attraverso indicatori di tipo on/off rispetto alle *roadmap* operative definite nel PT per ciascun obiettivo ad integrazione dell'insieme agli indicatori presenti nel cruscotto di monitoraggio Avanzamento Digitale; il SAL rispetto alle *roadmap* viene tracciato e raccolto in maniera sistematica attraverso un Format PT per le PA;

• monitoraggio dei risultati conseguiti complessivamente dal Piano triennale: misurato attraverso gli indicatori quali-quantitativi, i Risultati Attesi individuati per ciascun Obiettivo del PT, che compongono il sistema di monitoraggio degli obiettivi del Piano, basato sulle *source* già individuate e quelle in fase di implementazione;

• monitoraggio dell'andamento della spesa e degli investimenti ICT in coerenza con PT: misurati attraverso la rilevazione periodica della spesa ICT, da integrare alla raccolta dati e informazioni tramite il Format PT per le PA

Linee Guida sulla formazione, gestione e conservazione dei documenti informatici – AGID

Le linee guida **aggiornano** le regole vigenti in materia di formazione, protocollazione, gestione e conservazione dei documenti informatici. Allo scopo di semplificare l'approccio normativo, incorporano in un **unico documento** la normativa in materia che ad oggi è distribuita in tre DPCM e altri atti normativi di rango inferiore. **Il riferimento normativo primario è il CAD** (regole tecniche per molti ambiti disciplinati dal CAD).

Le Linee guida costituiscono **un elemento fondamentale nell'ambito della digitalizzazione della PA**

Come precisato dal Consiglio di Stato le Linee Guida adottate da AGID, ai sensi dell'art. 71 del CAD, **hanno carattere vincolante e assumono valenza *erga omnes***.

Ne deriva che, nella gerarchia delle fonti, le Linee Guida sono inquadrate come un atto di regolamentazione, seppur di natura tecnica, con la conseguenza che esse sono pienamente **azionabili davanti al giudice amministrativo** in caso di violazione delle prescrizioni ivi contenute. Nelle ipotesi in cui la violazione sia posta in essere da parte dei soggetti di cui all'art. 2, comma 2 del CAD, è altresì possibile presentare apposita segnalazione al **difensore civico per il digitale**, ai sensi dell'art. 17 del CAD

LE PRINCIPALI NOVITÀ

1 - RESPONSABILE DEL SERVIZIO DI CONSERVAZIONE

Nelle precedenti indicazioni Agid, avrebbe dovuto essere "**interno**" all'organizzazione "produttrice" del documento informatico, potendo **delegare** tutte o parte delle sue funzioni al **responsabile del servizio di conservazione**.

Le nuove Linee guida, nel ridisegnare e specificare i ruoli necessari nel processo di conservazione (che passano da 3 a 5), prevedono che, nella p.a., tale figura sia identificata nell'organigramma in un responsabile o funzionario interno **formalmente nominato** con adeguate competenze legali, informatiche e archivistiche. Può essere svolto dal responsabile della gestione documentale

2 - I METADATI

In attuazione dei principi di **interoperabilità e trasparenza**, sono aumentati il numero e la tipologia dei metadati utilizzati per indicizzare, identificare e ricercare i documenti inviati in un sistema di conservazione

COSA SONO I METADATI: Al momento della formazione del documento informatico immodificabile devono essere generati ed associati permanentemente a esso i relativi metadati o indici. Sono i dati collegati a documento informatico, fascicolo informatico o aggregazione documentale per identificarli, descrivendone il contesto, il contenuto e la struttura, così da permetterne la gestione nel tempo.

Ai fini dell'invio in conservazione, fino ad oggi erano richiesti come obbligatori solamente **5** metadati

Le nuove LLGG ne identificano in tutto **17**, di cui 13 obbligatori

LE PRINCIPALI NOVITÀ

3 – LA CERTIFICAZIONE DI PROCESSO

Sono state individuate specifiche **modalità operative** per ottenere la certificazione di processo che garantisca, in caso di **dematerializzazione massiva di documenti analogici**, la corrispondenza del contenuto e della forma della copia informatica con l'originale analogico, senza dover ricorrere al confronto puntuale dei documenti.

4 – MODALITÀ DI FORMAZIONE DEI DOCUMENTI

a) ~~redazione tramite l'utilizzo di appositi strumenti software~~ **creazione** tramite l'utilizzo di strumenti software o servizi cloud qualificati che assicurino la produzione di documenti nei formati e nel rispetto delle regole di interoperabilità di cui all'allegato 2;

b) **acquisizione** di un documento informatico per via telematica o su supporto informatico, acquisizione della copia per immagine su supporto informatico di un documento analogico, acquisizione della copia informatica di un documento analogico;

c) ~~registrazione informatica delle informazioni~~ **memorizzazione** su supporto informatico delle informazioni risultanti da transazioni o processi informatici o dalla presentazione telematica di dati attraverso moduli o formulari resi disponibili all'utente;

d) generazione o **raggruppamento** anche in via automatica di un insieme di dati o registrazioni, provenienti da una o più banche dati.

LE PRINCIPALI NOVITÀ

5 – ADEGUAMENTO AL REGOLAMENTO EIDAS
Per quanto attiene a due caratteristiche peculiari del documento informatico -> l'immodificabilità e l'integrità
Viene introdotto, accanto alla PEC, il **servizio elettronico di recapito certificato qualificato** ai sensi del Regolamento europeo 910/2014 eIDAS (*electronic IDentification Authentication and Signature*) che ha l'obiettivo di fornire una **base normativa comune** a livello comunitario per interazioni elettroniche sicure fra cittadini, imprese e pubbliche amministrazioni. Nelle linee guida compare il sigillo elettronico conforme al regolamento eIDAS che, in base allo scenario operativo di dettaglio, deve essere applicato in forma avanzata o in forma qualificata

6 – AGGIORNAMENTO DELLE MISURE DI SICUREZZA
Le misure di sicurezza sono aggiornate e devono essere conformi alle norme europee sulla protezione dei dati personali (**Regolamento 679/2016**) e alle misure minime di sicurezza ICT emanate dall'**AgID** con **circolare** del 18 aprile 2017, **n. 2/2017**. Sul piano operativo vengono coinvolte le numerose figure previste dalla normativa privacy e ovviamente il responsabile per la transizione digitale (RTD)

Linee Guida sulla formazione, gestione e conservazione dei documenti informatici – AGID

Il responsabile della gestione documentale

• è preposto al servizio di cui all'articolo 61 del TUDA

• deve possedere idonei requisiti professionali o professionalità tecnico archivistica acquisita a seguito di processi di formazione definiti secondo le procedure prescritte dalla disciplina vigente

• predispone il Manuale di gestione documentale d'intesa con il responsabile della conservazione, il responsabile per la transizione digitale e acquisito il parere del responsabile della protezione dei dati personali

Il responsabile della conservazione:

a) è un ruolo previsto dall'organigramma del Titolare dell'oggetto di conservazione;

b) è un dirigente o un funzionario interno formalmente designato e in possesso di idonee competenze giuridiche, informatiche ed archivistiche;

c) può essere svolto dal responsabile della gestione documentale o dal coordinatore della gestione documentale, ove nominato

d) può delegare, sotto la propria responsabilità, lo svolgimento delle proprie attività o parte di esse a uno o più soggetti che all'interno della struttura organizzativa abbiano specifiche competenze ed esperienze

IL MANUALE DI GESTIONE DOCUMENTALE

Il manuale di gestione documentale **descrive il sistema** di gestione informatica dei documenti e **fornisce le istruzioni** per il corretto funzionamento del servizio per la tenuta del **protocollo informatico**, della **gestione dei flussi documentali** e degli **archivi**.

La Pubblica Amministrazione è tenuta a **redigere**, adottare con **provvedimento formale** e **pubblicare** sul proprio sito istituzionale il **Manuale di gestione documentale**. La pubblicazione è realizzata in una parte chiaramente identificabile dell'area "Amministrazione trasparente" prevista dall'art. 9 del d.lgs. 33/201337.

Le Pubbliche Amministrazioni sono tenute ad ottemperare alle misure minime di sicurezza ICT emanate dall'AgID con circolare del 18 aprile 2017, n. 2/2017 (che prevedono tre livelli di sicurezza e forniscono una **check list** per poter verificare lo stato di attuazione delle misure di protezione). In tale ottica, il responsabile della gestione documentale, in accordo con il responsabile della conservazione, con il responsabile per la transizione digitale e acquisito il parere del responsabile della protezione dei dati personali, predispone **il piano della sicurezza** del sistema di gestione informatica dei documenti, prevedendo opportune misure tecniche e organizzative per garantire un livello di sicurezza adeguato al rischio in materia di protezione dei dati personali, ai sensi dell'art. 32 del Regolamento UE 679/2016 (GDPR).

La Piattaforma Digitale Nazionale Dati (PDND) e la valorizzazione del patrimonio informativo pubblico: adempimenti per la PA

Art. 50 CAD
«I dati delle pubbliche amministrazioni sono formati, raccolti, conservati, resi disponibili e accessibili con l'uso delle tecnologie dell'informazione e della comunicazione, onde ne siano consentite la fruizione e riutilizzazione (alle condizioni fissate dall'ordinamento) da parte delle altre pubbliche amministrazioni e dei privati (salvi i limiti alla conoscibilità dei dati previsti, le norme in materia di protezione dei dati personali, il rispetto della normativa comunitaria in materia di riutilizzo delle informazioni del settore pubblico)».

La valorizzazione del patrimonio informativo pubblico è un obiettivo strategico, soprattutto per affrontare efficacemente le nuove sfide dell'economia dei dati, supportare la costruzione del **mercato unico europeo per i dati** definito dalla Strategia europea in materia di dati, garantire la creazione di **servizi digitali a valore aggiunto** per cittadini, imprese e fornire ai *policy maker* strumenti *data-driven* da utilizzare nei **processi decisionali.**
I vantaggi dell'**interoperabilità** sono legati, in particolare, al principio ***once only***, ovvero il cittadino fornisce i dati una sola volta e gli enti si scambiano le informazioni attraverso banche dati che possono comunicare tra loro e rappresentano a tutti gli effetti un diritto di cittadini e imprese.

La Piattaforma Digitale Nazionale Dati (PDND) e la valorizzazione del patrimonio informativo pubblico: adempimenti per la PA

La condivisione di dati e informazioni avviene attraverso la messa a disposizione e l'utilizzo da parte dei soggetti accreditati, di "**interfacce di programmazione delle applicazioni**" (API, nell'acronimo di *Application Programming Interface*, ossia uno strumento di programmazione che 'interfaccia', rendendoli comunicanti, programmi o piattaforme altrimenti incompatibili)
Le interfacce sono sviluppate dai soggetti abilitati in conformità alle Linee guida AgID in materia di interoperabilità, e sono raccolte in un “catalogo API”, reso disponibile, ai soggetti accreditati, dalla medesima PDND.
Le pubbliche amministrazioni - nell'accezione ampia di cui all'articolo 2, comma 2, del Codice dell'amministrazione digitale - sono tenute ad **accreditarsi alla Piattaforma**, a sviluppare le interfacce e a rendere disponibili le proprie basi dati.
È prevista una disposizione sanzionatoria, per l'**inadempimento dell'obbligo di rendere disponibili e accessibili le proprie basi dati ovvero i dati aggregati e anonimizzati.**
l'accesso ai dati attraverso la Piattaforma digitale nazionale dati non modifica la disciplina relativa alla **titolarità del trattamento**; rimangono ferme le specifiche responsabilità in capo così al soggetto gestore della Piattaforma come ai soggetti accreditati che trattino i dati in qualità di titolari autonomi del trattamento.

Sistema di gestione deleghe (SGD)

DL Semplificazioni del 2021 - lo **SPID** potrà essere usato anche con **delega** a soggetti terzi
La presentazione della delega avviene mediante una delle modalità previste dall'articolo 65, comma 1 CAD
Enti locali (e non solo), che **sono tenuti ad accreditarsi al SGD**
A seguito dell'acquisizione della delega al SGD, è generato un attributo qualificato associato all'identità digitale del delegato, secondo le modalità stabilite dall'AgID con Linee guida. Tale attributo può essere utilizzato anche per l'erogazione di servizi in modalità analogica.

Con un futuro DPCM saranno definite le caratteristiche tecniche, l'architettura generale, i requisiti di sicurezza, le modalità di acquisizione della delega e di funzionamento del SGD. Con il medesimo decreto, inoltre, saranno individuate le modalità di adesione al sistema nonché le tipologie di dati oggetto di trattamento, le categorie di interessati e, in generale, le modalità e procedure per assicurare il rispetto della protezione dei dati sensibili.

Il Piano triennale per l’informatica comunale

Il Piano Triennale per l’informatica della Pubblica Amministrazione è uno strumento essenziale per promuovere la trasformazione digitale del Paese e, in particolare, quella della Pubblica Amministrazione italiana.

Previsto dal **CAD** (art. 14-bis, lettera b) *“monitoraggio delle attività svolte dalle amministrazioni, ivi inclusi gli investimenti effettuati ai sensi dell’articolo 1, comma 492, lettera a-bis), della legge 11 dicembre 2016, n. 232, in relazione alla loro coerenza con il Piano triennale di cui alla lettera b) e verifica dei risultati conseguiti dalle singole amministrazioni con particolare riferimento ai costi e benefici dei sistemi informatici secondo le modalità fissate dalla stessa Agenzia”* che ha attribuito ad AGID il compito di realizzare il monitoraggio delle attività e la verifica dei risultati delle amministrazioni, in termini sia di coerenza con il Piano triennale (PT) e sia di costi/benefici dei sistemi informativi delle singole PA.

Il Piano triennale per l’informatica comunale

Il Piano ICT individua su base triennale i fabbisogni informatici e tecnologici dell’ente e indica il programma degli acquisiti, in linea con la programmazione prevista dal Codice dei contratti pubblici e con le valutazioni comparative svolte ai sensi dell’art. 68 CAD e le possibili azioni di reingegnerizzazione volte alla digitalizzazione dei servizi e dei processi, coordinandosi con il *Piano integrato di attività e organizzazione” (PIAO)*.

La programmazione del Piano Triennale per l'Informatica deve essere resa coerente, infine, con la specifica allocazione di azioni nelle Missioni e Programmi del Documento Unico di Programmazione (DUP).

Le PA 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 PT e permette di evidenziare quali delle Linee di Azione previste nel PT siano state recepite dalle diverse amministrazioni e di approfondire quali altre azioni siano state individuate localmente per il conseguimento dei singoli Obiettivi previsti nel PT. Si chiederà inoltre alle amministrazioni di allegare il proprio Piano, per poter prendere visione di eventuali altri obiettivi definiti localmente.

Date		Capitolo	Obiettivo	Attività	Azioni / risultati	Rif. Atti amm.vi / DUP - PEG
da	set-20	servizi	OB.1.1 - Migliorare la capacità di generare ed erogare servizi digitali	Le PA finalizzano l'adesione a Web Analytics Italia per migliorare il processo evolutivo dei propri servizi online		
da	set-20	servizi	OB.1.1 - Migliorare la capacità di generare ed erogare servizi digitali	Le PA continuano ad applicare i principi Cloud First - SaaS First e ad acquisire servizi cloud solo se qualificati da AGID, consultando il Catalogodei servizi cloud qualificati da AGID per la PA https://cloud.italia.it/marketplace/		
da	set-20	servizi	OB.1.2 - Migliorare l'esperienza d'uso e l'accessibilità dei servizi	Nei procedimenti di acquisizione di beni e servizi ICT, le PA devono far riferimento alle Linee guida di design		
da	set-20	piattaforme	OB.3.2 - Aumentare il grado di adozione delle piattaforme abilitanti esistenti da parte delle pubbliche amministrazioni	Le PA e i gestori di pubblici servizi proseguono il percorso di adesione aSPID e PagoPA e dismettono le altre modalità di autenticazione e pagamento associate ai propri servizi online		
da	set-20	infrastrutture	OB.4.1 - Migliorare la qualità dei servizi digitali erogati dalle amministrazioni locali favorendonel'aggregazione e la migrazione su infrastrutture sicure e affidabili	Le PA proprietarie di data center di gruppo B richiedono l'autorizzazione ad AGID per le spese in materia di data center nelle modalità stabilite dalla Circolare AGID 1/2019		
da	set-20	interoperabilità	OB.5.1 - Favorire l'applicazione delleLinee Guida sul Modello di interoperabilità da parte degli erogatori di API	Le PA prendono visione della Linea di indirizzo sull'interoperabilità tecnica per la PA e programmano le azioni per trasformare i servizi per l'interazione con altre PA implementando API conformi		
da	set-20	interoperabilità	OB.5.2 - Adottare API conformi al Modello di interoperabilità	Le PA popolano gli strumenti su developers.italia.it con i servizi che hanno reso conformi alla Linea di indirizzo sull'interoperabilità tecnica		
da	set-20	sicurezza	OB.6.1 - Aumentare la consapevolezza del rischio cyber (Cuber Sercurity Awareness) nelle PA	Le PA nei procedimenti di acquisizione di beni e servizi ICT devono far riferimento alle Linee guida sulla sicurezza nel procurement ICT		
da	ott-20	servizi	OB.1.1 - Migliorare la capacità di generare ed erogare servizi digitali	Le PA dichiarano, all'interno del catalogo di Developers Italia, quali software di titolarità di un'altra PA hanno preso in riuso		
da	ott-20	infrastrutture	OB.4.3 - Migliorare l'offerta di servizidi connettività per le PA	Le PAL si approvvigionano sul nuovo catalogo MEPA per le necessità di connettività non riscontrabili nei contratti SPC (Sistema Pubblico di Connettività: definisce le modalità che i sistemi informativi delle PA devono adottare per essere tra loro interoperabili)		
entro	ott-20	servizi	OB.1.1 - Migliorare la capacità di generare ed erogare servizi digitali	Le PA adeguano le proprie procedure di procurement alle linee guida diAGID sull'acquisizione del software e al CAD (artt. 68 e 69) - analisi comparativa e riuso		

OBIETTIVI 2026

I 5 indicatori per portare l'Italia nel gruppo di testa

La strategia nazionale Italia digitale 2026

SCOPRI DI PIÙ

Identità digitale
% popolazione
70%

Competenze digitali
% popolazione
70%

Adozione cloud
% Pubblica Amministrazione
75%

Servizi pubblici online
% servizi pubblici essenziali
80%

Connessione banda ultralarga
% famiglie
100%

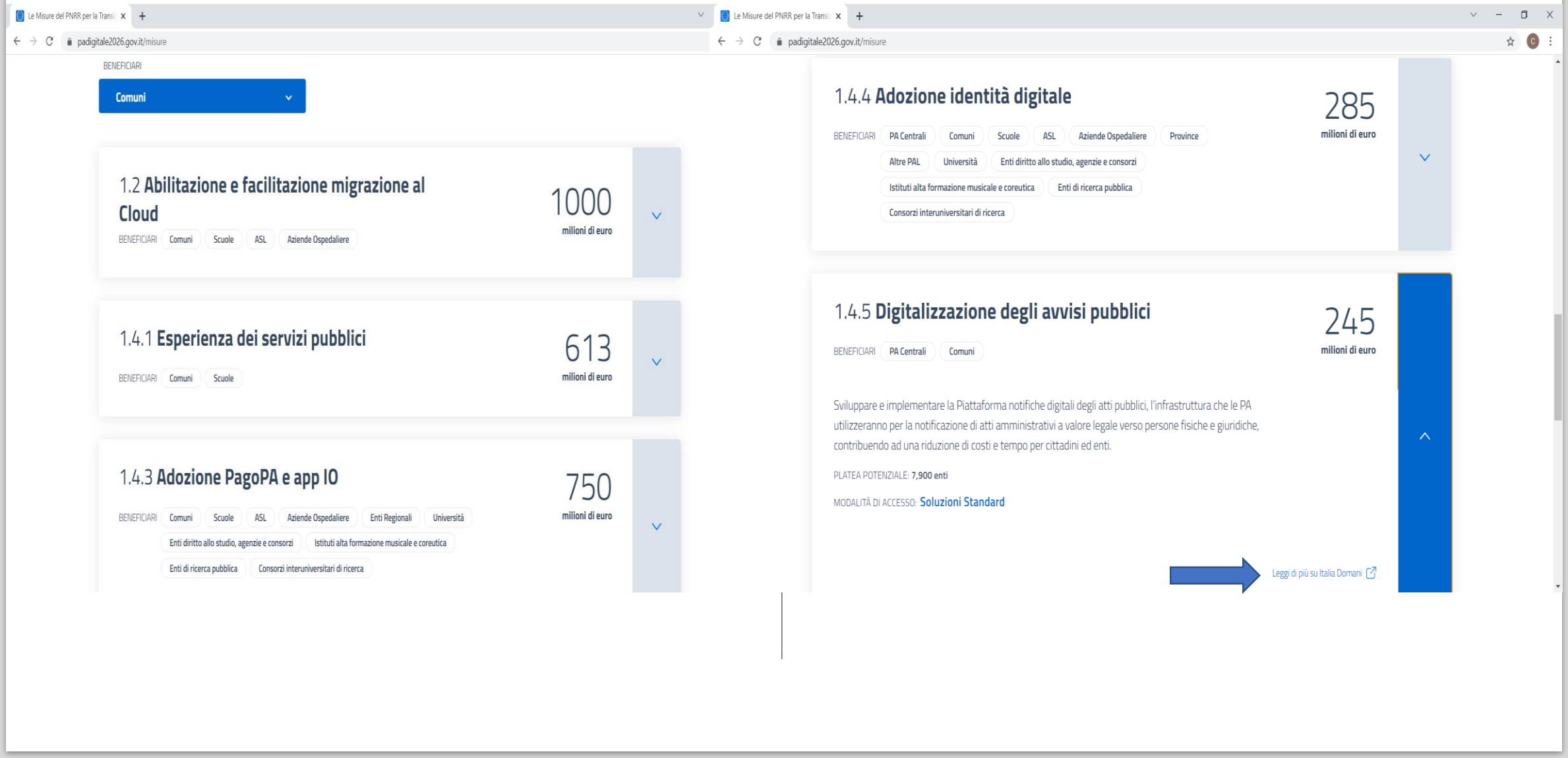
COME FUNZIONA PA DIGITALE 2026

Come accedere alle misure del PNRR

PA digitale 2026 è la piattaforma per accedere alle risorse dedicate alla **transizione digitale** e assistere le amministrazioni nel percorso verso Italia digitale 2026

SCOPRI DI PIÙ

VEDI I BENEFICIARI


Le Misure del PNRR per la Transi
padigitale2026.gov.it/misure
BENEFICIARI
Comuni
1.2 Abilitazione e facilitazione migrazione al Cloud
BENEFICIARI Comuni Scuole ASL Aziende Ospedaliere
1000
milioni di euro
1.4.1 Esperienza dei servizi pubblici
BENEFICIARI Comuni Scuole
613
milioni di euro
1.4.3 Adozione PagoPA e app IO
BENEFICIARI Comuni Scuole ASL Aziende Ospedaliere Enti Regionali Università
Enti diritto allo studio, agenzie e consorzi
Istituti alta formazione musicale e coreutica
Enti di ricerca pubblica
Consorzi interuniversitari di ricerca
750
milioni di euro
1.4.4 Adozione identità digitale
BENEFICIARI PA Centrali Comuni Scuole ASL Aziende Ospedaliere Province
Altre PAL
Università
Enti diritto allo studio, agenzie e consorzi
Istituti alta formazione musicale e coreutica
Enti di ricerca pubblica
Consorzi interuniversitari di ricerca
285
milioni di euro
1.4.5 Digitalizzazione degli avvisi pubblici
BENEFICIARI PA Centrali Comuni
245
milioni di euro
Sviluppare e implementare la Piattaforma notifiche digitali degli atti pubblici, l'infrastruttura che le PA utilizzeranno per la notificazione di atti amministrativi a valore legale verso persone fisiche e giuridiche, contribuendo ad una riduzione di costi e tempo per cittadini ed enti.
PLATEA POTENZIALE: 7,900 enti
MODALITÀ DI ACCESSO: Soluzioni Standard
Leggi di più su Italia Domani

Soluzioni standard

Per le misure con una platea ampia di beneficiari (oltre 1.000 PA), è prevista una modalità di accesso per soluzioni standard. Un percorso semplificato e guidato che va dalla richiesta dei finanziamenti all'erogazione dei fondi.

Richiesta dei fondi

Realizzazione delle iniziative

Erogazione dei fondi

Soluzioni a misura di PA

Semplificare la richiesta di finanziamenti e ridurre gli oneri amministrativi per tutta la PA

SOLUZIONI STANDARD

Ogni PA, in base a tipologia e dimensione, potrà accedere alle misure attraverso **soluzioni standard**, ciascuna con un valore economico predefinito. **Non sarà necessario scrivere e presentare progetti** per ricevere finanziamenti.

SOLUZIONI MULTIMISURA

Per semplificare l'accesso ai fondi del PNRR le amministrazioni potranno - **con un'unica candidatura** - accedere a soluzioni multimisura, che includono, per esempio, sia finanziamenti per la migrazione al cloud che per il miglioramento dei siti web.

Soluzioni standard

Per le misure con una platea ampia di beneficiari (oltre 1.000 PA), è prevista una modalità di accesso per soluzioni standard. Un percorso semplificato e guidato che va dalla richiesta dei finanziamenti all'erogazione dei fondi.

Richiesta dei fondi

Realizzazione delle iniziative

Erogazione dei fondi

Un portale dedicato e un team di supporto sul territorio

L'importanza di accompagnare le amministrazioni con competenze e strumenti

UN PORTALE DEDICATO

"PA digitale 2026" **accompagnerà gli Enti con risorse e informazioni** lungo tutto il percorso di attuazione delle misure previste dal PNRR: dalla prima fase informativa, che precede l'avvio degli avvisi, al momento dell'accesso ai fondi e fino all'implementazione stessa delle iniziative. I **fornitori saranno scelti dalla PA** anche avvalendosi di fornitori certificati attraverso strumenti Consip.

UN TEAM SUL TERRITORIO

Per sostenere la transizione digitale dei singoli Enti, nasce un team dedicato: il **Transformation Office**. Questa struttura, che sarà anche dislocata sul territorio con referenti locali, è parte del Dipartimento per la trasformazione digitale, e farà da ponte con amministrazioni locali e fornitori IT della PA, con **assistenza informativa e tecnica.**

Richiesta dei fondi

Realizzazione delle iniziative

Erogazione dei fondi

L'importanza dei risultati

Semplificazione dei processi per l'erogazione dei fondi

100% ONLINE

Attraverso "PA digitale 2026" le amministrazioni potranno **accedere ad un'area riservata**, per seguire la gestione amministrativa delle singole iniziative finanziate attraverso l'azione del Dipartimento per la trasformazione digitale. Con l'avvio degli avvisi avranno infatti la possibilità non solo di fare **richiesta per i fondi**, ma anche di **produrre i dati relativi all'avanzamento delle iniziative, ricevere comunicazioni dedicate** e **inviare documentazioni ufficiali per l'erogazione delle risorse.**

EROGAZIONI PER OBIETTIVI

Per semplificare l'erogazione delle risorse, i contributi saranno riconosciuti alle amministrazioni sulla base del **raggiungimento di specifici obiettivi predefiniti**. Il processo di rendicontazione sarà quindi alleggerito, e **non sarà necessario rendicontare le singole spese effettuate per ottenere i fondi.**

Le PA definiscono, sulla base di quanto proposto dal RTD, all'interno dei piani di formazione del personale, interventi sulle tematiche di *Cyber Security Awareness*

Formazione e rafforzamento delle competenze digitali nella PA: CAD, Syllabus e PNRR

Il tema delle competenze digitali nella PA è introdotto dall'art. 13 del CAD "Formazione informatica dei dipendenti pubblici", il quale prevede che:
"Le pubbliche amministrazioni, nell'ambito delle risorse finanziarie disponibili, attuano politiche di reclutamento e formazione del personale finalizzate alla conoscenza e all'uso delle tecnologie dell'informazione e della comunicazione, nonché dei temi relativi all'accessibilità e alle tecnologie assistive e altresì volte allo sviluppo delle competenze tecnologiche, di informatica giuridica e manageriali dei dirigenti, per la transizione alla modalità operativa digitale".

Il documento che descrive l'insieme minimo delle conoscenze e abilità che ogni dipendente pubblico, non specialista IT, dovrebbe possedere per partecipare attivamente alla trasformazione digitale della pubblica amministrazione, è il **Syllabus**
Nella redazione dei piani di formazione del personale, vanno previsti interventi formativi sulle tematiche della sicurezza informatica

Le PA definiscono, sulla base di quanto proposto dal RTD, all'interno dei piani di formazione del personale, interventi sulle tematiche di *Cyber Security Awareness*

Livello di padronanza BASE	3.1.1.1 Conoscere l'esistenza di rischi e minacce negli ambienti digitali; 3.1.1.2 Saper adottare le misure base di sicurezza per proteggere i dispositivi; 3.1.1.3 Saper definire e gestire le password in modo consapevole e protetto.	3.2.1.1 Conoscere i concetti di riservatezza, integrità e non ripudio dei dati; 3.2.1.2 Conoscere cos'è il regolamento europeo sulla protezione dei dati personali.
Livello di padronanza INTERMEDIO	3.1.2.1 Saper valutare i principali rischi per il dispositivo se soggetto ad attacchi informatici; 3.1.2.2 Conoscere l'esistenza delle misure minime di sicurezza ICT per le pubbliche amministrazioni; 3.1.2.3 Conoscere i principali tipi di attacco informatico, Virus, Trojan, Denial of Service (DoS), Distributed Denial of Service (DDoS).	3.2.2.1 Sapere come proteggere i dati personali negli ambienti digitali; 3.2.2.2 Comprendere la differenza tra i diversi tipi di dati personali. 3.2.2.3 Conoscere i principi generali definiti nel regolamento europeo sulla protezione dei dati personali.
Livello di padronanza AVANZATO	3.1.3.1 Sapere quali contromisure adottare per prevenire e difendersi dagli attacchi informatici; 3.1.3.2 Saper riconoscere quando il dispositivo è soggetto ad attacchi informatici.	3.2.3.1 Saper valutare i rischi e applicare le contromisure appropriate; 3.2.3.2 Saper declinare gli adempimenti connessi alla tutela dei dati personali nell'ambito dell'attività di una pubblica amministrazione.

Le PA valutano l'utilizzo del *tool di Cyber Risk Assessment* per l'analisi del rischio e la redazione del Piano dei trattamenti

Strumento che consente ad ogni PA di effettuare le operazioni di self assessment, predisporre gli opportuni piani di trattamento ed eseguire il monitoraggio delle iniziative volte a ridurre il livello di rischio informatico.

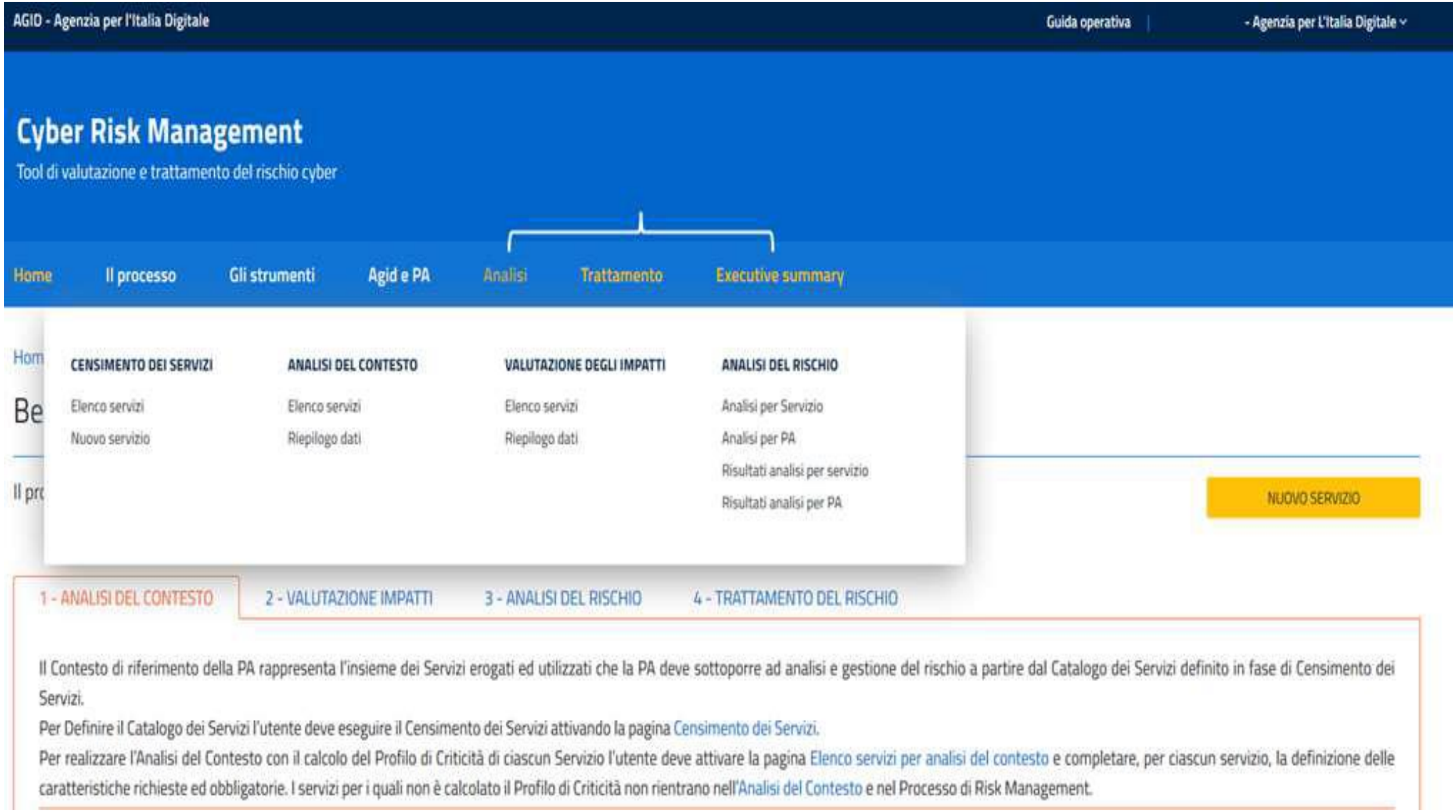
Il tool è web based e l'accesso per le PA avviene attraverso SPID.

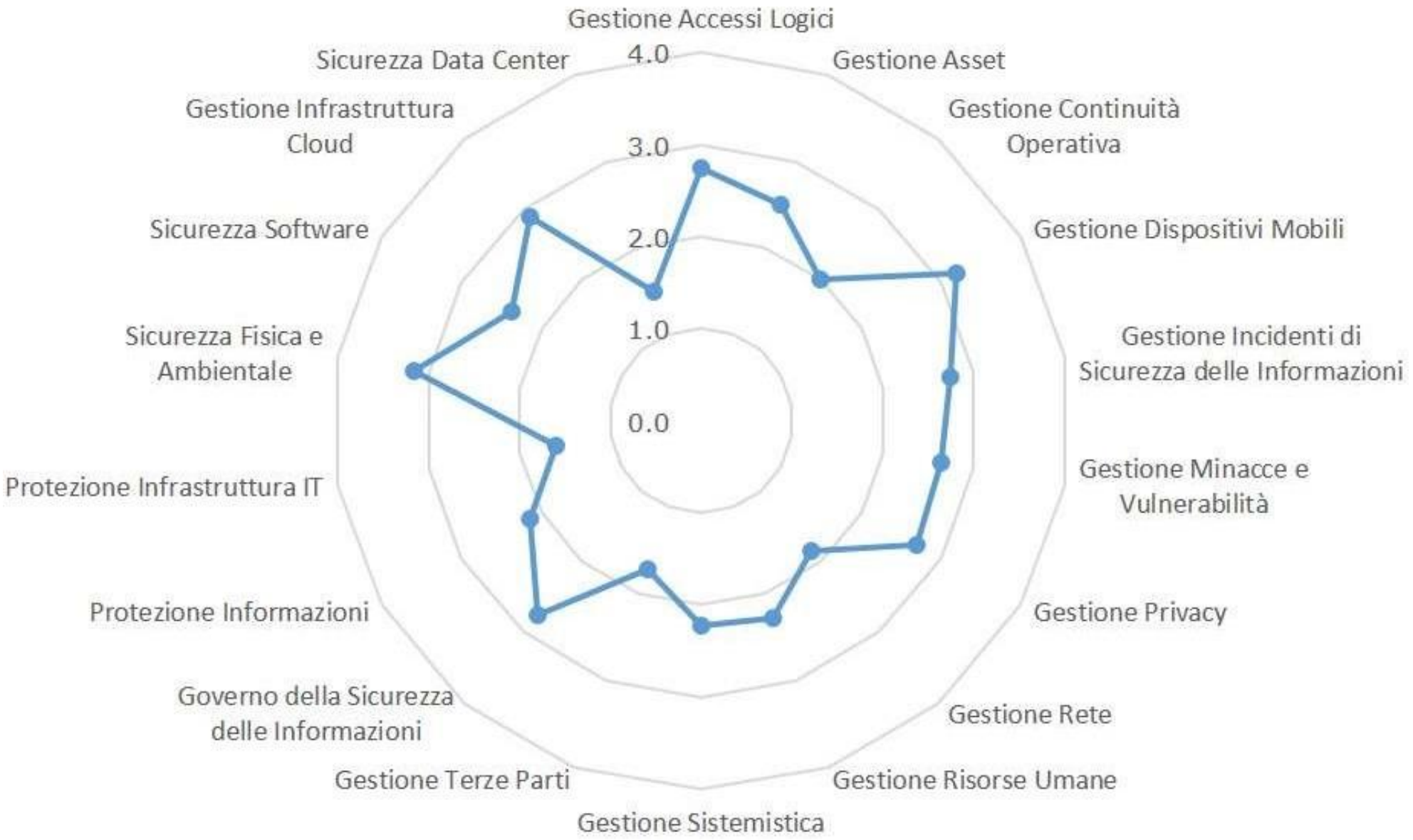
È organizzato in fasi:

- Fase iniziale: Definizione del contesto in cui opera la PA

- Fase di analisi: identificazione dei rischi, simulazione degli effetti di mitigazione delle azioni, piano dei trattamenti

- Fase operativa: Valutazione delle azioni da mettere in campo, orizzontale su tutta la PA o su singoli servizi


AGID - Agenzia per l'Italia Digitale
Guida operativa
- Agenzia per L'Italia Digitale
Cyber Risk Management
Tool di valutazione e trattamento del rischio cyber
Home
Il processo
Gli strumenti
Agid e PA
Analisi
Trattamento
Executive summary
CENSIMENTO DEI SERVIZI
Elenco servizi
Nuovo servizio
ANALISI DEL CONTESTO
Elenco servizi
Riepilogo dati
VALUTAZIONE DEGLI IMPATTI
Elenco servizi
Riepilogo dati
ANALISI DEL RISCHIO
Analisi per Servizio
Analisi per PA
Risultati analisi per servizio
Risultati analisi per PA
NUOVO SERVIZIO
1 - ANALISI DEL CONTESTO
2 - VALUTAZIONE IMPATTI
3 - ANALISI DEL RISCHIO
4 - TRATTAMENTO DEL RISCHIO
Il Contesto di riferimento della PA rappresenta l'insieme dei Servizi erogati ed utilizzati che la PA deve sottoporre ad analisi e gestione del rischio a partire dal Catalogo dei Servizi definito in fase di Censimento dei Servizi.
Per Definire il Catalogo dei Servizi l'utente deve eseguire il Censimento dei Servizi attivando la pagina Censimento dei Servizi.
Per realizzare l'Analisi del Contesto con il calcolo del Profilo di Criticità di ciascun Servizio l'utente deve attivare la pagina Elenco servizi per analisi del contesto e completare, per ciascun servizio, la definizione delle caratteristiche richieste ed obbligatorie. I servizi per i quali non è calcolato il Profilo di Criticità non rientrano nell'Analisi del Contesto e nel Processo di Risk Management.


Gestione Accessi Logici
Gestione Asset
Gestione Continuità Operativa
Gestione Dispositivi Mobili
Gestione Incidenti di Sicurezza delle Informazioni
Gestione Minacce e Vulnerabilità
Gestione Privacy
Gestione Rete
Gestione Risorse Umane
Gestione Sistemistica
Gestione Terze Parti
Governo della Sicurezza delle Informazioni
Protezione Informazioni
Protezione Infrastruttura IT
Sicurezza Fisica e Ambientale
Sicurezza Software
Gestione Infrastruttura Cloud
Sicurezza Data Center
4.0
3.0
2.0
1.0
0.0

Le PA si adeguano alle Misure minime di sicurezza ICT per le pubbliche amministrazioni aggiornate

Le Pubbliche Amministrazioni sono tenute ad ottemperare alle misure minime di sicurezza ICT emanate dall'AgID con circolare del 18 aprile 2017, n. 2/2017 (che prevedono tre livelli di sicurezza e forniscono una **check list** per poter verificare lo stato di attuazione delle misure di protezione). In tale ottica, il responsabile della gestione documentale, in accordo con il responsabile della conservazione, con il responsabile per la transizione digitale e acquisito il parere del responsabile della protezione dei dati personali, predispone **il piano della sicurezza** del sistema di gestione informatica dei documenti, prevedendo opportune misure tecniche e organizzative per garantire un livello di sicurezza adeguato al rischio in materia di protezione dei dati personali

Circolare AgID n. 2/2017 - Misure minime di sicurezza ICT

AMBITI DI CONTROLLO:

- INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI
- INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI
- PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER
- VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITÀ
- USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE
- DIFESE CONTRO I MALWARE
- COPIE DI SICUREZZA
- PROTEZIONE DEI DATI

Le PA devono mantenere costantemente aggiornati i propri portali istituzionali e applicare le correzioni alle vulnerabilità consultando la piattaforma Infosec aggiornata per rilevare le vulnerabilità dei propri *asset*

INFOSEC *(https://infosec.cert-pa.it/)* è una applicatione web focalizzata sulla gestione delle vulnerabilità applicative ed i rischi connessi. Ha lo scopo di fornire uno strumento per una corretta valutazione delle minacce cibernetiche portate verso le infrastrutture informatiche.

Il sito è un aggregatore di dati e informazioni relativi a tecniche d'attacco, vulnerabilità hardware e software. Partendo da una singola vulnerabilità è possibile risalire al tipo di debolezza (CVE - *Common Vulnerabilities and Exposures*) dell'entità oggetto della falla di sicurezza, e da questa prendere in considerazione le varie tecniche di attacco (CAPEC) associate alla debolezza stessa. Il proposito che si pone l'applicativo è quello di essere strumento a supporto della gestione della sicurezza in fase di assessment conseguente al rilascio di nuove vulnerabilità. Ma è anche possibile sviluppare una logica inversa che, dalla tecnica di attacco subita, permetta di arrivare ai CVE (e quindi le vulnerabilità) utilizzate.