Strategia Cloud Italia

Documento sintetico di indirizzo strategico per l'implementazione e il controllo del Cloud della PA

INDICE

AUTORI

Dipartimento per la Trasformazione Digitale

Agenzia per la Cybersicurezza Nazionale

In sintesi

L'irreversibile processo di trasformazione digitale della società, accelerato dalla emergenza pandemica ancora in corso, ha reso improcrastinabile un'analoga trasformazione della Pubblica Amministrazione. La digitalizzazione della Pubblica Amministrazione si impone oggi come obiettivo prioritario per garantire ai cittadini e alle imprese servizi pubblici di maggiore qualità, efficienza ed efficacia, oltre che per creare nuove opportunità di sviluppo per l'economia digitale del Paese. In questo processo trasformativo, il ricorso al Cloud Computing, o Cloud, riveste un ruolo centrale in ragione delle sue caratteristiche abilitanti per la semplificazione e ottimizzazione della gestione delle risorse IT, la riduzione dei costi, e l'introduzione di nuove tecnologie digitali.

Per questo, è stata elaborata la *Strategia Cloud Italia* con l'obiettivo di fornire l'indirizzo strategico per l'implementazione e il controllo di soluzioni Cloud nella Pubblica Amministrazione. La migrazione al Cloud permette alle pubbliche amministrazioni di fornire servizi digitali e di disporre di infrastrutture tecnologiche sicure, efficienti ed affidabili, in linea con i principi di tutela della privacy, con le raccomandazioni delle istituzioni europee e nazionali, mantenendo le necessarie garanzie di autonomia strategica del Paese, di sicurezza e controllo nazionale sui dati.

In tale prospettiva, la strategia si muove lungo tre direttrici fondamentali: i) la creazione del Polo Strategico Nazionale (PSN), un'infrastruttura nazionale per l'erogazione di servizi Cloud, la cui gestione e controllo di indirizzo siano autonomi da fornitori extra UE, ii) un percorso di qualificazione dei fornitori di Cloud pubblico e dei loro servizi per garantire che le caratteristiche e i livelli di servizio dichiarati siano in linea con i requisiti necessari di sicurezza, affidabilità e rispetto delle normative rilevanti e iii) lo sviluppo di una metodologia di classificazione dei dati e dei servizi gestiti dalle pubbliche amministrazioni, per permettere una migrazione di questi verso la soluzione Cloud più opportuna (PSN o Cloud pubblico qualificato).

1. Introduzione

L'emergenza sanitaria ha reso ancora più evidente, se necessario, quanto le infrastrutture digitali siano fondamentali e strategiche per il nostro Paese, al pari di infrastrutture tradizionali come le autostrade, le ferrovie, il sistema elettrico. L'adozione e la diffusione delle tecnologie digitali sono state infatti accelerate e favorite dalla pandemia per permettere nuove modalità di studio e lavoro da remoto.

Tra i fattori abilitanti della trasformazione digitale del Paese, un ruolo centrale è svolto dalle tecnologie di Cloud Computing, la cosiddetta "nuvola informatica", che permette di semplificare e ottimizzare la gestione delle risorse informatiche, nonché di facilitare l'adozione di nuove tecnologie digitali.

La necessità di tecnologie Cloud è destinata ad aumentare alla luce dell'incremento esponenziale del volume di dati trattati[1] e della pervasività dei servizi digitali, che necessitano di infrastrutture computazionali espandibili e scalabili in modo flessibile e immediato, obiettivo difficilmente raggiungibile tramite i data center tradizionali.

Questo irreversibile processo di trasformazione digitale della società ha imposto un'analoga trasformazione della Pubblica Amministrazione (PA), sia per assicurare una maggiore qualità, efficienza ed efficacia dei servizi pubblici, che per sostenere e creare nuove opportunità di sviluppo per l'economia digitale del Paese.

Per la PA, il ricorso al Cloud permette di raggiungere tali obiettivi con una significativa riduzione dei costi contribuendo, inoltre, ad aumentare l'efficienza energetica anche nell'ottica della sostenibilità ambientale. Al contempo, i differenti paradigmi architetturali e le modalità di erogazione dei servizi, impongono la necessità di adottare una strategia nazionale organica che possa imporre le necessarie garanzie di autonomia strategica e di resilienza del Paese, nonché di sicurezza e controllo nazionale dei dati dei cittadini e dei servizi offerti.

Questo documento si pone, pertanto, l'obiettivo di definire un piano strategico di indirizzo per l'adozione del Cloud Computing nella PA, alla luce delle sfide e dei rischi emergenti.

1 Dal 2018 al 2025 si stima un incremento del volume di dati intorno al 530% (European Commission, European data strategy. Making the EU a role model for a society empowered. Feb. 2020).

2. Il Cloud Computing

Il Cloud Computing, nel seguito Cloud, è un nuovo paradigma di utilizzo e gestione di risorse computazionali e di servizi informatici erogati su richiesta tramite internet. I servizi Cloud sono offerti mediante cataloghi standardizzati idonei a garantire, in modo sistematico e semplificato (*agilità*), l'attivazione dei servizi che possono scalare, a seconda dei picchi di carico, con modalità trasparente e automatica (*elasticità*) potendo operare in contemporanea e in sicurezza su dati e sistemi di utenti diversi (*multi-tenant*).

Tipicamente, i servizi Cloud si differenziano, sulla base del modello di risorse computazionali offerte, in tre modelli di servizio:

1. servizi sistemistici infrastrutturali, c.d. *Infrastructure-as-a-Service (IaaS)*, per l'erogazione, ad esempio, di server virtualizzati e spazio di salvataggio dati;
2. servizi di piattaforme computazionali, c.d. *Platform-as-a-Service (PaaS)*, per l'erogazione di ambienti pre-configurati e amministrati per lo sviluppo di specifiche applicazioni, ad esempio per lo sviluppo software, la gestione di dati o di applicazioni containerizzate;
3. servizi applicativi, c.d. *Software-as-a-Service (SaaS)*, per l'erogazione di un'applicazione agli utenti finali, ad esempio la posta elettronica o altri sistemi di collaborazione remota.

Questi diversi modelli di servizio permettono agli utenti dei servizi Cloud di evitare molte delle attività di gestione di base delle infrastrutture di un data center (si pensi ad esempio alla gestione degli edifici, delle componenti tecnologiche fisiche, ma anche alla possibilità di semplificare la gestione delle configurazioni iniziali e operative di applicativi e piattaforme) consentendo notevoli risparmi economici e maggior flessibilità nel gestire la richiesta di nuove risorse computazionali delle organizzazioni.
I servizi sono erogati da fornitori di servizi Cloud (*Cloud Service Provider,* d'ora innanzi anche *CSP*) che ne garantiscono il funzionamento secondo livelli contrattualmente determinati (*Service-Level Agreement, SLA*).
Il modello di distribuzione dei servizi Cloud può essere organizzato secondo queste modalità principali: *Cloud pubblico, Cloud privato, Cloud ibrido* e *Multi-Cloud*.

2.1 Cloud pubblico

Nel Cloud pubblico l'infrastruttura è di proprietà di un CSP che, avendone il pieno controllo, mette a disposizione di utenti, aziende ed enti pubblici i propri sistemi, distribuiti in diverse aree geografiche (o *region*) del mondo, con la condivisione di capacità elaborativa, applicazioni e *storage*. Tale distribuzione permette agli utenti dei servizi Cloud di beneficiare di capacità computazionali resilienti e scalabili a seconda delle effettive esigenze. Nell'ambito dei CSP di Cloud pubblico operano come leader di mercato un ristretto gruppo di aziende extraeuropee prevalentemente statunitensi. Queste aziende offrono servizi Cloud con capacità computazionale pressoché illimitata mediante soluzioni di elevata sofisticazione tecnologica, cosiddette "hyperscaler", ma al contempo con alta semplicità d'uso, configurabilità e interoperabilità.

2.2 Cloud privato

Il Cloud privato consiste in un ambiente Cloud riservato ad un singolo cliente per suo utilizzo esclusivo. Questo può essere *on-premise*, ovvero basato su infrastrutture che si trovano interamente nel dominio del cliente, che detiene il controllo e la totale responsabilità sulla manutenzione e la gestione della sicurezza dei dati e dei servizi ospitati, oppure può essere gestito presso i data center di un terzo soggetto, presso cui il cliente dispone di risorse dedicate.
Fra i vantaggi di un Cloud privato c'è sicuramente il maggior controllo che il cliente può esercitare sulle caratteristiche dell'infrastruttura e dei servizi Cloud, soprattutto per quanto riguarda la sicurezza.

Al contrario, fra gli svantaggi di questa soluzione, soprattutto nel caso di Cloud *on-premise*, occorre considerare il fatto che l'infrastruttura può non essere in grado di garantire l'adeguata scalabilità per gestire picchi non previsti di domanda.

2.3 Cloud ibrido

Combinazione del modello di Cloud pubblico e di quello privato, il Cloud ibrido si configura come un singolo ambiente creato a partire da più ambienti connessi in cui, a seconda delle necessità, sono messe a disposizione degli utenti risorse sia di un Cloud privato che di un Cloud pubblico. Tale modello consente, infatti, di estendere le capacità di un Cloud privato per utilizzare, su richiesta, le risorse di larga scala disponibili su un Cloud pubblico, ad esempio, per gestire improvvisi picchi di lavoro e garantire risparmi in termini di banda di trasmissione necessaria per lo scambio dei dati, rispetto a quanto sarebbe possibile con una connessione ad un data center.

2.4 Multi Cloud

Con *Multi-Cloud* si intende un modello che prevede l'utilizzo contemporaneo, per la realizzazione di determinati servizi o applicazioni, di più Cloud dello stesso tipo (pubblico o privato) offerti però da diversi fornitori.
A differenza del Cloud ibrido che prevede la realizzazione di un'unica infrastruttura che utilizzi in modo trasparente Cloud di diverso tipo (pubblico o privato), il modello Multi-Cloud si basa sull'utilizzo di diversi ambienti di Cloud pubblico o privato non interconnessi tra loro. In un ambiente di Cloud ibrido la distribuzione dell'utilizzo di risorse computazionali tra privato e pubblico è tipicamente semi-automatizzata e trasparente all'utente, mentre un ambiente Multi-Cloud si presenta come un insieme di risorse computazionali distinte potenzialmente integrabili a livello applicativo.

3. Le sfide poste dal Cloud Computing

L'adozione delle nuove tecnologie digitali, e le sfide che ne conseguono, sono oggetto di importanti regolamentazioni UE quali, tra le altre, i Regolamenti (UE) 2016/679 e 2018/1807 (c.d. GDPR e libera circolazione dei dati non personali) e la Direttiva 2016/1148 (c.d. Direttiva NIS), e di sicurezza nazionale, quali la legge 133/2019 (c.d. Perimetro di Sicurezza Nazionale Cibernetica, PSNC)[2].

3.1 Autonomia Tecnologica

Al fine di governare e gestire i processi di trasformazione digitale del Paese, come già riconosciuto nella prassi e dalle principali istituzioni europee, ricopre un'enorme importanza strategica l'autonomia nel controllo delle infrastrutture digitali del Cloud e conseguentemente nello stoccaggio e nell'elaborazione dei dati[3].
È noto, però, che le quote di mercato delle infrastrutture Cloud delle aziende europee rappresentano un valore residuale (inferiore al 10%) rispetto a quelle detenute dalle aziende extra UE[4]. Tale criticità, peraltro, non è circoscritta ai soli servizi e piattaforme digitali, ma anche e soprattutto alle infrastrutture che consentono il funzionamento degli stessi.
Alla luce di tale posizione di debolezza contrattuale per gli stati europei, l'adozione massiva di tecnologia Cloud per l'erogazione dei servizi della PA è soggetta al rischio di modifiche unilaterali delle condizioni dei servizi forniti, che potrebbero determinare variazioni significative degli stessi (dall'aumento dei costi di erogazione all'interruzione del servizio), in ragione di intenti potenzialmente non controllabili dal Paese. Per questo, il raggiungimento di un'autonomia tecnologica ha importanti ricadute non solo sulla possibilità di esercitare un diretto controllo sui dati e sui servizi, ma anche sulla possibilità di promuovere un ecosistema di tecnologie, indispensabile per lo sviluppo del Paese (Cloud Computing, IoT, Artificial Intelligence, Quantum Computing).

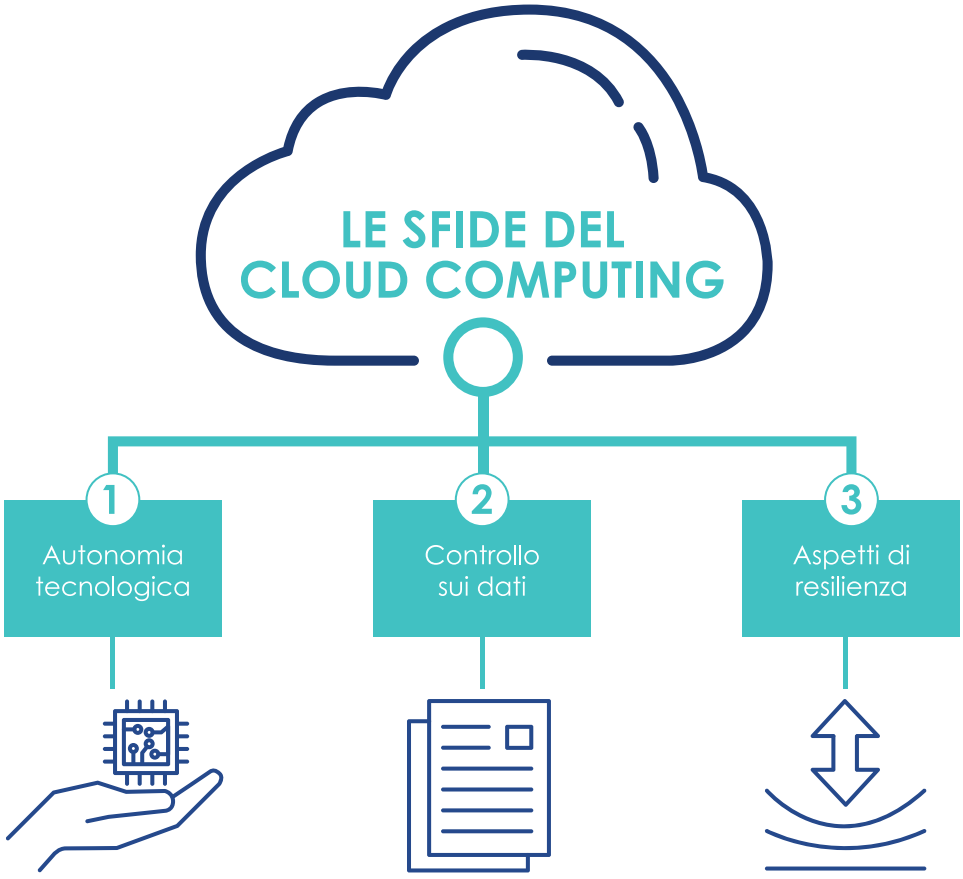
3.2 Controllo sui dati

La gestione dei servizi Cloud da parte di fornitori di paesi extra UE pone un rischio sistemico aggiuntivo dovuto alla normativa in essere in tali paesi. Come noto, legislazioni extra UE[5] possono portare, previa sussistenza delle previste circostanze, alla richiesta unilaterale al fornitore dei servizi Cloud di fornire l'accesso ai dati presenti sui sistemi. Tali fattispecie comportano la possibilità, per uno Stato estero (o Paese Terzo), di accedere a dati (o flussi di dati) particolarmente sensibili e strategici per i cittadini e le istituzioni italiane.
In tale ottica è necessario, nell'ambito della strategia, determinare in modo chiaro, attraverso una procedura di classificazione, le tipologie di dati che potranno essere gestiti da un fornitore extra UE attraverso un Cloud pubblico e quali dati invece avranno bisogno di essere gestiti da un fornitore Cloud che soddisfi specifici requisiti di sicurezza per abbattere il rischio che questi dati siano accessibili anche a governi di Paesi Terzi. La gestione di tali rischi, necessariamente, ha risvolti non soltanto tecnologici ma anche impatti geopolitici sulla scena internazionale che dovranno essere opportunamente considerati.

2 Conversione in legge, con modificazioni, del D.L. 21 settembre 2019, n. 105, recante disposizioni urgenti in materia di Perimetro di Sicurezza Nazionale Cibernetica.
3 OECD (2019) Regulation and IRC: challenges posed by the digital transformation. 20th meeting of the Regulatory Policy Committee, 17-18 April 2018, OECD Conference Centre, Paris, France.
4 Si veda, ad esempio, https://www.gartner.com/en/newsroom/press-releases/2019-07-29-gartner-says-worldwide- iaas-public-cloud-services-market-grew-31point3-percent-in-2018 e https://www.idc.com/getdoc.jsp?containerId=prUS45552219 e https://www.forbes.com/sites/steveandriole/2019/11/20/forrester-research-gets-cloud--computing-trends-right/#5b30ee4468a2.
5 Esempi sono il National Intelligence Law of the People's Republic of China, il Clarifying Lawful Overseas Use of Data Act (CLOUD Act) o il Foreign Intelligence Surveillance (FISA).

3.3 Aspetti di Resilienza

Le infrastrutture e i servizi Cloud che supportano le applicazioni della PA, e le funzioni essenziali del Paese, dovranno adottare opportuni accorgimenti, di tipo procedurale e tecnico, di sicurezza, ridondanza e interoperabilità. Infatti, per innalzare il livello di resilienza nei confronti di incidenti, quali attacchi cyber e/o guasti tecnici, si renderà necessaria da un lato l'applicazione di controlli di sicurezza stratificati (es. pseudoanonimizzazione, cifratura con gestione on-premise delle chiavi, ecc.) conformi ai requisiti specifici dei dati trattati, e dall'altro l'introduzione di funzionalità di continuità di servizio e disaster recovery in siti geograficamente distribuiti sul territorio nazionale.
In particolare, sebbene le prassi e gli standard tecnici internazionali siano largamente applicati dai fornitori di servizi Cloud, vista la criticità dei dati e dei servizi coinvolti, la strategia di migrazione al Cloud non può prescindere da un processo di *qualificazione dei fornitori di Cloud pubblico e dei loro servizi*.
Inoltre, la qualificazione non deve limitarsi a valutare gli aspetti di sicurezza sopra richiamati, ma anche quelli architetturali e organizzativi, poiché pure questi ultimi possono incidere sulla resilienza dei servizi forniti, ad esempio, in situazioni di *vendor lock-in*.
Un'altra importante direzione, in linea con le recenti iniziative e direttive dell'agenda digitale europea[6], è quella della standardizzazione, dell'armonizzazione e dell'interoperabilità dei servizi Cloud. In quest'ottica, con il coinvolgimento anche dell'Italia, è stato avviato il progetto GAIA-X[7] con l'obiettivo di sviluppare requisiti comuni per un'infrastruttura dati europea. Il progetto, rivolto alle imprese europee, mira a costituire un ecosistema digitale aperto e resiliente mediante la federazione di servizi Cloud, basati su standard comuni a garanzia di trasparenza e interoperabilità, in grado di collegare infrastrutture centralizzate e decentralizzate trasformandole in un sistema omogeneo.



6 https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age_en
7 https://www.data-infrastructure.eu/

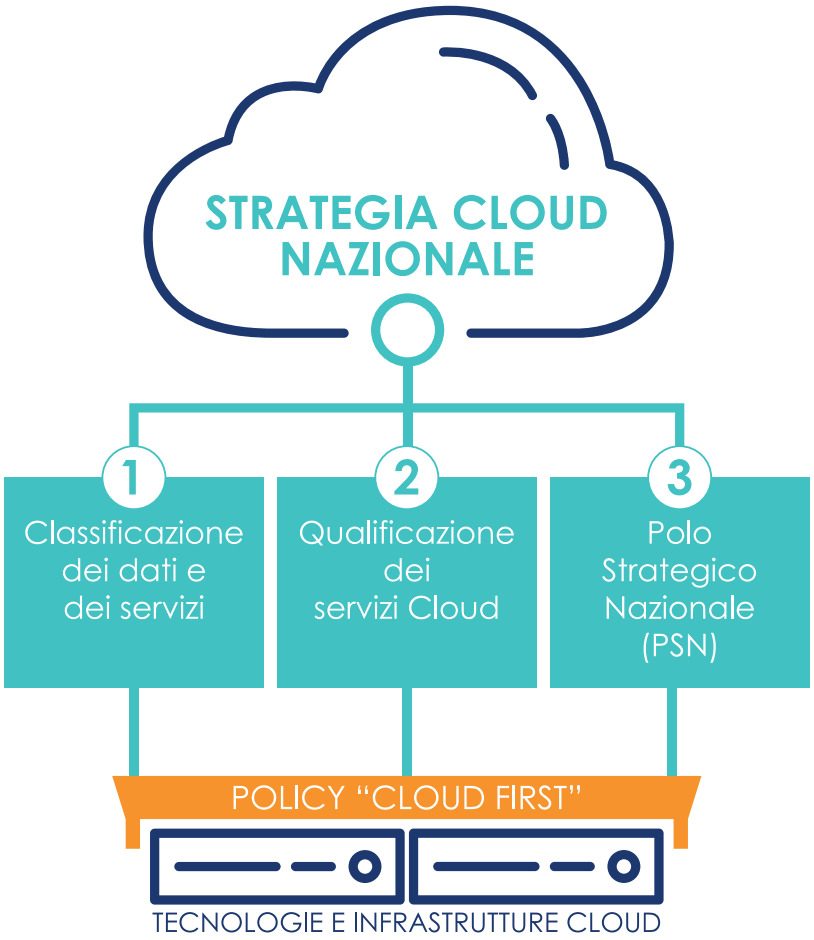
4. La strategia Cloud per la Pubblica Amministrazione

Attualmente, la maggior parte dei servizi pubblici vengono erogati tramite data center della PA che spesso non possiedono caratteristiche sufficienti per assicurare adeguati standard di affidabilità e resilienza[8]. Raggiungere e mantenere tali standard richiede investimenti e competenze che oggi non sono a disposizione di molte delle pubbliche amministrazioni centrali e locali. La *Strategia Cloud Italia* si pone in questo contesto come metodologia implementativa della policy "*Cloud-First*", pilastro del progetto di digitalizzazione della PA enunciato nel PNRR italiano. Questa policy permetterà di *guidare, e favorire l'adozione sicura, controllata e completa delle tecnologie Cloud per la PA*, con l'obiettivo, a tendere, che tutti i servizi erogati siano basati su applicazioni "*Cloud-native*", sviluppate cioè nativamente sulla base dei paradigmi Cloud.

La strategia Cloud per la PA si declina quindi sulla base delle seguenti linee di indirizzo strategico:

1. ***Classificazione dei Dati e dei Servizi:*** definizione di un processo di classificazione dei dati per guidare e supportare la migrazione dei dati e servizi della PA sul Cloud;
2. ***Qualificazione dei Servizi Cloud:*** realizzazione di un processo sistematico di scrutinio e qualificazione dei servizi Cloud utilizzabili dalla PA;
3. ***Polo Strategico Nazionale:*** creazione di un'infrastruttura nazionale per l'erogazione di servizi Cloud, la cui gestione e controllo siano autonomi da soggetti extra UE.

La realizzazione di queste macro-azioni permetterà di armonizzare e regolamentare l'adozione del Cloud nella PA, nonché applicare economie di scala per favorire una riduzione dei costi di gestione offrendo servizi digitali più affidabili e resilienti.



8 Dall'ultimo censimento AgID risulta come, ad oggi, il 95% dei circa 11mila data center utilizzati dagli enti pubblici italiani presenta carenze nei requisiti minimi di sicurezza, affidabilità, capacità elaborativa ed efficienza.

4.1 La classificazione dei dati e dei servizi

L'ampio spettro dei servizi Cloud disponibili, alla luce delle sfide tecnologiche e normative presentate, deve essere adottato in modo regolamentato così da mitigare i rischi sistemici dell'adozione del Cloud. L'elemento fondamentale per tale regolamentazione è individuare un *processo sistematico di classificazione dei dati e dei servizi* gestiti dalle PA, il cui risultato possa essere utilizzato per uniformare e guidare il processo di migrazione al Cloud della PA. Le classi dei dati e servizi sono identificate sulla base del danno che una loro compromissione, in termini di confidenzialità, integrità e disponibilità, provocherebbe al sistema Paese. Tali classi sono:

- ***Strategico:*** dati e servizi la cui compromissione può avere un impatto sulla sicurezza nazionale;
- ***Critico:*** dati e servizi la cui compromissione potrebbe determinare un pregiudizio al mantenimento di funzioni rilevanti per la società, la salute, la sicurezza e il benessere economico e sociale del Paese;
- ***Ordinario:*** dati e servizi la cui compromissione non provochi l'interruzione di servizi dello Stato o, comunque, un pregiudizio per il benessere economico e sociale del Paese.

Questa classificazione astrae da specifiche normative e requisiti di sicurezza descrivendo esclusivamente l'impatto per il sistema Paese di una eventuale compromissione di certi dati e servizi. L'applicazione del processo di classificazione, di seguito definito, permetterà un'analisi guidata degli impatti, nonché di eventuali requisiti di sicurezza e normativi, per l'identificazione dell'opportuna classe. Ad esempio, i dati e servizi afferenti funzioni essenziali dello Stato, ovvero identificati nell'ambito del PSNC, saranno classificati come *strategici*, i dati sanitari dei cittadini saranno classificati come *critici*, mentre dati e servizi relativi a portali istituzionali delle amministrazioni saranno classificati come *ordinari*.

4.2 La qualificazione dei servizi Cloud

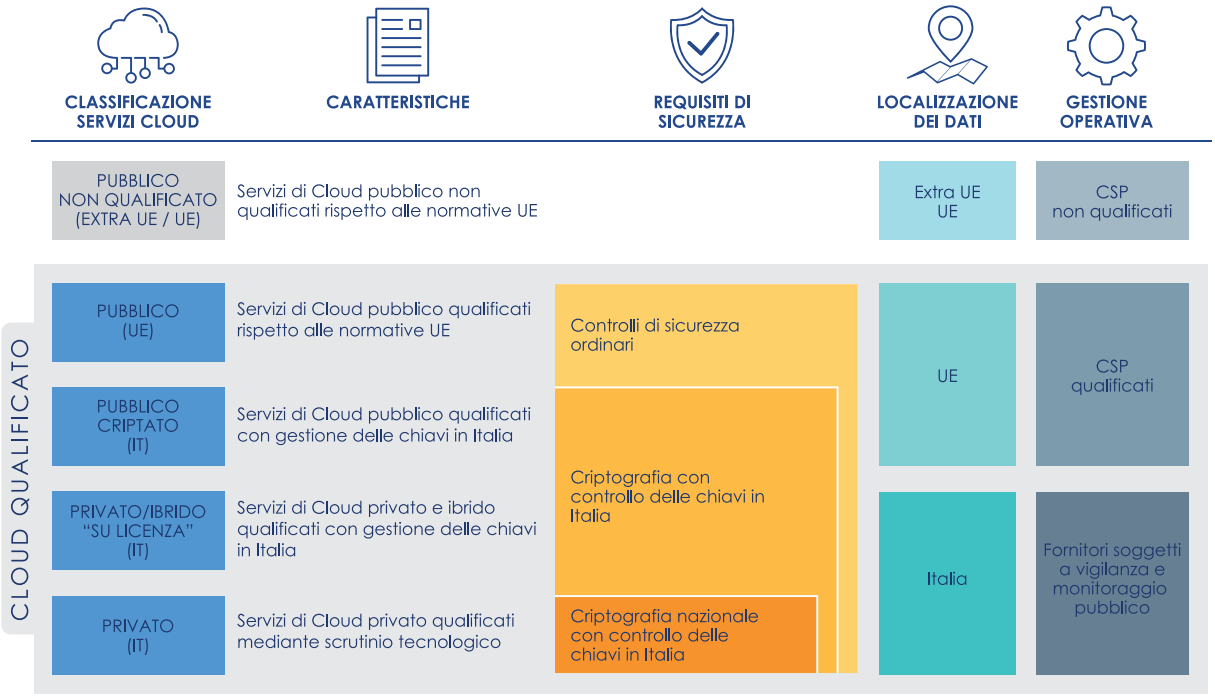
L'acquisizione di servizi Cloud da parte delle pubbliche amministrazioni avviene mediante procedure di acquisto la cui scarsa flessibilità difficilmente permette di tenere il passo del mercato e, soprattutto, di valutare gli effettivi rischi tecnici e organizzativi connessi all'adozione di uno specifico servizio.
Nella prospettiva di facilitare e guidare l'implementazione della policy "*Cloud-First*" per la PA, risulta dirimente offrire un *servizio di qualificazione ex-ante dei servizi Cloud acquistabili dalla PA*. Tale qualificazione, partendo dall'esperienza maturata da AgID, si pone l'obiettivo di semplificare e regolamentare, sia dal punto di vista tecnico che amministrativo, l'adozione di servizi Cloud. Alla luce della classificazione proposta e delle sfide poste dall'adozione del Cloud, la qualificazione dei servizi Cloud non potrà prescindere dall'analisi dei seguenti aspetti:

1. *gestione operativa* dei servizi Cloud, con dettaglio sugli standard tecnico-organizzativi applicati[9] e sulle misure di controllo sui dati;
2. *requisiti di sicurezza* applicati nella gestione dei dati ed erogazione di servizi, quali le modalità di gestione delle chiavi di cifratura e i controlli di sicurezza applicati;
3. *condizioni contrattuali* applicate all'erogazione del servizio (*Service-Level Agreement, SLA*) e alla sua rendicontazione, quali le garanzie di disponibilità e altri strumenti contrattuali a disposizione delle amministrazioni.

Sulla base dell'analisi delle soluzioni tecnologiche e organizzative disponibili sul mercato, i tre aspetti di analisi permettono di individuare a priori la qualificazione dei servizi Cloud riportata di seguito.

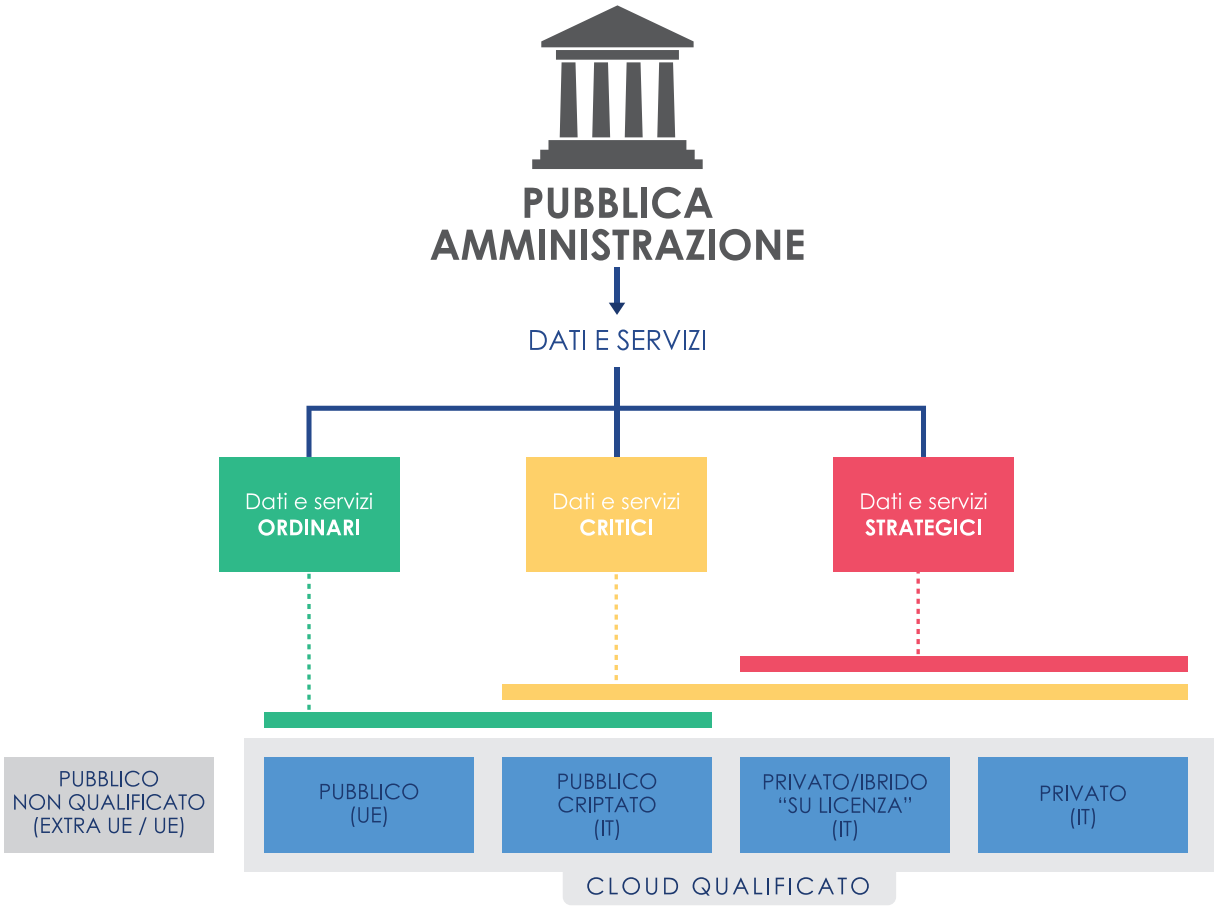
- I servizi di *Cloud Pubblico non qualificato (extra UE/UE)*, ovvero quei servizi che non rispondono ai criteri tecnico-organizzativi e normativi individuati in precedenza.
- I servizi di *Cloud Pubblico qualificato (UE)* compatibili con legislazioni rilevanti in materia (es. GDPR e NIS) che consento la localizzazione dei dati in UE e il rispetto di requisiti di sicurezza tecnico-organizzativi, tipicamente sulla base di sistemi di cifratura granulare gestiti dal fornitore CSP[10].

9 Ad esempio gli standard internazionali ISO 27017/27018, ISO 22301 e CSA STAR.
10 Tali servizi possono includere sistemi di gestione delle chiavi (KMS) realizzati con moduli hardware (HSM).



- I servizi di Cloud pubblico con controllo *on-premise* dei meccanismi di sicurezza, c.d. *Cloud Pubblico Criptato (IT),* che consentono di incrementare significativamente il livello di controllo sui dati e servizi, introducendo un maggior livello di autonomia dai CSP extra-UE nella gestione operativa e il controllo delle infrastrutture tecnologiche[11].
- Soluzioni di Cloud privato e ibrido, infine, permettono la localizzazione dei dati in Italia e maggior isolamento dalle region pubbliche dei principali CSP. Tali garanzie di autonomia sono ottenute mediante la gestione operativa da parte di un fornitore soggetto a vigilanza e monitoraggio pubblico. Queste implementazioni si possono distinguere tra:
  1. soluzioni basate su tecnologia hyperscaler licenziata da uno o più CSP, c.d. *Cloud privato/ ibrido "su licenza" (IT)*, oppure
  2. soluzioni basate su tecnologie commerciali qualificate mediante procedure di scrutinio e certificazione tecnologica, c.d. *Cloud Privato Qualificato (IT)*.

11 Ad esempio, mediante utilizzo di un HSM on-premise per la gestione delle chiavi utilizzate per la cifratura dei dati sul Cloud Pubblico.



I servizi Cloud qualificati potranno essere utilizzati, in accordo alla classificazione dei dati, con i seguenti vincoli:

- le offerte di Cloud Pubblico Qualificato e Pubblico Criptato, potranno ospitare dati e servizi *ordinari*;
- le offerte di Cloud Pubblico Criptato, Privato/Ibrido "su licenza" e Privato Qualificato potranno ospitare dati e servizi *critici*;
- le offerte di Cloud Privato/Ibrido "su licenza" e Privato Qualificato potranno ospitare dati e servizi *strategici*;

Questo processo di adozione dei servizi Cloud nella PA, dovrà culminare con la realizzazione di un *mercato elettronico dei servizi Cloud qualificati*[12]. Tale mercato dovrà rappresentare il mezzo mediante il quale le amministrazioni saranno guidate, in accordo al processo di classificazione dei dati e dei servizi, nella scelta dei servizi Cloud per loro più idonei e all'acquisto diretto con strumenti amministrativi semplificati e pre-negoziati.

12 Tale proposta è analoga a quanto già realizzato con successo in altre nazioni, ad esempio, il Digital Marketplace del Regno Unito https://www.digitalmarketplace.service.gov.uk

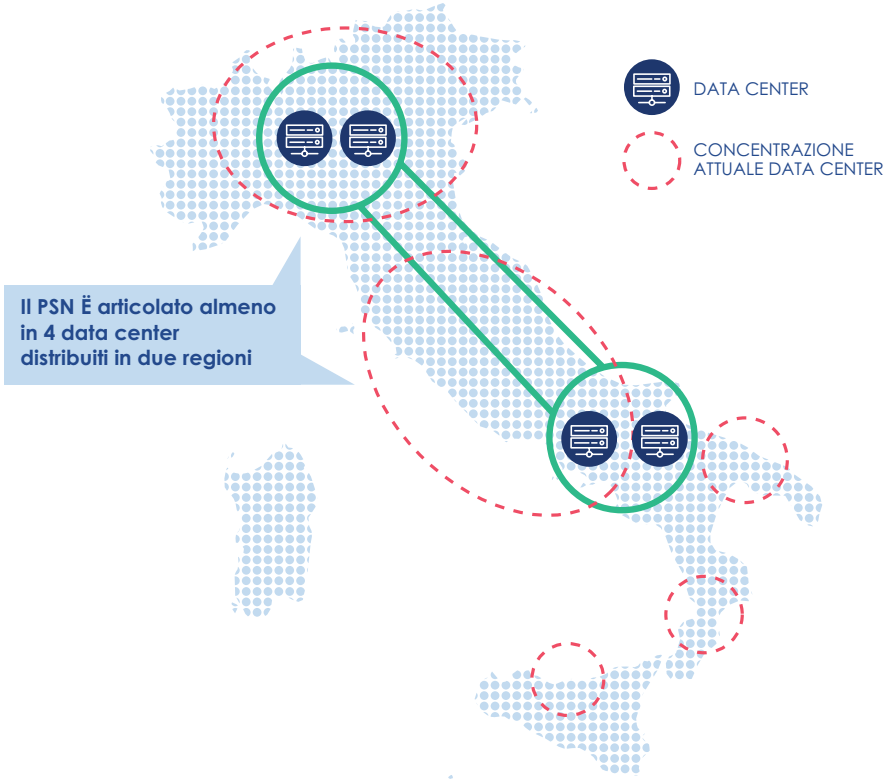
4.3 Il Polo Strategico Nazionale

Lo sviluppo di una nuova infrastruttura informatica a servizio della PA localizzata sul territorio nazionale, il *Polo Strategico Nazionale* (*PSN*)[13].

Il PSN ha infatti l'obiettivo di dotare la PA di tecnologie e infrastrutture Cloud che possano beneficiare delle più alte garanzie di affidabilità, resilienza e indipendenza. A tal fine, si prevede che il PSN sia *distribuito geograficamente* sul territorio nazionale presso siti opportunamente identificati[14], al fine di garantire adeguati livelli di continuità operativa e tolleranza ai guasti. La *gestione operativa* del PSN, sarà affidata a un fornitore qualificato sulla base di opportuni requisiti tecnico-organizzativi. Il fornitore dovrà garantire il controllo sui dati in conformità con la normativa in materia, nonché rafforzare la possibilità della PA di negoziare adeguate condizioni contrattuali con i fornitori di servizi Cloud.

Il PSN dovrà permettere alla PA di garantire, sin dalla progettazione (*by-design*), il rispetto dei requisiti in materia di sicurezza, ad esempio PSNC e NIS, e di abilitare la migrazione, almeno inizialmente con un processo *lift-and-shift*, verso tipologie di servizi Cloud IaaS e PaaS.

In accordo alla classificazione fornita nella sezione precedente, il PSN offrirà servizi di *Cloud Pubblico Criptato* (*IT*), ovvero permetterà di gestire, ad esempio, strumenti di cifratura *on-premise* integrati su Cloud pubblico per la PA, e offrirà lo spettro di servizi Cloud privato/ibrido, ovvero il *Cloud Privato/Ibrido "su licenza"* (*IT*), il *Cloud Privato Qualificato* (*IT*). Il PSN sarà destinato ad ospitare sul territorio nazionale principalmente dati e servizi strategici la cui compromissione può avere un impatto sulla sicurezza nazionale (in linea con quanto previsto in materia di perimetro di sicurezza nazionale cibernetica dal DL 21 settembre 2019, n. 105 e dal DPCM 81/2021) ma, a tendere, l'obiettivo del PSN, in accordo alle procedure di classificazione e qualificazione, è anche quello di offrire supporto alle amministrazioni centrali e alle principali amministrazioni locali, ad esempio Regioni, ASL e città metropolitane.

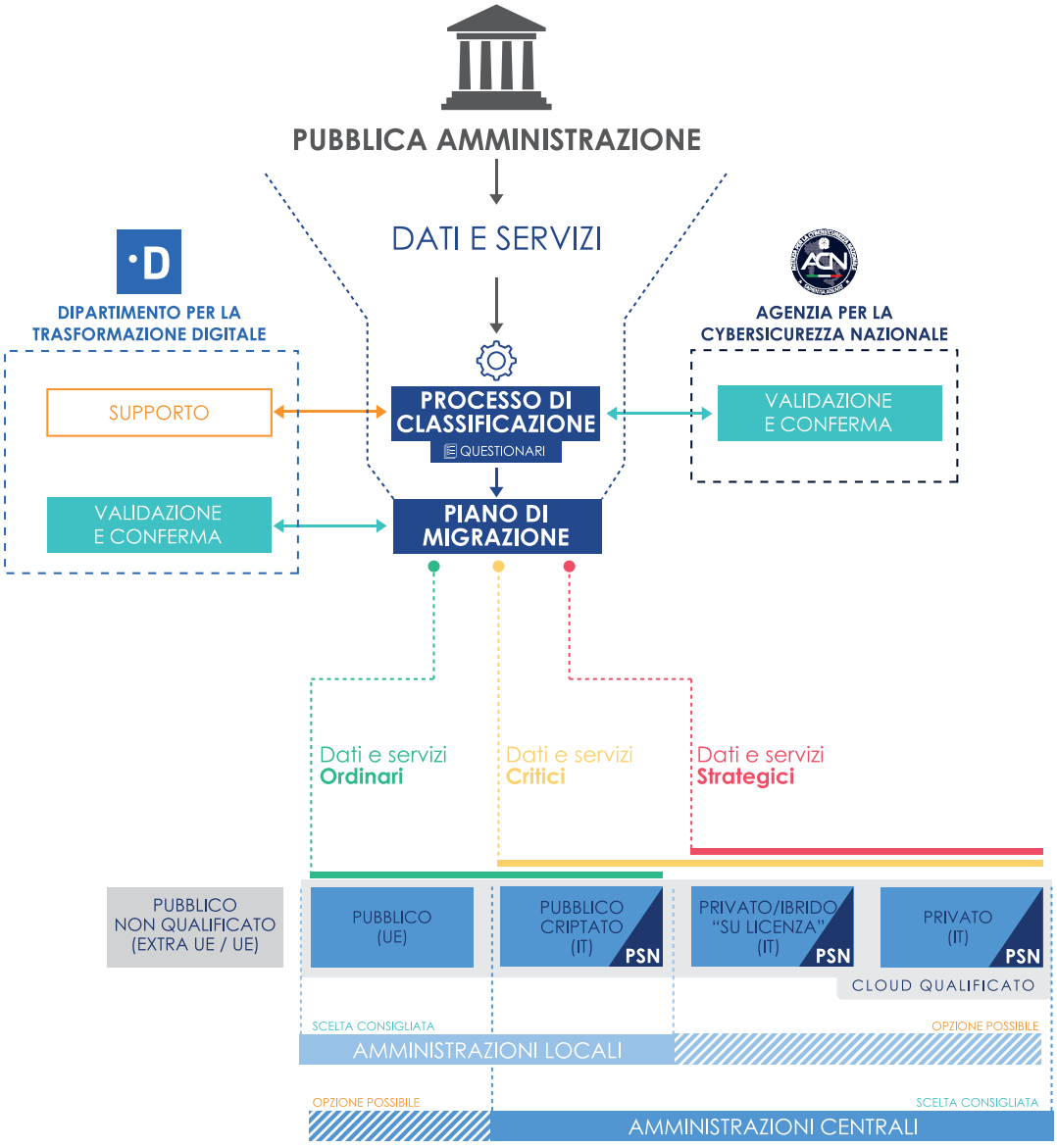


13 Così come previsto dall'articolo 33-septies, comma 4, del decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221.

14 Si pensi, ad esempio, ai livelli di sicurezza fisica dei data center, alla mitigazione del rischio di disastri naturali e all'integrazione con molteplici connettività.

5. La migrazione della Pubblica Amministrazione sul Cloud

La migrazione verso i diversi servizi Cloud qualificati e eventualmente all'interno del PSN dovrà essere governata tramite un processo centralizzato, agevole e uniforme per tutte le amministrazioni.
I piani di migrazione saranno quindi definiti in accordo con il risultato della classificazione dei dati e dei servizi. La classificazione e la redazione del piano di migrazione saranno definiti e supportati, per i rispettivi profili di competenza, dell'Agenzia per la Cybersicurezza Nazionale (ACN) e del Dipartimento per la Trasformazione Digitale (DTD).
Questo processo non potrà prescindere dalla responsabilizzazione del soggetto pubblico e permetterà di individuare e catalogare i dati e i servizi gestiti, applicando poi una categorizzazione rispetto agli impatti di eventuali compromissioni, dei vincoli normativi e di sicurezza.
L'esito della classificazione dei dati e servizi da migrare sul Cloud (ovvero dati strategici, critici o ordinari) permetterà di individuare i piani di migrazione al Cloud più idonei. Tali piani saranno validati e confermati dal Dipartimento e dall'Agenzia al fine di assicurare la congruità e il rispetto delle linee strategiche.



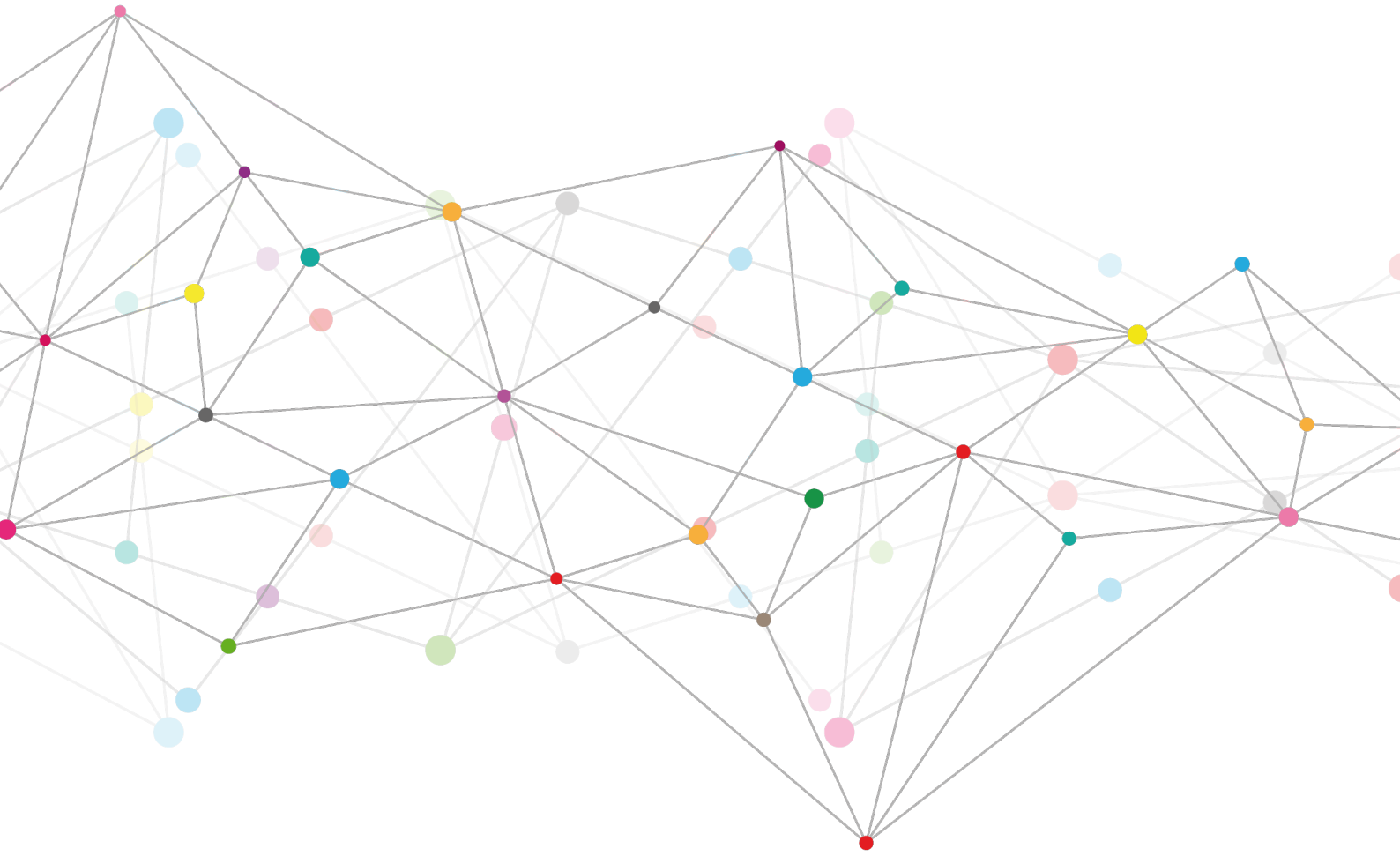
6. L'adozione della strategia Cloud

La Strategia Cloud Italia si articolerà in fasi successive secondo la scansione temporale di seguito proposta:

FASE 1 - *Pubblicazione del bando di gara per la realizzazione del PSN:* al più tardi entro la fine del 2021 si procederà a pubblicare il bando di gara per la realizzazione del PSN.

FASE 2 - *Aggiudicazione e Realizzazione del PSN*: al più tardi entro la fine del 2022 dovrà avvenire l'aggiudicazione del bando di gara.

FASE 3 - *Migrazione delle amministrazioni*: a partire dalla fine del 2022 dovrà iniziare la migrazione della PA verso il PSN, da concludersi entro la fine del 2025. Nella fase di migrazione verrà data precedenza alle PAC che attualmente operano con data center propri classificati, secondo il censimento AgID del patrimonio ICT della PA, in Categoria B (con carenze strutturali e/o organizzative o che non garantiscono la continuità dei servizi).



STRATEGIA CLOUD ITALIA

Dipartimento per la
Trasformazione Digitale

Agenzia per la
Cybersicurezza Nazionale