DIPARTIMENTO
PER LA TRASFORMAZIONE
DIGITALE

anci

Finanziato
dall'Unione europea
NextGenerationEU

GUIDA AI CONTRATTI DI SERVIZI CLOUD

Il sistema Anci a supporto della digitalizzazione dei Comuni

La presente linea guida è stata curata dallo staff del progetto

“Il sistema ANCI a supporto della digitalizzazione dei Comuni”

Redattrice: **Maria Catanese**

Supervisione del progetto: **Antonella Galdi,** Responsabile Area Innovazione tecnologica, Cultura, Politiche Giovanili, Mobilità sostenibile, TPL, Transizione energetica ANCI

Sommario

PREMESSA

Questo documento illustrativo e i modelli allegati, sono stati redatti con l'obiettivo di fornire al personale che si occupa di procurement per le amministrazioni comunali, un quadro di sintesi delle principali tappe che hanno portato il cloud computing ad imporsi come modello di riferimento dell'ICT. Il documento è rivolto in particolare ai dipendenti con competenze amministrative, in modo tale da dare loro il quadro degli elementi essenziali che caratterizzano il modello Cloud e l'indicazione dei principali atti normativi e di indirizzo tecnico/amministrativo di riferimento.

L'acquisto di servizi cloud presenta delle peculiarità significative rispetto ad altri ambiti del procurement ICT, in quanto presuppone scelte di governance che richiedono attività di analisi e revisione dei processi dell'amministrazione e attività di assesment dei servizi informativi e delle infrastrutture.

Indispensabili strumenti a supporto di questa fase di impostazione della strategia cloud delle amministrazioni sono i documenti presenti sul portale: https://docs.italia.it/

Di particolare importanza, il documento "Manuale di abilitazione al cloud"[1] che fa parte del Cloud Enablement Kit e che descrive l'insieme di metodi, strumenti e buone pratiche che le pubbliche amministrazioni dovrebbero usare per la migrazione al cloud di infrastrutture e applicativi esistenti. Il Manuale di abilitazione al cloud è strutturato in modo tale da essere uno strumento di supporto dalla fase di identificazione degli applicativi da migrare, fino alla valutazione degli indicatori di risultato a migrazione avvenuta.

Solo a valle di queste necessarie valutazioni di strategia, si colloca la programmazione dell'acquisto dei servizi cloud e la definizione della documentazione contrattuale.

I documenti contrattuali, oltre che essere conformi alle principali fonti in materia di appalti pubblici (Dlgs 36/2023 e ss modifiche - Codice dei contratti pubblici) e in materia di digitalizzazione della pubblica amministrazione (Dlgs 82/2005 e ssmm - Codice dell'Amministrazione Digitale), devono rispettare le numerose norme specifiche relative al cloud e gli atti di indirizzo tecnico amministrativo emanati dalle autorità competenti. I modelli di capitolato riportano l'indicazione della normativa e degli atti amministrativi di riferimento.

Nell'ambito dei servizi cloud, più che in altre categorie di acquisti ICT, ogni contratto presenta delle specificità che rendono difficile l'astrazione e la generalizzazione; è sempre necessaria un'analisi particolare che porta a scelte contrattuali mirate.

Tuttavia, descrivendo gli elementi generali che caratterizzano il modello cloud è possibile ricavare indicazioni su quali siano le clausole contrattuali da redigere con particolare cura, anche in funzione della mitigazione delle criticità insite nel modello stesso.

1 https://docs.italia.it/italia/manuale-di-abilitazione-al-cloud/manuale-di-abilitazione-al-cloud-docs/it/bozza/pianificare-la-migrazione/sla-richiesti-ai-servizi-qualificati.html

1 - LE TAPPE DELL'AFFERMAZIONE DEL MODELLO CLOUD

1.1 - Codice dell'Amministrazione Digitale – CAD (D.Lgs n. 82 del 7 marzo 2005 e ssmm)

Il Capo VI del Dlgs 82/2005 disciplina lo sviluppo, acquisizione e riuso di sistemi informatici delle Pubbliche Amministrazioni e nel definire le linee di indirizzo dell'analisi comparativa delle soluzioni che deve guidare il procurement, l'art. 68 comma 1, preliminarmente individua le opzioni di modelli di acquisizione/fruizione disponibili cui è possibile fare ricorso per soddisfare il fabbisogno:

a) software sviluppato per conto della pubblica amministrazione;
b) riutilizzo di software o parti di esso sviluppati per conto della pubblica amministrazione;
c) software libero o a codice sorgente aperto;
d) software fruibile in modalità cloud computing;
e) software di tipo proprietario mediante ricorso a licenza d'uso;
f) software combinazione delle precedenti soluzioni.

In attuazione dell'art. 68 comma 1 ter del CAD, Agid ha approvato con determinazione n. 115 del 9 maggio 2019[2], le Linee Guida sull'acquisizione e il riuso di software nelle pubbliche amministrazioni; documento in cui vengono definiti i criteri con cui le amministrazioni devono effettuare la valutazione tecnico-economica per definire le modalità di acquisizione del software.

Il percorso indicato dalle linee guida prevede che la valutazione tecnica, da parte delle amministrazioni, si sviluppi attraverso tre fasi principali:

1. **Individuazione dell'esigenza** – in questa fase l'amministrazione definisce con chiarezza il proprio bisogno, identificando anche eventuali vincoli di natura normativa o tecnologica e precisando le specifiche esigenze operative.
2. **Analisi delle soluzioni a riuso e open source** – si verifica la disponibilità di software già esistente, riutilizzabile o basato su licenze aperte, in grado di soddisfare i requisiti individuati.
3. **Valutazione di altre soluzioni** – qualora non siano disponibili opzioni a riuso o open source adeguate, si procede ad analizzare altre possibilità, come l'adozione di soluzioni proprietarie o lo sviluppo di software ex novo.

Il processo di verifica deve essere orientato in ogni caso all'individuazione di soluzioni che **privilegino l'utilizzo di formati di dati e di interfacce di tipo aperto**, nonché di standard in grado di assicurare **l'interoperabilità e la cooperazione applicativa** tra i diversi sistemi informatici della pubblica amministrazione; deve essere inoltre garantita la **sicurezza** e la conformità alla normativa in materia di **protezione dei dati personali.**

La verifica di tipo economico si basa sulla definizione del **Total Cost of Ownership (TCO)** delle soluzioni, calcolato su una finestra temporale adeguata al contesto della valutazione. Il TCO deve tenere in considerazione tutti gli elementi che concorrono al costo dell'intero ciclo di vita della soluzione (ad esempio, costi per l'acquisto di hardware e licenze software proprietarie necessari alla messa in esercizio del software che si sta acquisendo, costi per la personalizzazione del software, costi di manutenzione, correttiva ed evolutiva, costi di formazione, costi di migrazione dei dati).

Il TCO deve essere definito in relazione alla scelta delle soluzioni open source, nel processo di verifica della fase 2 e in relazione alla scelta fra soluzioni proprietarie o

2 https://www.agid.gov.it/it/design-servizi/riuso-open-source/linee-guida-acquisizione-riuso-software-pa

soluzioni realizzate ad hoc, nell'ambito della fase 3 (qualora il processo di verifica di soluzioni a riuso open source della fase 2 non abbia dato un esito positivo).

Nel processo di definizione delle modalità di acquisizione di software, il cloud computing rappresenta un possibile modello di fruizione (acquisto di soluzioni SaaS qualificate sul Cloud Marketplace), contrapposto alla scelta di installazione del software su server nella disponibilità dell'amministrazione. Ma sarebbe riduttivo fermarsi a questa classificazione.

L'adozione di un modello di servizi ICT incentrato sul cloud computing non rappresenta solo una scelta di tipo tecnologico, ma comporta una profonda revisione organizzativa della pubblica amministrazione, come si evince dall'analisi degli atti normativi di seguito descritti.

1.2 - Decreto-legge 179 del 18 ottobre 2012 e ssmm (art 33-septies)

L'Art.33-septies del Decreto-legge n. 179 del 2012[3] , nella sua progressiva evoluzione a seguito di interventi di modifica, è il riferimento normativo che ha disciplinato l'adozione del *paradigma cloud*, avviata con il processo di razionalizzazione delle

3 (Consolidamento e razionalizzazione dei siti e delle infrastrutture digitali del Paese)
1. Al fine di **tutelare l'autonomia tecnologica del Paese**, **consolidare e mettere in sicurezza le infrastrutture digitali delle pubbliche amministrazioni** di cui all'articolo 2, comma 2, lettere a) e c) del decreto legislativo 7 marzo 2005, n. 82, **garantendo, al contempo, la qualità, la sicurezza, la scalabilità, l'efficienza energetica, la sostenibilità economica e la continuità operativa dei sistemi e dei servizi digitali**, la Presidenza del Consiglio dei ministri promuove lo sviluppo di un'infrastruttura ad alta affidabilità localizzata sul territorio nazionale per la razionalizzazione e il consolidamento dei Centri per l'elaborazione delle informazioni (CED) definiti al comma 2, destinata a tutte le pubbliche amministrazioni. Le amministrazioni centrali individuate ai sensi dell'articolo 1, comma 3, della legge 31 dicembre 2009, n. 196, nel rispetto dei principi di efficienza, efficacia ed economicità dell'azione amministrativa, migrano i loro Centri per l'elaborazione delle informazioni (CED) e i relativi sistemi informatici, privi dei requisiti fissati dal regolamento di cui al comma 4, verso l'infrastruttura di cui al primo periodo o verso altra infrastruttura propria già esistente e in possesso dei requisiti fissati dallo stesso regolamento di cui al comma 4. Le amministrazioni centrali, in alternativa, possono migrare i propri servizi verso soluzioni cloud, nel rispetto di quanto previsto dal regolamento di cui al comma 4.
1-bis. *Le amministrazioni locali individuate ai sensi dell'articolo 1, comma 3, della legge 31 dicembre 2009, n.196, nel rispetto dei principi di efficienza, efficacia ed economicità dell'azione amministrativa, migrano i loro Centri per l'elaborazione delle informazioni (CED) e i relativi sistemi informatici, privi dei requisiti fissati dal regolamento di cui al comma 4, verso l'infrastruttura di cui al comma 1 o verso altra infrastruttura già esistente in possesso dei requisiti fissati* dallo stesso regolamento di cui al comma 4. Le amministrazioni locali, in alternativa, possono migrare i propri servizi verso soluzioni cloud nel rispetto di quanto previsto dal regolamento di cui al comma 4.
1-ter. L'Agenzia per l'Italia digitale (AgID), effettua con cadenza triennale, anche con il supporto dell'Istituto Nazionale di Statistica, **il censimento dei Centri per l'elaborazione delle informazioni (CED) della pubblica amministrazione** di cui al comma 2 **e, d'intesa con la competente struttura della Presidenza del Consiglio dei ministri,** nel rispetto di quanto previsto dai commi 1 e 1-bis e dalla disciplina introdotta dal decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, **definisce nel Piano triennale per l'informatica nella pubblica amministrazione la strategia di sviluppo delle infrastrutture digitali delle amministrazioni** di cui all'articolo 2, comma 2, lettere a) e c), del decreto legislativo 7 marzo 2005, n. 82, e **la strategia di adozione del modello cloud per la pubblica amministrazione**, alle quali le amministrazioni si attengono. Per la parte relativa alla strategia di sviluppo delle infrastrutture digitali e della strategia di adozione del modello cloud delle amministrazioni locali è sentita la Conferenza unificata di cui all'articolo 8 del decreto legislativo 28 agosto 1997, n. 281.
2. Con il termine CED è da intendere il sito che ospita uno o più sistemi informatici atti alla erogazione di servizi interni alle amministrazioni pubbliche e servizi erogati esternamente dalle amministrazioni pubbliche che al minimo comprende risorse di calcolo, apparati di rete per la connessione e sistemi di memorizzazione di massa.
3. Dalle attività previste al comma 1 sono esclusi i CED soggetti alla gestione di dati classificati secondo la normativa in materia di tutela amministrativa delle informazioni coperte da segreto di Stato e di quelle classificate nazionali secondo le direttive dell'Autorità nazionale per la sicurezza (ANS) che esercita le sue funzioni tramite l'Ufficio centrale per la segretezza (UCSe) del Dipartimento delle informazioni per la sicurezza (DIS).
4. L'Agenzia per la cybersicurezza nazionale, con proprio regolamento, d'intesa con la competente struttura della Presidenza del Consiglio dei ministri, nel rispetto della disciplina introdotta dal decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, **stabilisce i livelli minimi di sicurezza, capacità elaborativa, risparmio energetico e affidabilità delle infrastrutture digitali per la pubblica amministrazione, ivi incluse le infrastrutture di cui *((al comma 1))*. Definisce, inoltre, le caratteristiche di qualità, di sicurezza, di performance e scalabilità, interoperabilità, portabilità dei servizi cloud per la pubblica amministrazione. Con lo stesso regolamento sono individuati i termini e le modalità con cui le amministrazioni devono effettuare le migrazioni di cui ai commi 1 e 1-bis nonché le modalità del procedimento di qualificazione dei servizi cloud per la pubblica amministrazione.**
4-bis. Le disposizioni del presente articolo si applicano, fermo restando quanto previsto dalla legge 3 agosto 2007, n. 124, nel rispetto dell'articolo 2, comma 6, del decreto legislativo 7 marzo 2005, n. 82 e della disciplina e dei limiti derivanti dall'esercizio di attività e funzioni in materia di ordine e sicurezza pubblici, di polizia giudiziaria, nonché quelle di difesa e sicurezza nazionale svolte dalle infrastrutture digitali dell'amministrazione della difesa.
4-quater. Gli obblighi di migrazione previsti ai commi precedenti non si applicano alle amministrazioni che svolgono le funzioni di cui all'articolo 2, comma 6, del decreto legislativo 7 marzo 2005, n. 82. **4-quinquies.** La violazione degli obblighi previsti dal presente articolo è accertata dall'AgID ed è punita ai sensi dell'articolo 18-bis del decreto legislativo 7 marzo 2005, n. 82.
5. Dall'attuazione del presente articolo non derivano nuovi o maggiori oneri o minori entrate per il bilancio dello Stato.

infrastrutture ICT della pubblica amministrazione, al fine di rendere l'intero sistema sempre più efficiente, resiliente, sicuro e quindi più competitivo.

Lo scenario emergenziale imposto dalla pandemia ha accelerato un processo già attivato negli anni precedenti, che ha visto la prima tappa significativa nell'approvazione del **Piano Triennale per l'informatica della PA**, che, nell'edizione 2017/2019, introduceva il Modello Cloud della PA, che descrive l'insieme di infrastrutture IT e servizi cloud qualificati da AGID a disposizione della PA, la definizione e attuazione del programma nazionale di abilitazione al Cloud della PA e l'applicazione del principio cloud first, in base al quale: prima di qualsiasi altra opzione tecnologica, le PA sono tenute ad adottare il paradigma Cloud.

Il Piano Triennale 2019/2021 ha posto le basi per l'implementazione del modello definito nell'edizione precedente del documento, dando concreto impulso all'azione di razionalizzazione delle infrastrutture ICT.

Tappa fondamentale di questo processo è stato il censimento del patrimonio ICT delle Pubbliche Amministrazioni, avviato con la Circolare AGID 1/2019 finalizzato a definire il quadro dei data center utilizzati dalle Pubbliche Amministrazioni e avviare un processo di dismissione di quelli che presentavano un'inaccettabile obsolescenza.

A conclusione del censimento, nel febbraio 2020, sono stati individuati i data center candidabili all'utilizzo da parte del polo strategico nazionale o in possesso dei requisiti per essere classificati come Gruppo A.

Per le Amministrazioni che utilizzavano data center classificati nel gruppo B (quindi non in possesso dei requisiti richiesti dalla Circolare 1/2019), scattava l'impossibilità di investire ulteriori risorse su questa infrastruttura e l'obbligo di migrare verso il cloud.

Gli eventi straordinari derivanti dall'emergenza pandemica hanno accentuato l'esigenza di consolidare il Modello Cloud della PA e con l'art. 35 del DL 76 del 16 luglio 2020 (convertito con la Legge 120/2020), che dettava "Misure urgenti per la semplificazione e l'innovazione digitale", veniva modificato l'art. 33-septies del Decreto-legge n. 179 del 2012.

Nella nuova formulazione, l'art. 33-septies, al comma 1 prevede che "la Presidenza del Consiglio dei ministri promuove lo sviluppo di un'infrastruttura ad alta affidabilità localizzata sul territorio nazionale per la razionalizzazione e il consolidamento dei Centri per l'elaborazione delle informazioni (CED), destinata a tutte le pubbliche amministrazioni". La disposizione ha trovato attuazione con la realizzazione del **Polo Strategico Nazionale.**

Per le amministrazioni locali, il comma 2 pone l'obbligo di migrare i propri CED (e i relativi sistemi informatici) privi dei requisiti fissati dal Regolamento approvato da AGID, verso l'infrastruttura nazionale o in alternativa migrare i propri servizi verso soluzioni cloud.

1.3 - Strategia Cloud Italia[4]

Nel 2021 è stato definito il documento di indirizzo realizzato congiuntamente dal Dipartimento per la Trasformazione Digitale (DTD) e dall'Agenzia per la cybersicurezza nazionale (***Strategia Cloud Italia***), che contiene gli indirizzi per la migrazione verso il cloud qualificato della Pubblica Amministrazione e che risponde a tre sfide principali: assicurare l'autonomia tecnologica del Paese, garantire il controllo sui dati e aumentare la resilienza dei servizi digitali.

4 https://innovazione.gov.it/dipartimento/focus/strategia-cloud-italia/

Il documento individua le tre direttrici di attuazione della strategia:

1. **Classificazione dei dati e servizi,** sulla base del danno che una loro compromissione, in termini di confidenzialità, integrità e disponibilità, provocherebbe al sistema Paese. Sulla base di questa valutazione, dati e servizi vengono classificati in:
   - ***Strategici:*** dati e servizi la cui compromissione può avere un impatto sulla sicurezza nazionale;
   - ***Critici:*** 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;
   - ***Ordinari***: 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.

2. **Qualificazione dei Servizi Cloud**. È un processo previsto per semplificare e rendere più efficiente il procurement di servizi cloud per le PA. Si basa sulla verifica preventiva dei servizi cloud, rispetto ai seguenti parametri:

- Gestione operativa dei servizi cloud;
- Sicurezza;
- Clausole contrattuali applicate all'erogazione del servizio (SLA), alla sua rendicontazione.

La Pubblica Amministrazione può comprare esclusivamente servizi cloud qualificati. I requisiti di qualificazione sono strettamente connessi alla classificazione.

3. **Polo Strategico Nazionale (PSN)**. infrastruttura informatica a servizio della PA localizzata sul territorio nazionale prevista dall'art. Art.33-septies del Decreto-legge n. 179 del 2012, comma 1.

Il documento, inoltre, definisce il processo di migrazione ai servizi Cloud qualificati, per tutte quelle amministrazioni obbligate a dismettere i propri CED.

Nella seguente tabella si riportano le diverse categorie di strategie di migrazione, con l'indicazione sintetica dei vantaggi e svantaggi che comporta l'utilizzo di ognuna e l'ipotesi di impiego consigliata.

Strategia di Migrazione	Descrizione	Vantaggi	Svantaggi	Quando usarla
Lift & Shift (Re-host)	Migrazione diretta dell'infrastruttura esistente sul cloud senza modifiche	- Rapida da implementare; - Bassi costi iniziali; - Nessuna modifica al codice applicativo	- Non sfrutta pienamente i benefici del cloud; - Possibile lock-in con il provider; - Scalabilità limitata rispetto a soluzioni cloud-native.	Quando serve una transizione veloce senza riscrivere le applicazioni
Re-platform	Ottimizzazione parziale delle applicazioni per sfruttare alcuni vantaggi del cloud (es. database gestiti, containerizzazione)	- Maggiore efficienza rispetto a Lift & Shift; - Riduzione costi operativi nel lungo periodo; - Possibile miglioramento delle prestazioni	- Richiede modifiche moderate al codice; - Tempi di migrazione più lunghi rispetto al semplice rehost	Quando si vuole migliorare le prestazioni senza una completa riscrittura
Refactor (Re-architect)	Modifica significativa delle applicazioni per adattarle a un'architettura cloud-native (es. microservizi, serverless)	- Massima scalabilità ed efficienza; - Riduzione dei costi operativi sul lungo periodo - Migliore resilienza e sicurezza	- Costi e tempi elevati; - Necessita competenze avanzate - Rischio di incompatibilità con sistemi legacy	Quando si vuole una soluzione a lungo termine con ottimizzazione cloud-native

Repurchase (Replace)	Sostituzione delle applicazioni esistenti con soluzioni SaaS equivalenti	- Elimina la necessità di gestione; hardware/ software - Costi prevedibili (abbonamenti) - Aggiornamenti automatici	- Possibile perdita di funzionalità personalizzate; - Difficoltà nell'integrazione con sistemi esistenti	Quando un SaaS può sostituire un'applicazione legacy con costi e tempi ridotti
Retain (Hybrid Cloud o Multi-Cloud)	Mantiene alcune applicazioni on-premise e altre vengono migrate nel cloud	- Maggiore controllo su dati sensibili: - Flessibilità nella gestione delle risorse: - Evita lock-in con un unico provider	- Complessità nella gestione; - Possibili problemi di interoperabilità tra on-premise e cloud	Quando si devono mantenere sistemi legacy o per esigenze di sicurezza

1.4 - Piano Nazionale Ripresa e Resilienza (PNRR)[5]

Gli interventi del PNRR che interessano direttamente l'ambito cloud fanno parte della Missione 1 *"Digitalizzazione, innovazione, competitività, cultura e turismo"*, Componente 1 "*Digitalizzazione, innovazione e sicurezza nella PA"*:

Intervento 1.1 Infrastrutture Digitali: obiettivo di questo investimento è garantire che i sistemi, i dataset e le applicazioni della Pubblica Amministrazione siano ospitati in **data center altamente affidabili e con elevati standard di qualità** per sicurezza, prestazioni, scalabilità, interoperabilità europea ed efficienza energetica. A tal fine, l'investimento prevede la creazione di un'**infrastruttura ibrida** nazionale all'avanguardia basata su **cloud** (denominata "Polo Strategico Nazionale", PSN) o la certificazione di alternative cloud pubbliche sicure e scalabili a cui seguirà la migrazione di dataset e delle applicazioni della pubblica amministrazione. Nel successivo paragrafo 1.5 verranno approfondite le caratteristiche del Polo Strategico Nazionale.

Intervento 1.2 Abilitazione e facilitazione migrazione al Cloud: obiettivo dell'investimento è realizzare la migrazione di dataset e applicativi di una parte sostanziale della pubblica amministrazione locale verso un'**infrastruttura cloud sicura**, consentendo a ciascuna amministrazione di operare una scelta tra una serie di ambienti cloud pubblici certificati.

La Missione 1 Componente 1 del PNRR prevede l'Investimento 1.2 "ABILITAZIONE AL CLOUD", che stanzia nel suo complesso 1 miliardo di euro destinati alla migrazione al cloud di Comuni, Scuole, Aziende Sanitarie e Aziende Ospedaliere.

In continuità con i precedenti Avvisi è stato da ultimo pubblicato l'Avviso Investimento 1.2 "Abilitazione al Cloud per le PA Locali " Comuni settembre 2024, all'interno della Missione 1 Componente 1 del PNRR, finanziato dall'Unione europea nel contesto dell'iniziativa NextGenerationEU. L'investimento è collegato all'obbligo, introdotto dall'art. 35 del D.L. 76/2020, per la PA di migrare i propri CED verso ambienti cloud.

Le milestone e i target europei previsti per l'Investimento 1.2 sono i seguenti:

- **milestone M1C1-125**, *conseguita a marzo 2023*: "Notifica dell'aggiudicazione di (tutti) i bandi pubblici per ogni tipo di amministrazione pubblica coinvolta (comuni, scuole, enti sanitari locali) per la raccolta e la valutazione dei piani di migrazione. La pubblicazione di tre bandi mirati consentirà al Dipartimento per la Trasformazione Digitale di valutare le esigenze specifiche di ciascun tipo di amministrazione pubblica interessata. Aggiudicazione degli appalti (ossia pubblicazione dell'elenco delle PA ammesse a ricevere finanziamenti) relativi a tre bandi di gara pubblici, rispettivamente, per i comuni, le scuole e le aziende sanitarie locali, al fine di raccogliere e valutare i piani di migrazione, in conformità agli orientamenti tecnici sull'applicazione del principio "non arrecare un danno significativo" (2021/C58/01)

5 https://areariservata.padigitale2026.gov.it/Pa_digitale2026_dettagli_avviso?id=a01J7000000O59tIAC

mediante l'uso di un elenco di esclusione e il requisito di conformità alla pertinente normativa ambientale dell'UE e nazionale";

- **target M1C1-139,** conseguito entro il termine previsto di *settembre 2024*: "La migrazione di (numero) 4.083 pubbliche amministrazioni locali verso ambienti cloud certificati sarà realizzata quando la verifica di tutti i sistemi e dataset e della migrazione delle applicazioni incluse in ciascun piano di migrazione sarà stata effettuata con esito positivo";
- **target M1C1-147** *da conseguirsi entro giugno 2026:* "La migrazione di (numero) 12.464 pubbliche amministrazioni locali verso ambienti cloud certificati sarà realizzata quando la verifica di tutti i sistemi e dataset e della migrazione delle applicazioni incluse in ciascun piano di migrazione sarà stata effettuata con esito positivo".

L'importo del finanziamento concedibile ai Soggetti Attuatori è individuato, ai sensi dell'art. 53 par. 1. Lett. c) del Reg. UE 1060/2021, in un importo forfettario (lump sum) determinato in funzione:

- delle modalità di Migrazione al Cloud;
- della classe di popolazione residente di riferimento del medesimo Soggetto attuatore.

Oggetto di migrazione potranno essere tutti i servizi erogati in tutte le loro forme dal singolo Ente e il cui livello complessivo di efficienza possa essere ottimizzato attraverso una migrazione verso piattaforme Cloud qualificate. L'obiettivo è la migrazione completa (Full Migration) degli asset ICT on premises dell'ente.

In risposta all'avviso, i Comuni potranno effettuare la migrazione avvalendosi dei due modelli di migrazione come delineato nella Strategia Nazionale per il Cloud, in conformità al Il Piano di Migrazione presentato:

- Trasferimento in sicurezza dell'infrastruttura IT;
- Aggiornamento in sicurezza di applicazioni in Cloud.

L'opzione Trasferimento in sicurezza dell'infrastruttura IT (Migrazione Tip. A) consente di sfruttare la strategia di migrazione Lift&Shift (anche detta Rehost).

L'opzione Aggiornamento in sicurezza di applicazioni in Cloud (Migrazione Tip. B), invece, offre la possibilità di migrare le applicazioni utilizzando una tra le strategie repurchase/replace e replatform.

Nella tabella seguente sono riportati i possibili strumenti di procurement attivabili in relazione ai modelli di migrazione previsti dal Piano di migrazione.

	Migrazione Tip. A	**Migrazione Tip. B**
	trasferimento in sicurezza dell'infrastruttura IT:	**aggiornamento in sicurezza di applicazioni in cloud:**
Stream/Task	migrazione al cloud secondo la strategia di migrazione Lift&Shift (anche detta Rehost), ovvero la migrazione dell'intero servizio dell'amministrazione, comprensivo di applicazioni e dati su un hosting cloud senza apportare modifiche agli applicativi, ovvero replicando il servizio esistente in un ambiente cloud	**repurchase/replace:** migrazione del servizio dell'amministrazione verso una soluzione nativa in cloud, in genere erogata in modalità Software as a Service; **replatform:** riorganizzazione dell'architettura applicativa sostituendo intere componenti del servizio in favore di soluzioni Cloud native in modo da usufruire dei benefici dell'infrastruttura Cloud**;** **re-architect:** ha come obiettivo quello di ripensare significativamente l'architettura core di un applicativo in ottica cloud, attraverso un processo di redesign iterativo ed incrementale che miri ad adottare appieno i servizi cloud-native offerti dai cloud service provider per massimizzare i benefici che ne derivano
Repurchase SaaS		Mepa/Acquistinrete

Analisi, assessment e consulenza per la definizione della strategia di migrazione (servizi di supporto)	Cloud Enabling - PSN	Cloud Enabling - PSN
Abilitazione e conduzione infrastrutturale e gestione infrastrutturale (Servizi Specialistici)	Cloud Enabling - PSN	Cloud Enabling - PSN
Integrazioni, sviluppi applicativi di tipo greenfield	SacPal3 o Data Management	SacPal3 o Data Management
Messa in sicurezza e Cyber	PSN - MEPA - Bundle Servizi Consulenziali a brand dedicati Lotto 1 – Servizi di sicurezza da remoto per la PAL Lotto 2 – Servizi di sicurezza da remoto, di compliance e controllo per le Pubbliche Amministrazioni	PSN - MEPA - Bundle Servizi Consulenziali a brand dedicati Lotto 1 – Servizi di sicurezza da remoto per la PAL Lotto 2 – Servizi di sicurezza da remoto, di compliance e controllo per le Pubbliche Amministrazioni

1.5 - Polo Strategico Nazionale

In attuazione della Strategia Cloud, il Dipartimento per la Trasformazione Digitale della Presidenza del Consiglio ha attivato il Polo Strategico Nazionale, infrastruttura informatica a servizio della PA localizzata sul territorio nazionale prevista dall'art. Art.33-septies del Decreto-legge n. 179 del 2012, comma 1.

A conclusione di una procedura ad evidenza pubblica di partenariato pubblico-privato, il DTD ha stipulato una convenzione con la società di nuova costituzione Polo Strategico Nazionale S.p.A., partecipata da TIM, Leonardo, Cassa Depositi e Prestiti (CDP, attraverso la controllata CDP Equity) e Sogei.

La convenzione ha ad oggetto la realizzazione e la gestione dell'infrastruttura progettata, predisposta ed allestita ad alta affidabilità, localizzata sul territorio nazionale, con caratteristiche adeguate ad ospitare la migrazione delle infrastrutture, delle applicazioni e dei dati frutto della razionalizzazione e del consolidamento dei Centri di elaborazione Dati e dei relativi sistemi informatici delle pubbliche amministrazioni.

Il PSN rappresenta quindi l'infrastruttura che consente di superare l'obsolescenza dei Centri di elaborazione dati utilizzati dalle amministrazioni, fornendo servizi caratterizzati da affidabilità, resilienza e indipendenza.

Possono aderire alla convenzione per utilizzare i servizi del PSN, le amministrazioni pubbliche centrali e locali e le aziende sanitarie.

Nella sezione Documentazione del sito del Polo Strategico Nazionale è possibile trovare tutta la documentazione relativa alla convenzione (in particolare la Guida alla Convenzione, che sintetizza i servizi acquistabili e l'iter amministrativo di adesione) e i template da utilizzare per perfezionare l'adesione[6].

Nella seguente tabella si propone la sintesi dei servizi acquistabili in adesione alla Convenzione. Esigenze di sintesi richiedono una necessaria operazione di semplificazione della complessità dei servizi offerti; per una descrizione dettagliata e puntuale dei servizi si rinvia alla documentazione contrattuale.

6 https://www.polostrategiconazionale.it/obiettivo-cloud/documentazione/

CATEGORIA SERVIZI	Dettaglio
Servizi di migrazione	***Re-host***: migrazione che trasferisce applicazioni in cloud senza modifiche
	Re-platform: migrazione che modifica alcune componenti delle applicazioni
	Re-architect: le applicazioni vengono reingegnerizzate secondo il paradigma cloud-native
Housing & Hosting	***Housing***: utilizzo di spazio nei Datacenter PSN
	Hosting: Utilizzo di server dedicati nell'ambito del PSN
Servizi di Private Cloud	***IaaS shared***: servizio che permette alle PA di condividere risorse virtualizzate e segregate.
	IaaS dedicated: servizio che consente alle Amministrazioni di gestire uno spazio cloud privato.
	Paas: soluzioni che permettono alle amministrazioni utenti di sviluppare ed erogare applicativi.
	CaaS: servizio cloud basato su Kubernetes per l'erogazione di container
	Cloud Storage: Soluzioni on demand per l'archiviazione e la gestione di grandi quantità di dati.
	Data Protection: Conservazione dei dati: dal backup al golden copy fino al disaster recovery.
Servizi Cloud con CSP	***Hybrid Cloud On PSN Sit***: Servizi privati e ibridi del Cloud Service Provider Microsoft Azure
	Public Cloud PSN Managed: Il servizio che permette di implementare una doppia separazione logica e fisica.
Servizi Accessori	***Multicloud***
	Connettività dedicata
	Antivirus
	Sistema Operativo Windows/ Linux
Servizi Professionali	***Security Services and Compliance***: servizio di trasferimento dati che si divide in due fasi: migrazione e verifica
	Infrastructure Service Operation: Team dedicati di supporto all'Amminstrazione per la gestione cloud.
	Business and Culture Enablement: servizi di formazione, consulenza e supporto agli utenti

1.6 - Regolamento ACN

In attuazione del comma 4 dell'art. 33-septies del DL 179 del 18 ottobre 2012, l'Agenzia per la Cybersicurezza Nazionale, d'intesa con il Dipartimento per la Trasformazione Digitale, ha adottato il ***Regolamento unico per le infrastrutture digitali e i servizi cloud per la Pubblica Amministrazione*** (Decreto Direttoriale n. 21007/24 del 27 giugno 2024).

Dopo il via libera del Garante della Privacy, il periodo di "stand still" della Commissione Europea e la pubblicazione, il nuovo Regolamento 21007/24 è diventato esecutivo dal 1 agosto 2024.

Ambito soggettivo di applicazione: Pubbliche Amministrazioni presenti nell'Elenco Istat, predisposto annualmente ai sensi dell'art.1 comma 3 della legge 31 dicembre 2009, n.196.

Il Regolamento:

- Armonizza la normativa in materia, proponendosi come testo di riferimento;
- Rende ordinari e permanenti istituti come la classificazione di dati e servizi, il Catalogo dei servizi qualificati e delle infrastrutture conformi ai requisiti;
- Definisce il processo di qualifica e adeguamento di servizi e infrastrutture gestito da ACN, che porta all'inserimento nel Catalogo. La qualifica ha una durata di 36 mesi. Le amministrazioni sono obbligate ad acquistare esclusivamente servizi e infrastrutture qualificate/adeguate;
- Definisce i livelli minimi per rendere i servizi e le infrastrutture cloud conformi alla normativa (ad esempio al GDPR) e a standard qualitativi. In particolare, per le infrastrutture digitali per la PA vengono definiti i livelli minimi in termini di *sicurezza e affidabilità*, *capacità elaborativa*, *risparmio energetico;* per i servizi cloud sulla base dei *parametri di qualità, sicurezza, performance e scalabilità*, *interoperabilità e portabilità*;
- Introduce fra le infrastrutture cloud, le **infrastrutture di housing e servizi di prossimità (edge),** questi ultimi utili nei casi in cui è necessario ridurre i tempi di latenza per gli utenti finali; sfruttando la capacità di elaborare i dati localmente, vicino alla fonte in cui vengono generati, il loro impiego migliora le performance che prevedono ad esempio elaborazioni di dati in tempo reale.
- Prevede meccanismi di monitoraggio ex post rispetto alla qualifica/adeguamento;
- Definisce un percorso che consente di recuperare i casi di inadempimento alle prescrizioni del Regolamento, arrivando alla revoca come ipotesi estrema.

Le disposizioni del Regolamento (soprattutto in tema di Qualificazione dei servizi) sono approfondite al successivo Paragrafo 3.1.

1.7 - Piano Triennale per l'Informatica nella PA - 2024/2026 (aggiornamento 2025)

Il capitolo 6 dell'aggiornamento 2025 al Piano Triennale è dedicato alle infrastrutture e descrive lo stato di attuazione della Strategia Cloud avviata nel 2021, che ha visto la realizzazione di due tappe fondamentali nell'attivazione del Polo Strategico Nazionale (PSN), infrastruttura di riferimento per le amministrazioni che intendono migrare al cloud (insieme alle altre infrastrutture qualificate e sicure che rientrano nel gruppo A in conclusione del censimento Agid di cui alla circolare 1/2019) e nell'approvazione del Regolamento per il Cloud della PA, approvato da ACN, che fra le altre disposizioni che regolano la materia (come analizzato al precedente paragrafo 1.6), disciplina le infrastrutture di housing e servizi di prossimità.

Il quadro delineato dal Piano Triennale prevede quindi i seguenti possibili scenari per le amministrazioni che attuano la Strategia Cloud:

- Adesione al Polo Strategico Nazionale, secondo le regole definite dalla Convenzione e descritte al precedente paragrafo 1.6;
- Utilizzo dei servizi erogati da un'infrastruttura adeguata secondo i requisiti definiti dal Regolamento ACN (infrastrutture incluse nel Gruppo A dal Censimento AGID di cui alla circolare 1/2019);
- Adozione del modello del *"cloud federato"*, in base al quale "*due o più cloud service provider che si uniscono mediante un accordo che preveda un insieme concordato*

di procedure, processi e regole comuni finalizzato all'erogazione di servizi cloud".

In base a questo modello, quindi, le amministrazioni possono sottoscrivere accordi per la realizzazione di cloud federati, costituiti dalle rispettive infrastrutture in possesso dei necessari requisiti di adeguatezza.

Viene inoltre evidenziato il principio del SaaS first, ossia: in caso di disponibilità all'interno del Catalogo dei servizi cloud per la PA qualificati da ACN di una soluzione SaaS che risponda alle esigenze delle amministrazioni, è opportuno valutare la migrazione verso il SaaS come soluzione prioritaria (principio SaaS-first) rispetto alle altre tipologie di soluzioni.

Il documento mette a fuoco i temi che le amministrazioni devono prendere in considerazione nell'impostazione e adozione dei processi di migrazione al cloud, indicando il portale https://cloud.italia.it/, quale punto di riferimento per reperire gli strumenti di supporto.

Le tematiche verso cui le amministrazioni sono invitate a porre l'attenzione sono:

- come riconoscere e gestire possibili situazioni di lock-in;
- raccomandazioni sugli aspetti legati al back up dei dati e al disaster recovery;
- consigli sulla scelta della migliore strategia di migrazione dal re-host al re-architect in base alle caratteristiche degli applicativi da migrare;
- come migliorare la migrazione in cloud grazie a un approccio DevOps;
- come definire e separare correttamente i ruoli tra Unità di Controllo (chi governa il progetto di migrazione) e Unità di esecuzione (chi realizza la migrazione);
- come misurare costi/benefici derivanti dalla migrazione;
- come stabilire un perimetro di responsabilità condivise tra amministrazione utente e fornitore di servizi cloud;
- come sfruttare al massimo le opportunità del cloud grazie alle applicazioni cloud native, al rearchitect e al re-purchase.

1.8 - Strumenti di acquisto CONSIP

Il principale strumento di e-procurement nel perimetro dei servizi cloud e delle iniziative strategiche ICT, messo a disposizione delle PP.AA., è rappresentato dall'offerta Consip sotto forma di:

- Strumenti contrattuali già definiti nei contenuti e stipulati con i fornitori aggiudicatari delle gare Consip (Convenzioni, Accordi quadro), utilizzabili per acquistare servizi aderendo con un ordine diretto o con rilancio competitivo (nel caso in cui ci sia l'esigenza di ulteriore personalizzazione);
- strumenti di negoziazione per gestire in autonomia le procedure di gara sui mercati digitali (Mepa, Sdapa, Gare in Asp).

Nell'ambito del Piano delle Gare Strategiche ICT, definito da AgID e dal Dipartimento per la Trasformazione Digitale, in attuazione del Piano Triennale per l'Informatica nella PA, l'offerta messa a disposizione da Consip con appalti aggiudicati nella forma dell'Accordo quadro, consente a tutte le Amministrazioni, ed in particolare alle Pubbliche Amministrazioni Locali, di acquistare servizi necessari per attuare il percorso di transizione al digitale avvalendosi dell'ordine diretto ovvero attraverso lo strumento dell'appalto specifico tra i fornitori selezionati da Consip.

Rispetto agli obiettivi del Piano Triennale 2024-2026 – Aggiornamento 2025 l'indicatore "RA2.3.1 - Incremento del livello di trasformazione digitale mediante la disponibilità di Gare strategiche allo scopo definite" è parte del sistema di monitoraggio AGID

dei risultati attesi, appartenente all'obiettivo "2.3 - Favorire e monitorare l'utilizzo dei servizi previsti dalle Gare strategiche"[7].

Sono, dunque, in corso di implementazione ulteriori azioni finalizzate ad accompagnare le pubbliche amministrazioni verso una acquisizione sempre più consapevole degli strumenti disponibili all'interno del paniere delle gare strategiche, al fine di garantire contratti di elevata standardizzazione e qualità.

Le gare strategiche ICT si pongono pertanto il duplice obiettivo di:

- creare il "sistema operativo" del Paese, ovvero una serie di componenti fondamentali sui quali definire ed erogare servizi più semplici ed efficaci per i cittadini, le imprese e la stessa Pubblica Amministrazione;
- incentivare l'utilizzo e supportare le amministrazioni nella definizione di contratti coerenti con gli obiettivi definiti dal Piano triennale.

Le iniziative strategiche ICT sono realizzate attraverso appalti aggiudicati da Consip che vanno ampliandosi, nell'ottica di garantire specifici Target del Piano

- Target 2025 - Programma di iniziative strategiche necessarie al raggiungimento degli obiettivi del Piano, di cui alle lettere d) e g) dell'art. 14-bis comma 2 del Codice per l'Amministrazione Digitale
- Target 2026 - Disponibilità nuove gare strategiche necessarie al raggiungimento degli obiettivi del Piano triennale di cui alle lettere d) e g) dell'art. 14-bis comma 2 del Codice per l'Amministrazione Digitale.

Vi sono diversi strumenti attivi nella mappa dell'offerta di Consip, funzionali alla pianificazione, definizione ed attuazione della strategia di migrazione al cloud. Di seguito si fornisce una breve panoramica degli Accordi Quadro con specifica focalizzazione sui servizi cloud, a disposizione delle Amministrazioni anche per la realizzazione di progetti finanziati con fondi PNRR.

1.8.1 Data Management

Accordo Quadro che mette a disposizione delle PA servizi applicativi e professionali per la realizzazione di sistemi informativi a supporto dei processi decisionali. L'iniziativa si colloca nell'ambito del Piano delle gare strategiche ICT, definito da Agid e dal Dipartimento per la Trasformazione digitale in attuazione del Piano triennale dell'informatica nella PA. Ha ad oggetto l'affidamento di servizi di data management e l'affidamento di servizi di demand e PMO, in particolare, sono inclusi servizi applicativi quali sviluppo, manutenzione e personalizzazione di pacchetti software di mercato, gestione applicativa e supporto specialistico per le seguenti Aree Tecnologiche:

- Data Warehouse e Business Intelligence,
- BIG Data/Analytics,
- Open Data,
- Artificial Intelligence/Machine Learning.

Sono inoltre disponibili servizi di Demand e PMO nell'ambito dei servizi applicativi di Data Management così articolati:

- Project Management e Supporto al Monitoraggio per la verifica costante dei Servizi Applicativi di Data Management erogati;
- Change Management - supporto metodologico, progettuale e gestionale necessario per lo svolgimento di tutte le attività relative al cambiamento organizzativo dell'Amministrazione;
- Demand Management - attività finalizzate alla raccolta e strutturazione delle esigenze progettuali e di evoluzione dei processi collegati alle tematiche inerenti i Servizi Applicativi;

7 https://www.agid.gov.it/it/agenzia/piano-triennale/strumenti/strumento-1

- Customer Satisfaction - servizio di misurazione della Customer Satisfaction dei Servizi Applicativi erogati verso l'utente finale, sia interno che esterno.

1.8.2 Servizi applicativi in ottica Cloud e servizi di Demand e PMO per PAL 3

È un Accordo Quadro per l'acquisto di servizi applicativi in ottica Cloud per le Pubbliche Amministrazioni Locali. L'iniziativa fa parte del Piano delle Gare Strategiche ICT e comprende servizi ICT per la trasformazione digitale e l'innovazione delle soluzioni applicative, attraverso la realizzazione di servizi digitali inclusivi, centrati sul cittadino utente, la semplificazione delle interazioni con la PA e che consente di migrare gli applicativi esistenti al Cloud.

L'iniziativa si articola su due Lotti comprendenti i seguenti servizi:

Lotto 1 - Servizi applicativi e accessori

- Servizi realizzativi;
- Servizi di manutenzione;
- Servizio di Supporto Tecnico-Specialistico ICT;
- Servizio di Gestione del Portafoglio Applicativo;
- Servizi Accessori.

Lotto 2 - Servizi di Demand e PMO

Servizi di supporto all'Amministrazione nel governo dell'erogazione dei contratti relativi ai Servizi Applicativi e accessori (Lotto 1):

- Project Management - supporto per la pianificazione, il coordinamento e la gestione delle attività progettuali;
- Supporto al Monitoraggio - supporto alla verifica e al monitoraggio in fase di erogazione dei servizi applicativi;
- Change Management - supporto metodologico, progettuale e gestionale per lo svolgimento delle attività relative alla gestione del cambiamento organizzativo della PA;
- Demand Management - supporto finalizzato alla definizione, raccolta e organizzazione delle esigenze progettuali e di evoluzione dei processi connesse ai servizi applicativi;
- Customer Satisfaction - servizio di rilevazione e misurazione della Customer Satisfaction, verso l'utente finale, sia interno che esterno, relativamente all'erogazione dei servizi applicativi.

1 L'Accordo quadro utilizza un meccanismo di quote e tranche per la ricezione degli ordini da parte dei singoli aggiudicatari, secondo il ciclo di attivazione descritto nella Guida all'Accordo.

1.8.3 Cloud enabling

L'Accordo Quadro rende disponibili servizi professionali tecnici e di supporto all'adozione del cloud e PMO, in particolare:

- **Servizi di supporto**, per pianificare e definire la migliore strategia di migrazione al cloud, in relazione alle proprie caratteristiche, attraverso:
  - assessment e prioritizzazione degli applicativi da migrare;
  - identificazione e valutazione della strategia di migrazione;
  - studio di fattibilità e analisi costi-benefici, valutazione delle competenze necessarie e definizione della roadmap di migrazione;
  - supporto al monitoraggio e controllo dei risultati.

- **Servizi professionali tecnici**, per migrare i servizi IT da un modello di erogazione on-premise verso un modello di erogazione cloud, attraverso:
  - il disegno della soluzione ed architettura degli ambienti cloud;
  - la configurazione degli ambienti ed il trasferimento dei dati;
  - la definizione di policy di sicurezza e di scalabilità delle risorse, delle metriche di *alert* e di performance dei sistemi;
  - il monitoraggio degli ambienti ed il capacity planning;
  - supporto e affiancamento alle Amministrazioni nella formazione del personale su tematiche tecnologiche cloud.

1.8.4 Public Cloud SaaS - IT Service Management

L'Accordo Quadro offre alle PA un contratto "pronto all'uso" per acquistare servizi cloud di tipo IT Service management che consentono di:

- Gestire gli asset IT;
- Gestire le richieste di assistenza informatiche;
- Gestione delle patch di aggiornamento dei sistemi;
- Gestione dei contratti legati agli asset (manutenzione e garanzia).

In particolare, sono resi disponibili 4 distinti "bundle" di funzionalità SaaS:

- Bundle ITSM, che comprende la sola componente di Service Management, per la gestione dei processi e dei sistemi IT secondo le pratiche ITIL;
- Bundle Operation management, che comprende le funzionalità legate alle Operation dei Servizi IT;
- Bundle Asset management, che comprende le funzionalità di gestione del ciclo di vita degli asset;
- Bundle Contract management, che comprende le funzionalità di gestione e pianificazione degli economics dei contratti, delle scadenze, dei livelli di Servizio ed i KPI, etc.

1.8.5 Public Cloud SaaS - B.I.

L'Accordo Quadro rende disponibili prodotti cloud in modalità Software as a Service qualificati dall'Agenzia per la Cybersicurezza Nazionale nell'ambito della Business Intelligence. È uno strumento multi-brand che consente l'acquisto da diversi Cloud Service Provider (CSP).

Ciascun CSP offre un listino relativo a soluzioni tecnologiche BI SaaS proprietarie, contenenti almeno le seguenti funzionalità Base:

- Data Visualization;
- Data Preparation for BI;
- Reporting e Dashboard;
- Access management and security;
- Data Source Integration.

1.8.6 Public Cloud SaaS - Pr.In.Co.

Accordo Quadro per la Fornitura di prodotti SaaS per la produttività individuale e la collaboration. Lo strumento consente l'acquisto, anche in bundle separati, dei seguenti servizi di produttività e collaboration:

- Soluzioni SaaS di Posta elettronica in un modello di erogazione pubblico
- Soluzioni SaaS di Documentale in un modello di erogazione pubblico (gestione documentale e file sharing);
- Soluzioni SaaS di Collaboration in un modello di erogazione pubblico (Instant Messaging e di Audio/Video Conference).

1.8.7 Public Cloud SaaS - Gestione documentale

Accordo Quadro per la Fornitura di servizi SaaS:

- Soluzioni SaaS di Protocollo informatico in un modello di erogazione pubblico
- Soluzioni SaaS di Gestione documentale (Workflow e procedimenti amministrativi) in un modello di erogazione pubblico
- Soluzioni SaaS di Conservazione documentale in un modello di erogazione pubblico

1.8.8 Public Cloud SaaS - CRM

Accordo Quadro per la fornitura di un Catalogo di funzionalità CRM SaaS per le Pubbliche Amministrazioni che rende disponibili servizi SaaS per il CRM ed il marketing; lo strumento è multi-brand e consente quindi l'acquisto da diversi Cloud Service Provider (CSP). In particolare, l'AQ prevede:

- CRM 'classico', comprendente le funzionalità per la gestione dei clienti (in questo caso dei cittadini), i cui utenti sono operatori interni all'organizzazione;
- Marketing, con funzionalità rivolte alla creazione e gestione di campagne di contatto e comunicazione verso l'esterno.

1.8.9 Sicurezza da remoto

L'Accordo Quadro prevede l'affidamento di servizi erogati da remoto per la sicurezza dei perimetri tecnologici delle infrastrutture e servizi per la Governance, Analisi del Rischio e Compliance per le Pubbliche Amministrazioni.

Si compone di due Lotti uno dedicato ai **servizi di sicurezza** e l'altro a quello di **compliance e controllo:**

Lotto 1 - Servizi di sicurezza "da remoto": Next Generation Firewall, Web Application Firewall & API Protection, Security Operation Center, E-mail Gateway, Secure Web Gateway, Cloud Access Security Broker, Zero Trust Network Access, Threat Intelligence & Vulnerability Data Feed, Anti- APT, Endpoint & Server protection;

Lotto 2 - Servizi per la governance, analisi del rischio e compliance: Security Strategy, Risk Management, Vulnerability Assessment, Testing del codice, Supporto alla definizione dei processi cyber, Penetration Testing, Awareness e formazione, Compliance normativa, Controllo terze parti (supply-chain di approvvigionamento).

1.8.10 Digital Transformation

Con un perimetro ampio di servizi indirizzati alla trasformazione digitale, l'Accordo quadro investe i seguenti ambiti:

- *Strategia della Trasformazione Digitale*: attraverso i servizi di disegno strategia digitale, di definizione del Piano Strategico ICT e di disegno mappa dei servizi digitali della PA;
- *Digitalizzazione dei processi*: attraverso i servizi di disegno del modello di

erogazione del servizio digitale, disegno di processi digitali, supporto specialistico per l'implementazione di servizi digitali;

- *Gestione della Transizione al Digitale*: attraverso i servizi di change management dedicati alla Progettazione della transizione al digitale e all'affiancamento alla transizione digitale;
- *Servizi di PMO* funzionali al raggiungimento degli obiettivi di digitalizzazione.

2 - CONFRONTO FRA MODELLO "ON PREMISE" E MODELLO "CLOUD COMPUTING"

2.1 - Il Modello "on premise"

Il modello su cui si basava tradizionalmente l'information technology era incentrato su sistemi informativi on premise, che presuppongono infrastrutture di proprietà, o comunque gestite dall'amministrazione stessa.

Il modello prevede elevati costi iniziali, inclusi i costi sostenuti per l'acquisto di hardware e altre infrastrutture nonché i costi necessari per l'installazione del software, e soprattutto implica per l'amministrazione l'onere di farsi carico delle attività di tipo sistemistico e di manutenzione delle infrastrutture e dei sistemi informativi.

Le tipiche categorie di servizi/beni oggetto dei contratti ICT afferenti a questo modello possono sintetizzarsi nei seguenti:

- Hardware (acquisto, locazione o altre forme contrattuali);
- Implementazione, strumentale all'installazione, parametrizzazione e personalizzazione del sistema informativo;
- Assistenza e manutenzione (successive al periodo di garanzia);
- Servizi realizzativi di sviluppo;
- Licenza d'uso software, scegliendo fra soluzioni commerciali o open source, con forme contrattuali basate su acquisto o noleggio;
- Servizi di manutenzione delle licenze;

Questo modello consente all'amministrazione di avere il controllo completo delle risorse infrastrutturali e di avere un alto livello di personalizzazione delle funzionalità e dei livelli di servizio del sistema informativo, ma presenta il forte svantaggio di necessitare di un forte investimento iniziale in termini di infrastrutture, installazioni e successivamente, in termini di manutenzione (delle infrastrutture e dei software). Richiede inoltre una struttura organizzativa adeguata, con la presenza di diverse tipologie di profili professionali in grado di prendere in carico e gestire i sistemi.

2.2 Il Modello Cloud Computing

Al contrario, ***nei contratti basati sul cloud computing le risorse informatiche (infrastrutturali e applicative) consistono in servizi messi a disposizione dell'utente, da parte di fornitori qualificati, accessibili via web.***

Il fruitore di questo servizio ha la possibilità di utilizzare spazi di memorizzazione, software, server virtuali e ambienti di sviluppo, mediante collegamento a server remoti, gestiti da terze parti (i cosiddetti «cloud provider»).

Il contratto di cloud computing è un contratto atipico; non è riconducibile in modo immediato ad una categoria tipizzata dal codice civile.

È stato inquadrato fra i contratti di somministrazione, ma l›orientamento più recente lo riconduce alla categoria dei contratti di appalto, configurandosi in capo all›operatore economico un «obbligo di fare».

I contratti Cloud si basano sull'interazione fra tre soggetti:

- Il Fornitore di servizi – c.d. *Cloud Provider*. Colui che offre servizi, generalmente secondo un modello pay-per-use;
- Il Cliente amministratore, ovvero colui che sceglie e configura i servizi offerti dal cloud provider, generalmente offrendo un valore aggiunto;

- Cliente finale, ovvero il fruitore ultimo dei servizi cloud che utilizza le risorse opportunamente configurate dal cliente amministratore.

Nel paragrafo 3.2 sono descritti due fra i principali modelli di commercializzazione dei servizi cloud.

I servizi cloud possono essere classificati sulla base della *tipologia di risorse computazionali offerte* nei seguenti modelli di servizio[8]:

- *Servizi IaaS*: servizi sistemistici infrastrutturali, c.d. Infrastructure-as-a-Service (IaaS), per l'erogazione, ad esempio, di server virtualizzati e spazio di salvataggio dati;
- *Servizi PaaS*: 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;
- *Servizi SaaS*: 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.

I servizi cloud così come sopra classificati, possono essere distribuiti/fruiti secondo i seguenti modelli di distribuzione:

- ***Cloud Pubblico:*** l'infrastruttura cloud, di proprietà del provider, è messa a disposizione di una pluralità indistinta di utenti che ne fruiscono la condivisione;
- ***Cloud Privato;*** l'infrastruttura cloud è ad esclusivo utilizzo dell'organizzazione (amministrazione pubblica o soggetto privato), che ne fruisce e che ne conserva pertanto il pieno controllo;
- ***Cloud ibrido:*** è un ambiente che risulta dalla combinazione tra il modello pubblico e quello privato connessi fra loro;
- ***Multi cloud:*** modello che prevede l'utilizzo contemporaneo, per la realizzazione di determinati servizi o applicazioni, di più Cloud dello stesso tipo (pubblico o privato) offerti da diversi fornitori.

L'**oggetto** di un contratto di cloud computing è quindi la fruizione di un servizio.

Viene ribaltato il modello tradizionale basato sulla proprietà delle risorse informatiche (infrastrutturali e applicative) da parte del soggetto pubblico o privato, da cui deriva anche la responsabilità della gestione di queste risorse.

Nel modello basato sul cloud computing, la "parte acquirente" diventa «fruitore» di un servizio con rilevanti impatti, in primo luogo, sotto il profilo del controllo di infrastrutture e sistemi, della responsabilità.

Il focus diventa la gestione e la disciplina dell'accesso ai servizi per consentirne la loro fruizione ottimale.

Nell'ambito di questo modello, la disponibilità delle risorse dipende dal "cloud service provider"(fornitore), pertanto le clausole contrattuali devono essere orientate ad assicurare:

- la continuità della prestazione in condizioni di sicurezza;
- la cooperazione fra fornitore (CSP) e utilizzatore;
- la definizione degli ambiti di responsabilità fra le parti.

L'adozione di un modello tecnico/organizzativo basato sul cloud computing genera una serie di vantaggi sulla qualità ed economicità dei servizi erogati dall'Amministrazione, che si possono così sintetizzare:

- Azzeramento dei costi di acquisto e gestione delle infrastrutture;

8 Così definiti nel documento Strategia Cloud Italia.
https://docs.italia.it/italia/cloud-italia/strategia-cloud-italia-docs/it/stabile/2_il_cloud_computing.html#il-cloud-computing

- Azzeramento del problema dell'aggiornamento dei sistemi e dell'obsolescenza delle infrastrutture;
- Maggiore resilienza;
- Infrastrutture più sicure;
- Alta flessibilità nella fruizione dei servizi (è possibile la programmazione delle risorse informatiche da utilizzare sulla base di fattori relativi, ad esempio, a picchi di attività che si concentrano in determinati periodi).

Dalle caratteristiche dei servizi cloud e i relativi modelli di distribuzione, si possono individuare le principali **criticità** relative ai contratti di servizi cloud possono essere così sintetizzate:

- Rigidità nella negoziazione delle clausole contrattuali (soprattutto in relazione ai servizi cloud fruiti nell'ambito di un modello distribuzione di cloud pubblico in cui il potere negoziale dell'utente è pressoché nullo, riducendosi il potere decisionale alla sfera dell'utilizzare il servizio o non utilizzarlo affatto[9]);
- Basso controllo sulla gestione delle infrastrutture da parte dell'amministrazione;
- Difficoltà a controllare i livelli di sicurezza;
- La localizzazione delle infrastrutture può rappresentare un problema per l'attuazione delle misure di sicurezza e la compliance al GDPR;
- Rischio lock in di tipo tecnologico (ad esempio connesso alla difficoltà o elevato costo nella migrazione di dati/servizi ad altro CSP derivanti dall'utilizzo di particolari formati o di piattaforme di tipo proprietario) o gestionale/operativo (difficoltà a migrare dati/servizi ad altro CSP derivanti dalla scarsa condivisione del know how).

In sintesi, i due modelli possono essere confrontati evidenziando che cosa cambia per l'Amministrazione rispetto a parametri essenziali, **prima e dopo** l'adozione del cloud.

Parametro	Prima (On-Premise)	Dopo (Cloud Computing)
Costo gestione IT	Alto (hardware, licenze, manutenzione)	Ridotto (pagamento a consumo)
Scalabilità	Difficile da espandere rapidamente	Flessibile, adattabile ai picchi
Sicurezza	Dipende da risorse interne	Standard elevati garantiti dal provider
Disaster Recovery	Costoso (o dai costi non preventivabili), backup locali	Incluso nel servizio cloud

9 Si pensi ad esempio a servizi forniti da provider come Google che prevedono un progressivo aumento del canone sulla base dell'ampliamento delle funzionalità/servizi offerti; elementi aggiuntivi che però non sono oggetto di negoziazione e che pertanto potrebbero non essere necessari all'utente. Un altro elemento di rigidità riguarda le condizioni fissate per la dismissione del servizio.

3 - PECULIARITÀ DEI CONTRATTI DI SERVIZI CLOUD

3.1 - Qualificazione ACN

Dal 01 agosto 2024, con il Regolamento ACN del 27/06/2024 è entrato in vigore il regime ordinario di qualificazione/adeguamento di infrastrutture e servizi cloud.

Viene confermato **l'obbligo per le pubbliche amministrazioni di acquistare servizi cloud inclusi nel Catalogo aggiornato a cura di ACN,** contenente i servizi qualificati (se erogati da soggetti privati) o adeguati (se erogati da soggetti pubblici).

Il Regolamento disciplina, inoltre, le modalità e i tempi della migrazione in cloud di servizi e infrastrutture.

Il Regolamento regola il processo di "qualificazione", che viene definito come processo previsto per i **fornitori privati (CSP),** attraverso cui il CSP dichiara la conformità di servizi e infrastrutture ai requisiti indicati dal Regolamento. La verifica ex ante svolta da ACN ha la natura di verifica di conformità formale sulle dichiarazioni rese.

L'"adeguamento" è invece il processo a cui sono sottoposti i servizi cloud erogati da **soggetti pubblici** o le infrastrutture gestite da **operatori pubblici o privati,** attraverso cui viene dichiarato il possesso dei requisiti previsti dal Regolamento. La verifica ex ante, svolta da ACN, è di tipo formale sulla relazione di conformità presentata.

Il Regolamento individua quattro livelli di adeguamento/qualificazione di infrastrutture e servizi e definisce i requisiti connessi ad ogni livello.

Si indica inoltre quale livello deve essere garantito rispetto alla classificazione del servizio/infrastruttura in ordinario, critico, strategico.

I processi di qualificazione e di adeguamento andati a buon fine portano all'aggiornamento del *Catalogo delle Infrastrutture e dei Servizi Cloud per le Pubbliche Amministrazioni* a cura di ACN. La validità della qualifica o dell'adeguamento è di **36 mesi** a partire dalla data del suo conseguimento.

I servizi cloud adeguati o qualificati devono essere erogati, tramite un servizio cloud qualificato o adeguato, oppure tramite un'infrastruttura digitale o un'infrastruttura di servizi cloud adeguata.

I processi di adeguamento o qualificazione, quindi, verificano il rispetto del **principio della catena di adeguamento/qualificazione**.

Poiché il requisito della qualificazione ACN è indispensabile ai fini della validità dei contratti stipulati dall'Amministrazione, per evitare problemi di continuità dei servizi è opportuno presidiare l'operatività del fornitore nell'avvio del procedimento di rinnovo della qualificazione in tempo congruo, anche se la responsabilità della qualificazione e dell'attivazione del rinnovo è a totale carico del fornitore.

E' importante evidenziare, infine, che, in caso di dati e servizi critici e strategici, i requisiti di sicurezza necessari per ottenere la qualificazione, devono essere assicurati da tutta la catena di approvvigionamento (Supply Chain). A questo scopo il Regolamento prevede che siano definiti e implementati processi atti a identificare, valutare e gestire il rischio cyber legato alla catena di approvvigionamento. Tali processi sono identificati, ben definiti, validati, gestiti e approvati da attori interni all'organizzazione.

3.2 – Modelli di commercializzazione di Servizi Cloud

Si presentano di seguito due dei più diffusi modelli di commercializzazione dei Servizi Cloud

Modello n. 1 - Il produttore del servizio cloud coincide con il provider che lo qualifica sul Catalogo ACN e lo commercializza.

Attori coinvolti

- **Provider del servizio SaaS (Titolare della qualificazione)**: l'operatore economico che ha qualificato il proprio servizio presso sul Catalogo **ACN** e che lo eroga effettivamente ed è responsabile di SLA, compliance, requisiti di qualificazione. Il provider sottoscrive il contratto di fornitura del servizio direttamente con l'Amministrazione.
- **Pubblica Amministrazione (Cliente)**: l'ente che acquista e utilizza il servizio SaaS, contrattualizzando il servizio direttamente con il Provider che risponde degli SLA e dei requisiti di qualificazione.

Modello n. 2 – Il produttore di un servizio cloud stipula un contratto di commercializzazione dello stesso con un rivenditore.

Attori coinvolti

- **Provider del servizio SaaS (Titolare della qualificazione)**: l'operatore economico che ha qualificato il proprio servizio presso sul Catalogo **ACN** e che lo eroga effettivamente ed è responsabile di SLA, compliance, requisiti di qualificazione;
- **Rivenditore (Reseller / Partner commerciale)**: soggetto che stipula un accordo commerciale con il provider per poter offrire quel servizio SaaS alla PA. E' un soggetto terzo che commercializza il servizio SaaS qualificato, **senza modificarne le caratteristiche tecniche, di sicurezza o di conformità**. Nell'ambito del contratto stipulato con la PA, il rivenditore può integrare il servizio cloud con propri servizi (ad es. fornendo servizi accessori: supporto tecnico, formazione, migrazione dati);
- **Pubblica Amministrazione (Cliente)**: l'ente che acquista e utilizza il servizio SaaS. La PA acquista dal rivenditore, ma il servizio SaaS resta erogato tecnicamente e giuridicamente sotto la responsabilità del provider qualificato. La PA ha il diritto di essere informata del fatto che stipula un contratto con un rivenditore e che la responsabilità dell'erogazione del servizio è in capo al Provider.

3.3 - Livelli di servizio

La negoziazione dei livelli di servizio (e in generale di tutte le clausole contrattuali), come abbiamo visto rappresenta una delle criticità dei contratti di servizi cloud.

Il fatto che possano essere oggetto di contratto esclusivamente servizi qualificati rappresenta una garanzia per le amministrazioni sul fatto che sia verificato ex ante da ACN **l'impegno da parte del Provider del rispetto dei requisiti previsti dal Regolamento Cloud per la PA** e che in corso di esecuzione dei contratti sottoscritti con le Amministrazioni, sia vincolato al loro mantenimento.

Come visto ai paragrafi precedenti, il Regolamento ACN del 27 giugno 2024 definisce i livelli di servizio minimi che devono essere garantiti dalle infrastrutture digitali e dalle infrastrutture di servizi cloud e le caratteristiche base dei servizi cloud, rispetto ai parametri che caratterizzano le due categorie.

È previsto un aggiornamento periodico (almeno una volta ogni due anni) a cura di ACN.

Nel Regolamento vengono descritte le implementazioni minime attese, nonché le modalità richieste, al fine di descriverne l'adozione e dimostrarne l'attuazione.

L'Allegato 2 del Regolamento individua *i livelli minimi che devono essere garantiti dalle infrastrutture digitali e infrastrutture per servizi della Pubblica Amministrazione* in relazione ad ogni classe di dati e servizi gestiti (Ordinari, Strategici e Critici).

I parametri che consentono di definire i livelli qualitativi delle infrastrutture digitali e le infrastrutture per servizi della PA sono:

- Affidabilità;
- Capacità elaborativa;
- Risparmio energetico;
- Sicurezza.

L'**affidabilità** delle infrastrutture è definita in termini di:

- **Disponibilità dell'infrastruttura** digitale, quale percentuale di tempo in cui l'infrastruttura risulta essere accessibile e usabile e disponibilità di soluzioni per la configurazione dei servizi in alta affidabilità.
- **Business Continuity e Disaster Recovery**. Disponibilità di soluzioni di Disaster Recovery con tempi di ripristino garantiti.
- **Governance e Processi.** Adozione di processi e procedure in linea con le best practice indicate dalla ISO/IEC 20000-2 e individuazione di indicatori di servizio obbligatori.
- **Performance e scalabilità.** Garanzia di caratteristiche minime di connettività.

La **Capacità Elaborativa** è definita in termini di applicazione di best practice.

Il **Risparmio Energetico** è definito in termini di adozione di procedure per la gestione delle emissioni dei gas prodotti, o per la gestione dell'energia consumata o per la gestione ambientale dei propri Data Center. Sono indicati gli standard di riferimento (standard ISO 14064, ISO 50001 e ISO 14001, o equivalenti.

La **Sicurezza** è declinata in termini di Data Center Security, ossia misure di sicurezza fisica e infrastrutturale e in termini di descrizione delle modalità di implementazione delle funzioni tipiche del modello definito dal Framework Nazionale per la Cybersecurity e Data Protection (FNCS): Identify, Protect, Detect, Respond e Recover.

L'Allegato 3 del Regolamento definisce le *caratteristiche dei Servizi Cloud* per le Pubbliche Amministrazioni rispetto ai seguenti parametri:

- Interoperabilità, di portabilità;
- Performance e di scalabilità;
- Qualità;
- Sicurezza.

Nell'ambito di definizione del parametro della qualità, vengono definiti gli obiettivi minimi che devono essere garantiti dai servizi (Minimum Service Level Objective - SLO). In sede di definizione del contratto, gli SLO confluiranno negli SLA che vincolando giuridicamente il fornitore.

I Service Level Objective individuati sono:

- Disponibilità del servizio pari al 99% (percentuale di tempo in un mese in cui il servizio cloud risulta essere accessibile e usabile);
- Supporto tecnico per emergenze: 24 ore al giorno, 7 giorni a settimana per tutto l'anno;
- tempo massimo di risposta agli incidenti: 1 ora;
- "minor release": 3 giorni;
- "major release": 1 mese.

Così come per le infrastrutture, il parametro della sicurezza viene descritto mutuando le funzioni tipiche del modello definito dal Framework Nazionale per la Cybersecurity e Data Protection (FNCS).

Le *verifiche di conformità* svolte dall'Amministrazione nel corso di esecuzione dei contratti sono finalizzate ad accertare il rispetto degli SLA contrattualizzati e concorrono al monitoraggio continuo rispetto al mantenimento da parte dell'operatore economico (Cloud Service Provider) dei requisiti necessari per la qualificazione ACN, rispetto al livello previsto dal Regolamento sulla base della classificazione dei dati/servizi gestiti (che è espressamente richiamata nel contratto).

Le eventuali inadempienze riscontrate, oltre a determinare l'applicazione delle penali compensative da parte dell'Amministrazione, devono essere comunicate ad ACN.

È sempre opportuno che i contratti prevedano:

- Strumenti di monitoraggio: sistemi di reportistica che raccolgano dati in tempo reale, consentendo una verifica costante del rispetto degli SLA;
- Procedure di escalation chiare che includano notifiche automatiche, piani di intervento immediato e un percorso di escalation fino ai livelli dirigenziali in caso di persistenza del problema;
- Coinvolgere parti terze per audit indipendenti o verifiche periodiche da parte di terzi per garantire la trasparenza e l'accuratezza dei dati di monitoraggio.

3.4 - Perimetro di responsabilità

Il modello del Cloud Computing è caratterizzato dalla condivisione della responsabilità fra l'Amministrazione (soggetto fruitore) e il Cloud Service Provider. Definire il perimetro di responsabilità fra le parti è un'operazione che porta con sé insidie significative.

Per inquadrare gli obblighi delle parti, è utile individuare i principali ambiti da tenere in considerazione, che possono sintetizzarsi nei seguenti:

- Sicurezza dei servizi;
- Affidabilità dei servizi;
- Continuità dei servizi;
- Trattamento Dati (GDPR).

Per ognuno di questi, nella definizione del contratto, ci si deve porre il problema quali siano gli obblighi delle parti nell'esecuzione dei servizi.

La categoria di servizio (SaaS, PaaS, Iaas) e il modello di fruizione del servizio (Cloud pubblico, privato, ibrido) configurano livelli di responsabilità diversi.

Semplificando si potrebbe dire che nel caso di servizi SaaS erogati nell'ambito di un cloud pubblico, sono contenuti i profili di responsabilità per l'Amministrazione, che potrebbero riferirsi esclusivamente alla qualità dei dati, mentre il fornitore è

responsabile della componente infrastrutturale e applicativa.

Utilizzare metodologie standardizzate e condividere preventivamente un modello di individuazione del perimetro delle responsabilità che sia il più chiaro possibile facilita la gestione del contratto e consente di raggiungere l'obiettivo di avere servizi più efficienti contenendo i rischi potenziali insiti del modello del cloud providing.

Di seguito si propone una tabella con scopo esclusivamente esemplificativo del perimetro di responsabilità in capo al Cloud Provider/Amministrazione, rispetto ad alcuni ambiti tipici dei servizi cloud (SaaS, PaaS, IaaS).

Area di Responsabilità	SaaS	PaaS	IaaS
Infrastruttura Fisica e Data Center	Cloud Provider	Cloud Provider	Cloud Provider
Virtualizzazione e Networking	Cloud Provider	Cloud Provider	Cloud Provider
Sistema Operativo	Cloud Provider	Cloud Provider (gestito in parte)	Amministrazione
Middleware e Runtime	Incluso nel servizio (Provider)	Cloud Provider (in parte; integrazione condivisa)	Amministrazione
Applicazioni	Amministrazione	Amministrazione	Amministrazione
Dati	Amministrazione	Amministrazione	Amministrazione
Sicurezza Fisica e Infrastrutturale	Cloud Provider	Cloud Provider	Cloud Provider
Sicurezza del Sistema Operativo	Cloud Provider	Cloud Provider (parziale)	Amministrazione
Sicurezza Applicativa e dei Dati	Amministrazione (gestione degli accessi e conformità)	Amministrazione (con supporto e best practice fornite dal Provider)	Amministrazione
Backup e Disaster Recovery	Generalmente a carico del Provider (salvo accordi specifici)	In genere condivisa (accordi specifici definiscono ruoli)	Principalmente Amministrazione (con possibili servizi aggiuntivi offerti dal Provider)

3.5 - Protezione dei dati personali

Il Regolamento ACN sul Cloud della PA è stato approvato con il preventivo assenso del Garante per la Protezione dei Dati Personali ed è pertanto conforme al GDPR.

L'art. 22 del Regolamento ACN, al comma 1 prevede che "Le amministrazioni sono **titolari** dei trattamenti di dati personali effettuati nell'ambito delle infrastrutture digitali per le pubbliche amministrazioni, delle infrastrutture dei servizi cloud per le pubbliche amministrazioni e dei servizi cloud per le pubbliche amministrazioni".

Il comma 2 prevede che "gli operatori di infrastrutture digitali, i fornitori di servizi cloud e gli ulteriori soggetti coinvolti nei trattamenti di dati personali di cui al comma 1 o nelle attività di migrazione dei dati e dei servizi digitali della pubblica amministrazione di cui al capo IV, nonché i soggetti di cui questi si avvalgono per l'esecuzione di specifiche attività di trattamento per conto delle amministrazioni, operano come **responsabili del trattamento** ai sensi dell'articolo 28 del regolamento (UE) 2016/679".

Gli operatori/fornitori, in quanto Responsabili del Trattamento (e gli eventuali sub-

fornitori in qualità di sub-responsabili):

- adottano misure tecniche e organizzative idonee a garantire una tempestiva e adeguata informazione delle amministrazioni in caso di violazione dei dati personali;
- adottano misure tecniche e organizzative per fornire alle amministrazioni idonei strumenti di controllo delle attività di trattamento effettuate sotto la responsabilità da parte degli eventuali sub-responsabili (ad esempio subappaltatori);
- in caso di trasferimento di dati personali al di fuori dello Spazio economico europeo, sono tenuti ad attenersi alle istruzioni impartite delle amministrazioni (titolari del trattamento) e a mettere a disposizione delle stesse ogni informazione necessaria per valutare l'effettività delle misure appropriate poste in essere.

Per le violazioni dei dati personali contenuti nelle infrastrutture digitali e nei servizi cloud delle PA, resta ferma la competenza del Garante privacy.

Tuttavia, il Regolamento prevede che l'ACN comunichi al Garante le evidenze relative a possibili violazioni di dati personali, di cui venga a conoscenza.

Nell'ambito della documentazione contrattuale, le disposizioni in materia di protezione dei dati personali si attuano nel Data Protection Agreement che deve essere sottoscritto dalle parti, contestualmente al contratto. Con il DPA viene nominato il Responsabile del Trattamento ai sensi dell'art. 28 del GDPR e vengono definiti gli obblighi in relazione ai dati trattati.

Le misure tecniche che il Responsabile deve mettere in atto dovranno essere conformi al Framework Nazionale per la Cybersecurity e la Data Protection, richiamato nel Regolamento ACN.

Le misure di sicurezza previste dal Regolamento implicano che la **localizzazione delle infrastrutture che ospitano dati e servizi, posta al di fuori del territorio europeo è consentita solo previa verifica della compliance al GDPR della normativa in materia di protezione dei dati personali.**

Non è in ogni caso consentita, in caso di dati e servizi strategici e critici, che possono essere gestiti solo da cloud privati o dalla porzione privata di cloud ibridi, con datacenter collocati in territorio dell'Unione Europea.

La qualificazione/adeguamento di servizi e infrastrutture verifica anche questo requisito.

Nella predisposizione dei contratti di servizi cloud, in relazione alla protezione dei dati, può essere preso in considerazione l'inserimento delle seguenti clausole contrattuali:

- Previsione di audit da far svolgere a soggetti terzi, da considerare a carico dell'operatore economico. Questa previsione può essere particolarmente utile soprattutto nel caso in cui la localizzazione in territorio oltre i confini nazionali, possa rendere l'audit particolarmente oneroso per l'amministrazione;
- Previsione di strumenti per l'individuazione fisica del dato.

3.6 - Mitigazione del Lock in e clausole di Presa in carico ed Exit strategy

Nella definizione delle clausole contrattuali è opportuno prevedere una disciplina dettagliata degli aspetti volti a mitigare il rischio di lock in, ossia quella situazione di dipendenza che si verifica quando l'amministrazione è così vincolata a un cloud provider da non poter più sostituirlo senza gravi conseguenze in termini di:

- Gestione di complessità tecnologiche;
- Costi;
- Tempi.

La natura del lock in è essenzialmente tecnologica, con implicazioni giuridiche e contrattuali. Il fattore che più di tutti complica il passaggio dei servizi cloud verso un diverso CSP è l'incompatibilità tecnologica delle soluzioni.

Il Manuale di abilitazione al Cloud[10] oltre a definire le diverse tipologie di Lock in, fornisce le indicazioni per mitigare questo rischio che si concretizzano in pratiche tecnologiche, metodologiche e contrattuali.

Il Regolamento per il Cloud delle PA approvato da ACN il 27 giugno 2024, fornisce la cornice normativa per implementare servizi cloud sempre più flessibili.

I requisiti di **interoperabilità** e **portabilità** descritti dal Regolamento fra le caratteristiche di base dei servizi cloud (Allegato 4), rappresentano un presidio di difesa dai rischi di lock in. Oltre alle specifiche tecniche di base necessarie a garantire l'interoperabilità, è indicata la documentazione che deve essere resa disponibile. Deve essere consentita l'esportazione ed importazione massiva dei dati, garantendo l'utilizzo di formati aperti non proprietari, durante tutto il corso di esecuzione del contratto e a conclusione di questo, nell'ambito della disciplina della cosiddetta Exit Strategy.

E' opportuno quindi prevedere **la definizione di politiche e procedure per l'interoperabilità e la portabilità,** le quali vengono riviste e aggiornate almeno su base annuale, compresi requisiti per:

a. Comunicazioni tra le interfacce delle applicazioni;

b. Interoperabilità del trattamento delle informazioni;

c. Portabilità dello sviluppo di applicazioni;

d. Scambio, uso, portabilità, integrità e persistenza delle informazioni/dati. (limitatamente ai servizi PaaS, SaaS).

Il Regolamento fornisce inoltre le indicazioni sui contenuti minimi degli accordi fra amministrazione e CSP per garantire la portabilità dei dati:

- Formato dei dati;
- Durata del tempo in cui i dati saranno conservati;
- Portata dei dati conservati e messi a disposizione dell'Amministrazione;
- Politica di cancellazione dei dati. [PaaS, SaaS].

Pur garantendo i requisiti di interoperabilità e portabilità di base, i provider utilizzano tecnologie diverse per mantenere un vantaggio competitivo sul mercato;

- Non è sempre possibile negoziare con il provider formati e tecnologie;
- Necessità di forti investimenti in termini di sviluppo organizzativo delle amministrazioni.

Clausole contrattuali/metodologiche che prevedano condizioni migliorative rispetto ai requisiti base previsti dal regolamento:

- Piani di formazione;
- Adozione di procedure di trasferimento del Know How;
- Individuazione in sede contrattuale, in modo preciso e puntuale della documentazione che il CSP deve garantire;
- Impostazione delle clausole di exit strategy.

Nell'impostazione della exit strategy è importante definire clausole che disciplinano la ***restituzione dei dati e dei contenuti.*** Devono essere previsti i tempi entro cui la restituzione deve essere completata e le modalità. Nella definizione della durata del contratto deve essere preso in considerazione il tempo necessario per concludere questa attività. È opportuno condizionare il pagamento delle prestazioni contrattuali relative al periodo conclusivo del contratto, al completamento della migrazione e prevedere un'adeguata penale per il ritardato o mancato completamento della migrazione o per una migrazione che ha comportato la compromissione dei dati o dei contenuti da migrare.

10 https://docs.italia.it/italia/manuale-di-abilitazione-al-cloud/manuale-di-abilitazione-al-cloud-docs/it/bozza/pianificare-la-migrazione/lock-in.html

Oltre ai tempi, è importante definire le modalità e tecniche di restituzione dei dati, precisando il formato in cui gli stessi devono essere restituiti, la possibilità di esportazione massiva dei contenuti e le tempistiche per effettuare l'export.

Nella definizione dei formati in cui i dati devono essere restituiti è importante inserire in sede contrattuale, l'obbligo di restituzione in un formato machine readable.

La consegna dei dati deve essere validata dall'amministrazione e solo dopo la validazione può essere consentito l'avvio della fase di cancellazione dei dati e dei contenuti in possesso del fornitore a conclusione della quale è possibile la fatturazione del saldo delle prestazioni contrattualizzate.

La ***cancellazione dei dati e dei contenuti*** non riferibili al fornitore deve essere espletata nei tempi e modalità definiti contrattualmente.

Le clausole devono prevedere procedure di cancellazione sicura, che garantiscano l'effettiva permanente irrecuperabilità dei dati cancellati.

Le procedure di cancellazione devono riguardare sia i dati primari che i dati di back up (assicurandosi che l'eliminazione venga attuata su ciascuna infrastruttura in cui i dati sono ridondati per ragioni di sicurezza) e i dati di log.

4 - CONFORMITÀ AL CODICE DEI CONTRATTI PUBBLICI. CLAUSOLE CONTRATTUALI

Le procedure di acquisto dei servizi cloud, come tutte le categorie di servizi e forniture afferenti al procurement pubblico, devono essere conformi al Dlgs 36/2023 (Codice dei Contratti pubblici).

Si indicano di seguito alcuni istituti che trovano applicazione nei contratti di servizi informatici, con particolare riguardo ai servizi cloud; si forniscono inoltre dei suggerimenti sulla possibile declinazione contrattuale di elementi trasversali dei contratti.

4.1 Definizione dell'oggetto

L'oggetto del contratto deve essere definito in modo tale da inquadrare in modo preciso e specifico la prestazione da acquistare, le cui caratteristiche tecniche sono descritte in modo dettagliato nel capitolato tecnico.

In relazione ai servizi cloud erogati in modalità SaaS (soprattutto nel caso del modello di commercializzazione basato sulla rivendita) si osserva che possono caratterizzarsi da un'alta standardizzazione delle funzionalità; analizzando il mercato di riferimento la loro natura è inquadrabile nell'ambito delle forniture, ancorché la prestazione consiste nella fruizione di un servizio. Si pensi ad esempio i Customer Relationship Management (CRM), o i prodotti SaaS di gestione della posta elettronica o prodotti SaaS di gestione documentale.

4.2 Durata

Definire la durata del contratto è una decisione vincolata dalla disponibilità finanziaria.

Quando possibile, sarebbe preferibile impostare una durata che tenga conto del ciclo di vita dei servizi. Una durata inferiore difficilmente garantisce la piena migrazione e l'entrata in esercizio dei servizi, tale da rendere il contratto pienamente efficiente.

4.3 Importo

L'importo dell'appalto deve essere calcolato ai sensi dell'art. 14 del Dlgs 36/2023.

In particolare, il comma 4 stabilisce che per importo dell'appalto si intende **l'importo pagabile al fornitore, al netto dell'Imposta sul Valore Aggiunto (IVA). Il calcolo deve comprendere le eventuali premialità e qualsiasi forma di opzione o rinnovo**, **che, se presenti, devono essere espressamente previsti nei documenti di gara.**

Il CIG dell'appalto, quindi, è comprensivo di tutte le opzioni di modifica e rinnovo.

4.4 Proroga

Nella definizione della documentazione di gara devono essere individuate le eventuali opzioni di proroga previste dall'art. 120 Del Dlgs 36/2023 ai commi 10 e 11.

Importante distinguere i due tipi di proroga previsti dall'art. 120 del Dlgs 36/2023:

- Proroga contrattuale (comma 10 dell'Art. 120 dlgs 36/2023);
- Proroga tecnica (comma 11 dell'Art. 120 dlgs 36/2023).

La proroga (c.d. «contrattuale») prevista dal comma 10 deve essere prevista già dal bando e nei documenti di gara. Il codice non dà indicazioni sulla durata di questa proroga. Deve però essere quantificata (in termini di durata e importo) in fase di predisposizione dell a documentazione di gara. Concorre pertanto a determinare l'importo a base di gara.

La proroga prevista dal comma 11, rientra nella fattispecie della «proroga tecnica». Può essere attivata in casi eccezionali nei quali risultino oggettivi e insuperabili ritardi nella conclusione della procedura di affidamento del contratto, e per il tempo necessario ad individuare il nuovo fornitore, **nei casi in cui l'interruzione della prestazione dedotta nella gara determinerebbe un grave danno all'interesse pubblico che è destinata a soddisfare.** Questa ipotesi è particolarmente plausibile rispetto ai servizi cloud. Per la sua natura non può essere prederminata nel bando di gara. ANAC è intervenuta con una faq a precisare che non è necessario prendere un nuovo CIG in caso di attivazione di questa tipologia di proroga. Per convenzione la durata è fissata in sei mesi, mutuando la norma prevista nel Dlgs 50/2016.

4.5 Modifiche e rinnovi contrattuali

Le possibili opzioni di modifica e rinnovi da prendere in considerazione per il calcolo dell'importo dell'appalto sono definite dai seguenti articoli del codice:

Art. 14 comma 4 (rinnovi);

Art. 120 (opzioni di modifica in corso di esecuzione).

In particolare:
art. 120, comma 1, lettera a), si tratta delle opzioni di modifica da prevedere nella documentazione di gara, fornendo la descrizione quanto più precisa della circostanza che ne determina l'attivazione durante il corso di esecuzione del contratto. Qualora sia una modifica onerosa della prestazione l'importo deve considerato nel calcolo dell'importo dell'appalto. Presupposto imprescindibile: la modifica non deve alterare la struttura del contratto. Le clausole di modifica devono essere chiare, precise e inequivocabili. Possono consistere in clausole di opzione. Questa categoria di modifiche può essere presa in considerazione, come analizzato nel precedente paragrafo 3.2, nel caso in cu, in corso di esecuzione del contratto l'Amministrazione ha l'esigenza di modificare il servizio e di conseguenza gli SLA (ad esempio quando, anche per l'entrata in vigore di norme che rendano obbligatorio un livello di classificazione dei dati diverso rispetto a quello previsto dal contratto e di conseguenza un livello di qualificazione più stringente);

art. 120, comma 9, (quinto d'obbligo). Durante il corso di esecuzione del contratto, le prestazioni oggetto dello stesso possono essere aumentate o diminuite entro il limite del venti per cento dell'importo contrattualizzato;

art. 120, comma 10 proroga (l'istituto della proroga previsto da questo comma è alternativo e non cumulabile all'ipotesi di rinnovo);

Art. 76 comma 6 (ripetizione servizi analoghi).

4.6 Metriche di dimensionamento dei servizi cloud

Concorrono al dimensionamento e valutazione dei servizi cloud:

- Metriche di Disponibilità - Misurano la capacità del servizio di essere operativo e accessibile;
- Metriche di Prestazione - Monitorano l'efficienza e la velocità del servizio;
- Metriche di Scalabilità - Valutano la capacità del servizio di adattarsi a carichi variabili;
- Metriche di Sicurezza - Misurano la capacità di proteggere dati e risorse;
- Metriche di Affidabilità – Misurano la robustezza e l'operatività continua del servizio.;

- Metriche di utilizzo – Monitorano l'effettivo utilizzo delle risorse
- Metriche di Esperienza Utente (UX) – Misura il livello di soddisfazione utente.

In sede di definizione delle clausole contrattuali è importante specificare la documentazione e i report che il fornitore deve produrre per dare evidenza rispetto dei livelli di servizio.

Il contratto deve prevedere i tempi di presentazione della documentazione richiesta e la quantificazione delle penali per il mancato rispetto.

4.7 Direttore dell'esecuzione

L'Art. 114 del Dlgs 36/2023 al comma 1 prevede che l'esecuzione dei contratti è diretta dal RUP, che controlla i livelli di qualità delle prestazioni. Il RUP, nella fase dell'esecuzione, si avvale del direttore dell'esecuzione del contratto [..].

Ai sensi del comma 7 dello stesso articolo, per i contratti aventi ad oggetto servizi e forniture le funzioni e i compiti del direttore dell'esecuzione sono svolti, di norma, dal RUP, che provvede, anche con l'ausilio di uno o più direttori operativi individuati dalla stazione appaltante *in relazione alla complessità dell'appalto*, al coordinamento, alla direzione e al controllo tecnico contabile e amministrativo dell'esecuzione del contratto anche, qualora previsto, mediante metodi e strumenti di gestione informativa digitale di cui all'allegato I.9, assicurando la regolare esecuzione da parte dell'esecutore, in conformità ai documenti contrattuali. L'allegato II.14 del Codice individua i contratti di servizi e forniture di particolare importanza, per qualità o importo delle prestazioni, per cui il direttore dell'esecuzione deve essere diverso dal RUP.

In particolare, l'art. 32 dell'allegato II.14 individua i servizi di particolare importanza, per i quali il direttore di esecuzione deve essere diverso dal RUP.

Fra questi, il comma 2 dell'art. 32, prevede i servizi informatici, in quanto servizi complessi sotto il profilo tecnologico.

Pertanto, in questi casi, indipendentemente dall'importo, il ruolo di direttore di esecuzione deve essere svolto da un soggetto diverso rispetto al RUP.

4.8 Garanzie assicurative

Il Regolamento ACN dispone che il contratto preveda garanzie assicurative adeguate, per compensare il danno derivante dalla revoca della qualificazione o della dichiarazione di adeguatezza previsti dall'Art. 21 del Regolamento.

Le polizze devono essere definite sulla base della classe di rischio corrispondente al livello di classificazione di dati e servizi gestiti (ordinari, critici, strategici).

Possono essere previste ulteriori forme di assicurazione a fronte di una valutazione del rischio collegata a interruzioni del servizio, violazioni di dati, perdita dei dati (anche in fase di exit strategy).

4.9 Obblighi del fornitore

Oltre all'obbligo generale di eseguire tutte le prestazioni a perfetta regola d'arte, nel rispetto delle norme vigenti e secondo le condizioni, le modalità, i termini e le prescrizioni contenute nella documentazione contrattuale, è opportuno individuare gli obblighi specifici da inserire come clausole contrattuali.

- Mantenimento della Qualificazione ACN per tutta la durata del contratto;
- Manleva dell'Amministrazione dalla responsabilità per violazione di diritti di terzi;
- Obblighi derivanti dal PNRR (Rapporto di genere, Obblighi assunzionali, attestazione Do No Significant Harm" (DNSH).

4.10 Clausole di recesso e risoluzione

- Clausole di recesso unilaterale: possibilità per la PA di recedere dal contratto in caso di inadempimenti o mutamenti normativi;
- Clausole di Recesso nel caso in cui il fornitore offra o fornisca prodotti, ovvero la prestazione di servizi, che non abbiano i requisiti di conformità e/o le caratteristiche tecniche minime stabilite dalle normative vigenti;
- Clausola di Risoluzione in caso di intervenuta la decadenza dell'attestazione di qualificazione per aver prodotto falsa documentazione o dichiarazioni mendaci. (ai sensi dell'art. 1456 cod. civ nonché ai sensi dell'art.1360 cod. civ)
- Clausola di risoluzione nel caso in cui la qualificazione Cloud secondo le disposizioni dell'ACN del/dei servizio/i cloud oggetto di acquisizione venga a scadenza, senza che sia rinnovata, ovvero venga revocata in via definitiva (1456)

Nota per la lettura dei modelli allegati

In allegato alla Guida sono forniti i modelli che possono essere utilizzati come riferimento per l'impostazione della documentazione di gara per l'acquisto di servizi cloud.

I modelli sono i seguenti:

- ***Allegato A_Capitolato generale amministrativo***: sono indicate le clausole generali di carattere amministrativo che definiscono le modalità di esecuzione delle prestazioni, descritte da un punto di vista tecnico nel capitolato tecnico;

- ***Allegato B1_Capitolato tecnico (MOD. 1)***: contiene le indicazioni di massima riferite a servizi di migrazione, servizi cloud e servizi accessori. In particolare, per ogni categoria di servizi si indicano:
  - Caratteristiche della prestazione e requisiti che devono essere definiti dall'amministrazione;
  - metriche di dimensionamento;
  - modalità di esecuzione;
  - Esempi di SLA, relative penali e documentazione da consegnare**. *In relazione agli SLA si precisa che i servizi cloud oggetto dei contratti devono essere obbligatoriamente qualificati sul catalogo ACN. Pertanto, il fornitore deve garantire gli SLA richiesti ai fini della qualificazione. L'Amministrazione ha la possibilità di richiedere ulteriori SLA o SLA migliorativi. Quelli indicati nel modello allegato hanno una funzione indicativa utile a descrivere gli elementi peculiari del servizio utili a definirne la qualità e si riferiscono a servizi che gestiscono dati ordinari***

- **Allegato B2_Capitolato tecnico acquisto servizi Public Cloud SaaS (MOD. 2)**. Lo schema ha come riferimento servizi SaaS che trattano dati e servizi classificati come ordinari, per i quali è richiesto un livello di qualificazione di livello 1 QC1. Vengono fornite le indicazioni per rendere il capitolato conforme ai requisiti previsti dal Regolamento Cloud per la PA per una specifica categoria si servizi cloud;

- **Alleagato C_Schema di contratto**: disciplina dei rapporti fra le parti sulla base delle indicazioni contenute nel capitolato generale amministrativo e capitolato tecnico. Il modello è riferito a procedure di gara che prevedono il confronto competitivo fra operatori economici (procedure negoziate o procedure aperte).

Tali indicazioni devono essere considerate come esemplificative e non esaustive delle casistiche possibili e richiedono una necessaria operazione di contestualizzazione da parte dell'Amministrazione.

Il sistema Anci a supporto della digitalizzazione dei Comuni

Via dei Prefetti, 46 - 00186 Roma
trasformazionedigitale@anci.it

www.sistemacomunidigitali.anci.it

DIPARTIMENTO
PER LA TRASFORMAZIONE
DIGITALE

anci

Finanziato
dall'Unione europea
NextGenerationEU