Progetto «Progetto formativo CIVITAS - Competenze Innovative per Valorizzare l'Innovazione Territoriale Amministrativa Strategica.»
PON GOVERNANCE E CAPACITA' ISTITUZIONALE 2014-2020

Lezione n. 3.2.3. *Cloud Computing per la PA: strategia e implementazione - Principi della Strategia Cloud Italia, modelli di servizio e deployment*

Ing. Fabio Massimi

26 Gennaio 2026
Università LUMSA

UPI

LUMSA UNIVERSITÀ

AGENDA

1.Il Cloud nella trasformazione digitale della Pubblica Amministrazione

- Dal modello infrastrutturale tradizionale al paradigma cloud
- Il Cloud come infrastruttura abilitante dei servizi digitali

2.La Strategia Cloud Italia

- Razionali e obiettivi strategici
- Classificazione dei dati e dei servizi
- Ruolo e responsabilità delle amministrazioni pubbliche

3.Modelli di servizio Cloud

- IaaS, PaaS, SaaS
- Vantaggi, limiti e casi d’uso nella PA

4. Modelli di deployment

- Public, Private, Hybrid e Multicloud
- Criteri di scelta in relazione a sicurezza, continuità e governance

5.Considerazioni di governance

- Impatti organizzativi e decisionali
- Errori ricorrenti e lezioni apprese nella PA

OBIETTIVI

- Comprendere **il ruolo strategico del Cloud** nel processo di trasformazione digitale della PA italiana
- Conoscere i **principi fondamentali della Strategia Cloud Italia** e il quadro di riferimento nazionale
- Distinguere correttamente i **modelli di servizio Cloud (IaaS, PaaS, SaaS)** e i relativi ambiti di applicazione nella PA
- Valutare i **modelli di deployment** più adeguati in funzione:
  - della tipologia di dati
  - dei requisiti di sicurezza
  - delle esigenze organizzative
- Acquisire consapevolezza delle **responsabilità decisionali e di governance** legate all'adozione del Cloud
- Evitare approcci meramente tecnologici, riconoscendo il Cloud come **scelta strategica e organizzativa**, non solo infrastrutturale

PERCHE’ IL CLOUD E’ CENTRALE PER LA PA

La Pubblica Amministrazione italiana è chiamata a:

- garantire **servizi digitali affidabili, sicuri e interoperabili**
- gestire volumi crescenti di dati e applicazioni
- assicurare continuità operativa e resilienza dei sistemi

Il modello ICT tradizionale della PA presenta limiti strutturali:

- frammentazione dei data center
- elevati costi di gestione e manutenzione
- difficoltà di aggiornamento tecnologico
- scarsa scalabilità e flessibilità

Il Cloud Computing rappresenta il cambio di paradigma:

- da infrastrutture locali a servizi condivisi
- da gestione tecnica a **governance del servizio**
- da investimenti rigidi a modelli flessibili e misurabili

È **abilitatore della trasformazione digitale**, non un fine tecnologico. Consente:

- maggiore **scalabilità** dei servizi
- migliore **sicurezza e resilienza**
- supporto all’**interoperabilità** e alla cooperazione applicativa

È un **prerequisito** per:

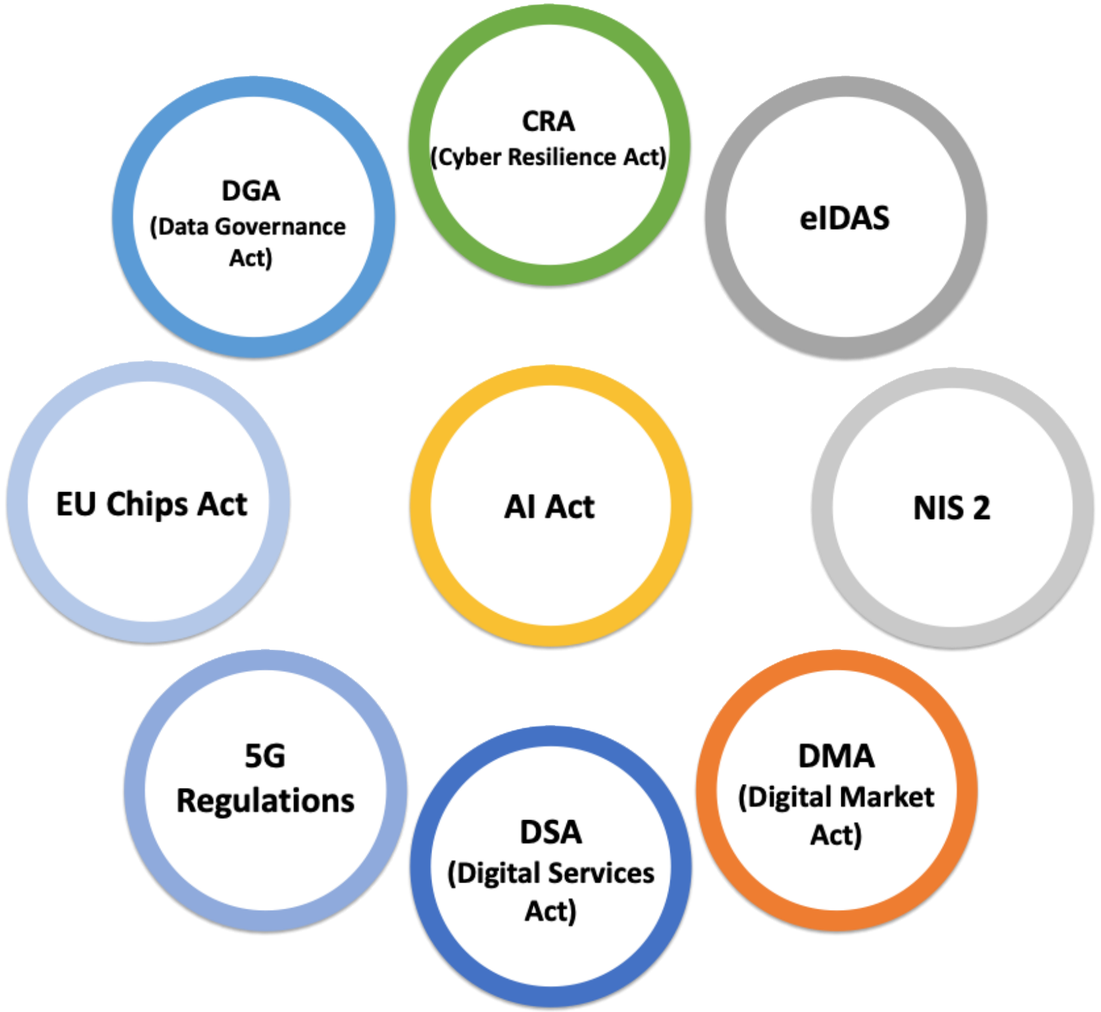
- digitalizzazione dei servizi
- attuazione del PNRR
- innovazione tecnologica nella PA

Attraverso regole comuni, **standard condivisi** e **interoperabilità**, l'Europa punta a creare un ecosistema dove **innovazione**, **sicurezza** e **tutela dei diritti** procedano insieme, favorendo la crescita e la competitività di cittadini, imprese e pubbliche amministrazioni.

Brussels Effect

L'UE stabilisce **regole rigorose per i beni e servizi** che accedono al suo mercato. Tali regole sono adottate dalle grandi imprese anche fuori dall'Europa, generando un **impatto sul mercato globale**.

EU Digital Single Market



La Strategia Cloud Italia

CONTESTO ED OBIETTIVI

Tre sfide principali:

- assicurare l'**autonomia tecnologica** del Paese,
- garantire il **controllo sui dati**,
- aumentare la **resilienza dei servizi digitali**.

Obiettivo:
75% delle PA italiane in cloud qualificato

AGID Agenzia per l'Italia Digitale

Consolidamento datacenter della PA
Censimento AgID del 2019: su 1252 DC censiti, solo 62 avevano requisiti adeguati

FATTORI ABILITANTI

Italiadomani
PIANO NAZIONALE DI RIPRESA E RESILIENZA

INTERVENTO 1.1

Valore: 900 M€
PSN e relativa migrazione di 280 PAC/ASL

INTERVENTO 1.2

Valore: 1000 M€
Migrazione di 12.464 PAL a servizi cloud qualificati

ALTRI INTERVENTI

Progettualità settoriali, con particolare riferimento all'**ambito sanitario**, ad es. **Fascicolo Sanitario Elettronico**

Le linee di indirizzo strategiche

Classificazione di dati e servizi

- ➔ Guida le PA nella scelta della soluzione cloud più adeguata.
- ➔ Valuta il **danno che una loro compromissione può provocare al Paese**.

Qualificazione dei servizi cloud

- ➔ **Semplifica e regolamenta l'acquisizione di servizi cloud da parte delle PA,**
  dal punto di vista tecnico (ad es. gestione operativa, sicurezza) e amministrativo (ad es. condizioni contrattuali).

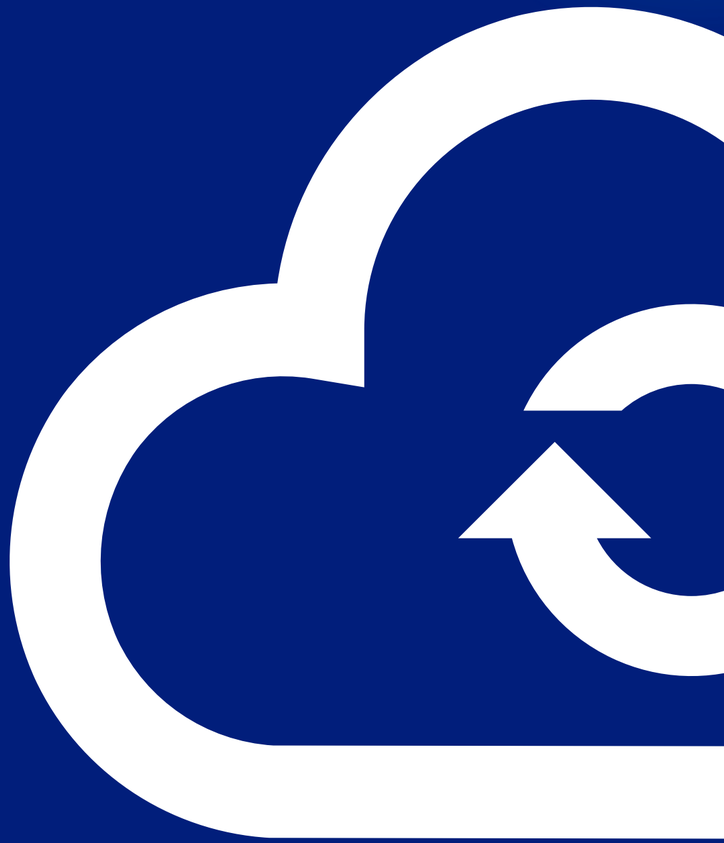
Polo Strategico Nazionale (PSN)

- ➔ Garantisce **continuità operativa e tolleranza ai guasti** per i servizi strategici e critici della PA.
- ➔ Distribuito su territorio nazionale, il controllo e le linee di indirizzo sono
  pubbliche e indipendenti da soggetti terzi.
- ➔ La gestione operativa è affidata a un fornitore selezionato mediante **partenariato pubblico-privato e gara UE.**

Dal censimento AgID del 2019, su 1252 Data Center censiti, solo 62 avevano requisiti adeguati.

AGID | Agenzia per l'Italia Digitale

Definizioni e contesto



Cloud computing: definizioni

Cloud computing is a model for enabling **ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources** (e.g., networks, servers, storage, applications, and services) that can be **rapidly provisioned and released** with **minimal management effort or service provider interaction. (NIST Special Publication 800-145, September 2011)**

Paradigm for enabling network access to a **scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand.**

Note 1 to entry: Examples of resources include servers, operating systems, networks, software, applications, and storage equipment. Note 2 to entry: Self-service provisioning refers to the provisioning of resources provided to cloud services (3.1.2) performed by cloud service customers (3.3.2) through automated means.

(ISO/IEC 22123-1:2023(en) Information technology — Cloud computing — Part 1: Vocabulary)

Paradigma che abilita l'accesso via rete ad un insieme **condivisibile, scalabile ed elastico di risorse fisiche o virtuali** attivabile **autonomamente su richiesta dall'utente.**

(Regolamento Cloud, ACN Decreto Direttoriale n. 21007/24 del 27 giugno 2024)

Glossario cloud

Compute
Risorse di calcolo (fisiche o virtuali) messe a disposizione da un cloud provider per l'esecuzione di carichi di lavoro.

Memory
Risorse di memoria volatile (fisiche o virtuali) utilizzate per l'elaborazione temporanea dei dati e il supporto all'esecuzione dei processi.

Storage
Risorse di archiviazione (fisiche o virtuali) che consentono la conservazione e gestione dei dati su richiesta del cliente cloud.

Network
Risorse di rete (fisiche o virtuali) che permettono la connettività, la comunicazione e il trasferimento dei dati tra risorse cloud, servizi e utenti.

Abstraction
Capacità di rappresentare e gestire le risorse fisiche come entità logiche e virtuali, semplificando l'interazione con i servizi cloud senza esporre dettagli infrastrutturali.

Virtualisation
Tecnologia che consente di creare istanze virtuali di risorse fisiche (es. server, rete, storage), permettendo la condivisione efficiente delle risorse fisiche sottostanti.

Scalability
Capacità del cloud di aumentare o diminuire le risorse disponibili in modo dinamico per soddisfare variazioni di domanda senza interruzioni di servizio.

Interoperability
Capacità di sistemi e servizi cloud di scambiarsi dati e interagire tra loro in modo coerente, secondo termini e tecnologie standard.

Caratteristiche fondamentali del cloud computing

Resource pooling

Le risorse fisiche o virtuali del provider sono **aggregate in pool** per servire uno o più clienti, abilitando la multi-tenancy e nascondendo la complessità tramite **astrazione**. Il cliente non controlla né conosce l'esatta allocazione o localizzazione delle risorse, salvo vincoli definiti.

Broad network access

Le risorse cloud sono **accessibili tramite rete** con meccanismi standard, da diversi dispositivi e luoghi, attraverso reti pubbliche o private, nel rispetto di policy e sicurezza, garantendo accessibilità e **interoperabilità per utenti, applicazioni e servizi cloud**.

Measured service

L'utilizzo dei servizi cloud è **misurato, monitorato, controllato e rendicontato**, consentendo modelli di costo basati sul consumo effettivo. La misurazione supporta fatturazione, gestione operativa e rispetto degli SLA, includendo risorse fisiche e virtuali.

Rapid elasticity and scalability

La capacità dei servizi cloud può essere **aumentata o ridotta rapidamente**, anche in modo automatico, facendo apparire le risorse come potenzialmente illimitate. La **scalabilità può essere orizzontale**, tramite l'aggiunta di istanze, **o verticale**, tramite l'aumento delle risorse assegnate.

On-demand self-service

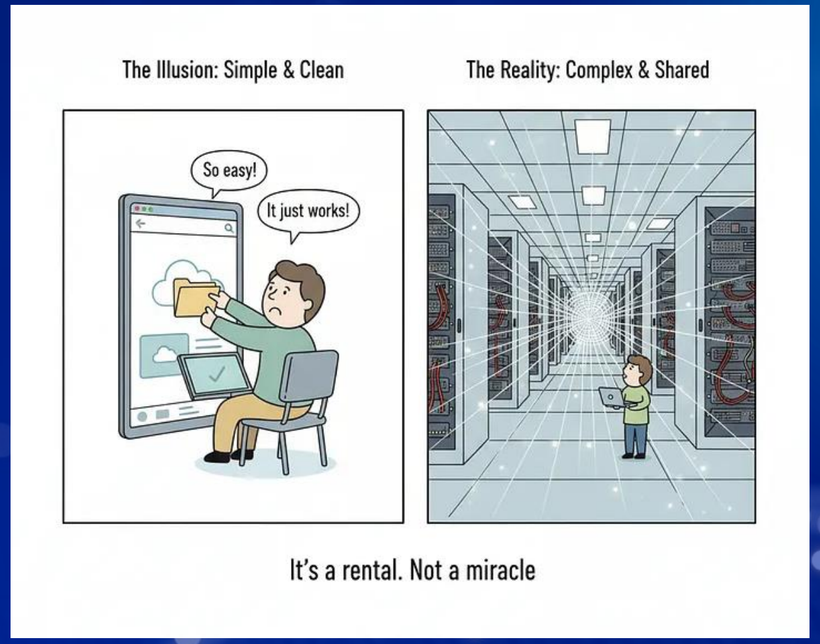
I servizi cloud possono essere **attivati e configurati autonomamente dal cliente**, in modo automatico o con minima interazione con il fornitore. Questo consente di **ridurre tempi, costi e sforzi operativi**, permettendo di allocare risorse come memoria o spazio disco senza intervento umano.

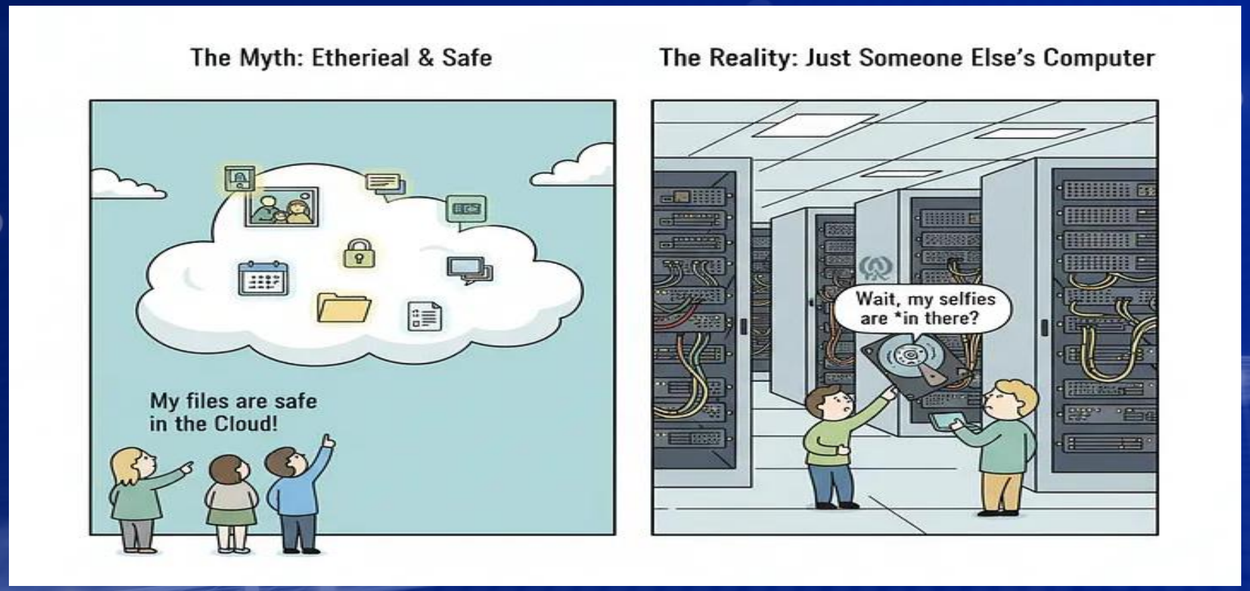
Multi-tenancy

Le risorse fisiche o virtuali sono condivise tra più tenant, garantendo l'isolamento e l'inaccessibilità reciproca di dati e carichi di lavoro. La multi-tenancy può riguardare utenti di una o più organizzazioni e richiede adeguati **meccanismi di identità, accesso e sicurezza**.

Fonte: ISO/IEC 22123-2:2023 - Information technology — Cloud computing — Part 2: Concepts

*





Il cloud non costituisce una tecnologia “magica”, ma consiste nell’utilizzo di **risorse di calcolo di terzi accessibili tramite rete.** L’elemento distintivo non risiede nell’hardware, bensì nel **modello di servizio**, basato su **astrazione**, **automazione**, **scalabilità**, **pagamento a consumo** e **responsabilità condivise**. Comprendere il cloud significa quindi **analizzare i meccanismi di gestione**, **controllo dei dati** e **governo dei servizi**, piuttosto che la localizzazione fisica delle infrastrutture.

*Campagna blog e social almeno dal 2016

Riduzione dei costi iniziali

Astrazione e semplificazione

Scalabilità ed elasticità

Affidabilità e resilienza

Automazione operativa

Perdita di controllo diretto sull’infrastruttura

Costi non prevedibili se mal governati

Lock-in

Trasparenza limitata

Responsabilità condivisa, non trasferita

Espansione dei data center: sfide e fattori critici

Energia

Raffredamento e risorse idriche

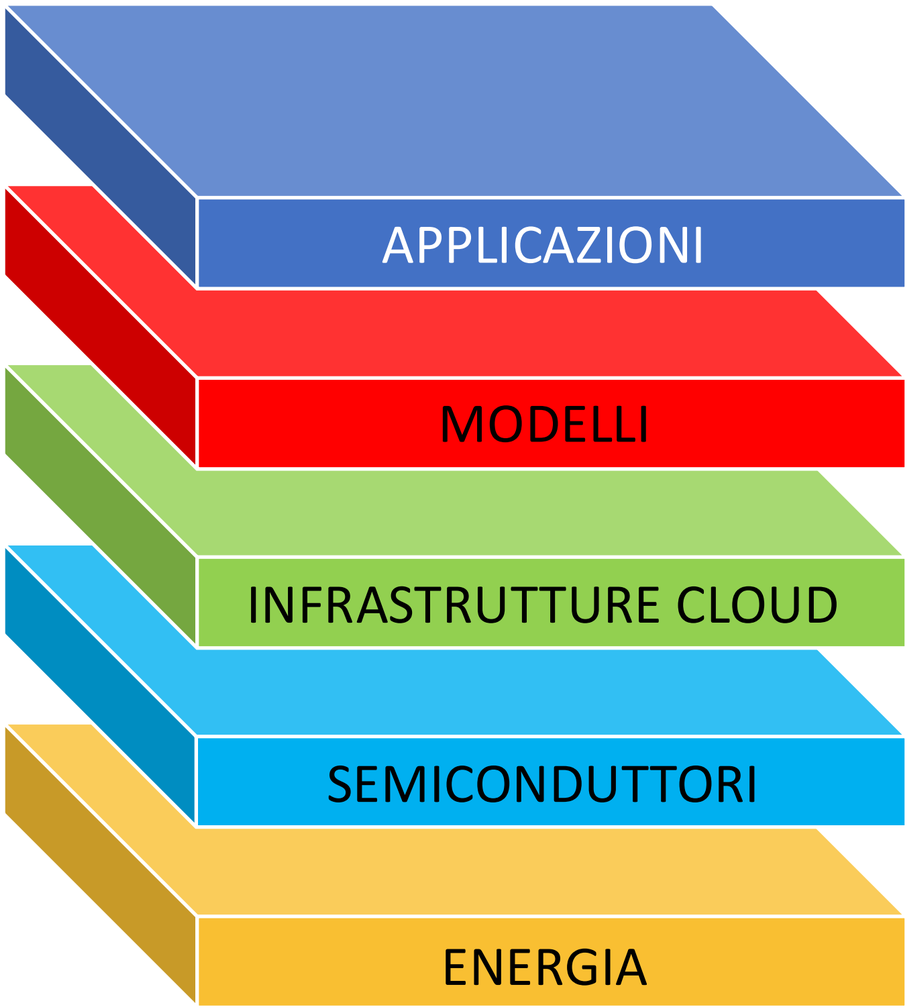
Conformità normativa

Spazio fisico

Sovranità

«Per l'IA stiamo realizzando la più grande infrastruttura della storia umana»
Jensen Huang, CEO di NVIDIA, WEF Davos 2026

Ruolo del Cloud nello sviluppo dell'Intelligenza Artificiale



*Jensen Huang, CEO di NVIDIA

*Pila NVIDIA**

Valore economico e sociale. L'IA diventa servizio, prodotto e supporto alle decisioni per cittadini, imprese e PA.

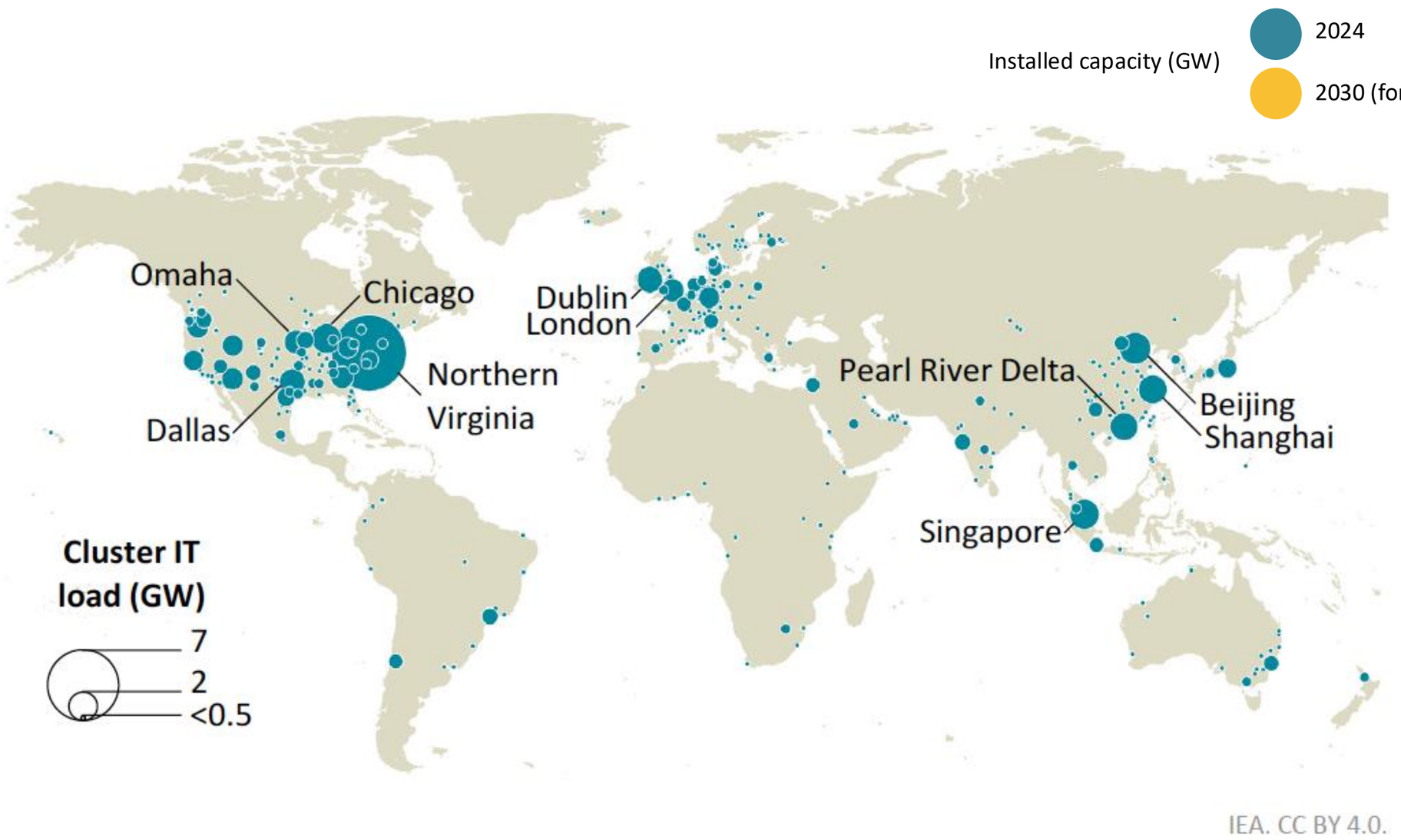
Intelligenza codificata. Algoritmi e modelli fondazionali concentrano conoscenza, elaborazione dati e capacità predittiva.

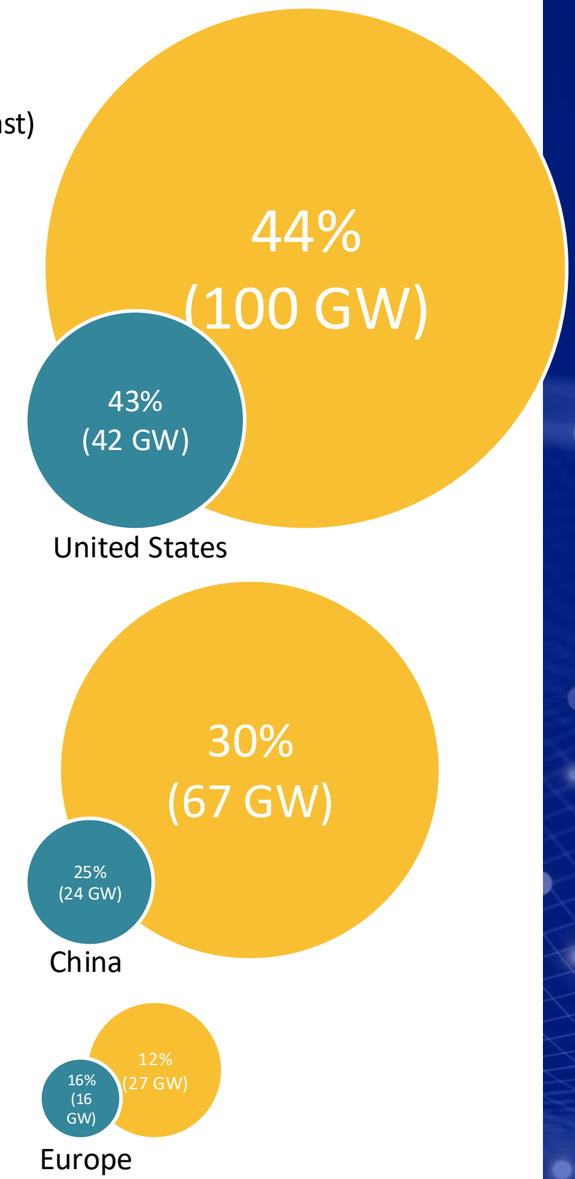
Strato abilitante e moltiplicatore. Trasforma energia e chip in capacità di calcolo accessibile, scalabile e governabile su larga scala.

Cuore computazionale. Chip specializzati (GPU, acceleratori) determinano prestazioni, efficienza e autonomia tecnologica.

Fondamento materiale dell'IA. Senza disponibilità energetica stabile e scalabile non esiste capacità di calcolo né addestramento dei modelli.

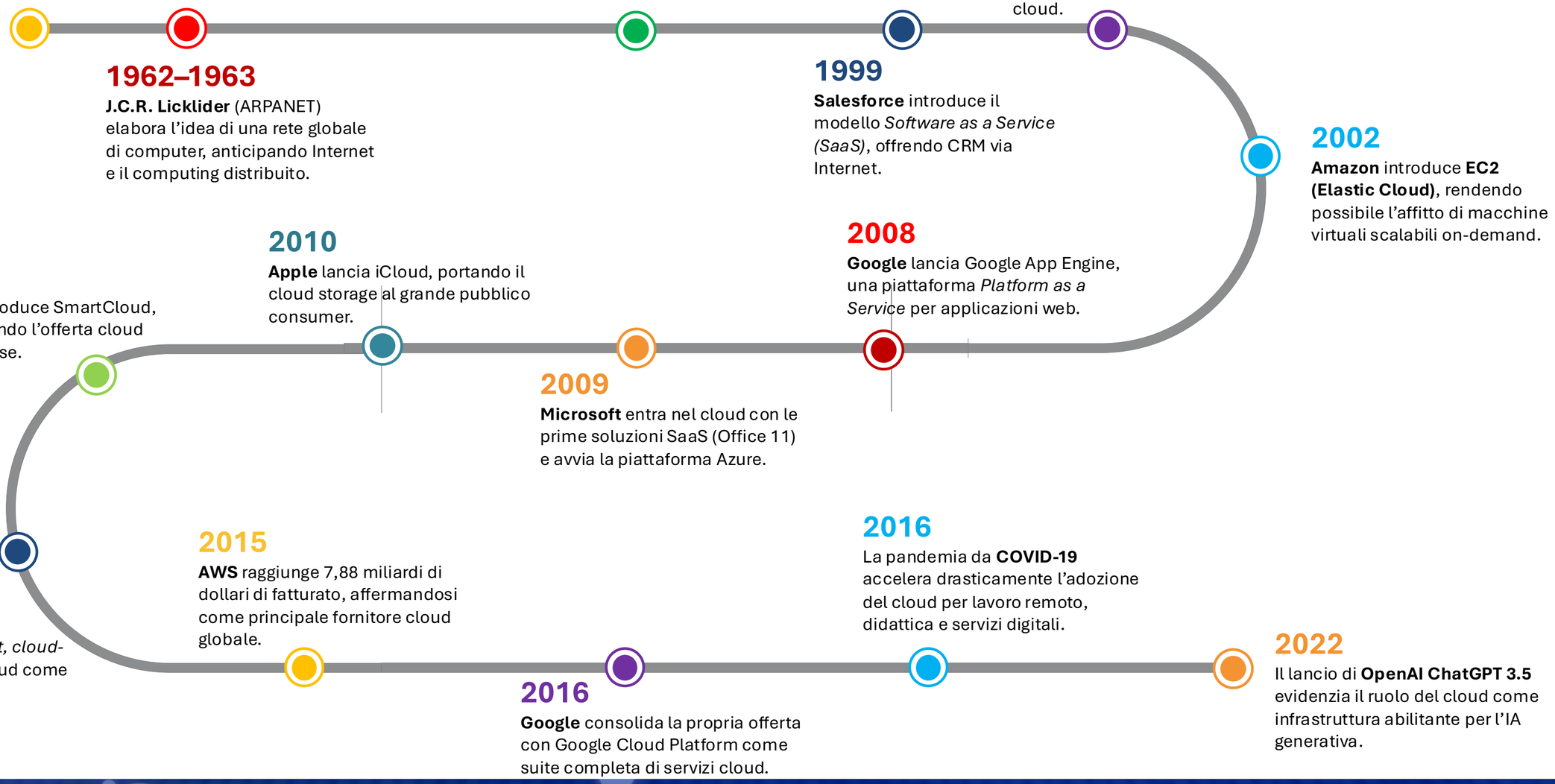
Global map of large data centre clusters 2024*





Source: World Energy Outlook Special Report – Energy and IA – IEA 2025

Evoluzione del Cloud Computing



1960s

John McCarthy introduce i concetti di *time sharing* e *utility computing*: l'informatica come servizio on-demand con modelli a consumo.

1962–1963

J.C.R. Licklider (ARPANET) elabora l'idea di una rete globale di computer, anticipando Internet e il computing distribuito.

1997

Ramnath Chellappa utilizza per la prima volta il termine *cloud computing* in un lavoro sull'economia del computing.

1999

Salesforce introduce il modello *Software as a Service (SaaS)*, offrendo CRM via Internet.

2002

Amazon Web Services viene lanciato, ponendo le basi per servizi di storage e calcolo in cloud.

2002

Amazon introduce **EC2 (Elastic Cloud)**, rendendo possibile l'affitto di macchine virtuali scalabili on-demand.

2008

Google lancia Google App Engine, una piattaforma *Platform as a Service* per applicazioni web.

2009

Microsoft entra nel cloud con le prime soluzioni SaaS (Office 11) e avvia la piattaforma Azure.

2010

Apple lancia iCloud, portando il cloud storage al grande pubblico consumer.

2011

IBM introduce SmartCloud, rafforzando l'offerta cloud enterprise.

2014

Microsoft adotta la strategia *"mobile-first, cloud-first"*, segnando il cloud come priorità aziendale.

2015

AWS raggiunge 7,88 miliardi di dollari di fatturato, affermandosi come principale fornitore cloud globale.

2016

Google consolida la propria offerta con Google Cloud Platform come suite completa di servizi cloud.

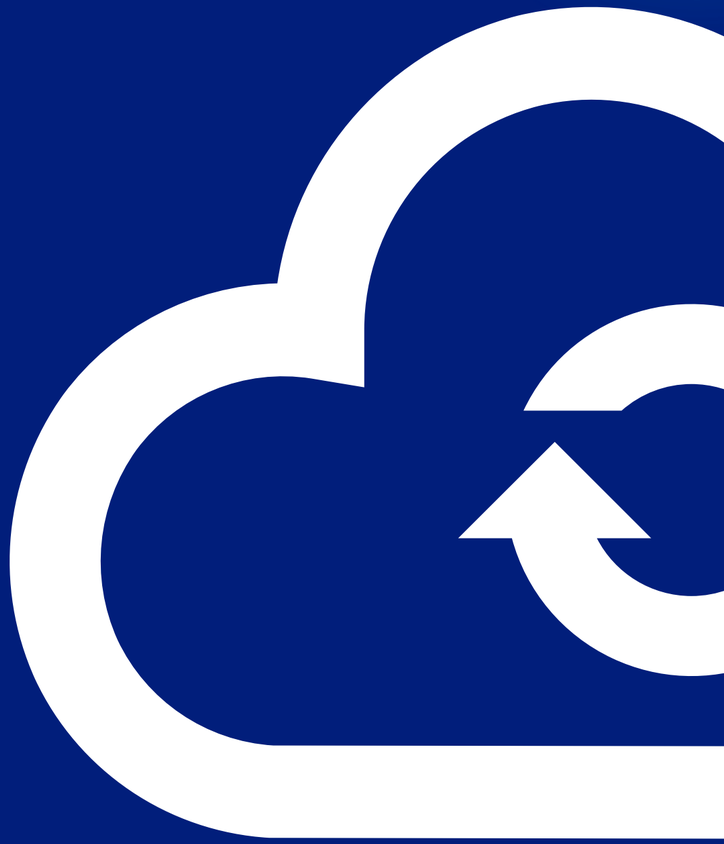
2016

La pandemia da **COVID-19** accelera drasticamente l'adozione del cloud per lavoro remoto, didattica e servizi digitali.

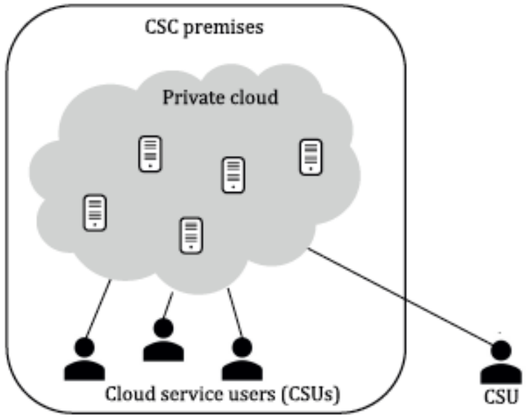
2022

Il lancio di **OpenAI ChatGPT 3.5** evidenzia il ruolo del cloud come infrastruttura abilitante per l'IA generativa.

Modelli di erogazione e tipologia di servizio

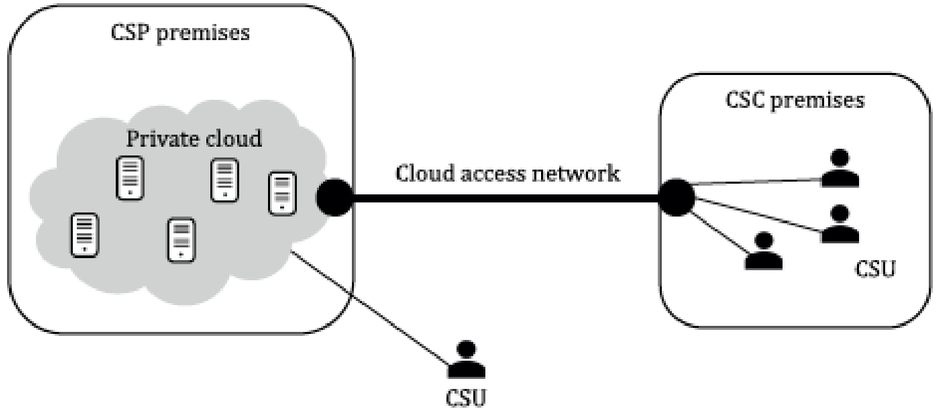


Modeli di erogazione: private cloud



Private Cloud on-premise

Infrastruttura cloud **dedicata a un'unica organizzazione (CSC)**, **realizzata e gestita all'interno dei propri data center** o sotto il suo diretto controllo.
Consente **massimo controllo su dati, sicurezza, configurazioni e localizzazione**, facilitando il rispetto di requisiti normativi e di sovranità. Richiede però alla CSC di **sostenere direttamente i costi di investimento, gestione e capacità di riserva** necessari a garantire scalabilità ed elasticità.



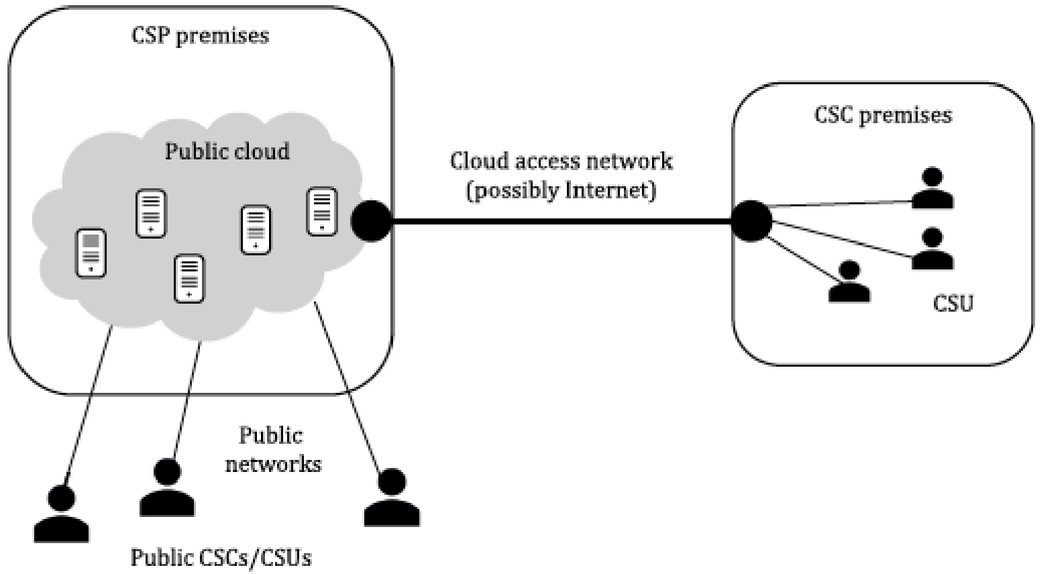
Private Cloud off-premise (Dedicated Cloud)

Infrastruttura cloud **dedicata a un'unica organizzazione (CSC)**, **ospitata presso un Cloud Service Provider** che ne può essere proprietario e responsabile operativo.
Offre **isolamento logico, controllo e garanzie contrattuali**, mantenendo molte **caratteristiche operative del cloud pubblico** (scalabilità, automazione, resilienza). Rappresenta un compromesso tra **controllo, conformità e flessibilità**, con dinamiche di integrazione simili a quelle di un **modello ibrido**.

Fonte: ISO/IEC 22123-2:2023 - Information technology — Cloud computing — Part 2: Concepts

CSC cloud service customer - CSP cloud service provider - CSU cloud service user

Modelli di erogazione: public cloud



Public Cloud

Modello di erogazione in cui i **servizi cloud sono resi disponibili a una pluralità di organizzazioni (CSC)**, tipicamente tramite **reti pubbliche**, e basati su **infrastrutture condivise**.

Il cloud è **di proprietà e sotto il controllo del Cloud Service Provider**, mentre il singolo CSC **non ha visibilità né controllo sugli altri utenti** che condividono le risorse.

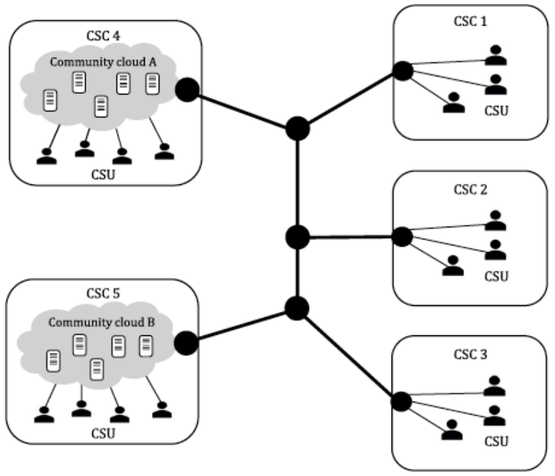
Il modello abilita **elevata scalabilità, elasticità e ottimizzazione dei costi** grazie alla multi-tenancy

L'accesso è soggetto a **vincoli contrattuali, normativi e giurisdizionali**.

Fonte: ISO/IEC 22123-2:2023 - Information technology — Cloud computing — Part 2: Concepts

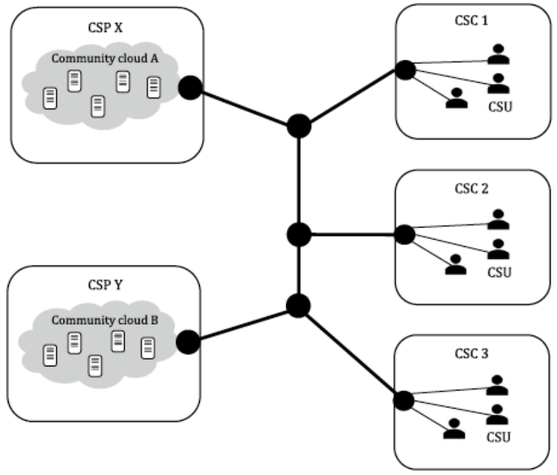
CSC cloud service customer - CSP cloud service provider - CSU cloud service user

Modelli di erogazione: community cloud



Community Cloud on-premises

Modello di erogazione in cui i **servizi cloud sono condivisi esclusivamente tra un gruppo definito di organizzazioni (CSC)** che presentano **esigenze comuni** in termini di missione, sicurezza, policy o conformità normativa.
L'infrastruttura è **ospitata presso una o più organizzazioni della comunità**, che ne mantengono il controllo diretto.
Le CSC partecipanti possono **accedere sia alle risorse locali sia a quelle delle altre organizzazioni**, favorendo cooperazione, riuso e ottimizzazione, pur mantenendo **confini di accesso verificati**.



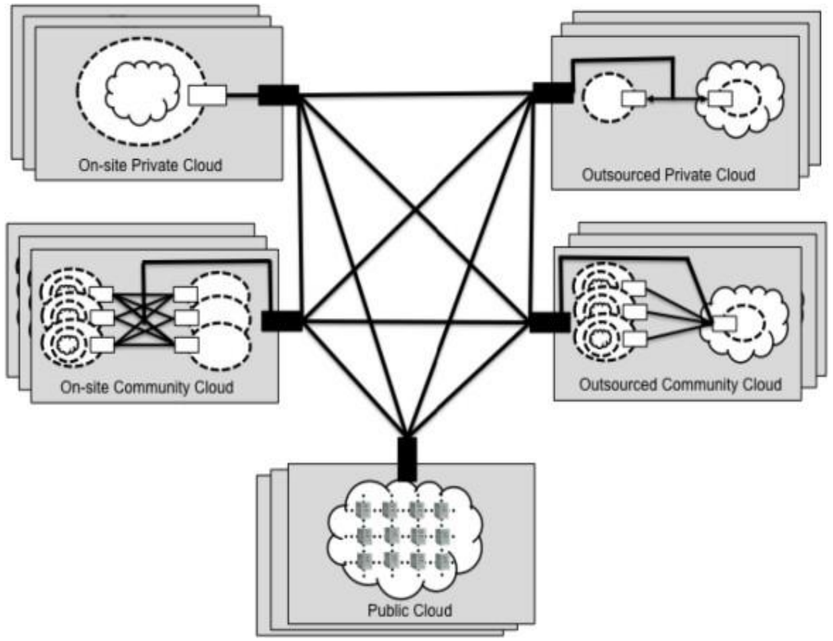
Community Cloud off-premises

Modello di erogazione in cui i **servizi cloud sono dedicati a una comunità definita di organizzazioni**, ma l'infrastruttura è **ospitata e gestita off-premises**, tipicamente da un **Cloud Service Provider o da un soggetto terzo**.
Combina **benefici economici e di scalabilità tipici del cloud pubblico** con **livelli rafforzati di privacy, sicurezza e compliance**, grazie a **meccanismi contrattuali di controllo dell'appartenenza alla comunità**, autorizzazione degli utenti e **verifiche indipendenti** sull'esclusività delle risorse.

Fonte: ISO/IEC 22123-2:2023 - Information technology — Cloud computing — Part 2: Concepts

CSC cloud service customer - CSP cloud service provider - CSU cloud service user

Modelli di erogazione: Hybrid Cloud



Hybrid Cloud

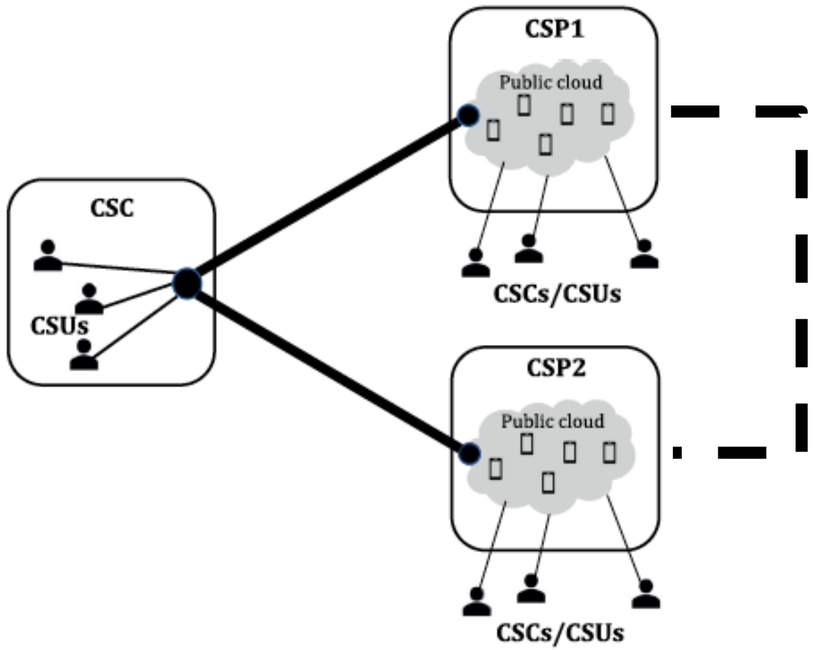
Modello di erogazione che **combina un private cloud e uno o più public cloud**, mantenuti come **entità distinte ma integrate** tramite tecnologie che abilitano **interoperabilità, portabilità dei dati e delle applicazioni**.

Consente di **distribuire carichi di lavoro e dati tra ambienti diversi** in funzione di requisiti di sicurezza, prestazioni, costi o conformità.

I singoli ambienti possono essere **on-premises o off-premises**, gestiti dall'organizzazione o da terzi, e coinvolgere **uno o più Cloud Service Provider**, anche senza una loro reciproca consapevolezza.

Fonti: ISO/IEC 22123-2:2023 - Information technology — Cloud computing — Part 2: Concepts; NIST Cloud Computing Reference Architecture SP 500-292.

Modelli di erogazione: multi-cloud



Multi-cloud

Modello di erogazione in cui un'organizzazione (**CSC**) utilizza **servizi cloud di più Cloud Service Provider**, mantenendo il **controllo centralizzato sugli utenti (CSU), sulle politiche e sulle attività di gestione**.

Il CSC stipula **accordi contrattuali e SLA distinti con ciascun CSP**, che possono differire per funzionalità, livelli di servizio, localizzazione e costi.

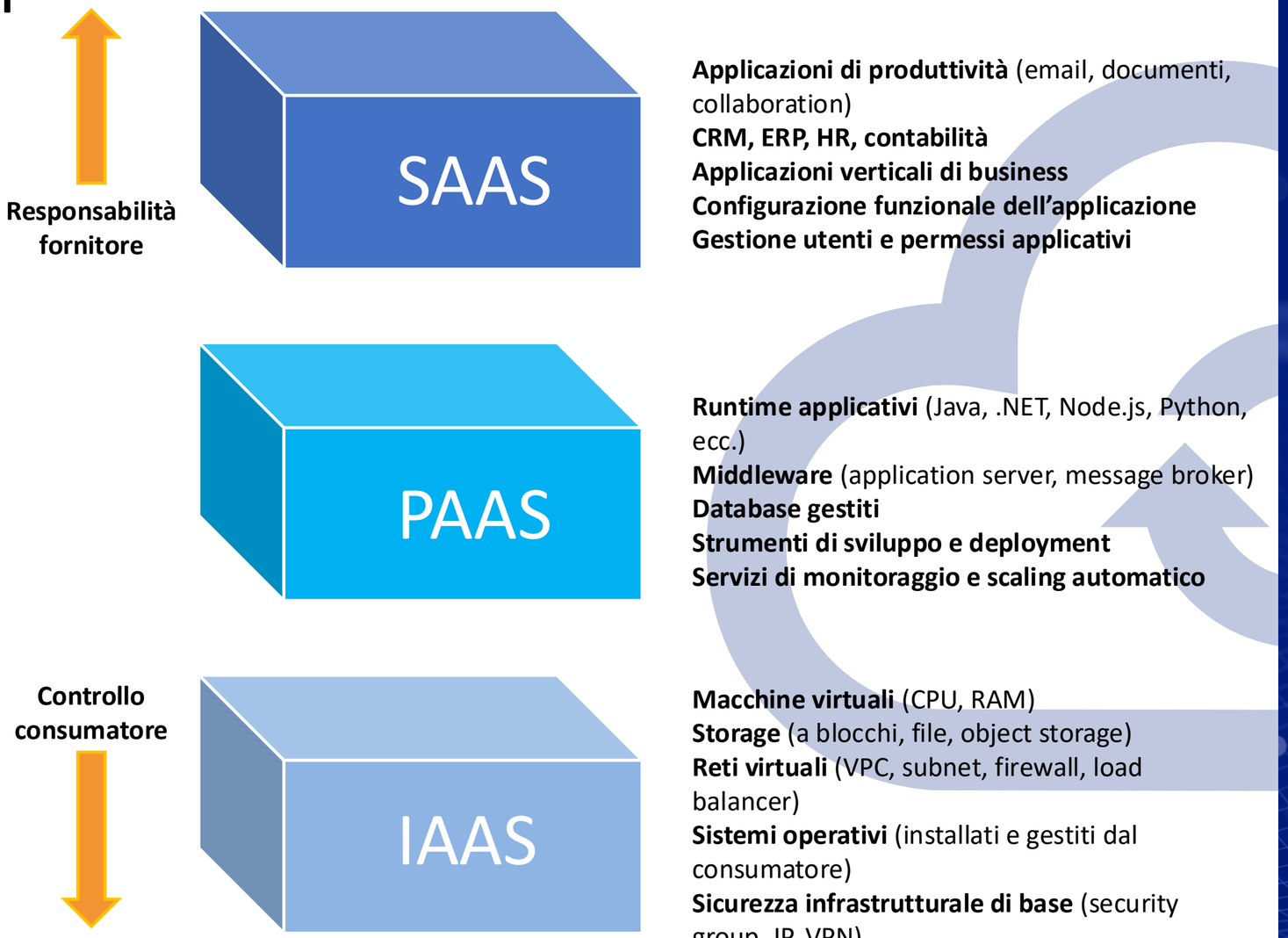
Il modello può essere **CSC-mediated**, con interazioni gestite direttamente dal CSC, oppure **CSP-connected**, in cui l'integrazione tecnica tra i cloud è controllata dal CSC.

La multi-cloud aumenta **flessibilità e resilienza**, ma richiede **forte capacità di governance e coordinamento**.

Fonti: ISO/IEC 5140:2024 Information technology — Cloud computing — Concepts for multicloud and the use of multiple cloud services.

Tipologie di servizio fondamentali

- **IaaS, PaaS e SaaS** rappresentano **livelli crescenti di *astrazione*** del **servizio cloud**.
- Salendo nella **pila dei servizi**, diminuisce la **gestione tecnica diretta** in capo all'**organizzazione**.
- Aumentano **velocità di adozione, scalabilità operativa** e **responsabilità del provider**.
- I modelli si differenziano per il diverso equilibrio del **Shared Responsibility Model**.

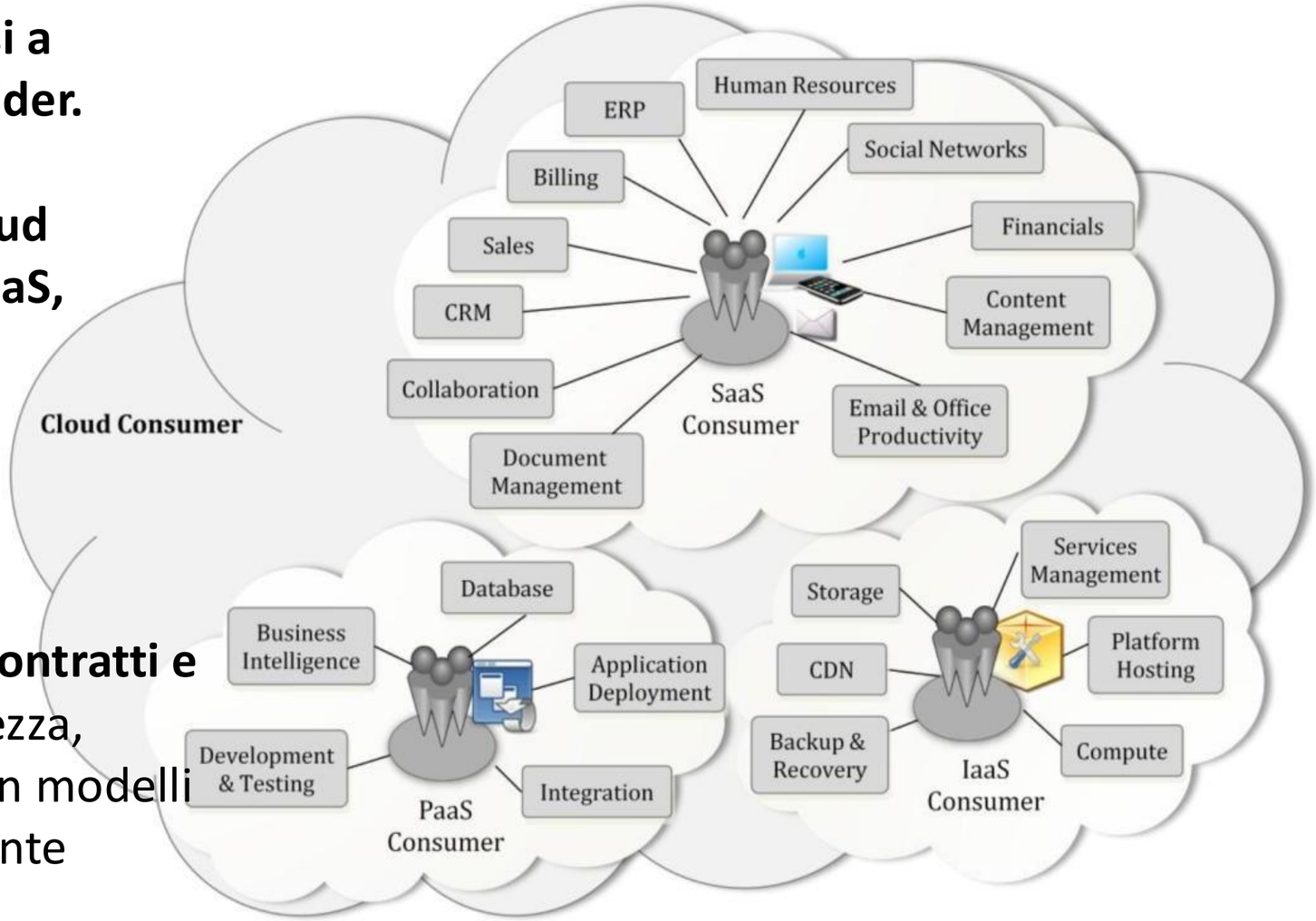


Esempi di servizi cloud disponibili per il Cloud Consumer

Il Cloud Consumer è il soggetto che seleziona, contratta e utilizza i servizi cloud messi a disposizione da un Cloud Service Provider.

Attraverso il catalogo dei servizi, il Cloud Consumer può accedere a soluzioni SaaS, PaaS e IaaS, scegliendo il livello di astrazione più adatto alle proprie esigenze operative, organizzative e di governance.

L'erogazione dei servizi è regolata da contratti e SLA, che definiscono prestazioni, sicurezza, responsabilità e modalità di utilizzo, con modelli di costo basati sulle risorse effettivamente consumate.



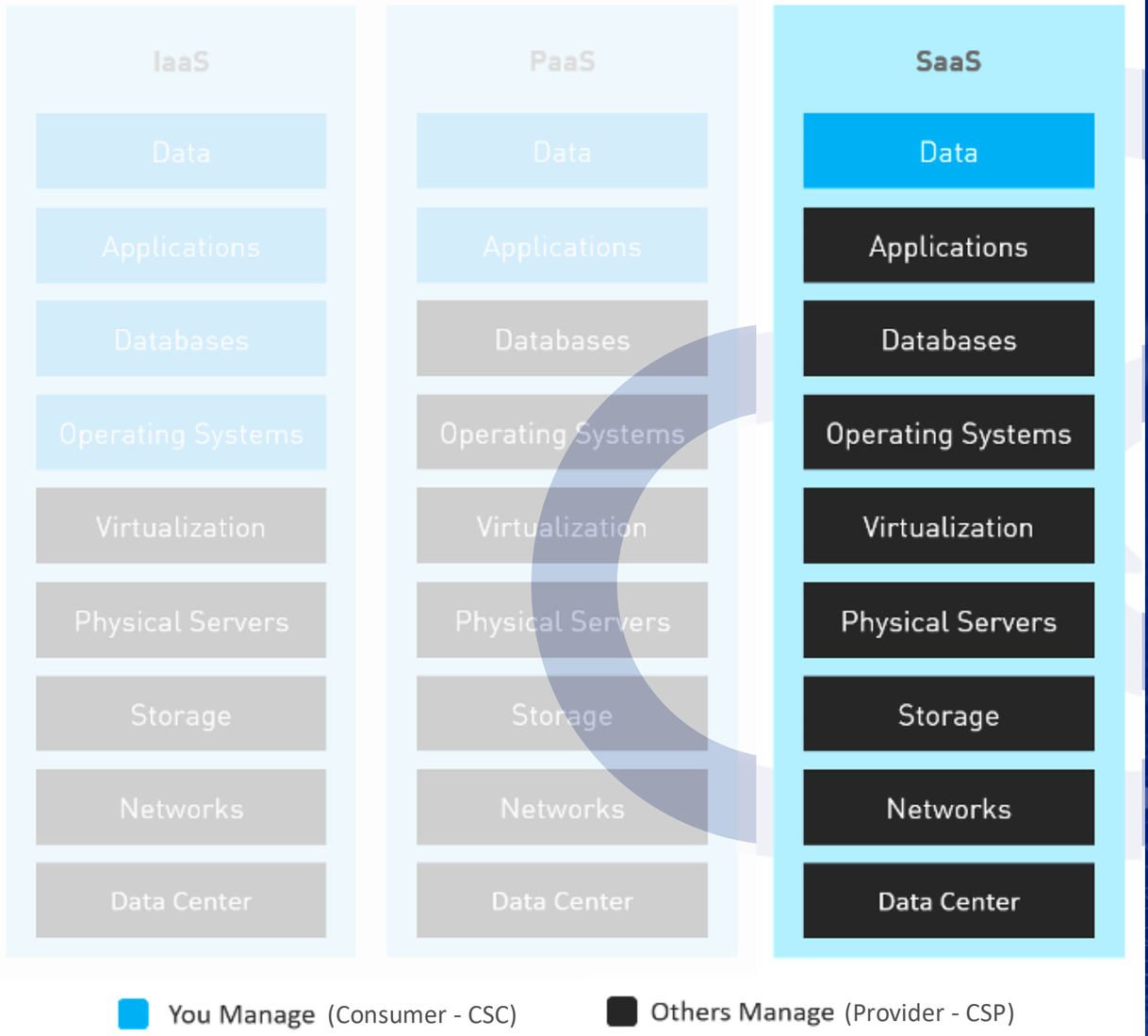
Fonti: NIST Cloud Computing Reference Architecture SP 500-292.

SAAS – Software As A Service

Categoria di servizio cloud in cui al **Consumatore di Servizi Cloud** vengono fornite **capacità applicative complete**, eseguite su **infrastrutture e risorse del Cloud Service Provider**.

Le applicazioni sono accessibili tramite **interfacce leggere** (es. browser web) o **API**, nel rispetto di **contratti e SLA** definiti. Il consumatore **non gestisce né controlla** infrastruttura, piattaforma o applicazione, ad eccezione di **limitazioni di configurazione specifiche per l'utente**.

Il **provider è responsabile dell'intero ciclo di vita del software**, inclusi distribuzione, configurazione, manutenzione e aggiornamenti, anche quando lo sviluppo dell'applicazione è affidato a soggetti terzi.



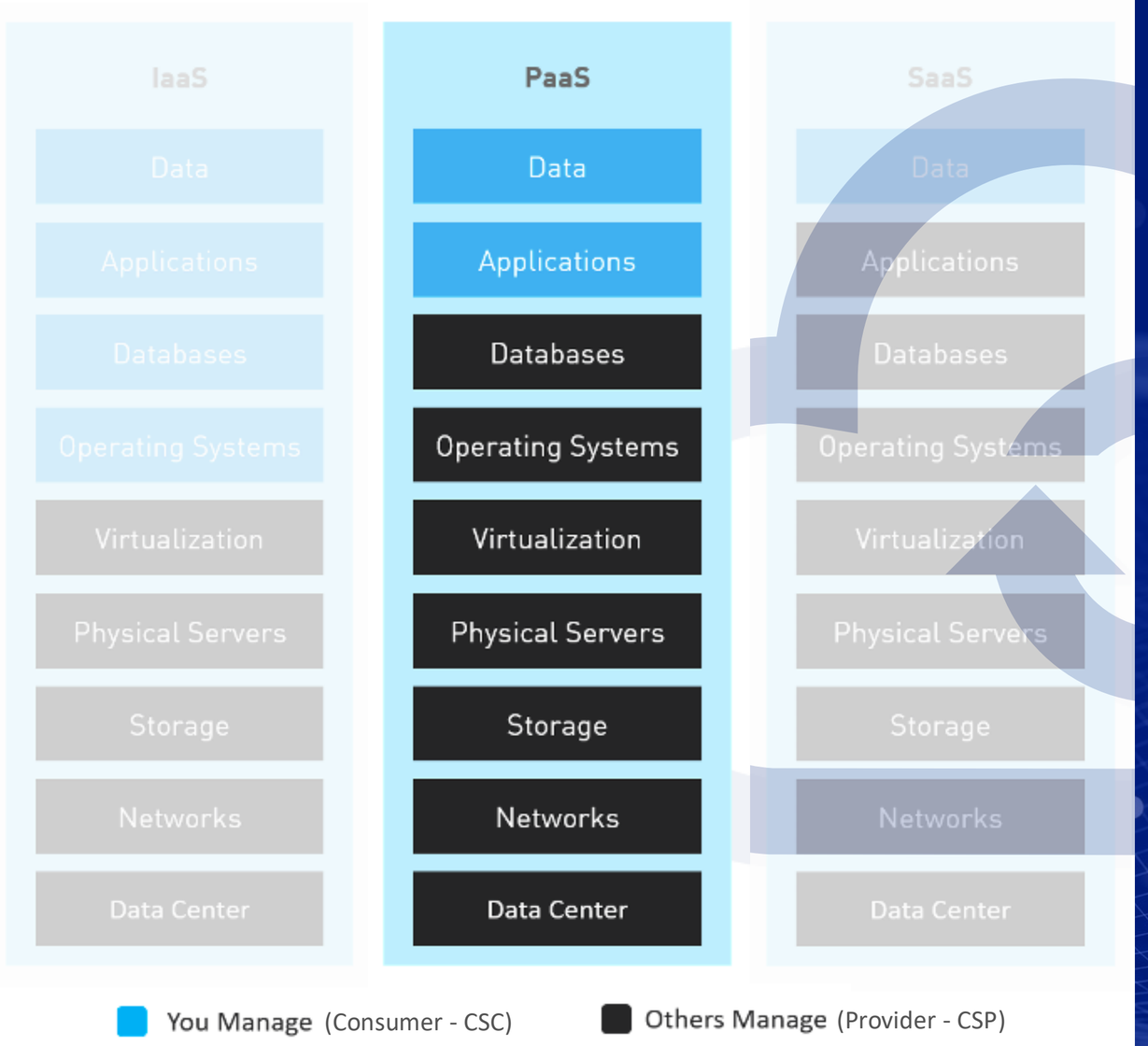
Fonte: ISO/IEC 22123-2:2023 - Information technology — Cloud computing — Part 2: Concepts

PAAS – Platform As A Service

Categoria di servizio cloud in cui al **Consumatore di Servizi Cloud** vengono fornite **capacità di piattaforma** per **sviluppare, testare, distribuire e gestire applicazioni** eseguite su **risorse del Cloud Service Provider**.

Il servizio mette a disposizione **linguaggi di programmazione, librerie, servizi e strumenti** supportati dal provider, senza escludere l'uso di componenti compatibili di terze parti. Il termine *piattaforma* indica un **ambiente di sviluppo e di esecuzione per applicazioni cloud-native**, destinato principalmente a **sviluppatori e personale operativo**, e non agli utenti finali.

Il consumatore **non gestisce l'infrastruttura sottostante** (rete, server, sistemi operativi, storage), ma mantiene il **controllo sulle applicazioni distribuite** e su alcune **configurazioni dell'ambiente di esecuzione**, nel rispetto dei **contratti e degli SLA** concordati.



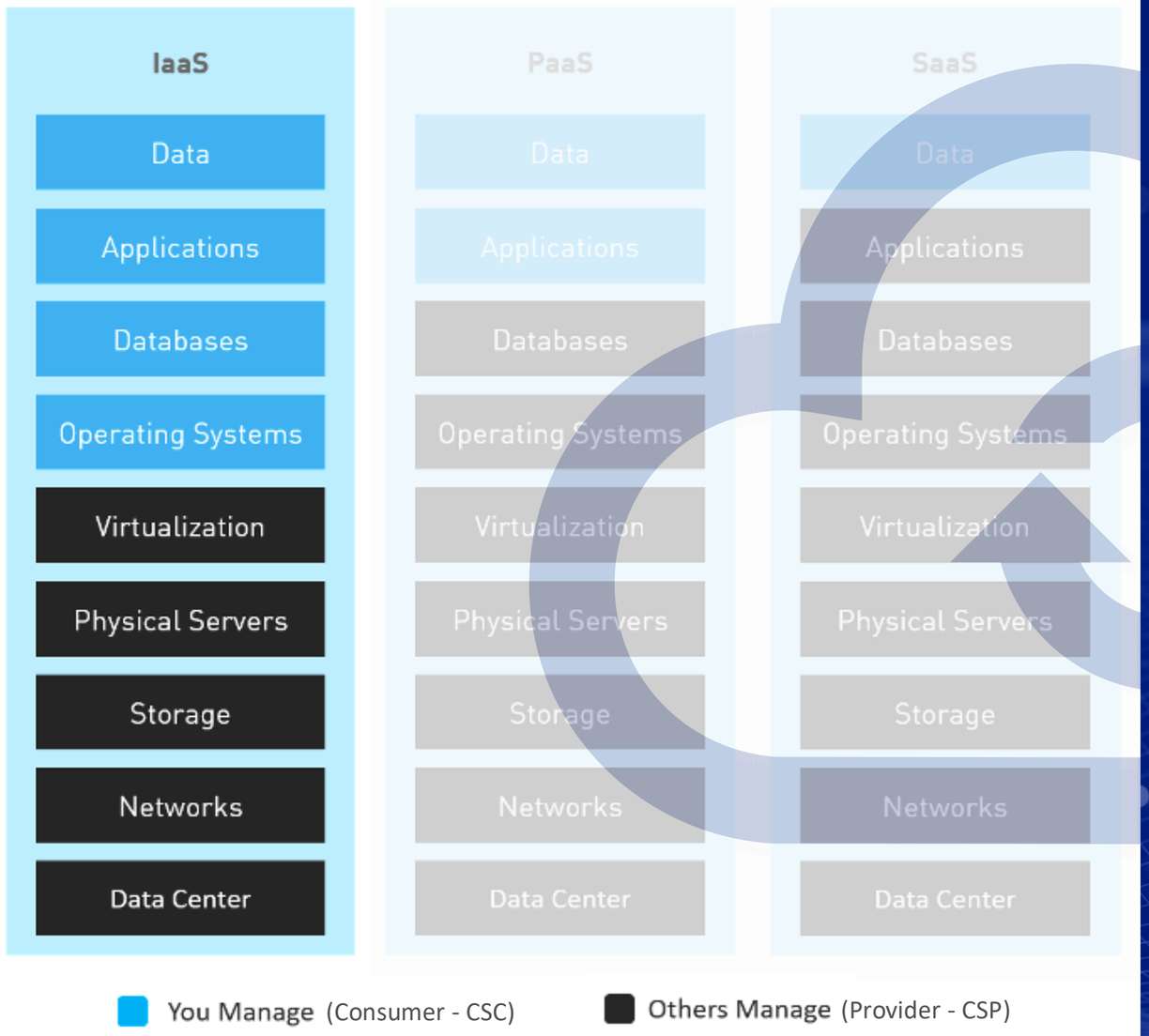
Fonte: ISO/IEC 22123-2:2023 - Information technology — Cloud computing — Part 2: Concepts

IaaS - Infrastructure as a service

Categoria di servizio cloud in cui al **Consumatore di Servizi Cloud** vengono fornite **capacità infrastrutturali fondamentali**, quali **calcolo, storage e rete**, su cui è possibile **distribuire ed eseguire software arbitrario**, inclusi **sistemi operativi e applicazioni**.

Il consumatore **non gestisce l'infrastruttura fisica sottostante**, ma mantiene il **controllo sui sistemi operativi, sullo storage e sulle applicazioni distribuite**, con **limitata capacità di configurazione di alcuni componenti di rete** (es. firewall host).

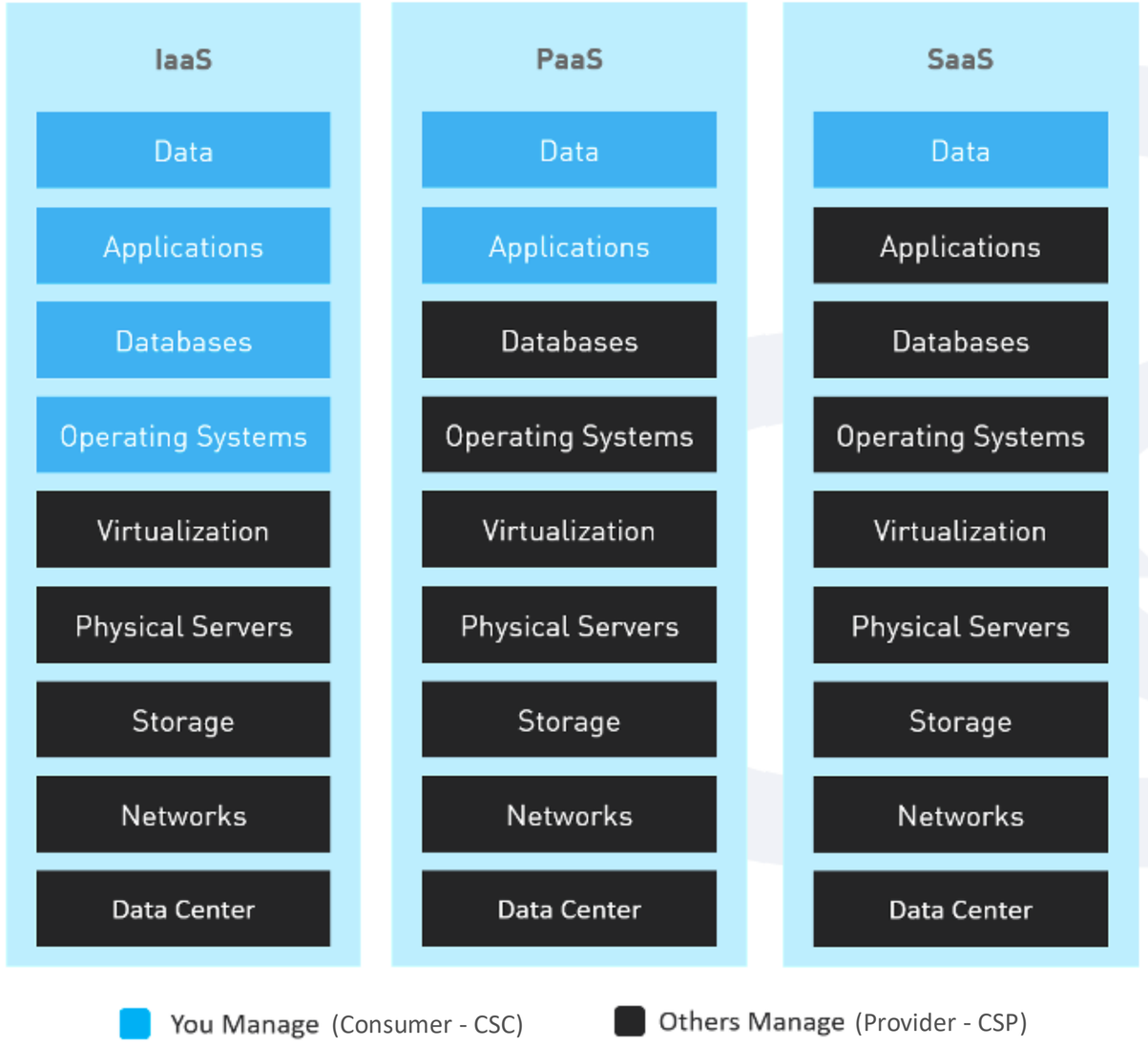
Il modello IaaS offre **massima flessibilità tecnologica** nella scelta del software, a fronte di una **maggiore responsabilità di gestione, manutenzione e sicurezza** delle componenti installate, nel rispetto dei **contratti e degli SLA** definiti con il provider.



Fonte: ISO/IEC 22123-2:2023 - Information technology — Cloud computing — Part 2: Concepts

Modello di shared responsability

Servizio	Responsabilità	
	Provider - CSP	Consumer - CSC
SaaS	Il **Cloud Service Provider (CSP)** è responsabile della **quasi totalità degli aspetti di sicurezza**, inclusi **sicurezza perimetrale**, **registrazione, monitoraggio e controllo**, nonché la **sicurezza delle applicazioni**.	Il **Consumatore del servizio** mantiene un **ruolo limitato**, focalizzato principalmente sulla **gestione delle autorizzazioni**, dei **diritti di accesso** e delle **configurazioni utente**.
PaaS	Il **Cloud Service Provider (CSP)** è responsabile della **sicurezza della piattaforma**, inclusi **patching**, **configurazione di base** e protezione dei **servizi gestiti** (es. database come servizio).	Il **Consumatore del servizio** è responsabile di **tutto ciò che viene implementato sulla piattaforma**, comprese la **configurazione delle funzionalità di sicurezza offerte**, la **gestione degli account**, le **politiche di accesso** e i **meccanismi di autenticazione** utilizzati.
IaaS	Il **Cloud Service Provider (CSP)** è responsabile della **sicurezza di base dell'infrastruttura**, inclusa la **protezione perimetrale** e il **monitoraggio degli attacchi** sull'ambiente fisico e virtualizzato.	Il **Consumatore del servizio** è **pienamente responsabile della sicurezza di tutto ciò che costruisce sull'infrastruttura**, inclusa la **progettazione e configurazione della rete virtuale**, l'uso corretto degli **strumenti di sicurezza messi a disposizione dal servizio**, e la **protezione dei sistemi operativi e delle applicazioni**.



Fonte: ISO/IEC 22123-2:2023 - Information technology — Cloud computing — Part 2: Concepts

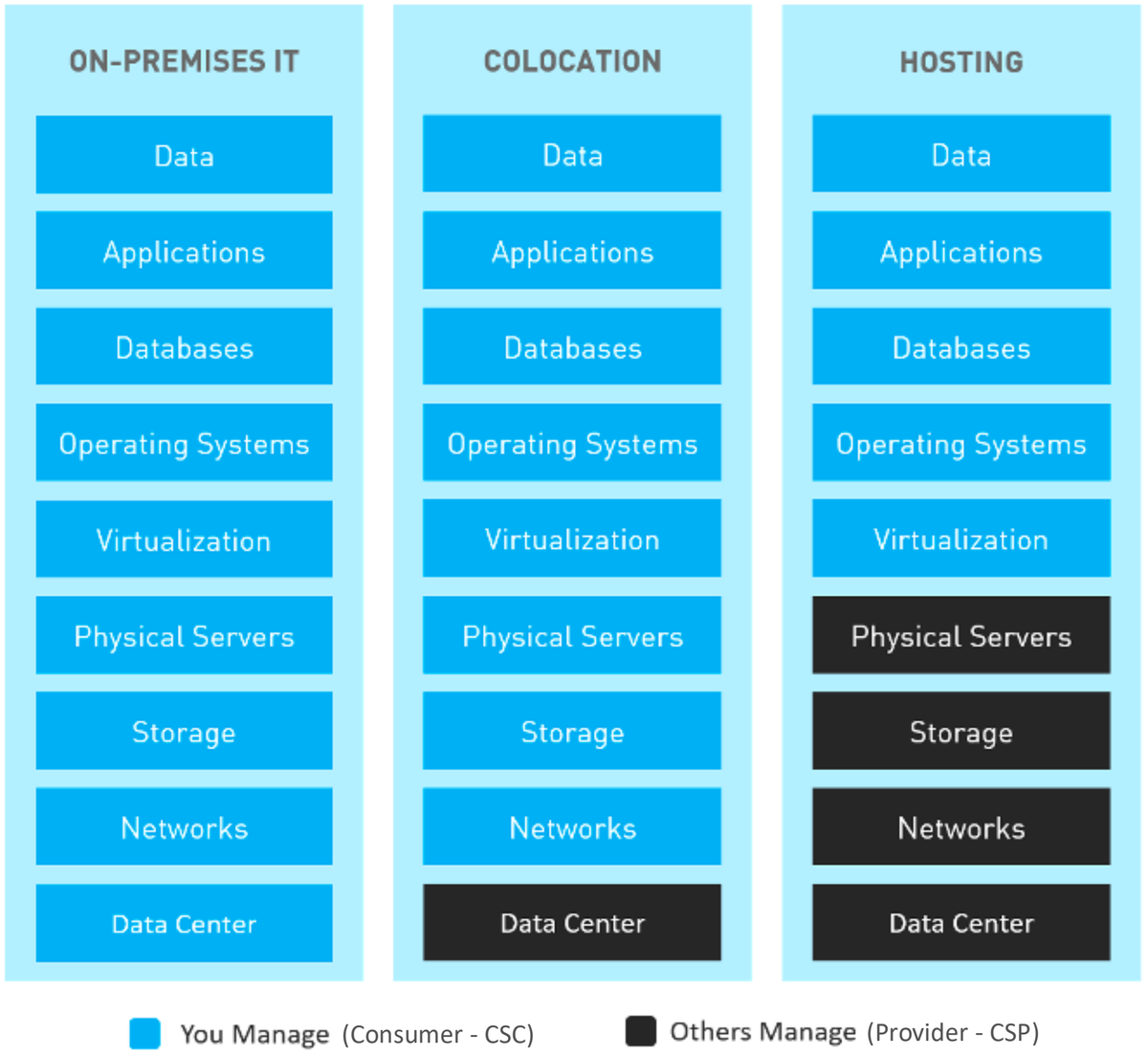
Hosting

Il cloud hosting consiste nell'**accesso on-demand e da remoto a risorse di calcolo online**, ospitate in un **data center interamente gestito da un Cloud Service Provider (CSP)**.
Il provider è responsabile dell'infrastruttura e dei servizi di base, mentre il cliente utilizza le risorse secondo modelli di servizio e contratti definiti.

Co-location

La **co-location** si riferisce all'utilizzo di un **data center condiviso**, in cui le organizzazioni **affittano spazio (rack o cage)**all'interno di una struttura di proprietà di terzi.
Il fornitore mette a disposizione **alimentazione, connettività, raffreddamento e sicurezza fisica**, ma **non fornisce servizi cloud o infrastrutture virtualizzate**: l'hardware e la sua gestione restano interamente sotto il controllo del cliente.

Hosting e Co-location

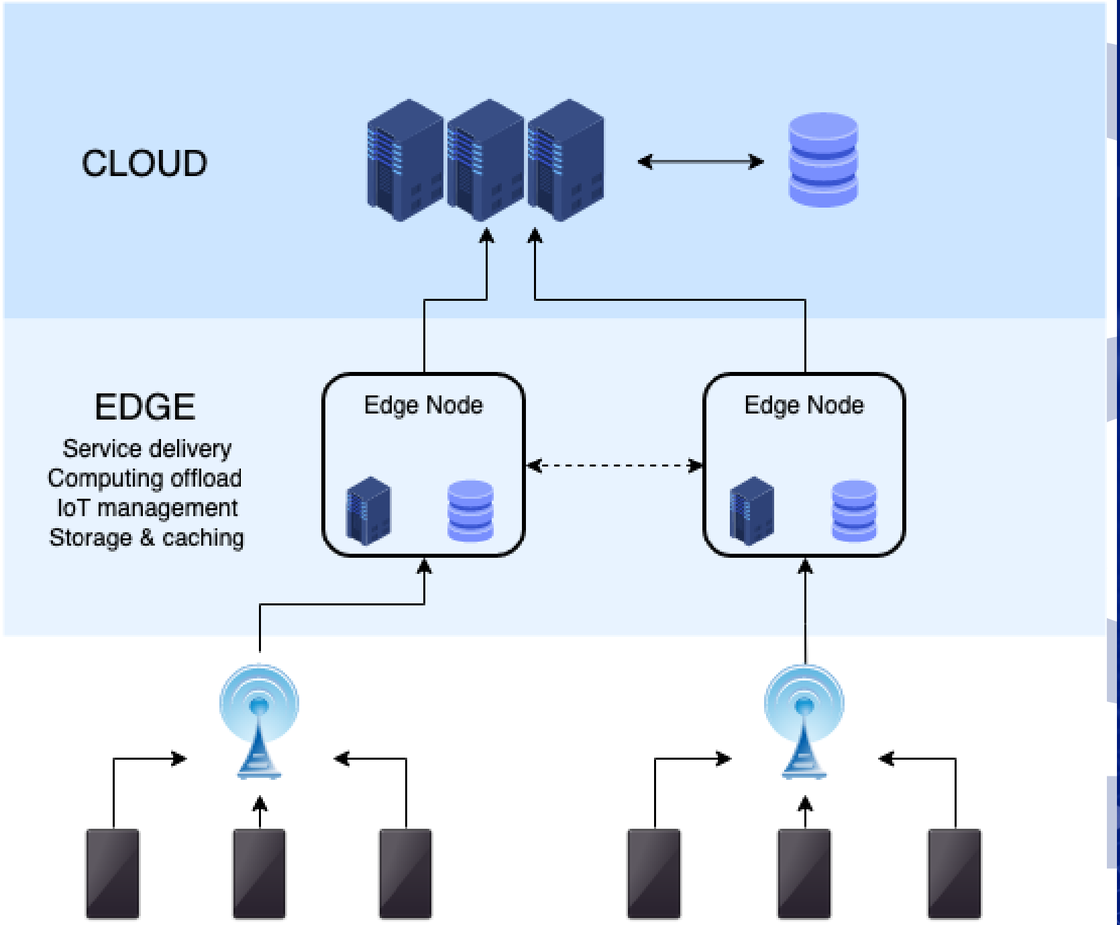


Fonte: ISO/IEC 22123-2:2023 - Information technology — Cloud computing — Part 2: Concepts

Edge Computing

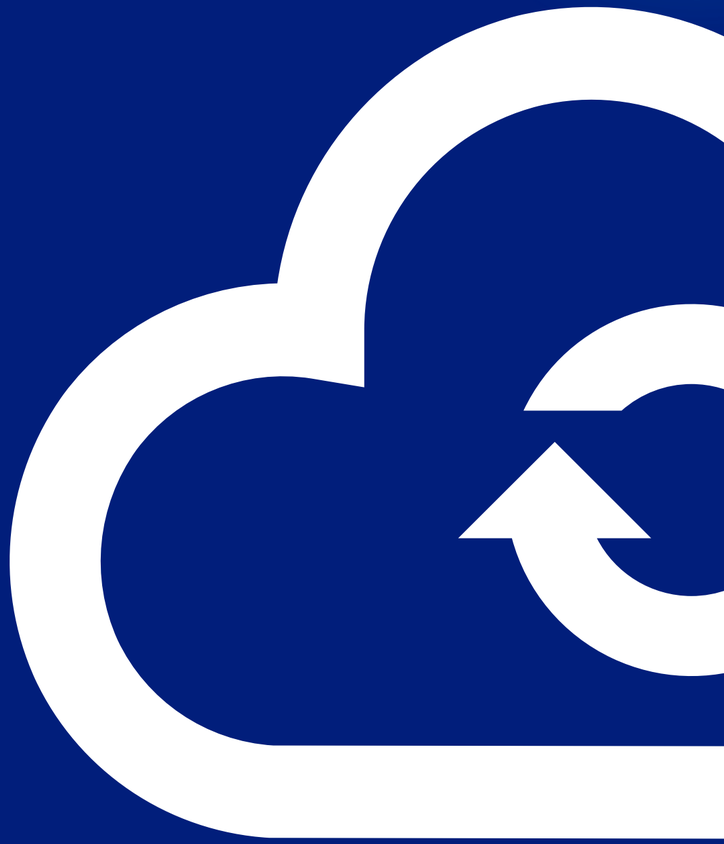
Modello di **computazione distribuita** che **sposta elaborazione e storage dei dati vicino alla loro sorgente**, riducendo la dipendenza dal cloud centralizzato.
Si integra nell'**architettura dei sistemi cloud** ed è utilizzato principalmente per **scenari che richiedono bassa latenza, continuità operativa e trattamento locale dei dati**, come **IoT, smart city, sanità, video analytics e applicazioni di intelligenza artificiale in tempo reale**.
Offre numerosi vantaggi:

- **Privacy e sicurezza** → i dati vengono elaborati localmente e si muovono meno
- **Affidabilità** → **ridondanza dei nodi** e maggiore resilienza del sistema
- **Velocità** → **computazione prossima al terminale**, con riduzione della latenza e migliore utilizzo della banda
- **Efficienza** → **livello intermedio tra cloud centrale e terminali**, che riduce il carico e l'utilizzo delle risorse dei data center



Wikipedia, https://en.wikipedia.org/wiki/Edge_computing

La Strategia Cloud Italia e il contesto normativo nazionale



La Strategia Cloud Italia

CONTESTO ED OBIETTIVI

Tre sfide principali:

- assicurare l'**autonomia tecnologica** del Paese,
- garantire il **controllo sui dati**,
- aumentare la **resilienza dei servizi digitali**.

Obiettivo:
75% delle PA italiane in cloud qualificato

AGID Agenzia per l'Italia Digitale

Consolidamento datacenter della PA
Il censimento AgID del 2019, su 1252 DC censiti, solo 62 avevano requisiti adeguati

FATTORI ABILITANTI

Italiadomani
PIANO NAZIONALE DI RIPRESA E RESILIENZA

INTERVENTO 1.1

Valore: 900 M€
PSN e relativa migrazione di 280 PAC/ASL

INTERVENTO 1.2

Valore: 1000 M€
Migrazione di 12.464 PAL a servizi cloud qualificati

ALTRI INTERVENTI

Progettualità settoriali, con particolare riferimento all'**ambito sanitario**, ad es. **Fascicolo Sanitario Elettronico**

Le linee di indirizzo strategiche

Classificazione di dati e servizi

- ➔ Guida le PA nella scelta della soluzione cloud più adeguata.
- ➔ Valuta il **danno che una loro compromissione può provocare al Paese**.

Qualificazione dei servizi cloud

- ➔ **Semplifica e regolamenta l'acquisizione di servizi cloud da parte delle PA,**
  dal punto di vista tecnico (ad es. gestione operativa, sicurezza) e amministrativo (ad es. condizioni contrattuali).

Polo Strategico Nazionale (PSN)

- ➔ Garantisce **continuità operativa e tolleranza ai guasti** per i servizi strategici e critici della PA.
- ➔ Distribuito su territorio nazionale, il controllo e le linee di indirizzo sono
  pubbliche e indipendenti da soggetti terzi.
- ➔ La gestione operativa è affidata a un fornitore selezionato mediante **partenariato pubblico-privato e gara UE.**

Dal censimento AgID del 2019, su 1252 Data Center censiti, solo 62 avevano requisiti adeguati.

La qualificazione dei servizi cloud

CLASSIFICAZIONE SERVIZI CLOUD

CARATTERISTICHE

REQUISITI DI SICUREZZA

LOCALIZZAZIONE DEI DATI

GESTIONE OPERATIVA

CLASSIFICAZIONE SERVIZI CLOUD	CARATTERISTICHE	REQUISITI DI SICUREZZA	LOCALIZZAZIONE DEI DATI	GESTIONE OPERATIVA
PUBBLICO NON QUALIFICATO (EXTRA UE / UE)	Servizi di Cloud pubblico non qualificati rispetto alle normative UE		Extra UE UE	CSP non qualificati
CLOUD QUALIFICATO				
PUBBLICO (UE)	Servizi di Cloud pubblico qualificati rispetto alle normative UE	Controlli di sicurezza ordinari	UE	CSP qualificati
PUBBLICO CRIPTATO (IT)	Servizi di Cloud pubblico qualificati con gestione delle chiavi in Italia	Criptografia con controllo delle chiavi in Italia		
PRIVATO/IBRIDO "SU LICENZA" (IT)	Servizi di Cloud privato e ibrido qualificati con gestione delle chiavi in Italia		Italia	Fornitori soggetti a vigilanza e monitoraggio pubblico
PRIVATO (IT)	Servizi di Cloud privato qualificati mediante scrutinio tecnologico	Criptografia nazionale con controllo delle chiavi in Italia		

Normativa di riferimento

DL 18 ottobre 2012, n. 179

Art. 33–septies *(Consolidamento e razionalizzazione dei siti e delle infrastrutture digitali del Paese)*

INFRASTRUTTURE PER LA PA

Promozione dello sviluppo di un'**infrastruttura ad alta affidabilità** localizzata sul territorio nazionale per la razionalizzazione e il consolidamento dei CED, al fine di tutelare l'autonomia tecnologica del Paese e mettere in sicurezza le infrastrutture digitali delle PA

Per le **amministrazioni centrali e locali**, obbligo di migrazione dei CED e dei relativi sistemi informativi, privi dei requisiti minimi, verso:

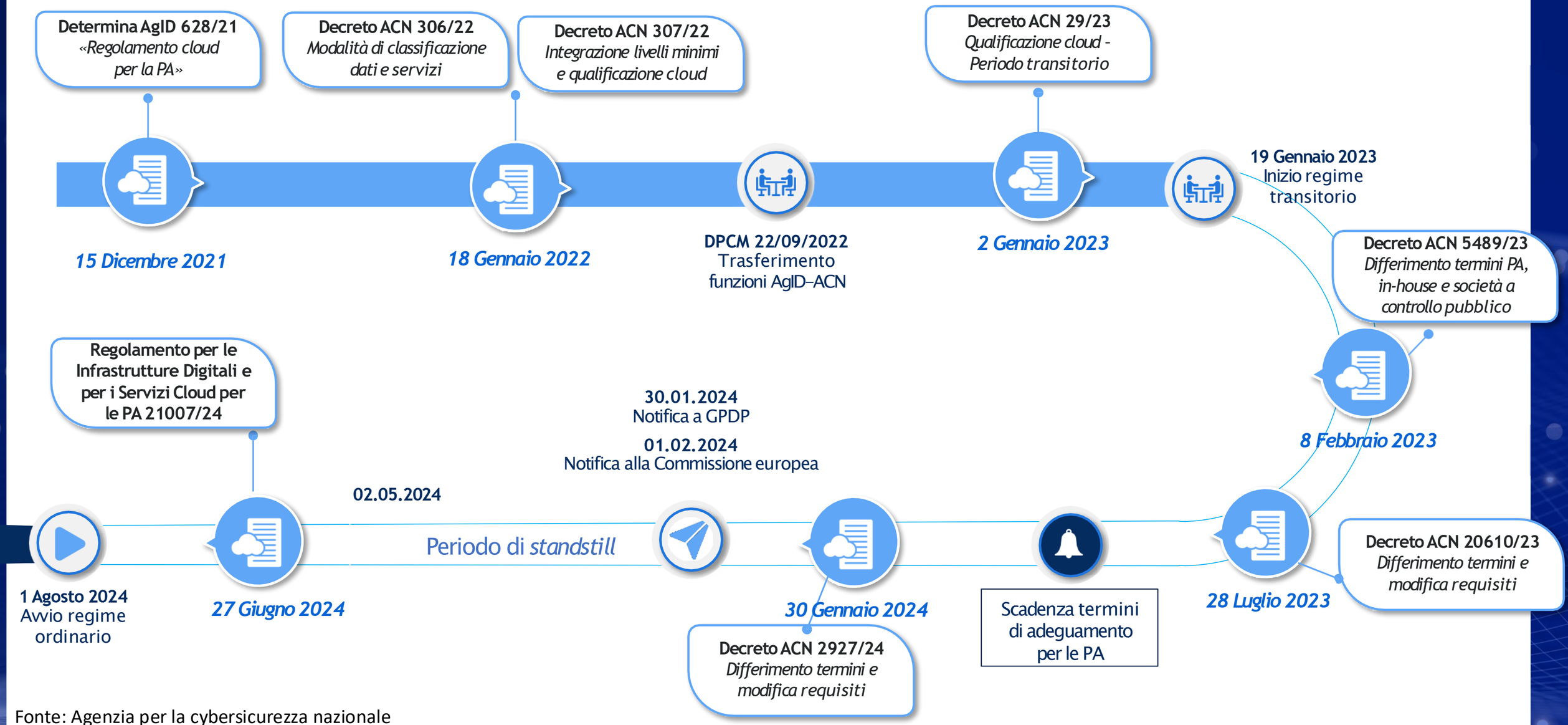
- l'infrastruttura di cui al primo punto
- altra infrastruttura propria già esistente e in possesso dei requisiti minimi
- soluzioni cloud qualificate

COMPITI ACN e AgID

- Definizione dei **livelli minimi** di sicurezza, capacità elaborativa, risparmio energetico e affidabilità delle **infrastrutture digitali** per la PA
- Definizione delle **caratteristiche** di qualità, di sicurezza, di performance e scalabilità, interoperabilità, portabilità dei **servizi cloud** per la PA
- Individuazione dei termini e delle modalità di **migrazione**
- Individuazione delle modalità del procedimento di **qualificazione** dei servizi cloud per la PA

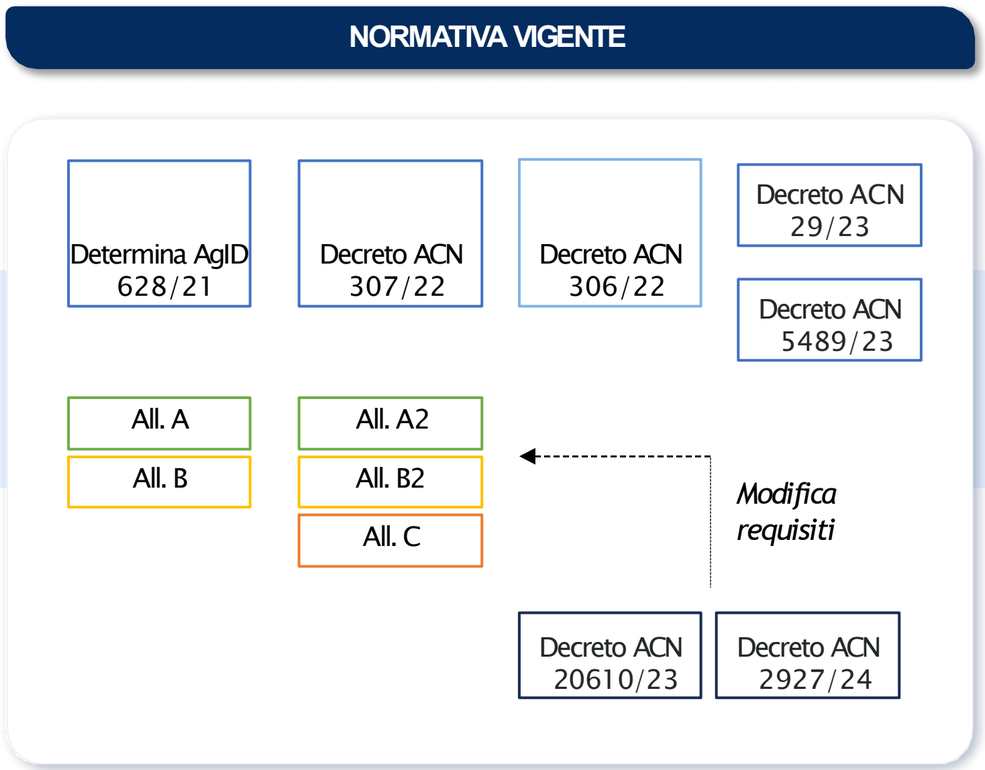
- **Censimento** dei CED della PA con cadenza triennale
- Definizione – nel Piano triennale per l'informatica nella PA – della **strategia di sviluppo** delle infrastrutture digitali delle amministrazioni
- Definizione della **strategia di adozione del modello cloud** per la PA, alle quali le amministrazioni si attengono
- Accertamento **violazioni**

Evoluzione normativa



Fonte: Agenzia per la cybersicurezza nazionale

Il Regolamento Cloud



Testo del Regolamento

Allegato 1
*Modalità per la predisposizione dell'elenco e della **classificazione dei dati e dei servizi** della PA*

Allegato 2
***Livelli minimi** di sicurezza e affidabilità, capacità elaborativa, risparmio energetico delle **infrastrutture digitali** e delle infrastrutture dei servizi per la PA*

Allegato 3
***Caratteristiche di base** di qualità, di sicurezza, di performance e di scalabilità, di interoperabilità, di portabilità dei **servizi cloud** per la PA*

Allegato 4
***Requisiti per l'adeguamento e la qualificazione** delle infrastrutture digitali, infrastrutture dei servizi cloud e dei servizi cloud per la PA*

Rispetto ai decreti attualmente in vigore, nell'Allegato 4 sono stati spostati i requisiti ad oggi previsti negli allegati A/A2, B/B2 che si applicano solo ad operatori pubblici o privati, per evitare così di ambiguità

Macro-processo

Qualificazione delle infrastrutture e dei servizi cloud

Livelli minimi di sicurezza e affidabilità, capacità elaborativa, risparmio energetico delle **infrastrutture digitali per la PA**

Caratteristiche di qualità, sicurezza, performance e scalabilità, interoperabilità e portabilità dei **servizi cloud per la PA**

Requisiti da rispettare, coerentemente con livello di criticità

Migrazione

Classificazione dei dati e dei servizi per la PA

Elenco dei servizi e dei dati classificati, secondo il proprio livello di criticità

Adeguamento delle infrastrutture e dei servizi da parte delle **PA, in-house** o **società a controllo pubblico**, che erogano servizi alla PA per espressa previsione normativa

Dichiarazione di conformità entro il 18 gennaio 2024

Classificazione dati e servizi per la PA

Classificazione dei dati e servizi della P.A. di dati e servizi la cui compromissione:

NON provochi interruzione servizi dello Stato o un pregiudizio per il benessere economico e sociale	**ORDINARI**
rechi pregiudizio al mantenimento di funzioni rilevanti per la società, la salute, la sicurezza e il benessere economico e sociale	**CRITICI**
causi impatti sulla sicurezza nazionale	**STRATEGICI**

Aggiornamento **almeno una volta ogni due anni o in presenza dei dati e dei servizi digitali ulteriori rispetto a quelli già oggetto di trasmissione e classificazione**

CLASSIFICAZIONE PREDEFINITA

Dati e servizi inclusi nel Perimetro di sicurezza nazionale cibernetica	**STRATEGICI**	
Dati e servizi degli Operatori di Servizi Essenziali (NIS)	**CRITICI**	**STRATEGICI** se valenza nazionale

DEROGA

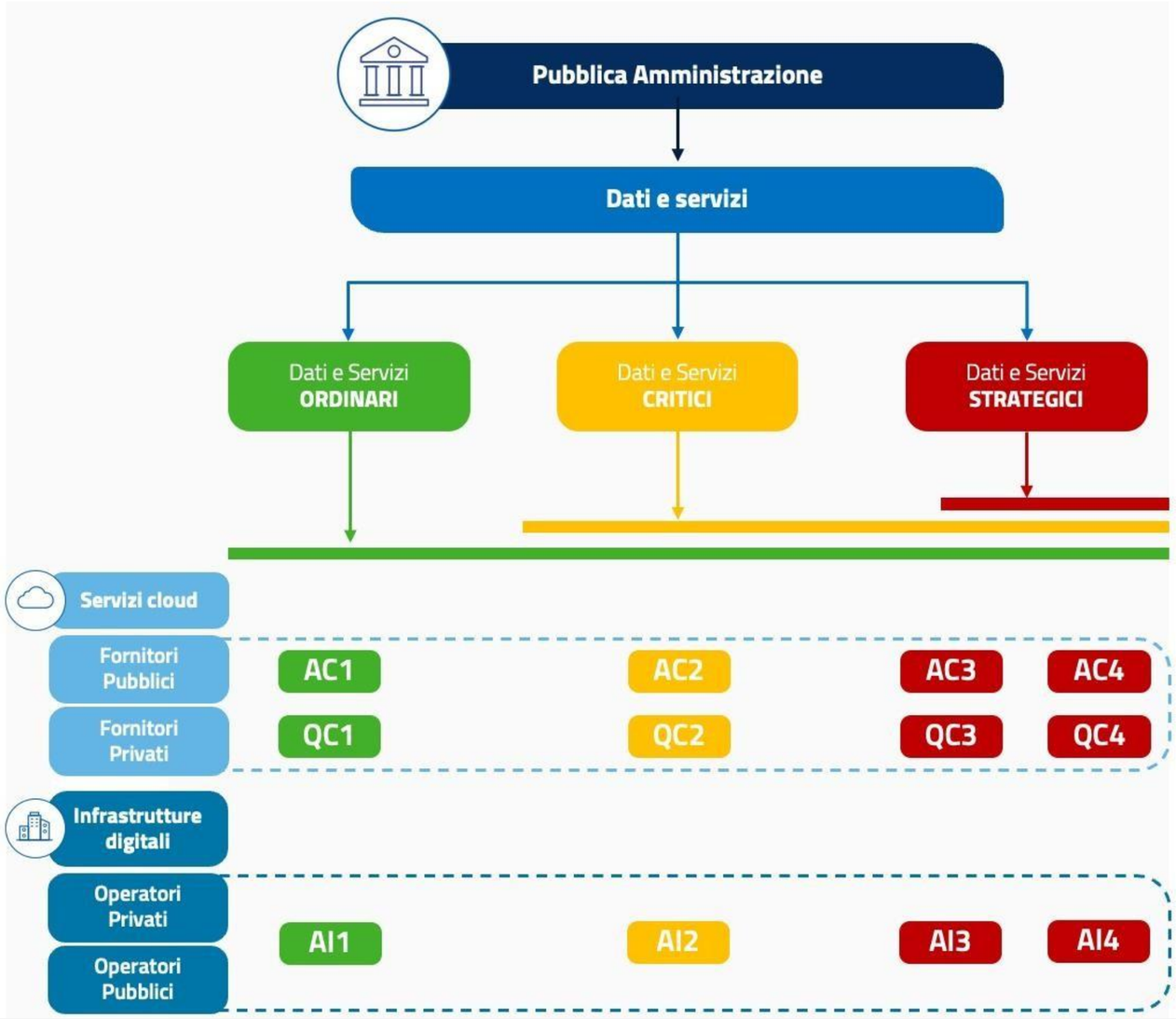
Casi di deroga alla migrazione dei dati su cloud (art. 33-septies, comma 4-bis, DL 179/2012):

- Ordine e sicurezza pubblici
- Polizia giudiziaria
- Difesa e sicurezza nazionale (infrastrutture digitali dell'amministrazione della difesa)

Esempio di classificazione dati e servizi per la PA

Livello di sicurezza	Descrizione	Esempi (dati e servizi)	Tipo di cloud
Ordinario	Dati e servizi la cui compromissione non comporta impatti significativi su diritti fondamentali, sicurezza nazionale o continuità dei servizi pubblici.	• Siti web informativi • Portali open data • Contenuti istituzionali pubblici • Newsletter • Ambienti di test senza dati reali	Cloud pubblico qualificato (anche extra-UE, se conforme ai requisiti minimi)
Critico	Dati e servizi il cui incidente può generare impatti rilevanti su cittadini, continuità operativa della PA o affidabilità dei servizi pubblici.	• Dati personali (GDPR) • Protocollo informatico • Gestione documentale • Servizi digitali al cittadino • Sistemi contabili e HR	Cloud qualificato ACN con localizzazione UE e misure di sicurezza rafforzate
Strategico	Dati e servizi la cui compromissione può produrre impatti gravi o sistemici su sicurezza nazionale, ordine pubblico o funzioni essenziali dello Stato.	• Dati di sicurezza nazionale • Sistemi di emergenza • Infrastrutture critiche • Servizi core di PA centrali • Sistemi di identità e autenticazione strategici	Cloud strategico con sovranità nazionale e controllo diretto dello Stato

Qualificazione di infrastrutture e servizi cloud



Requisiti di conformità

Caratteristiche di base per i servizi cloud

- Qualità
- Performance e scalabilità
- Interoperabilità e portabilità
- Sicurezza

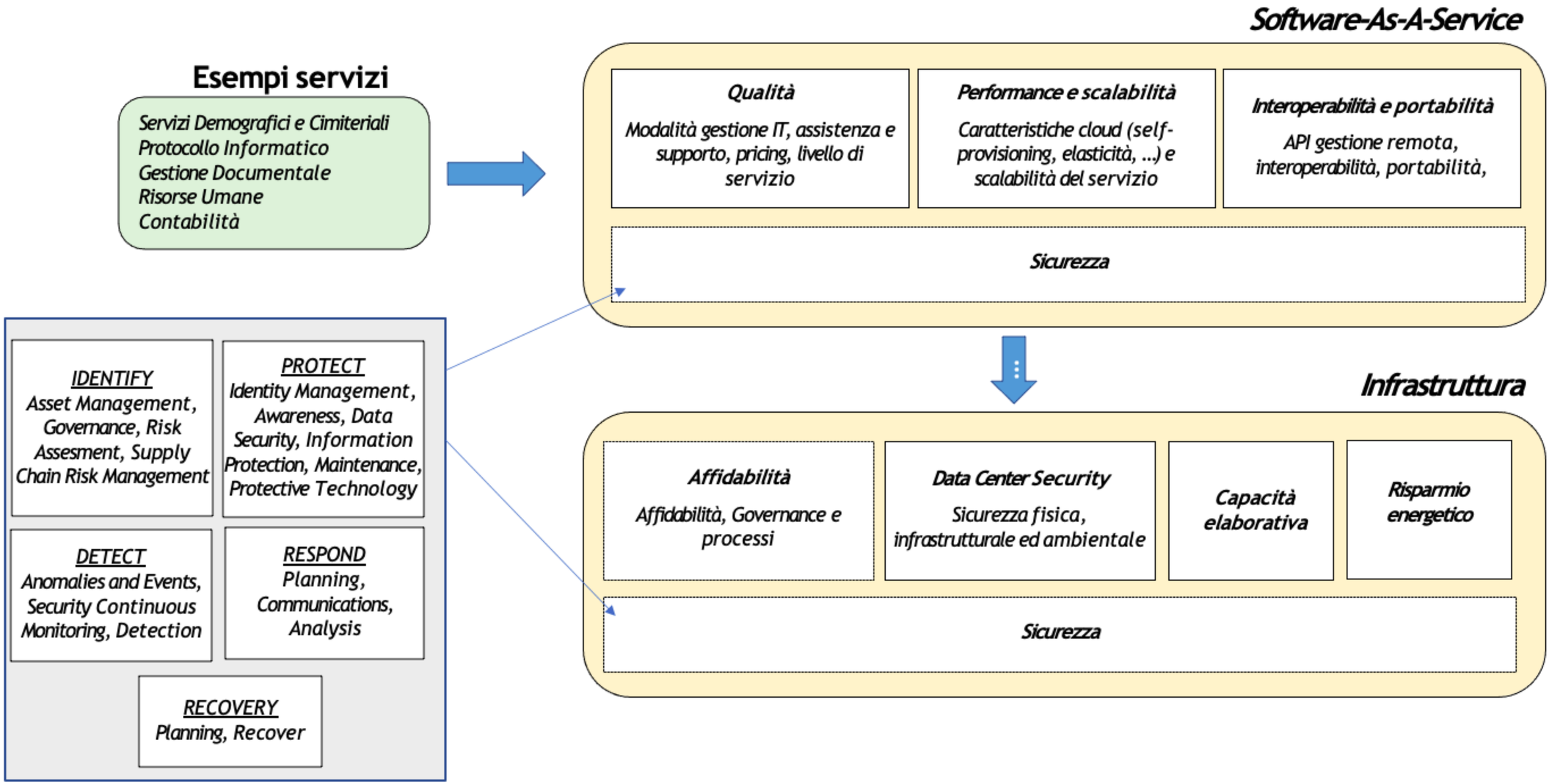
Livelli minimi per le infrastrutture digitali

- Affidabilità
- Datacenter Security
- Capacità elaborativa
- Risparmio energetico
- Sicurezza

Misure derivate da:
- Framework Nazionale per la Cybersecurity e la Data Protection
- Norme e best practice internazionali

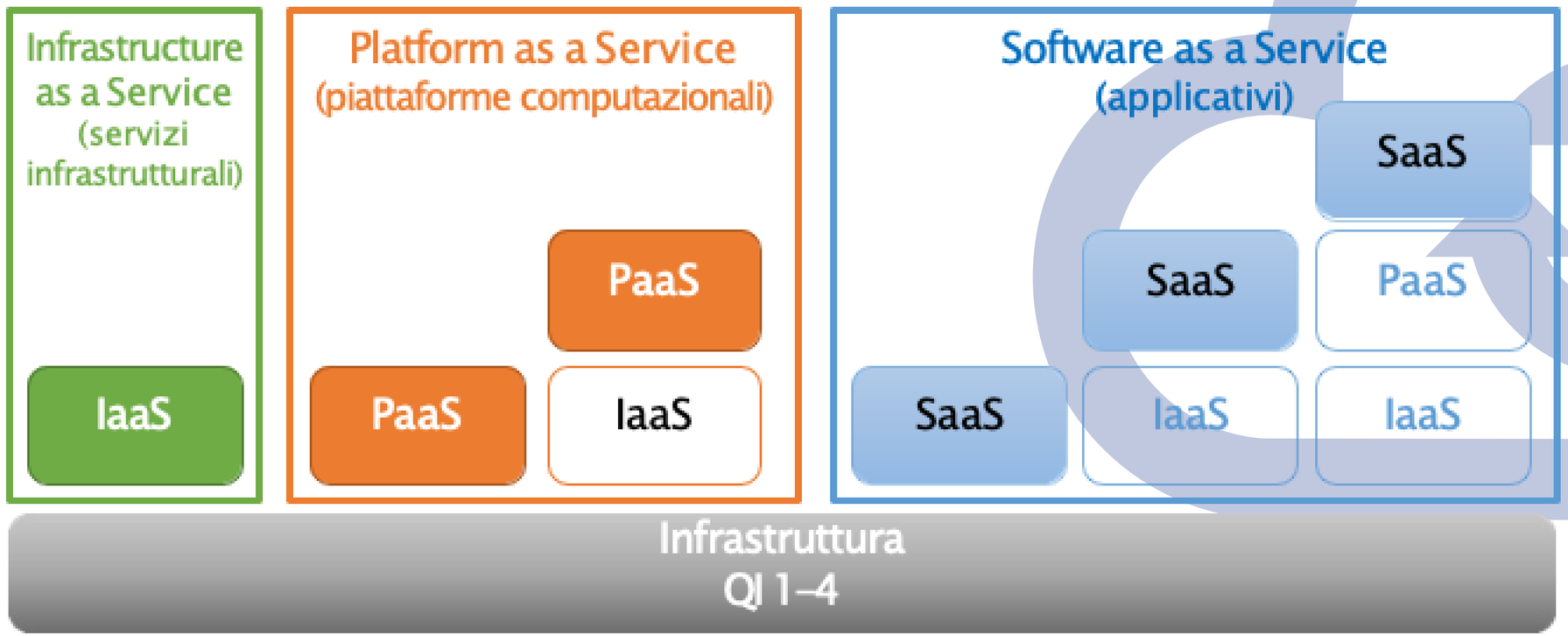
Fonte: Agenzia per la cybersicurezza nazionale

Qualificazione di infrastrutture e servizi cloud

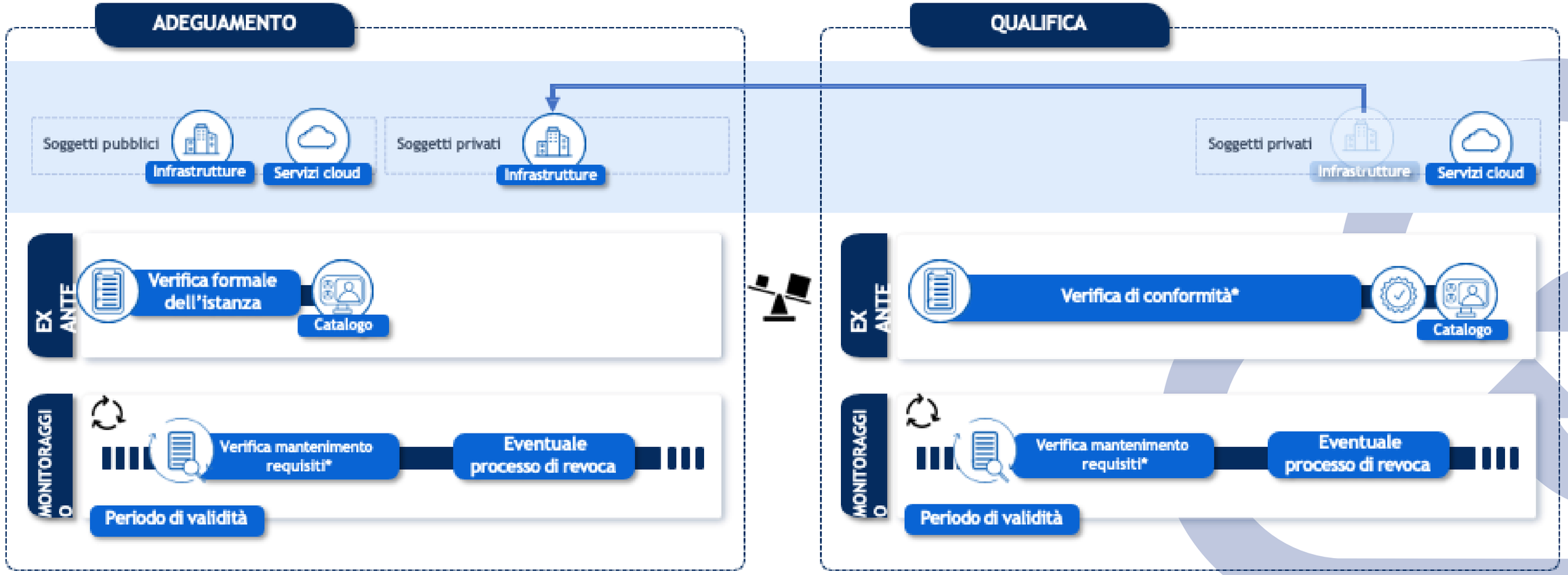


CATENA DI QUALIFICAZIONE

Un servizio (IaaS, PaaS, Saas) è erogato, in ultima istanza, da un'infrastruttura fisica Per poter qualificare un servizio ad un certo livello, **tutti gli strati sottostanti devono avere almeno pari livello di qualifica.**



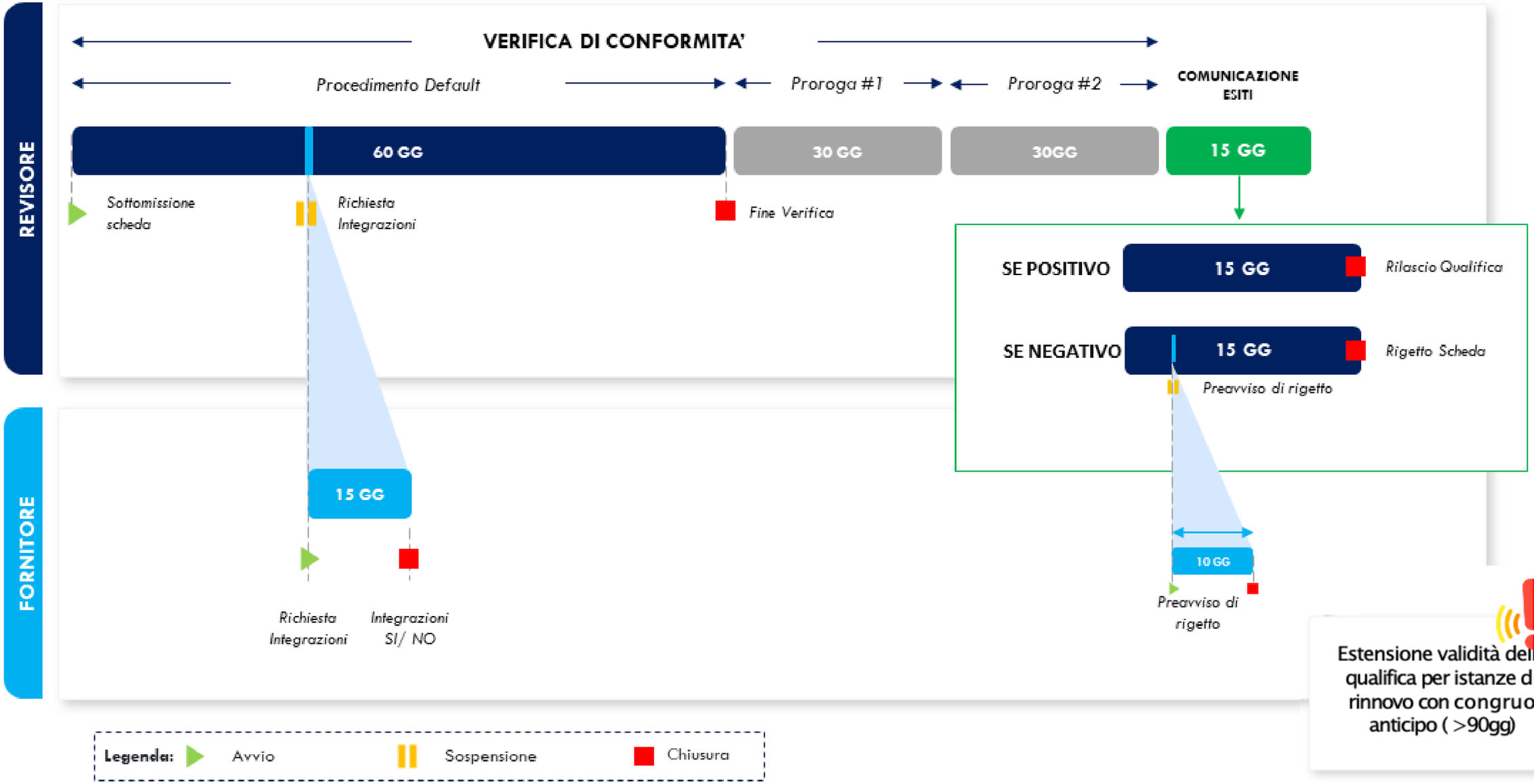
Processi di adeguamento e qualifica



***Nell'ambito delle verifiche, ACN può**

- *Formulare quesiti*
- *Richiedere integrazioni, informazioni aggiuntive e la produzione di ulteriore documentazione*
- Effettuare **accertamenti di carattere tecnico**, incluse le verifiche di sicurezza mirate ad accertare la presenza di vulnerabilità nei sistemi, anche mediante **accesso all'infrastruttura fisica e logica** dell'infrastruttura dei servizi cloud ovvero del servizio cloud
- *Audire il soggetto richiedente.*

Qualifica di servizi cloud



Estensione validità della qualifica per istanze di rinnovo con congruo anticipo (>90gg)

Fonte: Agenzia per la cybersicurezza nazionale

Considerazioni su tipologia servizi e misure

INFRASTRUTTURE DIGITALI

Infrastrutture digitali per le PA tramite le quali sono erogati i servizi digitali della PA

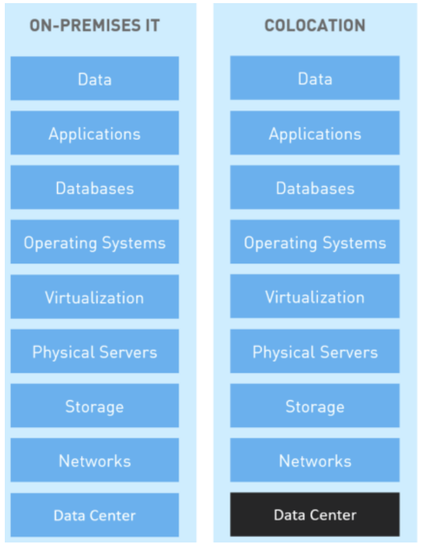
Infrastrutture dei servizi cloud per le PA, infrastrutture digitali tramite le quali sono erogati i servizi cloud per la PA

Centro Elaborazione Dati (CED)

Infrastruttura di housing

Infrastruttura di prossimità

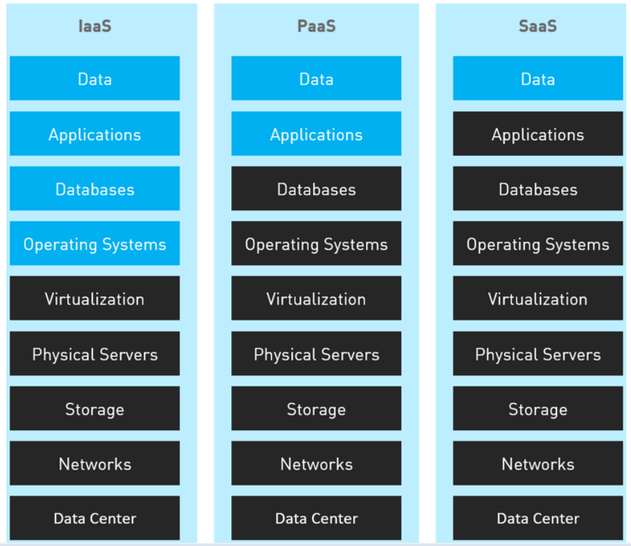
Nuove categorie introdotte dal Regolamento



Esempio

01/02/2025

SERVIZI CLOUD



Esempio

Infrastructure as-a-Service (Iaas)

Platform as-a-Service (Paas)

Software as-a-Service (Saas)

Servizi di prossimità (edge)

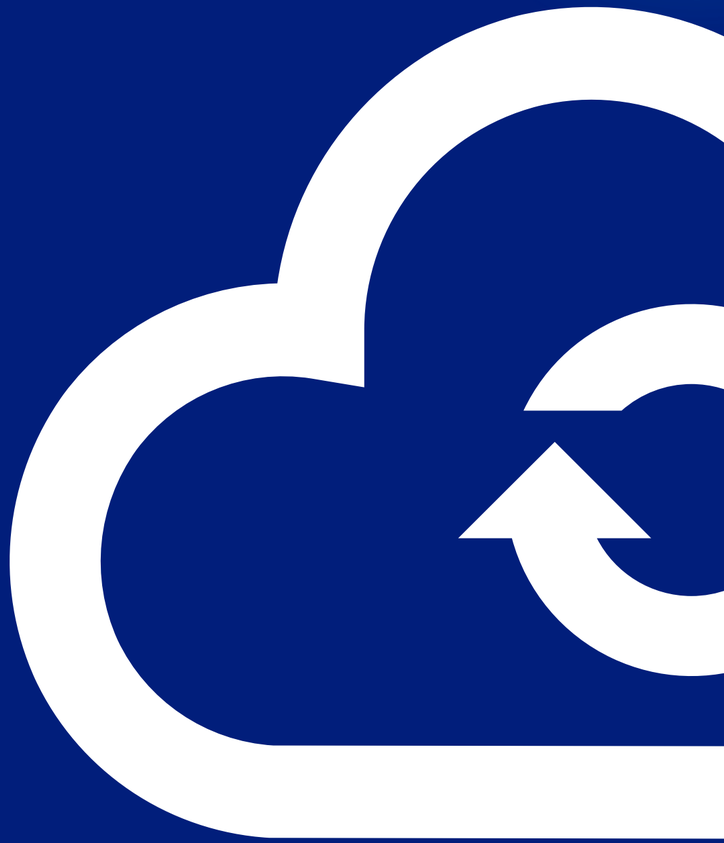
Nuova categoria introdotte dal Regolamento

Amministrazione

CSP

Fonte: Agenzia per la cybersicurezza nazionale

Polo Strategico Nazionale



Polo Strategico Nazionale

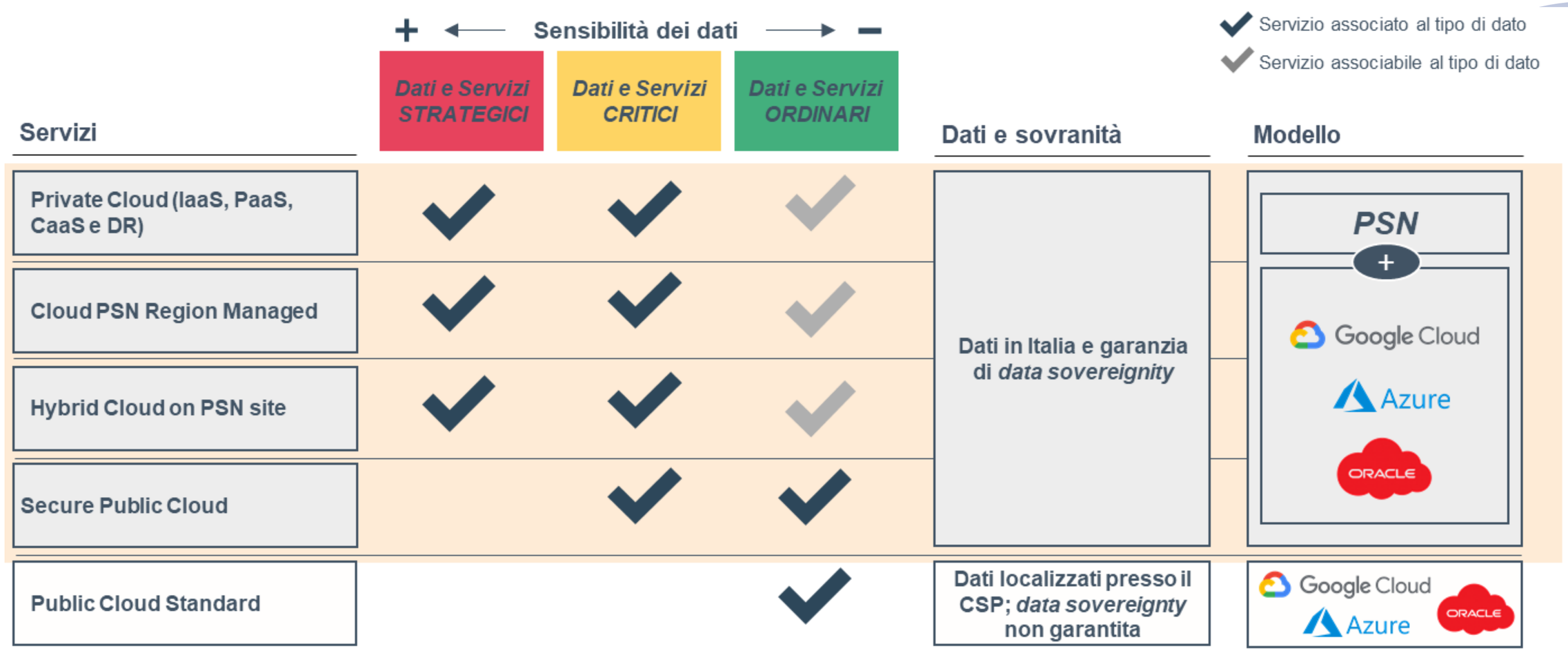
Il PSN è una infrastruttura digitale a servizio della PA italiana, che la dota di tecnologie e infrastrutture cloud affidabili, resilienti e indipendenti.

Conforme ai requisiti di sicurezza PSNC e NIS e al Regolamento Cloud,
abilita la migrazione inizialmente con un processo *lift-and-shift*, verso tipologie di servizi cloud IaaS e PaaS.

Offre servizi di cloud privato qualificato, permette di gestire strumenti di cifratura *on-premise* integrati su cloud pubblico qualificato per la PA, oltre che cloud ibrido su licenza.

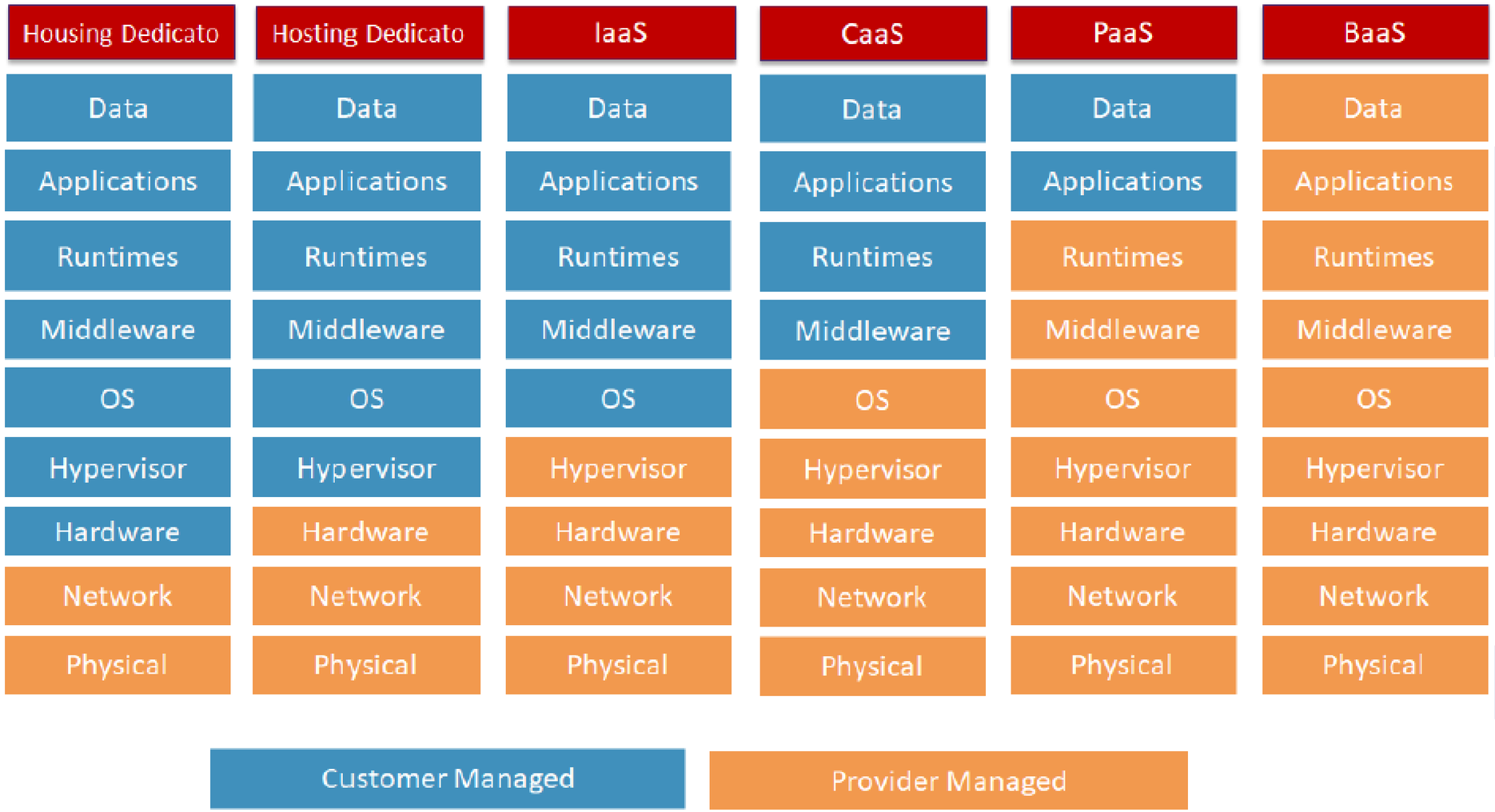
Rivolto prioritariamente alle PA che gestiscono dati e servizi strategici e critici

Caratteristiche dei servizi



Fonte: Polo Strategico Nazionale

Caratteristiche dei servizi

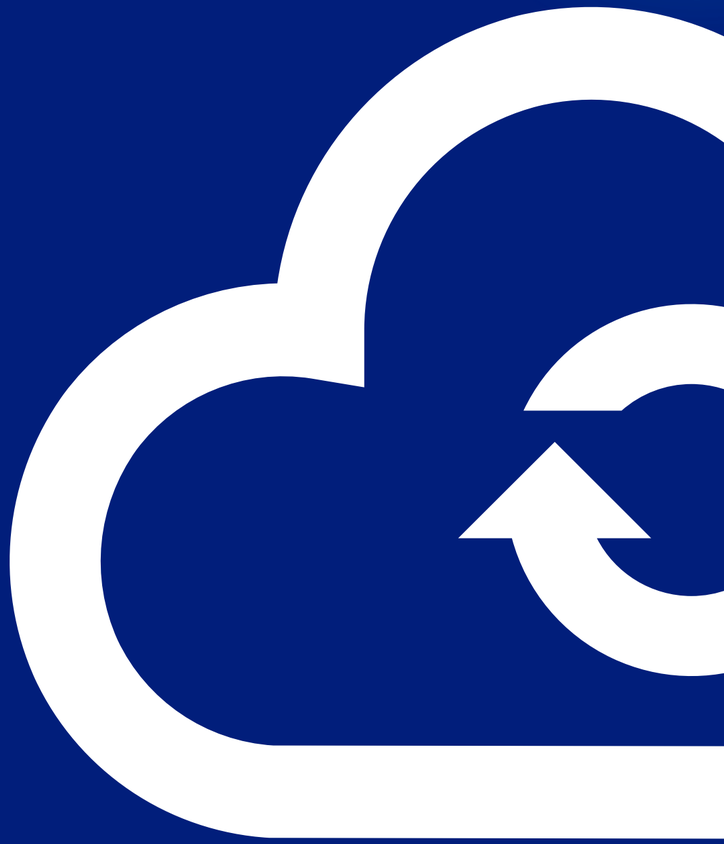


Fonte: Polo Strategico Nazionale

CAAS: Container As A Service

BAAS: Back-up As A Service

Sovranità Digitale



I principi della sovranità digitale per un ecosistema tecnologico sicuro e autonomo

Controllo sulle infrastrutture critiche. Garantire che dati, piattaforme e servizi essenziali siano gestiti in modo affidabile e sotto governance nazionale ed europea.

Sicurezza e resilienza dei sistemi. Proteggere reti, applicazioni e identità digitali da minacce esterne rafforzando capacità difensive e standard comuni.

Autonomia tecnologica e capacità locali. Sviluppare competenze, infrastrutture e soluzioni europee per ridurre dipendenze critiche da provider extra-UE.

Conformità e fiducia nelle tecnologie. Assicurare che algoritmi e piattaforme rispettino standard, regole e valori europei a tutela dei diritti fondamentali.

Sicurezza – Autonomia – Fiducia – Innovazione

Cloud Sovereignty Framework - Version 1.2.1 – Oct. 2025

#	Obiettivo	Descrizione
SOV-1	Sovranità strategica	La sovranità strategica misura il **grado in cui i servizi di un provider cloud (o attore tecnologico) sono ancorati all'ecosistema legale, finanziario e industriale dell'Unione Europea.** Valuta la stabilità della proprietà, l'influenza sulla governance e l'**allineamento con le priorità strategiche dell'UE**.
SOV-2	Sovranità legale e giurisdizionale	La sovranità legale e giurisdizionale valuta il contesto normativo, l'**esposizione ad autorità straniere** e la **possibilità effettiva di far valere i diritti** che regolano i servizi di un fornitore tecnologico. Determina quanto tali servizi siano **ancorati alla giurisdizione europea** e protetti da rivendicazioni legali esterne.
SOV-3	Sovranità dei dati e dell'IA	La sovranità dei dati e dell'IA si concentra sulla **protezione, il controllo e l'indipendenza dei dati** e dei **servizi di intelligenza artificiale** all'interno dell'UE. Considera come i dati vengono protetti, dove vengono trattati e il **livello di autonomia che i clienti mantengono sulle capacità di IA.**
SOV-4	Sovranità Operativa	La **sovranità operativa** misura la capacità pratica degli attori europei di gestire, **supportare e sviluppare una tecnologia in modo indipendente da controlli stranieri**. Si focalizza sulla continuità operativa, sulla disponibilità di competenze e sulla resilienza rispetto a dipendenze esterne.
SOV-5	Sovranità della catena di fornitura	La **sovranità della supply chain valuta l'origine geografica**, la trasparenza e la resilienza della catena di fornitura tecnologica, verificando **in che misura componenti e processi critici restano sotto controllo dell'UE o risultano dipendenti da attori extra-UE**.
SOV-6	Sovranità tecnologica	La **sovranità tecnologica misura il grado di apertura, trasparenza e indipendenza dello stack tecnologico sottostante**, assicurando che gli attori europei possano interoperare, verificare e far evolvere le soluzioni senza essere **vincolati da sistemi proprietari esteri**.
SOV-7	Sovranità della sicurezza e della conformità	La sovranità nella sicurezza e nella conformità misura quanto **le operazioni di sicurezza, gli obblighi normativi e le misure di resilienza siano controllati all'interno dell'UE**, garantendo **indipendenza dalle giurisdizioni straniere** e affidabilità operativa nel lungo periodo.
SOV-8	Sostenibilità ambientale	La sostenibilità ambientale valuta **l'autonomia e la resilienza dei servizi cloud nel lungo periodo** in relazione al **consumo energetico, alla dipendenza da risorse critiche e alla scarsità di materie prime**.

Progetto «Progetto formativo CIVITAS - Competenze Innovative per Valorizzare l'Innovazione Territoriale Amministrativa Strategica.»
PON GOVERNANCE E CAPACITA' ISTITUZIONALE 2014-2020

GRAZIE

Ing. Fabio Massimi

26 Gennaio 2026
Università LUMSA