La classificazione dei dati e dei servizi della PA e la qualificazione dei servizi cloud

Luca Nicoletti

14 giugno 2022

Cloud della PA: realizziamo il sistema operativo del Paese

La classificazione dei dati e dei servizi della PA e la qualificazione dei servizi cloud:

caratteristiche e prospettive

14.06.2022

CLASSIFICAZIONE DEI DATI E QUALIFICAZIONE DEI SERVIZI CLOUD

15 Dicembre 2021

Adozione del "Regolamento Cloud", che definisce il quadro normativo della Strategia Cloud Italia

AGID

Classificazione del catalogo dei servizi erogati dalle PA

- Modello di classificazione a 3 livelli basato sull'identificazione del **livello di criticità dei servizi** (**Ordinari**, **Critici** e **Strategici**)
- La classificazione è funzionale al processo di migrazione: dati critici e strategici dovranno essere ospitati presso **strutture in possesso di requisiti adeguati**.

Determina 306/18
Gennaio 2022

Processo di qualificazione dei servizi cloud e dei datacenter delle PA

- Il regolamento prescrive requisiti di **sicurezza, affidabilità e qualità che devono possedere,** a seguito di un **processo di qualificazione,** tutte le infrastrutture che ospitano dati e servizi delle PA (datacenter e servizi forniti dagli operatori cloud)
- Il **livello di qualificazione** raggiunto stabilisce il livello di criticità che una data infrastruttura può ospitare

Determina 307/18
Gennaio 2022

CLASSIFICAZIONE DEI DATI E DEI SERVIZI DELLA PA

CRITICITA' DI UN SERVIZIO

Servizi classificati su tre livelli, in base ai possibili effetti di una loro compromissione, in termini di **disponibilità, confidenzialità e integrità**

- **Strategici**: la cui compromissione può avere impatto sulla **sicurezza nazionale;**

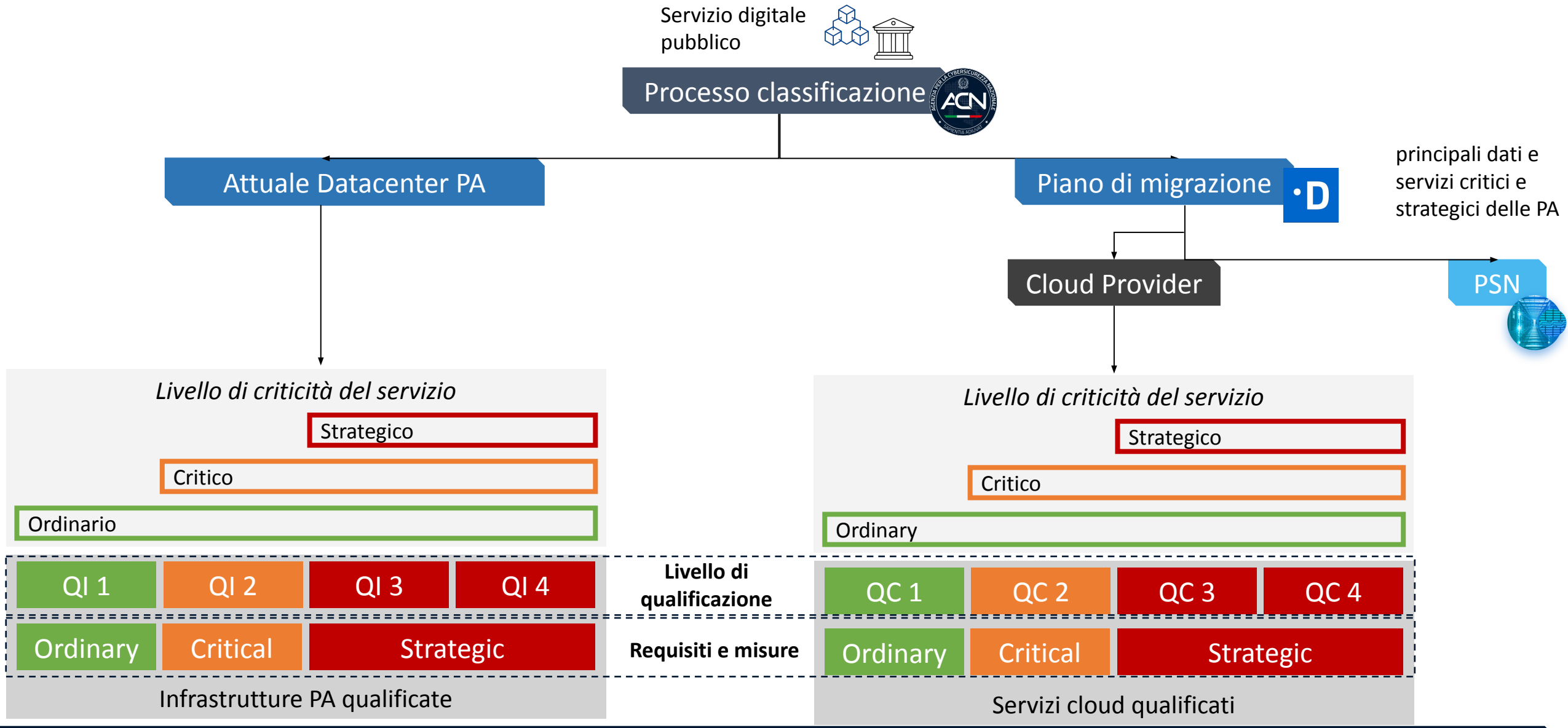
  es. servizi inclusi nel Perimetro di Sicurezza Nazionale Cibernetica (PSNC), servizi essenziali di Operatori NIS erogati a livello nazionale

- **Critici**: 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;**

  es. servizi che trattano grandi moli di dati personali o sanitari, servizi essenziali di Operatori NIS erogati a livello locale

- **Ordinari:** gli altri servizi.

QUALIFICAZIONE DEI SERVIZI CLOUD E DELLE INFRASTRUTTURE DELLA PA



STRATEGIA CLOUD ITALIA

SERVIZI CLOUD: REQUISITI DI QUALIFICAZIONE

- Certificazione richiesta
- Dichiarazione di conformità allo schema richiesta

		Requisiti (incrementali)	Requisiti principali (sovranità)	Certificazioni richieste
ORDINARIO	QC1	**40 Sicurezza** **17 Qualità, Performance, Interoperabilità**	• **Infrastruttura e dati localizzati in EU** (no vincoli sui metadati) • Richieste accesso ai dati della PA da entità extra-EU **notificate ad ACN e alla PA.** • **Nessun accesso è accordato** senza l'autorizzazione della PA	• ISO 27001 (est. 27017/18 o CSA STAR L2) • ISO 9001 (Qualità)
CRITICO	QC2	**+ 8 Sicurezza (48)** [+23 estesi]	• **Localizzazione in EU anche per i metadati** • **Funzionalità Bring-Your-Own-Key (BYOK) fornite dal provider** (inclusi requisiti specifici sugli HSM, e su generazione e gestione delle root keys)	• ISO 27001 (est. 27017/18 o CSA STAR L2) • ISO 9001 (Qualità) • ISO 20000 (IT Service Management) • ISO 22301 (Business Continuity)
STRATEGICO	QC3	**+ 2 Sicurezza (50)** [+ 21 estesi]	• **Controllo delle attività** privilegiate (inclusi aggiornamenti e accessi ai dati della PA) **esteso al personale del CSP** • Aggiornamenti verificati in ambiente di test, anche ai fini di sicurezza • **Informazioni su sedi e infrastrutture da cui è erogato il servizio cloud** rese disponibili alla PA	• ISO 27001 (with 27017/018°) • CSA STAR L2 • ISO 9001 (Qualità) • ISO 20000 (IT Service Management) • ISO 22301 (Business Continuity)
	QC4	**+1 Sicurezza (51)** [+ 2 estesi]	• **Funzionalità Hold-Your-Own-Key (HYOK) fornite dal provider** (inclusi requisiti specifici di gestione autonoma PA degli HSM e generazione e gestione delle chiavi) • **Flussi** dati da/verso esterno **soggetti a procedure di approvazione,** monitoraggio e controllo **concordate con la PA** • **Autonomia operative: il CSP deve essere** autonomo nella fornitura del servizio cloud e nella gestione dell'infrastruttura fisica e logica sottostante. Terze parti solo se assicurata la fungibilità	• ISO 27001 (with 27017/018°) • CSA STAR L2 • ISO 9001 (Qualità) • ISO 20000 (IT Service Management) • ISO 22301 (Business Continuity)

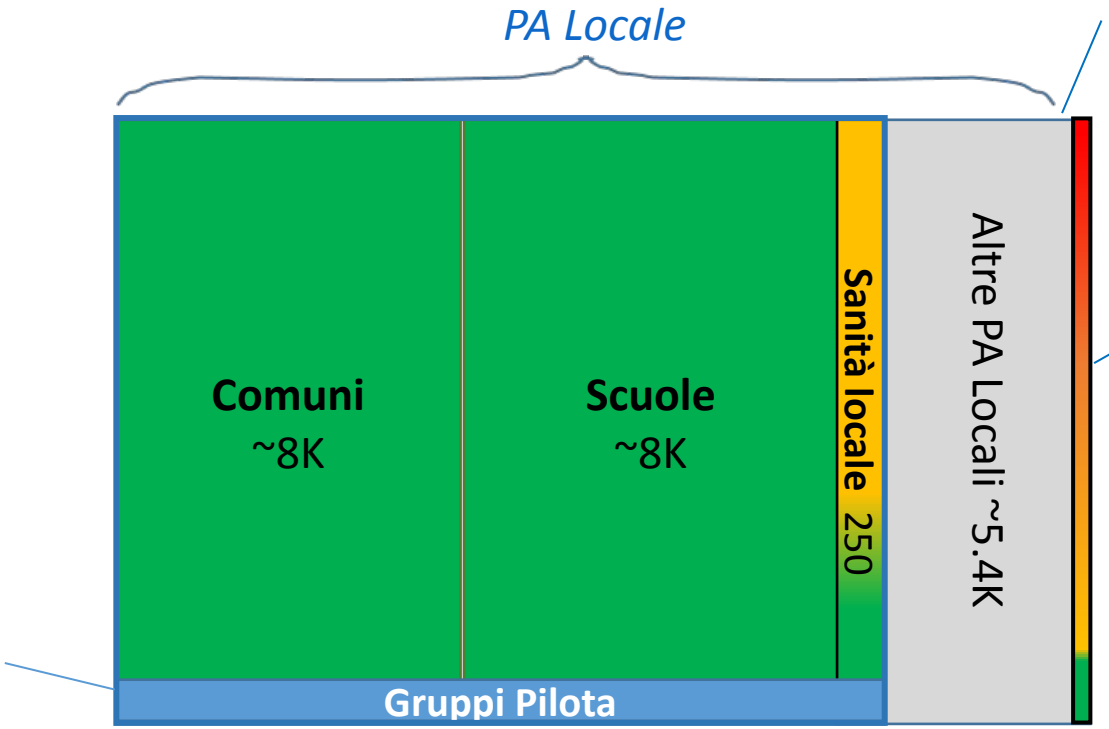
PA: COMPOSIZIONE

PA totali: ~22K

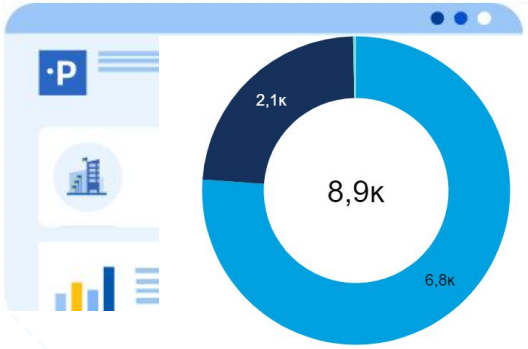
Alcuni gruppi omogenei di PA sono stati coinvolti in **esercizi pilota di classificazione** per determinare un **catalogo comune di servizi** e una corrispondente **pre-classificazione**

Livello	Comuni	Scuole	ASL/AO
Ordinari	95*	32	17
Critici	-	-	28
Strategici	-	-	-

Per lo più **servizi ordinari**
(Unioni di comuni, camere di commercio, agenzie ed enti per il turismo, …)



contiene il nucleo Strategico della PA



Statistiche classificazione (Giugno 22)

- **8.9K pratiche totali**
- **6.8K chiuse (inviate da PA e validate ACN)**
- 2.1K in fase di compilazione PA

* 3 di 95 servizi sono stati preclassificati come Critici solo per Comuni grandi (5 città principali con popolazione > 800K)

CLASSIFICAZIONE DEI DATI E DEI SERVIZI DELLA PA

IL PROCESSO DI CLASSIFICAZIONE

Classificazione

Accettazione catalogo preclassificato

(*per alcune PA*)

Eliminazione servizi

Aggiunta servizi

Tool di impact-assessment semplificato a due livelli

Validazione

Valutazione di conformità rispetto al modello

Migrazione

*Elaborato un **piano di migrazione**, identificando la tipologia di cloud di destinazione (PSN o servizio cloud qualificato) sulla base dell'esito della classificazione*

TOOL DI IMPACT-ASSESSMENT SEMPLIFICATO: APPROCCIO

APPROCCIO A DUE LIVELLI

Il processo implementato tramite la compilazione di un **form digitale (questionario)**:

- Valutazione del contesto di erogazione del servizio per valutare l'impatto di una sua eventuale compromissione (**livello di criticità**);
- Identificazione dei **servizi e dati digitali** che implementano il servizio.

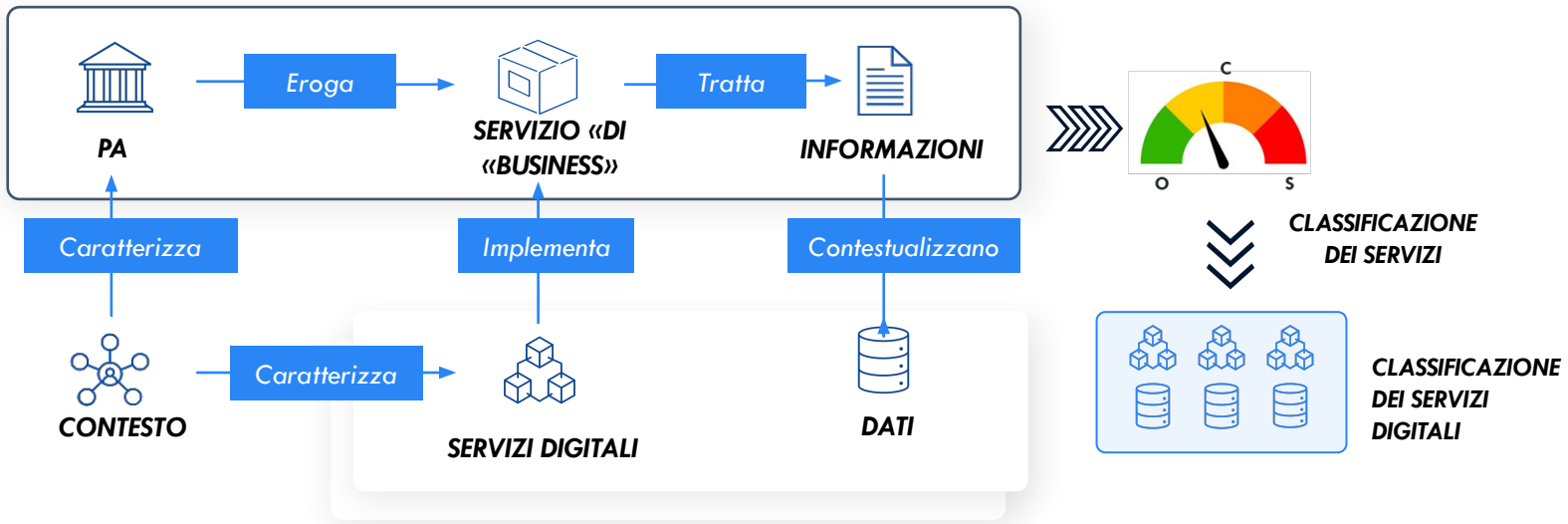
CLASSIFICAZIONE DEI SERVIZI DIGITALI

I dati e i servizi digitali sottostanti ereditano il livello di criticità del servizio che supportano.

METODOLOGIA

La valutazione è basata su metodologie standard di Risk assessment/BIA. L'obiettivo è fornire alla PA uno strumento semplificato e omogeneo di effettuare la classificazione dei servizi.
Il calcolo del punteggio è basato su un **algoritmo** che pesa le risposte alle varie sezioni per determinare un **livello finale di criticità**.

La PA può in ogni caso **proporre una differente classificazione** fornendo le motivazioni e documentazione a supporto (BIA o risk-assessment condotto in proprio).



RISULTATI E UTILIZZO

Una volta collezionati dalla piattaforma digitale, i risultati sono valutati dall'**Agenzia Nazionale per la Cybersicurezza** e formeranno la base per la preparazione del piano di migrazione.