



STRATEGIA CLOUD ITALIA



1. Classificazione dei dati e dei servizi della PA

Modello di classificazione a 3 livelli (**Ordinari**, **Critici** e **Strategici**) in base all'impatto di una loro compromissione sul sistema Paese.

Funzionale al processo di migrazione: dati critici e strategici dovranno essere ospitati presso strutture in possesso di requisiti adeguati.

2. Qualificazione dei servizi cloud

Basata su requisiti che i servizi cloud devono possedere per poter ospitare dati e servizi della PA, per mitigare in particolare i rischi sistemici di sicurezza e affidabilità.

Semplifica e regola l'acquisizione di servizi Cloud da parte delle PA.

3. Polo Strategico Nazionale (PSN)

Situato su territorio nazionale, con controllo e linee di indirizzo pubbliche. La gestione operativa sarà affidata a un fornitore qualificato.

Garantisce adeguati livelli di continuità operativa e tolleranza ai guasti per i servizi strategici e critici della PA.

STRATEGIA CLOUD ITALIA: SVILUPPO TEMPORALE



CLASSIFICAZIONE DEI DATI E DEI SERVIZI

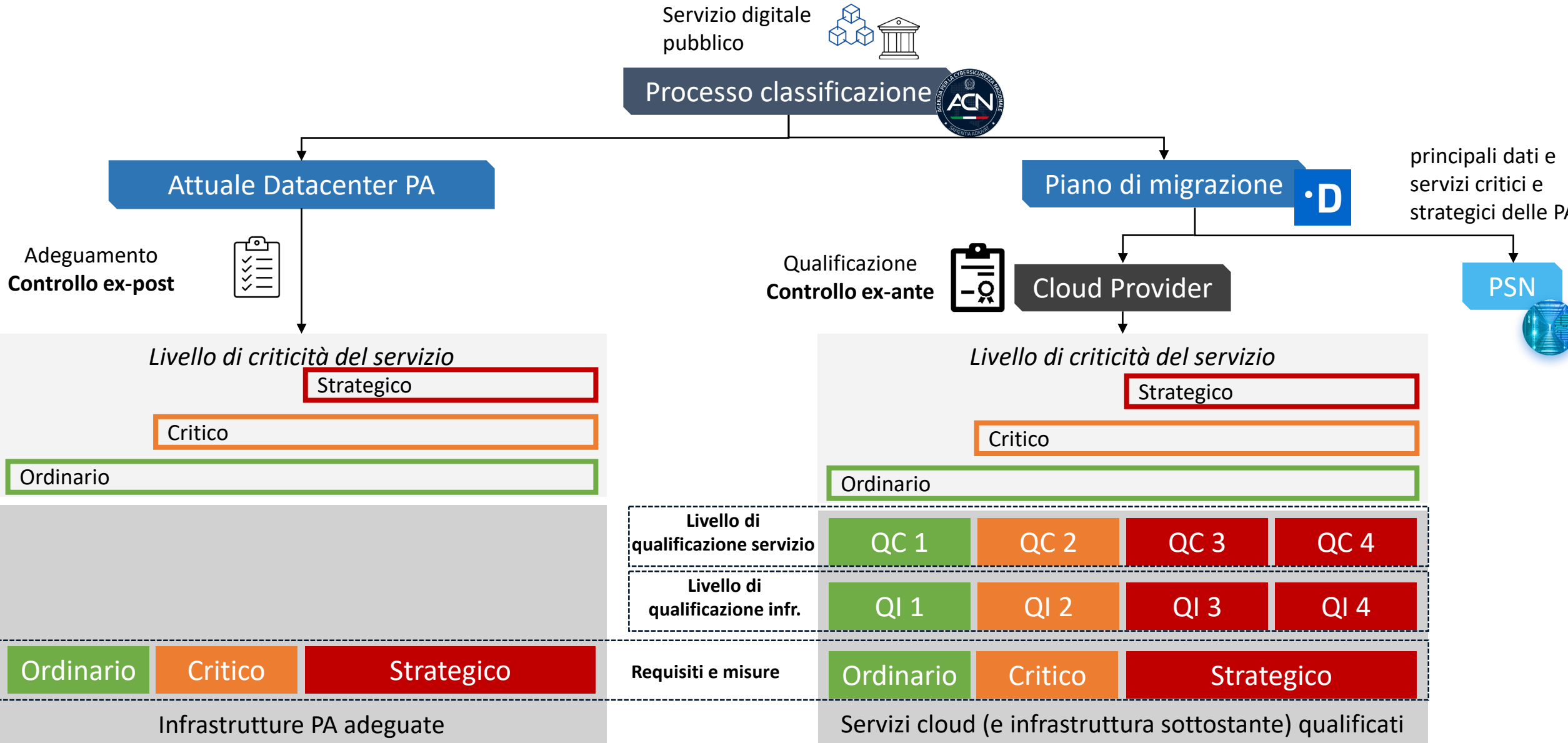


Servizi classificati su tre livelli, in base ai possibili effetti di una loro compromissione, in termini di **disponibilità, confidenzialità e integrità**

- **Strategici:** la cui compromissione può avere impatto sulla **sicurezza nazionale**
servizi/funzioni PSNC
servizi essenziali NIS erogati a livello nazionale
servizi che trattano dati personali di un numero molto elevato di cittadini
- **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;**
servizi essenziali NIS erogati a livello locale
servizi che trattano dati personali di un numero elevato di cittadini
servizi che trattano dati sanitari di un numero consistente di cittadini
- **Ordinari:** gli altri servizi.

Ai livelli di criticità sono associati differenti requisiti di sicurezza che dovranno possedere infrastrutture digitali e servizi cloud che li ospitano
(Regolamento Cloud, Artt. 7 e 8)

QUALIFICAZIONE DEI SERVIZI CLOUD E DELLE INFRASTRUTTURE DELLA PA



REQUISITI DI SICUREZZA

	ORDINARIO (40 misure)	CRITICO (66 misure)	STRATEGICO (72 misure)
ID.AM	<ul style="list-style-type: none"> Asset Management 	<ul style="list-style-type: none"> Comunicazione dei nominativi dell'incaricato e del referente tecnico all'ACN 	
ID.GV	<ul style="list-style-type: none"> Governance 		
ID.RA	<ul style="list-style-type: none"> Risk Assessment 	<ul style="list-style-type: none"> Requisiti specifici per le relazioni periodiche vulnerability assessment metriche monitoraggio 	
ID.SC	<ul style="list-style-type: none"> Supply Chain Risk Management 	<ul style="list-style-type: none"> Shared Security Responsibility Model Diversificazione/ridondanza fornitori Ambito contrattuale: misure per dipendenze interne/esterne Audit fornitori 	<ul style="list-style-type: none"> Valutazione affidabilità tecnica dei fornitori Verifica qualità del codice sorgente
PR.AC	<ul style="list-style-type: none"> Identity Management, Authentication and Access Control 		<ul style="list-style-type: none"> Accesso ai dati approvati formalmente dall'Amministrazione
PR.AT	<ul style="list-style-type: none"> Awareness and Training 		
PR.D	<ul style="list-style-type: none"> Data Security 	<ul style="list-style-type: none"> Key management (BYOK) 	
PR.IP	<ul style="list-style-type: none"> Information Protection Processes and Procedures 	<ul style="list-style-type: none"> Disaster Recovery 	<ul style="list-style-type: none"> Piano di gestione vulnerabilità aggiornato su base semestrale
PR.PT	<ul style="list-style-type: none"> Protective Technology 	<ul style="list-style-type: none"> Sito di Disaster Recovery 	
DE.AE	<ul style="list-style-type: none"> Anomalie e Eventi 	<ul style="list-style-type: none"> Analisi e correlazione degli eventi 	
DE.CM	<ul style="list-style-type: none"> Monitoraggio 	<ul style="list-style-type: none"> Requisiti su 	
DE.DP	<ul style="list-style-type: none"> Processi di rilevamento 		
RS.RP – Response Planning	<ul style="list-style-type: none"> Piano di risposta 	<ul style="list-style-type: none"> Elementi specifici del piano di risposta 	
RS.CO – Communications	<ul style="list-style-type: none"> Communications 	<ul style="list-style-type: none"> Attività di risposta 	
RS.AN – Analysis		<ul style="list-style-type: none"> Penetration test e vulnerability assessment – Vulnerability mgmt 	
RS.MI – Mitigation		<ul style="list-style-type: none"> Mitigazione delle vulnerabilità 	
RC.RP	<ul style="list-style-type: none"> Response Planning 	<ul style="list-style-type: none"> Recovery plan 	<ul style="list-style-type: none"> Esercitazioni
PR.MA - Maintenance	<ul style="list-style-type: none"> PR.MA - Maintenance 		
RC.CO –			<ul style="list-style-type: none"> Communications - Attività di ripristino e comunicazione al CSIRT

SPECIALIZZAZIONI





ORDINARIO – Le misure di sicurezza per i dati ed i servizi ordinari sono ereditati da framework di riferimento standard (FNSC, CCM) - misure base

CRITICI e STRATEGICI – Per dati e servizi critici e/o strategici, le misure di sicurezza previste per i dati ordinari sono state specializzate (ove necessario), è stato ampliato l'insieme dei domini di riferimento e sono state incluse misure più stringenti derivanti dal PSNC

Framework Nazionale per la Cybersecurity e la Data Protection



QUALIFICAZIONE DEI SERVIZI CLOUD

	CARATTERISTICHE	CERTIFICAZIONI	REQUISITI CARATTERIZZANTI
QC1	40 Sicurezza 11 Qualità 2 Portabilità 4 Interoperabilità	 ISO 27001/17/18* ISO 9001 (Qualità)	<ul style="list-style-type: none"> Localizzazione in EU: infrastrutture fisiche e tecnologiche servizio cloud, dati Amministrazioni;
QC2	66 Sicurezza	 ISO 27001/17/18* ISO 9001 (Qualità) ISO 20000 (Gestione Servizio) ISO 22301 (Continuità Operativa)	<ul style="list-style-type: none"> Importazione delle chiavi di cifratura generate esternamente, BYOK (HSM gestito dall'Amministrazione)
QC3	72 Sicurezza	 ISO 27001/17/18 CSA STAR* Level 2	<ul style="list-style-type: none"> Localizzazione in EU: metadati; Controllo delle attività privilegiate e aggiornamenti hw/sw Verifica aggiornamenti ambiente di test
QC4		 ISO 9001 (Gestione Qualità) ISO 20000 (Gestione Servizio) ISO 22301 (Continuità Operativa)	<hr style="border-top: 1px dashed #0000FF;"/> <ul style="list-style-type: none"> Gestione delle chiavi autonoma esterna, HYOK (HSM gestito dall'Amministrazione) Flussi da/verso esterno sono soggetti a procedure di approvazione, monitoraggio e controllo dell'Amministrazione Metodologie di verifica e controllo del personale sono condivise con l'Amministrazione

oppure CSA STAR Level 2 – ** Level 2 richiede la certificazione da parte di un ente esterno



Richiesta certificazione



Richiesta aderenza allo standard (e.g. auto dichiarazione di conformità)

CLASSIFICAZIONE: METODOLOGIA

APPROCCIO AD ALTO LIVELLO

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 «di business»** della PA.

CLASSIFICAZIONE DEI SERVIZI DIGITALI

I dati e i servizi digitali sottostanti ereditano il livello di criticità del servizio che supportano (elencazione facoltativa)

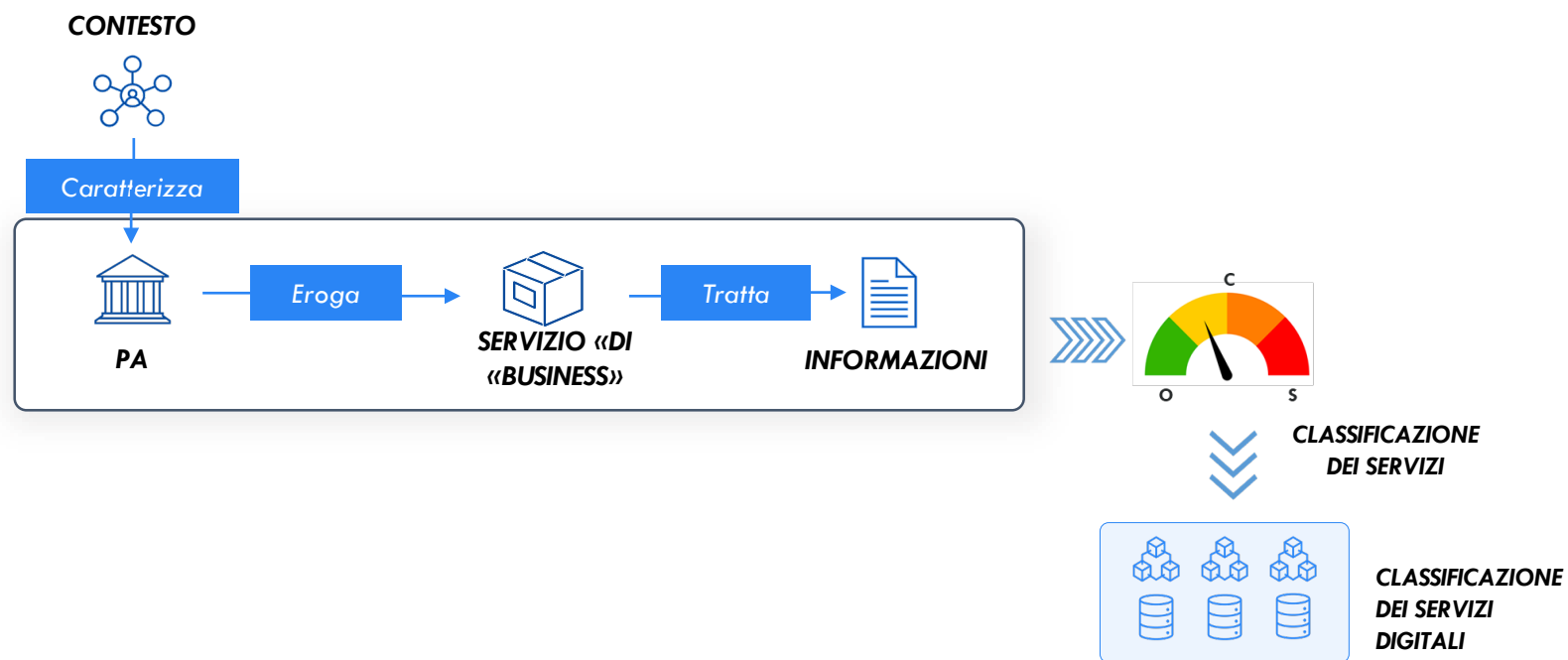
METODOLOGIA

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.

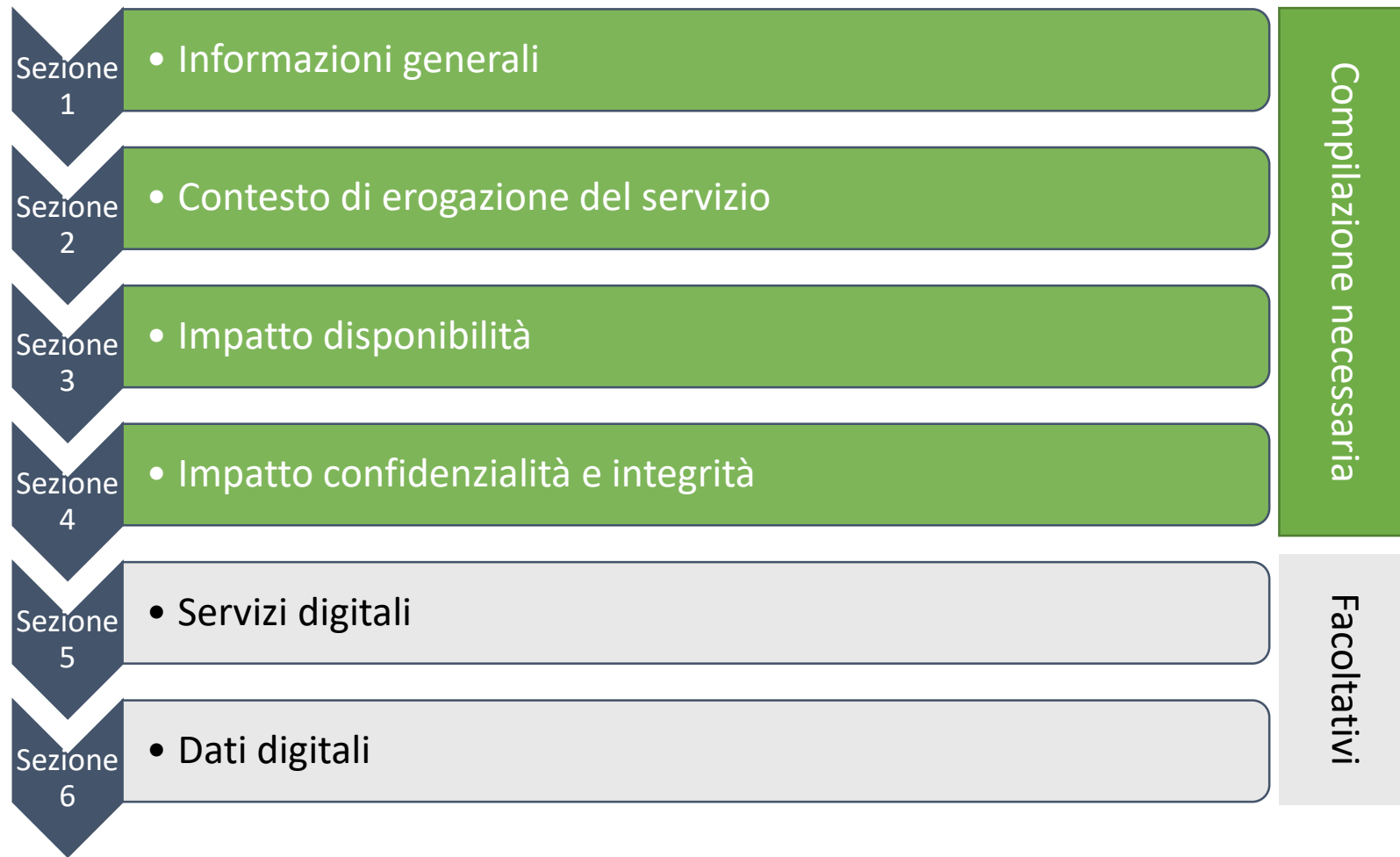
Il calcolo del punteggio è basato su un **algoritmo** che pesa le risposte alle varie sezioni per determinare un **livello finale di criticità**.

RISULTATI E UTILIZZO

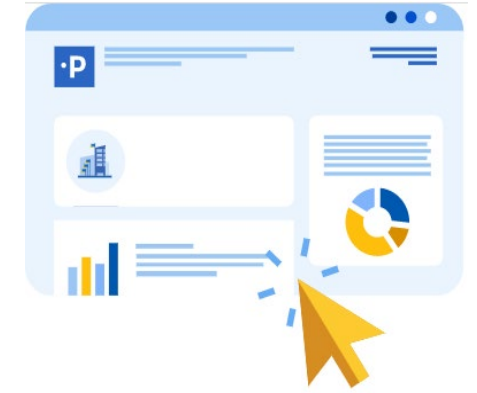
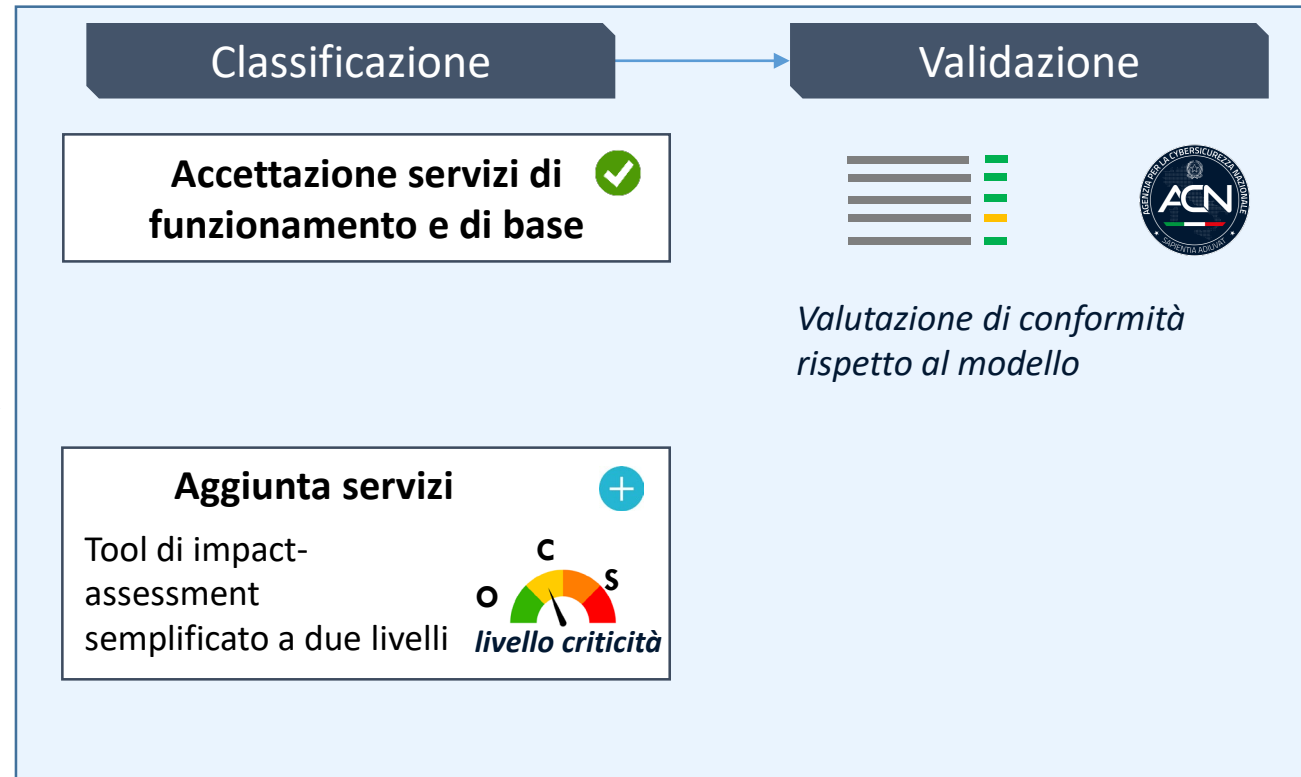
Una volta collezionati dalla piattaforma digitale, i risultati sono valutati dall'**Agenzia per la Cybersicurezza Nazionale** e formeranno la base per la preparazione del piano di migrazione.



CLASSIFICAZIONE: QUESTIONARIO



CLASSIFICAZIONE: PIATTAFORMA

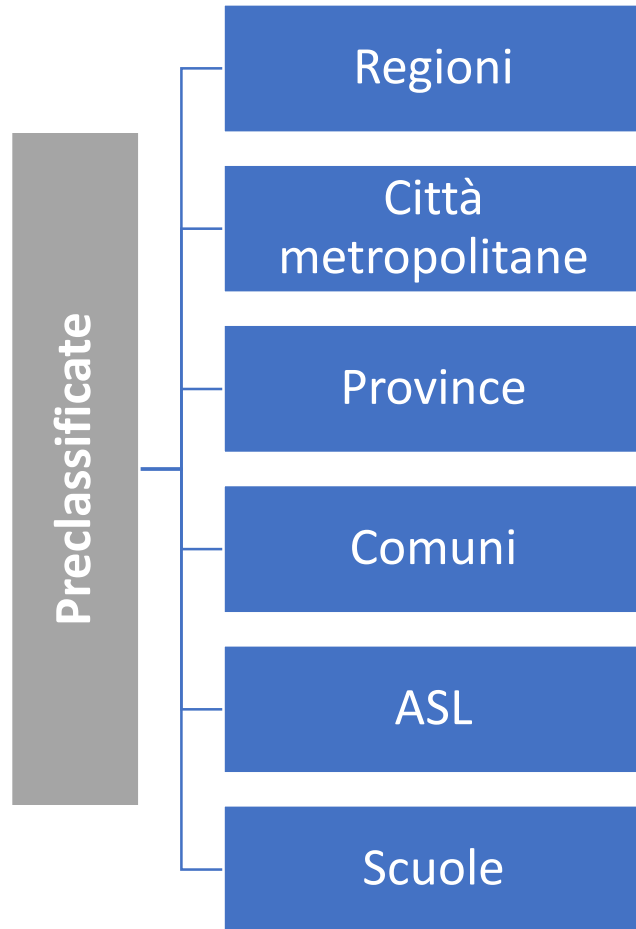


<https://padigitale2026.gov.it/>

Statistiche classificazione (Novembre 22)

- **18K pratiche totali**
- **16K chiuse (inviate da PA e validate ACN)**
- 2K in fase di compilazione PA e/o validazione ACN

CLASSIFICAZIONE: STRUMENTI



CLASSIFICAZIONE: SERVIZI COMUNI ALLE PA

CATEGORIA	NOME SERVIZIO	CLASSIFICAZIONE PROPOSTA
Servizi di funzionamento	Conservazione digitale	ORDINARIO
Servizi di funzionamento	Acquisti	ORDINARIO
Servizi di funzionamento	Contabilità, Bilancio e Controllo	ORDINARIO
Servizi di funzionamento	Gestione documentale	ORDINARIO
Servizi di funzionamento	Organi istituzionali e di supporto, Rapporti istituzionali	ORDINARIO
Servizi di funzionamento	Personale	ORDINARIO
Servizi di funzionamento	Produttività individuale e Collaboration	ORDINARIO
Servizi di funzionamento	Protocollo	ORDINARIO
Servizi di funzionamento	Sicurezza fisica delle sedi	ORDINARIO
Servizi di funzionamento	Trasparenza, Privacy e Controlli interni	ORDINARIO
Servizi di base della PA	Accesso agli atti, accesso civico e URP	ORDINARIO
Servizi di base della PA	Comunicazione istituzionale web e open data	ORDINARIO
Servizi di base della PA	Albo pretorio	ORDINARIO
Servizi di base della PA	Contenzioso	ORDINARIO
Servizi di base della PA	Finanziamenti	ORDINARIO
Servizi di base della PA	Notifiche	ORDINARIO

CLASSIFICAZIONE: ESITI

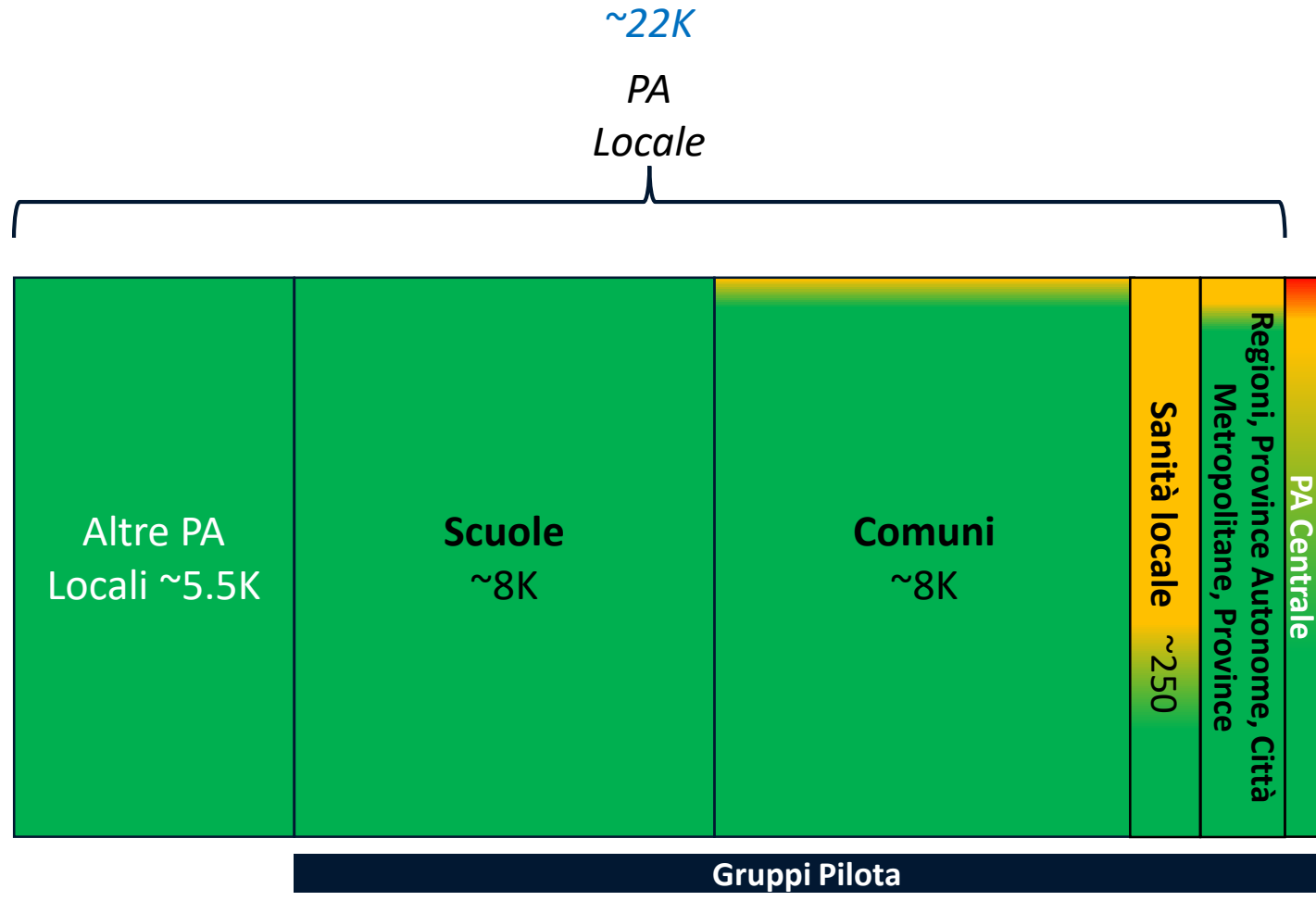


↓
DATI E SERVIZI

Dati e servizi
ORDINARI

Dati e servizi
CRITICI

Dati e servizi
STRATEGICI



CLASSIFICAZIONE: ESITI

