Transizione Digitale

www.transizionedigitale.it

Regolamento per le Infrastrutture Digitali e per i Servizi Cloud per la Pubblica Amministrazione

Ambito di Applicazione del Regolamento Cloud per le Pubbliche Amministrazioni

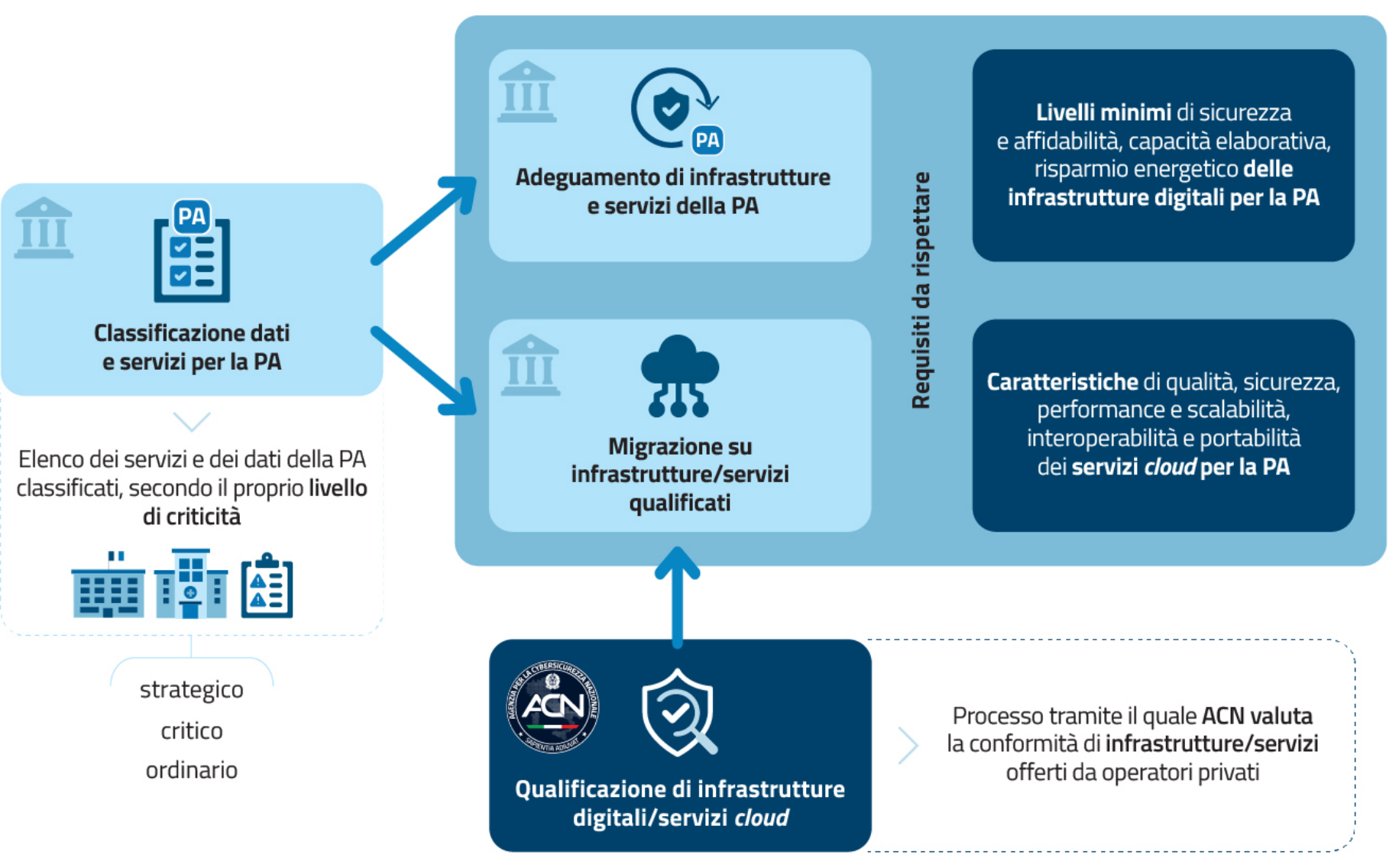
- 1. Definizione delle Amministrazioni coinvolte
  - **Amministrazioni centrali**
  - **Amministrazioni locali**
  - Il termine "amministrazioni"
  - *Tutte definite dall'articolo 1, comma 3, della legge 31 dicembre 2009, n. 196*
    - La ricognizione delle amministrazioni pubbliche di cui al comma 2 è operata annualmente dall'ISTAT con proprio provvedimento e pubblicata nella Gazzetta Ufficiale entro il 30 settembre.
    - Qui l'aggiornamento 2023 di ISTAT
    - Qui la pagina con la ricognizione di tutti gli anni
- 2. Oggetto del regolamento
  - Infrastrutture digitali per le pubbliche amministrazioni
    - Centri di Elaborazione Dati (CED): Siti che ospitano reti e sistemi informativi per l'erogazione di servizi interni ed esterni delle amministrazioni.
      - Questi comprendono almeno risorse di calcolo, apparati di rete per la connessione e sistemi di memorizzazione di massa.
    - L'infrastruttura promossa dalla Presidenza del Consiglio dei ministri di cui all'articolo 33-septies, comma 1, del decreto-legge n. 179 del 2012.
    - Componenti di un'infrastruttura digitale messi a disposizione da terze parti per l'erogazione di servizi cloud per la pubblica amministrazione (c.d. housing).
    - Infrastrutture di prossimità: Componenti di un'infrastruttura digitale, eventualmente messi a disposizione da terze parti, finalizzati all'incremento delle prestazioni nell'erogazione in prossimità dei servizi digitali delle amministrazioni.
  - Infrastrutture dei servizi cloud per le pubbliche amministrazioni
    - Queste sono le infrastrutture digitali di cui al punto precedente, fornite da un operatore di infrastrutture digitali, tramite le quali sono erogati i servizi cloud per le pubbliche amministrazioni.
  - Servizi cloud per le pubbliche amministrazioni
    - Servizi sistemistici infrastrutturali (Infrastructure-as-a-Service, IaaS): Per l'erogazione, ad esempio, di server virtualizzati e spazio di salvataggio dati.
    - Piattaforme computazionali (Platform-as-a-Service, PaaS): Per l'erogazione di ambienti pre-configurati e amministrati per lo sviluppo di specifiche applicazioni, come lo sviluppo software, la gestione di dati o di applicazioni.
    - Servizi applicativi (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. In questo modello, il gestore del servizio si occupa della predisposizione, configurazione, messa in esercizio e manutenzione del servizio, lasciando all'amministrazione il solo ruolo di utilizzatore delle funzionalità offerte.
- 3. Ambito temporale
  - Il regolamento si applica a decorrere dal 1 agosto 2024.
  - Le attività di migrazione previste dal piano devono essere completate entro il 30 giugno 2026.
- 4. Esclusioni specifiche
  - I dati e i servizi digitali soggetti agli obblighi del decreto-legge 21 settembre 2019, n. 105 (perimetro di sicurezza nazionale cibernetica) sono classificati come "strategici" e non sono oggetto dell'elencazione e classificazione generale prevista dal regolamento.
  - I dati e i servizi digitali soggetti agli obblighi del decreto legislativo 18 maggio 2018, n. 65 (direttiva NIS) sono classificati come "critici" se non a valenza nazionale, e come "strategici" se a valenza nazionale.
- 5. Applicazione ai servizi digitali
  - I servizi digitali non ancora classificati non possono essere resi disponibili agli utenti finali.
- 6. Estensione agli ambienti di sviluppo e test
  - Le caratteristiche di base si applicano principalmente agli ambienti di produzione.
  - Per gli ambienti di pre-produzione, test, sviluppo e simili, le caratteristiche si applicano in coerenza con quelle dell'ambiente di produzione, eventualmente in relazione a un'analisi del rischio.
- 7. Applicazione ai fornitori di servizi
  - Include disposizioni specifiche per i fornitori di servizi cloud, sia pubblici che privati.
  - Introduce un processo di qualificazione per i servizi cloud offerti da fornitori privati.
- 8. Considerazioni sulla localizzazione dei dati
  - Stabilisce requisiti specifici per la localizzazione dei dati dell'amministrazione e dei metadata, con particolare attenzione al territorio dell'Unione Europea.

1. Introduzione

- **Scopo del regolamento:** Il regolamento, adottato da ACN con Decreto Direttoriale n. 21007/24 del 27 giugno 2024 e applicabile dal 1 agosto 2024, fornisce un quadro normativo completo per la digitalizzazione della PA.
  - Definire i livelli minimi di sicurezza, capacità elaborativa, risparmio energetico e affidabilità delle infrastrutture digitali per la PA
  - Stabilire le caratteristiche di qualità, sicurezza, performance, scalabilità, interoperabilità e portabilità dei servizi cloud per la PA
  - Determinare le modalità di migrazione dei dati e servizi digitali della PA
- **Definizioni chiave:** Le definizioni chiave forniscono un linguaggio comune per tutti gli attori coinvolti.
  - Infrastruttura digitale – L'infrastruttura digitale comprende hardware, software e reti
  - Servizi cloud (IaaS, PaaS, SaaS) – I servizi cloud sono categorizzati in IaaS (infrastruttura), PaaS (piattaforma) e SaaS (software)
  - Dati dell'amministrazione – I dati dell'amministrazione sono tutte le informazioni gestite dalla PA
  - Metadata – I metadata sono dati sui dati, cruciali per la gestione e l'organizzazione
  - Dipendenze interne ed esterne – Le dipendenze indicano le relazioni tra sistemi e servizi.

2. Classificazione dei dati e servizi digitali

- Ordinari
  - I dati ordinari sono informazioni di routine che, se compromesse, non causano danni gravi.
  - Potrebbero includere informazioni pubbliche o dati non sensibili.
  - La loro protezione è importante, ma non richiede misure di sicurezza estreme.
  - Un esempio potrebbe essere l'orario di apertura di un ufficio pubblico o statistiche anonime sull'utilizzo dei servizi.
- Critici
  - I dati critici sono essenziali per il funzionamento della società. Includono informazioni sanitarie, finanziarie o di pubblica sicurezza.
  - La loro compromissione potrebbe causare interruzioni significative dei servizi pubblici.
  - Ad esempio, i dati del sistema sanitario nazionale o le informazioni sul traffico stradale in tempo reale sono considerati critici.
  - Richiedono misure di sicurezza avanzate e piani di continuità operativa.
- Strategici
  - I dati strategici sono di importanza cruciale per la sicurezza nazionale. Includono informazioni militari, di intelligence o relative a infrastrutture critiche.
  - La loro compromissione potrebbe minacciare direttamente la sicurezza del paese.
  - Esempi includono piani di difesa nazionale o dettagli su infrastrutture energetiche critiche.
  - Questi dati richiedono il massimo livello di protezione e sono soggetti a protocolli di sicurezza estremamente rigorosi.

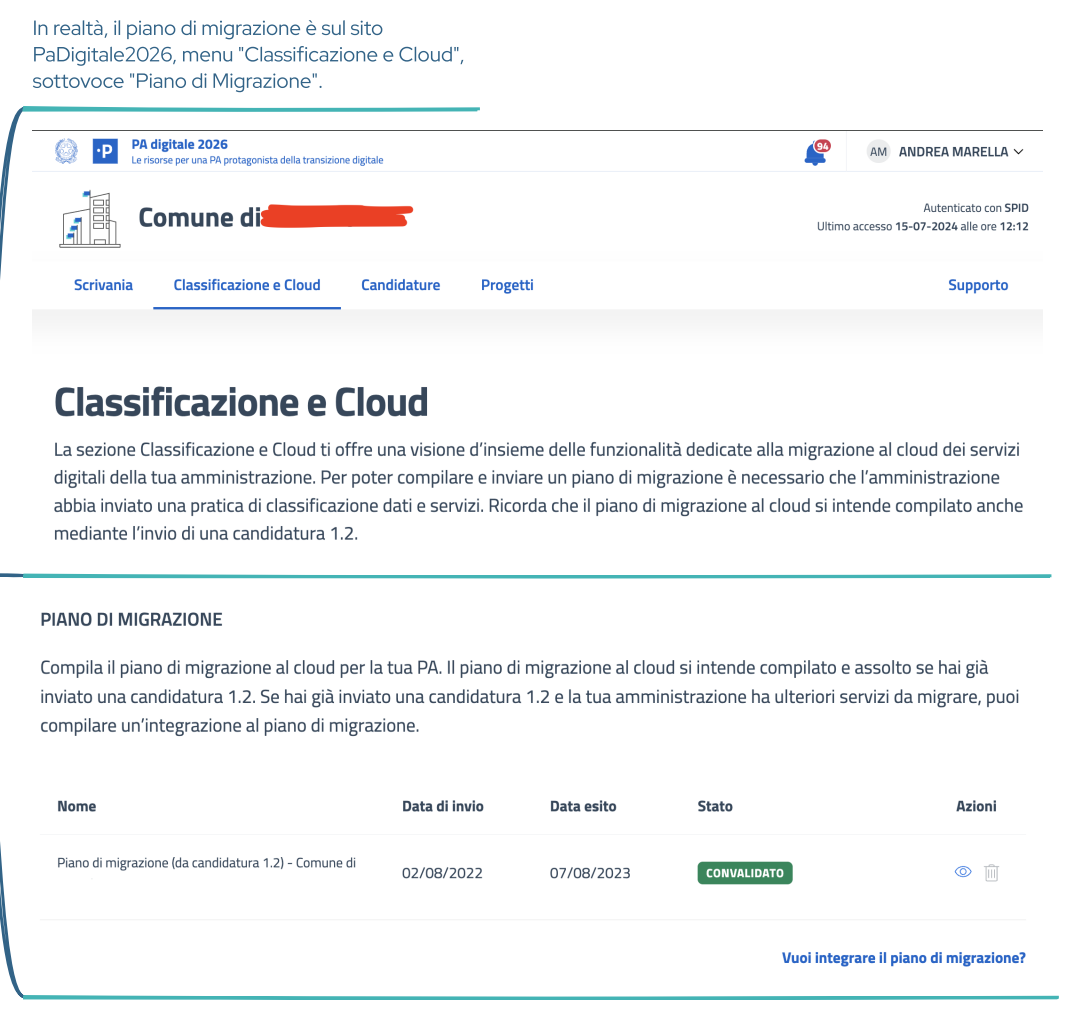

Classificazione dati e servizi per la PA
Elenco dei servizi e dei dati della PA classificati, secondo il proprio livello di criticità
strategico
critico
ordinario
Adeguamento di infrastrutture e servizi della PA
Migrazione su infrastrutture/servizi qualificati
Requisiti da rispettare
Livelli minimi di 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
Qualificazione di infrastrutture digitali/servizi cloud
Processo tramite il quale ACN valuta la conformità di infrastrutture/servizi offerti da operatori privati

3. Livelli minimi di sicurezza e affidabilità

- **Per infrastrutture digitali**
  - Requisiti di sicurezza fisica e logica
    - La sicurezza fisica include controlli d'accesso e protezione da disastri naturali
    - La sicurezza logica riguarda firewall, crittografia e gestione degli accessi.
  - Capacità elaborativa minima – assicura performance adeguate
  - Efficienza energetica – riduce costi e impatto ambientale
  - Disponibilità e continuità operativa – garantisce l'accesso continuo ai servizi, con piani di disaster recovery
- **Per infrastrutture dei servizi cloud** Le infrastrutture cloud devono garantire sicurezza end-to-end.
  - Requisiti di sicurezza per l'erogazione di servizi cloud – protezione dei dati in transito e a riposo, isolamento tra tenant e controlli d'accesso robusti
  - Scalabilità e performance
    - La scalabilità permette di gestire picchi di domanda.
    - Le performance sono monitorate costantemente.
  - Interoperabilità e portabilità
    - L'interoperabilità assicura che diversi sistemi possano comunicare.
    - La portabilità permette di migrare dati e applicazioni tra provider cloud senza lock-in.
- **Per servizi cloud** Ogni tipo di servizio cloud ha requisiti specifici
  - Requisiti di sicurezza specifici per IaaS, PaaS e SaaS
    - IaaS – focus su sicurezza della rete e dell'hypervisor
    - PaaS – focus sicurezza delle API e del runtime
    - SaaS – protezione dei dati applicativi
  - Gestione delle identità e degli accessi
    - autenticazione multi-fattore
    - controllo degli accessi basato sui ruoli
  - Protezione dei dati e crittografia – protegge i dati sia in transito che memorizzati, con gestione sicura delle chiavi.

4. Migrazione dei dati e servizi digitali

- **Criteri per la migrazione** Prima della migrazione, si valutano i rischi associati.
  - Analisi sensibilità dei dati e la criticità dei servizi.
  - Verifica compatibilità del cloud target con la classificazione dei dati.
  - Si assicura che il provider cloud soddisfi tutti i requisiti di sicurezza.
  - Pianificazione test di sicurezza pre e post migrazione.
  - Definizione procedure di rollback in caso di problemi.
- Modalità e termini
  - Piano di migrazione
    - Si sviluppa un piano dettagliato di migrazione, includendo fasi, responsabilità e milestone.
    - *Le PA devono presentare un piano di migrazione mediante un modello reso disponibile sul sito DTD nella sezione CLOUD.*
      - In realtà, il piano di migrazione è sul sito PaDigitale2026, menu "Classificazione e Cloud", sottovoce "Piano di Migrazione".
  - Tempistiche di completamento – Il piano deve essere presentato e le attività associate concluse entro e non oltre il 30 giugno 2026
  - Monitoraggio e reporting del processo di migrazione



Comune di [redacted]

Autenticato con SPID

Ultimo accesso 15-07-2024 alle ore 12:12

Classificazione e Cloud

La sezione Classificazione e Cloud ti offre una visione d'insieme delle funzionalità dedicate alla migrazione al cloud dei servizi digitali della tua amministrazione. Per poter compilare e inviare un piano di migrazione è necessario che l'amministrazione abbia inviato una pratica di classificazione dati e servizi. Ricorda che il piano di migrazione al cloud si intende compilato anche mediante l'invio di una candidatura 1.2.

PIANO DI MIGRAZIONE

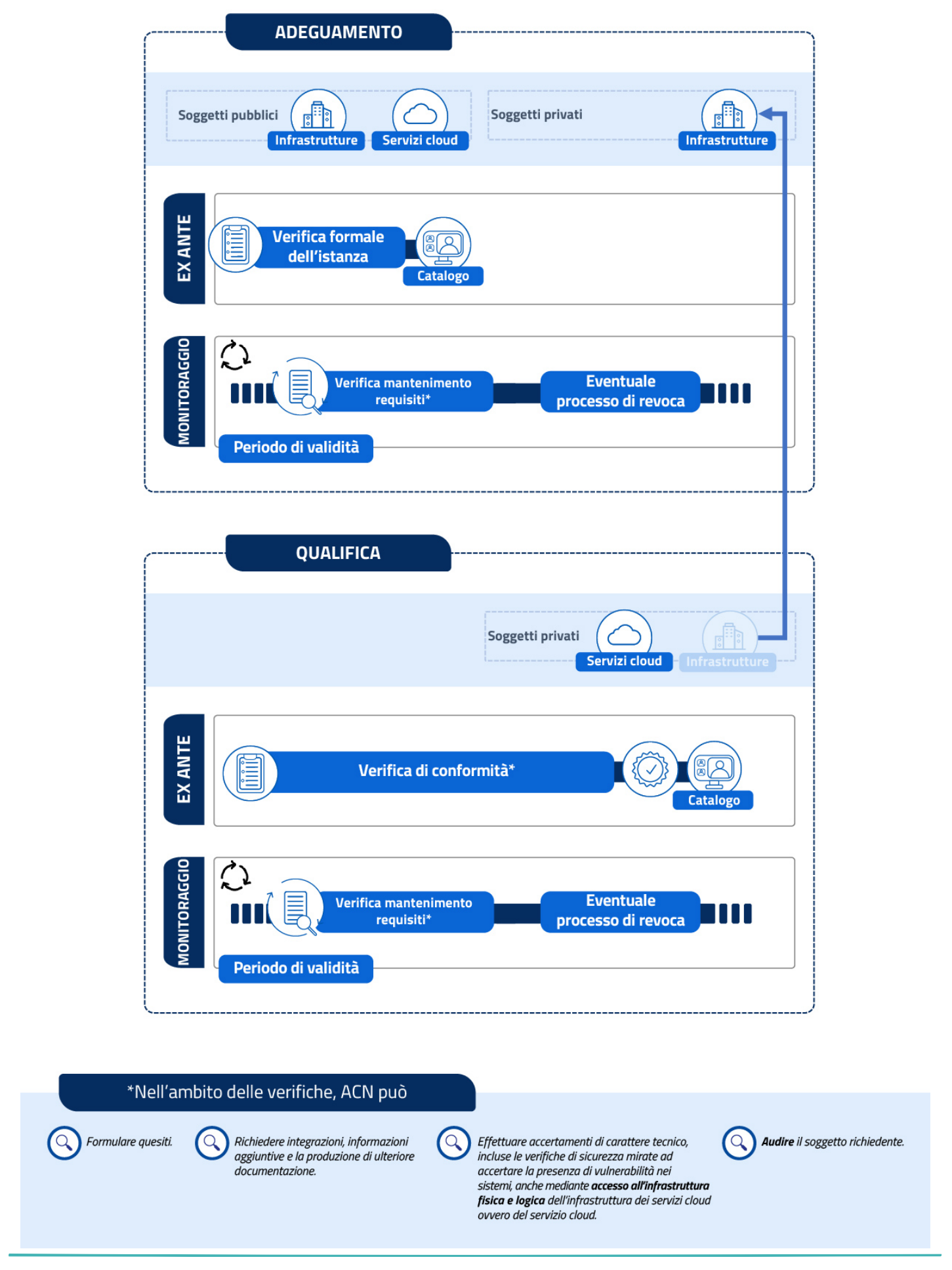
Compila il piano di migrazione al cloud per la tua PA. Il piano di migrazione al cloud si intende compilato e assolto se hai già inviato una candidatura 1.2. Se hai già inviato una candidatura 1.2 e la tua amministrazione ha ulteriori servizi da migrare, puoi compilare un'integrazione al piano di migrazione.

Nome	Data di invio	Data esito	Stato	Azioni
Piano di migrazione (da candidatura 1.2) - Comune di	02/08/2022	07/08/2023	CONVALIDATO	

Vuoi integrare il piano di migrazione?

5. Adeguamento e qualificazione

- Infrastrutture digitali
  - L'adeguamento delle infrastrutture segue un processo strutturato.
  - Si valuta lo stato attuale rispetto ai requisiti.
  - Si identificano gap e si pianificano interventi.
  - Si implementano miglioramenti per sicurezza, capacità e efficienza.
  - Si verifica la conformità attraverso audit e test.
  - Si documentano tutte le modifiche e si aggiornano le politiche di gestione.
  - Il processo è iterativo, con revisioni periodiche per mantenere l'adeguamento nel tempo.
- Infrastrutture dei servizi cloud
  - L'adeguamento delle infrastrutture cloud richiede attenzione particolare.
  - Si valuta l'architettura multi-tenant e la segregazione dei dati.
  - Si implementano controlli per la gestione delle risorse condivise.
  - Si rafforzano i meccanismi di isolamento tra clienti.
  - Si migliorano le capacità di monitoraggio e logging.
  - Si implementano strumenti per la gestione automatizzata della sicurezza.
  - Si stabiliscono procedure per la gestione degli incidenti specifici del cloud.
- Servizi cloud
  - La qualificazione dei servizi cloud segue un processo rigoroso.
  - Si verifica la conformità a standard di settore (es. ISO 27001, CSA STAR).
  - Si valutano le pratiche di sviluppo sicuro e la gestione del ciclo di vita del software.
  - Si esaminano le politiche di backup e disaster recovery.
  - Si verificano le capacità di crittografia e gestione delle chiavi.
  - Si valutano le procedure di patch management e aggiornamento.
  - Il processo include audit periodici e rivalutazioni.

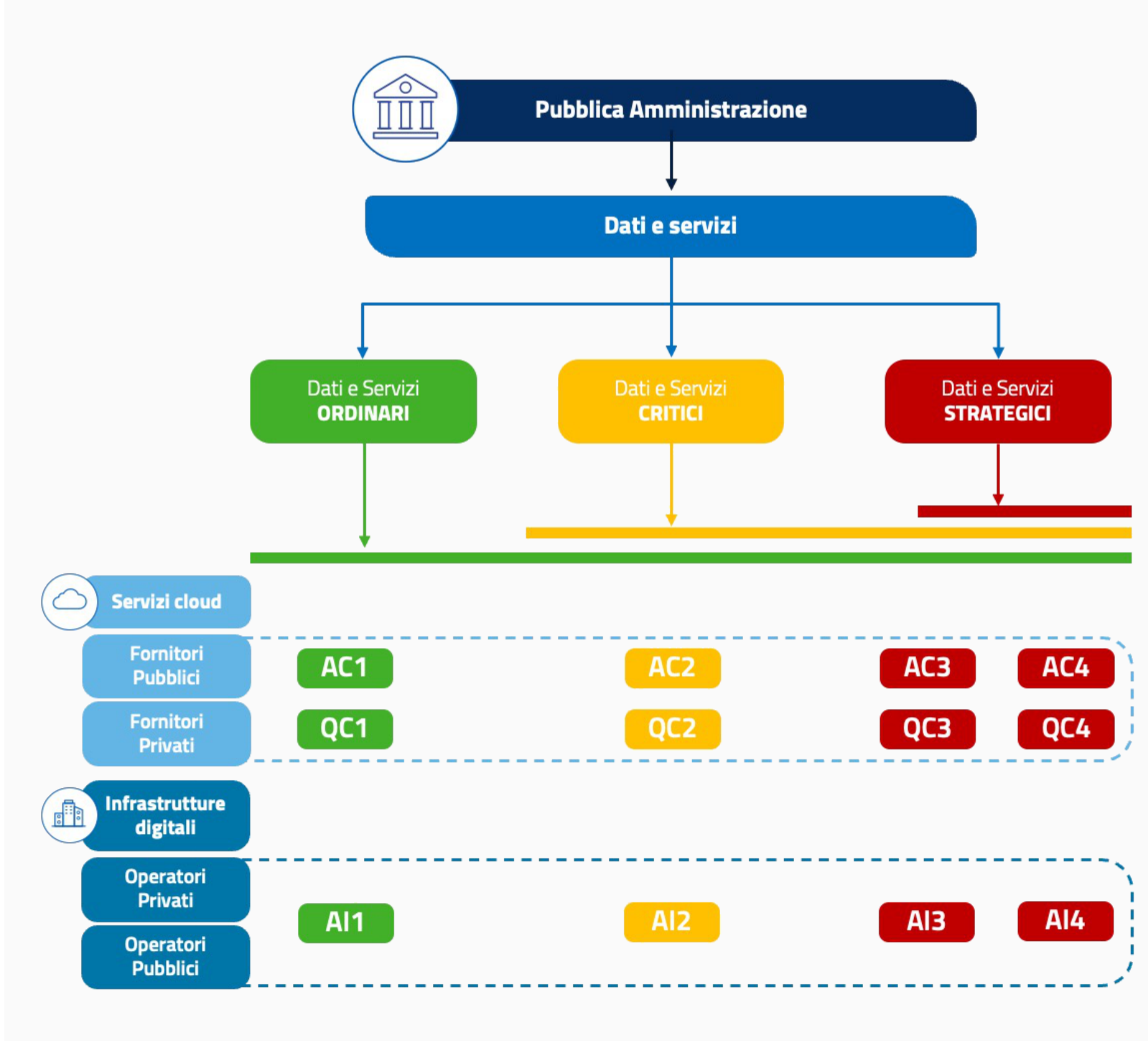


*Nell'ambito delle verifiche, ACN può

- *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.*

6. Livelli di adeguamento/qualificazione

- **Livello 1 (AI1/AC1/QC1)** Requisiti di base per dati e servizi ordinari
  - Il Livello 1 rappresenta i requisiti minimi accettabili.
  - Include controlli di sicurezza di base come autenticazione, firewall e backup regolari.
  - Richiede una politica di sicurezza documentata e formazione base per il personale.
  - Prevede un piano di continuità operativa semplice.
  - Adatto per dati pubblici o non sensibili.
  - Richiede aggiornamenti di sicurezza regolari e patch management di base.
- **Livello 2 (AI2/AC2/QC2)** Requisiti intermedi per dati e servizi critici
  - Il Livello 2 aumenta significativamente la sicurezza.
  - Introduce crittografia per dati sensibili, autenticazione a due fattori, e logging avanzato.
  - Richiede una gestione degli incidenti più strutturata e test di penetrazione periodici.
  - Prevede un piano di disaster recovery dettagliato con RPO e RTO definiti.
  - Adatto per dati finanziari o sanitari non sensibili.
  - Introduce controlli di accesso basati sui ruoli e monitoraggio continuo.
- **Livello 3 (AI3/AC3/QC3)** Requisiti avanzati per dati e servizi strategici
  - Il Livello 3 offre protezione per dati altamente sensibili.
  - Implementa crittografia end-to-end e gestione avanzata delle chiavi.
  - Richiede segmentazione di rete avanzata e controlli di accesso granulari.
  - Prevede monitoraggio in tempo reale e risposta automatizzata agli incidenti.
  - Adatto per dati personali sensibili o informazioni strategiche aziendali.
  - Include audit di terze parti regolari e gestione del rischio continua.
- **Livello 4 (AI4/AC4/QC4)** Requisiti massimi di sicurezza e affidabilità
  - Il Livello 4 rappresenta il massimo livello di protezione.
  - Implementa misure di sicurezza all'avanguardia come l'uso di hardware security modules (HSM) e tecniche di obfuscation avanzate.
  - Richiede isolamento fisico e logico completo.
  - Prevede ridondanza geografica e failover automatico.
  - Adatto per dati critici per la sicurezza nazionale o segreti industriali di alto valore.
  - Include simulazioni di attacco regolari e revisioni di sicurezza continue.



7. Requisiti per ciascun livello

- Caratteristiche dei servizi
  - Disponibilità e continuità operativa – La disponibilità aumenta progressivamente, da un uptime base a una disponibilità 24/7 con zero downtime pianificato
  - Performance e scalabilità – Le performance scalano da capacità fisse a risorse elastiche on-demand
  - Interoperabilità e portabilità
    - L'interoperabilità evolve da formati standard a API aperte e documentate.
    - La portabilità progredisce da backup esportabili a migrazione completa senza interruzioni.
- Certificazioni richieste
  - ISO 9001, ISO/IEC 27001, ISO 22301
    - ISO 9001 assicura qualità dei processi, richiesta per tutti i livelli.
    - ISO/IEC 27001 per la sicurezza delle informazioni è obbligatoria dal Livello 2 in su.
    - ISO 22301 per la continuità operativa è necessaria per Livelli 3 e 4
  - Certificazioni specifiche per ciascun livello
    - Certificazioni specifiche come CSA STAR o FedRAMP possono essere richieste per livelli superiori.
    - Le certificazioni devono essere mantenute e rinnovate regolarmente.
- Requisiti di sicurezza aggiuntivi
  - Crittografia e gestione delle chiavi – La crittografia evolve da base a avanzata, con gestione delle chiavi sempre più sofisticata.
  - Monitoraggio e logging – Il monitoraggio passa da reattivo a proattivo, con analisi in tempo reale e intelligenza artificiale.
  - Gestione degli incidenti
    - La gestione degli incidenti progredisce da procedure base a centri operativi di sicurezza 24/7.
    - Si aggiungono requisiti come la sicurezza della supply chain e la protezione contro minacce avanzate persistenti (APT).

8. Monitoraggio e controllo

- Audit e verifiche
  - Pianificazione degli audit – La pianificazione va da annuale a trimestrale per livelli superiori
  - Metodologie di verifica – Le metodologie includono revisioni documentali, interviste, test tecnici e simulazioni di incidenti. Il reporting deve essere dettagliato e tempestivo.
  - Reporting e follow-up
    - Il follow-up verifica la correzione delle non conformità.
    - Per livelli superiori, si richiedono audit di terze parti indipendenti e valutazioni di vulnerabilità continue.
- Gestione delle non conformità
  - Processo di segnalazione – Il processo di segnalazione deve essere chiaro e accessibile, con canali multipli.
  - Azioni correttive – Le azioni correttive vanno pianificate e implementate entro tempi definiti, più stretti per livelli superiori.
  - Revoca della qualificazione o dichiarazione di inadeguatezza
    - La revoca della qualificazione è l'ultima risorsa, preceduta da avvisi e periodi di correzione.
    - Si mantiene un registro delle non conformità per identificare tendenze e migliorare continuamente.

9. Protezione dei dati personali

- Ruoli e responsabilità
  - Titolare del trattamento – Il titolare (PA) determina finalità e mezzi del trattamento
  - Responsabile del trattamento – Il responsabile (provider cloud) tratta i dati per conto del titolare.
  - Incaricati del trattamento – Gli incaricati sono le persone autorizzate a compiere operazioni di trattamento.
  - *Questa struttura assicura che ogni parte coinvolta comprenda le proprie responsabilità legali e operative nella gestione dei dati personali, garantendo conformità al GDPR e altre normative sulla privacy.*

Misure di sicurezza

- Pseudonimizzazione e cifratura
  - La pseudonimizzazione rende i dati non direttamente attribuibili a un individuo senza informazioni aggiuntive.
  - La cifratura protegge i dati da accessi non autorizzati.
- Garanzia di riservatezza, integrità, disponibilità e resilienza – La garanzia di riservatezza, integrità, disponibilità e resilienza assicura che i dati siano protetti, accurati, accessibili quando necessario e resistenti a incidenti.
- Procedure di ripristino – Le procedure di ripristino permettono di recuperare rapidamente i dati in caso di incidenti.

10. Disposizioni transitorie

- Valutazione del pregresso
  - Il regolamento prevede disposizioni per gestire la transizione dal vecchio al nuovo sistema.
  - Le infrastrutture dei servizi cloud e i servizi cloud che hanno ottenuto una qualifica valida prima dell'applicazione del nuovo regolamento mantengono tale qualifica con lo stesso livello e scadenza.
  - Gli elenchi dei dati e servizi e i piani di migrazione trasmessi prima dell'adozione del nuovo regolamento rimangono validi.
  - Questo approccio assicura continuità e riduce il carico amministrativo durante la transizione.
- Tempistiche di adeguamento
  - Scadenze per l'adeguamento delle infrastrutture e dei servizi – Gli operatori di infrastrutture digitali e i fornitori di servizi cloud hanno tempo fino al **18 ottobre 2024** per completare l'adeguamento, se hanno dichiarato di essere in corso di adeguamento.
  - Periodo di grazia per le PA – Questo periodo permette agli operatori di allinearsi ai nuovi requisiti senza interruzioni di servizio. Le PA beneficiano di un periodo di transizione per aggiornare i loro piani e contratti in conformità con il nuovo regolamento.

11. Allegati tecnici

- **Allegato 1:** Modalità per la predisposizione dell'elenco e della classificazione dei dati e dei servizi
  - Linee guida per la classificazione
  - Processi di aggiornamento
  - *L'Allegato 1 fornisce istruzioni dettagliate su come le PA devono classificare i loro dati e servizi. Include modelli e criteri per determinare se un dato o servizio è ordinario, critico o strategico. Questo allegato è cruciale per garantire una classificazione coerente in tutte le PA, facilitando così la corretta applicazione dei livelli di sicurezza.*
- **Allegato 2:** Livelli minimi di sicurezza per le infrastrutture
  - Requisiti di sicurezza fisica e logica
  - Parametri di performance e affidabilità
  - *Questo allegato definisce in dettaglio i requisiti tecnici che le infrastrutture devono soddisfare per ciascun livello di adeguamento (AI1-AI4). Include specifiche su sicurezza fisica, controlli di accesso, capacità di elaborazione, efficienza energetica e continuità operativa. È essenziale per gli operatori di infrastrutture per comprendere e implementare le misure necessarie.*
- **Allegato 3:** Caratteristiche dei servizi cloud
  - Requisiti di qualità, sicurezza e performance
  - Criteri di interoperabilità e portabilità
  - *L'Allegato 3 si concentra sui requisiti specifici per i servizi cloud. Definisce le caratteristiche che i servizi devono possedere in termini di disponibilità, scalabilità, sicurezza dei dati e facilità di migrazione. Questi criteri sono fondamentali per garantire che i servizi cloud siano affidabili, sicuri e adatti alle esigenze delle PA.*
- **Allegato 4:** Requisiti per l'adeguamento e la qualificazione
  - Criteri dettagliati per ciascun livello di adeguamento/qualificazione
  - Processi di verifica e mantenimento
  - *Questo allegato è il cuore tecnico del regolamento, fornendo i requisiti dettagliati per ogni livello di adeguamento (AI1-AI4) e qualificazione (AC1-AC4, QC1-QC4). Include checklist, metriche e processi di verifica. È essenziale per fornitori e operatori per comprendere esattamente cosa è necessario per ottenere e mantenere un determinato livello di adeguamento o qualificazione.*

12. Implicazioni pratiche per le PA

- Verifica dei contratti esistenti
  - Confronto con i requisiti degli allegati
    - verifica di aspetti come backup, disaster recovery, tempi di risposta in assistenza, accesso ai dati, e SLA di servizio.
    - È consigliabile coinvolgere personale qualificato o consulenti esterni per questa valutazione.
  - Identificazione di eventuali gap
    - È consigliabile coinvolgere personale qualificato o consulenti esterni per questa valutazione.
    - L'obiettivo è identificare eventuali discrepanze tra i contratti attuali e i nuovi standard richiesti.
- Verifica e aggiornamento piano di migrazione
  - PA che **hanno** avuto accesso all'avviso 1.2 Cloud.
    - Integrare il piano di migrazione con ulteriori servizi da migrare.
  - PA che **NON hanno** avuto accesso all'avviso 1.2 Cloud
    - Registrarsi e accedere al portale PaDigitale2026
    - Compilare il piano di migrazione

PIANO DI MIGRAZIONE

Compila il piano di migrazione al cloud per la tua PA. Il piano di migrazione al cloud si intende compilato e assolto se hai già inviato una candidatura 1.2. Se hai già inviato una candidatura 1.2 e la tua amministrazione ha ulteriori servizi da migrare, puoi compilare un'integrazione al piano di migrazione.

Nome	Data di invio	Data esito	Stato	Azioni
Piano di migrazione (da candidatura 1.2) - Comune di	02/08/2022	07/08/2023	CONVALIDATO	

Vuoi integrare il piano di migrazione?

- Pianificazione degli adeguamenti
  - Sviluppo di roadmap per l'allineamento ai nuovi requisiti
    - Basandosi sull'analisi dei gap, le PA devono sviluppare piani dettagliati per allinearsi ai nuovi requisiti.
    - Questo potrebbe includere l'upgrade di servizi, la rinegoziazione di contratti, o la migrazione a nuovi fornitori.
  - Gestione del budget e delle risorse – È importante considerare l'impatto sul budget e sulle risorse umane, pianificando adeguatamente per eventuali costi aggiuntivi o necessità di formazione del personale.
- Monitoraggio continuo e reporting
  - Implementazione di processi di verifica periodica
    - Le PA devono istituire processi interni per il monitoraggio continuo della conformità ai nuovi standard.
    - Questo include la verifica regolare dei livelli di servizio, la sicurezza dei dati e l'efficacia delle misure di continuità operativa.
  - Preparazione per audit e controlli – È importante preparare documentazione adeguata per eventuali audit da parte dell'ACN o di altri enti di controllo, dimostrando l'aderenza continua ai requisiti del regolamento.