5 domande sul futuro digitale di ogni Comune

Dopo il PNRR, le priorità del 2027 per mantenere il controllo strategico sulla propria evoluzione digitale.

aruba.it



INTRODUZIONE

Da oltre trent'anni, insieme al Paese digitale

Da oltre trent'anni Aruba cresce insieme all'Italia digitale. Dall'accesso a Internet ai siti web e alla posta elettronica, dalla PEC e dalle firme digitali fino al cloud, ai data center, alla cybersecurity e oggi all'Intelligenza Artificiale, il nostro percorso ha accompagnato l'evoluzione delle esigenze di cittadini, imprese e Pubbliche Amministrazioni.
In questi anni è cresciuta anche la nostra responsabilità. Servizi diventati parte della vita quotidiana richiedono infrastrutture solide, competenze specialistiche e la capacità di sostenerne il funzionamento nel tempo.

In un certo senso, **il nostro primo grande cliente è stata Aruba stessa**. Gestire ogni giorno milioni di clienti, grandi volumi di transazioni e processi complessi ci ha portato ad affrontare direttamente le sfide della continuità operativa, della sicurezza, della crescita e della gestione dei dati. L'esperienza che mettiamo al servizio delle organizzazioni nasce anche da ciò che abbiamo costruito e verificato al nostro interno.
Abbiamo continuato a investire in infrastrutture proprietarie, tecnologie e persone, mantenendo una forte identità italiana e una visione europea. Su queste fondamenta lavoriamo insieme a clienti e partner per costruire servizi capaci di rispondere a esigenze diverse e di evolvere quando cambiano le priorità.

Per i Comuni, questa capacità ha un significato concreto. Il digitale sostiene il rapporto quotidiano tra amministrazione e cittadini: una pratica da presentare, un pagamento da effettuare, una comunicazione da ricevere, un documento da reperire. Dietro ciascuna di queste attività devono esserci servizi affidabili e responsabilità chiare.

Aruba vuole contribuire mettendo a disposizione le proprie fondamenta tecnologiche e l'esperienza maturata nel tempo, insieme agli enti e ai partner che ne conoscono applicazioni e processi, con un obiettivo preciso: rafforzare la capacità del Comune di governare le proprie scelte.

Accompagnare il Paese digitale significa sostenere, ogni giorno, i servizi sui quali cittadini e comunità fanno affidamento.

Stefano Sordi - Direttore Generale, Aruba

Perché questo documento

Negli ultimi anni il PNRR ha permesso a tutta la PA italiana, dalle amministrazioni centrali ai Comuni, di accelerare la trasformazione digitale e, in molti casi, di avviarla.
Con la fine dei fondi, gli enti devono consolidare quanto realizzato in un contesto complesso: un'Europa in profonda trasformazione e una congiuntura economica difficile da gestire.

A questi cambiamenti si sommano due tendenze.

I cittadini sono sempre più abituati ai servizi digitali e se li aspettano anche dal proprio Comune. Nello stesso tempo il personale comunale si riduce: secondo diverse analisi, negli ultimi quindici anni i Comuni italiani hanno perso circa un quarto dei dipendenti, e nei prossimi anni un'ulteriore quota consistente lascerà il servizio, per pensionamento o dimissioni.

In questo scenario il digitale è un'opportunità di trasformazione e, insieme, la leva per continuare a erogare servizi con meno persone, sfruttando le nuove tecnologie.

Le scelte da fare riguardano gli strumenti: quale prodotto, con quali caratteristiche, a quali costi. E riguardano soprattutto la strategia: come essere certi di operare in sicurezza e nel rispetto delle norme? Come conservare la libertà di cambiare in futuro? Come mantenere il controllo strategico del nostro ecosistema digitale oggi e tra due, cinque, dieci anni?

Sono domande che toccano il cuore del lavoro del Comune, oltre agli strumenti con cui lo svolge.
Per trovare soluzioni adatte, il primo passo è porsi le domande giuste e scegliere i partner con cui affrontare il percorso.

Questo documento propone cinque domande da condividere tra amministratori, dirigenti e responsabili della transizione digitale.
Per governare queste scelte occorre sapere quali risultati chiedere, chi ne risponde e come verificarli, senza entrare in ogni dettaglio tecnico.

Il percorso tiene conto delle risorse dei piccoli Comuni e della collaborazione tra enti, nel quadro del Piano triennale per l'informatica nella PA, delle piattaforme nazionali e delle regole di ACN e AgID.

L'obiettivo è aprire la conversazione e mettere a fuoco i punti da affrontare già nel 2027, senza pretese di esaustività.

Buona lettura.

Le cinque domande

1

DOPO IL PNRR, COME MANTENIAMO SERVIZI DIGITALI CHE FUNZIONANO, CON **COSTI SOSTENIBILI** PER IL COMUNE?

2

SE UN ATTACCO INFORMATICO BLOCCA I SISTEMI DEL COMUNE, COME CONTINUIAMO A GARANTIRE I **SERVIZI ESSENZIALI** AI CITTADINI?

3

I DATI RESTANO SOTTO IL **NOSTRO CONTROLLO**? E POSSIAMO CAMBIARE FORNITORE SENZA BLOCCARE IL COMUNE?

4

COME PUÒ L'AI AIUTARE GLI UFFICI A LAVORARE MEGLIO, **PROTEGGENDO I DATI** DEI CITTADINI E LASCIANDO ALLE PERSONE LA RESPONSABILITÀ DELLE DECISIONI?

5

COME ASSICURIAMO CHE ATTI, COMUNICAZIONI E DOCUMENTI SIANO **VALIDI**, **REPERIBILI** E **VERIFICABILI** NEL TEMPO?

Sommario

01 | **Sostenibilità dei servizi** 6

02 | **Resilienza cyber** 8

03 | **Controllo dei dati** 10

04 | **AI utile e governata** 12

05 | **Fiducia digitale** 14

06 | **Scheda di lavoro – Le quindici verifiche** 16

07 | **Perché Aruba** 18

CAPITOLO 01

Sostenibilità dei servizi

Dopo il PNRR, come manteniamo servizi digitali che funzionano, con costi sostenibili per il Comune?

Il successo del PNRR si misura anche nella capacità di mantenere i servizi utili, affidabili e sostenibili nel tempo.

Per un Comune, mantenere un servizio digitale significa consentire a cittadini e imprese di presentare una pratica, effettuare un pagamento o ricevere una risposta, con costi che il bilancio possa sostenere. **Una migrazione completata o una piattaforma attivata acquistano valore quando cittadini e uffici possono utilizzarle in modo semplice, affidabile e continuativo**.

Un servizio digitale deve essere utilizzabile anche da chi ha minori competenze o incontra difficoltà di accesso. La qualità si misura nella possibilità di completare la pratica, con percorsi semplici e assistenza quando serve.

Molti servizi attivati con il PNRR dialogano con le piattaforme nazionali: pagamenti con pagoPA, messaggi su App IO, notifiche con SEND, anagrafe su ANPR, scambio di dati attraverso PDND.

Mantenere un servizio significa anche mantenere queste integrazioni quando cambiano versioni, regole o fornitori applicativi. Il contratto deve indicare chi se ne occupa.

Dopo la migrazione, l'attenzione si sposta sulla gestione: quali sistemi affidare a quale infrastruttura, con quali responsabilità e con quale livello di controllo.
Il Comune deve conoscere chi gestisce gli aggiornamenti, chi monitora le prestazioni e chi interviene quando il servizio peggiora.

Affidare un sistema all'esterno richiede una catena di responsabilità chiara tra ente, provider e fornitore applicativo.

Il costo va considerato lungo il ciclo di vita: risorse cloud, licenze, assistenza, integrazioni, manutenzione e competenze. Un canone iniziale conveniente può accompagnarsi a spese variabili o attività escluse.

Il Comune deve poter collegare il budget al servizio che intende assicurare e comprendere cosa succede quando crescono utilizzo e volumi di dati. La sostenibilità riguarda anche le persone: procedure documentate e supporto adeguato riducono la dipendenza da un singolo dipendente o referente.

Un approccio utile è la componibilità: introdurre o sostituire componenti senza rifare ogni volta l'intero sistema. L'ente può far convivere gli strumenti esistenti con nuove capacità, mantenendo comprensibili integrazioni e responsabilità.

L'affidabilità va verificata attraverso livelli di servizio, monitoraggio e gestione delle anomalie; l'utilità attraverso tempi di lavorazione, passaggi evitati e qualità dell'esperienza di cittadini e uffici. Il numero di servizi migrati, da solo, non descrive questi risultati.

Domanda 1

DOPO IL PNRR, COME MANTENIAMO SERVIZI DIGITALI CHE FUNZIONANO, CON COSTI SOSTENIBILI PER IL COMUNE?

PER I COMUNI PIÙ PICCOLI

Con un solo referente, la priorità è avere tutto scritto e reperibile: contratti, scadenze, contatti dei fornitori e costi annui dei servizi in un unico documento aggiornato.

Acquistare servizi insieme ad altri Comuni dell'Unione o del territorio può consentire economie di scala e una migliore condivisione delle competenze.

TRE VERIFICHE DA FARE

- Conosciamo il costo complessivo dei servizi per i prossimi tre anni, comprese le attività escluse?
- Sono definiti livelli di servizio, responsabili e modalità di escalation, anche per le integrazioni con le piattaforme nazionali?
- Misuriamo se cittadini e imprese riescono a completare le pratiche, quanto tempo risparmiano e dove incontrano difficoltà?

IL CONTRIBUTO DI ARUBA

Aruba costruisce e gestisce direttamente le infrastrutture su cui eroga i servizi cloud, con un'offerta per la PA che comprende servizi qualificati ACN fino a QC3. La scelta del servizio, i livelli di assistenza e i costi di gestione si definiscono rispetto alle esigenze dell'ente. Il Comune e i suoi partner applicativi possono così consolidare i servizi esistenti e pianificarne l'evoluzione. Le infrastrutture sono alimentate da energia rinnovabile, in parte prodotta da impianti del Gruppo, un elemento che contribuisce alla sostenibilità del modello infrastrutturale.

APPROFONDISCI

Governare la complessità digitale con il cloud europeo · Dal cambiamento alla scelta

Leggi il paper principale

CAPITOLO 02

Resilienza cyber

Se un attacco informatico blocca i sistemi del Comune, come continuiamo a garantire i servizi essenziali ai cittadini?

La resilienza si dimostra nella capacità di continuare a servire i cittadini e di ripristinare ciò che si è interrotto. Un attacco può fermare le pratiche, impedire agli uffici di consultare informazioni e lasciare i cittadini senza risposte. Per l'amministrazione, la priorità è sapere quali servizi mantenere e come organizzare la risposta; per i tecnici, tradurre queste priorità in protezione e recupero dei sistemi.

La cybersecurity parte quindi dall'impatto sul servizio pubblico e coinvolge responsabilità amministrative, organizzative e tecniche.

La resilienza collega prevenzione, rilevamento, risposta e recupero. Per il Comune significa conoscere sistemi e accessi, ridurre le vulnerabilità, formare il personale e organizzare la gestione delle anomalie.

La protezione deve comprendere anche i servizi esternalizzati: un problema di un fornitore può interrompere un procedimento pur lasciando funzionanti i sistemi interni.

Una copia di backup è necessaria. Per sapere se gli uffici possono davvero riprendere a lavorare occorre verificare dati, configurazioni, accessi e dipendenze applicative.

Prima dell'emergenza vanno stabiliti l'ordine di ripristino, il tempo di indisponibilità tollerabile e la quantità di dati che può essere necessario recuperare o ricostruire. I test devono produrre risultati utilizzabili per migliorare il piano.

Durante la crisi servono un coordinamento riconoscibile e contatti disponibili anche se posta e sistemi ordinari non funzionano. Chi autorizza le azioni? Chi coordina i fornitori? Come si informano uffici e cittadini?

Comune e partner devono preparare insieme la risposta e le eventuali modalità temporanee di erogazione dei servizi. È utile chiedere evidenze di funzionamento dei controlli, oltre alle procedure scritte.

La Legge 90/2024 prevede specifici adempimenti di cybersicurezza per determinate amministrazioni, incluse alcune categorie di enti locali. Ambito soggettivo, procedure e termini di segnalazione degli incidenti devono essere verificati rispetto alle disposizioni e alle indicazioni ACN applicabili al singolo ente, aggiornate alla data di pubblicazione.

Il D.Lgs. 138/2024, che recepisce la direttiva NIS2, rafforza gli obblighi di gestione del rischio e di sicurezza della catena di fornitura per i soggetti che rientrano nel relativo ambito di applicazione.
Non tutti i Comuni sono automaticamente soggetti ai medesimi obblighi: occorre verificare il perimetro applicabile. Anche per gli enti non inclusi, restano utili procedure chiare per la gestione degli incidenti e il coordinamento con i fornitori.

Domanda 2

SE UN ATTACCO INFORMATICO BLOCCA I SISTEMI DEL COMUNE, COME CONTINUIAMO A GARANTIRE I SERVIZI ESSENZIALI AI CITTADINI?

PER I COMUNI PIÙ PICCOLI

Un piccolo ente difficilmente disporrà di un presidio di sicurezza dedicato. Può però stabilire in anticipo quali servizi devono ripartire, conservare i contatti di emergenza su un canale esterno ai sistemi comunali e chiedere ai fornitori una prova di ripristino documentata.
Nell'Unione una figura di riferimento per la sicurezza è una soluzione organizzativa praticabile.

TRE VERIFICHE DA FARE

- Abbiamo identificato i servizi da ripristinare per primi e le modalità temporanee da attivare?
- Abbiamo effettuato una prova di recupero completo e ne conosciamo data, risultato e tempi?
- Esiste un piano con ruoli, contatti e canali alternativi condiviso con i fornitori?

IL CONTRIBUTO DI ARUBA

Aruba mette a disposizione servizi di protezione, monitoraggio, backup e disaster recovery per affrontare le diverse fasi di un incidente. Con il Comune e i partner applicativi si definiscono servizi inclusi, priorità e modalità di recupero. Il contributo concreto è collegare la difesa dei sistemi alla ripresa del lavoro degli uffici, con responsabilità concordate prima della crisi. Un Security Operations Centre attivo 24 ore su 24 offre servizi gestiti di rilevamento e risposta. Il servizio può affiancare i tecnici e i partner del Comune, con attività e responsabilità definite nel perimetro concordato.

APPROFONDISCI

L'economia dell'integrità · Oltre la compliance · Cybersecurity come controllo strutturale

Leggi il paper principale

CAPITOLO 03

Controllo dei dati

I dati restano sotto il nostro controllo? E possiamo cambiare fornitore senza bloccare il Comune?
Un Comune mantiene il controllo quando può scegliere oggi senza compromettere le scelte di domani.

Se un fornitore aumenta i prezzi o non risponde più alle esigenze del Comune, l'ente deve poter valutare alternative senza compromettere il lavoro degli uffici e il patrimonio informativo. Per farlo deve sapere dove i dati vengono conservati ed elaborati, chi può accedervi e come recuperarli. La collocazione geografica conta insieme alla giurisdizione, alle modalità di amministrazione e alle dipendenze tecnologiche.

Il controllo strategico è la capacità di governare ed evolvere l'ambiente digitale mantenendo autonomia sulle scelte. Per il Comune questo significa rendere visibili le dipendenze rilevanti, senza dover possedere ogni tecnologia, valutarne l'impatto e predisporre alternative proporzionate alla criticità dei servizi. La domanda è cosa accade se una componente diventa indisponibile, troppo costosa o inadatta alle nuove esigenze.

La libertà di cambiare fornitore va esaminata prima di sottoscrivere un contratto. Occorre conoscere quali dati e configurazioni siano esportabili, in quali formati, con quale assistenza e in quali tempi. Un archivio scaricabile può essere insufficiente se mancano relazioni tra dati, documentazione o strumenti per ricostruire il servizio. La valutazione deve comprendere anche applicazioni, licenze e integrazioni: la portabilità dell'infrastruttura non elimina automaticamente i vincoli degli altri livelli.
Standard aperti, interoperabilità e architetture modulari aiutano il Comune a introdurre nuove funzioni o sostituire componenti preservando il lavoro già svolto.
La reversibilità deve essere concretamente praticabile: vanno stimati tempi, attività, costi e impatto sui servizi. Contratti e architettura devono sostenere la stessa possibilità di scelta.

La PDND offre un esempio concreto di interoperabilità: gli enti scambiano dati attraverso interfacce comuni e regole condivise. Lo stesso principio vale per i sistemi interni del Comune, che restano governabili quando dati e funzioni sono accessibili attraverso interfacce documentate.

I DATI RESTANO SOTTO IL NOSTRO CONTROLLO? E POSSIAMO CAMBIARE FORNITORE SENZA BLOCCARE IL COMUNE?

Domanda_3

PER I COMUNI PIÙ PICCOLI

Un ente con poche persone può partire da un elenco essenziale: quali servizi usa, quale fornitore li gestisce, dove stanno i dati e come se ne ottiene una copia completa.

Valutare insieme ad altri Comuni dell'Unione le condizioni di uscita dai contratti più importanti rafforza anche la posizione negoziale.

TRE VERIFICHE DA FARE

- Conosciamo localizzazione dei dati, accessi privilegiati e soggetti coinvolti nella gestione?
- Dati, configurazioni e documentazione sono recuperabili e riutilizzabili altrove?
- Abbiamo valutato un percorso di uscita con tempi, costi e dipendenze applicative?

IL CONTRIBUTO DI ARUBA

Le infrastrutture europee di Aruba, gli ambienti ibridi e l'impiego di tecnologie aperte offrono una base per integrare ed evolvere i servizi.

Per ogni soluzione si definiscono localizzazione dei dati, accessi, modalità di esportazione e condizioni di transizione. Il Comune può così valutare le proprie dipendenze e mantenere la libertà di evolvere e cambiare fornitore.

APPROFONDISCI

Dal cambiamento alla scelta · Governare la complessità digitale con il cloud europeo

Leggi il paper principale

CAPITOLO 04

AI utile e governata

Come può l'AI aiutare gli uffici a lavorare meglio, proteggendo i dati dei cittadini e lasciando alle persone la responsabilità delle decisioni?

L'AI è utile quando migliora un'attività e il Comune mantiene il controllo su dati, accessi, risultati e responsabilità.

Per gli uffici, il valore dell'AI può essere ritrovare più rapidamente una disposizione, estrarre informazioni da una pratica o preparare una prima risposta da verificare. Il beneficio atteso è liberare tempo per il lavoro amministrativo e il rapporto con i cittadini.

Si parte da un'attività circoscritta, misurando tempo, errori e qualità dei risultati prima di estendere l'utilizzo.

Prima di usare il sistema, il Comune deve comprendere quali dati riceva, dove vengano elaborati e conservati, chi possa accedervi e se possano essere riutilizzati per addestrare modelli.
Anche richieste, allegati e risposte possono contenere informazioni riservate.

Un ambiente dedicato può aiutare a controllare il perimetro, ma richiede comunque regole, autorizzazioni e verifiche coerenti con il caso d'uso.

Per usare l'AI occorre sapere chi gestisce l'infrastruttura, chi fornisce il modello e chi integra il sistema nel lavoro degli uffici. Le responsabilità devono essere chiare lungo tutto il percorso.

Il controllo deve seguire il dato fino alla risposta mostrata all'operatore.

Un assistente deve rispettare i permessi già previsti per l'utente. Le risposte devono poter essere controllate, corrette e ricondotte alle fonti quando il caso d'uso lo richiede.

Il Comune deve definire chi verifica gli esiti e come interrompere l'utilizzo quando la qualità è insufficiente.
Il passaggio all'uso quotidiano richiede inoltre di misurare costi, prestazioni e affidabilità.

Un'architettura modulare permette di aggiornare modelli e strumenti senza vincolare l'intero servizio a una scelta iniziale.

La Legge 132/2025 stabilisce che nella pubblica amministrazione l'AI è uno strumento di supporto: la decisione resta alla persona che ne risponde. I documenti AgID su adozione, sviluppo e acquisto di sistemi di IA offrono il riferimento operativo.
L'adozione dell'Intelligenza Artificiale deve inoltre tenere conto del quadro europeo definito dal Regolamento (UE) 2024/1689 (AI Act), con particolare attenzione alla classificazione dei rischi, alla supervisione umana e agli obblighi applicabili ai singoli casi d'uso.

Domanda 4

COME PUÒ L'AI AIUTARE GLI UFFICI A LAVORARE MEGLIO, PROTEGGENDO I DATI DEI CITTADINI E LASCIANDO ALLE PERSONE LA RESPONSABILITÀ DELLE DECISIONI?

PER I COMUNI PIÙ PICCOLI

Per un piccolo Comune la strada più sicura è una sperimentazione limitata a un'attività ripetitiva, in un ambiente controllato e con regole d'uso scritte per il personale.

Condividere esperienze, criteri e formazione con altri enti del territorio riduce tempi e rischi.

TRE VERIFICHE DA FARE

- Quale attività vogliamo migliorare e quali risultati, errori e costi misureremo?
- Sappiamo dove vanno dati e richieste, chi vi accede e come possono essere riutilizzati?
- Chi verifica le risposte e come gestiamo permessi, errori e aggiornamenti dei modelli?

IL CONTRIBUTO DI ARUBA

Aruba mette a disposizione capacità di calcolo, ambienti dedicati e piattaforme per utilizzare modelli e strumenti di AI. Queste capacità possono sostenere applicazioni come ricerca documentale ed estrazione delle informazioni, sviluppate con il Comune e i partner. Dati ammessi, permessi, verifica delle risposte e responsabilità si definiscono sul caso d'uso, per portare benefici misurabili al lavoro degli uffici.

APPROFONDISCI

Dal laboratorio alla produzione · Oltre la compliance

Leggi il paper principale

CAPITOLO 05

Fiducia digitale

Come assicuriamo che atti, comunicazioni e documenti siano validi, reperibili e verificabili nel tempo?

La fiducia digitale richiede di poter attribuire, verificare e preservare le azioni e i documenti nel tempo.

Un Comune deve poter ritrovare un atto, verificare una sottoscrizione e dimostrare l'invio o la ricezione di una comunicazione anche quando la pratica è conclusa. Questo tutela la correttezza del procedimento e la fiducia dei cittadini.

Il documento va quindi formato, gestito, trasmesso e conservato insieme alle evidenze necessarie, lungo tutto il suo ciclo di vita.

SEND e il domicilio digitale stanno portando sul digitale una parte crescente delle comunicazioni con valore legale.

PEC, firme e conservazione restano strumenti centrali del procedimento: la loro integrazione con le piattaforme nazionali completa la catena delle evidenze.

Per ogni procedimento il Comune può chiedersi:

- chi ha agito e con quale autorizzazione?
- come è stata formalizzata la sottoscrizione?
- come dimostriamo il momento rilevante, l'invio o la ricezione?
- come preserviamo documento ed evidenze nel tempo?

PEC, firme, marche temporali e conservazione presidiano funzioni differenti.

Un backup sostiene il recupero operativo, mentre la conservazione documentale riguarda la preservazione e la verificabilità nel tempo secondo le regole applicabili.

Il percorso deve collegare documenti, metadati, ricevute e registrazioni pertinenti.
Servizi acquistati separatamente possono funzionare bene, ma è la loro integrazione nei procedimenti a rendere completa la catena delle evidenze.

La fiducia riguarda anche gli accessi: credenziali, ruoli, deleghe e revoche devono riflettere le responsabilità effettive. Questo vale per dipendenti, fornitori e sistemi automatici che operano nei processi.

L'evoluzione verso identità e wallet europei richiede preparazione e interoperabilità, distinguendo ciò che è disponibile dagli sviluppi futuri.

Standard, qualificazione e specifici effetti giuridici devono essere verificati per il servizio utilizzato.

COME ASSICURIAMO CHE ATTI, COMUNICAZIONI E DOCUMENTI SIANO VALIDI, REPERIBILI E VERIFICABILI NEL TEMPO?

PER I COMUNI PIÙ PICCOLI

Anche con un solo referente, molti strumenti di fiducia sono già in uso: PEC, firma digitale, protocollo.

Il passo utile è verificare che siano collegati tra loro e con la conservazione, e che deleghe e accessi vengano aggiornati quando cambiano persone e incarichi.

TRE VERIFICHE DA FARE

- Per ogni procedimento sappiamo quali evidenze servono e con quali strumenti produrle?
- Documenti, metadati e ricevute restano reperibili e collegati durante il loro ciclo di vita?
- Accessi, deleghe e revoche sono coerenti con i ruoli e tracciabili?

IL CONTRIBUTO DI ARUBA

PEC, firme digitali, servizi di identità, marche temporali e conservazione consentono ad Aruba di contribuire ai diversi passaggi del procedimento. Integrati con i sistemi dell'ente, aiutano a collegare documenti, sottoscrizioni, ricevute ed evidenze nel tempo.
Il percorso verso i wallet europei si costruisce su questo patrimonio di servizi e competenze.

APPROFONDISCI

L'economia dell'integrità · Oltre la compliance · Il futuro dell'identità digitale e della digital integrity

Leggi il paper principale

Domanda_5

CAPITOLO 06

Le quindici verifiche

Qui accanto le verifiche delle cinque sezioni in un unico strumento, da usare in riunione con segretario comunale, responsabile per la transizione al digitale e fornitori.

Per ogni voce si indica lo stato, chi deve fornire la risposta e il prossimo intervento.

1. SOSTENIBILITÀ DEI SERVIZI

VERIFICA	STATO	CHI DEVE RISPONDERE	PROSSIMO INTERVENTO
Abbiamo stimato il costo complessivo dei servizi per i prossimi tre anni, comprese le attività escluse	☐ VERIFICATO ☐ DA COMPLETARE ☐ DA VERIFICARE		
Sono definiti livelli di servizio, responsabili e modalità di escalation, anche per le integrazioni con le piattaforme nazionali	☐ VERIFICATO ☐ DA COMPLETARE ☐ DA VERIFICARE		
Misuriamo se cittadini e imprese riescono a completare le pratiche, quanto tempo risparmiano e dove incontrano difficoltà	☐ VERIFICATO ☐ DA COMPLETARE ☐ DA VERIFICARE		

2. RESILIENZA CYBER

VERIFICA	STATO	CHI DEVE RISPONDERE	PROSSIMO INTERVENTO
Abbiamo identificato i servizi da ripristinare per primi e le modalità temporanee da attivare	☐ VERIFICATO ☐ DA COMPLETARE ☐ DA VERIFICARE		
Abbiamo effettuato una prova di recupero completo e ne conosciamo data, risultato e tempi	☐ VERIFICATO ☐ DA COMPLETARE ☐ DA VERIFICARE		
Esiste un piano con ruoli, contatti e canali alternativi condiviso con i fornitori	☐ VERIFICATO ☐ DA COMPLETARE ☐ DA VERIFICARE		

3. CONTROLLO DEI DATI

VERIFICA	STATO	CHI DEVE RISPONDERE	PROSSIMO INTERVENTO
Conosciamo localizzazione dei dati, accessi privilegiati e soggetti coinvolti nella gestione	☐ VERIFICATO ☐ DA COMPLETARE ☐ DA VERIFICARE		
Dati, configurazioni e documentazione sono recuperabili e riutilizzabili altrove	☐ VERIFICATO ☐ DA COMPLETARE ☐ DA VERIFICARE		
Abbiamo valutato un percorso di uscita con tempi, costi e dipendenze applicative	☐ VERIFICATO ☐ DA COMPLETARE ☐ DA VERIFICARE		

4. AI UTILE E GOVERNATA

VERIFICA	STATO	CHI DEVE RISPONDERE	PROSSIMO INTERVENTO
Abbiamo scelto l'attività da migliorare e definito risultati, errori e costi da misurare	☐ VERIFICATO ☐ DA COMPLETARE ☐ DA VERIFICARE		
Sappiamo dove vanno dati e richieste, chi vi accede e come possono essere riutilizzati	☐ VERIFICATO ☐ DA COMPLETARE ☐ DA VERIFICARE		
Abbiamo definito chi verifica le risposte e come gestire permessi, errori e aggiornamenti dei modelli	☐ VERIFICATO ☐ DA COMPLETARE ☐ DA VERIFICARE		

5. FIDUCIA DIGITALE

VERIFICA	STATO	CHI DEVE RISPONDERE	PROSSIMO INTERVENTO
Per ogni procedimento sappiamo quali evidenze servono e con quali strumenti produrle	☐ VERIFICATO ☐ DA COMPLETARE ☐ DA VERIFICARE		
Documenti, metadati e ricevute restano reperibili e collegati durante il loro ciclo di vita	☐ VERIFICATO ☐ DA COMPLETARE ☐ DA VERIFICARE		
Accessi, deleghe e revoche sono coerenti con i ruoli e tracciabili	☐ VERIFICATO ☐ DA COMPLETARE ☐ DA VERIFICARE		

CAPITOLO 07

Perché Aruba

CINQUE CONDIZIONI PER UNA SCELTA CONSAPEVOLE

Le cinque domande aiutano il Comune a definire le proprie priorità. Queste condizioni aiutano a valutare il contributo di Aruba come partner tecnologico, insieme ai fornitori applicativi e alle competenze dell'ente.

1. Fondamenta italiane e governo europeo

Aruba progetta, costruisce e gestisce direttamente infrastrutture proprietarie in Italia, all'interno di un gruppo italiano. Per il Comune significa poter valutare con chiarezza localizzazione, gestione e responsabilità delle fondamenta digitali.

> 8 DATA CENTER PROPRIETARI IN EUROPA, TRA ITALIA E REPUBBLICA CECA, CON I CAMPUS ITALIANI DI AREZZO, PONTE SAN PIETRO E ROMA, PROGETTATI E GESTITI DAL GRUPPO. IL CAMPUS DI PONTE SAN PIETRO È NATO DALLA RIGENERAZIONE DELL'AREA INDUSTRIALE EX LEGLER.

2. Servizi qualificati per la PA

Le qualificazioni ACN dei servizi cloud e la presenza negli accordi Consip pertinenti offrono riferimenti concreti per la selezione e l'acquisto. Il livello di qualificazione si sceglie in base alla classificazione dei dati e dei servizi del Comune.

> HOSTED PRIVATE CLOUD E VIRTUAL PRIVATE CLOUD SONO QUALIFICATI ACN QC3 E ACQUISTABILI TRAMITE L'ACCORDO QUADRO CONSIP PER SERVIZI IAAS E PAAS.

3. Un insieme coerente di competenze

Data center, cloud, connettività, cybersecurity e servizi fiduciari consentono di affrontare le esigenze digitali lungo più livelli. Il valore per il Comune è rendere coerenti infrastruttura, sicurezza e fiducia, definendo il ruolo di Aruba e quello dei partner.

> IL PORTAFOGLIO ARUBA RIUNISCE DATA CENTER, CLOUD, CONNETTIVITÀ, CYBERSECURITY E SERVIZI FIDUCIARI. IL MODELLO PER LA PA DISTINGUE LA RESPONSABILITÀ INFRASTRUTTURALE DI ARUBA DALLE SOLUZIONI SPECIFICHE DELL'ENTE E DEI PARTNER. ARUBA UNISCE IL RUOLO DI CLOUD PROVIDER E QUELLO DI PRESTATORE DI SERVIZI FIDUCIARI QUALIFICATO, ATTRAVERSO ARUBAPEC E ACTALIS.

4. Controllo e libertà di evoluzione

L'approccio Aruba valorizza apertura, interoperabilità e componibilità. Per il Comune questo si traduce nella possibilità di integrare nuovi servizi ed esaminare percorsi di evoluzione o cambio di fornitore.

> L'OFFERTA PER LA PA PREVEDE AMBIENTI IBRIDI E TECNOLOGIE OPEN SOURCE E STANDARD DI MERCATO; ARUBA È MEMBRO DI GAIA-X E SOCIO FONDATORE DI CISPE, ED È TRA I PROMOTORI, CON IONOS E DYNAMO, DI SECA API, SPECIFICA APERTA PER LA GESTIONE DELLE INFRASTRUTTURE CLOUD.

5. Un partner che sostiene il percorso nel tempo

La continuità della collaborazione richiede competenze, supporto e coordinamento con i fornitori applicativi. Per il Comune conta poter individuare interlocutori, responsabilità e modalità di gestione anche dopo l'attivazione dei servizi.

> L'OFFERTA PER LA PA COMPRENDE SERVIZI GESTITI STANDARD O PERSONALIZZATI, SUPPORTO TECNICO E UNA RETE DI PARTNER QUALIFICATI SUL TERRITORIO. LIVELLI DI SERVIZIO, COPERTURA E RESPONSABILITÀ SONO DEFINITI PER LA SOLUZIONE ADOTTATA.

L'INFRASTRUTTURA DI ARUBA

Infrastruttura europea
Aruba serve oltre 200.000 clienti cloud in più di 100 paesi, da 8 cloud region proprietarie distribuite in 6 paesi europei.

La piattaforma cloud, basata su standard aperti, standard Kubernetes e altri progetti open (Liqo, ArubaKube), garantisce la portabilità dei workload tra ambienti Aruba, hyperscaler e on-premise, senza vincoli proprietari.

Integrazione ibrida e qualificazione per il settore pubblico
Multi-Cloud Link e Hybrid Connect offrono connettività diretta e dedicata verso AWS, Azure, Google Cloud e infrastrutture on-premise, con una struttura di costi trasparente.

Aruba Cloud è qualificata per la Pubblica Amministrazione italiana (ACN QC3, Consip) ed è membro del Board di Gaia-X, operando come nodo attivo del Gaia-X Digital Clearing House.

+200K
CLIENTI CLOUD
SERVITI DA ARUBA

8
CLOUD REGION
PROPRIETARIE

+16MLN
UTENTI

8
DATA CENTER
PROPRIETARI
IN EUROPA

aruba.it

Il ruolo di Aruba nell'ecosistema di attori ICT a supporto della PA

La collaborazione fra vendor, provider di servizi infrastrutturali come Aruba e fornitori di servizi professionali è definita da Consip stessa, che ha costruito un framework di accordi quadro e convenzioni dedicati alle diverse categorie di attori. Con la recente attivazione del **lotto Aruba dell'Accordo Quadro Consip per i servizi IaaS e PaaS**, il ruolo di Aruba nell'evoluzione digitale della Pubblica Amministrazione centrale e locale assume una rilevanza strategica nell'ecosistema degli attori ICT. I servizi Aruba mettono a disposizione della PA un set completo di servizi IaaS e PaaS, **qualificati ACN fino al livello 3**, su cui costruire evoluzioni progressive e governabili, costruito su infrastrutture cloud europee sicure e conformi. Questo consente **agli attori ICT abilitati da analoghi accordi quadro e convenzioni Consip per servizi di cloud enabling e di system integration di dispiegare le proprie potenzialità** a un livello ancora più avanzato di quanto è stato possibile finora:

- operando su **fondamenta robuste e certificate**, evitando frammentazioni e soluzioni tattiche;
- contribuendo in modo concreto alla **dematerializzazione e remotizzazione dei processi più complessi e delicati**, preservando sicurezza, continuità e responsabilità istituzionale.

In questo scenario, **Aruba agisce come abilitatore sistemico**, rendendo possibile una collaborazione efficace tra amministrazioni, system integrator e provider di servizi, nel rispetto dei requisiti di sovranità e interesse pubblico.



CONCLUSIONI

Le scelte di oggi, la libertà di evolvere domani

Le cinque domande di questo documento portano a una scelta concreta: a chi affidare le fondamenta digitali del Comune, con quali responsabilità e con quale libertà di evolvere.

È su questo che Aruba vuole essere scelta. Per le infrastrutture che costruisce e gestisce direttamente, per i servizi qualificati destinati alla PA, per le competenze che collegano cloud, sicurezza e fiducia digitale. E per la capacità di lavorare insieme agli enti e ai loro partner, trasformando queste fondamenta in servizi utili ai cittadini.

Il nostro impegno è rendere questo patrimonio accessibile a Comuni con esigenze e risorse diverse. Un piccolo ente e una grande città affrontano complessità differenti, ma condividono la stessa responsabilità: garantire servizi affidabili, proteggere le informazioni e utilizzare bene le risorse pubbliche.

Per questo il rapporto con un partner tecnologico deve durare oltre l'attivazione. Deve offrire interlocutori riconoscibili, competenze disponibili e condizioni chiare. Deve aiutare il Comune a introdurre nuove capacità, integrare ciò che già funziona e cambiare direzione quando serve.

Con Aruba il Comune costruisce un percorso del quale conosce ogni passaggio. Dove risiedono i dati, chi vi accede, come si protegge un servizio, quali tecnologie adottare e come farle evolvere: sono scelte che devono restare comprensibili e governabili.

Vogliamo continuare ad accompagnare il Paese digitale a fianco dei Comuni, perché l'evoluzione raggiunga tutti, ovunque, e ogni territorio possa costruire il proprio futuro.

Il primo passo concreto è utilizzare le quindici verifiche di questa guida per individuare le priorità del Comune. Aruba può affiancare l'ente e i suoi partner nel definire condizioni infrastrutturali, sicurezza, responsabilità e interventi possibili.

Il futuro digitale del Comune si costruisce insieme. Il controllo delle scelte resta al Comune.

Maurizio Pecori - Chief Revenue Officer, Aruba

About Aruba

Aruba, fondata nel 1994, è il Cloud Champion italiano e uno dei principali provider europei di infrastrutture e piattaforme digitali basate su asset proprietari. L'azienda progetta e gestisce l'intero stack tecnologico: dalla progettazione e costruzione di data center alle piattaforme cloud, dai servizi di trust e security alla connettività e alle soluzioni software che supportano strategie digitali e applicazioni basate su AI.

Con capitale interamente italiano, Aruba conta 16 milioni di utenti attivi sulle proprie piattaforme provenienti da oltre 100 nazioni e gestisce un'infrastruttura distribuita su 8 data center in Europa, che ospita oltre 2,7 milioni di domini, 10 milioni di caselle e-mail, 9 milioni di caselle PEC e migliaia di infrastrutture IT di clienti.

Copyright © Aruba. All rights reserved.
Disclaimer: This content is provided for general information purposes and is not intended to be used in place of consultation with our professional advisors.

aruba.it