SYNSPHERE

WHITE PAPER · GIUGNO 2026

Azure sotto controllo: governance e gestione dei costi per le PMI

Sottoscrizioni, tagging, RBAC, policy e FinOps: come usare il cloud Microsoft senza sorprese in bolletta.

In sintesi

Microsoft Azure permette a una PMI di accendere infrastruttura in pochi minuti, ma senza regole il cloud tende a crescere in modo disordinato: risorse dimenticate, costi imprevisti, permessi distribuiti senza criterio. Questo white paper propone un percorso di governance pensato per le piccole e medie imprese italiane: gerarchia di sottoscrizioni e gruppi di risorse, naming e tagging, controllo degli accessi con RBAC, Azure Policy, modelli di costo e pratica FinOps. Tutti i temi sono trattati con taglio operativo, senza prerequisiti enterprise: bastano poche ore al mese e una manciata di strumenti inclusi nella piattaforma. Chiude il documento una roadmap di adozione in novanta giorni con l'automazione PowerShell e una checklist pronta da usare.

Azure sotto controllo: governance e gestione dei costi per le PMI — Prima edizione: giugno 2026.

Indice

1. Perché Azure sfugge di mano nelle PMI

Microsoft Azure ha abbattuto una barriera storica: per avere un server, un database o un sito non servono più ordini d'acquisto, attese di settimane e armadi rack. Bastano un contratto, qualche clic nel portale e la risorsa è accesa. È un vantaggio enorme per una PMI, ma è anche l'origine del problema più comune che si incontra sul campo: il cloud cresce più in fretta della capacità dell'azienda di governarlo. Dopo dodici o diciotto mesi di utilizzo, la fotografia tipica è una sottoscrizione unica dove convivono produzione, test ed esperimenti, con decine di risorse di cui nessuno ricorda il motivo.

Il sintomo più visibile è la bolletta: cresce mese dopo mese senza che il valore percepito cresca allo stesso ritmo. Ma la fattura è solo l'effetto finale. Le cause stanno più a monte e ricorrono con una regolarità impressionante, indipendentemente dal settore e dalla dimensione dell'azienda.

I quattro meccanismi dello sprawl

- **Ambienti di test dimenticati.** Si crea una macchina virtuale per provare una configurazione, il test finisce, la VM resta accesa. Nessuno la spegne perché nessuno sa con certezza se serve ancora a qualcuno.
- **Risorse orfane.** Quando si elimina una VM, dischi gestiti, indirizzi IP pubblici, snapshot e interfacce di rete possono sopravvivere alla cancellazione e continuare a generare costi, invisibili a chi guarda solo l'elenco delle macchine.
- **Assenza di ownership.** Le risorse non hanno un responsabile dichiarato: davanti a un nome criptico come vm-test-2 nessuno se la sente di cancellare, e tutto resta lì per anni.
- **Proof of concept promossi a produzione.** Un esperimento funziona, il business lo adotta, ma nessuno torna indietro a ridisegnare dimensionamento, sicurezza e backup: l'architettura provvisoria diventa definitiva.

C'è poi un quinto fattore, tipico delle migrazioni lift-and-shift: si portano in cloud le macchine virtuali così com'erano on-premises, con lo stesso sovradimensionamento prudenziale di quando l'hardware si comprava ogni cinque anni. In cloud quel margine di sicurezza si paga ogni ora, ventiquattro ore al giorno, weekend compresi.

Il costo non è solo economico. Una risorsa che nessuno governa è anche una risorsa che nessuno aggiorna, che non rientra nei backup e che non viene monitorata: lo sprawl è prima di tutto una superficie di attacco che si allarga in silenzio. Per questo la risposta giusta non è un taglio dei costi una tantum, ma un sistema di regole leggere che impedisca al disordine di riformarsi.

SynSphere lavora su infrastrutture Microsoft dal 2008, e la lezione di oltre dieci anni di progetti è sempre la stessa: la governance costa molto meno se si imposta presto. Le sezioni che seguono descrivono le fondamenta nell'ordine in cui conviene costruirle, con un taglio volutamente pratico e dimensionato sulla realtà di una PMI, non di una multinazionale con un reparto cloud dedicato.

2. Le fondamenta: gerarchia, naming e tag

Azure organizza le risorse su quattro livelli: i gruppi di gestione (management group), le sottoscrizioni, i gruppi di risorse e le risorse vere e proprie. Ogni livello eredita da quello superiore permessi e policy, ed è proprio questa ereditarietà a rendere la gerarchia lo strumento di governance più potente della piattaforma: una regola applicata a un management group vale automaticamente per tutte le sottoscrizioni sottostanti, senza doverla ripetere risorsa per risorsa.

Per una PMI non serve una gerarchia complessa. Uno schema che funziona quasi sempre prevede un management group radice con sotto due o tre sottoscrizioni: una per la produzione, una per i carichi non produttivi (sviluppo, test, collaudo) e, se il team sperimenta spesso, una sandbox con budget rigido dove si può creare liberamente sapendo che tutto verrà ripulito a scadenza. La sottoscrizione è anche il confine naturale di fatturazione: separare produzione e non produzione rende leggibile la bolletta da subito, prima ancora di qualsiasi analisi sofisticata.

I gruppi di risorse vanno pensati per ciclo di vita: tutto ciò che nasce, vive e muore insieme sta nello stesso gruppo. L'applicazione gestionale con il suo database e il suo storage in un gruppo, il sito web in un altro. Così dismettere un progetto significa eliminare un gruppo, senza cacce al tesoro fra risorse sparse.

La naming convention

Un nome ben costruito risponde a tre domande prima ancora di aprire la risorsa: che cos'è, a cosa serve, in che ambiente vive. Il Cloud Adoption Framework di Microsoft suggerisce uno schema a segmenti che conviene adottare quasi alla lettera: tipo di risorsa, carico di lavoro, ambiente, regione, progressivo. Per esempio rg-gestionale-prod-itn-001 per un gruppo di risorse di produzione in Italia Nord, vm-app01-test-weu-001 per una macchina di test in Europa occidentale. L'importante non è trovare lo schema perfetto: è sceglierne uno, scriverlo in una pagina condivisa e non derogare mai, perché ogni eccezione di oggi è un punto interrogativo fra due anni.

Il tagging: i metadati che mancano ai nomi

I tag sono coppie chiave-valore applicabili a sottoscrizioni, gruppi di risorse e risorse. Sono il complemento del naming: il nome dice che cos'è una risorsa, i tag dicono di chi è, chi la paga e fino a quando deve esistere. Attenzione a un dettaglio che sorprende molti: i tag non si ereditano automaticamente dal gruppo di risorse alle risorse contenute. Per propagarli serve una Azure Policy con effetto Modify, di cui parliamo nella sezione 4.

Tag	Scopo	Esempio di valore
env	Distingue produzione, test e sviluppo	prod, test, dev
owner	Responsabile da contattare prima di toccare la risorsa	m.rossi@azienda.it
cost-center	Centro di costo o commessa per il riaddebito interno	IT-2026, COMM-042
project	Progetto o servizio applicativo di appartenenza	gestionale, sito-web
expiry	Data di revisione o dismissione per risorse temporanee	2026-09-30

Con questi cinque tag si copre la quasi totalità dei casi d'uso reali: riaddebito dei costi per centro di costo, individuazione del responsabile prima di uno spegnimento, pulizia periodica delle risorse scadute.

> **Il consiglio SynSphere**
> Partite con quattro o cinque tag obbligatori, non con venti. Un sistema di tagging troppo ambizioso muore in poche settimane perché nessuno lo compila; uno minimale ma applicato con una policy che blocca le risorse non taggate sopravvive da solo. Potrete sempre aggiungere chiavi più avanti: **rimuovere il disordine costa molto più che prevenirlo**.

3. Identità e accessi: RBAC e least privilege

Il controllo degli accessi in Azure si chiama RBAC, role-based access control: a un'identità (utente, gruppo o applicazione) si assegna un ruolo, cioè cosa può fare, su un ambito, cioè dove può farlo. L'ambito può essere un management group, una sottoscrizione, un gruppo di risorse o una singola risorsa, e l'assegnazione si eredita verso il basso. Qui si gioca la differenza fra un cloud ordinato e uno in cui, dopo un anno, metà azienda risulta Owner della sottoscrizione di produzione senza che nessuno sappia dire perché.

Il principio guida è il least privilege: ogni persona riceve il minimo set di permessi necessario al suo lavoro, nell'ambito più ristretto possibile. In pratica, per una PMI, tre regole coprono la maggior parte delle situazioni: i ruoli si assegnano ai gruppi di Microsoft Entra ID e mai ai singoli utenti; il ruolo Owner si concede a pochissime persone e solo dove serve davvero; chi deve solo consultare riceve Reader, non Contributor.

Ruolo integrato	Cosa permette	A chi assegnarlo
Reader	Sola lettura su risorse e configurazioni	Consulenti, auditor, controllo di gestione
Contributor	Crea e modifica risorse, non gestisce i permessi	Tecnici che operano sugli ambienti
Owner	Tutto, inclusa l'assegnazione di ruoli ad altri	Pochissime persone, ambiti limitati
Cost Management Reader	Vede costi e budget senza toccare le risorse	Amministrazione e finance
User Access Administrator	Gestisce solo le assegnazioni di ruolo	Casi particolari, da usare con cautela

La separazione fra ambienti è il secondo pilastro. Chi sviluppa deve poter creare e distruggere liberamente nella sottoscrizione di test, ma in produzione dovrebbe avere al massimo visibilità in lettura: le modifiche all'ambiente di produzione passano da poche persone autorizzate o, meglio ancora, da pipeline automatiche con identità dedicate. Questa semplice asimmetria elimina gran parte degli incidenti da modifica accidentale.

Lo stesso criterio vale per i fornitori esterni: un consulente che deve verificare una configurazione riceve Reader con una scadenza, non Contributor per sempre. E le assegnazioni vanno riviste periodicamente: una revisione trimestrale degli accessi, anche fatta a mano su un foglio di calcolo, intercetta gli account di ex collaboratori e i permessi rimasti attivi oltre la necessità.

Un cenno a PIM

Per chi vuole fare un passo ulteriore, Privileged Identity Management (PIM) di Microsoft Entra consente l'elevazione just-in-time: l'amministratore non è Owner in modo permanente, ma attiva il ruolo solo quando serve, per una finestra temporale limitata, con eventuale approvazione e tracciatura completa. Richiede un livello di licenza Microsoft Entra adeguato, quindi non è il primo investimento da fare; ma quando gli amministratori sono più di due o tre, riduce drasticamente la finestra di esposizione dei privilegi elevati. Nei progetti di governance sui tenant dei clienti, la combinazione di gruppi, ruoli minimi e revisione periodica resta comunque il controllo con il miglior rapporto fra sforzo e beneficio: PIM arriva dopo, non al posto di queste basi.

4. Azure Policy: le regole che si applicano da sole

RBAC stabilisce chi può fare cosa; Azure Policy stabilisce che cosa è consentito fare in assoluto, da chiunque. È la differenza fra consegnare le chiavi e mettere i cartelli stradali: anche chi ha pieni permessi non può creare una risorsa in una regione vietata se una policy lo impedisce. Per una PMI è lo strumento che trasforma le convenzioni scritte su una pagina in vincoli tecnici che non dipendono dalla buona volontà delle persone.

Una policy è una regola valutata su ogni risorsa, esistente o in fase di creazione. Gli effetti principali da conoscere sono quattro: Audit segnala le risorse non conformi senza bloccarle; Deny impedisce la creazione o la modifica non conforme; DeployIfNotExists distribuisce automaticamente configurazioni mancanti, per esempio le impostazioni di diagnostica; Modify corregge proprietà al volo, come l'aggiunta dei tag ereditati dal gruppo di risorse.

Le policy si raggruppano in iniziative (initiative), pacchetti di regole assegnabili in un colpo solo a un management group o a una sottoscrizione. Azure ne offre molte già pronte, incluse baseline di sicurezza allineate alle principali normative; per cominciare, però, bastano poche regole mirate.

- Regioni consentite: solo le aree europee scelte dall'azienda, per controllo dei dati e coerenza dei costi.
- Tag obbligatori alla creazione: senza env, owner e cost-center la risorsa non nasce.
- SKU consentite per le macchine virtuali: si escludono le taglie più costose, che in una PMI raramente hanno una giustificazione.
- Divieto di indirizzi IP pubblici sulle risorse che non devono essere esposte a internet.
- Trasferimento dati solo cifrato: HTTPS obbligatorio su storage account e servizi applicativi.

L'errore da evitare è partire in modalità repressiva. Una policy con effetto Deny applicata di colpo a un ambiente esistente può bloccare operazioni legittime e generare rigetto nel team, che inizierà ad aggirare le regole invece di rispettarle. Il percorso che adottiamo nei progetti di governance è graduale e in quattro passi:

1. Assegnare le policy in modalità Audit e lasciarle lavorare per qualche settimana.
2. Analizzare il report di conformità: ogni non conformità è una scoperta sull'ambiente reale.
3. Sanare l'esistente, con remediation automatiche dove possibile e interventi manuali dove serve.
4. Solo a questo punto passare a Deny sulle nuove risorse, lasciando l'esistente in osservazione.

Per i casi legittimi che non rientrano nelle regole, lo strumento corretto sono le esenzioni: una risorsa specifica viene esclusa dalla valutazione, con una motivazione scritta e idealmente una scadenza. È molto diverso dal disattivare la policy: la regola resta in vigore per tutti, e l'eccezione è documentata e rivedibile invece che invisibile.

Il risultato finale è una dashboard di conformità consultabile in ogni momento: una fotografia oggettiva, aggiornata di continuo, di quanto l'ambiente rispetta le regole che l'azienda stessa si è data. È anche un ottimo strumento da portare in direzione o davanti a un auditor: la conformità smette di essere un'opinione e diventa un numero verificabile, con l'elenco esatto delle eccezioni da motivare.

5. I modelli di costo, spiegati senza listini

Capire come Azure fattura è il prerequisito di qualunque ottimizzazione. In questa sezione non troverete prezzi, che cambiano nel tempo e dipendono dal contratto: troverete i meccanismi, che invece sono stabili e bastano per orientare le decisioni. I modelli da conoscere sono cinque.

Modello	Come funziona	Quando conviene
Pay-as-you-go	Si paga il consumo effettivo, senza impegno	Carichi variabili, test, primi mesi
Reserved Instances	Impegno di 1 o 3 anni, principalmente su una famiglia di VM	VM stabili che girano sempre
Savings Plan	Impegno di spesa oraria sul compute, flessibile	Compute stabile ma eterogeneo
Azure Hybrid Benefit	Riuso di licenze Windows Server e SQL Server	Chi ha licenze con Software Assurance
Tariffe Dev/Test	Condizioni dedicate agli ambienti non produttivi	Sviluppo e collaudo, con i requisiti

Il pay-as-you-go è il punto di partenza naturale: nessun impegno, si paga il consumo effettivo, misurato in modo diverso a seconda del servizio (ore di esecuzione per le VM, spazio occupato e operazioni per lo storage, capacità riservata per i database). È perfetto finché non si conosce il proprio profilo di consumo; diventa il modello più costoso quando i carichi sono stabili e prevedibili.

Per i carichi stabili esistono gli impegni pluriennali, in due varianti. Le Reserved Instances riservano una specifica famiglia di macchine virtuali in una specifica regione per uno o tre anni: lo sconto è massimo, la flessibilità minima. I Savings Plan impegnano invece una spesa oraria sul compute in generale: lo sconto è inferiore, ma l'impegno segue i carichi anche se nel frattempo cambiate taglia o regione delle macchine. La logica di scelta è semplice: riservazioni per ciò che è inchiodato, savings plan per ciò che è stabile come volume ma mobile come forma.

L'Azure Hybrid Benefit merita un discorso a parte, perché è il meccanismo più trascurato: chi possiede licenze Windows Server o SQL Server con Software Assurance attiva, o licenze in sottoscrizione, può riutilizzarle sulle VM Azure, pagando la sola infrastruttura e non la licenza inclusa nella tariffa. Per le PMI che migrano da server on-premises è spesso il primo risparmio concreto, ed è cumulabile con riservazioni e savings plan. L'ottimizzazione del licensing è del

resto il terreno con i margini più ampi: nei progetti seguiti da SynSphere la revisione complessiva delle licenze ha prodotto in media una riduzione del 30 per cento dei costi di licensing per i clienti.

Ultimo tassello: gli ambienti non produttivi. Le tariffe dedicate Dev/Test, riservate a chi dispone di una sottoscrizione Visual Studio attiva, riducono il costo degli ambienti di sviluppo e collaudo. Anche senza questi requisiti, le VM della serie B con consumo a crediti (burstable) sono spesso la scelta giusta per carichi leggeri e saltuari. E un ambiente di test, per definizione, non ha bisogno di girare di notte e nel weekend: torneremo su questo punto nella sezione dedicata al FinOps.

> **Il consiglio SynSphere**
> Non acquistate riservazioni il primo giorno. Lasciate girare l'ambiente in pay-as-you-go per due o tre mesi, finché Cost Management non mostra un profilo di consumo stabile: **gli impegni pluriennali si prendono sui dati reali, mai sulle stime di progetto**. Una riservazione sbagliata è un risparmio che si trasforma in vincolo.

6. FinOps operativo: il controllo dei costi come abitudine

FinOps è una parola di moda per un concetto antico: i costi si governano con un processo, non con uno strumento. Azure mette a disposizione tutto il necessario dentro Microsoft Cost Management, incluso nella piattaforma; quello che nessuna piattaforma può fornire è la disciplina di usarlo ogni mese. Questa sezione descrive le quattro pratiche che, insieme, formano un sistema.

Budget e alert: il termometro

Il primo passo richiede meno di un'ora: definire un budget mensile per ogni sottoscrizione, ed eventualmente per i gruppi di risorse più rilevanti, con soglie di avviso progressive, per esempio al 50, 80 e 100 per cento. Al superamento, Cost Management invia notifiche ai responsabili tramite un action group: email e, idealmente, una notifica che arrivi anche in un canale Teams dedicato, così che tutto il team la veda. Il budget non blocca la spesa, ma elimina l'effetto sorpresa: nessuna fattura dovrebbe più essere una notizia. A complemento, gli avvisi di anomalia segnalano scostamenti inattesi dal profilo di spesa abituale anche quando il budget non è ancora stato superato.

Se avete applicato i tag della sezione 2, Cost Management permette anche di raggruppare la spesa per centro di costo o per progetto: è il riaddebito interno, anche solo informativo, che rende i costi visibili a chi li genera. La conversazione cambia natura: non più un generico costo IT da discutere a budget, ma il costo di ogni singolo progetto, attribuito a chi lo usa.

Rightsizing: pagare la taglia giusta

Azure Advisor analizza l'utilizzo effettivo delle macchine virtuali e segnala quelle sottoutilizzate, con una raccomandazione di ridimensionamento. È il punto di partenza del rightsizing: si verifica la raccomandazione con le metriche di CPU e memoria delle ultime settimane, si concorda una finestra con chi usa l'applicazione, si riduce la taglia e si osserva il comportamento. Le macchine migrate dall'on-premises sono le prime candidate: quasi sempre conservano un sovradimensionamento che in cloud non ha più ragione di esistere.

Spegnere ciò che non lavora

In cloud il tempo è denaro in senso letterale: una VM di test accesa solo nelle ore lavorative dei giorni feriali costa una frazione di una macchina sempre accesa. Lo spegnimento automatico serale si configura direttamente sulla singola macchina; per scenari più articolati, con accensione programmata al mattino e gestione dei weekend, si usano automazioni PowerShell o le funzionalità di avvio e arresto pianificato. È l'intervento con il miglior rapporto fra sforzo e risparmio dell'intero catalogo FinOps.

La revisione mensile: il rito che tiene tutto insieme

Niente di tutto questo sopravvive senza un appuntamento ricorrente. La revisione mensile dei costi richiede un'ora, una persona responsabile e una scaletta fissa:

1. Confrontare la spesa del mese con il budget e con il mese precedente, voce per voce.
2. Indagare ogni scostamento sopra una soglia concordata: ogni anomalia ha un nome e un perché.
3. Rivedere le raccomandazioni di Azure Advisor e decidere quali applicare.
4. Cercare le risorse orfane: dischi non collegati, IP pubblici inutilizzati, snapshot datati.
5. Verificare la copertura di riservazioni e savings plan rispetto ai consumi reali.
6. Chiudere con tre azioni concrete assegnate, da verificare alla revisione successiva.

> **Il consiglio SynSphere**
>
> Date un proprietario unico alla revisione mensile e mettetela a calendario come una riunione vera, con un report di una pagina come risultato. Nella nostra esperienza è la singola abitudine che separa le aziende con i costi sotto controllo da quelle che li subiscono: **non serve un reparto FinOps, serve un'ora al mese fatta bene**.

7. Sicurezza di base: il minimo che non è negoziabile

La governance dei costi e quella della sicurezza sono due facce dello stesso problema: risorse senza padrone. Questo white paper non è una guida alla cybersecurity, ma una baseline di sicurezza fa parte delle fondamenta di qualunque ambiente Azure, e gli strumenti per costruirla sono in larga parte già inclusi nella piattaforma.

Microsoft Defender for Cloud

Defender for Cloud ha due anime. La prima, disponibile senza costi aggiuntivi, è la gestione della postura di sicurezza: il Secure Score misura quanto l'ambiente rispetta le raccomandazioni Microsoft e propone interventi ordinati per impatto, dalla macchina senza aggiornamenti allo storage esposto. La seconda, a pagamento e attivabile per singolo tipo di carico (server, database, storage e altri), aggiunge la protezione attiva dalle minacce. Per una PMI il percorso ragionevole è netto: attivare subito la parte gratuita, portare il Secure Score a un livello dignitoso lavorando sulle raccomandazioni, e solo poi valutare i piani a pagamento partendo dai carichi più esposti.

La rete: chiudere le porte

I Network Security Group (NSG) sono il firewall di base di Azure: regole che consentono o negano il traffico verso subnet e interfacce di rete. La regola d'oro è una sola: niente RDP o SSH aperti verso internet, mai. L'accesso amministrativo alle macchine passa da una VPN, da Azure Bastion o da meccanismi di accesso just-in-time che aprono la porta solo su richiesta e per un tempo limitato. Un controllo periodico delle regole NSG, anche con uno script, intercetta le aperture fatte di fretta durante un'emergenza e mai più richiuse.

Backup e disaster recovery

La ridondanza dello storage non è un backup: protegge dal guasto hardware, non dalla cancellazione accidentale, dal ransomware o dall'errore umano. Azure Backup copre macchine virtuali, database e file con retention configurabile e protezioni contro la cancellazione malevola dei backup stessi, come il soft delete; va attivato in modo sistematico, idealmente con una policy DeployIfNotExists che lo imponga su ogni VM di produzione. Azure Site Recovery risponde a una domanda diversa: non recuperare un dato, ma rimettere in piedi un intero servizio in un'altra regione se quella primaria diventa indisponibile. Per molte PMI un backup ben fatto è sufficiente; Site Recovery entra in gioco quando il fermo prolungato di un'applicazione ha un costo che giustifica l'investimento.

Tre verifiche periodiche chiudono il cerchio: controllare che i backup vengano davvero eseguiti, perché un job fallito che nessuno guarda equivale a non avere backup; fare un ripristino di prova almeno una volta l'anno, misurando quanto tempo serve davvero; tenere la lista di chi può eliminare i backup ristretta quanto quella degli Owner. La domanda da porsi non è se l'azienda ha i backup, ma se domattina saprebbe ripartire, in quanto tempo e perdendo quanti dati: retention e frequenza si dimensionano a partire da questa risposta, non viceversa.

8. Monitoraggio: pochi alert, ma che contano

Azure Monitor raccoglie due famiglie di dati: le metriche, valori numerici rilevati a intervalli regolari come CPU, memoria e latenza, e i log, eventi dettagliati su ciò che accade dentro le risorse e sul piano di controllo. I log confluiscono in un workspace Log Analytics, interrogabile con il linguaggio KQL: per una PMI la scelta giusta è quasi sempre un workspace unico e centralizzato, che semplifica permessi, query e gestione dei costi di raccolta.

Il rischio del monitoraggio non è la mancanza di dati, è il rumore. Un sistema che manda cinquanta notifiche al giorno viene ignorato nel giro di un mese, e con lui anche l'unica notifica davvero importante. La regola pratica: ogni alert deve avere un destinatario chiaro e un'azione associata. Se alla notifica non corrisponde niente da fare, non è un alert: è spam autoprodotto.

Una dotazione minima ma efficace per una PMI si costruisce con pochi avvisi mirati:

- Service Health: Azure avvisa di manutenzioni e incidenti che toccano i vostri servizi e le vostre regioni.
- Budget e anomalie di costo, configurati come descritto nella sezione FinOps.
- Disponibilità dei servizi critici: la VM di produzione spenta, l'applicazione che non risponde.
- Job di backup falliti: l'alert più sottovalutato e quello che salva l'azienda.
- Scadenze di certificati e segreti delle applicazioni, segnalate prima della scadenza e non dopo.

- Operazioni amministrative sensibili: eliminazione di risorse di produzione, modifiche ai ruoli.

Per le macchine virtuali, l'abilitazione di VM Insights aggiunge metriche dettagliate su processi e dipendenze: sono le stesse informazioni che alimentano il rightsizing della sezione FinOps, perché monitoraggio e controllo dei costi si sostengono a vicenda. Vale anche al contrario: una macchina costantemente al limite delle risorse è un problema di affidabilità prima che di costo, e il monitoraggio lo fa emergere prima che diventi un disservizio.

Gli alert si collegano agli action group, che smistano le notifiche verso email, Teams o sistemi di ticketing. Per la visione d'insieme, i workbook di Azure Monitor permettono di costruire dashboard leggibili anche da chi non è tecnico: una pagina con spesa del mese, stato dei backup, Secure Score e disponibilità dei servizi critici è un ottimo report ricorrente per la direzione.

> **Il consiglio SynSphere**
> Anche i log hanno un costo, proporzionale ai dati ingeriti e alla durata di conservazione. Raccogliete ciò che servirà a rispondere a domande concrete, non tutto il possibile: **un piano di raccolta scritto, con retention differenziate fra log di sicurezza e log di diagnostica**, evita che lo strumento di controllo diventi a sua volta una voce di costo fuori controllo.

9. Roadmap in novanta giorni e automazione PowerShell

Tutto quanto visto finora può sembrare tanto, ma non va fatto tutto insieme. L'esperienza maturata sui progetti di governance suggerisce una sequenza in quattro fasi, dimensionata su una PMI con risorse IT limitate: l'ordine conta più della velocità.

Fase	Settimane indicative	Risultato atteso
Assessment	1-2	Inventario completo, mappa dei costi, risorse orfane individuate
Fondamenta	3-6	Gerarchia delle sottoscrizioni, naming, tag, RBAC rivisto
Policy e FinOps	7-10	Azure Policy attive, budget e alert, primo rightsizing
Regime	dalla settimana 11	Revisione mensile, report ricorrente, automazione PowerShell

La fase di assessment è la più sottovalutata e la più preziosa: prima di cambiare qualsiasi cosa serve l'inventario completo di ciò che esiste, con costi, utilizzo e, dove ricostruibile, il motivo per cui ogni risorsa è nata. È qui che emergono le risorse orfane e gli ambienti dimenticati della sezione 1, e spesso l'assessment si ripaga da solo con le prime pulizie.

Le fasi successive seguono i capitoli di questo white paper: prima le fondamenta, cioè gerarchia, naming, tag e RBAC; poi le regole automatiche e il controllo dei costi; infine il regime, con la revisione mensile come perno. Conviene resistere alla tentazione di partire dalle policy con effetto Deny o dall'acquisto di riservazioni: senza fondamenta, ogni automatismo amplifica il disordine invece di ridurlo.

PowerShell: la governance che si ripete da sola

Il portale Azure va benissimo per esplorare e configurare, ma la governance è fatta di controlli ripetuti, e i controlli ripetuti vanno automatizzati. Il modulo Az di PowerShell permette di interrogare l'intero ambiente con script di poche righe: l'inventario delle risorse con i rispettivi tag, l'elenco dei dischi non collegati e degli IP pubblici inutilizzati, le assegnazioni di ruolo per ambito, lo stato di conformità delle policy. Eseguiti ogni mese, magari in apertura della revisione dei costi, trasformano controlli da mezza giornata in un report di cinque minuti.

Per non partire da zero, SynSphere ha pubblicato nella sezione Download di synsphere.it tre toolkit PowerShell gratuiti dedicati proprio a questi temi: uno per la governance di Azure, con inventario, audit dei tag, risorse orfane e assegnazioni RBAC; uno per il cost management, con analisi dei consumi, verifica dei budget e individuazione delle risorse candidate al rightsizing; e uno per il monitoraggio, con il censimento di regole di alert e action group, lo stato dei job di backup e le impostazioni di diagnostica. Sono script in sola lettura, pensati per essere letti e capiti prima ancora che eseguiti: l'automazione è utile solo se chi la lancia sa che cosa sta guardando.

L'ultimo ingrediente è la competenza interna. Non serve che la PMI assuma un cloud architect a tempo pieno, ma serve almeno una persona che conosca i concetti di questo documento e li presidi nel tempo: la formazione del referente IT, anche poche giornate mirate su governance e costi, vale più di qualunque strumento. È una convinzione che per SynSphere nasce dai numeri della propria attività formativa, con oltre 5.000 ore di formazione erogate e più di 800 professionisti formati: la governance attecchisce quando in azienda c'è qualcuno che la sente propria.

10. Checklist operativa

Questa checklist riassume l'intero percorso in azioni verificabili. Il modo migliore di usarla: spuntate ciò che è già in ordine, trasformate il resto in un piano con date e responsabili, e ripassatela per intero ogni sei mesi, perché la governance non è uno stato che si raggiunge ma una condizione che si mantiene.

Fondamenta

- Sottoscrizioni separate per produzione e non produzione, sotto un management group.
- Gruppi di risorse organizzati per ciclo di vita applicativo.
- Naming convention scritta, pubblicata e applicata a ogni nuova risorsa.
- Tag obbligatori definiti e documentati: env, owner, cost-center, project, più expiry per le risorse temporanee.
- Policy con effetto Modify attiva per ereditare i tag dal gruppo di risorse.

Identità e accessi

- Ruoli assegnati a gruppi di Microsoft Entra ID, non a singoli utenti.
- Owner limitato a pochissime persone; Reader come ruolo predefinito per la consultazione.
- Chi sviluppa non ha permessi di modifica sulla produzione.
- Accessi di fornitori e consulenti con scadenza definita.
- Revisione trimestrale delle assegnazioni di ruolo, fissata a calendario.

Costi

- Budget con soglie di avviso al 50, 80 e 100 per cento su ogni sottoscrizione.
- Avvisi di anomalia di costo attivi.
- Spegnimento automatico configurato su tutte le VM di test e sviluppo.
- Raccomandazioni di Azure Advisor riviste ogni mese.
- Riservazioni o savings plan valutati solo dopo due o tre mesi di consumi reali.
- Azure Hybrid Benefit verificato per ogni VM Windows Server e SQL Server.
- Revisione mensile dei costi a calendario, con responsabile e report di una pagina.

Sicurezza e monitoraggio

- Defender for Cloud attivo almeno nella parte gratuita, con Secure Score monitorato.
- Nessuna porta RDP o SSH esposta verso internet.
- Azure Backup attivo su tutte le VM di produzione, con test di ripristino annuale.
- Alert su Service Health, job di backup falliti e operazioni amministrative sensibili.
- Workspace Log Analytics unico, con piano di raccolta e retention scritto.

Da rivedere ogni trimestre

- Assegnazioni di ruolo: chi ha ancora bisogno dei permessi che ha?
- Regole NSG: ci sono aperture temporanee mai richiuse?
- Report di conformità di Azure Policy: le eccezioni sono ancora motivate?
- Copertura di riservazioni e savings plan rispetto al consumo effettivo.
- Risorse con tag expiry scaduto: prorogare consapevolmente o eliminare.

I primi cinque passi, questa settimana

1. Esportare l'inventario completo delle risorse e identificare quelle senza un proprietario certo.
2. Creare un budget con soglie di avviso sulla sottoscrizione principale.
3. Cercare dischi non collegati, IP pubblici liberi e snapshot datati, e pianificarne la rimozione.
4. Attivare lo spegnimento automatico sulle VM di test.
5. Fissare a calendario la prima revisione mensile dei costi.

Chi è SynSphere

SynSphere Italia è un partner Microsoft specializzato nelle piccole e medie imprese italiane. Dal 2008 affianchiamo le aziende su Microsoft 365, Azure, Dynamics 365, sicurezza informatica e formazione, con sedi operative a Milano (Segrate) e Bolzano.

+150	**+10.000**	**0**
tenant Microsoft 365 gestiti	utenti migrati	downtime medio nelle migrazioni
+5.000	**+800**	**95%**
ore di formazione erogate	professionisti formati	soddisfazione dei corsi

Vuoi una mano sui temi di questo white paper? Parliamone: **synsphere.it/contattaci** · **info@synsphere.com**. Sul sito trovi anche strumenti gratuiti di assessment, toolkit PowerShell, template operativi e il catalogo completo di corsi e certificazioni Microsoft.