Transizione Digitale

www.transizionedigitale.it

Suggerimenti per l'Adeguamento al Nuovo Regolamento Cloud per le PA Italiane

1. Valutazione iniziale

- Effettuare un censimento completo dei dati e servizi digitali attualmente in uso.
- Classificare questi dati e servizi secondo le categorie previste dal regolamento (ordinari, critici, strategici).

2. Analisi dei gap

- Confrontare l'infrastruttura e i servizi cloud attuali con i requisiti del nuovo regolamento.
- Identificare le aree di non conformità o che necessitano di miglioramento.

3. Pianificazione della migrazione

- Sviluppare un piano dettagliato di migrazione al cloud, utilizzando il modello fornito dal Dipartimento per la Trasformazione Digitale.
- Assicurarsi che il piano sia completato e presentato entro il 30 giugno 2026.

4. Revisione dei contratti

- Esaminare i contratti esistenti con i fornitori di servizi cloud.
- Verificare la conformità dei fornitori ai nuovi requisiti di qualificazione (QC1-QC4).

5. Formazione del personale

- Organizzare sessioni di formazione per il personale sui nuovi requisiti e le best practices di sicurezza.
- Assicurarsi che i ruoli e le responsabilità in materia di cybersecurity siano chiaramente definiti e compresi.

6. Implementazione delle misure di sicurezza

- Adottare le misure di sicurezza richieste per il livello di classificazione dei dati (ordinari, critici, strategici).
- Implementare controlli di accesso, crittografia e monitoraggio come specificato negli allegati del regolamento.

7. Certificazioni e conformità

- Verificare che i fornitori di servizi cloud possiedano le certificazioni richieste (ISO 9001, ISO/IEC 27001, ISO 22301).
- Assicurarsi che l'infrastruttura interna soddisfi i requisiti di adeguamento (AI1-AI4) se applicabile.

8. Monitoraggio e reporting

- Implementare sistemi di monitoraggio continuo per verificare la conformità ai requisiti del regolamento.
- Preparare processi di reporting regolari per dimostrare la conformità durante gli audit.

9. Gestione del budget

- Valutare l'impatto finanziario dell'adeguamento al nuovo regolamento.
- Allocare risorse per eventuali upgrade necessari o nuovi servizi richiesti.

10. Collaborazione con ACN

- Mantenere un dialogo aperto con l'Agenzia per la Cybersicurezza Nazionale.
- Partecipare a eventuali sessioni informative o workshop organizzati dall'ACN sul nuovo regolamento.

11. Preparazione per la continuità operativa

- Sviluppare e testare piani di disaster recovery e business continuity in linea con i requisiti del regolamento.

12. Revisione periodica

- Stabilire un processo di revisione periodica per assicurare la continua conformità al regolamento, considerando che alcuni requisiti potrebbero essere aggiornati ogni due anni.