Checklist per le verifiche di conformità ed i collaudi del software v. 4

Il presente documento rappresenta un elenco esemplificativo ed esaustivo di verifiche che ogni software, realizzato per il committente Regione Marche ed in generale per le PA, deve tipicamente rispettare, ed il cui esito ai controlli finali deve risultare positivo.
Per ogni verifica, da effettuarsi secondo le tempistiche e le modalità previste dal capitolato di gara e dal contratto stipulato con il fornitore incaricato dell'esecuzione di un appalto per la realizzazione di sistemi e applicazioni ICT, andrà indicata l'opzione di risultato corretta (Verificato, Non Verificato, Non Previsto) e le eventuali motivazioni per cui il controllo non è applicabile.
Le verifiche riguardano sia gli aspetti di performance, sia quelli di sicurezza (disponibilità – integrità – riservatezza), sia le specifiche funzionalità offerte dall'applicazione software.

Nel caso in cui le applicazioni vengano installate presso i datacenter di Regione Marche, ulteriori verifiche riguarderanno le modalità in cui i processi di sviluppo, deploy, test, manutenzione, etc. si integrino con quanto previsto dalle procedure di erogazione servizi definite dal Centro Controllo Reti e Sistemi del settore Transizione Digitale ed Informatica, dal momento che i datacenter "Sanzio" e "Tiziano":
- hanno ottenuto, in quanto considerate infrastrutture del "gruppo A", la qualificazione di nodi compatibili con i requisiti del Polo Strategico Nazionale (PSN);
- risultano gestite da un "Cloud Service Provider (CSP)" di tipo C
- sono abilitate a fornire servizi Iaas Paas e Saas, in quanto presenti nel cloud marketplace nazionale di ACN https://catalogocloud.acn.gov.it/
E dal momento che sono inoltre attive, per le infrastrutture regionali, le seguenti certificazioni:
- *ISO/IEC 27001:2013* per l'erogazione in sicurezza di servizi Iaas e Paas di cloud computing, di housing ed hosting e di gestione fisica e logica delle server farm;
- estensioni della *ISO 27001: 27017* (controlli di sicurezza delle informazioni per i servizi in cloud) e *27018* (protezione delle informazioni di identificazione personale in cloud pubblici);
- *ISO9001* (gestione della qualità dei processi dell'organizzazione);
- *ISO 20000-1* (sistema di gestione dei servizi IT);
- *ISO 22301* (gestione della Business Continuity)

Laddove invece ci si avvalga di soluzioni installate presso datacenter di terze parti o fornite in SaaS, valgono i regolamenti vigenti relativi alla qualificazione dei servizi e delle infrastrutture forniti dai Cloud Service Provider verso le PA.

Specifiche generali

Rispetto dei requisiti minimi di sicurezza AgID
La soluzione deve rispettare i requisiti minimi di sicurezza e fornire una relazione / batteria di test relativamente al rispetto di tali requisiti.

Performance, scalabilità e livelli di servizio SLA da capitolato
Nel capitolato sono presenti specifiche di performance, scalabilità e SLA: i test devono mostrare che la soluzione è conforme alle specifiche richieste.

% availability / downtime annuale
I test devono mostrare che la soluzione è conforme alle specifiche relativamente alla percentuale di disponibilità annuale del sistema e che tutta la catena di supporto è in grado di mantenere le attività nel rispetto di questo valore.

Verifica applicazione patch di aggiornamento delle componenti
Deve essere fornito un documento che preveda tempi e attività per l'aggiornamento continuo della soluzione per applicazioni di patch di sicurezza e/o di upgrade delle componenti utilizzate.

Monitoraggio
Deve essere fornito un documento che indichi i sistemi di monitoraggio integrabili e/o supportati, compatibili con quelli abitualmente utilizzati nell'ambito della gestione del Data Center ospitante (come indicati dal capitolato o in sede di sopralluogo) e spieghi inoltre gli indicatori rilevanti per valutare lo stato ed il corretto funzionamento del sistema.

Continuità operativa / Disaster Recovery
Definizione e corrispondenza delle RPO/RPO dei backup. Esistenza della documentazione RFC (Request For Call) nel caso in cui la soluzione sia ospitata presso macchine virtuali o fisiche residenti nei datacenter regionali.

Accessi autenticati
Nel capitolato, nel caso di accesso riconosciuto degli utenti, deve essere previsto l'accesso tramite SPID/CIE/CNS e loro evoluzioni. I log di accesso al sistema devono essere gestiti, nel rispetto della normativa della privacy e di specifiche riferite al settore di applicazione (es. whistleblower).

Accessibilità, responsività e usabilità delle interfacce
Nel capitolato, ma anche nella normativa di settore, sono stabilite specifiche relative e la soluzione rilasciata deve documentare il loro rispetto nelle modalità prestabilite (es. dichiarazione di accessibilità AgID, test user experience, etc.).

GDPR
Nel capitolato e nella disciplina normativa e regolamentare di settore, sono stabilite specifiche per la gestione e la protezione dei dati (trattamento, localizzazione in Unione Europea, data retention, anomimizzazione dati personali, etc.) che devono essere rispettate.
Devono essere forniti e verificati le informative sulla privacy, il disclaimer (termini d'uso), la cookie policy ed ogni altro strumento e contenuto obbligatorio.
Deve essere prevista la gestione degli incidenti e dei data breach, la loro registrazione e l'integrazione di tale sistema con quello in uso per il Data Center ospitante (regionale o in gestione da parte di un Cloud Service Provider abilitato per la PA).
Deve essere fornito l'elenco dei tecnici autorizzati (sia interni che esterni) coinvolti nell'attività di sviluppo e manutenzione, che nell'ambito di tali attività possano aver accesso ai dati; in tal senso andrà inoltre stipulato un accordo integrativo con il fornitore esterno per la raccolta di specifiche garanzie per il mantenimento dei dati gestiti in sicurezza e riservatezza.

Crittografia
Deve essere prevista la crittografia in transito (TSL / HTTPS).
Deve essere prevista, se di pertinenza, la crittografia at-rest (FDE, DB encryption etc).

Proprietà del codice
Nelle specifiche deve essere prevista la proprietà del codice e la messa a disposizione dello stesso, per il riuso, nel repository regionale GitHub integrato con il repository nazionale developers ITA o in alternativa forme di licensing compatibili o comunque espressamente concordate con la stazione appaltante.

Ulteriori verifiche
Test di carico
Deve essere allegato una batteria di test che mostri il comportamento globale e/o di componenti rilevanti in termini di reazione all'aumentare del carico sia in senso di utenti che di dati coinvolti, per quanto di pertinenza. Per gli stress test il fornitore può avvalersi di soluzioni di mercato ad hoc a proprio carico o strumenti interni a sua disposizione.

Test di vulnerabilità
Test (es. OpenVAS) che dimostri come la soluzione superi i test standard di vulnerabilità.

Test di velocità

Test (es. Google Pagespeed Insight) che dimostri come le pagine web dell'interfaccia vengono caricate con velocità adeguata rispetto a soluzioni analoghe ed accettabile da parte degli utenti.

Test di backup e restore dell'intero sistema (codice, configurazione e dati)

Deve essere presente un test che mostri i tempi necessari per effettuare un backup della soluzione tale da poterla ripristinare da zero. Altresì deve essere presente un test che mostri come la soluzione possa essere ripristinata senza attività non previste da un backup.
Il test deve mostrare anche i tempi di esecuzione e, nel caso di aumento rilevante dei tempi nel corso di utilizzo (es: aumento dei dati), i tempi in diverse condizioni di crescita.

Piani di test sulle funzionalità di front-end, back-office e User eXperience

Deve essere previsto un piano di test che verifichi il funzionamento non degradante del sistema e delle singole componenti funzionali sui tre aspetti.
In particolare, va verificata la corretta ed esaustiva gestione della comunicazione con l'utenza di eventuali errori interni.

Manualistica

Deve essere presente un manuale per gli utenti e un manuale per i tecnici manutentori del sistema.

Erogazione dei servizi

La qualità di erogazione dei servizi deve essere conforme alle pèoliticge di gestione dei servizi del datacenter regionale.
Deve inoltre essere presente un questionario/indagine sulla customer satisfaction, con relativa reportistica periodica.
La soluzione deve essere iscritta al marketPlace dell'Agenzia Cybersecurity Nazionale ACN, nel rispetto delle circolari relative ai servizi SaaS e ai Cloud Provider verso le PA.