Misure di sicurezza Cloud		
RC1	Cloud Service Support	Il Fornitore Cloud fornisce al Cliente un servizio di **supporto tecnico** con costi e orari di servizio definiti. Il supporto deve essere accessibile mediante opportuni canali di comunicazione e adeguati sistemi di gestione (issue tracking), al fine di consentire al Cliente di effettuare in completa autonomia le segnalazioni di malfunzionamenti e potenziali pericoli per la sicurezza e la fruibilità del servizio.
RC2	Cloud Service Support	Il Fornitore Cloud assicura la massima trasparenza nella **gestione delle segnalazioni**, garantendo al Cliente appropriata visibilità dei processi di issue tracking e assistenza tecnica. Il Fornitore Cloud deve definire le tempistiche per la presa in carico e gestione delle segnalazioni in funzione di diverse priorità, dichiarando i livelli di servizio garantiti.
RC3	Cloud Service Support	Il Fornitore Cloud fornisce la **documentazione tecnica, le guide d'uso e/o altro materiale di supporto**, ivi compresa la documentazione dettagliata delle API e delle interfacce CLI, GUI e SOAP/REST, se previste dal servizio.
RC4	Service Level Indicator	Il Fornitore Cloud dichiara gli obiettivi corrispondenti agli **indicatori di qualità del servizio** sotto riportati e ne garantisce il rispetto nei rapporti contrattuali: - Availability (Percentuale di tempo in cui il servizio risulta essere accessibile e usabile) - Support hours (L'orario in cui il servizio di supporto tecnico è operativo) - Maximum First Support Response Time (Il tempo massimo che intercorre tra la segnalazione di un inconveniente da parte del cliente e la risposta iniziale alla segnalazione) - Cloud Service Bandwidth (La quantità di dati che può essere trasferita in un determinato periodo di tempo.) - Limit of Simultaneous Connections (Numero massimo di connessioni simultanee supportate dal servizio.) - Cloud Service Throughput (Nmero di transazioni processate in ciascuna unità di tempo dal servizio.) - Recovery Time Objective (RTO) - Recovery Point Objective (RPO) - Backup Interval (tempo che intercorre tra un backup e l'altro.) - Retention period of backup data - Data retention period (Il periodo di tempo in cui i dati del cliente vengono mantenuti dal CSP dopo la notifica di cessazione del servizio.) - Log retention period (I periodo di tempo in cui i file di log relativi al servizio vengono conservati dopo la notifica di cessazione del servizio.)
RC5	Change Management	Il Fornitore Cloud implementa un processo di **change management**, al fine di garantire che vengano utilizzate procedure e metodi standard per la gestione tempestiva ed efficiente di ogni cambiamento nell'ambito dell'infrastruttura e dei servizi offerti, .
RC6	Change Management	Il Fornitore Cloud garantisce la disponibilità tempestiva di informazioni al Cliente circa i **cambiamenti** e le migliorie introdotti in seguito ad aggiornamenti apportati alle modalità di funzionamento e fruizione dei servizi erogati. E' definito un periodo temporale prima del quale il Fornitore Cloud deve dare comunicazione al Cliente diegli **interventi di manutenzione** attraverso un canale di comunicazione diretto.
RC7	Incident Management	Il Fornitore Cloud garantisce l'adozione di processi di **gestione degli incidenti** coerenti con quanto raccomandato dagli standard di sicurezza internazionali (p.e. ISO/IEC 27002, ISO/IEC 27035).
RC8	Vulnerability Management	Il Fornitore Cloud garantisce l'adozione di un processo di gestione delle vulnerabilità tecniche che prevede l'esecuzione su base regolare di vulnerability assessment e penetratione test.
RC9	Vulnerability Management	Il Fornitore Cloud, in caso di servizio Saas, dichiara se le componenti che costituiscono il servizio sono state sottoposte ai **test OWASP** con esito positivo.
RC10	Event logging	Il Fornitore Cloud garantisce l'adozione di un sistema centralizzato di event logging e da la possibilità al Cliente di esportare i log sui propri sistemi.
RC11	Business Continuity	Il Fornitore Cloud garantisce l'adozione di un processo per la gestione della **continuità operativa** (business continuity) in cui sono previste azioni orientate al ripristino dell'operatività del servizio e delle risorse da esso gestite al verificarsi di eventi catastrofici/imprevisti, specificando l'applicazione delle buone pratiche presenti nello standard ISO/IEC 22313.
RC12	Certifications	Il Fornitore Cloud dichiara di esserere in possesso della certificazione secondo lo standard **ISO/IEC 27001** estesa con i controlli degli standard **ISO/IEC 27017 e ISO/IEC 27018**. La certificazione deve essere stata rilasciata da organismi nazionali di accreditamento riconosciuti dalla Unione Europea.
RC13	Data Deletion	Il Fornitore Cloud garantisce l'adozione di un processo definito di cancellazione sicura dei dati.
RC14	Data Portability	Il Fornitore Cloud garantisce al Cliente la possibilità di estrarre in qualsiasi momento una **copia completa dei dati e metadati** memorizzati come, a titolo esemplificativo ma non esaustivo: volumi, object e block storage, dump di DB, ecc.
RC15	Data Protection	Il Fornitore Cloud garantisce che il servizio proposto è conforme agli obblighi e agli adempimenti previsti dalla normativa (europea e italiana) in materia di **protezione dei dati personali.**
RC16	Data Location	Il Fornitore Cloud rende nota la **localizzazione dei data center propri e/o dell'infrastruttura Cloud** utilizzata per erogare anche parzialmente il servizio e/o all'interno dei quali transiteranno anche temporaneamente i dati gestiti dal servizio (ivi compresi i siti di disaster recovery e di backup), specificando quando la localizzazione sia all'interno del territorio nazionale, all'interno della UE oppure extra UE.
RC17	Data Protection	Il Fornitore Cloud, in caso di localizzazione dei data center in territorio extra UE, dichiara l'applicabilità di accordi bilaterali (Privacy Shield EU-USA, ecc.) volti alla salvaguardia dei dati elaborati, conservati ed a vario titolo gestiti per erogare il servizio.

RC18	Notification of a data breach involving PII	Il Fornitore Cloud avvisa tempestivamente il cliente in caso di accesso non autorizzato alle informazioni personali o accesso non autorizzato alle apparecchiature o strutture di elaborazione con conseguente perdita, divulgazione o alterazione delle informazioni personali.
RC19	Data Encryption	Il Fornitore Cloud dichiara quale tipo di **crittografia** utilizza per proteggere la riservatezza dei dati scambiati tra Fornitore e Cliente.
RC20	Data Encryption	Il Fornitore Cloud dichiara quale tipo di **crittografia** utilizza per proteggere la riservatezza dei dati archiviati presso i Datacenter.
RC21	Termination of service	Il Fornitore Cloud garantisce l'adozione di un processo di notifica della cessazione del servizio e di restituzione o trasferimento degli asset del Cliente (comprese le informazioni personali)
RC22	Segregation in virtual computing environments	Il Fornitore Cloud garantisce l'applicazione di misure di sicurezza per separare logicamente l'ambiente virtuale del Cliente da quello degli altri Clienti e impedire di accedere o esporre il contenuto a persone non autorizzate.