IS7.2.M REV01 PROTOCOLLO DI AFFIDAMENTO SERVIZI CLOUD

1. PREMESSA

L'affidamento dei dati in cloud ai sensi della ISO 27017 prevede la verifica di determinati requisiti sia per il Cliente che per Clesius S.r.l..

Clesius in completa trasparenza per la gestione dei servizi offerti vi fornisce in seguito un riepilogo dei vostri adempimenti anche riferiti a quelli che Clesius adotta come fornitore in ottemperanza alla ISO 27017 e alle altre norme ISO acquisite. Qualora riscontriate delle difformità rispetto a quanto sotto riportato e gli eventuali servizi offerti, vi invitiamo a segnalarcelo tramite i nostri consueti canali di comunicazione.

2. PROTOCOLLO DI AFFIDAMENTO SERVIZI CLOUD

2.1. I dati memorizzati nell'ambiente di cloud computing possono essere soggetti all'accesso e alla gestione da parte di Clesius; a tutela del Cliente, Clesius adotta l'applicazione di metodi e processi certificati da terzi in ambito sicurezza delle informazione con particolare riferimento alle norme ISO 27001, ISO 27018 e ISO 27017.

2.2. Per fruire del servizio del servizio cloud, ricordiamo che devono essere ben definiti gli utenti che accedono al perimetro cloud. A tal fine, Clesius adotta due diverse tipologie di profili di accesso:

- Utenti del Cliente con profilo amministrativi del servizio cloud che hanno accesso privilegiato.
- Utenti con un profilo User che possono eseguire operazioni limitate sul servizio cloud.

Pertanto, alla stipula del contratto, il Cliente dovrà individuare e nominare un operatore con il ruolo di Amministratore Locale e dovrà comunicarne i dati anagrafici (nome, cognome, luogo e data di nascita, codice fiscale) all'indirizzo PEC di Clesius (clesius@pec.it). Al momento della ricezione della PEC verrà creato il profilo dell'utente Amministratore Locale e verranno abilitati i servizi acquistati. Sarà l'Amministratore Locale a creare e gestire gli utenti ed associare loro le funzionalità.

2.3. Clesius ha un'adeguata attribuzione dei ruoli e delle responsabilità in materia di sicurezza delle informazioni e conferma che è nelle condizioni di adempiere ai propri ruoli e responsabilità in materia di sicurezza dei dati. L'utilizzo dei servizi per tutti gli utenti avviene tramite l'accesso al perimetro informatico e riservato del Cliente attraverso autenticazione con login e password, adottando tutti i criteri necessari per garantire la massima sicurezza possibile (protocollo HTTPS, complessità delle password, scadenza, ecc.). In tale contesto, inoltre, sono eseguite periodiche rivalutazioni dell'analisi dei rischi, vulnerability assestmet e penetration test. Il Cliente che ritiene di modificare e/o integrare le prassi di controllo di Clesius è tenuto a definire tali aspetti preventivamente, in uno specifico accordo tra le parti.

2.4. L'accesso alle piattaforme di Clesius dovrà avvenire tramite stazioni di lavoro del Cliente connesse ad Internet mediante un sistema di connettività affidabile e sicuro messo a disposizione ai propri utenti. Le stazioni di lavoro dovranno essere dimensionate in funzione del lavoro che dovranno svolgere e la connettività dovrà essere adeguata al carico di lavoro che deve sostenere. Se l'infrastruttura del Cliente non fosse adeguata, Clesius non si assume nessuna responsabilità relativamente a problemi di lentezza, perdita di dati, interruzioni di servizio ed altri tipi di malfunzionamento dovuti all'inadeguatezza dell'infrastruttura.

2.5. Clesius non garantisce nessun intervento riguardante installazione, configurazione, sicurezza e altri servizi sistemistici che riguardano le stazioni di lavoro e la connettività del Cliente. È escluso qualsiasi intervento del personale di Clesius per fasi di ripristino dati, riconfigurazione del sistema rese necessarie da anomalie indipendenti dalla responsabilità o dalle obbligazioni assunte. Relativamente agli interventi precedentemente citati, qualora necessario, dovrà essere previsto un ulteriore accordo con Clesius.

2.6. Clesius ha identificato nel Garante della Privacy, l'Agenzia per l'Italia Digitale (AgID), l'Agenzia per la Cybersicurezza Nazionale (ACN) e nella Polizia Postale le Autorità rilevanti per la protezione dei dati. Qualora il Cliente ritenga di modificare e/o integrare tali organismi, è tenuto a definire tali aspetti preventivamente, in uno specifico accordo tra le parti. Salvo espressamente vietato dalla legge, se una Autorità Giudiziaria dovesse richiedere dati o informazioni del Cliente a Clesius, quest'ultima si impegna a dare comunicazione al Cliente circa i dati/informazioni comunicati, mediante PEC opportunamente protocollata.

2.7. Il Cliente prende atto e accetta che la piattaforma verrà utilizzata in completa autonomia e sotto la sua esclusiva responsabilità, anche riguardo all'attività dei suoi dipendenti, collaboratori e consulenti esterni. Si ricorda che il Cliente è tenuto ad aggiungere ai propri programmi di formazione degli elementi di sensibilizzazione per:

- I responsabili.
- Gli amministratori.
- Gli integratori di servizi cloud.
- Gli utenti del servizio cloud, inclusi i dipendenti e gli appaltatori interessati.

La consapevolezza della sicurezza delle informazioni, i programmi di istruzione e la formazione sui servizi cloud dovrebbero essere forniti a tutto il personale compresa la direzione, i responsabili della supervisione e le unità operative. In particolare, il Cliente si impegna a responsabilizzare, controllare ed eventualmente sanzionare i comportamenti dei propri dipendenti e/o collaboratori interni ed esterni relativi ad una non corretta gestione dell'account di accesso alla piattaforma che l'operatore riceve dal proprio Amministratore Locale o da Clesius. Il Cliente si assume la responsabilità per qualsiasi danno arrecato a Clesius e/o a terzi in dipendenza della mancata osservanza dei predetti obblighi di diligente conservazione delle credenziali di accesso ricevute.

Questi sforzi supportano un efficace coordinamento delle attività di sicurezza delle informazioni in ambiti quali:

- standard e procedure per l'utilizzo dei servizi cloud;
- rischi per la sicurezza delle informazioni relativi ai servizi cloud e come tali rischi sono gestiti;
- rischi per l'ambiente di rete e di sistema con l'uso di servizi cloud;
- considerazioni legali e normative applicabili.

2.8. Clesius eroga i servizi proposti, nelle modalità così descritte, con la massima diligenza, rispettando i tempi concordati ed utilizzando personale dotato della necessaria preparazione tecnico-professionale.

2.9. Clesius esegue periodicamente l'inventario delle proprie risorse tenendo conto delle informazioni e delle risorse associate archiviate nell'ambiente di cloud computing. Appositi registri dell'inventario permettono di individuare le risorse.

2.10. Clesius utilizza una infrastruttura digitale Cloud Solution Provider (CSP) qualificata ACN di un fornitore individuato come sub-responsabili esterno adeguatamente verificato e responsabilizzato nell'esecuzione del contratto, nelle leggi applicabili in materia, nella protezione dei dati personali.

Clesius si riserva la facoltà di cambiare in qualsiasi momento il fornitore CSP senza necessità di avvisare o di chiedere l'autorizzazione al Cliente, pur assicurando che i dati dei Clienti siano sempre e solo su server all'interno dell'Unione Europea e che il cambiamento non comporti impatti negativi considerevoli per il cliente. Clesius si impegna comunque a informare qualunque cambiamento che possa avere impatti sul servizio cloud.

Clesius non è responsabile per cause di Forza Maggiore e cioè eventi che, oggettivamente, impediscano al personale di Clesius di garantire il servizio contrattualizzato (in via meramente esemplificativa e non esaustiva: scioperi e manifestazioni con blocco delle vie di comunicazione; incidenti stradali; guerre e atti di terrorismo; catastrofi naturali quali alluvioni, tempeste, uragani, etc). Clesius inoltre non è responsabile per cause che determinano l'inaccessibilità, totale o parziale, al Servizio imputabili a guasti nella rete internet esterna al perimetro di Clesius e comunque fuori dal suo controllo (in via meramente esemplificativa guasti o problemi).

2.11. Il trattamento dei dati personali avviene con la massima diligenza, da personale adeguatamente formato e secondo la normativa vigente. Il Cliente si assume la piena responsabilità circa la proprietà, la veridicità e l'esattezza dei dati gestiti tramite le soluzioni cloud proposte, direttamente o per conto terzi. Il Cliente assicura che l'esattezza dei dati sono nella sua legittima disponibilità, non contrari a norme imperative e non violano alcun diritto d'autore, marchio di fabbrica, segno distintivo, brevetto o altro diritto di terzi. Garantisce di essere in possesso di tutti i necessari consensi e di aver espletato tutti gli adempimenti necessari per assicurare la regolarità del trattamento. Il Cliente esonera infine Clesius da ogni responsabilità ed onere di accertamento e/o controllo a riguardo.

2.12. Clesius è legittima proprietaria del servizio oggetto di affidamento cloud, del Know how, dei concetti, delle idee e delle tecniche di elaborazione dati impiegati e titolare di ogni altro diritto di proprietà intellettuale inerente ai Servizi. L'accesso ai servizi non è mutuabile né cedibile a terzi.

I software oggetto di affidamento cloud sono di esclusiva proprietà di Clesius e il suo utilizzo viene concesso al Cliente in licenza d'uso, non esclusiva e non trasferibile. Il Cliente non ha diritto a ricevere una copia fisica del software utilizzato, né alla concessione di alcun diritto sul software.

Le parti si impegnano a mantenere riservate e non divulgare le informazioni di cui vengono a conoscenza nel corso dell'esecuzione delle attività previste dalla presente proposta.

2.13. Ogni informazione dislocata nel cloud di Clesius è identificata ed etichettata. Un'apposita procedura interna ne garantisce l'applicazione. Clesius rimane a completa disposizione del Cliente sia per fornirgli indicazioni circa la procedura di classificazione delle informazioni che attua sia il registro delle attività di trattamento per il servizio in essere con il Cliente nel ruolo di responsabile.

2.14. La politica di controllo dell'accesso in cloud al servizio cha adotta Clesius prevede la compartimentazione per ciascun servizio cloud.

2.15. Si ricorda che il Cliente deve sempre utilizzare credenziali sufficientemente sicure per autenticare i suoi utenti con profilo amministratore e user. In tale contesto, opportune policy adottate di Clesius impediscono di usare credenziali deboli o inadatte allo scopo. Clesius si riserva di adottare tutte le precauzioni che riterrà più opportune con l'obiettivo di assicurare un sufficiente grado di sicurezza per l'accesso ai servizi.

2.16. Si invita il Cliente a verificare che la procedura di gestione di Clesius per l'allocazione delle informazioni di autenticazione segreta, come le password, soddisfi i propri requisiti.

2.17. Si invita il Cliente a verificare e garantire che l'accesso alle informazioni nel servizio cloud possa essere limitato in conformità con la sua politica di controllo degli accessi e che tali restrizioni siano realizzate. Ciò include:

- La limitazione dell'accesso ai servizi cloud.
- Alle funzioni del servizio cloud.
- Ai dati dei clienti gestiti dal servizio cloud.

2.18. il Cliente identifica i programmi di utilità da utilizzare nel proprio ambiente e assicura che non interferiscano con i controlli del servizio cloud offerti.

2.19. Per il corretto utilizzo dei servizi cloud, il Cliente deve implementare una propria valutazione del rischio e adoperarsi per mitigare i rischi identificati, indipendentemente dai controlli di sicurezza forniti da Clesius.

Clesius adotta una specifica procedura scritta per il controllo e la manutenzione dell'efficacia delle chiavi crittografiche per ciascuna fase del ciclo di vita, ossia: la generazione, la modifica o l'aggiornamento, la memorizzazione, il ritiro, il recupero, il mantenimento e la distruzione.

Normalmente Clesius applica i controlli crittografici su tutte le transazioni da/per il Cliente, con standard di protezione in linea con il mercato, con valutazione periodica dello stato del certificato utilizzato. Quando Clesius offre la crittografia, il Cliente deve esaminare tutte le informazioni fornite da Clesius per confermare se le funzionalità di crittografia:

- soddisfano i suoi requisiti di politica;
- sono compatibili con qualsiasi altra protezione crittografica già utilizzata;
- sono applicate ai dati a riposo e in transito e all'interno del servizio.

Si ricorda che il Cliente non dovrebbe consentire a Clesius di archiviare e gestire le chiavi di crittografia per operazioni crittografiche quando il Cliente impiega la propria gestione delle chiavi o un servizio di gestione delle chiavi separato e distinto.

2.20. Clesius ha specifiche politiche e procedure scritte per lo smaltimento sicuro o il riutilizzo delle risorse. Se richiesto, Clesius fornirà tali documenti.

2.21. Il processo di gestione del servizio in cloud offerto al Cliente deve tenere conto del profilo di accesso al servizio fornito da Clesius. A tale fine, Clesius informa il Cliente sulle modalità di accesso standard, durante l'attivazione del servizio.

2.22. Il Cliente deve assicurarsi che la capacità di erogazione del servizio concordata con Clesius venga soddisfatta. Il Cliente deve monitorare l'utilizzo dei servizi e prevedere le proprie esigenze di capacità richiesta, al fine di garantire le prestazioni dei servizi cloud che gli necessitano nel tempo. Clesius si rendere disponibile a mettere a disposizione adeguati strumenti per facilitare al Cliente questa attività.

2.23. Laddove Clesius applichi funzionalità di backup come parte del servizio cloud, il Cliente deve:

- richiedere le specifiche della capacità di backup da Clesius;
- verificare che le specifiche di backup siano compatibili con le proprie necessità di conservazione.

Clesius adotta sistemi di disaster recovery messi a disposizione dal proprio fornitore di servizi CSP, sia per la parte dei dati e/o informazioni, sia per la parte di software, che per i sistemi, con verifica dei dati backuppati e con periodici test di ripristino. I backup sono crittografati e l'accesso è limitato a personale di Clesius specifico.

Diversamente, il Cliente deve essere responsabile dell'implementazione, mantenimento e verifica e delle funzionalità di backup per i servizi non offerti da Clesius.

2.24. Clesius implementa un set di log standard che consentono di monitorare una serie di eventi. Ciò non toglie che il Cliente è tenuto a verificare se tale set di log è sufficiente e in linea con le proprie politiche; diversamente, deve definire con Clesius i requisiti per la registrazione degli eventi e verificare che il servizio cloud soddisfi tali requisiti.

2.25. Se le operazioni di amministrazione informatica sono delegate al Cliente, è necessario registrare l'operazione e le prestazioni di tali operazioni. Quando questo servizio è erogato da Clesius, il Cliente deve determinare se le funzionalità di registrazione fornite dal Clesius sono appropriate.

2.26. Clesius adotta una policy di sincronizzazione di tutti gli orologi aziendali, e ne verifica periodicamente l'applicazione, in modo da garantire che ogni ambiente sia sincronizzato. Su richiesta, Clesius può fornire informazioni al Cliente sulla policy di sincronizzazione dell'orologio utilizzata per i servizi cloud.

2.27. Il Cliente deve richiedere informazioni a Clesius sulla gestione delle vulnerabilità tecniche che possono influenzare i servizi forniti. In ogni caso, in tale ambito Clesius adotta una propria politica di vulnerability assessment e di penetration test; su esplicita richiesta del Cliente, Clesius è in grado di fornire documentazione a riguardo.

2.28. Ricordiamo che il Cliente deve identificare le vulnerabilità tecniche di cui sarà responsabile e dovrà definire chiaramente un processo per gestirle.

2.29. Clesius adotta una politica di separazione delle reti per ottenere l'isolamento nell'ambiente condiviso per il servizio cloud. Su esplicita richiesta del Cliente, Clesius è in grado di fornire documentazione a riguardo.

2.30. Clesius effettua le operazioni di sviluppo in ambiente sicuro e dedicato, con dati di prova non reali. Le operazioni di sviluppo sono governate da specifiche procedure scritte. Su esplicita richiesta del Cliente, Clesius è in grado di fornire documentazione a riguardo.

2.31. Il Cliente deve includere Clesius nella sua politica di sicurezza delle informazioni, nelle relazioni con i fornitori. Ciò contribuirà a mitigare i rischi associati all'accesso e alla gestione dei dati relativi ai servizi offerti da Clesius.

2.32. Il Cliente deve confermare i ruoli e le responsabilità in materia di sicurezza delle informazioni relative al servizio cloud, descritti nel contratto di servizio. Questi possono includere, a seconda dei servizi offerti, i seguenti processi:

- protezione da malware;
- backup;
- controlli crittografici;
- gestione della vulnerabilità;
- gestione degli incidenti;
- controllo della conformità tecnica;

- test di sicurezza;
- auditing;
- raccolta, manutenzione e protezione delle prove, compresi i registri e le liste di controllo;
- protezione delle informazioni al termine del contratto di servizio;
- autenticazione e controllo degli accessi;
- identità e gestione degli accessi.

2.33. Clesius ha una specifica procedura scritta per la gestione degli incidenti di sicurezza delle informazioni in ottemperanza alle normative vigenti. Il Cliente deve verificare se l'assegnazione delle responsabilità per la gestione degli incidenti di sicurezza delle informazioni è adeguate e deve assicurarsi che soddisfi i propri requisiti.

In caso di incidente che coinvolga la perdita di una o più caratteristiche tra Riservatezza, Integrità, Disponibilità, riguardanti informazioni personali (Data Protection), è compito della Parte che identifica l'incidente dare immediata informazione all'altra Parte. Ove necessario, entro un tempo massimo di 48 ore, deve essere deciso di comune accordo quale delle due Parti debba aprire il Data Breach, ed inviare entro un massimo di 72 ore la comunicazione al Garante della Privacy, così come previsto dal Regolamento UE 2016/679 – GDPR.

2.34. Il Cliente deve richiedere informazioni a Clesius riguardo ai meccanismi per:

- segnalare a Clesius un evento di sicurezza delle informazioni che ha rilevato;
- ricevere segnalazioni riguardanti un evento di sicurezza delle informazioni rilevato da Clesius;
- tenere traccia dello stato di un evento di sicurezza delle informazioni segnalato.

2.35. Il Cliente deve considerare che Leggi e Regolamenti pertinenti che possono essere quelli delle giurisdizioni che regolano Clesius, oltre a quelli che regolano lui stesso. Il Cliente deve richiedere evidenza della conformità di Clesius con le normative e gli standard pertinenti richiesti per le sue attività. Tali prove possono essere le certificazioni prodotte dagli auditor di terze parti in ambito ISO.

2.36. Si ricorda che il Cliente deve richiedere informazioni a Clesius sulla protezione dei record raccolti e archiviati da Clesius rilevanti per l'utilizzo dei servizi. Clesius si impegna a fornire tali informazioni.

2.37. Si ricorda che il Cliente deve richiedere prove documentate che l'implementazione dei controlli di sicurezza delle informazioni e linee guida per il servizio cloud sia in linea con quanto definito in sede contrattuale. Tali prove devono includere certificazioni rispetto agli standard pertinenti. A tal proposito, Clesius è in possesso di varie certificazioni del proprio sistema; per maggiori dettagli, si veda il sito www.clesius.it.

2.38. Si ricorda che il Cliente deve definire o estendere le sue politiche e procedure esistenti in conformità con il suo uso dei servizi cloud e rendere gli utenti del servizio consapevoli dei loro ruoli e responsabilità nell'uso del servizio cloud.

2.39. Si ricorda che il Cliente può richiedere a Clesius una descrizione documentata del processo di cessazione del servizio che copra il reso e la rimozione delle risorse del Cliente seguita dalla cancellazione di tutte le copie di tali risorse dai sistemi di Clesius. La riconsegna dei dati avverrà in modo sicuro, attraverso canali protetti. Avvenuta la restituzione, i dati "in linea" del CLIENTE saranno immediatamente eliminati, attraverso metodi di cancellazione sicura. Quando è attivo un servizio di backup (si veda punto 2.20), il Cliente deve essere consapevole della complicazione delle operazioni necessarie all'eliminazione definitiva dei dati del Cliente dai backup di Clesius, e pertanto accetta che questi rimangano nei backup di Clesius al più e non oltre 12 mesi. Qualora il Cliente richieda comunque

di procedere all'eliminazione definitiva immediata dei dati dai backup, invierà una richiesta formale, adeguatamente motivata e giustificata.

Trento, 22/06/2026

CLESIUS S.R.L.
Amministratore Unico

ELENCO REVISIONI

Revisione	Data	Motivo della Revisione	Visto Preparazione	Visto Approvazione
01	22/06/2026	Documento di nuova adozione	SGI	Alta Direzione