Allegato Tecnico
Cloud Virtual Data Center

release	1.0
data	31.10.2023
redazione documento	Federico Calò, Licia Mignardi, Alessandro Sabbi
verifica documento	Federico Calò, Licia Mignardi
approvazione documento	Gianluca Mazzini

Nota di lettura

Lepida ScpA, di seguito Lepida, si riserva la facoltà di poter intervenire sulle misure tecniche e organizzative descritte nel presente documento, al fine di rendere il sistema conforme alle successive indicazioni normative che dovessero subentrare in argomento. Si riserva inoltre di intervenire per la correzione di meri errori materiali o refusi.

1. Descrizione del Servizio

1.1. Definizioni e acronimi

- **API** - Application Programming Interface: insieme di servizi usabili tramite programmi per l'accesso alle funzioni di interazione con il sistema di gestione dell'infrastruttura Cloud del Tenant
- **Cloud** - insieme condiviso di risorse di sistema (risorse computazionali, storage, rete), che consentono l'astrazione del livello di competenza del Cliente ai soli sistemi virtuali, evitando i costi di gestione e di acquisto delle infrastrutture fisiche, che sono sotto la responsabilità del provider
- **CVDC** - Cloud Virtual Data Center
- **IAAS** - Infrastructure As A Service: le risorse computazionali (macchine virtuali, storage, rete) sono fornite come infrastruttura, ovvero sono in gestione totale da parte del Cliente, con le responsabilità che ne derivano
- **Tenant** - entità organizzativa che rappresenta il Cliente tramite un pool di risorse e credenziali di amministrazione per l'accesso all'interfaccia di gestione
- **VM** - Virtual Machine: macchine virtuali che il Tenant definisce e gestisce entro il pool di risorse assegnatogli contrattualmente.

1.2. Descrizione generale

Il servizio Cloud Virtual Data Center erogato da Lepida ScpA può essere fruito a seguito di un contratto stipulato tra Lepida ScpA e il Cliente, di cui il presente documento costituisce l'allegato tecnico. All'atto della adesione al servizio, il presente documento

entra a far parte del contratto formale tra Lepida e il Cliente e obbliga entrambe le parti a quanto di seguito indicato, nel rispetto dei reciproci ruoli e responsabilità.

Il servizio CVDC consente al Cliente la creazione di una propria infrastruttura virtuale (in ambiente condiviso), all'interno di un pool di risorse virtuali ad esso assegnate. Si tratta pertanto di un servizio Cloud IAAS, per il quale Lepida ScpA (Provider) rende disponibile e gestisce l'infrastruttura fisica che consente al Cliente (Tenant) la creazione di una propria infrastruttura virtuale, segregata da quella di ogni altro Cliente e da quella di Lepida ScpA stesso, e rispetto alla quale il Tenant ha il totale controllo in autonomia delle risorse assegnate.

1.2 Principali caratteristiche e funzionalità

Il servizio CVDC permette al Cliente di creare e gestire in autonomia uno o più Virtual Data Center contenenti risorse virtuali quali server, aree di storage, reti. Al Cliente viene assegnato un pool di risorse definite in termini di:

- Cicli di CPU (in Ghz)
- GB Ram
- GB Storage
- Indirizzi IP Pubblici
- Utenze di Gestione.

All'interno di tali risorse il Cliente ha autonomia, attraverso web console e API, nel creare il proprio CVDC per:

- creare macchine virtuali dotate ciascuna delle risorse computazionali (VCPU, RAM, storage) ad esse assegnate, esclusivamente a partire da template base messi a disposizione dal provider, presenti in un catalogo esposto dallo strumento;
- usare le reti virtuali a disposizione, secondo la topologia predefinita del servizio, e assegnare alle macchine virtuali indirizzi IP Pubblici messi a disposizione da Lepida ScpA o indirizzi IP privati del Cliente stesso (previa adeguata configurazione della Rete Lepida);
- effettuare in autonomia snapshot delle VM del Tenant, mentre per l'eventuale ripristino delle immagini salvate, è necessario ricorrere all'assistenza Lepida.
  E' consentita la creazione di una sola snapshot per ciascuna VM.

Il Cliente ha il pieno controllo dei sistemi creati, ne possiede le credenziali di amministrazione ed ha in carico la completa gestione del software e dei dati da essi trattati, comprese tutte le problematiche di sicurezza e protezione dei dati, fatto salvo gli obblighi di Lepida ScpA.

Il servizio CVDC viene erogato attraverso i data center regionali gestiti da Lepida ScpA, collegati nativamente alla Rete Lepida.

1.3. Fruizione del servizio

Ogni Tenant ha la propria configurazione dedicata nell'infrastruttura virtuale che gli viene fornita, completamente segregata rispetto a quella di altri Tenant e dalla parte di infrastruttura di Lepida ScpA. Ha inoltre un proprio amministratore, configurato sul sistema di gestione, al quale accede tramite autenticazione.
L'Ente è tenuto a comunicare a Lepida ScpA i riferimenti del proprio Referente Tecnico cui verrà assegnato il ruolo di amministratore del Tenant. L'Ente dovrà comunicare eventuali variazioni del proprio referente.

L'amministratore del Tenant può successivamente registrare e assegnare i diritti a ulteriori utenti del Cliente.

Il portale di accesso al servizio è disponibile alla url https://vracloud.lepida.it/vcac/org/enti/[nomente], raggiungibile solamente via VPN opportunamente configurata per il cliente.

A seguito dell'accesso al portale Cloud con le credenziali amministrative per il proprio Tenant, l'amministratore del Tenant potrà in autonomia creare e gestire tutti gli elementi costitutivi del proprio Virtual Data Center (risorse delle VM, storage e virtual network).

Attraverso la console di gestione l'amministratore può inoltre effettuare, limitatamente al Tenant, il monitoraggio dello stato delle VM e dei loro parametri principali di utilizzo e accedere alle informazioni di log rilevanti per la gestione del servizio, comprensivi degli accessi alla console di gestione e delle chiamate API effettuate.

Lepida ScpA mette a disposizione dei Clienti documenti di supporto per l'utilizzo della console di gestione.

Il Cliente ha inoltre la possibilità di accedere al servizio anche attraverso API per le quali viene fornita documentazione tecnica per l'utilizzo.

1.4. Licenze software

Sono a carico di Lepida ScpA tutte le licenze per il software installato sulla piattaforma fisica utilizzata per l'erogazione del servizio CVDC, ovvero dei sistemi di virtualizzazione, degli storage, della rete e del portale di gestione.

Sono invece a carico del Tenant tutte le licenze necessarie per il software (di base e applicativo) installato sulle macchine virtuali da lui gestite. In tutti i casi è compito del Cliente verificare se il licensing dei software da esso utilizzati sulle proprie macchine virtuali è conforme alle regole imposte dal produttore per gli ambienti virtuali e fare in modo di essere conforme, rispondendo direttamente di ogni anomalia eventuale.

1.5. Backup

Lepida ScpA, qualora richiesto ed acquistato dal cliente, mette a disposizione un sistema di backup centralizzato ed automatico che gestisce le copie delle VM, tramite snapshot delle VM senza quiescenza degli applicativi. Il backup viene conservato su infrastrutture storage fisicamente distinte da quelle di produzione in un differente data center. Viene applicata la seguente policy di backup: scheduling giornaliero con retention di 7 giorni.

Il Cliente può richiedere a Lepida ScpA di effettuare fino a 2 test di restore annuali. In tali casi Lepida ScpA si impegna a trasmettere al Cliente i report dei test eseguiti.

Il servizio viene presidiato da personale dedicato che controlla il corretto svolgimento della schedulazione, intervenendo tempestivamente in caso di problemi.

Il restore non può essere eseguito in autonomia dal Cliente, ma deve essere richiesto dal Referente Tecnico del Cliente tramite i canali messi a disposizione da Lepida ScpA per il supporto tecnico. Esso comporterà il ripristino dell'intera VM, lasciando al Cliente il compito di ulteriori azioni. Lepida ScpA si impegna ad avviare il restore al più entro 8 ore lavorative dalla richiesta. Per nessun motivo Lepida ScpA farà restore di VM del Cliente, se non a fronte di una richiesta ricevuta dal Cliente.

1.6. Disaster Recovery

Lepida ScpA offre la possibilità di acquistare un servizio opzionale aggiuntivo di disaster recovery (DR) per assicurare il ripristino del Virtual Data Center del Tenant in un sito secondario in caso di incidente disastroso occorso al sito di produzione.

Il DR è normalmente spento e si può attivare una volta all'anno, per test di durata massima 15 giorni, in una bolla di rete, che isola il contesto dal resto di Internet. I test di DR devono essere concordati con Lepida ScpA. Il Cliente viene messo in condizione di verificare il funzionamento delle sue applicazioni collegandosi alla bolla.

Il DR è attivabile solo da parte di Lepida ScpA. In caso di occorrenza di un evento disastroso al sito di produzione, Lepida ScpA si impegna a informarne tempestivamente il Cliente. Compete quindi al Cliente la decisione in merito all'opportunità di attivare il servizio di DR, nel quale caso deve farne richiesta a Lepida ScpA. In tal caso Lepida ScpA si impegna ad attivare la procedura di DR al più entro 4 ore lavorative dalla richiesta. Lepida ScpA manterrà comunque costantemente aggiornato il Cliente sull'evoluzione della situazione fino alla conclusione dell'emergenza.

1.7. Localizzazione del servizio

I siti di erogazione del servizio ove sono conservati i dati sono ubicati presso i quattro data center regionali situati a Ferrara, Ravenna, Parma e Modena. All'attivazione dell'erogazione del servizio viene selezionato il sito primario e contestualmente comunicato al cliente.
Lepida ScpA si impegna a comunicare al Cliente, con adeguato preavviso, ogni variazione all'ubicazione del sito.

In caso di acquisto del servizio di disaster recovery, il sito secondario verrà selezionato tra i rimanenti.

1.8. Evoluzione dell'infrastruttura e del servizio

Al fine di garantire che le piattaforme utilizzate per l'erogazione del servizio CVDC siano mantenute sempre allineate allo stato dell'arte della tecnologia, e quindi l'evoluzione degli ambienti in linea con i requisiti di sicurezza delle informazioni, Lepida ScpA si impegna a predisporre adeguate roadmap evolutive, annuali, di tipo infrastrutturale ed

applicativo, in modo da permettere gli aggiornamenti dell'infrastruttura e del software con una continua valutazione e gestione del rischio.

1.9. Aggiornamenti software e manutenzioni programmate

Lepida ScpA si riserva una finestra per effettuare gli aggiornamenti software e le manutenzioni programmate della propria infrastruttura Cloud. Tipicamente tali interventi interessano i sistemi di gestione (es: portale di accesso, sistemi di monitoraggio e raccolta metriche, etc) e non impattano la funzionalità delle VM del Tenant. L'interruzione del servizio è breve, solitamente in orario notturno e comunque al di fuori degli orari di punta (9-17), e non viene notificata preventivamente al Cliente.

Eventuali manutenzioni di componenti infrastrutturali o aggiornamenti software che invece possano impattare sulla produzione (es. funzionalità delle VM o della rete) vengono comunicati al Referente Tecnico del Cliente con almeno 3 giorni lavorativi di anticipo rispetto alla data di pianificazione, e fatti seguire da ulteriori comunicazioni all'avvio e alla conclusione dell'attività. Eccezionalmente interventi urgenti inerenti la sicurezza possono essere effettuati senza preavviso se ritenuti particolarmente critici, ma con notifica a posteriori.

1.10. Gestione dei malfunzionamenti, degli incidenti di Sicurezza e dei data breach

Lepida ScpA assicura la gestione H24x365 dei malfunzionamenti e degli incidenti aventi impatto sulla disponibilità del servizio CVDC o sull'integrità o riservatezza dei dati trattati.

I malfunzionamenti/incidenti di competenza del provider sono, per il caso Cloud IAAS cui si riferisce questo servizio, quelli relativi alle infrastrutture e alle interfacce di gestione e di logging del servizio Cloud, o le eventuali segnalazioni di furti di credenziali rispetto alle quali sia richiesta una azione rapida del provider (blocco, reset). Restano esclusi eventuali malfunzionamenti/incidenti che avvengano entro il perimetro delle macchine del Cliente. In questi casi il Cliente può comunque effettuare una segnalazione a Lepida ScpA qualora fosse necessaria qualche forma di supporto per il confinamento o per la raccolta delle evidenze (tramite log, backup o cloni forensi).

I malfunzionamenti/incidenti possono essere rilevati sia attraverso un monitoraggio proattivo da parte di Lepida ScpA sia tramite la ricezione di segnalazioni fatte pervenire dai Clienti attraverso i canali messi a disposizione da Lepida ScpA per il supporto tecnico.

Al momento dell'apertura del ticket relativo a un malfunzionamento/incidente questo deve essere classificato in relazione alla gravità, assegnandogli uno dei seguenti valori:

- gravità alta: in caso di interruzione del servizio o di impatto grave sull'integrità o riservatezza dei dati;
- gravità media: in caso di impatto medio sulla disponibilità del servizio o sull'integrità o riservatezza dei dati;
- gravità bassa: in caso di impatto basso sulla disponibilità del servizio o sull'integrità o riservatezza dei dati.

Lepida ScpA si impegna ad assicurare i livelli di servizio relativi alla risoluzione del malfunzionamento/incidente riportati al § 4.1, dipendenti dalla gravità ad esso assegnata. In fase di analisi la sua gravità può essere modificata a proprio insindacabile giudizio da parte di Lepida ScpA.

Il Cliente viene mantenuto aggiornato in relazione alla gestione del malfunzionamento/incidente fino alla sua risoluzione nelle seguenti modalità:

- in caso di segnalazione proveniente dal Cliente: attraverso il sistema di trouble ticketing a cui il Cliente può accedere autonomamente;
- in caso di rilevazione da parte di Lepida ScpA: tramite mail successiva alla rilevazione del malfunzionamento/incidente e ulteriore mail successiva alla sua risoluzione.

Lepida ScpA si impegna ad assicurare i livelli di servizio relativi al supporto tecnico riportati al § 4.1.

Ogni qualvolta possibile, a seguito della risoluzione del malfunzionamento/incidente, Lepida ScpA ne richiede una verifica da parte del Cliente prima della chiusura del ticket.

In caso di eventi catastrofici, Lepida ScpA ha previsto l'attivazione di una unità di crisi, che assume la responsabilità di dichiarare lo stato di "emergenza" e coordinare la gestione della stessa, comprese le comunicazioni verso l'esterno, così come previsto nel Piano di continuità operativa aziendale. La gestione dell'emergenza può richiedere

l'attivazione del Disaster Recovery, se acquistato dal Cliente. In tali casi Lepida ScpA si impegna a informare tempestivamente il Cliente e a mantenerlo costantemente aggiornato sull'evoluzione della situazione fino alla conclusione dell'emergenza.

Quando l'incidente si configura come violazione di dati personali, Lepida ScpA procede in ottemperanza agli Art. 33 e 34 del Regolamento UE 2016/679 (GDPR) e in particolare:

- se l'incidente interessa dati personali di cui Lepida ScpA è Titolare (es. anagrafiche con i recapiti degli utenti predisposti per il servizio), provvede a effettuare una valutazione dei rischi per i diritti e le libertà delle persone fisiche, e successivamente alla eventuale notifica al Garante Privacy entro 72 ore dal momento in cui ne è venuta a conoscenza, e alla eventuale comunicazione agli interessati;
- se l'incidente interessa dati personali di cui Lepida ScpA è Responsabile (es. dati del Cliente raccolti attraverso il servizio CVDC), provvede a informarne il Cliente Titolare entro 72 ore dal momento in cui ne è venuta a conoscenza o comunque non oltre i termini definiti nell'accordo di designazione.

Qualora Lepida ScpA si accorgesse o fosse informato da soggetti terzi della presenza di comportamenti anomali di indirizzi IP di competenza del Cliente, Lepida ScpA informerà tempestivamente il Cliente target aprendo un ticket specifico, riservandosi azioni di sospensione della connettività per gli indirizzi IP coinvolti, se fossero a rischio componenti infrastrutturali o per ridurre effetti avversi o disservizi all'infrastruttura.

1.11. Sicurezza delle Informazioni e compliance normative

Lepida ScpA è certificata rispetto alle norme ISO 9001 e ISO/IEC 27001, estesa con i controlli previsti nelle norme ISO/IEC 27017 e ISO/IEC 27018, per il servizio CVDC, che eroga nel ruolo di Cloud Service Provider fornendo i propri servizi al Cloud Service Customer. Viene quindi sottoposta annualmente ad audit da parte dell'Ente Certificatore esterno per la conferma della certificazione stessa.

Al fine di garantire la conformità sia alla suddetta norma sia ai requisiti cogenti applicabili (in particolare GDPR, Misure Minime di Sicurezza ICT per le PA emanate da AgID, requisiti di qualificazione Agid per i CSP della PA), Lepida ScpA si è dotata di adeguate misure tecniche e organizzative, che provvede a attuare, monitorare,

correggere e migliorare in modo continuativo. Di seguito vengono sinteticamente riportate le principali misure adottate:

- sicurezza fisica dei Data Center coinvolti: videosorveglianza, impianto antintrusione, controllo accessi, servizio di vigilanza;
- sicurezza ambientale e delle infrastrutture di supporto dei data center: impianto antincendio, sensori antiallagamento, impianto di condizionamento idronico ridondato, unità di condizionamento in row all'interno delle cage, impianto elettrico ridondato, sistemi di continuità elettrica e gruppo elettrogeno, esecuzione di manutenzioni preventive e test periodici;
- progettazione delle infrastrutture e dei servizi CVDC effettuata prendendo in considerazione la sicurezza sin dalla fase di design, ma anche nelle fasi di implementazione (deploy) e di major change;
- progettazione e implementazione delle infrastrutture e delle piattaforme utilizzate per l'erogazione del servizio CVDC, e delle relative evoluzioni, al fine di garantire la continuità operativa tramite l'uso di ridondanze e meccanismi di alta affidabilità in tutti i componenti (es. facility, rete, server, storage, piattaforma di virtualizzazione);
- esecuzione di analisi e valutazioni dei rischi con periodicità annuale o in caso di cambiamenti significativi;
- utilizzo di un sistema di gestione degli asset e delle configurazioni centralizzato per tutte le componenti fisiche, le VM e i software;
- cancellazione sicura dei dati dei clienti in caso di cessazione del servizio;
- gestione degli accessi ai sistemi e alle applicazioni da parte dei clienti e del provider: procedure per la registrazione/deregistrazione degli utenti e per l'assegnazione/revoca dei diritti di accesso, account individuali, password policy, protocolli di logon sicuri, registrazione e conservazione dei log degli accessi;
- cifratura dei dati in transito tramite l'adozione di protocolli che la implementano (es. TLS, SSH, RDP) e negli storage del provider;
- sincronizzazione del clock dell'infrastruttura cloud con una fonte di riferimento affidabile, che può essere utilizzata anche nelle VM dei Clienti;
- registrazione dei log relativi a funzionamento, prestazioni, utilizzo e sicurezza (es. accessi) dell'infrastruttura cloud e loro conservazione per almeno 6 mesi;
- monitoraggio H24x365 dell'infrastruttura e del servizio (non delle VM e degli applicativi dei Clienti) per prevenire e rilevare criticità e incidenti;

- esecuzione periodica di verifiche di sicurezza (es. vulnerability assessment, penetration test) su infrastruttura e servizi applicativi;
- rilevazione e gestione delle vulnerabilità tecniche e hardening dell'infrastruttura;
- gestione degli aggiornamenti software e delle manutenzioni programmate all'infrastruttura (change) secondo quanto riportato al § 1.9;
- backup dei componenti dell'infrastruttura di competenza del provider e delle VM del Cliente secondo quanto riportato al § 1.5;
- continuità operativa e disaster recovery secondo quanto riportato al § 1.6;
- gestione dei malfunzionamenti e degli incidenti di sicurezza, inclusi i data breach, secondo quanto riportato al § 1.10;
- servizio di supporto tecnico ai clienti H24x365 e sistema di trouble ticketing accessibile dai clienti per segnalazioni di malfunzionamenti e incidenti e per richieste di modifica delle risorse acquistate o di configurazioni di competenza del provider;
- segregazione tra le risorse di amministrazione dell'infrastruttura cloud e gli ambienti dei Tenant e tra gli ambienti, le reti e i dati dei singoli Tenant, anche a livello di logging e interfacce di gestione, attraverso l'uso di applicazioni multitenant per la gestione di reti e sistemi virtuali con funzionalità di isolamento e di adeguati protocolli e configurazioni;
- utilizzo di personale tecnico professionale e altamente qualificato, di cui viene assicurata la formazione continua e la consapevolezza in tema di continuità e disponibilità del servizio e sicurezza delle informazioni;
- utilizzo di fornitori adeguatamente selezionati e qualificati, e le cui attività sono strettamente monitorate e tenute sotto controllo.
- presenza di sistemi e dispositivi di protezione a livello perimetrale (next generation firewall e IPS) in grado di controllare e filtrare il traffico di rete interessato.

Rispetto alla sicurezza delle informazioni ed in generale alla gestione dell'infrastruttura virtuale, si evidenzia altresì il ruolo del Tenant (Cliente) che deve gestire e rispondere dei propri asset (definiti tramite il portale di gestione che fornisce una naturale interfaccia di management dell'asset cliente), della corretta implementazione della sicurezza tramite la definizione delle policy di sicurezza, su cui è autonomo, e del disegno delle proprie architetture di CVDC, adottando le misure che ritiene idonee per garantire la

funzionalità, affidabilità, integrità e riservatezza opportune, ed implementando azioni di controllo, logging, aggiornamento dei sistemi, e gestione accessi e amministratori di sistema come prescritto dalle normative vigenti.

Nel caso in cui il Cliente ritenga necessario lo svolgimento di un audit o ispezione presso Lepida ScpA per verificare il rispetto degli adempimenti contrattuali in termini di sicurezza, occorre che la richiesta venga formalizzata tramite canali ufficiali (PEC o equivalente) e trasmessa con congruo anticipo (almeno 30 giorni solari) per consentire la pianificazione dell'attività, che non potrà comunque durare più di 8 ore.

2. Attivazione del servizio

Il Cliente, in fase di sottoscrizione del contratto, deve definire i propri requisiti in termini di risorse computazionali facendo riferimento alla seguente tabella:

Parametro	Unità di misura	Valore minimo	Tagli Incrementali
Cicli CPU - potenza calcolo	Ghz	1	1
RAM - memoria disponibile	GB	8	2
STORAGE - disco	GB	100	100
STORAGE - disco SSD	GB	0	100

Nella tabella sopra sono indicati per ogni parametro il valore minimo e i "tagli" di incremento possibili. Per ciascun parametro possono essere acquistate dal Cliente risorse pari al valore minimo più un multiplo intero del taglio incrementale.

Il Cliente deve inoltre comunicare a Lepida ScpA eventuali configurazioni richieste sulla Rete Lepida per poter utilizzare il servizio CVDC dalla propria sede.

Il Cliente deve infine indicare un proprio Referente Tecnico (Nome Cognome, Codice Fiscale, mail, numero telefonico) al quale verrà intestata l'utenza personale per l'accesso al sistema di gestione Cloud. Lo stesso sarà anche il destinatario delle comunicazioni da parte di Lepida ScpA relative a change o ad incidenti.

In fase di setup del servizio Lepida ScpA provvederà allo svolgimento delle configurazioni richieste sulla Rete Lepida e all'allocazione delle risorse virtuali acquistate dal Cliente sulla propria infrastruttura Cloud entro 30 giorni solari dalla ricezione della richiesta debitamente formalizzata (es. sottoscrizione del contratto), salvo diversi accordi tra le parti. Il servizio si considererà attivato nel momento in cui il Referente Tecnico del Cliente riceverà le credenziali amministrative per l'accesso al sistema di gestione Cloud. Nel caso in cui riscontri problematiche sul setup del servizio, il Cliente è tenuto a segnalarle a Lepida ScpA e a richiedere la posticipazione dell'avvio del servizio fino alla relativa risoluzione.

La tariffazione del servizio avviene sulla base delle risorse massime allocate al Virtual Data Center del Cliente, definite al momento della stipula del contratto e successivamente modificabili su richiesta del Cliente. Il Cliente ha la possibilità di mantenere visibilità sulle risorse acquistate attraverso l'interfaccia di gestione del servizio Cloud.

3. Esercizio del servizio

Lepida ScpA assicura la completa gestione della propria infrastruttura cloud, comprensiva delle seguenti attività: aggiornamenti software, manutenzioni programmate e straordinarie, gestione della sicurezza dell'infrastruttura e del servizio, monitoraggio e gestione degli incidenti, evoluzione dell'infrastruttura e del servizio, supporto tecnico ai Clienti, gestione dei backup delle VM presenti nei CVDC dei Clienti. Inoltre Lepida ScpA è responsabile della gestione della sicurezza fisica e ambientale e delle infrastrutture di supporto dei data center regionali, oltre che della Rete Lepida a cui essi sono collegati.

E' invece di completa responsabilità del Cliente la gestione della propria infrastruttura virtuale, delle macchine virtuali create su di essa e degli applicativi ospitati sulle VM, comprensiva della relativa sicurezza.

4. Gestione e monitoraggio

Le attività di gestione e monitoraggio del sistema da parte di Lepida prevedono gli aggiornamenti software, l'analisi proattiva delle performance, il monitoraggio delle risorse e di eventuali problemi.

4.1. Livelli di servizio

Lepida ScpA si impegna ad assicurare il rispetto dei livelli di servizio riportati di seguito.

Disponibilità del servizio: percentuale di tempo in un dato periodo di riferimento in cui il servizio risulta essere accessibile e usabile, tenendo conto dei fermi programmati	
Regole di misurazione	Finestra di erogazione del servizio: H24 x 365 Il calcolo dell'indicatore si basa sulle misurazioni eseguite da Lepida ScpA Periodo di riferimento: annuale Vengono considerati i fermi: ● occorsi e risolti nel periodo di osservazione corrente ● occorsi nel periodo di osservazione precedente e risolti in quello corrente.
Formula di calcolo	$\frac{Tempo\_totale - \sum Durata\_fermo}{Tempo\_totale} \times 100$ dove: ● Durata_fermo=durata del singolo fermo ● Tempo_totale = tempo contrattuale di erogazione del servizio nel periodo di riferimento esclusi i tempi di fermo programmati
Regole di arrotondamento	La percentuale va arrotondata alla frazione decimale di punto sulla base del secondo decimale:

	• per difetto se la parte decimale è minore o uguale a 0,05 • per eccesso se la parte decimale è maggiore di 0,05
Obiettivo	99,8%
Esclusioni	La disponibilità del servizio viene calcolata al netto di: • fermi programmati da Lepida ScpA • fermi richiesti dal Cliente • fermi dovuti a malfunzionamenti attribuibili al Cliente o non direttamente attribuibili a Lepida ScpA • fermi dovuti a interventi straordinari da effettuarsi con urgenza ad insindacabile giudizio di Lepida ScpA per mitigare minacce alla sicurezza dell'infrastruttura o dei dati da essa trattati • fermi causati da azioni non direttamente imputabili a Lepida ScpA, ovvero cause di forza maggiore • situazioni di disastro che coinvolgono il sito data center di erogazione del servizio. Tale condizione di esclusione non si applica nei casi in cui sia stato acquistato il servizio opzionale di disaster recovery.

Tempo massimo di prima risposta del supporto tecnico di cui al §5: tempo massimo che intercorre tra la segnalazione di un inconveniente/incidente da parte del Cliente e la risposta iniziale alla segnalazione da parte del Provider	
Regole di misurazione	Finestra di erogazione del supporto tecnico: H24 x 365 Il calcolo dell'indicatore si basa sulle misurazioni eseguite da Lepida ScpA

	Periodo di riferimento: quadrimestrale Viene considerato il tempo intercorrente tra il primo tentativo documentato di segnalazione del disservizio da parte del Cliente e l'emissione del relativo Ticket
Obiettivo	Segnalazione con gravità alta: entro 1 ora nel 90% dei casi Segnalazione con gravità media: entro 6 ore nel 90% dei casi Segnalazione con gravità bassa: entro 12 ore nel 90% dei casi

Tempo massimo di risoluzione di un guasto o malfunzionamento sull'infrastruttura	
Regole di misurazione	Finestra di erogazione del supporto tecnico: H24 x 365 Il calcolo dell'indicatore si basa sulle misurazioni eseguite da Lepida ScpA Periodo di riferimento: annuale Viene considerato il tempo intercorrente tra il primo tentativo documentato di segnalazione del disservizio da parte del Cliente e la risoluzione del problema effettivamente riscontrato
Obiettivo	Segnalazione con gravità alta: entro 4 ore nel 95% dei casi - entro 6 ore nel 100% dei casi Segnalazione con gravità media: entro 36 ore nel 95% dei casi - entro 48 ore nel 100% dei casi Segnalazione con gravità bassa: entro 120 ore nel 95% dei casi - entro 168 ore nel 100% dei casi

4.2. Cessazione del servizio

La richiesta di cessazione del servizio da parte di un Cliente deve essere fatta pervenire a Lepida ScpA via PEC e può essere effettuata in qualunque momento.

In caso di cessazione del servizio il Cliente ha a disposizione gli strumenti forniti dalla console di gestione per provvedere in autonomia e in qualsiasi momento a recuperare e trasferire su propri sistemi tutti i dati e le configurazioni presenti sul CVDC nel formato standard OVF, esportando e trasferendo via rete le immagini delle macchine virtuali.

In caso di cessazione, il Cliente è tenuto a completare l'esportazione dei propri dati entro la data di cessazione stessa.

In situazioni particolari (es. grosso volume di dati) è possibile richiedere supporto tecnico a Lepida ScpA per l'esportazione dei dati. Lepida ScpA si impegna ad erogare tale servizio entro 30 giorni solari dalla richiesta formalizzata, comunicando le relative modali.

Trascorsa la data di cessazione del servizio, Lepida ScpA provvederà:

- entro 10 giorni solari, alla disattivazione delle credenziali di accesso al servizio Cloud (per il Cliente non sarà più possibile la connessione) e di quelle relative al supporto, in assenza di altri servizi;
- entro 30 giorni solari, alla deallocazione delle risorse assegnate al CVDC rimuovendo gli oggetti eventualmente ancora presenti (es. VM, backup), compresi i dati del Cliente.

La cancellazione dei dati del Cliente conservati dai sistemi di storage avviene mediante "de-linking", procedura che dissolve le LUN allocate restituendole al pool generale, rendendo così inaccessibile ogni contenuto originale, dal momento che i dati sono conservati su sistemi storage condivisi con altri servizi e sono quindi impraticabili altre forme di cancellazione.

5. Servizio di assistenza

Lepida ScpA mette a disposizione dei Clienti un servizio di supporto tecnico disponibile H24x365, accessibile mediante i canali di comunicazione riportati nel sito Internet aziendale al link https://www.lepida.net/assistenza/richiesta-assistenza-data center-cloud, al fine di consentire sia le segnalazioni di malfunzionamenti e incidenti

relativi alla sicurezza e alla fruibilità del servizio sia le richieste di modifica delle risorse acquisite o di configurazioni di competenza del provider. Inoltre ai Clienti viene fornito l'accesso in autonomia a un sistema di trouble ticketing, al fine di mantenere la visibilità sul processo di gestione dei ticket.

Al momento dell'apertura del ticket relativo a un malfunzionamento/incidente questo deve essere classificato dal Cliente in relazione alla gravità, assegnandogli uno dei seguenti valori:

- gravità alta: in caso di interruzione del servizio o di impatto grave sull'integrità o riservatezza dei dati;
- gravità media: in caso di impatto medio sulla disponibilità del servizio o sull'integrità o riservatezza dei dati;
- gravità bassa: in caso di impatto basso sulla disponibilità del servizio o sull'integrità o riservatezza dei dati.

In fase di analisi la sua gravità può essere modificata a proprio insindacabile giudizio da parte di Lepida ScpA.