Misure di sicurezza delle informazioni per i servizi di datacenter

1. Obiettivi e generalità

Obiettivo del presente documento è descrivere le principali misure di sicurezza fisiche, tecniche e organizzative adottate da Lepida per assicurare sia la continuità e la disponibilità dei propri servizi di datacenter sia l'integrità e la riservatezza dei dati trattati da essi.
Quelle di seguito riportate rappresentano anche le misure che Lepida (in qualità di Responsabile), in mancanza di ulteriori o più specifiche misure richieste dai clienti (in qualità di Titolari), ritiene adeguate per i dati personali dei clienti trattati dai servizi di datacenter, al fine di garantire un livello di sicurezza adeguato al rischio come previsto dal Regolamento UE 2016/679 (GDPR).
Il campo di applicazione del presente documento è costituito dai seguenti servizi di datacenter offerti da Lepida agli Enti Soci:

- Housing;
- Blade as a service/Computing Blade as a service;
- Storage as a service;
- Server Virtuali;
- Database as a service;
- Backup as a service;
- Data Domain as a service;
- Firewall as a service;
- SIEM as a service.

Le caratteristiche e le modalità di erogazione dei suddetti servizi sono descritte nei relativi Allegati Tecnici al contratto, laddove presenti, pubblicati sul sito Internet di Lepida al link https://lepida.net/contratti-listini/allegati-tecnici-servizi.
Tali servizi vengono erogati attraverso tre datacenter, collocati all'interno della regione Emilia-Romagna, progettati, realizzati e gestiti da Lepida.
Lepida implementa un sistema di gestione per la sicurezza delle informazioni, certificato secondo la norma ISO/IEC 27001, che comprende nel proprio campo di applicazione anche i servizi di datacenter e i siti da cui sono erogati. Il presente documento utilizza come riferimento i controlli applicabili presenti nell'Appendice A della norma.
In caso di incongruenze tra quanto riportato nel presente documento e quanto negli Allegati Tecnici succitati, occorre fare riferimento a questi ultimi.

2. Descrizione dei servizi di datacenter e responsabilità in capo a Lepida e ai clienti

Housing
Il servizio consiste nella fornitura dello spazio fisico all'interno dei datacenter Lepida, comprensivo di facility (alimentazione e raffrescamento) e connettività con la rete geografica Lepida, per ospitare rack e apparati dei clienti, previo rispetto dei requisiti tecnici minimi definiti da Lepida. Le responsabilità in capo a Lepida e ai clienti sono descritte nel relativo Allegato Tecnico e di seguito sinteticamente riportate.
In fase di attivazione del servizio è in carico al cliente il trasporto dei materiali e la consegna nel datacenter Lepida. Lepida provvede alla loro installazione e alle necessarie configurazioni della rete geografica Lepida e di quella di datacenter.

Durante l'erogazione del servizio Lepida assume la responsabilità relativamente agli aspetti di manutenzione e gestione del datacenter, delle facility e delle componenti di rete in essi presenti. E' invece responsabilità del cliente la gestione e manutenzione dei propri rack, componenti di rete e apparati, nonchè dei sistemi e applicativi in essi ospitati.

BAAS/CBAAS

Il servizio consiste nella fornitura di server fisici di tipo blade dedicati (BAAS), eventualmente con installato e licenziato VMware vCloud Advanced (CBAAS). Le responsabilità in capo a Lepida e ai clienti sono descritte nel relativo Allegato Tecnico e di seguito sinteticamente riportate.
In fase di attivazione del servizio Lepida provvede alle attività iniziali di configurazione della rete geografica Lepida, della rete di datacenter, dell'interfaccia di gestione del server e del virtualizzatore, in caso di servizio CBAAS, quindi comunica al cliente le credenziali di accesso.
Durante l'erogazione del servizio la responsabilità relativamente agli aspetti di gestione del sistema e degli applicativi su esso ospitati è in carico al cliente. Lepida mantiene invece la responsabilità sulla gestione e manutenzione dell'hardware dei server, oltre che della rete e delle facility del datacenter in cui sono ospitati.

Storage as a service

Il servizio consiste nella fornitura di spazio disco tramite le infrastrutture multitenant di storage presenti nei datacenter Lepida. Le responsabilità in capo a Lepida e ai clienti sono descritte nel relativo Allegato Tecnico e di seguito sinteticamente riportate.
In fase di attivazione del servizio Lepida provvede alle attività iniziali di configurazione della rete geografica Lepida, della rete di datacenter e dello storage, quindi comunica al cliente le eventuali credenziali di accesso necessarie.
Durante l'erogazione del servizio Lepida mantiene la responsabilità sulla gestione e manutenzione delle infrastrutture di storage, oltre che della rete e delle facility del datacenter in cui sono ospitate. E' in carico al cliente la responsabilità della gestione dei propri sistemi che utilizzano lo storage Lepida.

Server Virtuali

Il servizio consiste nella fornitura di macchine virtuali ospitate sulle infrastrutture multitenant di virtualizzazione e di storage presenti nei datacenter Lepida. Le responsabilità in capo a Lepida e ai clienti sono descritte nel relativo Allegato Tecnico e di seguito sinteticamente riportate.
In fase di attivazione del servizio Lepida provvede alle attività iniziali di configurazione della rete geografica Lepida, della rete di datacenter, della macchina virtuale, dello storage e della web console di gestione della VM, e all'installazione, configurazione e aggiornamento del sistema operativo sulla macchina virtuale, quindi comunica al cliente le credenziali di accesso.
Durante l'erogazione del servizio la responsabilità della gestione del sistema operativo e degli applicativi su esso ospitati è in carico al cliente. Lepida mantiene invece la responsabilità sulla gestione e manutenzione delle infrastrutture di virtualizzazione e storage, oltre che della rete e delle facility del datacenter in cui sono ospitate.

Database as a service

Il servizio consiste nella fornitura di istanze di database Oracle tramite le infrastrutture IT e di storage presenti nei datacenter Lepida. Le responsabilità in capo a Lepida e ai clienti sono descritte nel relativo Allegato Tecnico e di seguito sinteticamente riportate.
In fase di attivazione del servizio Lepida provvede alle attività iniziali di configurazione della rete geografica Lepida, della rete di datacenter e dell'istanza di database, quindi comunica al cliente le credenziali di accesso aventi i privilegi richiesti dallo stesso.

Durante l'erogazione del servizio, se i privilegi di amministrazione dell'istanza di database restano a Lepida, quest'ultima risulta responsabile della gestione ordinaria e manutenzione del database; se viceversa i privilegi di amministrazione sono richiesti dal cliente, tale responsabilità passa in carico al cliente. Lepida rimane comunque responsabile delle infrastrutture IT e dei sistemi che ospitano il database, della rete e delle facility del datacenter. Sono invece sempre di competenza dei clienti eventuali attività di gestione straordinaria dei database (es. monitoraggio o tuning sui database dipendenti dagli applicativi utilizzati dai clienti).

Backup as a service

Il servizio consiste nella fornitura di istanze di backup tramite infrastrutture multitenant di backup e di storage presenti nei datacenter Lepida e del software da installare sui client (agent). Le responsabilità in capo a Lepida e ai clienti sono descritte nel relativo Allegato Tecnico e di seguito sinteticamente riportate.
In fase di attivazione del servizio Lepida provvede alle attività iniziali di configurazione della rete geografica Lepida, della rete di datacenter, dell'istanza di backup e della web console di gestione, quindi comunica al cliente le credenziali di accesso.
Durante l'erogazione del servizio la responsabilità per le attività di configurazione e gestione dei backup e restore, così come per quelle di gestione e manutenzione di tutte le infrastrutture e i sistemi del cliente collegati con le infrastrutture di backup di Lepida, è in carico al cliente. Lepida mantiene invece la responsabilità sulla gestione e manutenzione delle infrastrutture di backup e di storage presenti nel datacenter Lepida, oltre che della rete e delle facility dello stesso.

Data Domain as a service

Il servizio consiste nella fornitura di un repository di backup con funzionalità di deduplica tramite l'uso dell'appliance EMC Data Domain. Le responsabilità in capo a Lepida e ai clienti sono descritte nel relativo Allegato Tecnico e di seguito sinteticamente riportate.
In fase di attivazione del servizio Lepida provvede alle attività iniziali di configurazione della rete geografica Lepida, della rete di datacenter, dell'istanza Data Domain, quindi comunica al cliente le credenziali di accesso.
Durante l'erogazione del servizio Lepida mantiene la responsabilità sulla gestione e manutenzione delle infrastrutture Data Domain, oltre che della rete e delle facility del datacenter in cui sono ospitate.
E' in carico al cliente la responsabilità della gestione dei propri sistemi collegati con le infrastrutture Data Domain di Lepida.

Firewall as a service

Il servizio consiste nella fornitura di istanze su firewall e log server multitenant presenti nei datacenter Lepida. Per tale servizio non è al momento disponibile un Allegato Tecnico.
In fase di attivazione del servizio Lepida provvede alle attività iniziali di configurazione della rete geografica Lepida, della rete di datacenter, dell'istanza di firewall, del log server e dello storage, quindi comunica al cliente le credenziali di accesso.
Durante l'erogazione del servizio la responsabilità relativamente alle attività di configurazione e gestione dell'istanza di firewall e di log server è in carico al cliente. Lepida mantiene invece la responsabilità sulla gestione e manutenzione delle infrastrutture di firewall, log server e storage, oltre che della rete e delle facility del datacenter in cui sono ospitate.

SIEM as a service

Il servizio consiste nella fornitura di una macchina virtuale dedicata, ospitata sulle infrastrutture multitenant di virtualizzazione e di storage presenti nei datacenter Lepida, su cui viene installato un applicativo SIEM. Per tale servizio non è al momento disponibile un Allegato Tecnico.
In fase di attivazione del servizio Lepida provvede alle attività iniziali di configurazione della rete geografica Lepida, della rete di datacenter, della macchina virtuale e dello storage, e all'installazione, configurazione e aggiornamento del sistema operativo e dell'applicativo SIEM, quindi comunica al cliente le credenziali di accesso.
Durante l'erogazione del servizio la responsabilità relativamente alle attività di configurazione e gestione del sistema operativo e dell'applicativo SIEM è in carico al cliente. Lepida mantiene invece la responsabilità sulla gestione e manutenzione delle infrastrutture di virtualizzazione e storage, oltre che della rete e delle facility del datacenter in cui sono ospitate. Il cliente ha la possibilità di acquistare il servizio "gestito", nel qual caso le attività di configurazione e gestione del sistema operativo e dell'applicativo SIEM vengono delegate al fornitore selezionato da Lepida, pur permanendo la responsabilità in carico al cliente.

3. Sicurezza delle risorse umane

Lepida effettua le attività di installazione, configurazione, gestione, monitoraggio, manutenzione e assistenza sulle infrastrutture IT e i servizi di datacenter attraverso personale aziendale professionale e altamente qualificato, di cui assicura la formazione continua e la consapevolezza in tema di continuità e disponibilità del servizio e sicurezza delle informazioni.
Alcune attività possono essere svolte dal personale di fornitori, di cui Lepida garantisce la professionalità e la competenza attraverso le modalità di selezione e controllo descritte al § 17.

4. Sicurezza fisica e ambientale dei siti datacenter

I siti datacenter Lepida sono ubicati in:

- Ravenna, zona industriale Bassette, Via Fernando Santi, 10;
- Parma, Via Largo Torello de Strada 13/A;
- Ferrara, Via Trenti 39.

Ciascuno dei datacenter è dotato delle misure di sicurezza fisica e ambientale descritte di seguito.
Il sito è equipaggiato con sistema antintrusione perimetrale e telecamere esterne. Sul sito è attivo un servizio di vigilanza che provvede ad intervenire in caso di attivazione dell'allarme.
L'accesso al locale principale e alle singole sale presenti al suo interno (sala apparati IT dedicata a Lepida, sala apparati IT dedicata a un partner privato, sala apparati di rete, altri locali tecnici) è consentito solo al personale tecnico di Lepida e al personale di suoi fornitori, clienti o partner opportunamente autorizzato. L'accesso richiede il possesso di un badge e di un PIN. Per i soggetti esterni Lepida valuta caso per caso se assegnare un badge/PIN o se consentirne l'accesso esclusivamente accompagnato da personale Lepida. Gli accessi vengono registrati e monitorati da Lepida o da suoi fornitori H24x365. Le singole sale interne sono telecontrollate attraverso un sistema di videosorveglianza.
Il datacenter è dotato di impianto di rilevamento incendi, collegato a un sistema di allarme, e impianto di spegnimento automatico tramite gas estinguente.
L'impianto elettrico ha le seguenti caratteristiche:

- il sito riceve dal gestore della rete elettrica una fornitura in media tensione e dispone di una cabina di trasformazione con ridondanza 2N;

- l'impianto in bassa tensione prevede doppia linea e doppi quadri elettrici posizionati nelle varie sale dell'edificio (ridondanza 2N);
- è presente un gruppo elettrogeno configurato per entrare in funzione in caso di interruzione di una qualsiasi delle due linee, dimensionato per permettere un'autonomia dell'impianto di almeno 24 ore prima di un eventuale rabbocco di carburante;
- ogni linea è protetta da sistema UPS, con inverter e pacchi batterie in ridondanza 2N, in grado di mantenere alimentati gli apparati in assenza di alimentazione di rete per il tempo necessario all'entrata in funzione del gruppo elettrogeno;
- in ogni cage è presente un quadro elettrico per ciascuna linea e ogni rack all'interno della cage è dotato di una power distribution unit metered per ciascuna linea.

E' presente un impianto di condizionamento d'aria così strutturato:

- l'impianto è di tipo idronico, circuiti di tubazioni e pompe in ridondanza 2N;
- i chiller sono sono esterni all'edificio in grado di lavorare anche in free cooling, in ridondanza N+1;
- è presente un serbatoio di acqua fredda che funge da volano termico e consente la disponibilità di acqua fredda nel circuito in caso di assenza dell'alimentazione di rete per il periodo di tempo necessario all'attivazione del gruppo elettrogeno grazie all'alimentazione fornita dai gruppi di continuità (continuous cooling);
- ogni cage nelle sale apparati è dotata di unità di condizionamento in row in configurazione N+1 o 2N (a seconda del sito), collegate ad entrambi i circuiti idronici, che possono funzionare a corridoio freddo o caldo a seconda della scelta adottata per ciascun datacenter.

Il datacenter è dotato di sistema di rilevamento degli allagamenti e di misure per il deflusso di eventuali accumuli di acqua.
Tutti gli impianti vengono sottoposti a manutenzioni preventive e test di resilienza periodici.

5. Gestione degli asset e delle configurazioni

Attraverso l'uso di sistemi di gestione centralizzati Lepida mantiene un database costantemente aggiornato degli asset fisici presenti in datacenter, delle risorse logiche assegnate ai clienti e delle relative configurazioni. Gli asset fisici e le risorse logiche vengono identificati utilizzando una codifica di associazione con il servizio e il cliente da cui vengono utilizzati.

6. Rimozione degli asset e dei dati dei clienti al termine del contratto

A conclusione del contratto Lepida provvede alla rimozione degli asset fisici e delle risorse logiche assegnate ai clienti e di tutti i dati dei clienti conservati su di esse, adottando le seguenti procedure specifiche per ciascun servizio:

- Housing: Lepida provvede alla disinstallazione del materiale del cliente e alla rimozione di tutte le configurazioni precedentemente eseguite per l'utilizzo del servizio da parte del cliente, mentre sono in carico al cliente la rimozione e il trasporto del materiale al di fuori del datacenter;
- BAAS/CBAAS: Lepida provvede al ripristino alla configurazione di fabbrica del server e alla cancellazione sicura dei dati in essi contenuti, e inoltre alla rimozione di tutte le configurazioni precedentemente eseguite e delle credenziali di accesso create per l'utilizzo del servizio da parte del cliente;

- Storage as a service: Lepida provvede alla deassegnazione delle risorse di storage precedentemente assegnate al cliente, attraverso una procedura che riassegna le risorse al pool generale, rendendo di fatto i dati del cliente inaccessibili, e alla rimozione di tutte le configurazioni precedentemente eseguite per l'utilizzo del servizio da parte del cliente;
- Server Virtuali: Lepida provvede alla cancellazione della macchina virtuale, alla deassegnazione delle risorse di storage precedentemente assegnate al cliente e alla rimozione di tutte le configurazioni precedentemente eseguite e delle credenziali di accesso create per l'utilizzo del servizio da parte del cliente;
- Database as a service: Lepida provvede alla cancellazione dell'istanza di database o della macchina virtuale che la ospita, alla deassegnazione delle risorse di storage precedentemente assegnate al cliente e alla rimozione di tutte le configurazioni precedentemente eseguite e delle credenziali di accesso create per l'utilizzo del servizio da parte del cliente;
- Backup as a service: Lepida provvede alla cancellazione dell'istanza di backup, alla deassegnazione delle risorse di storage precedentemente assegnate al cliente e alla rimozione di tutte le configurazioni precedentemente eseguite e delle credenziali di accesso create per l'utilizzo del servizio da parte del cliente;
- Data Domain as a service: Lepida provvede alla cancellazione dell'istanza di Data Domain, alla deassegnazione delle risorse di storage precedentemente assegnate al cliente e alla rimozione di tutte le configurazioni precedentemente eseguite e delle credenziali di accesso create per l'utilizzo del servizio da parte del cliente;
- Firewall as a service: Lepida provvede alla cancellazione delle istanze di firewall e log server, alla deassegnazione delle risorse di storage precedentemente assegnate al cliente e alla rimozione di tutte le configurazioni precedentemente eseguite e delle credenziali di accesso create per l'utilizzo del servizio da parte del cliente;
- SIEM as a service: Lepida provvede alla cancellazione della macchina virtuale, alla deassegnazione delle risorse di storage precedentemente assegnate al cliente e alla rimozione di tutte le configurazioni precedentemente eseguite e delle credenziali di accesso create per l'utilizzo del servizio da parte del cliente.

7. Dismissione dei supporti di memorizzazione

Nel caso in cui abbia necessità di dismettere un supporto di memorizzazione contenuto in una delle proprie infrastruttura IT di datacenter, Lepida adotta una fra le seguenti procedure, al fine di assicurare che i dati dei clienti non possano essere accessibili a terzi:

- cancellazione sicura dei dati in esso contenuti o sua distruzione fisica, in proprio o mediante servizio esterno;
- stoccaggio presso un proprio magazzino ad accesso controllato e registrazione del supporto, al fine di poter effettuare successivamente le operazioni di cancellazione dei dati o distruzione.

8. Gestione degli accessi alle infrastrutture IT da parte di Lepida

L'accesso alle infrastrutture IT di datacenter e alle relative console di gestione è consentito solo al personale tecnico di Lepida e al personale di suoi fornitori opportunamente autorizzato. Ogniqualvolta tecnicamente possibile i sistemi sono configurati per:

- utilizzare un sistema centralizzato di autenticazione e autorizzazione;
- richiedere credenziali di accesso amministrativo nominative;
- applicare una opportuna policy di complessità, scadenza e riutilizzo delle password;
- registrare e conservare i log degli accessi amministrativi, garantendone la protezione da manomissioni e accessi non autorizzati.

Le infrastrutture IT di datacenter e le console di gestione sono accessibili esclusivamente su indirizzamento di rete privato dalla rete aziendale o attraverso collegamento in VPN su protocolli sicuri.
Lepida si assicura di disabilitare le credenziali e/o i privilegi assegnati agli utenti nel momento in cui cessa la condizione che ne ha richiesta la creazione o abilitazione (es. interruzione del rapporto di lavoro da parte di un dipendente, conclusione di un contratto con un fornitore). Inoltre esegue riesami periodici di verifica sulle utenze attive.

9. Gestione degli accessi ai servizi e alle interfacce di gestione da parte dei clienti

I clienti possono accedere ai servizi di datacenter e alle relative interfacce di gestione nelle modalità descritte di seguito:

- BAAS/CBAAS: i clienti possono accedere ai propri server blade attraverso la loro interfaccia di gestione. Il primo accesso deve essere effettuato con credenziali amministrative fornite da Lepida, successivamente il cliente è autonomo nella gestione dei propri utenti. L'interfaccia di gestione, su indirizzamento di rete privato, viene reso raggiungibile tramite l'uso di una VPN client to site messa a disposizione da Lepida;
- Server Virtuali: i clienti possono accedere alle proprie macchine virtuali in una duplice modalità:
  - tramite RDP per i sistemi Windows o SSH per quelli Unix/Linux su indirizzamento di rete privato, a condizione che siano stati resi raggiungibili dalla rete del cliente tramite VPN configurata sulla rete Lepida. Il primo accesso deve essere effettuato con credenziali amministrative fornite da Lepida, successivamente il cliente è autonomo nella gestione dei propri utenti di sistema;
  - tramite piattaforma web di gestione delle macchine virtuali su indirizzamento di rete pubblico, configurata da Lepida in modo tale da fornire visibilità limitata alle sole macchine del cliente.
- Database as a service: Lepida fornisce ai clienti credenziali di accesso alle proprie istanze di database aventi i privilegi richiesti dagli stessi. Di norma si tratta di utenze con privilegi limitati, ma qualora il cliente lo richieda possono essere concessi i privilegi amministrativi di SYSDBA. Il cliente, in base ai privilegi ricevuti, può essere in grado di creare ulteriori utenti con visibilità limitata a risorse all'interno dell'istanza. Il database, su indirizzamento di rete privato, viene reso raggiungibile dalla rete del cliente tramite VPN configurata sulla rete Lepida oppure tramite l'uso di una VPN client to site messa a disposizione da Lepida;
- Backup as a service: i clienti possono accedere alla web console di gestione dell'infrastruttura di backup, configurata da Lepida in modo tale da fornire visibilità limitata alle risorse assegnate al singolo tenant. Il primo accesso deve essere effettuato con credenziali amministrative fornite da Lepida, successivamente il cliente è autonomo nella gestione dei propri utenti. La console, su indirizzamento di rete privato, viene resa raggiungibile dalla rete del cliente tramite VPN configurata sulla rete Lepida oppure tramite l'uso di una VPN client to site messa a disposizione da Lepida;

- Firewall as a service: i clienti possono accedere alle web console di gestione della propria istanza di firewall e di log server, configurate da Lepida in modo tale da fornire visibilità limitata alle risorse assegnate al singolo tenant. Il primo accesso deve essere effettuato con credenziali amministrative fornite da Lepida, successivamente il cliente è autonomo nella gestione dei propri utenti. Le console, su indirizzamento di rete privato, vengono rese raggiungibili dalla rete del cliente tramite VPN configurata sulla rete Lepida;
- SIEM as a service: i clienti possono accedere al sistema operativo della macchina virtuale dedicata creata da Lepida e alla web console di gestione dell'applicativo SIEM. Il primo accesso deve essere effettuato con credenziali amministrative fornite da Lepida, successivamente il cliente è autonomo nella gestione dei propri utenti di sistema e di console. Il sistema, su indirizzamento di rete privato, viene reso raggiungibile dalla rete del cliente tramite VPN configurata sulla rete Lepida oppure tramite l'uso di una VPN client to site messa a disposizione da Lepida.

Tutte le richieste relative alla creazione di utenze o all'assegnazione ad esse di privilegi per l'utilizzo dei servizi e delle relative interfacce di gestione devono essere fatte pervenire alla struttura competente di Lepida da parte del soggetto che il cliente ha indicato come referente per il servizio. Solo a quest'ultimo Lepida provvederà a comunicare le credenziali di autenticazione create.
Lepida si assicura di disabilitare le credenziali e/o i privilegi assegnati ai clienti sui propri sistemi di autenticazione, a seguito di esplicita richiesta proveniente dal referente del cliente, o in caso di cessazione del contratto per l'erogazione del servizio da parte del cliente. Inoltre esegue riesami periodici di verifica sulle utenze attive.

10. Protezione dagli attacchi di rete e separazione delle reti dei clienti

Lepida è responsabile di proteggere da attacchi di rete le proprie infrastrutture IT condivise dai clienti e di garantire la separazione delle reti tramite cui i clienti accedono ai servizi.
Tutti i servizi di datacenter e le relative interfacce di gestione sono erogati su indirizzamenti di rete privati e la raggiungibilità dei servizi dalle sedi dei clienti prevede l'uso di VPN Layer 2 o 3 realizzate sulla rete geografica Lepida o di una VPN client to site messa a disposizione da Lepida. All'interno dei datacenter le reti dei singoli clienti e servizi sono segregate tramite l'uso di VLAN e di next generation firewall presenti in ciascuno di essi. Inoltre vengono applicate, e periodicamente controllate, tecniche di hardening (es. disabilitazione di servizi non utilizzati, chiusura di porte non necessarie, limitazioni alle connessioni di rete).
Attraverso il servizio Firewall as a service Lepida mette i propri next generation firewall multitenant di datacenter anche a disposizione dei clienti, fornendo loro uno strumento per implementare policy di sicurezza su tutti i servizi di datacenter da essi utilizzati e sui propri sistemi ospitati nei datacenter, fermo restando che la responsabilità della relativa gestione è in capo ai clienti.

11. Separazione degli ambienti e dei dati dei clienti

Lepida è responsabile di garantire la separazione degli ambienti e dei dati dei singoli clienti sulle proprie infrastrutture IT condivise dai clienti.
A tale scopo sulle infrastrutture IT Lepida adotta le funzionalità di multitenancy rese disponibili dai prodotti utilizzati e configurazioni adeguate a garantire la completa separazione delle risorse assegnate (cioè VM, LUN, file system, library di backup, istanze di database, istanze di firewall) e dei

dati dei singoli clienti. Inoltre gli accessi dei clienti alle interfacce di gestione vengono configurati in modo tale che ciascun cliente abbia visibilità limitata esclusivamente alle proprie risorse.

12. Backup

Fra i servizi di datacenter offerti da Lepida quelli che prevedono l'esecuzione di backup da parte di Lepida sono i seguenti:

- Database as a service: vengono effettuati backup logici, cioè export di schemi di database, e fisici, cioè backup RMAN dell'intero database, secondo la policy richiesta dal cliente o con la seguente policy standard: export giornaliero notturno con retention di 7 giorni e tre backup RMAN full

Per tali servizi le copie di backup sono conservate su sistemi storage posizionati in un sito datacenter differente da quello di erogazione del servizio. In entrambi i casi è condizione necessaria che il cliente abbia acquistato lo storage necessario. Lepida provvede al restore dei dati su richiesta del cliente.

Inoltre il servizio Backup as a service prevede che i clienti possano opzionalmente conservare una seconda copia di backup in un differente datacenter Lepida o presso la sede del cliente.

13. Cifratura dei dati

La cifratura dei dati in transito è assicurata dall'uso di protocolli che la implementano (es. TLS, SSH, RDP, IPSec).
Tutti gli storage di tipo SAN utilizzati da Lepida dispongono della funzionalità di cifratura dei dati a riposo abilitata di default.

14. Gestione degli aggiornamenti software

Lepida mantiene costantemente monitorato il rilascio di aggiornamenti software e firmware relativi a major release, minor release e patch da parte dei produttori dell'hardware e dei software utilizzati nei propri datacenter.
Ogni rilascio viene analizzato da Lepida al fine di valutare da un lato la criticità dei bug risolti, dall'altro l'impatto sull'erogazione del servizio conseguente alla sua installazione, tenendo conto in particolare dell'architettura e delle caratteristiche con cui viene erogato il servizio e delle compatibilità tra software di differenti produttori che concorrono all'erogazione di un medesimo servizio. I servizi di datacenter offerti da Lepida sono stati progettati e vengono gestiti con la finalità di minimizzare la necessità di interruzioni del servizio in caso di attività di manutenzione, pertanto la quasi totalità degli aggiornamenti può essere effettuata senza impatti sul servizio. Le attività di aggiornamento vengono eseguite in modo controllato e, quando necessario, mantenendone informati i clienti, come descritto nella procedura di gestione dei cambiamenti (§ 17).
Tipicamente le patch critiche di sicurezza e quelle aventi significativo impatto sulle funzionalità sono tempestivamente installate, mentre le minor release sono installate con cadenza periodica. L'installazione delle major release, invece, non è garantita, ma viene decisa autonomamente da Lepida tenuto conto delle politiche di mantenimento, d'uso e di prezzo per le licenze adottate dai produttori.

15. Verifiche di sicurezza e gestione delle vulnerabilità tecniche

Lepida effettua con cadenza periodica verifiche di sicurezza (vulnerability assessment e/o penetration test) sulle reti, i sistemi e le applicazioni utilizzate per l'erogazione dei servizi di datacenter, allo scopo di rilevare l'eventuale presenza di vulnerabilità tecniche che potrebbero essere sfruttate per la compromissione delle infrastrutture IT e dei dati in essi presenti. Si mantiene inoltre costantemente aggiornata sui bollettini e le segnalazioni di sicurezza rilasciati dal CERT-PA, presso il quale è accreditata, o da ulteriori soggetti.
Le vulnerabilità rilevate vengono analizzate e, in caso di vulnerabilità critiche, sono messe in atto tempestivamente le contromisure necessarie per la loro risoluzione o mitigazione (es. installazione di patch, disabilitazione di servizi, modifiche di configurazioni). Le attività di remediation vengono eseguite in modo controllato e, quando necessario, mantenendone informati i clienti, come descritto nella procedura di gestione dei cambiamenti (§ 17).

16. Gestione della capacità delle infrastrutture IT e dei servizi

I datacenter Lepida sono stati equipaggiati con infrastrutture IT altamente scalabili a livello di risorse hardware e di licenze software. Lepida effettua periodicamente pianificazioni delle risorse necessarie per l'erogazione dei propri servizi, tenendo conto dei servizi venduti e della stima della domanda attesa. Inoltre mantiene costantemente monitorate le prestazioni e l'utilizzo delle proprie infrastrutture IT e servizi, al fine di rilevare eventuali criticità. Nel caso in cui riscontri carenze di risorse, Lepida interviene, laddove possibile, apportando modifiche alle configurazioni, o, in caso contrario, provvedendo ad approvvigionarsi delle ulteriori risorse necessarie. Le attività di modifica ai servizi in produzione vengono effettuate in modo controllato e, quando necessario, mantenendone informati i clienti, come descritto nella procedura di gestione dei cambiamenti (§ 17).

17. Gestione dei cambiamenti alle infrastrutture IT e ai servizi di datacenter

Lepida si è dotata di una procedura per gestire in modo controllato i cambiamenti alle infrastrutture IT e ai servizi di datacenter (es. modifiche hardware, aggiornamenti software, modifiche architetturali, modifiche di configurazioni, manutenzioni preventive, test di resilienza, ecc…), allo scopo di minimizzare gli impatti sull'erogazione dei servizi ai clienti. La suddetta procedura viene di seguito descritta:

- le richieste di cambiamento originate dalle strutture interne di Lepida o provenienti dai clienti, vengono ricevute dalla struttura competente di Lepida, tracciate su sistema informativo aziendale, analizzate per verificare che siano accettabili da un punto di vista tecnico e contrattuale e sottoposte ad approvazione;
- le richieste approvate che possono essere soddisfatte senza impatto sul servizio vengono trattate come segue:
    - Lepida pianifica ed esegue in autonomia l'intervento;
    - successivamente, se la richiesta proviene da un cliente, quest'ultimo ne viene informato tramite e-mail;

- le richieste approvate la cui implementazione prevede un impatto sul servizio vengono trattate come segue:
    - Lepida definisce un piano di implementazione, comprensivo di schedulazione temporale, studiato con l'obiettivo di minimizzare l'impatto sul servizio. Quando la richiesta proviene dal cliente o quando la tipologia di intervento lo richiede, la schedulazione viene concordata con i clienti interessati, o almeno con quelli ritenuti più critici;
    - Lepida predispone inoltre: eventuali documenti tecnici necessari per l'implementazione, un piano di test da svolgere a conclusione dell'intervento e, quando tecnicamente possibile, un piano di roll-back per poter tornare alla situazione antecedente al cambiamento in caso di necessità;
    - l'attività di implementazione viene anticipata ai clienti interessati con un preavviso minimo di 3 giorni lavorativi rispetto alla data di pianificazione o comunque non inferiore a quanto previsto nell'Allegato Tecnico del servizio, a meno di interventi urgenti inerenti la sicurezza che possono essere effettuati senza preavviso se ritenuti particolarmente critici, attraverso una e-mail contenente almeno: descrizione dell'intervento, data e ora di inizio, durata prevista, disservizio previsto;
    - l'inizio dell'intervento viene comunicato ai clienti interessati attraverso una e-mail avente i medesimi contenuti di quella di preavviso;
    - una volta eseguito l'intervento, vengono effettuati i test previsti, che possono richiedere il coinvolgimento dei clienti interessati, o almeno di quelli ritenuti più critici. Quindi si procede come segue:
        - in caso di esito positivo, la richiesta viene chiusa e viene trasmessa a tutti i clienti interessati una e-mail, in cui si comunica l'esito positivo dell'intervento e si ricordano le modalità con cui può essere contattata l'assistenza Lepida in caso di problemi;
        - in caso di esito negativo, vengono apportate le correzioni necessarie e ripetuti i test;
        - in caso di roll-back, la richiesta resta aperta e viene trasmessa a tutti i clienti interessati una e-mail, in cui si comunica l'esito negativo dell'intervento e la necessità di una sua riprogrammazione;
    - ogni qualvolta un cambiamento lo richiede, la documentazione tecnica eventualmente fornita ai clienti (es. manuali utente) o quella necessaria a Lepida per la gestione e manutenzione del servizio (es. schemi architetturali, linee guida di configurazione, informazioni tecniche) viene coerentemente aggiornata.

18. Gestione dei fornitori

Per attività di configurazione, gestione, monitoraggio, manutenzione e assistenza Lepida può avvalersi di fornitori esterni. I fornitori sono selezionati attraverso procedure in linea con quanto previsto dal Codice degli Appalti. In tali procedure Lepida prevede sempre specifici requisiti tecnici, modalità operative e livelli di servizio e introduce ulteriori modalità di controllo in base alla tipologia di servizio richiesto, come ad esempio: reportistica, incontri periodici, obbligo per il fornitore di utilizzare sistemi (es. sistemi di trouble ticketing) messi a disposizione da Lepida, possibilità per Lepida di effettuare audit sulle attività dei fornitori.

19. Monitoraggio delle facility, delle infrastrutture IT e dei servizi di datacenter

Lepida assicura la sincronizzazione del clock di tutti i sistemi con una fonte di riferimento affidabile e la registrazione dei log relativi a funzionamento, prestazioni, utilizzo e sicurezza delle facility, delle infrastrutture IT e dei servizi di datacenter con i relativi timestamp.
Inoltre Lepida effettua il monitoraggio H24x365 delle infrastrutture e dei servizi tramite proprio personale o tramite fornitori incaricati. A fronte della rilevazione di malfunzionamenti o di incidenti di sicurezza delle informazioni viene attivata la procedura descritta al § 21.

20. Assistenza tecnica ai clienti

I clienti hanno la possibilità di segnalare l'interruzione o il degrado delle funzionalità o delle prestazioni di un servizio o di richiedere modifiche ai servizi già contrattualizzati utilizzando le modalità e i canali di comunicazione messi a disposizione da Lepida descritti negli Allegati tecnici dei servizi e nella sezione del sito Internet aziendale relativa all'assistenza (https://lepida.net/assistenza). Le segnalazioni di malfunzionamento vengono gestite secondo la procedura descritta al § 21; mentre le richieste di cambiamento seguono la procedura riportata al § 17.

21. Gestione dei malfunzionamenti e degli incidenti di sicurezza delle informazioni

Lepida si è dotata di una procedura per la gestione H24x365 dei malfunzionamenti delle infrastrutture IT e dei servizi di datacenter e degli incidenti che possono compromettere la disponibilità del servizio o l'integrità o la riservatezza dei dati trattati, al fine di minimizzarne l'impatto in caso di occorrenza. La suddetta procedura viene di seguito descritta:

- a seguito della rilevazione di un malfunzionamento/incidente tramite i sistemi di monitoraggio in uso o della ricezione di una segnalazione da parte di un cliente, la struttura competente di Lepida provvede a tracciare l'evento su sistema informativo aziendale, ad analizzarlo e a classificarlo in termini di gravità. La classificazione viene effettuata tenendo conto della criticità del servizio e dei dati coinvolti, del numero di risorse tecnologiche impattate, del numero e tipologia di clienti impattati e del tipo di danno arrecato, e prevede l'uso dei tre livelli "bassa", "media" e "alta";
- in caso di malfunzionamenti/incidenti classificati di gravità "alta", in questa fase viene effettuata una comunicazione ai clienti coinvolti, o, in caso di impatto su un elevato numero di clienti, almeno quelli ritenuti più critici, tramite e-mail o telefono (laddove l'incidente abbia causato l'indisponibilità del servizio di posta elettronica del cliente), allo scopo di informare i clienti che il malfunzionamento/incidente è stato rilevato ed è in fase di analisi e, quando possibile, comunicare il tempo di ripristino stimato;
- successivamente la struttura competente di Lepida provvede allo svolgimento delle attività richieste per la gestione e risoluzione del malfunzionamento/incidente, che possono comprendere: contenimento, rimozione della causa, ripristino del servizio, acquisizione forense di evidenze digitali di reato. In alcuni casi può essere richiesto il coinvolgimento del cliente. Lepida si impegna ad assicurare i tempi di ripristino previsti dai livelli di servizio riportati negli Allegati Tecnici dei servizi;
- una volta concluse le attività, vengono svolte opportune verifiche, quando possibile con il coinvolgimento dei clienti interessati, al fine di accertare l'effettivo ripristino del servizio, e viene trasmessa ai clienti interessati una e-mail contenente: data e ora di inizio del

malfunzionamento/incidente, data e ora di conclusione, causa, risorse tecnologiche impattate, clienti coinvolti, disservizi causati, azioni intraprese per il ripristino del servizio;

- per i malfunzionamenti/incidenti di gravità “alta”, o nei casi in cui si ritiene opportuno, viene prodotto un rapporto di incidente secondo un formato prestabilito e viene effettuata un’analisi a posteriori finalizzata a rilevare eventuali criticità riscontrate ed identificare eventuali azioni migliorative (“lesson learned”);
- in caso di malfunzionamenti/incidenti particolarmente critici, Lepida attiva il proprio Comitato 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 piano di disaster recovery per i servizi coinvolti. In questi casi i clienti coinvolti vengono informati delle decisioni assunte dal Comitato di Crisi in modo da consentire loro di attivare i propri piani di continuità operativa;
- nel caso in cui l’incidente si configuri come violazione di dati personali, Lepida procede in ottemperanza agli Art. 33 e 34 del Regolamento UE 2016/679 (GDPR) e in particolare:
    - se Lepida è Titolare, 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 Lepida è Responsabile, provvede a informarne il Titolare entro 72 ore dal momento in cui ne è venuta a conoscenza o comunque non oltre i termini definiti nell’accordo di designazione.

Le responsabilità di Lepida in relazione alla rilevazione e risoluzione dei malfunzionamenti e degli incidenti di sicurezza sono limitate a quanto previsto nell’Allegato Tecnico del singolo servizio.
Qualora Lepida si accorgesse o fosse informata da soggetti terzi della presenza di comportamenti anomali di IP di competenza del cliente, Lepida informerà tempestivamente il cliente target, riservandosi azioni di sospensione della connettività per gli IP coinvolti, se fossero a rischio componenti infrastrutturali o per ridurre effetti avversi.

22. Ridondanze e alta affidabilità delle reti, delle infrastrutture IT e dei servizi

I servizi di datacenter offerti da Lepida sono stati progettati con la finalità di minimizzare il degrado o l’interruzione del servizio in caso di guasti o malfunzionamenti e di assicurare il rispetto dei livelli di servizio dichiarati nei relativi Allegati Tecnici. Di seguito vengono descritte le principali misure adottate in termini di ridondanza e alta affidabilità sulle reti e le infrastrutture IT utilizzate per l’erogazione dei servizi:

- Rete: è costituita da un livello di aggregazione e distribuzione, da un livello di routing e da un livello di edge MPLS verso la rete geografica Lepida; a tutti i livelli la rete è ridondata in termini di di apparati e collegamenti; gli apparati di rete sono dotati di alimentatori ridondati, sono attestati su due distinte linee di alimentazione e sono cablati e configurati per assicurare ridondanza di percorso; l’apparato di edge è uno chassis attestato su due distinte linee di alimentazione, ridondato in tutti i suoi componenti (routing engine, ventole, alimentatori), collegato in doppia via fisica (in fibra ottica) con due differenti nodi di backbone della rete Lepida;
- Server: sono dotati di alimentatori e ventole ridondati, componente di management ridondata, dischi interni in RAID1 hardware, sono attestati su due distinte linee di alimentazione e hanno connettività ridondata verso apparati di rete differenti sia nelle reti LAN che SAN;

- Infrastrutture di storage: possono essere costituite da controller e cassetti disco o da moduli scale-out, in entrambi i casi sono dotate di alimentatori ridondati, sono attestate su due distinte linee di alimentazione, dispongono di dischi in RAID e hanno connettività di front end (Fiber Channel e/o IP) ridondata;
- Infrastrutture di virtualizzazione: sono costituite da più server in cluster, implementano una funzionalità di alta disponibilità che, in caso di blocchi di un host fisico, esegue il riavvio automatico delle macchine virtuali su un altro host del cluster, e in caso di blocchi sul sistema operativo di una macchina virtuale, riavvia la VM sullo stesso host, e sono dotate di reti di management e di servizio ridondate;
- Database Oracle: il servizio prevede due differenti modalità di erogazione:
    - istanza non ridondata: istanza Oracle su una singola macchina virtuale o su un cluster Oracle RAC (di server fisici o virtuali) in configurazione active-standby, cioè in caso di blocco del nodo su cui risiede, l'istanza viene spenta e riaccesa automaticamente su un altro nodo del cluster;
    - istanza ridondata: istanza su un cluster Oracle RAC (di server fisici o virtuali) in configurazione active-active, cioè l'istanza è attiva contemporaneamente su almeno due nodi del cluster garantendo il failover e il bilanciamento di carico.
- Infrastrutture di backup: sono costituite da backup server (fisici o virtuali) e da storage di archiviazione per i backup. Le componenti fisiche sono dotate di alimentatori ridondati, sono attestate su due distinte linee di alimentazione, dispongono di dischi in RAID e hanno connettività ridondata;
- Infrastrutture Data Domain: sono costituite da una appliance dotata di una coppia di controller per assicurare l'alta affidabilità, l'appliance è dotata di alimentatori ridondati, è attestata su due distinte linee di alimentazione, dispone di dischi in RAID e ha connettività ridondata;
- Firewall: è costituito da uno chassis attestato su due distinte linee di alimentazione, ridondato in tutti i suoi componenti (service processing card, ventole, alimentatori), collegato tramite più linee aggregate al nodo di edge di datacenter.

Le ridondanze e i meccanismi di alta affidabilità vengono sottoposti a test periodici da parte di Lepida.

23. Continuità operativa e disaster recovery

Lepida si è dotata di un piano di continuità operativa che descrive gli aspetti organizzativi e tecnologici definiti al fine di assicurare il funzionamento ininterrotto o il ripristino nel più breve tempo possibile dei propri processi e servizi critici, in caso di disastri o di incidenti potenzialmente in grado di causarne una prolungata indisponibilità (es. disastri naturali, interventi umani dolosi e colposi, malfunzionamenti, ecc...).
A livello organizzativo Lepida ha definito le procedure, i ruoli e le responsabilità per la gestione delle emergenze, comprese le comunicazioni verso l'esterno, prevedendo l'attivazione di un Comitato di Crisi che in tali circostanze assume il compito di coordinare e supervisionare le attività necessarie per il ripristino dei servizi. Da un punto di vista tecnico la continuità dei servizi di datacenter viene assicurata adottando le misure di sicurezza fisica e ambientale e i meccanismi di ridondanza e alta affidabilità descritti nei §§ 4 e 22.
Tutti i servizi di datacenter prevedono che la continuità e la disponibilità del servizio dichiarata nei relativi Allegati Tecnici sia garantita solo limitatamente alle infrastrutture IT in un singolo sito datacenter da cui ciascuno di essi viene erogato; non è pertanto richiesto che Lepida disponga per tali servizi di un piano di disaster recovery tra differenti infrastrutture IT all'interno di uno stesso datacenter nè tra il datacenter di produzione e un datacenter secondario.

I tre datacenter di Lepida sono stati tuttavia equipaggiati con infrastrutture IT e tecnologie abilitanti per l'implementazione di tecniche di disaster recovery basate su repliche sincrone o asincrone e meccanismi di automazione sia tra cage differenti all'interno del sito di produzione sia tra il sito di produzione e un sito secondario. Lepida utilizza tali infrastrutture IT e tecnologie per le proprie piattaforme applicative e le mette a disposizione dei clienti che lo richiedano sulla base di progetti condivisi, fermo restando che in tali casi la responsabilità nella definizione e implementazione dei piani di disaster recovery è in carico ai clienti.