COMUNE DI
REGGIO EMILIA

MANUALE DI GESTIONE DEL PROTOCOLLO INFORMATICO, DEI FLUSSI DOCUMENTALI E DEGLI ARCHIVI

ALLEGATO M

Piano di continuità operativa dei sistemi ICT e misure tecniche di protezione dei dati

Comune di Reggio Emilia

COMUNE DI
REGGIO EMILIA

Indice generale

COMUNE DI
REGGIO EMILIA

Introduzione

Il tema della continuità operativa per le pubbliche amministrazioni è sancito dal comma 2 dell'art. 51 del D.Lgs 82/2005 "Codice dell'Amministrazione Digitale" che così recita: "*I documenti informatici delle pubbliche amministrazioni devono essere custoditi e controllati con modalità tali da ridurre al minimo i rischi di distruzione, perdita, accesso non autorizzato o non consentito o non conforme alle finalità della raccolta*".

Dal punto di vista ICT la maggior parte dei servizi utilizzati dagli uffici del Comune di Reggio Emilia (di seguito "Ente") per le finalità istituzionali o erogati ai cittadini è gestita dai sistemi informatici e dal "Servizio Gestione e sviluppo delle Tecnologie e dei Sistemi Informativi" all'interno del Datacenter dell'Ente (d'ora in poi DC primario).

L'Ente ha attivato alcuni servizi applicativi erogati in modalità SaaS su server di fornitori. In questo caso, in fase di affidamento del servizio, l'Ente richiede all'affidatario di specificare *politiche di backup e di disaster recovery* che si intendono adottare per garantire l'integrità dai dati in caso di ripristino. Questi elementi rientrano nella valutazione tecnica in caso di affidamento tramite procedura di gara.

Il presente documento fa riferimento all'infrastruttura informatica e di telecomunicazioni (ICT) dell'Ente e non alle misure che possono essere attivate da fornitori di servizi SaaS di cui sopra. In particolare descrive:

- gli accorgimenti tecnici messi in campo e le misure adottate per prevenire/mitigare il rischio di indisponibilità dei servizi nel sito principale (Data Center dell'Ente);
- le misure di sicurezza presenti nel sito secondario (DataCenter di Lepida);
- i procedimenti organizzativi e tecnici per gestire l'indisponibilità di uno o più servizi e ripristinare l'operatività anche in casi di eventi particolarmente gravi che rendano inutilizzabile il sito principale.

Il presente documento costituisce inoltre un approfondimento tecnico/organizzativo rispetto a quanto indicato nell'ALLEGATO L_PIANO DI SICUREZZA DEI DOCUMENTI INFORMATICI al " "Manuale di gestione del protocollo, dei flussi documentali e degli archivi" vigente nell'Ente.

L'indisponibilità dei servizi erogati da un sistema informatico può essere conseguenza di molteplici fattori tra cui ad esempio:

- errori/malfunzionamenti dei processi (il processo organizzativo che usa il servizio ICT non ha funzionato come avrebbe dovuto per errori materiali, errori nell'applicazione di norme ovvero per il verificarsi di circostanze non adeguatamente previste dalle stesse);
- malfunzionamento dei sistemi, delle applicazioni e delle infrastrutture;
- attacchi o eventi naturali di tipo accidentale;
- azioni dolose;
- disastri.

E' quindi fondamentale adottare misure per prevenire l'indisponibilità di tutto o parte dei sistemi informativi e definire quali sono le operazioni preventive o da adottare in caso di emergenza.

1. Misure relative al Data Center Primario

Nei paragrafi seguenti sono evidenziati gli accorgimenti sia dal punto di vista logistico che da quello tecnico, che organizzativo per ridurre il rischio di indisponibilità dei sistemi all'interno del DC primario.

1.1 Dati Logistici specifici

Il DC primario rientra nella categoria "Data center small" secondo la classificazione delle Linee Guida AGID par. 3.1.1 ed è utilizzato esclusivamente per l'erogazione dei servizi ICT dell'Ente e di eventuali soggetti istituzionali esterni che vi accedono.

E' posizionato al 1° piano di un edificio di proprietà dell'Ente in centro storico e quindi in una zona con alta disponibilità di infrastrutture per le telecomunicazioni, rete elettrica ecc.

All'interno dell'area dedicata al "Servizio Gestione e Sviluppo delle Tecnologie e dei Sistemi Informativi" (d'ora in poi SGT) che ne ha in carico la gestione, è stato allestito uno spazio di circa 60 mq dedicato alle funzioni di DC primario per il sistema informativo dell'Ente.

Tale spazio è:

- facilmente raggiungibile dai sistemisti del servizio SGT in caso di necessità di interventi diretti;
- privo di finestre, terrazzi o altri accessi che possano essere violati;
- in prossimità di spazi in cui sono presenti sale riunioni, uffici e altri spazi attrezzati con prese di rete, telefoni ecc. in cui possono essere gestite installazioni provvisorie o situazioni di emergenza;
- allestito con pavimenti galleggianti strutturati per reggere pressioni statiche di 400 kg/mq con una intercapedine di circa 1,5 mt.;
- attrezzato con 9 rack di cui 4 dedicati a server/storage e 5 a patch panel di terminazione dei cablaggi strutturati ed apparati di rete (switch di core, firewall, ecc.);
- dotato di sistema di illuminazione dedicata con tecnologie di illuminazione efficienti e impianto spento per il 99% del tempo, in modo da ridurre il carico termico.

1.2 Infrastrutture di continuità e protezione fisica

- Tutti i sistemi critici sono dotati di doppia alimentazione: una linea è collegata all'alimentazione Enel, l'altra al gruppo di continuità.
- Il gruppo di continuità (Meta System 40KVA) si trova in un locale tecnico dedicato rialzato di circa 40cm rispetto al piano strada ed è posizionato su supporti a circa 30 cm da terra. E' in grado di garantire un'autonomia di circa 40 minuti con tutti i sistemi attivi, che può essere aumentata spegnendo quelli meno critici o ridondati.
- Il DC primario è protetto da un sistema di raffreddamento costituito da 3 gruppi frigo indipendenti da 5Kw ognuno, collegati tra loro tramite CANBUS. Nel periodo estivo tutti e tre i gruppi sono in funzione, mentre nel periodo invernale funzionano 2 gruppi H24 ed il terzo si attiva automaticamente in caso di indisponibilità di uno dei 2. E' in funzione un sistema di telecontrollo GSM per la gestione delle temperatura di mandata dei singoli condizionatori.

- Il locale è protetto da un impianto di rilevazione fumi / incendio costituito da 4 centraline interfacciate da un quadro sinottico e 100 rilevatori posti sotto al pavimento galleggiante, sopra e sotto al contro-soffitto. Inoltre ai vari piani del SGT sono posizionate sirene bitonali con avvisatori ottici bicolore, pulsanti di pre-allarme, allarme evacuazione e allarme incendi. L'impianto è costantemente collegato tramite combinatore telefonico alla Centrale Operativa della Polizia Locale, attiva 24X7.
- Il sistema di spegnimento incendi è affidato a 12 Bombole di Azoto – IG 100 da 140Lt a 200Bar interfacciato con l'impianto di rilevazione fumi incendio di cui sopra.
- E' attivo un contratto 24X7 per gli impianti di condizionamento/riscaldamento. La chiamata di assistenza deve essere effettuata dal tecnico reperibile del Servizio Manutenzione dell'Ente.
- Il sistema di monitoraggio NetEye di Wurth, utilizzato per il controllo dei server e altri sistemi ICT (vedi par.16), è dotato di sensori ambientali per temperatura, umidità, fumo e presenza acqua e può essere configurato per inviare allarmi sia SMS ai tecnici reperibili.

1.3 Controllo fisico degli accessi

L'area del servizio SGT in cui si trova il DC primario è protetta da un sistema di controllo accessi tramite badge nominativo configurato dal Servizio Personale per consentire l'ingresso ai soli dipendenti autorizzati. L'accesso al servizio SGT a persone sprovviste di badge è consentito solo previo passaggio alla portineria dell'Ente, deposito di documento d'identità e ritiro di badge temporaneo.

In questo modo l'accesso ai locali è tracciabile e sempre riconducibile ad una persona fisica.

L'ingresso al DC Primario è ulteriormente ristretto da un successivo controllo accessi a cui sono abilitati solo i tecnici del SGT. L'accesso di personale esterno al DC Primario avviene solo in presenza dei tecnici del SGT.

Tutta l'area del servizio SGT, incluso gli accessi al DC primario sono protetti da:

1. sistema di allarme con:

- sensori volumetrici su tutti i piani;
- contatti su porte e finestre;
- sirene interne ed esterne;
- doppio combinatore telefonico sia GSM che in rame collegato alla Centrale Operativa della Polizia Municipale;
- attivazione automatica nelle fasce orarie in cui il personale non è presente.

2. nr. 6 telecamere di videosorveglianza interna con memorizzazione dei filmati per 7 giorni, controllo da parte della Centrale Operativa della Polizia Municipale e posizionate come segue:

- 3 su ogni accesso dell'area del SGT;
- 2 sui pianerottoli di accesso ai vari piani;
- 1 all'interno del DC a garanzia di ulteriore tutela e controllo del sito.

1.4 Connettività

Tutti gli uffici sono collegati al datacenter in fibra ottica ad alta velocità tramite anelli che garantiscono la ridondanza del percorso. In caso di interruzione fisica di un percorso automaticamente

grazie a protocolli di ridondanza tipo STP o LACP, la connessione passa sul percorso alternativo, di pari prestazioni, con tempi di convergenza minimi e quindi senza disservizi per l'utente.

Tutte le fibre ottiche convergono in due punti distinti di accentramento (POP) tra loro collegati mediante 2 link aggregati con protocollo LACP in fibra ottica a 10 GB. In caso di indisponibilità di un POP tutte le sedi connesse all'altro rimangono funzionanti.

Nei due POP sono installati gli switch per gestire i collegamenti delle sedi ad essi afferenti. Il POP principale e' quello all'interno del DC primario dove l'apparato di rete ha sia il ruolo di aggregatore dei link delle sedi che di punto di collegamento tra server, storage e firewall.

L'apparato installato è un EXTREME NETWORKS BD 8900 modulare con 10 slot, alimentazione e management ridondata. Le connessioni che prevedono il doppio percorso sono attestate su schede diverse in modo da evitare disservizi derivati dal fault della scheda. Questo vale in particolar modo per i 4 link 10 Gb verso il sottosistema server e per quelli verso il POP secondario.

Anche nel POP secondario sono previsti 2 switch Extreme Networks 670-48X ciascuno con alimentazione ridondata, 48 P fibra 1/ 10 GB, 2 qsfp 40 GB; le connessioni che prevedono la doppia via sono attestate anche in questo caso su apparati diversi.

L'architettura e configurazione sopra descritte garantiscono la ridondanza dei componenti e dei percorsi e quindi un alto livello di affidabilità delle connessioni logiche anche in caso di indisponibilità di un percorso fisico.

Inoltre, considerata la criticità dei dispositivi nei due POP, l'Ente ha attivo un contratto di assistenza HW che prevede un tempo di ripristino in caso di guasti bloccanti di 4 ore su una finestra di erogazione del servizio H24. E' inoltre previsto un carnet di ore per assistenza sistemistica anche on-site. Il servizio è erogato dalla ditta MEAD Informatica che, a garanzia della competenza, è in possesso delle certificazione di livello massimo prevista dal produttore (PartnerWorks di Livello Diamond).

Sulla stessa rete fisica vengono poi gestite diverse reti logiche tramite la creazione di VLAN in modo da separare collegamenti che devono avere livelli diversi di sicurezza. Ad esempio la network delle postazioni è separata da quella dei server, cosi' come la rete di videosorveglianza è isolata da tutte le altre e non ha accesso ad internet.

Nel POP principale presso il SGT è attivo il punto di consegna dell'accesso alla rete Lepida che viene utilizzato:

- per l'accesso ad internet degli utenti;
- per la pubblicazione dei servizi dell'Ente;
- per l'accesso alla rete SPC delle PA;
- per l'accesso al Datacenter secondario.

Il collegamento con la rete Lepida è in fibra ottica, con percorso ridondato, simmetrico e senza limiti di banda. L'unico limite è determinato dalla caratteristiche dell'interfaccia fisica degli apparati di rete.

Il tipo di collegamenti e di topologia adottati consentono di rendere disponibile l'accesso alla rete Lepida in qualsiasi punto della rete dell'Ente anche diverso dal SGT.

L'accesso da/verso internet è gestito tramite apparati perimetrali che ne garantiscono la sicurezza. Inoltre i server che erogano servizi accessibili da internet sono pubblicati tramite un sistema dedicato (F5 BIG-IP) che permette di definire configurazioni molto granulari in cui si puo' ad esempio decidere:

- quali sono gli uri accessibili e su che protocolli;
- pubblicare con protocolli sicuri siti/applicazioni che all'interno utilizzano ancora protocolli non criptati;
- ridirigere un URL pubblico su differenti URL privati;

Anche in questo caso, essendo in sistema critico per la disponibilità dei servizi esposti al cittadino, la configurazione prevede 2 appliance active-passive.

Il dialogo tra le varie reti logiche e con internet è controllato da un firewall costituito da 2 Gateway Check Point con bundle NGTX, su piattaforma Open Certified Server.

Sono installati i moduli:

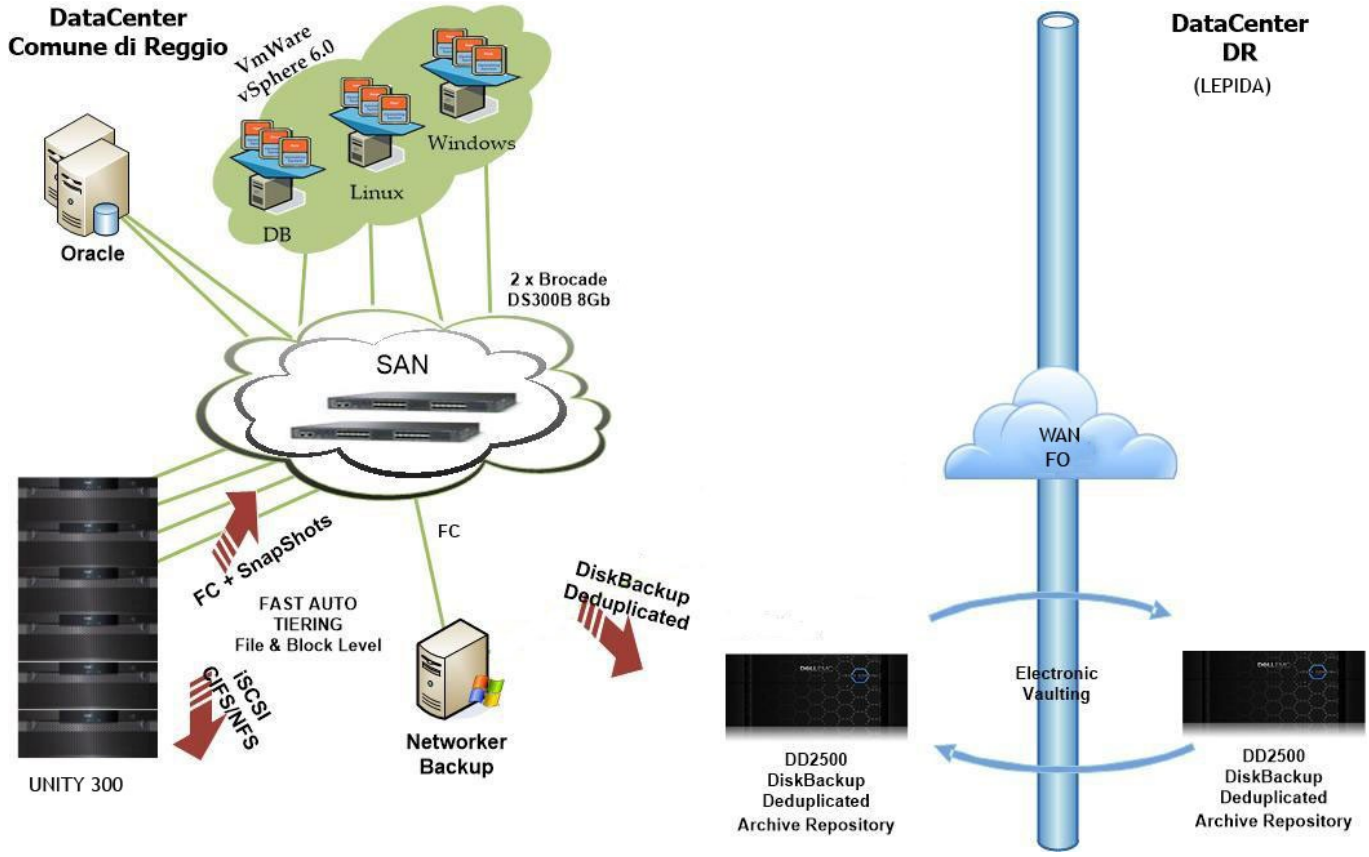
- Identity Awareness
- Application Control
- URL Filtering
- Anti-Virus
- Intrusion Prevention System
- Antibot
- Antispam
- Mobile Access
- Applicance Sand-box

L'Ente ha inoltre attivo:

- contratto di Supporto hardware/software di tipo Collaborative Enterprise Standard Edition erogato direttamente dal produttore (Checkpoint) che include gli aggiornamenti di release, i servizi a canone e la possibilità di scalare in caso di problemi complessi ed ottenere supporto direttamente dal produttore.
- Contratto di assistenza sistemistica con un partner Checkpoint (vedi par.5.2.5).

1.5 Sistemi Hardware

Il sistema ICT del DC primario è basato su un'infrastruttura server costituita da una enclosure Blade HP C7000 e 10 lame Blade. Il sottosistema server è collegato allo switch di core EXTREME NETWORK BD 8900 (vedi par. 1.4) e al sottosistema storage DELL EMC UNITY 300. Il progetto è stato realizzato senza Single-point-of-failure: quindi tutte le componenti e link sono ridondanti sia per avere una struttura in alta affidabilità che per bilanciare il carico.



Di seguito si riporta una breve descrizione dei due sottosistemi:

Server:

- Enclosure Blade HP C7000 che costituisce il contenitore fisico dei server veri propri e fornisce i servizi di base comuni a tutti i server:
  - alimentatori e ventole ridondati e sostituibili a caldo;
  - moduli di interconnessione fiber channel verso lo storage;
  - sistema di amministrazione e di management dei server dell'enclosure con funzionalità di inventory, controllo dei parametri di funzionamento (es: temperatura, alimentazione, ecc.);
  - possibilità di installare fino a 16 server blade.
- 14 server blade HP BL460c GEN7/8/9:
  - doppio processore con 6 o 8 core per socket;
  - RAM da 96 GB a 160 GB;
  - 2 dischi SAS in RAID1 per l'installazione di ESX per le blade che compongono il cluster Vmvare (ved. Par.xxx) o del sistema operativo + oracle RAC per le blade del db server;
  - controller di rete con due porte 10 Gb per il collegamento verso lo switch di core;
  - 2 schede dual port fiber channel per il collegamento verso lo storage.

Per tutti i server fisici, inclusa l'enclosure, è attivo un contratto di manutenzione hardware erogato direttamente da HP che prevede interventi on-site NBD.

Storage: l'architettura prevede un unico storage in grado di presentare lo spazio disco necessario ai vari server collegati. Questo e' realizzato tramite un sistema EMC UNITY 300 di fascia midrange utilizzabile sia per ambienti virtuali che transazionali con le seguenti caratteristiche:

- di tipo Unified (file e blocchi) e multiprotocollo;
- ridondato in ogni sua parte;
- dotato di due controller active/active in grado presentare lo spazio disco tramite collegamenti fibre Channel (SAN) o su rete TCP-IP (NAS);
- collegamento a 40 Gb verso lo switch di core e 4x16Gb verso i server;
- in grado di gestire tipologie di dischi diversi (SSD, SAS, NL_SAS, ecc.) vedendoli come un unico pool logico. All'interno del pool funzioni di ottimizzazione consentono di spostare i blocchi dati dinamicamente su dischi veloci o lenti in base alle richieste di accesso;
- supporta diversi livelli di (RAID 1,5, 6 ecc.) ed è configurato con almeno un disco SPARE per tipologia;
- dotato di sistemi di caching in ram o su SSD per ottimizzare le prestazioni;
- mette a disposizione dei server/utenti 94 TB di spazio utili;
- integrato con Vmware site recovry Manager (SRM), con Legato Networker e Data Protection Suite;
- supporta il protocollo CAVA utilizzato dai sistemi antivirus per proteggere lo storage da intrusioni (vedi par. 1.7);
- funzionalità di snapshot e replica native utilizzate in abbinamento al back-up per rendere più semplice il restore di parti del NAS (vedi par. 1.8);
- coperto da contratto di manutezione hardware e software erogato direttamente da EMC e di tipo mission-critical (livello premium) on site 24 x 7;
- sistema di monitoraggio con collegamento diretto verso il servizio di manutenzione del produttore. Questo elemento, abbinato al contratto di cui al punto precedente fa si che a fronte di un qualsiasi problema hardware, anche non critico, e che non determina nessun disservizio per l'utente, venga inviata una segnalazione ad EMC ed aperto un ticket per la soluzione del problema.

Lo storage sopra descritto è quindi utilizzato tramite i protocolli Block (SAN):

- dai sistemi oracle per i dischi su cui sono memorizzati i DB;
- dai server ESX per rendere disponibile lo spazio su cui sono creati i dischi "dependent" delle VM;
- dai server ESX per creare dei dischi di tipo "persistent indipendent" gestiti al di fuori dei file vmdk;

e tramite i protocolli file (NAS):

- per rendere disponibile dischi di rete (Share) su cui, configurando opportunamente gli accessi per i vari gruppi di utenti, gli uffici dell'Ente memorizzano i documenti;
- per rendere disponibile aree di archiviazione per applicazioni che debbano salvare documenti direttamente su percorsi UNC.

1.6 Software di infrastruttura

La maggior parte dei server di infrastruttura o che erogano servizi applicativi sono sistemi virtuali configurati sull'infrastruttura Vmware installata sui nodi blade fisici descritti al par. 1.5.

Sul pool di nodi fisici e' stato creato un cluster vmware che include due ambienti: produzione e sviluppo/test differenziati in base all'uso delle risorse condivise.

L'utilizzo della piattaforma virtuale da numerosi vantaggi tra cui:

- semplicità nell'assegnazione delle risorse: se un server ha bisogno di maggiori prestazioni è semplice allocare maggiore RAM, aggiungere virtual CPU o disco;
- ottimizzazione delle risorse: le risorse fisiche dei nodi sono condivise tra gli N sistemi virtuali con tecniche di ottimizzazione previste da VMWARE. Inoltre il sistema Distributed Resource scheduler (DRS) di vmware permette di bilanciare il carico sui vari nodi fisici spostando dinamicamente i server senza disservizi per gli utenti;
- semplicità nella creazione di nuovi server: per installare un nuovo server non è più necessario avere a disposizione un hardware fisico con i relativi tempi di approvvigionamento;
- meccanismi di fault tolerance: la funzionalità di Vmotion permette di spostare automaticamente tutti server virtuali da un nodo fisico agli altri , senza disservizi per gli utenti, qualora questo sia indisponibile;
- possibilità di fare snapshot a caldo dei server virtuali e ritornare rapidamente al momento dello snapshot: in caso di aggiornamenti software critici questo previene eventuali indisponibilità dei servizi applicativi qualora l'aggiornamento stesso non sia andato a buon fine;
- possibilità di fare il back-up/restore dell'intero server virtuale in modo semplice e veloce senza l'uso di agenti installati sul server. Il restore è possibile sia per l'intera Virtual machine che per singoli file.

I sistemi critici per la disponibilità dei servizi applicativi, indipendentemente che siano server fisici o virtuali, sono configurati su più nodi in modalità active-active o active-passive in modo che l'indisponibilità del singolo sistema non determini quella dell'intero servizio.

I casi principali sono:

- Gestori dell'accesso al Dominio: repository di utenti, credenziali, sistemi Microsoft in rete e servizi di infrastruttura (DNS, DHCP, DFS) : Microsoft Active Directory con due Domain controller sempre attivi;
- DataBase oracle: repository utilizzato dalla maggioranza delle applicazioni. Basato su ORACLE Enterprise Edition + Oracle Real Application Cluster 11.2.0.4. Il DB è memorizzato su dischi condivisi gestiti dal ASM di oracle e accessibili dai due nodi fisici. La configurazione attivata permette di vedere i due server come uno solo (SRV-ORA) che risponde a 3 IP differenti ruotati con il round-robin del DNS. I dati di tutti gli applicativi che usano oracle sono divisi in 3 istanze logiche (EDI, UGO e DWH) che, tramite gli oracle services insistono ciascuna su due istanze fisiche (una per server). Questo permette, in situazioni normali, di bilanciare il carico tra i due nodi fisici ma, in caso di manutenzione (ad esempio patching del sistema operativo) o di fault di un nodo, di mantenere SEMPRE la disponibilità/accessibilità dei dati. Il passaggio da un nodo all'altro è fatto automaticamente da Oracle quando il sistema si accorge dell'indisponibilità del nodo stesso o può essere programmato in caso di manutenzione. In tutti i casi non sono necessarie modifiche di configurazione agli applicativi e il disservizio per l'utente si limita, nel peggiore dei casi, a ripetere la transazione in corso;
- Application Server Tomcat/jboss/WildFly: questi application server sono utilizzati da diversi applicativi critici quali Albo Pretorio, suite jEnte (atti, protocollo, segreteria, demografici, finanziaria, Garsia, Geac, ecc.). La configurazione adottata prevede due macchine virtuali sulle quali è stato attivato il Network Load Balancer di Microsoft. Questo software, attraverso un unico ip virtuale, permette di accedere agli Apache di front-end di entrambi i nodi con un unico URL, effettuando un bilanciamento del carico. A loro volta gli Apache di front-end

gestiscono il reindirizzamento sul Tomcat/jboss di uno o di entrambi i nodi;

- Firewall: 2 Gateway Check Point con bundle NGTX, su piattaforma Open Certified Server installati su due server fisici HP DL360p Gen9. Configurazione Active-passive con attivazione automatica del nodo in stand-by in caso di fault di quello attivo senza perdita di servizio per gli utenti. Possibilità di passare da un nodo all'altro anche in caso di attività di manutenzione / aggiornamento riducendo eventuali tempi di fermo.

L'Ente ha ritenuto prioritario aumentare la sicurezza della rete agendo non solo sulla parte perimetrale esposta su internet, ma anche sul lato interno.

Nel corso degli anno il SGT ha adottato politiche verso le software houses tese a condividere lo stack tecnologico necessario per il funzionamento dei vari applicativi, evitando in questo modo il prolificare dei server e la creazione di sistemi dedicati al singolo applicativo.

Le regole interne prevedono che se più applicazioni necessitano degli stessi software middleware vengano installate su server condivisi: allo stesso modo nei requisiti tecnici per la scelta di un applicativo viene indicato come criterio preferenziale la compatibilità con Oracle.

Questo ha permesso di attivare configurazioni più complesse, come quelle descritte sopra, ma che prevedono la ridondanza dei nodi, visto che lo stesso ambiente viene utilizzato da più software houses.

I sistemi in rete vengono mantenuti aggiornati sia dal punto di vista delle versioni del sistema operativo che di quelle dei software di piattaforma che del patching di sicurezza, fermo restando i vincoli imposti dal software applicativo.

Nei casi in cui il software applicativo non consente l'aggiornamento, ne viene tenuto traccia nel documento "MM_sistemi_critici". Per ogni sistema non aggiornabile viene anche attribuito un livello di rischio (ad esempio in base alla differenza tra il livello di patching presente rispetto a quello auspicabile) e un livello di criticità legato all'impatto di quel sistema sui servizi applicativi dell'Ente. Nello stesso documento vengono altresì indicate le misure / piano di attività previste per sanare la criticità.

Le modalità di aggiornamento e di patching sono descritte nel documento MisureMinime Comune Re.pdf di cui alla determinazione dirigenziale AD 2017/1889 e successive modificazioni.

L'Ente ha installato sui propri sistemi il sistema di monitoraggio NetEye di Wurth che consente di tenere sotto controllo alcuni indicatori importanti per il funzionamento dei sistemi e definire soglie di criticità / eventi al cui raggiungimento / verificarsi vengono inviate notifiche via email ai sistemisti responsabili del servizio.

Questo rende possibile un monitoraggio pro-attivo dei sistemi permettendo di intervenire quando si verificano situazioni non ancora critiche che, se non gestite correttamente, potrebbero determinare l'indisponibilità dei sistemi. Consente anche di avere accortezza immediatamente di un malfunzionamento di un componente dell'infrastruttura ICT, determinando l'intervento prima della segnalazione dell'utente e semplificando l'analisi delle cause del disservizio.

I principali check effettuati sono i seguenti:

- raggiungibilità di oggetti in rete quali server, appliance, controllo accessi, timbratori, sistemi di videosorveglianza, ecc;
- disponibilità di link di rete e log dell'utilizzo di banda effettuato;

- controlli su utilizzo di CPU e RAM, occupazione disco e uptime del server;
- verifica sull'effettiva disponibilità dello specifico servizio installato/configurato nel server controllando ad esempio che il servizio LDAP risponda o, in caso di servizio web, la pagina arrivi in tempi corretti;
- parametri significativi per monitorare la funzionalità di Oracle DB quali:
  - il numero di connessioni e di utenti connessi;
  - il tempo di risposta della connessione;
  - la dimensione della FRA e di alcune TS che non hanno l'estensione automatica;
  - l'assenza di job orfani;
  - l'esito di alcuni job eseguiti direttamente sul server Oracle;
- l'assenza di errori di deploy per i server tomcat/jboss;
- parametri significativi per monitorare la funzionalità del db Ms-Sql quali:
  - il numero di connessioni e di utenti connessi;
  - il tempo di risposta della connessione;
  - la dimensione di alcuni data file;
  - l'esito dei backup e la loro consistenza;
- la disponibilità della share di rete per alcuni server Linux che la utilizzano;
- che la directory dei file di log non abbia file superiori ad una certa dimensione;
- controlli specifici sul funzionamento del DNS;
- controlli specifici per verificare il corretto funzionamento dell'host e della Control Center per i server Vmware.

Per la piattaforma NetEye è attivo un contratto di manutenzione direttamente con il produttore che prevede gli aggiornamenti software e la possibilità di aprire ticket di assistenza.

Parallelamente a NetEye è in funzione anche un sistema di monitoraggio specifico per gli apparati di rete: NetSight di Extreme Networks.

Anche in questo caso sono configurate notifiche automatiche in caso di:

- indisponibilità di un apparato di rete;
- problemi sul funzionamento dell'apparato stesso (es: temperature elevate, problemi sulle ventole, ecc.);
- login falliti;
- problemi su protocolli per la gestione dei link ridondati tipo LACP, STP;
- il passaggio da un percorso ad un altro.

1.7 Sistemi di sicurezza

L'Ente ha ritenuto prioritario aumentare la sicurezza della rete agendo non solo sulla parte perimetrale esposta su internet, ma anche sul lato interno, agendo in due modalità:

1. attivando una piattaforma di controllo degli accessi alla rete sia wired che wirelless in grado di

dare accesso, ai soli dispositivi abilitati, alle risorse interne della rete dell'Ente.

2. Intervenendo sul software di protezione installato sui singoli endpoint su cui è stato installato l'antivirus Kaspersky Endpoint Security for Business.

   Il prodotto è stato scelto valutando diverse soluzioni di mercato, dopo aver effettuato un periodo di test che ha previsto il confronto con altri prodotti come Sentinel One, Symantec Endpoint Security e l'esame del feed-back di altri enti che lo avevano già adottato.

   Il prodotto scelto implementa, oltre alle tecniche tradizionali per l'identificazione di agenti malevoli basate su firme o altri meccanismi reputazionali, sistemi comportamentali incluse tecnologie di machine learning statiche e dinamiche. Prevede inoltre una console centralizzata che consente la definizione di policies da applicare a tutte le PDL e il monitoraggio dell'effettivo funzionamento.

   Tutti i PDL e Server si aggiornano automaticamente ricevendo, dal Server su cui è presente la console di mangement, gli aggiornamenti dell'AV e delle policies di sicurezza.

   Le policies sono configurate per controllare in modalità real-time l'apertura, esecuzione e scrittura dei file sia su dischi locali e di rete che su dispositivi esterni (removable drives). Viene controllato anche il download durante la navigazione WEB. Sono attive anche policies Advanced relative a Behaviour Detection (controllo comportamentale), Exploit Prevention (attività legate a malware), Host Intrusion Prevention. Tutti i client vengono scansionati settimanalmente (Server) e mensilmente (Client) per l'eventuale presenza di virus su file system. Tutti i dispositivi removibili vengono scansionati prima del loro utilizzo in modo automatico. Nel caso venga rilevata la presenza di Virus, l'antivirus, prova a ripulire l'oggetto infetto. Nel caso fallisca o non sia possibile ripulire l'oggetto, verrà eliminato.

E' stato anche installato Kaspersky security for storage: è un modulo della stessa suite che, tramite protocollo CAVA, dialoga direttamente con lo storage NAS Unity per prevenire l'ingresso di agenti malevoli che non transitano dalle postazioni client. Un caso particolarmente importante che si è verificato riguarda malware contenuti in allegati di caselle PEC. Questi messaggi vengono gestiti automaticamente dall'applicazione del protocollo e in assenza del modulo suddetto avrebbero provocato la memorizzazione sullo storage condiviso di documenti infetti, che sono invece stati bloccati preventivamente.

In aggiunta a queste misure l'Ente ha anche attivato il servizio Breach Detection, Investigation & Response previsto all'interno della convenzione Intercenter "Servizi di trasmissione dati e voce su reti fisse (Lotto 1)". Il servizio tramite l'installazione di una sonda che cattura il traffico da/per internet di tutta la rete e sistemi remoti SIEM è in grado di:

- Identificare la presenza di anomalie nel traffico di rete e nell'esecuzione dei processi applicativi all'interno di sistemi server e client;
- Svolgere attività mirate di analisi ed investigazione per comprendere la natura delle anomalie ed identificare l'eventuale presenza di attacchi informatici;
- Confermare la presenza di intrusioni e tentativi di frode ed identificare le operazioni di gestione dell'incidente per la riduzione dell'impatto sulla disponibilità dei sistemi.

Il servizio comprende la consulenza di specialisti in problematiche di sicurezza per cui, a fronte di una potenziale minaccia, vengono attivati allarmi che sono notificati via email ai referenti per la sicurezza del SGT. Per ogni allarme sono suggerite misure dettagliate per verificare l'effettiva compromissione e contenere il danno.

I sistemisti del SGT possono accedere alla piattaforma Certego PanOptikon su cui gestire l'evoluzione dell'incidente e su cui è anche possibile aprire ticket per richiedere verifiche specifiche in caso di segnalazioni di potenziali eventi di sicurezza provenienti da altre fonti.

1.8 Politiche di back-up

Il back-up di tutti i dati/sistemi dell'Ente viene effettuato tramite il software legato Networker - Data Protection Suite che, tramite una unica console di gestione, permette di definire vari job, politiche di copia (schedulazione, la retention, ecc.) diverse a seconda del tipo di dato, la notifica dell'esito ed effettuare i restore quando neccessario.

L'output dei processi di back-up viene salvato, in un formato proprietario, criptato e non direttamente accessibile senza il sw di back-up che lo ha creato, su un dispositivo dedicato DELL EMC DATADOMAIN 2500 costituito da un insieme di dischi SAS. Questo dispositivo utilizza algoritimi di deduplica hardware per ottimizzare lo spazio disco necessario consentendo alti periodi di retention, riducendo i tempi di back-up e soprattutto quelli di un eventuale restore. Il fattore di deduplica è dipendente dalla tipologia di dato salvato ma è circa di 10x – 20x.

Sono stati inoltre attivati protocolli come BOOST che consentono di usare meccanismi di deduplica già alla sorgente del back-up riducendo il traffico di rete ma soprattutto i tempi sia di copia che di ripristino.

Il DataDomain, supportando protocolli NFS e CIFS, è stato configurato per presentare parti del suo spazio disco direttamente ai DB server Oracle e My-sql che lo utilizzano come destinazione di back-up prodotti dagli strumenti nativi dei DB stessi (es: RMAN, EXPORT, ecc.).

Lepida utilizza nei propri data center dispositivi analoghi; avendo attivato i servizi DataDomain As a Service con lepida (vedi sez.2) sono state configurate le funzionalità di replica disponibili su questi apparati per avere una copia del back-up, indipendentemente da come e' stato ottenuto (netwoker, Rman, ecc.) nel il DC secondario.

Tutti i back-up sono effettuati a caldo e senza fermo dei servizi: dove necessario vengono utilizzati agenti specifici per le varie piattaforme o modalità di copia certificate (vedi DB) per garantire la congruenza e consistenza dei dati.

Di seguito sono descritte le policies di back-up per le principali tipologie di dati:

1. Dati del NAS (ad esempio dati dei dischi di rete su cui sono memorizzati i documenti dei vari uffici):

   back-up incrementale durante la notte da LUN a DOM (escluso un giorno in cui viene eseguito in modalità FULL);

   back-up full una notte in giorni diversi della settimana in base al File System copiato a partire dalle ore 19:00. In base alla mole di dati da copiare il tempo per il backup full varia dall'ora alle 40 ore;

   retention: 3 mesi;

   Oltre al back-up sopra descritto, lo storage UNITY 300 che presenta i servizi NAS dispone di funzionalità di snapshot che tenendo traccia delle variazioni, permettono di avere una immagine ad un dato momento in tempi rapidi. Con questo metodo, è quindi stata configurata una copia dei volumi NAS 4 volte al giorno (alle ore 2, 8, 14 e 20) con retention 15 giorni. Ciò consente di ripristinare molto velocemente parte dei dischi di rete come descritto nel par. 5.1.3.

2. Dati di Lotus Domino (piattaforma utilizzata per sito istituzionale e parte della intranet):

   stesse politiche del punto 1. ma con utilizzo dell'agent di Networker per Domino in modo da garantire la congruenza degli NSF, visto che il back-up viene effettuato a caldo.

3. Server fisici (ad esempio i due nodi di Oracle):

   Back-up full a livello di file system una volta a settima e incrementale negli altri giorni eseguito tutte le notti tramite agent installato sul server. Per il back-up dei dati del DB a caldo fare riferimento al punto 5;

   retention: 4 settimane.

4. Server Virtuali (la maggioranza dei server/appliance dell'infrastruttura ICT):

   La combinazione tecnologica del sw di back-up (Legato Networker, piattaforma di virtualizzazione (Vmware), sistema di memorizzazione degli ouput del processo di copia (DD2500) consente di effettuare salvataggi dei server virtuali e dei dischi "dependent" ad essi assegnati, direttamente dai server ESX, senza necessità di avere agent installati sul singolo sistema e garantendo la congruenza del file system.

   Back-up full ogni notte per i server in produzione, solo il sabato notte per i server di test/sviluppo.

   retention: 1 mese.

5. Server di posta (DEB-ZMAIL):

   il back-up viene effettuato tramite Zextras Suite (Zbackup) che intercetta e analizza le azioni eseguite dal server Zimbra e crea istantaneamente una copia del dato grezzo e di tutti i cambiamenti che avvengono a seguito di ogni operazione, applicando meccanismi di deduplica e compressione. Quindi il contenuto della casella di posta è costantemente salvato: email in entrata o in uscita, appuntamenti, contatti, file. Anche tutte le variazioni degli attributi sono preservati: quale cartella contiene il messaggio, come sono organizzate, i tag utilizzati, lo stato di lettura nonchè le proprietà dell'account quali preferenze, firme, filtri, password. Zextras gestisce tutte le informazioni inclusa la definizione del domino, le liste di distribuzione e tutte le configurazioni del sistema. L'output di Zbackup viene memorizzato su un disco dedicato di tipo "depedent" agganciato alla vm DEB-ZMAIL.

   Il server viene quindi copiato con le modalità descritte la punto 4, poiché la congruenza della casella di posta è garantita dall'uso del modulo ZBackup.

6. DataBase Oracle:

   Oltre a quanto detto al punto 3., tramite l'agent di legato networker + RMAN vengono copiati 4 volte al giorno (alle ore 8,10,13,16) gli archive log dei DB transazionali EDI e UGO e una volta al giorno l'intero DB con ouput sul DD2500, con retention di 7 giorni.

   Per gli stessi DB ogni notte viene fatto un export FULL dei dati e dei metadati (DDL): anche in questo caso l'output è memorizzato sul DD2500, ma nell'area esposta tramite CIFS.

   L'istanza DWH, dedicata al DataWharehouse, ha modalità di aggiornamento non real-time, ma solo tramite processi schedulati. Di conseguenza anche le politiche di back-up possono essere meno stringenti e non è necessaria la copia degli archive log.

   Pertanto, per l'istanza DWH ,viene schedulato un export FULL il giorno 1 e 15 di ogni mese e giornalmente l'export full dei soli metadati (DDL). Anche in questo caso si utilizza l'area CIFS del DD2500 per memorizzare il back-up.

7. DataBase MS-Sql:

   Oltre a quanto detto al punto 4., per i database non soggetti a transazioni viene fatto un back-up full tutte le sere.
   Per gli altri, oltre al back-up full tutte le sere, viene eseguito un back-up dei transaction log ogni 4 ore (8.30, 12:30, 16:30, 20:30). In questo caso, a differenza di quanto avviene per Oracle, si utilizzano le funzionalità di export native di Mysql senza la necessità di avere l'agent di Legato Networker installato sul server. Anche in questo caso si usa l'area CIFS del DD2500 per memorizzare il back-up.

Per i back-up visti al punto 6 e 7, le aree CIFS del DD2500 configurate per questo scopo vengono poi copiate tutte le sere con retention di 28 giorni e una volta al mese con retention 6 mesi usando la funzionalità Mtree di DataDomain.

Il DD2500 è coperto da un contratto di assistenza hardware e software erogato direttamente dal produttore (EMC Enhanced Support) con interventi on-site, copertura 24x7 o livelli di interventi in base alla criticità del problema da 1 a 10 ore.

1.8.1 Politiche di replica/clone verso il DC Secondario

Come meglio descritto in seguito nella sezione 2, l'Ente ha definito il Datacenter di Lepida come sito di disaster recover. Di seguito sono descritte le politiche di replica dei back-up dal DD2500 installato presso il DC Primario al DC Secondario (Datacenter di Lepida). Tale politiche sono rese possibili grazie all'uniformità di stack tecnologico (anche nel DC di Lepida sono presenti apparati DataDomain anche se con maggiori prestazioni), ai contratti in corso e al tipo di connettività garantita dal punto di accesso alla rete Lepida.

Le repliche/clone verso il DC Secondario, realizzate verso apparati tecnologiche affini al nostro, sono notevolmente facilitate ed ottimizzate. Al termine del backup dei server Virtuali sui nostro dispositivo, viene eseguito un job di clone che si occupa di copiare i dati verso il dispositivo presente presso il DC Secondario, per le altre tipologie di dati vengono eseguiti job di clone opportuni come descritto in seguito. Questo processo ci consente di definire anche politiche di retention differenti per i dati clonati. Più precisamente:

- backup server virtuali: clone al termine del backup con retention di una settimana;
- backup server fisici, Oracle Archive e full, Lotus Notes (Full e Incrementali): clone giornaliero con retention di una settimana;
- Oracle Full, Lotus Notes (Full): clone mensile con retention 6 mesi;
- backup full NAS: clone mensile con retention 6 mesi;
- backup incrementale NAS: clone giornaliero con retention di una settimana.

1.9 Documentazione

In caso di incidenti l'accesso alla documentazione aggiornata e' di fondamentale importanza perché consente di avvalersi del supporto di professionalità esterne che potrebbero non avere la conoscenza completa dell'infrastruttura ICT.

Il SGT ha sviluppato un repository in cui sono censiti:

- applicazioni: per ognuna sono indicate informazioni come:
  - referenti informatici,

  - referenti degli uffici utilizzatori,
  - riferimenti sw houses e contratti di manutenzione,
  - piattaforme necessarie al funzionamento,
  - basi dati fisiche e logiche utilizzate,
  - server su cui l'applicazione è installata,
  - web service invocati,
  - utenti abilitati e ruoli,
  - integrazioni con altre procedure/processi.
- Banche dati fisiche e logiche: per ognuna sono censite:
  - tipo di RDBM (es: oracle / Ms-sql),
  - Utenti DB proprietari ed applicativi che lo utilizzano,
  - Presenza di dati personali o particolari,
  - Responsabile del trattamento,
  - Trattamenti effettuati, finalità e categoria degli interessati.
- Server: per ognuno sono censiti:
  - sistema operativo,
  - piattaforme installate,
  - ruolo,
  - servizi / attività pianificate configurate.
- Amministratori: utenze amministrative:
  - persona fisica a cui l'utenza è assegnata,
  - eventuali riferimenti del fornitore in caso di personale esterno,
  - ambito di attività (es: server, dominio, software complesso, apparato di rete, ecc.) ed elenco dei dispositivi di quella tipologia su cui l'utenza ha ruoli amministrativi,
  - link al documento di nomina ad "amministratore di Sistema, in caso il ruolo, in base alla normativa sulla protezione dei dati personali, lo preveda.
- Rete: censimento di tutti gli oggetti connessi alla rete:
  - Indirizzo IP,
  - Tipologia (es: server, controllo accessi, telefonia, access point , ecc.),
  - Network logica a cui appartiene.

All'interno del repository sono gestite le relazioni tra le varie entità censite. Questo permette, ad esempio, di sapere rapidamente:

- se un server non è funzionante, quali servizi applicativi sono compromessi e viceversa;
- se un DB non è disponibile, quali servizi applicativi sono compromessi, se sono interessati dati sensibili o giudiziari, chi sono i responsabili del trattamento da coinvolgere ecc.;

- se un servizio applicativo non è disponibile, chi sono i referenti interni o le software houses da coinvolgere;
- se occorre accedere ad un server per verifiche tecniche, chi sono per persone abilitate all'amministrazione del sistemato.

E' inoltre disponibile il sistema documentale basato su Alfresco che include il modulo Alftresco Share su cui è stata creata un'area per la memorizzazione dei documenti del SGT con ricerca full-text. L'area è suddivisa in 4 macro sotto aree:

- Amministrativi: documentazione relativa ad atti, forniture, convenzioni, ecc.;
- Applicativi: documenti relativi ad applicativi (ad esempio Data Wharehouse, Jasper report, Contabilità, Edilizia, ecc.);
- Assistenza: documenti relativi all'assistenza delle PDL e al servizio di Help Desk;
- Sistemi: documenti sistemistici riguardanti ad esempio: application server, database, geoserver, piattaforme specifiche (Esri, BIG-IP F5, Plone, ecc.).

Tale documentazione viene periodicamente copiata sull'area del NAS del SGT e soggetta alle politiche di copia descritte al par 1.8 comma 1, in modo che in caso di incidente o di indisponibilità del sistema documentale sia semplice reperirla dal back-up.

Altra documentazione rilevante sia per la prevenzione che per la gestione di incidenti è la seguente:

- Disciplinare per utenti dei sistemi informativi: descrive le regole tecniche ed organizzative da applicare da parte degli utenti che accedono al sistema informativo dell'Ente per l'utilizzo di strumentazioni informatiche.
- Regolamento per la gestione degli incidenti di sicurezza relativi alla protezione dei dati personali (Data breach): descrive lo schema di procedura operativa dell'Ente per la gestione degli incidenti di sicurezza che possono comportare una violazione di dati personali comunque trattati.
- Misure minime di sicurezza ICT per le pubbliche amministrazioni: modalità di adozione dell'Ente delle misure minime per la sicurezza ICT indicate da AGID con la circolare del 17 marzo 2017 al fine di contrastare le minacce più comuni e frequenti cui sono esposti i sistemi informativi.

2. CN-ER e Lepida

La Regione Emilia Romagna da diversi anni ha intrapreso un ruolo molto importante per lo sviluppo della Società dell'Informazione per tutti gli Enti locali della regione tramite l'istituzione della Community Network ER e la società Lepida Scpa, in ottemperanza anche al testo aggiornato dell'art. 14 del CAD, in materia di rapporti tra Stato, Regioni ed autonomie locali.

La CN-ER rappresenta il modello inter-istituzionale concepito e realizzato all'interno del Piano Telematico dell'Emilia-Romagna al fine di consentire a tutti gli enti emiliano-romagnoli di disporre dei medesimi strumenti, vantaggi ed opportunità offerti dall'ICT in funzione dell'avvio, dello sviluppo e del dispiegamento dei processi di e-government.

La Community Network Emilia-Romagna è, prima di tutto, un insieme di persone che, nell'ambito della propria amministrazione di appartenenza, lavora per lo sviluppo di servizi innovativi da erogare a cittadini e imprese.

Il principio ispiratore su cui si basa la CN-ER è quello di "fare sistema" tra gli enti locali per poter mantenere, e possibilmente aumentare, il buon livello di coesione territoriale raggiunto in questi anni. Per "fare sistema" è indispensabile ideare, progettare e dispiegare i sevizi in costante e fattiva collaborazione tra tutti gli enti locali tra loro e tra i singoli enti locali e la Regione Emilia-Romagna, contribuendo ad armonizzare ed integrare lo sviluppo tecnologico dell'intera regione.

Il quadro normativo di riferimento è la L.R. 4/10 "Sviluppo regionale della società dell'informazione" (aggiornamento della L.R. 11/04), che all'art 4bis, rafforza ulteriormente il ruolo della CN-ER, come organizzazione e modalità di collaborazione tra Regione ed EE.LL. per l'attuazione degli interventi e misure previsti dalla legge stessa a cui è attribuito anche il compito di assicurare l'indirizzo e il controllo determinante, coordinati e congiunti, nei confronti della società in-house Lepida.

Lepida Scpa è lo strumento operativo promosso dalla Regione Emilia-Romagna per la pianificazione, lo sviluppo e la gestione delle infrastrutture di telecomunicazione degli Enti-Soci e degli Enti collegati alla rete Lepida e per l'erogazione dei servizi informatici inclusi nell'architettura di rete.

Il Comune di Reggio Emilia ha approvato la "Convenzione tra la Regione Emilia-Romagna e gli enti locali dell'Emilia-Romagna e le loro forme associate per la costituzione della Community Network Emilia-Romagna " con deliberazione di Giunta Comunale n. 141 del 05/09/2019.

Lepida ScpA agisce, nell'ambito della Community Network dell'Emilia-Romagna, sulla dimensione tecnologica per quanto concerne il sistema infrastrutturale e sui servizi innovativi, produce innovazione per la Pubblica Amministrazione ed opera come partner facilitatore per l'innovazione.

Il Comune di Reggio Emilia ha aderito alla sottoscrizione dell'aumento di capitale sociale deliberato dalla società Lepida S.c.p.a con determina dirigenziale P.G. n. 7550 del 08/04/2009, diventandone socio a tutti gli effetti.

Lepida fornisce dal 01/01/2009 a tutti gli enti del territorio connettività in banda ultra larga tramite collegamenti in fibra ottica con alta affidabilità e percorsi ridondati.

Oltre alla connettività, mette anche a disposizione servizi di infrastruttura che l'Ente utilizza da tempo(es: federa, Payer, ecc.).

Da diversi anni Lepida ha anche attivato Datacenter dislocati sul territorio regionale (Ravenna, Ferrara, Parma) con un alto livello tecnologico ed in grado di garantire livelli di disponibilità elevati.

I servizi offerti sono tipicamente di tipo cloud Iaas e sono:

- housing (gestione di sistemi di proprietà dell'Ente, ospitati presso il DatacentER);

- hosting su piattaforma dedicata;
- hosting su infrastruttura virtuale;
- backup remoto;
- servizi per il disaster recovery (electronic vault, replica su DC remoto, DataDomain as a service);
- Storage as a Services;
- Firewall as a Services;
- Oracle as a Service.

Per la descrizione completa dei servizi erogati da Lepida Scpa fare riferimento all'"Allegato A - Misure di sicurezza per i servizi di datacenter Lepida Scpa".

2.1 Caratteristiche Data Center Secondario

La complessità delle tematiche relative alle soluzioni di continuità operativa e di Disaster recovery, la scarsità delle risorse umane ed economiche disponibile, la necessità di razionalizzare la spesa, ha portato il Comune di Reggio Emilia a stipulare contratti con Lepida Scpa, in modo da considerare il Datacenter di Lepida come Datacenter secondario su cui attivare i sistemi necessari ad erogare i servizi in caso di indisponibilità totale del DC primario. Pertanto d'ora in poi si fara' riferimento al sistema di datacenter di Lepida come "DC Secondario".

Questo e' anche in linea con quanto suggerito della Linee Guida per il Disaster recovery delle PPAA di Agid come sotto riportato.

"…. può rendere conveniente il ricorso a politiche di co-gestione delle soluzioni di CO e di DR tra più Amministrazioni omogenee per struttura, organizzazione e ubicazione geografica; l'associazione di più Amministrazioni può anche essere realizzata utilizzando, in tutto o in parte, le infrastrutture esistenti presso le singole Amministrazioni partecipanti all'associazione. Tale modalità è quella definita come "mutuo soccorso".

Il Datacenter di Lepida è in realtà un insieme di 3 datacenter collocate in località della regione distanti tra loro, connessi con collegamenti ad altissima velocità e magliati che si possono pertanto considerare come un unico Datacenter logico.

Il Comune di Reggio Emilia ha attivato diversi contratti con Lepida Scpa tra cui i seguenti sono rilevanti ai fini del piano di continuità operativa:

- Contratto servizi di accesso alla Rete Lepida, FedERA, PayER, ICAR-ER, MultiplER e ConfERence 2018-2020; oltre ai vari servizi di piattaforma include quello di accesso alla rete Lepida che consente:
  - l'accesso dei sistemi della rete dell'Ente ad internet e ai servizi SPC delle PA con banda illimitata e doppia via;
  - l'accesso tramite collegamenti in fibra ottica sempre attivo con banda illimitata e in doppia via ai datacenter di Lepida Scpa;
- Contratto servizi Datacenter per il Comune di Reggio Emilia – Codice progetto 35033 DC/2018-2020; include:

- Server Virtuali;
- Storage as a Service;
- Data Domain as a service;

e può essere ampliato attivando atri servizi di Datacenter previsti nel listino.

I DC di Lepida hanno caratteristiche tali da essere candidabili a Poli Strategici Nazionali (PSN) secondo la classificazione del piano triennale di AgID. Sono inoltre in corso di certificazione come AgID Cloud Service Provider (CSP).

Le misure di sicurezza volte a prevenire indisponibilità dei sistemi all'interno del DC secondario sono riportate nell'"Allegato A - Misure di sicurezza per i servizi di datacenter Lepida Scpa".

3. Servizi erogati e livello di criticità

Nell'"Allegato B - Elenco Servizi" sono riportati i principali servizi erogati dal sistema informativo dell'Ente con i seguenti indicatori:

- livello di criticità (alto/medio/basso): determinato a seconda dell'importanza del servizio per l'Ente/cittadini. Il livello di criticità determina in caso di incidente di gravità medio/alta la priorità da assegnare per il ripristino dei sistemi necessari all'erogazione;
- tipologia di utenza (utenti interni/eterogenea): a seconda che il servizio sia utilizzato esclusivamente dagli uffici dell'Ente o anche dai cittadini;
- RPO - Recovery Point Objective, indica la perdita dati tollerata: rappresenta il massimo tempo che intercorre tra la produzione di un dato e la sua messa in sicurezza (ad esempio attraverso backup) e, conseguentemente, fornisce la misura della massima quantità di dati che il sistema può perdere a causa di un evento imprevisto;
- RTO - Recovery Time Objective, indica il tempo di ripristino del servizio: è la durata di tempo entro il quale un business process ovvero il Sistema Informativo primario deve essere ripristinato dopo un disastro o una condizione di emergenza (o interruzione), al fine di evitare conseguenze inaccettabili.

4. Ruoli e responsabilità

Analogamente a quanto previsto nel documento di "Gestione degli incidenti di sicurezza relativi alla protezione dei dati personali (data breach)" in vigore nell'Ente con il presente documento si istituisce il **"Gruppo di lavoro per la continuità operativa ICT"** composto prevalentemente da personale del SGT. Vista la rilevanza delle tematiche inerenti la protezione dei dati personali, e particolari, in relazione al contesto generale della sicurezza dei Sistemi Informativi, si ritiene indispensabile includere nel gruppo di lavoro anche un Responsabile dell'Ufficio Privacy.

E' anche individuato un responsabile del **"Gruppo di lavoro per la continuità operativa ICT"**.

I riferimenti nominativi dei componenti del gruppo, i ruoli, incluso quello di responsabile, gli indirizzi e-mail e numeri di telefono sono elencati nell'"Allegato C - Composizione del Gruppo di lavoro per la continuità operativa ICT" allegato al presente documento.

I responsabili per la gestione della sicurezza informatica sono il Dirigente del Servizio Gestione e Sviluppo delle Tecnologie e dei Sistemi Informativi ed il Responsabile della transizione al digitale dell'Ente.

Il "Gruppo di lavoro per la continuità operativa ICT" ha un ruolo sia preventivo che in fase di gestione dell'emergenza, come descritto di seguito.

4.1 Gestione Ordinaria del Piano di DR

In condizioni ordinarie il "Gruppo di lavoro per la continuità operativa ICT" si riunisce con periodicità almeno annuale, allo scopo di valutare lo stato della soluzione di continuità ICT, verificare le criticità, attuare e pianificare le iniziative per il miglioramento continuo dei processi che garantiscono la continuità operativa.

I principali compiti del "Gruppo di lavoro per la continuità operativa ICT" in condizioni ordinarie sono:

- approvazione degli aggiornamenti al presente documento;
- definire la tipologia di test da effettuare e la loro periodicità;

  Alcuni test da effettuare possono essere ad esempio:
  - Verifica delle ridondanze delle componenti più critiche;
  - Verifica della funzionalità del gruppo di continuità e delle procedure in caso di mancanza di alimentazione;
  - Verifica delle procedure di ripristino di server critici in ambiente di test;
  - Verifica delle procedure di rispristino dal DB oracle in ambiente di test;
  - Verifica delle procedure di ripristino del DB MS-Sql in ambiente di test.
- controllo dello stato di aggiornamento della documentazione;
- promozione e coordinamento delle attività di formazione e sensibilizzazione sul tema della continuità operativa del personale dell'amministrazione.

Le procedure messe in campo dovranno assicurare la piena conformità agli obblighi previsti dalla normativa vigente in materia di protezione dei dati personali con particolare con particolare

riferimento al Regolamento europeo 67972016.

In caso di modifiche tecnologiche importanti all'infrastruttura ICT (ad esempio modifiche rilevanti dei servizi o delle applicazioni software, modifiche dell'hardware e/o della rete), può essere convocato per sessioni straordinarie.

4.2 Gestione dell'emergenza

In condizioni di emergenza ICT, il "Gruppo di lavoro per la continuità operativa ICT" assume il controllo di tutte le operazioni e le responsabilità sulle decisioni per affrontare l'emergenza ICT, ridurne l'impatto e soprattutto ripristinare le condizioni preesistenti.

I principali compiti del "Gruppo di lavoro per la continuità operativa ICT", in condizioni di emergenza ICT sono:

- valutazione delle situazioni di emergenza ICT e dichiarazione dello stato di emergenza ICT;
- definizione di un piano delle attività di ripristino delle funzionalità informatiche e controllo del loro svolgimento: a seconda del tipo di incidente potrà essere deciso di valutare soluzioni temporanee che consentano, ad esempio, di riattivare i servizi su sistemi non correttamente dimensionati;
- rapporti con l'esterno e comunicazioni ai dipendenti;
- attivazione e monitoraggio del processo di rientro dall'emergenza ICT;
- gestione di tutte le situazioni non contemplate;
- in caso di servizi SaaS,controlla le attività del fornitore al fine di garantire il rispetto di quanto dichiarato in sede d'offerta e/o specificato contrattualmente;
- gestione dei rapporti interni e risoluzione dei conflitti di competenza;
- dichiarazione di conclusione dello stato di emergenza ICT. In caso siano stati messi in atto soluzione temporanee dovrà essere deciso un piano di attività per il rientro nella situazione di normalità;
- redazione della documentazione relativa alle attività effettuate e ad eventuali problemi / discordanze rispetto a quanto programmato. Questa fase è particolarmente importante perché dovrà evidenziare miglioramenti tecnici ed organizzativi che, in condizione di normalità, dovranno essere messe in campo per migliore/prevenire la gestione dell'emergenza.

Il "Gruppo di lavoro per la continuità operativa ICT", immediatamente convocato dai soggetti individuati nell'"Allegato C - Composizione del Gruppo di lavoro per la continuità operativa ICT", a seguito delle segnalazioni pervenute, effettua una valutazione dell'evento avvalendosi, nel caso, di altre professionalità necessarie per la corretta analisi della situazione.

In questa fase è importante analizzare ciascun evento, esaminarne la criticità e stimarne la gravità.

Nel corso del processo di valutazione il Gruppo potrà essere coadiuvato dal personale dei SGT, o da tutti coloro che il Gruppo riterrà necessario coinvolgere a seconda della tipologia di incidente, incluso responsabili per la privacy.

Oltre al personale interno, il "Gruppo di lavoro per la continuità operativa ICT" dovrà individuare i fornitori e/o agli altri soggetti esterni che si ritiene opportuno allertare.

Il "Gruppo di lavoro per la continuità operativa ICT" coinvolgerà altresì i Coordinatori del trattamento

dei dati interessati nell'incidente di sicurezza per valutare, in relazione alla gravità dell'incidente stesso, le modalità di comunicazioni interne ed esterne. A seconda del livello di gravità il Gruppo di lavoro attiverà i vertici istituzionali nella figura del Sindaco e del Direttore Generale i quali valuteranno le conseguenti misure organizzative da adottare.

Per la definizione della gravità dell'incidente si fa riferimento alla tabella seguente:

Gravità incidente di sicurezza	***Descrizione***
Alta	Il grado di compromissione di servizi e/o sistemi è elevato. Si rilevano danni consistenti sugli asset. Il tempo di ripristino stimato è superiore alla giornata. Il grado di indisponibilità di servizi e/o sistemi è totale o molto rilevante. Interruzione dell'attività lavorativa della maggioranza dei servizi dell'Ente. Forte impatto sulla cittadinanza e/o sulle funzioni istituzionali. Per il ripristino delle normali condizioni operative NON sono sufficienti gli asset presenti nel DC Primario ma è necessario ricorrere al DC secondario in Lepida e al supporto di fornitori esterni.
Media	L'incidente non presenta nessuna condizione che porti alla catalogazione "gravità alta". Il grado di indisponibilità di servizi e/o sistemi è di una certa rilevanza e possono essere rilevati danni sugli asset di una certa consistenza. Generalmente si verifica quando sono indisponibili servizi di infrastruttura o trasversali: ad esempio data base, sistema di posta, Dominio Active Directory. Il ripristino ha tempi stimati di qualche ora, ma inferiori alla giornata. Interruzione dell'attività lavorativa di più di un servizio dell'Ente. Medio impatto sulla cittadinanza e/o sulle funzioni istituzionali. Per il ripristino delle normali condizioni operative sono sufficienti gli asset presenti nel DC Primario, ma è necessario ricorrere al supporto sistemistico di fornitori esterni oltre alle competenze del personale del SGT.
Bassa	L'incidente non presenta nessuna condizione che porti alla catalogazione "gravità alta o media". Viene reso indisponibile un singolo servizio/sistema. Interruzione dell'attività lavorativa di un numero ristretto di dipendenti e per un breve periodo di tempo. Scarso impatto sulla cittadinanza e/o sulle funzioni istituzionali dell'Ente. Per il ripristino delle normali condizioni operative sono sufficienti gli asset presenti nel DC Primario e le competenze sistemistiche del personale del SGT. Potrebbe essere necessario il supporto della software house che ha installato il layer applicativo sul server.

5. Modalità operative per la gestione dell'emergenza

Le misure tecniche descritte nella sezione 1 sono state progettate per ridurre il rischio del verificarsi di incidenti di gravità medio/bassa o per ridurre i tempi di rientro nella condizione operativa di normalità.

Nella tabella seguente sono riportate le misure più rilevanti ai fini della prevenzione e del contenimento dei tempi di risoluzione.

Infrastrutture di continuità e protezione fisica: alimentazione ridondata dei sistemi, sistemi antincendio, UPS.	Par. 1.2
Collegamento di tutte le sedi in FO e con doppio percorso. Presenza di due punti di accentramento delle FO (POP) con possiblità di trasferire la connettività verso internet e verso il DC secondario nel secondo POP in caso di indisponibilità di quello all'interno del DC primario.	Par. 1.4
Collegamento ridondato in FO ad alta velocità con il DC Secondario. Collegamenti logici tra le due reti già configurati in modo da semplificare l'attivazione del sito DC secondario.	Par. 1.4
Assenza di Single Point of Failure nell'infrastruttura fisica di storage e server utilizzata per i sistemi che erogano i servizi (ridondanza di tutte le componenti, link, ecc.).	Par. 1.5
Presenza di contratti di assistenza con SLA per tutte le componenti critiche e, nel caso dello storage, azioni proattive in cui il fornitore viene allertato al fault del singolo componente.	Par. 1.4-1.5
Utilizzo di sistemi di virtualizzazione (VMWARE) che rendono irrilevante l'indisponibilità del nodo fisico, semplificano il ripristino del sistema virtuale in caso di fault o l'attivazione sul DC Secondario.	Par. 1.6
Politiche di accentramento dei servizi applicativi a parità di requisiti tecnici (middleware, db richiesti) che consentono di ottimizzare i processi di ripristino.	Par. 1.6
Configurazione in alta disponibilità dei sistemi critici (es: application server utilizzati dai servizi demografici, protocollo, atti ecc.) e dei repository in cui questi memorizzano i dati (es: Oracle RAC).	Par. 1.6
Presenza di sistemi di monitoraggio interni che rilevano criticità sia di elementi base (es: raggiungimento soglie di riempimento o di livelli di prestazioni definiti critici) che indisponibilità di interi servizi consentendo interventi proattivi.	Par. 1.6 Par. 1.2
Censimento continuativo degli asset con evidenza dei legami tra servizi erogati e sistemi IT necessari al funzionamento.	Par. 1.9

Politiche backup : sistema centralizzato di gestione, moduli specifici per DB per garantire coerenza dei dati, ambiente virtuale per ottimizzare i tempi di ripristino, backup su sistemi disco (DataDomain) per velocizzare restore, periodi di retention lunghi, notifica automatica di anomalie nei processi di salvataggio.	Par. 1.8
Strumenti nativi dello storage o del Datadomain (snapshot, Mtree) o moduli aggiuntivi (suite Zextras) che semplificano le politiche di back-up e il metodo di restore.	Par.1.8
Replica dei back-up nel sito di DC secondario tramite collegamento in FO sempre attivo.	Par. 1.8.1
Appartenenza alla Comunity Network Emilia Romagna, adozione di convenzioni / contratti con Lepida SPA per servizi di Disaster Recovery, utilizzo di server virtuali e storage all'interno dei DC di Lepida.	Sez. 2

Le linee guida di AGID per il Disaster Recover per le PPAA (par. 4.2.3) stabilivano le soluzioni tecnologiche (Tier) da applicare; la soluzione Tecnologica determina di conseguenza il RPO e il RTO.

Nell'"Allegato D - Definizione Tier" sono riportate le soluzioni tecnologiche (Tiers) previste da AgID.

Inoltre nelle stesse linee guida (par.2.7.2) viene data come indicazione "...l'utilizzo del Tier3 per medi comuni con collegamento fra le sedi del sito primario e secondario tramite collegamento privato e riservato al dialogo tra la PA e il DC e con vincoli di RPO pari al massimo a 1 giorno e RTO da 1g. a 3 gg.".

Le misure tecnologiche adottate e descritte precedentemente rientrano nella soluzione Tecnologica Tier 3, descritta sotto e consigliata da AgID, che l'Ente quindi è in grado di applicare per tutti i servizi elencati nella sezione 2 (inclusi quelli classificati come di rischio Basso).

	Rto min/Max	**RPO max**	***Modalità minime di copia/aggiornamento per il conseguimento dei valori max di RPO***	***Aspetti minimali connessi al sito di DR***
Tier 3	1g /3g	Max 1 gg	Electronic vaulting: soluzione che comporta il backup dei dati presso il sito alternativo in maniera elettronica, con una riduzione del tempo necessario per il trasporto dei dati e la possibilità di un recovery time più veloce.	Il sito dispone di hardware e connettività già funzionante ma su scala inferiore rispetto al sito principale o ad un site alternativo sempre disponibile e con replica costante dei dati. Il backup avviene in modalità elettronica e quindi sono necessari collegamenti fra i siti tenuto conto della tipologia, quantità e periodicità dei dati da backuppare.

Inoltre, a dimostrazione dell'efficienza delle misure di continuità messe in atto sono riportati di seguito:

- Tempo di Uptime del DC primario: 99,99999. Negli ultimi 5 anni non si è mai verificato un

evento di criticità alta che abbia compromesso tutti servizi erogati dal sistema informativo.

- Negli ultimi 5 anni si sono verificati SOLO 2 eventi di gravità media che hanno provocato l'indisponibilità di alcuni servizi in un caso per qualche decina di minuti e nell'altro per meno di 3 ore.

5.1 Modalità operative per incidenti di Bassa gravità

Di seguito vengono illustrate le procedure operative per il ripristino di singoli servizi nelle principali casistiche che potrebbero verificarsi. Tramite il censimento delle applicazioni (vedi par.1.9) è possibile sapere quali sono i componenti tecnologici coinvolti nell'erogazione di un servizio applicativo e quindi, a seconda del problema, decidere cosa si deve ripristinare (server, data base, porzione del file system, ecc.).

5.1.1 Ripristino di server

RESTORE DI SERVER VIRTUALE

La maggioranza dei server che eroga i servizi applicativi o di infrastruttura necessari al funzionamento del sistema informativo sono server virtuali su piattaforma Vmware, con dischi "dependent". Malfunzionamenti hardware non danno quindi nessun disservizio perchè le funzionalità di Vmware (vmotion, high availability) provocano lo spostamento del server logico su un altro server fisico senza alcuna perdita di funzionalità.
Questa configurazione permette inoltre di usare gli strumenti nativi di Vmware, insieme al sistema di back-up, per ripristinare agevolmente un server seguendo i passi sotto:

- collegarsi alla console software di gestione del backup;
- selezionare il server che si deve ripristinare;
- selezionare il save set con la data di ripristino;
- effettuare il restore della virtual machine sul cluster VMWARE esistente.

RESTORE DI SERVER FISICO

Qualora il server sia fisico o abbia dischi "persistent indipendent" o debba utilizzare agenti specifici per la piattaforma logica da copiare (es: agent Domino, Agent Oracle) i passi da effettuare sono i seguenti:

- se si tratta di un server fisico e l'RTO lo consente si attiveranno i contratti di assistenza Hardware stipulati direttamente con HP che prevedono l'intervento entro 24 ore;
- in caso negativo si potrà effettuare un ripristino su un server virtuale creato ex- novo con caratteristiche sufficienti a reggere il carico per il periodo di tempo necessario a ripristinare la condizione di normalità;
- installare il nuovo server fisico o virtuale dal template con lo stesso sistema Operativo e versioni di patching di quello da ripristinare;

- installare il client del software di back-up legato Networker, nella stessa versione di quello in uso, per poterlo vedere come destinazione del percorso di restore;
- installare eventuali agenti specifici della piattaforma da ripristinare, se necessari;
- effettuare il restore dei dati su questa nuova macchina.

In caso di server fisico ripristinato sul virtuale si dovrà pianificare l'attività di rientro nella condizione di normalità una volta che il server fisico sarà nuovamente operativo.

5.1.2 Ripristino di Data base singoli

In caso di indisponibilità di un servizio applicativo la causa potrebbe essere legata o a uno o più server applicativi coinvolti o alla base dati del singolo applicativo. Nel caso il cui il problema sia riconducibile al server applicativo che non contiene la base dati che risulta integra si procederà come indicato al par 5.1.1.

Qualora invece l'indisponibilità fosse legata al DB della singola applicazione:

per Oracle Database: tale restore avverrà con il comando IMPDP, partendo dall'EXPDP effettuato nella prima finestra temporale utile al restore;

per MS SQL Server: tale restore avverrà con il comando Restore Database, partendo dal backup effettuato nella prima finestra temporale utile al restore.

In caso di indisponibilità dell'intero server data base (oracle o Ms-sql) fare riferimento alle casistiche del par. 5.2.

5.1.3 Ripristino di parti del NAS

Un evento di bassa criticità che potrebbe verificarsi è la perdita di cartelle sul NAS su cui insistono tutti di dischi di rete utilizzati dagli uffici dell'Ente per la memorizzazione dei documenti. Le indicazioni sotto riportate possono essere utilizzate per il caso descritto ma anche genericamente per ripristinare altri parti del NAS incluse quelle eventualmente necessarie per l'erogazione di servizi applicativi.

RIPRISTINO DEI DOCUMENTI DI UN SERVIZIO

In caso di perdita di tutti i documenti di un servizio memorizzati sui dischi di rete si possono utilizzare le funzionalità di snapshot attivate sul NAS DELL EMC Unity 300 per ripristinare velocemente il file system e i diritti di accesso.

Fare riferimento al par. 1.8 per la frequenza con cui vengono fatte gli snapshot e per il lasso temporale in cui sono mantenuti.

Le operazioni da fare in questo caso sono:

- accedere ad una qualsiasi postazione di lavoro con credenziali di Amministratore di sistema o Amministratore di PDL;
- posizionarsi sul livello più alto dell'albero di directory che si vuole ripristinare;
- Proprietà → versioni Precedenti;
- Selezionare lo snapshot che si vuole ripristinare: Copia e incolla di tutte le directory.

In caso di grosse moli di documenti conviene fare l'operazione da un server windows con credenziali opportune.

5.1.4 Ripristino di una casella di posta Zimbra

Il sistema di posta ha tra le funzionalità la possibilità di tenere un log delle variazioni della singola casella come descritto al par. 1.8. Questo permette quindi di ripristinare il singolo elemento (Messaggio, contatto, appuntamento ecc.) qualora sia stato cancellato.

Inoltre tramite il modulo aggiuntivo (suite Zextras) è possibile ripristinare l'intera casella qualora sia corrotta o cancellata.

In caso di indisponibilità di tutto il sistema di posta queste funzionalità non saranno disponibili e si dovranno applicare i passi descritti in par. 5.2.4.

5.2 Modalità operative per incidenti di Media gravità

Rientrano in questa categoria incidenti di componenti strategiche per il funzionamento del sistema informativo dell'Ente. Considerata la criticità, ciascun servizio è generalmente erogato da più di un server (vedi par. 1.6) o in caso di sistemi hw (NAS, switch di core) da apparati completamente ridondati e senza Single-Point-Of-Failure (vedi Unity 300 o Extreme Networks Black Diamond 8900 – par. 1.4-1.5).

Per i sistemi software quindi il rischio di indisponibilità è causato alla corruzione logica dell'infrastruttura più che all'indisponibilità del singolo nodo.

Descriviamo sotto i principali passi/contratti per gestire l'indisponibilità di uno di questi servizi:

5.2.1 Ripristino del Dominio Microsoft Active Directory

Active Directory è il repository di tutti le credenziali e sistemi all'interno della sistema informativo. Include servizi DNS, DHCP, DFS integrati.

Tra le funzionalità configurate sui Domain Controller c'e' il "cestino" - Recycle Bin che consente di ripristinare oggetti o parti dell'albero di AD erroneamente cancellati. La stessa cosa si può fare dal back-up del server (ripristinando solo l'oggetto di AD e non l'intero server), visto che e' stato attivato l'agente di legato Networker specifico per Active Directory.

Il servizio è erogato da due server (Domain Controller) e quindi, in caso di fault di uno, non si verificano disservizi.

Qualora uno dei due Domain Controller non funzioni, il modo più veloce per ripristinare la condizione di normalità, sfrutta la funzionalità di replica di Active Directory, visto che è ancora funzionante un sistema con tutte le informazioni corrette. I passi da fare sono i seguenti:

- rimozione dal domain controller ancora funzionante dei riferimenti a quello in fault;
- re-installazione di un server virtuale Windows con stessa release e livello di patching del domain controller funzionante;
- elevazione del nuovo server a Domain controller;
- replica del DNS;
- attivazione del servizio DHCP e restore dalla copia della configurazione dal back-up del server in fault;

- rimozione e ripristino del failover del DHCP;
- replica del DFS.

In caso di failure dell'interno dominio (per indisponibilità di entrambi i domain controller o per corruzione del repository) si dovrà:

- ripristinare il primo Domain controller dal back-up come indicato al par. 5.1.1 – restore di un server virtuale;
- eseguire tutte le operazioni indicate al punto sopra.

Vista la criticità di Active Directory per il funzionamento della rete, l'Ente ha attivato un contratto (IAS) con la ditta Progel – partner Microsoft certificato di livello GOLD sulle competenze DATACENTER per assistenza sistemistica su server Microsoft critici tra cui i domain controller, con tempo di risposta per eventi classificata ad alta priorità di 4 ore.

Quindi le fase sopra descritte verranno effettuate sotto la loro supervisione per garantire il ripristino in tempi bervi.

5.2.2 Ripristino del DataBase Oracle

E' il database utilizzato dalla maggior parte dei servizi applicativi per la memorizzazione dei dati.
Anche in questo caso il servizio è erogato da due server in cluster e quindi in caso di fault di uno non si verificano disservizi ma si provvederà al ripristino come nel caso di incidente a bassa gravità.

Lo scenario descritto di seguito indica i passi in caso di ripristini dell'intera infrastruttura. Ovviamente potrà essere applicato parzialmente qualora i server fisici che costituiscono i nodi del cluster siano ancora disponibili/funzionanti.

I passi da fare sono i seguenti:

- ripristinare il primo server del cluster come descritto in par. 5.1.1 RESTORE SERVER FISICO verificare che:
  - sia installato il software per il Grid Oracle, necessario per ASM nella stessa versione di quello in uso, possibilmente con lo stesso patching.
  - sia installato il software per il Database Oracle nella stessa versione di quello in uso, possibilmente con lo stesso patching.
  - siano agganciate al server le 3 LUN con dimensioni simili alle esistenti.
  - siano disponibili i diskgroup su ASM, con stessi nomi esistenti (DATA, FRA, OCR_VOTE).
  - sia presente l'istanza database con stesso sid (EDI,UGO,DWH). In caso contrario crearla utilizzando i template con tablespace già pronti.
- configurare RMAN Impostando i settaggi di default di RMAN come quelli in uso.
- restore controlfile da RMAN:
  - avviare il database senza montarlo (NOMOUNT) con pfile esterno.
  - eseguire il restore dei controlfile con SETID del database in uso.
  - montare il database (MOUNT).
- Restore e recover del database da RMAN:
  - Eseguire restore e recover con rman.
  - Chiudere il database con parametro IMMEDIATE.
- Resetlogs.
  - Modificare il pfile con i controlfile corretti.
  - Montare il database con il pfile appena sistemato.

- Aprire il database con l'opzione RESETLOGS.
- Creare spfile su +DATA dal pfile appena modificato.
- Chiudere il database con parametro IMMEDIATE.
- Montare il database con SPFILE.
- Valutare se metterlo in modalità NOARCHIVELOG.
- Chiudere il database con parametro IMMEDIATE.
- Aprire il database con i comandi del grid (SRVCTL).

L'Ente ha attivato un contratto di manutenzione con Lepida che oltre a permettere di avere gli aggiornamenti / patch delle licenze consente di aprire Service Request al supporto di Oracle. In situazioni come quella descritta il livello di priorità attribuito sarebbe di Severity Level 1 (CRITICO) e quindi l'intervento avverrebbe entro 1 ora.

5.2.3 Ripristino del DataBase Ms-SQL Server

L'istanza MS-SQL Server risiede su un server virtuale con dischi independent, copiati con le funzionalità di Vmware. Per il ripristino si dovranno seguire le istruzioni al per. 5.1.1 - RESTORE DI SERVER VIRTUALE.

In caso di inconsistenza dei dati verranno eseguiti i restore dei database e dei relativi log transazionali salvati periodicamente su Data Domain.

L'Ente ha attivato un contratto (IAS) con la ditta Progel – partner Microsoft certificato di livello GOLD sulle competenze DATACENTER per assistenza sistemistica su server Microsoft critici con tempo di risposta per eventi classificata ad alta priorità di 4 ore.

5.2.4 Ripristino del Sistema di posta ZIMBRA

Il sistema di posta Zimbra è costituito da due server:
DEB-ZMAIL che contiene le caselle di posta vere e proprie e permette l'accesso dalle postazioni interne alla rete dell'Ente.
DEB-ZPROXY con non ha dati ma rende accessibile l'ambiente di posta da internet.

Entrambi i server sono virtuali con dischi dependent e quindi sono copiati con le funzionalità di Vmware senza la necessità di nessun agente. Come indicato al par 1.8 la suite Zextras garantisce la congruenza dell'ambiente gestendo i log delle modifiche su un disco dependent dedicato, agganciato alla macchiana virtuale.

Per il ripristino si dovranno seguire le istruzioni al per. 5.1.1 - RESTORE DI SERVER VIRTUALE per entrambi i sistemi.
Per quanto riguarda DEB-ZMAIL, i messaggi di posta più vecchi di 30 giorni vengono spostati autotmaticamente su una "estesnsione logica" della casella di posta memorizzata su una LUN che si trova sullo storage nel DC secondario. Il sistema funziona anche senza questa LUN; semplicemente l'utente non riesce ad accedere alle mail dei masi precedente. Per ripristinare completamente il servizio sarà quindi necessario ricollegare al server virtuale il disco remoto.

Anche in questo caso sono attivi contratti con la ditta STUDIO STORTI, distributore italiano della soluzione ZIMBRA + ZEXTRAS che interviene con SLA di 4 ore.

5.2.5 Ripristino del Firewall Checkpoint

Il firewall Checkpoint è il sistema perimetrale che consente l'accesso ad internet e governa il dialogo tra la varie zone logiche della rete dell'Ente (Server, DMZ, Client, ecc.): è composto da due server fisici in cluster ciascuno con un sistema Operativo dedicato.
I due nodi sono gestiti da una console di management costituita da un'appliance vertuale anch'essa con un prorpio sistema operativo di cui viene fatto il back-up con gli strumento di Vmware/legato Networker.
Anche in questo caso la console di managment (SRV-DORY) non è critica perché non è indispensabile al funzionamento del firewall ma solo per la modifica delle policies.
Il servizio di firewalling vero e proprio è erogato dai due nodi fisici: quindi in caso di crash di uno dei due nodi non si verificano disservizi.
La console gestisce lo storico della configurazione quindi in caso di problemi è possibile ripristinare la versione precedente dalla console stessa.
Qualora la configurazione sia corrotta e non sia possibile l'operazione di cui sopra è possibile ripristinare quella copiata sul server FTP (SRV-NEMO) su cui viene copiata anche la configurazione dei due nodi Hansel e Gretel oppure ripristinare l'intera appliance con le operazione viste nel par. 5.1.1.

Qualora sia necessario installare tutto il sistema (entrambi i nodi - Hansel e Gretel + management) o per supporto nelle operazioni descritte sopra, l'Ente ha un contratto di assistenza attivo con la ditta VEM SISTEMI, partner certificato Checkpoint di livello massimo (4 *) che prevede per interventi critici SLA da 1 a 4 ore. L'Ente ha inoltre attivo un contratto di manutenzione hardware/software con il produttore descritto al par. 1.7.
Anche i server HP su cui è installato il sw del firewall, sono coperti da contratto di manutenzione hardware come descritto al par. 1.5.

5.2.6 Ripristino dello switch di core

Tutti i server fisici/virtuali sono connessi allo switch di core Extreme Networks Black Diamond 8900 su cui convergono anche i collegamenti del firewall, del POP secondario e delle sedi perifiche.

Si tratta quindi di un apparato vitale per l'erogazione dei servizi dell'Ente. Per questa ragione in fase di progetto è stato scelto un apparato con le seguenti caratteristiche:

- di fascia enterprise e con alte prestazioni;
- completamente modulare: composto da uno chassis senza nessun componente attivo e da più schede per le varie tipologie di collegamenti;
- completamente ridondato: N alimentatori, doppia management, schede ridondate per i collegamenti critici.

Questo ha fatto si, che dal momento della sua installazione non si siano mai verificati fault tali da provocare disservizi a tutta la rete dell'Ente.

Lo switch di core e tutti gli altri apparati di rete sono gestiti tramite l'appliance virtuale Netsight di Extreme Networks che consente anche di effettuare back-up settimanali della configurazione di tutti gli apparati di rete, con retention di 6 mesi.
L'appliance di gestione non è un punto di criticità per l'erogazione dei servizi, ma consente, in caso di malfunzionamenti dello switch di core legati alla configurazione, di ripristinarne rapidamente una funzionante.
Inoltre, come indicato nel par. 1.4 sono attivi contratti di manutenzione hardware con tempi stringenti.

5.3 Modalità operative per incidenti di Alta gravità

Gli scenari di questo tipo prevedono la ripartenza dei servizi almeno quelli più critici, con sistemi del DC di Lepida che è il DC secondario per l'Ente.

Come già descritto in precedenza l'Ente ha già:

- collegamenti banda ultra larga privata e dedicata sempre attivi con il DC secondario;
- una replica di tutti i propri dati (Virtual machine, NAS, DB, ecc.) su un dispositivo di archiviazione analogo a quello del DC Primario (DELL EMC DATADOMAIN);
- parte di dati (Archivio, parte delle caselle email) memorizzati sullo storage nel DC secondario tramite il servizio IaaS di Lepida Storage as a Service;
- contratti con Lepida Scpa, di cui il Comune di Reggio Emilia è socio, per servizi di Data Center (vedi sez. 2). Questi contratti prevedono la possibilità di aumentare in modo semplice la quantità / tipo dei servizi in DC erogati all'Ente.

I passi principali da effettuare sono:

- Richiedere a Lepida SPA l'attivazione di:
  1. una VM nel DC secondario sulla stessa rete in cui si trova il DATADOMAIN con lo stesso sistema operativo del server di back-up;
  2. una infrastruttura fisica "Blade as A Service" costituita da 4 nodi su cui attivare la piattaforma di virtualizzazione Vmware;
  3. il servizio di storage As a Service con:
     - 4 TB di tipo Storage Extreme Performance per i server DB;
     - 30 TB di tipo Storage Base per i server virtuali;
     - 30 TB di tipo Storage Archiviazione per il NAS:
  4. il servizio "Firewall as A service" per attivare le regole di dialogo tra la rete dei server e quella dei client. In caso di indisponibilità del Firewall dell'Ente dovranno essere attivate anche le regole per l'accesso degli utenti / server da verso internet.
- Installare sulla VM di cui al punto 1), il client di Legato Networker per accedere ai back-up delle VM archiviate sul DataDomain del DC secondario;
- Recuperare dal Beack-up del NAS relativo alla documentazione del SGT eventuali file con informazioni/istruzioni necessarie ai punti successivi;
- Reinstallare Vmware sui nodi di cui al punto 2);
- Ripristinare i servizi di infrastruttura indispensabili al funzionamento della rete: DNS, DHCP, DFS, AD. Fare riferimento al par.5.2.1;
- Ricreare i file system DATI, SERVIZI e UTENTI per il NAS e le LUN per oracle e i server virtuali sullo storage di cui al punto 3);
- Ripristinare i servizi di DataBase Oracle. Fare riferimento al par.5.2.2;
- Ripristinare i servizi di DataBase MS-DQL. Fare riferimento al par.5.2.3;
- Ripristinare i servizi di Posta Zimbra. Fare riferimento al par.5.2.4;
- Ripristinare i server che erogano servizi applicativi in base all'ordine di criticità indicata nella sez. 2. Fare riferimento al par.5.1.1;
- Ripristinare i documenti sui dischi di rete dei vari uffici utilizzando il client di legato networker e la copia degli stessi fatta sul DATADOMAIN nel DC secondario;

Per tutti i ripristini dovrà essere utilizzata al copia sul DATADOMAIN nel DC secondario e non il back-up nel DC Primario come invece era previsto negli scenari di bassa/media gravità.

6. Allegati

Allegato A - Misure di sicurezza per i servizi di datacenter Lepida Scpa

COMUNE DI
REGGIO EMILIA

Versione: 1.1
Data: 11-7-2019

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.

Allegato B - Elenco Servizi

Piano di continuità operativa dei sistemi ICT

ALLEGATO B

Elenco Servizi

Comune di Reggio Emilia

COMUNE DI
REGGIO EMILIA

Servizio(TabellaAgid)	Nome	Descrizione	Classe Criticità	Tipologia di utenza	RPO	RTO
Servizi on line cittadini	Servizi Online	Servizi on line per i cittadini: iscrizione nidi o alle scuole dell'infanzia, portale del cittadino, gestione prestiti bibliotecari ecc.	Media	Esterna	4h	1g
Albo pretorio	Albo pretorio	Pubblicazione atti e affissioni ai fini di trasparenza amministrativa	Alta	Eterogenea	3h	1g
Gestione atti amministrativi (determine, delibere)	JEnte Atti e Segreteria	Gestione e consultazione atti e iter documentale, Segreteria e relative pubblicazioni	Media	Eterogenea	3h	1g
Gestione atti amministrativi (determine, delibere)	JEnte Protocollo	Gestione Affari Generali Protocollo	Media	Utenti interni	3h	1g
Gestione atti amministrativi (determine, delibere)	Retain	Gestione invio al sistema di conservazione ParER	Media	Utenti interni	24 h	2g
Gestione SUAP	Pubblicità e Affissioni	Gestione della pubblicità e affissioni (ICP)	Media	Utenti interni	3h	1g
Biblioteche	Sebina POLO-BSRE	Gestione prestito libri SBN Biblioteche Specialistiche di Reggio Emilia	Media	Eterogenea	24 h	2g
Biblioteche	Zetesis Biblioteche	Gestione prestito libri biblioteca Panizzi	Media	Utenti interni	4h	1g
Gestione Economato (inventario, buoni economali)	JEnte Finanziaria	Gestione contabilità finanziaria (fatturazione, mutui, investimenti etc.) ed economica	Media	Utenti interni	3h	1g
Gestione Bilancio	JEnte Pianificazione e Controllo Obiettivi	Controllo di Gestione e Obiettivi (PEG)	Media	Utenti interni	3h	1g
Gestione Servizi Sociali	Ufficio Casa	Gestione dati Erp, fondo affitto, morosità e alloggi	Media	Utenti interni	3h	1g
Servizi Demografici (anagrafe, CIE, stato civile, elettorale)	JEnte Demografici	Gestione dei servizi demografici: anagrafe, elettorale e stato civile, certificati anagrafici on-line	Alta	Eterogenea	3h	1g
Servizi Demografici (anagrafe, CIE, stato civile, elettorale)	Polizia Mortuaria	Gestione cimiteriale ufficio Polizia Mortuaria e portale per imprese	Media	Eterogenea	3h	1g
Gestione Edilizia	Compravendite	Gestione dati Compravendite e Varianti al PSC/RUE delle Aree Fabbricabili	Bassa	Utenti interni	3h	1g
Gestione Edilizia	Edilizia Oracle	Gestione pratiche edilizie, permessi di costruire, dia, varianti, subentri, abusi, ecc. e portale di consultazione per esterni	Media	Eterogenea	3h	1g
Gestione SIT (cartografia, civici e toponomastica)	GEO-SERVER	Gestione cartografia	Media	Eterogenea	3h	1g
Gestione SIT (cartografia, civici e toponomastica)	ACI-VESTA	Gestione toponomastica (vie, civici e archi stradali) e di tutti gli atti che comportano variazioni di tali oggetti.	Media	Utenti interni	3h	1g

COMUNE DI
REGGIO EMILIA

Servizio(TabellaAgid)	Nome	Descrizione	Classe Criticità	Tipologia di utenza	RPO	RTO
Manutenzione e Lavori Pubblici	Cityworks	Gestione concessioni e ordinanze relativamente agli interventi stradali per nuove infrastrutture o manutenzione infrastrutture esistenti	Bassa	Eterogenea	3h	1g
Manutenzione e Lavori Pubblici	Segnalazioni	Gestione segnalazioni e chiamate manutenzione	Media	Eterogenea	3h	1g
Manutenzione e Lavori Pubblici	STR PBM Linea Amministrativa	Gestione Amministrativa Lavori Pubblici e relativi adempimenti	Media	Eterogenea	3h	1g
Gestione Patrimonio	Babylon Patrimonio	Gestione patrimonio beni mobili ed immobili	Bassa	Utenti interni	3h	1g
Gestione Patrimonio	Locazioni	Gestionale per gli affitti attivi e passivi dell'Ente	Bassa	Utenti interni	3h	1g
Gestione Patrimonio	Utenze	Gestione utenze elettriche, gas e telefonia	Bassa	Utenti interni	3h	1g
Gestione Stipendi	Gestione Personale	Gestione Integrata del Personale (giuridica ed economica)	Media	Utenti interni	3h	1g
Gestione Personale (giuridico, presenze)	Gestione Presenze	Procedura rilevazione presenze e gestione timbrature	Media	Utenti interni	3h	1g
Gestione SUAP	P.M. - Controlli Violazioni Amministrative	Gestione delle sanzioni amministrative del commercio	Media	Utenti interni	3h	1g
Gestione Sanzioni, Incidenti, Turni di servizio	PIEMMEGU - CDS	Gestione verbali codice della strada	Media	Utenti interni	3h	1g
Gestione Sanzioni, Incidenti, Turni di servizio	Verbatel Polizia Municipale	Gestione Centrale Operativa, infortunistica,polizia giudiziaria, rimozioni-sequestri,rapporti,restituzione veicoli,TSO,agenda e gestione utenti	Alta	Utenti interni	4h	1g
Scuole	Materne	Gestione fatturazione scuole dell'infanzia, nidi e primarie con refezione	Media	Utenti interni	3h	1g
Scuole	Scuole e Nidi	Gestione iscrizioni alle scuole e nidi d'infanzia per il servizio annuale ed estivo con assegnazioni punteggi, graduatorie, formazioni sezioni	Media	Utenti interni	3h	1g
Gestione Servizi Sociali	Garsia e GEAC	Gestionale dei Servizi Sociali del Distretto di Reggio Emilia, Assegni di cura anziani e disabili	Media	Eterogenea	3h	1g
Gestione sito web e posta	Posta	Sistema di gestione posta elettronica Zimbra	Media	Utenti interni	0,5h	1g
Gestione sito web e posta	Sito web	CMS per gestione sito web istituzionale e sottositi	Media	Eterogenea	24h	2g

COMUNE DI
REGGIO NELL'EMILIA

Allegato C

Composizione del Gruppo di lavoro per la continuità operativa ICT

SOGGETTO	RUOLO NEL GRUPPO	NOME E COGNOME	RECAPITI
DIRIGENTE SERVIZIO GESTIONE E SVILUPPO DELLE TECNOLOGIE E DEI SISTEMI INFORMATIVI	RESPONSABILE SICUREZZA INFORMATICA	LORENZA BENEDETTI	lorenza.benedetti@comune.re.it
RESPONSABILE TRANSIZIONE DIGITALE (Art. 17 D.Lgs 82/2005)	RESPONSABILE TRANSIZIONE DIGITALE	LORENZA BENEDETTI	lorenza.benedetti@comune.re.it
UOC UFFICIO PRIVACY	REFERENTE NORMATIVO e ORGANIZZATIVO GESTIONE INCIDENTI	STEFANIA SABATTINI	privacy@comune.re.it
UOC GESTIONE DELLE STRUTTURE TECNOLOGICHE	REFERENTE TECNICO SICUREZZA INFRASTRUTTURE	PATRIZIA BONDAVALLI	patrizia.bondavalli@comune.re.it
UOC GESTIONE DEI SISTEMI INFORMATIVI	REFERENTE TECNICO SICUREZZA APPLICAZIONI	BARBARA LEONI	barbara.leoni@comune.re.it

Allegato D - Definizione Tier

Piano di continuità operativa dei sistemi ICT

ALLEGATO D
Definizione di Tier
Comune di Reggio Emilia

COMUNE DI
REGGIO EMILIA

Definizione delle soluzioni tecnologiche (Tier) in base alle LINEE GUIDA PER IL DISASTER RECOVERY DELLE PUBBLICHE AMMINISTRAZIONI

par. 4.2.3 - Le Tipologie di soluzioni tecniche

Le tipologie di soluzioni tecniche elencate qui di seguito sono definite in senso generale con riguardo alle funzionalità richieste e/o da assicurare e come tali non fanno riferimento a specifiche tecnologie e/o prodotti o soluzioni di mercato.

Tier 1: è la soluzione minimale coerente con quanto previsto dall'articolo 50-bis. Prevede il backup dei dati presso un altro sito tramite trasporto di supporto (nastro o altro dispositivo). I dati sono conservati presso il sito remoto. In tale sito deve essere prevista la disponibilità, in caso di emergenza, sia dello storage disco dove riversare i dati conservati, sia di un sistema elaborativo in grado di permettere il ripristino delle funzionalità IT. Nel caso di affidamento del servizio di custodia ad un fornitore, tale disponibilità deve essere regolamentata contrattualmente.
Per questa soluzione:
— potrebbero non essere presenti procedure di verifica della presenza dei dati sul supporto, della coerenza dei dati ed esistere un'unica copia storage;
— la disponibilità dei dispositivi (storage disco e sistemi di elaborazione) potrebbe prevedere tempi non brevi (anche più settimane per l'assegnazione da parte del fornitore);
— la disponibilità dei dispositivi potrebbe non garantire le performance rispetto al sistema primario;
— la disponibilità dei dispositivi potrebbe essere assegnata per un periodo di tempo limitato.

Poiché i dati salvati possono essere relativi all'intera immagine dello storage primario o solo ai dati delle elaborazioni, la disponibilità dei dispositivi ausiliari deve essere chiaramente definita in termini di ambiente hardware e software di riferimento.
Vengono quindi assicurate l'esecuzione e conservazione dei backup e, per i casi in cui si renda necessario assicurare il ripristino, la disponibilità di un sito "vuoto" attrezzato, pronto a ricevere le componenti e configurazioni necessarie, ove fosse richiesto, per far fronte all'emergenza (*on demand*).

Tier 2: la soluzione è simile a quella del Tier 1, con la differenza che le risorse elaborative possono essere disponibili in tempi sensibilmente più brevi, viene garantito anche l'allineamento delle performance rispetto ai sistemi primari ed esiste la possibilità di prorogare, per un tempo limitato, la disponibilità delle risorse elaborative oltre il massimo periodo di base.
Vengono assicurate l'esecuzione e conservazione dei backup e la disponibilità presso il sito dei sistemi e delle configurazioni da poter utilizzare per i casi in cui si renda necessario il ripristino.

Tier 3: la soluzione è simile a quella del Tier 2, con la differenza che il trasferimento dei dati dal sito primario e quello di DR avviene attraverso un collegamento di rete tra i due siti. Questa soluzione, che può prevedere tempi di ripristino più veloci rispetto ai Tier precedenti, rende necessario dotarsi di collegamenti di rete con adeguati parametri di disponibilità, velocità di trasferimento e sicurezza (sia della linea, sia delle caratteristiche dipendenti dalla quantità di dati da trasportare).Va periodicamente verificato l'allineamento dei dati.

Tier 4: la soluzione prevede che le risorse elaborative, garantite coerenti con quelle del centro primario, siano sempre disponibili, permettendo la ripartenza delle funzionalità in tempi rapidi. Le altre caratteristiche sono quelle del Tier 3, con la possibilità di aggiornamento dei dati (RPO) con frequenza molto alta, ma non bloccante per le attività transazionali del centro primario (aggiornamento asincrono).

Tier 5: la soluzione è analoga a quella del Tier 4, con la differenza che l'aggiornamento finale dei dati avviene solo quando entrambi i siti hanno eseguito e completato i rispettivi aggiornamenti (aggiornamento sincrono). Allo stato attuale della tecnologia questa soluzione non può prescindere dalle caratteristiche della connettività sia in termini di distanza, sia in termini di latenza; ne consegue che tale modalità (sincronizzazione), nonché l'eventuale bilanciamento geografico del carico di lavoro, risulta difficile oltre significative distanze fisiche fra sito primario e secondario. Debbono essere attentamente valutati se sussistono, per aspetti tecnologici, vincoli di operatività del sito primario in caso di problemi su quello secondario. E' quindi fondamentale, per questa tipologia di soluzione, valutare la distanza fra i siti.

Tier 6: la soluzione prevede che nel sito di DR le risorse elaborative, oltre ad essere sempre attive, siano funzionalmente "speculari" a quelle del sito primario, rendendo così possibile ripristinare l'operatività dell'IT in tempi molto ristretti. Le altre caratteristiche sono uguali a quelle del Tier 5.
E' fondamentale, per questa tipologia di soluzione, valutare la distanza fra i siti.