### ALLEGATO A7

**Programma Operativo Regionale (POR), parte FESR, della Regione del Veneto, Programmazione 2014- 2020, Asse 2 “Agenda Digitale”, Priorità d’investimento: 2 (a) – “Rafforzare le applicazioni delle TIC per l'e-government, l'e-learning, l'e-inclusione, l'e-culture e l'e-health”, Azione 2.2.1 “Soluzioni tecnologiche per la digitalizzazione per l'innovazione dei processi interni dei vari ambiti della Pubblica Amministrazione nel quadro del Sistema pubblico di connettività, quali ad esempio la giustizia (informatizzazione del processo civile), la sanità, il turismo, le attività e i beni culturali, i servizi alle imprese", Azione 2.2.2 "Soluzioni tecnologiche per la realizzazione di servizi di e-Government interoperabili, integrati (joined-up services) e progettati con cittadini e imprese, e soluzioni integrate per le smart cities and communities (non incluse nell'OT4) (2.2.2 AdP)", Azione 2.2.3 "Interventi per assicurare l'interoperabilità delle banche dati pubbliche [gli interventi comprendono prioritariamente le grandi banche pubbliche - eventualmente anche nuove basi dati, nonché quelle realizzate attraverso la gestione associata delle funzioni ICT, in particolare nei Comuni ricorrendo, ove, a soluzionicloud]".**

**Bando pubblico “Agire per la cittadinanza digitale”**

**SCHEMA MIGRAZIONE DATA CENTER**

1. **Obiettivi del documento**

Il presente documento si pone l’obiettivo di facilitare le aggregazioni nell’individuazione delle azioni organizzative, tecniche e operative che dovranno essere intraprese per poter esercitare la loro funzione nel territorio.

Quanto appena rappresentato si traduce, fattivamente, nella produzione di un elenco di requisiti (obbligatori o preferibili) e di linee guida che ciascuna aggregazione dovrà utilizzare per valutare lo scostamento della propria infrastruttura informatica rispetto a quanto richiesto e progettare, di conseguenza, un piano di azioni mirate volte a sanare, totalmente o parzialmente, quanto emerso dalla Gap Analysis appena citata.

I contenuti che seguono sono stati sostanzialmente divisi in due parti: la prima entra nel merito delle facility di un Data Center fornendo un elenco di requisiti obbligatori o non obbligatori (preferibili), in particolare vengono trattati i macro temi legati all’architettura in senso lato, ai sistemi per le telecomunicazioni, agli impianti elettrici, meccanici, di spegnimento, di sicurezza e di monitoraggio; la seconda, invece, sposta l’attenzione sul cuore di un Data Center focalizzandosi quindi principalmente sulle componenti attive trattandole in modo verticale e definendo delle linee guida rispetto ai macro ambiti di connettività, rete, sicurezza, sistemi (intesa come elaborazione dati e basi dati) e protezione dei dati.

Infine, verrà data una breve descrizione delle modalità con le quali sarà possibile dare evidenza del rispetto dei requisiti e dell’aderenza, parziale o totale, alle linee guida.

Si precisa che le indicazioni fornite nel presente Allegato, sia in termini di requisiti sia per quanto riguarda le linee guida, sono state elaborate tenendo in forte considerazione le Agende Digitali nazionale (Agenzia per l’Italia Digitale - AgID) e regionale (Regione Veneto - RVE) ed i rispettivi Piani Triennali per l’informatica che, sebbene diverse nella forma, perseguono obiettivi e finalità comuni. Per tale motivo da una parte i requisiti, sebbene rivisti, si rifanno agli stessi forniti da AgID per il censimento del Patrimonio ICT della Pubblica Amministrazione, mentre dall’altra le linee guida sono volte a rafforzare il modello multi-cloud ibrido progettato e voluto dalla Regione Veneto.

# Requisiti e Linee Guida

## Requisiti delle Facility

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **N****.** | **Ambito** | **Indicatore** | **Valutazione** | **Requisit o obbligato rio** | **Requisito non obbligator io (preferibil****e)** |
| **Telecomunicazioni** |
| 1 | Generale | Area principale di distribuzione telecomunicazioni ridondata | Si | **X** |  |
| 2 | Generale | Cablaggi telecomunicazioni e percorsi orizzontali ridondanti | Si | **X** |  |
| 3 | Generale | Pozzetti di Accesso della fibra con distanza superiore ai 20 m | Si |  | **X** |
| 4 | Generale | Router e Switch hanno alimentatori e control station ridondati | Si | **X** |  |
| 5 | Generale | Router ridondanti e switch con uplink ridondato | Si | **X** |  |
| **Architettura** |
| 6 | Componenti costruttive | Tipo di pannelli del pavimento rialzato (se presente) | Pannelli con opportuna capacità di carico (es. Solfato di Calcio) |  | **X** |
| 7 | Componenti costruttive | Accoppiamento pannello e sottostruttura (quando il pavimento rialzato è presente) | Struttura con resistenza al carico di almeno 1600 Kg/mq |  | **X** |
| 8 | Corridoi di uscita | Separazione antincendio corridoi di uscita dalla sala computer e dalle aree di supporto | secondo le normative, non inferiore a REI 60 |  | **X** |
| 9 | Corridoi di uscita | Larghezza dei corridoi di uscita | secondo le normative, non inferiore a 1,2 m |  | **X** |
| 10 | Area di spedizione/ricez ione | Area spedizioni separata fisicamente dalle altre aree del Data Center | Si | **X** |  |
| 11 | Locali di stoccaggio combustibile e generatori | Prossimità locali di stoccaggio combustibile e generatori alle sale dati ed alle aree di supporto | Se all'interno dell'edificio, dotato di compartimentazione REI 120 al minimo con eventuali prescrizioni VVFF, se all'esterno secondo le prescrizioni dei VVFF | **X** |  |
| 12 | Sicurezza | Sistema di controllo (TVCC, Accessi, Antiintrusione), dispositivi in campo e apparati di visualizzazione sotto continuità | UPS dedicato al sistema di controllo e visualizzazione oppure batterie locali sui dispositivi di campo, con autonomia di 8 ore | **X** |  |
| 13 | Sicurezza | Personale di sicurezza fisica | 24h/7gg | **X** |  |
| 14 | Controllo accessi | Controllo accessi ai varchi di tutte le sale del Data center, compresa l'entrata principale | Entrata e uscita con badge o biometrico, sistema antiintrusione, allarme porta/finestra aperta | **X** |  |
| 15 | Ingresso edificio | Ingresso dell'edificio con guardiola e bancone della sorveglianza per il controllo dei documenti e delle autorizzazioni, adeguatamente protetto | Si |  | **X** |
| 16 | Ingresso edificio | Ingresso dell'edificio con porte e finestre antincendio | Almeno REI 60 (se presente permesso specifico rilasciato dai VVFF è considerato conforme) | **X** |  |
| 17 | Ingresso edificio | Ingresso edificio con porte interbloccate con accesso singolo, sistemi fisici anti scavalcamento e anti passback | Si |  | **X** |
| 18 | Uffici amministrativi | Uffici amministrativi separati dall'area del CED | Si | **X** |  |
| 19 | Aree del personale | Separazione antincendio dei servizi igienici e sale ristoro dalle sale dati e dalle aree di supporto | Almeno REI 60 | **X** |  |
| 20 | Videosorveglia nza | Controllo TVCC a tutte le aree ristrette con accesso tramite porte con badge | Si | **X** |  |
| 21 | Videosorveglia nza | TVCC dei varchi con controllo d'accesso | Si | **X** |  |
| 22 | Videosorveglia nza | Registrazione TVCC di tutte le attività su tutte le telecamere | Sì, in digitale (mantenimento delle registrazioni di almeno 7 giorni) | **X** |  |
| **Impianto Elettrico** |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 23 | Generale | Il sistema di distribuzione elettrica consente la manutenzione a caldo | Sì, senza esclusioni | **X** |  |
| 24 | Generale | Cavi elettrici per server e apparecchiature per telecomunicazioni | Cavi di alimentazione ridondanti con capacità del 100% sui rimanenti cavo o cavi | **X** |  |
| 25 | Sistemi UPS | Ridondanza sistemi UPS | N+1 | **X** |  |
| 26 | Sistemi UPS | Bypass automatico e bypass di manutenzione | Bypass automatico alimentato con interruttore dedicato e presenza di interruttore di bypassesterno per esclusione totale UPS | **X** |  |
| 27 | Sistemi UPS | Distribuzione elettrica in uscita dai sistemi UPS | Quadro elettrico con interruttori estraibili con funzioni adjustable long time e instantaneous trip | **X** |  |
| 28 | Sistemi UPS | Tipo di batterie dei sistemi UPS | Batterie progettate per 5-10 anni di vita media con UPS statici oppure UPS rotanti | **X** |  |
| 29 | Sistemi UPS | Durata minima delle batterie del sistemi UPS | 10 minuti con UPS statici o UPS rotanti | **X** |  |
| 30 | Sistemi UPS | Sistema di monitoraggio delle batterie dei sistemi UPS | Monitoraggio gestito dall'UPS a livello dei banchi | **X** |  |
| 31 | Sistemi UPS | Topologia sistemi UPS | Ridondanti, distribuiti su moduli o blocchi | **X** |  |
| 32 | Scariche Atmosferiche | Impianto di protezione dalle scariche atmosferiche | Si | **X** |  |
| 33 | Messa a terra | Messa a terra delle masse metalliche in Computer Room | Si | **X** |  |
| 34 | Monitoraggio centralizzato | Punti monitorati | Rete elettrica pubblica, Trasformatore principale, UPS, Generatore, Stato Interruttori, STS, ATS, PDU | **X** |  |
| 35 | Monitoraggio centralizzato | Metodo di notifica degli allarmi | Sala di controllo, cercapersone, Email e/o SMS | **X** |  |
| 36 | Locali batterie | Locale batterie separato dal locale UPS | Non obbligatorio a meno che non sia richiesto espressamente dai VVFF. La separazione ècomunquepreferibile. |  | **X** |
| 37 | Locali batterie | I singoli gruppi di batterie sono isolati fra loro | Si |  | **X** |
| 38 | Generatori di backup | Dimensionamento dei generatori elettrici automatici di backup (Standby generating system) | Dimensionati per il carico dell'intero edificio con ridondanza N+1 |  | **X** |
| 39 | Generatori di backup | Generatori su singola barratura | Si | **X** |  |
| 40 | Manutenzione apparati | Personale operativo e di manutenzione apparati elettrici | Onsite 24 ore su 7 giorni | **X** |  |
| 41 | Manutenzione apparati | Manutenzione preventiva apparati elettrici | Generatore e UPS | **X** |  |
| 42 | Manutenzione apparati | Programma di formazione del personale operativo | Formazione completa per regolare esercizio degli apparati | **X** |  |
| **Impianto Meccanico** |
| 43 | Generale | Ridondanza degli apparati meccanici (es. unità di condizionamento, dry cooler, pompe, torri evaporative, condensatori). I requisiti di ridondanza si applicano anche alle aree di supporto che non sono critiche alla continuità delle operazioni della computer room | Ridondanza N+1 allo scopo di garantire le operazioni di manutenzione a caldo. La perdita temporanea di alimentazione elettrica o di acqua (dove applicabile) non provoca l'indisponibilità del raffreddamento, ma può causare l'innalzamento della temperatura entro i livelli di operatività degli apparecchi critici/essenziali. Le manovre per garantire la manutenzione a caldo possono essere manuali. | **X** |  |
| 44 | Generale | Passaggio di tubazioni non attinenti al data center all'interno dello spazio data center. | non permesso | **X** |  |
| 45 | Generale | Sistemi meccanici alimentati da gruppo elettrogeno in mancanza di rete pubblica | Si | **X** |  |
| 46 | Generale | Controllo dell'umidità nella Computer Room | Si | **X** |  |
| 47 | Sistemi raffreddati ad acqua | Unità interne | Aggiungere un'unità in ridondanza ogni 5-8 unità installate |  | **X** |
| 48 | Sistemi raffreddati adacqua refrigerata e adaria | Alimentazione elettrica agli apparati meccanici | N+1 configurata per garantire la manutenzione a caldo | **X** |  |
| 49 | Sistema di controlloHVAC | Sistema di controllo HVAC | Progettato per manutenzione a caldo | **X** |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 50 | Sistemi condensati adacqua | Ripristino livello acqua dei circuiti | Due punti di connessione alla rete di alimentazione dell'acqua | **X** |  |
| 51 | Carburante per i generatori | Quantità di carburante | Per garantire un'autonomia di 6 ore (previo possesso di permesso specifico rilasciato dai VVFF) | **X** |  |
| 52 | Carburante per i generatori | Serbatoi | Multipli |  | **X** |
| 53 | Carburante per i generatori | Pompaggio carburante e tubazioni | Per ogni generatore |  | X |
| 54 | Anti incendio | Rilevazione Fumi VESDA per Computer Room ed Entrance Room con presenza di apparati attivi o sistema equivalente | Del tipo pre action con valvola comandata dalla rilevazione | **X** |  |
| 55 | Anti incendio | Spegnimento automatico a gas per Computer Room ed Entrance Room con presenza di apparati attivi | Si | **X** |  |
| 56 | Anti allagamento | Sistema di rilevazione in Computer Room edEntrance Room con presenza di apparatiattivi | Si | **X** |  |

* 1. **Linee guida per l’infrastruttura**

Le intenzioni dichiarate di Regione Veneto, comuni a quelle dell’Agenzia per l’Italia Digitale, sono quelle di seguire il mantra “Cloud First”, ovvero lavorare affinché il punto di caduta della razionalizzazione del Patrimonio ICT della pubblica amministrazione sia il Cloud nella sua accezione più generica.

Nonostante quanto appena dichiarato, risulta palese anche solo dopo un’analisi preliminare che il parco applicativo, sia gli asset trasversali sia quelli verticali, non è pronto, nel breve periodo, per una migrazione verso il cloud e per tale motivo necessita di un percorso con tappe intermedie che possa agevolare e, di conseguenza, catalizzare il processo di razionalizzazione dei Data Center offrendo alternative On-Premise.

La razionalizzazione e la migrazione del patrimonio ICT della Regione Veneto avranno dunque tre possibili alternative:

* + 1. Cloud (first);
		2. Infrastruttura Informatica di Regione Veneto;
		3. Infrastruttura Informatica dell’aggregazione.

A tal proposito Regione del Veneto (2) ha iniziato e quasi completato una profonda trasformazione digitale dell’infrastruttura informatica dei propri Data Center, sia il sito primario sito a Marghera (VE) sia il secondario sito a Padova (PD).

L’analisi di questa trasformazione è stata condotta avendo bene in mente il processo di razionalizzazione dei Data Center che ha condizionato ed indirizzato le scelte tecnologiche e dei prodotti che hanno contribuito alla costituzione dell’architettura informatica ormai quasi completamente in esercizio.

### Connettività

In un interesse di convergenza delle infrastrutture fisiche, delle piattaforme abilitanti e dei sistemi informativi, si rende necessario creare un punto di interconnessione fisica individuato nella struttura Neutral Access Point (NAP) del Nord-Est, ovvero il Veneto Service Internet eXchange (VSIX) di Padova (PD).

Ogni aggregazione dovrà predisporre una propria infrastruttura in fibra ottica per raggiungere la meet-me-room del VSIX. Gli apparati dovranno essere ridondati in maniera tale da garantire la continuità del servizio erogato e dotati di interfacce 1/10GB in rame o Fibra Ottica. Da quest’ultimo punto sarà possibile collegare l’apparato di terminazione dell’aggregazione all’infrastruttura regionale.

In caso di impossibilità di un collegamento diretto, è possibile considerare un collegamento MPLS o VPLS con i provider indicati da VSIX in una configurazione di ridondanza [[https://www.vsix.it/it/servizi-e-tariffe/come-](https://www.vsix.it/it/servizi-e-tariffe/come-connettersi.htm) [connettersi.htm](https://www.vsix.it/it/servizi-e-tariffe/come-connettersi.htm)].

### Rete

L’attuale infrastruttura Network di Regione del Veneto (RVE) è gestita da apparati che lavorano in IPv4 in grado di gestire un numero limitato di VLAN (4096), per questo motivo presso VSIX verrà sostituito il TAG ID utilizzato dall’aggregazione con una numerazione compliance con quelle definite da RVE.

Regione offre la possibilità di utilizzare 30 ID differenti di VLAN, il numero limitato di ID serve ad evitare overlap (dei VLAN ID) tra un soggetto ed un altro. La comunicazione con l’infrastruttura regionale dovrà avvenire necessariamente tramite NAT in modo tale da evitare l’overlap IP.

RVE si sta adoperando per una trasformazione digitale che coinvolge anche il proprio Data Center (DC) da una struttura Campus di tipo collapsed core ad un prodotto che si cali maggiormente ad affrontare le necessità di un DC moderno e multi tenant, in particolare si tratterà di una soluzione Software Defined Network (SDN) unica che gestirà sia la rete underlay che quella overlay.

In questa direzione sarà possibile considerare l’utilizzo dell’IPv6 e delle VXLAN per la micro-segmentazione dei vari Tenant in modo tale da poter gestire la coesistenza e quindi l’overlap delle subnet e degli IP. Ogni aggregazione comunicherà con gli altri servizi di RVE, o gli altri tenant, direttamente attraverso dei contract.

### Sicurezza

All’interno del contesto di RVE le aggregazioni verranno visti come “bolle” che si attesteranno su un VDOM del cluster Firewall in esercizio.

I Firewall di RVE sono disposti in due bastioni uno di Front End (FE) ed uno di Back End (BE) in una configurazione ridondata presso VSIX. Nel primo risiedono i contesti che si devono interfacciare con il mondo esterno, nel secondo invece si attestano tutte le segregazioni interne del DC.

Ogni aggregazione, una volta eseguito il *re-tagging* delle VLAN lato Network, verrà quindi attestato su un personale VDOM all’interno del Firewall di BE. Da lì sarà possibile raggiungere i servizi RdV tramite NAT, gli accessi ai servizi di Regione Veneto pertanto verranno mediati dal VDOM del firewall di Regione Veneto.

In una prossima evoluzione del DC di RVE, con una soluzione *Software Defined*, verrebbero dedicati ugualmente dei VDOM per ogni aggregazione in modo tale da potere garantire *policy* differenziate a seconda delle necessità. Le comunicazioni con i servizi regionali verranno stabiliti tradizionalmente tramite NAT o direttamente dall’infrastruttura network.

### Elaborazione Dati

L’infrastruttura tecnologica su cui si basano poi tutti i servizi dell’ente deve essere tale da avere solide basi di affidabilità, resilienza, scalabilità, innovazione, semplicità di gestione e manutenzione.

I sistemi iperconvergenti, che stanno guadagnano sempre più mercato nell’ambito dei sistemi ICT, offrono una valida e conveniente soluzione alle necessità appena descritte, al punto da configurarsi come possibile evoluzione dell’attuale tecnologia Industry Standard delle principali piattaforme hardware ospitate presso i Data Center della pubblica amministrazione oggetto di convergenza regionale.

In particolar modo si citano alcuni dei vantaggi di maggior rilievo derivanti dall’adozione di questo tipo di tecnologia/infrastruttura:

* accorpamento di più funzionalità (rete, elaborazione, storage, software, deduplica, compressione) nel medesimo dispositivo;
* conseguimento di un risparmio in termini di consumo energetico derivante dall’ingegnerizzazione a fattor comune di più componenti;
* riduzione del numero di apparati hardware che implica:
	+ la riduzione delle attività di gestione (unica appliance) e di manutenzione (a volte molto specialistiche e costose come per esempio per lo storage dedicato);
	+ l’ottimizzazione dello spazio fisico necessario in Data Center;
	+ la scalabilità del sistema complessivo che risulta costituito da un’unica tipologia di appliance;
	+ la semplificazione della gestione dell’intero Data Center grazie alla presenza di una sola interfaccia utente volta al governo di tutti gli aspetti dell’architettura modulare costituente l’infrastruttura iperconvergente;
* ottimizzazione indiretta dei costi di acquisto in quanto l'infrastruttura iperconvergente disegna un modello di ICT sostenibile che consente una implementazione graduale, ovviando di fatto alla necessità di dover eliminare apparecchiature o di doverle sostituire prima della fine del naturale periodo di ammortamento;
* rapidità negli aggiornamenti dell’infrastruttura hardware (one-click);
* miglioramento dell'erogazione dei servizi all’utenza finale in quanto risultano più rapidi messa in esercizio e distribuzione dei servizi software, nonché il ripristino di quest’ultimi in caso di malfunzionamenti, poiché non è più necessario pianificare con largo anticipo il dimensionamento di ogni componente hardware ed agire separatamente sui vari livelli di componenti hardware e software come nel caso di un’architettura tradizionale;
* Quanto alla protezione dei dati, l’architettura iperconvergente consente in maniera nativa l’applicazione di politiche di Business Continuity (BC) e Disaster Recovery (DR) su un sito remoto secondario attraverso replica geografica sincrona o asincrona del dato.

Le caratteristiche generali del sistema iperconvergente devono essere almeno le seguenti:

* Il sistema deve essere resiliente alla perdita di un nodo per cluster;
* il sistema deve essere resiliente alla rottura di un disco, i dati presenti sul disco rotto devono essere automaticamente ricostruiti dal sistema e senza intervento da parte di un operatore;
* non devono essere presenti meccanismi di caching in scrittura dei dati in RAM al fine di preservare l’integrità dei dati in caso di mancanza improvvisa di energia elettrica;
* La soluzione proposta deve garantire il Tiering automatico dei dati tra dischi SSD e HDD al fine di avere i dati caldi nella parte SSD e quelli acceduti meno frequentemente (dati freddi) nella componente capacitiva (rotativa) del tier dischi, migliorando le prestazioni ed i tempi di latenza in lettura;
* La soluzione deve poter utilizzare il tier SSD, non solo per i metadata o per cache ma anche per l’archiviazione di tutte le tipologie di dati;
* La soluzione, al fine di massimizzare gli investimenti attuali e futuri, deve supportare anche le nuove tecnologie per dischi NVMe;
* Il sistema dovrà consentire l’espansione del cluster a caldo ed in maniera automatizzata mediante funzionalità di discovery di nuovi nodi presenti su rete, altresì consentirà la rimozione a caldo di nodi dal cluster. Inoltre, il cluster dovrà avere scalabilità illimitata in termini di numero di nodi.
* l’espandibilità della soluzione deve essere possibile la creazione di cluster con più di N nodi (valutato caso per caso) senza dover spezzare il file system;
* La soluzione deve utilizzare insieme algoritmi di deduplica e compressione senza impattare sulla performance dell’infrastruttura stessa;
* In caso di guasto di un singolo nodo i nodi rimanenti nella piattaforma automaticamente e in modo trasparente dovranno garantire l'accesso allo storage;
* Le macchine virtuali che erano in esecuzione sul nodo non funzionante vengono automaticamente riavviate su nodi rimanenti utilizzando le funzioni standard di HA;
* L’infrastruttura deve permettere la massima flessibilità nella gestione del Datastore: incrementare o decrementare le dimensioni del Datastore senza la distruzione delle VM;
* Aggiornamento a caldo di major e minor release del sistema operativo del fornitore dell’hypervisor attraverso la GUI senza l’utilizzo di strumenti esterni e deve essere one-click;
* L’upgrade dell’hypervisor deve essere indipendente dal software di iperconvergenza;
* Possibilità di inserire nodi eterogenei nello stesso cluster senza alcun disservizio e dalla console di amministrazione.
* Il sistema iperconvergente deve garantire il supporto di più di un hypervisor (multi-hypervisor);
* La soluzione deve garantire un’unica piattaforma di controllo e console di amministrazione valida sia per il cluster iperconvergente sia per il DRaaS.

### Base Dati

Entrando invece nel merito della gestione del dato mediante Base Dati, RVE, continuando a perseguire la volontà innovazione, trasformazione digitale e osteggiando qualsivoglia forma di vincolo (Lock-In), si è dotata dei più utilizzati Data Base relazionali a livello globale, fra cui Oracle, MS SQL Server, PostgreSQL, MySQL e MariaDb.

Nell’ultimo decennio i Data Base non relazionali (no-SQL) hanno subito una forte spinta e una forte verticalizzazione rispetto all’ambito di utilizzo, anche su questo fronte RVE ha un importante installato fra cui istanze di MongoDB, Redis, ElasticSearch, ecc.

Dal punto di vista infrastrutturale i Data Base citati negli ultimi due capoversi non presentano peculiarità tecniche o di licenziamento che impediscano di utilizzare con ottime prestazioni e affidabilità l’infrastruttura iperconvergente già a descritta al paragrafo precedente.

Oracle, in tal senso, fa eccezione. Come è ampiamente noto agli esperti del settore, presenta, soprattutto a livello Enterprise, dei punti critici e di attenzione per i quali è necessario prestare la massima attenzione per non incorrere in scelte discutibili che potrebbero far lievitare i costi in modo esponenziale.

Questo rischio è stato gestito, nel corso del tempo, dalle aziende ICT, pubbliche e private, e dovrà avvenire lo stesso anche ora attraverso le decisioni strategiche delle aggregazioni. Le soluzioni a questo problema sono molteplici ed hanno gradi di complessità architetturale diversi. Nonostante siano ancora presenti nel mercato soluzioni valide che puntano a mitigare quanto espresso sopra attraverso l’utilizzo di processori molto performanti a parità di Core (strategia ha le sue fondamenta sul modello di licensing applicato da Oracle), siano essi host basati su architettura Intel x86 o IBM Power, RVE consiglia l’adozione di infrastrutture iperconvergenti anche in questo specifico e verticale frangente.

Nella fattispecie l’infrastruttura iperconvergente consigliata è quella Ingegnerizzata Oracle che si porrà quale elemento fondante nella gestione del dato relazionale Mission Critical. Principalmente sono due le soluzioni di mercato: Oracle Database Appliance (ODA) e Oracle Exadata.

Le componenti necessarie all’implementazione dell’infrastruttura tecnologica portano in dote molteplici benefici esclusivi della soluzione, di cui se ne riporta di seguito un estratto dell’elenco completo (a titolo esemplificativo ma non esaustivo):

* Hardware sviluppato in sinergia con la componente Software;
* Integrazione di Hardware e Software con Oracle DB;
* Singolo punto di controllo per monitoraggio/gestione HW infrastrutturale e SW Oracle DB;
* Latenze comprovate nell’ordine del microsecondo per garantire l’erogazione di servizi di eccellenza nell’ambito della convergenza infrastrutturale della PA;
* Certificazione in soluzioni PCI-DSS per garantire le necessità di segregazione degli ambienti nell’ambito della convergenza infrastrutturale della PA;
* Classificazione “AL4 Fault Tolerant System” nel caso di Oracle Exadata (tolleranza all’errore “5 nove” o 99,999% del tempo di utilizzo).

### Protezione dei Dati

I servizi di backup e restore, essenziali e strategici per l’ente, devono essere basati su soluzioni che abbiamo un approccio moderno al backup e siano progettate per il Cloud, per gli ambienti virtualizzati e per fornire un’estrema semplicità e scalabilità. La soluzione deve essere *SOFTWARE-DEFINED*, completamente resiliente e fornire i migliori Service Level Agreement (SLA) in termini di Recovery Point Objective (RPO) e di Recovery Time Objective (RTO).

Tale soluzione deve avere le seguenti caratteristiche generali minime:

* Scale-out, per consentire all’ente di indirizzare la crescita legata a future esigenze;
* deve basarsi su appliance iperconvergenti per fornire una semplice architettura building-block per la protezione dei dati ad elevate prestazioni, combinando all’interno software di protezione dati, destinazione di backup, deduplica, catalogo e ricerca;
* deve garantire una gestione semplice e veloce, una facile installazione e deve avere un framework Restful API aperto per consentire orchestrazione e automazione;

Inoltre, la soluzione deve garantire almeno le seguenti caratteristiche tecniche specifiche:

* essere scalabile virtualmente senza limiti su base modulare (capacità e prestazioni);
* avere una resilienza di livello Triple mirror (RF3) o Erasure Coding (EC) 4+2 o superiori, per garantire la massima disponibilità del servizio in caso di guasti;
* poter offrire una storicizzazione su “tier” differenti e target di archiviazione multipli (Cloud, Object Store, NFS o simili);
* supportare la replica su appliance differenti per aumentare la resilienza del servizio, anche in ottica di Disaster Recovery (DR);
* essere supportato l’accesso basato su ruoli (RBAC), deve essere integrabile con Active Directory e deve essere strutturato per gestire il multi-tenancy;
* avere le componenti software e hardware strettamente legate e non devono esserci componenti terze presenti;
* Prevedere, oltre ad una gestita tramite una semplice ed unica interfaccia web moderna e adattiva (HTML5) on-premise ed in cloud, una interazione con i principali Framework RestFul API quali, ad esempio, Red Hat Ansible,
* deve supportare ambienti virtuali VMware vSphere, Microsoft Hyper-V e Nutanix AHV, attraverso la stessa interfaccia grafica e rendendo disponibile per tutti e tre gli hypervisor restore granulari in un unico passaggio a livello di file e di cartelle;
* non deve prevedere agenti per la protezione delle VM (sono contemplati solo connettori “*stateless*” che non richiedano gestione e soprattutto riavvio dei sistemi);
* deve integrarsi con le API di VMware ed essere certificata “VMware Ready”;
* deve consentire il recupero di database MS SQL point-in-time al minuto della giornata desiderato (o all’ID della transazione) in un singolo passaggio, con la possibilità di “montare” il database stesso sull’appliance offerto, senza necessità di trasferire dati via rete;
* deve consentire il backup e la recovery di DB Oracle utilizzando un’integrazione con RMAN e deve supportare la modalità di backup Oracle Incremental Merge;
* deve consentire il backup completamente indicizzato di set di file e volumi di sistemi operativi Linux, Windows e AIX in modalità agent-less o tramite connettori “*stateless*” che non richiedano gestione o riavvio dei sistemi;
* deve poter proteggere NAS direttamente senza l’impiego di proxy e poter eseguire restore e download di singoli file in-place e out-of-place;
* non deve introdurre carichi prestazionali per l'ambiente primario durante le procedure di backup;
* non deve prevedere classici job di protezione o schedulazioni, ma semplici impostazioni di RPO basate su policy SLA che possono incorporare più host e applicazioni
* deve essere basata su TCP/IP per quanto riguarda le comunicazioni interne ed il trasferimento dati.

Per quanto concerne la sicurezza (Encryption, GDRP e Ransomware) la soluzione:

* deve essere “*secure by design*”, ovvero tutti i trasferimenti dati devono viaggiare in forma cifrata, i dati e i metadati devono essere memorizzati in forma cifrata all’interno della soluzione stessa, eventuali archiviazioni su “tier” differenti di terze parti (storage o cloud) devono avvenire in forma cifrata e la memorizzazione su questi “tier” deve avvenire in forma cifrata. La caratteristica “*secure by design*” di cui sopra garantisce la piena conformità all’articolo 32 del GDPR;
* deve garantire l’immutabilità delle copie dei dati salvati, anche in seguito ad attacchi di tipo Ransomware;
* deve offrire strumenti di monitoraggio, analisi e recovery per intercettare attacchi di tipo Ransomware, offrendo la possibilità di revert a file e documenti non “infetti” (per esempio non cifrati) con pochi semplici click tramite un’interfaccia web dedicata;
* Essendo l’ente rivolto al paradigma cloud, la soluzione deve permettere l’archiviazione dei dati in Cloud pubblici e privati. I trasferimenti verso il Cloud (pubblici o privati) devono avvenire in modalità cifrata e i dati devono essere conservati in modalità cifrata all’interno del Cloud stesso.

Fondamentale alcune precisazioni e vincoli legati al Cloud:

* Per quanto riguarda offerte di Cloud pubblico devono essere supportati almeno i tre grandi player del mercato attuale, ovvero: Amazon Web Services (AWS), MS Azure e Google Cloud Platform (GCP);
* Deve inoltre essere supportato ufficialmente SPC Cloud (*Servizi di Cloud Computing per le Pubbliche Amministrazioni*);
* I dati archiviati su Cloud devono essere ricercabili e recuperabili con granularità a livello di file; i metadati devono essere conservati all’interno dell'archivio Cloud per consentire la recuperabilità dei backup nel caso in cui l'appliance on-site risulti essere inutilizzabile o vada distrutto.

# 3. Conclusioni

A conclusione del presente documento si vogliono riportare due precisazioni importanti:

1. All’interno del presente documento sono state riportate solo linee guida volutamente senza alcun riferimento a precisi prodotti, marchi, produttori o brand. Tuttavia, è possibile, per chi ne fosse interessato, richiedere all’amministrazione regionale un chiarimento circa le soluzioni tecnologiche specifiche che sono state adottate da RVE;
2. Le caratteristiche tecniche che sono state enunciate sono, come ovviamente accade nell’ambito della tecnologia in generale ma in particolare per quella ICT, soggette ad obsolescenza e devono pertanto essere lette ed interpretate con cognizione di causa nonché, nel tempo, aggiornate, adeguate e contestualizzate.