Procedura negoziata con RDO a cinque operatori ai sensi dell'art. 62 e 36 comma 2 lett. b) e comma 6 del d.lgs. 50/2016, per la fornitura e l'installazione di un sistema dedicato alla Protezione dei Dati critici aziendali e dei server virtuali, contenuti nei 3 data center aziendali e nei server di terze parti presenti nella rete Aziendale, unitamente al servizio di formazione, al servizio di assistenza per 36 mesi ed al servizio di supporto sistemistico evolutivo – CIG 89753060D2

SPECIFICHE TECNICHE

SOMMARIO

1. Premessa

L'Azienda Ospedaliera Santobono, nell'ambito della continua evoluzione del proprio sistema informativo, ha la necessità di implementare una soluzione di backup per affiancarre e ottimizzare l'attuale soluzione considerata non più in linea con le proprie esigenze di protezione e conservazione del dato in particolare legata all'esigenza di resilienza in caso di attacchi alla sicurezza informatica che possano compromettere l'operatività di ambienti ritenuti mission critical.
Il Piano Ospedaliero Regionale identifica infatti l'AORN quale:

- Centro della Grande Emergenza e dell'Emergenza Specialistica Pediatrica;
- HUB Unico Regionale della Rete dell'Emergenza Pediatrica;
- HUB Regionale (attraverso l'istituzione di Dipartimento Interaziendale con la Seconda Università degli Studi di Napoli) della Rete Oncologica pediatrica;
- HUB pediatrico della Rete Regionale della Terapia del Dolore;
- HUB pediatrico per la Rete dell'Alta Specialità Riabilitativa;
- Centro Trauma ad Alta specializzazione (CTS) per l'età pediatrica della rete regionale della Rete per il Trauma;
- Centro Regionale per le Emergenze Neuropsichiatriche Infantili;
- Terapia Intensiva Neonatale di Alta Specialità, nell'ambito della Rete per l'Assistenza Neonatale;
- Integrazione con la ASL NA1 Centro nel Dipartimento Funzionale Interaziendale Ospedale-Territorio per l'assistenza pediatrica, allocato presso il Presidio SS. Annunziata della ASL

da cui si evince l'importanza, la sensibilità e la delicatezza dei dati che tratta e per i quali è richiesto un livello elevato di riservatezza. L'azienda attualmente dispone di un sistema di backup ritenuto non più affidabile ed in linea con l'evoluzione tecnologica in atto con particolare riguardo ai servizi IT di tipo serverless e, più in generale, di quelle che abbracciano il paradigma cloud.
Per tale motivo l'Azienda ha avviato da tempo uno studio specifico in termini di tecnologie e soluzioni che il mercato potesse offrire a garanzia degli obiettivi appena descritti. Lo studio basato soprattutto nella ricerca di una soluzione tecnologica fondata sulla protezione da attacchi di tipo Ransomware ha portato all'individuazione di una soluzione specifica che presenta un approccio moderno al backup, progettata per il cloud privato, per ambienti virtualizzati e per fornire un'estrema semplicità di applicazione e utilizzo. La soluzione individuata è quella Rubrik in quanto:

1. completamente resiliente e in grado di fornire i massimi SLA in termini Recovery Point Objective (RPO) e Recovery Time Objective (RTO);
2. di tipo scale-out per consentire ampliamenti a future esigenze;
3. dotata di framework API aperto che consente l'orchestrazione e l'automazione della soluzione di back-up.

La soluzione dovrà garantire una gestione semplice e veloce, una facile installazione e deve essere comprensiva dei servizi di supporto e garanzia completi per 3 anni in modalità 12x5 (12 ore per 5 giorni a settimana). Il supporto deve includere le attività di upgrade/patching della soluzione.

2. Contesto

L'esigenza dell'Azienda è quella di proteggere tutti i dati sensibili, i servizi ed i server virtuali attraverso un ambiente sicuro che ne consenta il ripristino in caso di attacco hacker (Data Protection). In particolare, per rispondere a questi requisiti si è deciso di puntare su infrastrutture definite SDD di nuova generazione definite "iperconvergenti" ovvero mediante *un singolo stack SW che combina tutte le funzionalità del classico datacenter capace di girare a monte di un singolo gruppo di risorse condivise di tipo x86 e che*

fornisce prestazioni di tipo enterprise su HW economico integrando: risorse di calcolo, storage, sw di virtualizzazione e funzionalità di protezione dei dati.
La soluzione dovrà essere assemblabile tramite la fornitura di singoli blocchi dell'occupazione rack di 2U che integrino :

- *Storage di tipo SSD*
- *Storage SAS/SATA*
- *Risorse cpu*
- *RAM*
- *SW di backup e orchestrazione*
- *SW per la virtualizzazione dei datastore e la deduplica/compressione*
- *SW per la gestione della protezione del dato*
- *Garanzia di recovery in caso di attacchi di tipo ransomware*

La soluzione Rubrik, a seguito di approfondita analisi di mercato, è stata valutata idonea a soddisfare le esigenze dell'Azienda in quanto possiede le seguenti specifiche caratteristiche che devono essere completamente soddisfatte:

Architetturali

- appliance scale-out che fornisce un semplice building-block per la protezione dei dati ad elevate prestazioni;
- combina software, destinazione di backup, deduplica e ricerca in un unico building-block;
- garantisce scalabilità senza limiti su base modulare (capacità e prestazioni);
- supporta target di archiviazione multipli (Cloud, Object Store, NFS);
- supporta la replica *appliance su appliance*;
- si basa su principi di webscale e master-less, offrendo alta affidabilità su ogni componente, senza nessun singolo punto di failure e completamente distribuita;
- è di tipo zero trust design;
- integra funzionalità di "ransomware detection e remediation" in grado di intercettare anomalie sui set di backup in base a livelli di encryption troppo elevati o entropia/disordine (non solo change rate, in quanto valore influenzabile da aggiornamenti software o cambiamenti in file molto grandi);
- offre subito anche visibilità di dettaglio di un eventuale attacco, con la possibilità di individuare singoli file o cartelle compromessi (indipendentemente dal sistema operativo o NAS sorgente) e ripristinarli massivamente in automatico all'ultima versione non compromessa;
- è possibile licenziare tutto lo spazio disco netto con tutte le funzionalità disponibili, sia nel sito primario che nell'eventuale sito di Disaster Recovery.

Tecniche:

- garantisce la reliability mediante algoritmo di Erasure Coding 4+2;
- immagazzina – nativamente - i dati in formato immutabile
- Il file system– per questioni di sicurezza - non è accessibile dall'esterno tramite protocolli standard NFS o SMB/CIFS;
- possibilità di montare in tempo reale e senza necessità di trasferire dati, le immagini di backup di virtual machine, database SQL e Oracle a scopo di DR e dev/test;

- integrazione di un sistema di indicizzazione nativo, che NON si basa su server ad-hoc e/o servizi esterni alla soluzione stessa. L'indicizzazione non è un opzione (quindi non può essere disattivata) e non impatta le performance del sistema stesso;
- offre una global search predittiva a livello di singoli file e documenti senza la necessità di specificare server di provenienza o cartelle;
- offre – nativamente - funzionalità di "Continuous Data Protection" fruibile dalla stessa interfaccia di gestione del backup, che consente di recuperare le VM VMware da punti di consistenza locali o remoti con RPO "near zero" a scopo DR con granularità al secondo e storico fino a 24 ore;
- fornisce solamente un backup di tipo "incremental forever" per tutti i workload (VM, server fisici, Database NAS…); in particolar modo, nel caso di macchine virtuali, il backup è eseguito in maniera incrementale anche dopo eventi come il trasferimento di macchine virtuali da un vCenter all'altro;
- offre una restore incrementale sulle VM VMware, andando quindi a ripristinare solo i blocchi modificati rispetto a quanto in essere;
- adatta dinamicamente la programmazione dei backup delle VM alla disponibilità di risorse nell'ambiente di produzione per non sovraccaricare i sistemi di produzione stessi;
- aggiorna automaticamente eventuali agenti o connettori installati sui server da sottoporre a backup durante l'aggiornamento del sistema stesso o prima di un job di backup;
- non richiede il reboot dei server a valle dell'installazione di eventuali agenti o connettori;
- offre una semplicità di implementazione massima: "rack & go", senza nessun software, proxy, agente, servizio o componente Microsoft (o di terze parti) da installare;
- offre automazione e orchestrazione via RestFul-API incluse nativamente nella piattaforma;
- offre un D/R nativo e integrato nella soluzione, tramite replica nativa per permetterne una eventuale estensione futura verso siti remoti;
- consentire il backup completamente indicizzato di set di file di S.O. Linux e Windows;
- non introduce carichi prestazionali per l'ambiente primario durante le procedure di backup
- la compressione dei dati e la deduplica sono globali ed automatizzate;
- nel caso in cui la soluzione faccia uso di un clustered file-system, la tolleranza ai guasti, le elevate prestazioni, la scalabilità e l'affidabilità sono parte integrante del file-system;
- consente semplici impostazioni di RPO basate su policy che possono incorporare più host ed applicazioni;
- è basata su TCP/IP per quanto riguarda le comunicazioni interne ed il trasferimento dati;
- effettua il recovery dei dati in locale sia in modalità in-place, nella stessa posizione di origine del dato, che out-of-place, in una posizione differente;
- possiede la funzionalità di replica nativa utilizzabile sia in LAN che WAN. Il dato replicato è mantenuto in formato deduplicato e compresso per tutto il suo ciclo di vita;
- permette l'archiviazione dei dati in Cloud pubblici e privati, idealmente su S3. Per quanto riguarda offerte di Cloud pubblico sono supportati AWS e Azure;
- i dati archiviati su cloud sono ricercabili e recuperabili con granularità a livello di file;
- i metadati sono conservati all'interno dell'archivio Cloud per consentire la recuperabilità dei backup nel caso in cui l'appliance on-site risulta essere inutilizzabile o vada distrutto;
- protegge le applicazioni in Cloud pubblico Azure e AWS;

- protegge NAS direttamente senza l'impiego di proxy ed esegue il restore di singoli file in place e out-of-place.

Sicurezza e Certificazioni:

- la soluzione è "secure by design", ovvero tutti i trasferimenti dati viaggiano in forma cifrata, i dati e i metadati sono memorizzati in forma cifrata all'interno della soluzione stessa, eventuali archiviazioni su "tier" differenti di terze parti avvengono solo in forma cifrata e la memorizzazione su questi "tier" deve avvenire in forma cifrata;
- offre - nativamente - un sistema di autenticazione a due livelli TOTP, integrabile con gli standard Google Authenticator, Microsoft Authenticator e Okta, per poter ricevere su un dispositivo mobile un codice "one-time" necessario per l'autenticazione stessa;
- si integra con sistemi di Multi Factor Authentication (MFA) utilizzando lo standard SAML 2.0;
- consente di implementare i backup di tipo WORM (Write Once Read Many) in modo da essere compliant con le richieste della normativa SEC Rule 17a-4(f). La modalità worm non può essere disattivata da un amministratore, ma deve prevedere una doppia approvazione di due utenti compliance definiti al momento dell'attivazione;
- offre una protezione nativa contro eventuali attacchi a server NTP (orologio), per evitare che la modifica all'orologio possa far "scadere" e quindi cancellare i backup (time drift); a garanzia di quanto sopra, la soluzione utilizza un clock di tipo monotonico (e non un semplice time of day);
- La soluzione e l'azienda produttrice hanno le seguenti certificazioni di sicurezza, privacy e compliance:
    - Common Criteria EAL 2+
    - SEC 17a-4(f)
    - FINRA 4511(c)
    - DoDIN Approved Products List (APL)
    - FIPS 140-2
    - SOC 2 Type 2 report
    - SOC 3
    - ISO 27001
    - EU-US Privacy Shield certification
    - GDPR

Installazione/Usabilità:

- il building block è di dimensioni standard per adattarsi agli attuali armadi presenti nel DataCenter. Un approccio modulare 2U è da considerarsi come standard
- la curva di apprendimento è molto breve
- la GUI centrale è in grado di gestire più dispositivi e sedi
- l'aumento di capacità è un processo semplice e rapido.

Inoltre Rubrik ha molteplici referenze italiane sia presso aziende private che Pubbliche Amministrazioni oltre ad essere presente come leader all'interno dell'ultima versione disponibile del *Magic Quadrant for Data Center Backup and Recovery Solutions* di Gartner.

3. Oggetto della Fornitura

Di seguito la descrizione di dettaglio tecnico degli apparati e dei servizi richiesti:

Codice Prodotto	Descrizione	Q.tà
RBK-R6408S-HW-01	r6408s Appliance, 4-node, 96TB raw HDD, 1.6TB SSD, SFP+ NIC (Appliance Hardware iperconvergente composto da 4 nodi all'interno di uno chassis da 2U con 12 dischi da 8 TB capacitivi sul frontale (96 TB raw; 60 TB netti)	1
RBK-SVC-BASIC-HW	Basic Support for hardware, prepay, M-F; 8am-8pm support (manutenzione Basic 12x5 sulla componente hardware (con sostituzione parti guaste in regime NDB)	36 mesi
RBK-CMPPRO-R6408	Rubrik Complete Edition Pro for r6408, incl. RCDM, Polaris GPS, CloudOn, Radar, 200 instances/VMs of cloud native protection and Basic Support, subscription prepay, limit 1 per customer, M-F; 8am-8pm support. (36 mesi di Subscription per l'utilizzo della piattaforma Rubrik che include tutti gli agenti e le opzioni per il backup dei dati in data center, funzionalità di storicizzazione dai in Cloud o storage terzi, servizio RADAR per Ransomware Detect&Remediation	36 mesi
RBK-SFP-TSR-01	10G/1G Dual Rate SFP+ Transceiver, pack of 4	2

La soluzione dovrà essere completata con 4 cavi DAC 3M per il collegamento in rete e delle relative spese di trasporto.

4. Servizi

I servizi che devono essere inclusi nel progetto sono:

- consegna installazione e configurazione dell'infrastruttura in sito dell'AORN in Napoli (da definire)
- configurazione della baseline di backup
- tuning e ottimizzazione
- collaudo
- training del personle interno AORN (2 giorni di formazione di durata di 8 ore ciascuno;

e dovranno essere svolti da partner certificati almeno Select da Rubrik e soprattutto da personale qualificato ed in possesso delle seguenti certificazioni:

- Rubrik RTP-Rubrik Technical Professional
- Rubrik RTA-Rubrik Technical Associate
- Rubrik RSP-Rubrik Sales Specialist
- Rubrik RCIE-Rubrik Certified Implementation Engineer

Di seguito le varie fasi ritenute essenziali e minime per la gestione della fornitura:

1. Kick off di progetto
2. redazione delle specifiche di dettaglio e della test list
3. verifica e tuning della configurazione HW proposta
4. delivery ed installazione delle componenti SW

5. test e collaudo della soluzione tramite esecuzione della test list
6. rilascio in produzione

Si richiede che il fornitore comunichi all'atto del kick off del progetto un referente tecnico con la qualifica di PM, che si occuperà di :

- Trasmettere il GANNT del progetto
- Comunicare con i diversi componenti del gruppo di lavoro
- Fornire pianificazioni e comunicare gli avanzamenti di progetto
- Gestire e allocare le risorse per la corretta riuscita dell'installazione
- Convocare (su richiesta del committente) SAL e riunioni di controllo
- Consegnare documenti e SW quando richiesto

Il sistema si riterrà accettato in caso di esito positivo dei collaudi eseguiti secondo la test list proposta dal Fornitore ed accettata dall'Azienda.

5. Supporto Sistemistico

A corredo dell fornitura è richiesto un servizio di supporto sistemistico qualificato al fine di supportare nei prossimi anni l'evoluzione dell'infrastruttura Rubrik oggetto della gara a seguito di novità tecnologiche e/o ad esigenze interne all'Azienda.
Di seguito si sintetizza la tipologia del Servizio richiesto:

- Affiancare il personale dell'Azienda nella progettazione di soluzioni che facciano evolvere nel tempo l'attuale Infrastruttura
- Documentare e certificare le variazioni architetturali di cui sopra

Per le seguenti attività sono richieste un totale di 20gg.