



## RELAZIONE

**Procedura telematica per l'acquisizione di nuove apparecchiature hardware, licenze software, servizi di manutenzione e servizi cloud avanzati per il potenziamento delle infrastrutture, della cybersecurity e dei servizi digitali di Regione del Veneto, nell'ambito del sistema dinamico di acquisizione della pubblica amministrazione (SDAPA) per la fornitura di prodotti e servizi per l'informatica e le telecomunicazioni - ID SIGEF 2681. Lotto 1 CIG n. B8986AFB16, Lotto 2 CIG n. B8986B0BE9, Lotto 3 CIG n. B8986B1CBC, Lotto 4 CIG n. B8986B2D8F, Lotto 5 CIG n. B8986B3E62.**

Il Responsabile unico del progetto, dott. Idelfo Borgo, Direttore della direzione Ict, Agenda digitale e Sos affidamento servizi e forniture ICT,

### rileva quanto segue

#### **Lotto 1: Fornitura Hardware "Nutanix"**

Sussiste l'impellente necessità di garantire la continuità operativa dei servizi erogati attraverso l'infrastruttura di virtualizzazione iperconvergente. Il fattore critico che rende indispensabile procedere con tale urgenza è l'imminente fine del supporto (End-of-Life - EOL) per una parte significativa dell'hardware oggetto della fornitura. Nello specifico, i nodi del sistema Nutanix che andranno fuori supporto riguardano la generazione 6 (G6). Questi apparati rappresentano un pilastro dell'infrastruttura e sono distribuiti presso i due data center regionali: il datacenter di Venezia e il datacenter di Padova.

Il raggiungimento della data di EOL comporta conseguenze immediate e gravi per la gestione dell'infrastruttura:

1. Assenza di Aggiornamenti Software/Firmware: Nutanix interromperà la fornitura di patch di sicurezza e aggiornamenti che mantengono l'ambiente protetto e performante.
2. Cessazione dell'Assistenza Tecnica: Non sarà più disponibile il supporto tecnico qualificato per la risoluzione di problemi complessi o il ripristino in caso di guasti.
3. Indisponibilità di Ricambi (Spare Parts): Verrà meno la possibilità di ottenere pezzi di ricambio ufficiali, rendendo molto problematica, se non impossibile, la riparazione rapida in caso di guasti hardware.

La mancata sostituzione tempestiva esporrebbe l'intera infrastruttura a rischi elevati di sicurezza, instabilità operativa e potenziali interruzioni di servizio prolungate, compromettendo l'erogazione di servizi essenziali alla Regione (interruzione di pubblico servizio in caso di fault dei sistemi).

Parallelamente all'attività di sostituzione per obsolescenza, l'acquisto di nuovi nodi è stato altresì necessario per rispondere a esigenze di sviluppo e innovazione. In particolare, è stata prevista l'attivazione di un cluster dedicato al sistema NDB (Nutanix Data Base). Questo ambiente specializzato è fondamentale per

**REGIONE DEL VENETO**

giunta regionale

L'ottimizzazione della Gestione Dati: Creazione di un'infrastruttura ottimizzata per l'hosting e la gestione di database critici.

Per garantire la piena operatività e la sostenibilità a lungo termine dell'investimento, l'acquisto dei nuovi nodi hardware per la sostituzione e l'espansione è stato accompagnato dall'acquisizione contestuale delle relative licenze software e dei contratti di manutenzione (supporto tecnico e aggiornamenti). Questo approccio integrato assicura che il nuovo ambiente sia immediatamente conforme, supportato e pronto per l'esercizio.

**Lotto 2: Fornitura Hardware “Dell”**

Sussiste l'esigenza impellente di acquisire complessivamente 8 server, distribuiti nelle infrastrutture regionali: quattro unità destinate al datacenter di Venezia e quattro unità indirizzate al datacenter di Padova.

Tale dotazione hardware non è finalizzata a una semplice espansione, bensì alla costituzione di un cluster di management robusto e resiliente specificamente progettato per ospitare e gestire l'infrastruttura di virtualizzazione basata su VCF (VMware Cloud Foundation).

L'installazione e la messa in opera di VCF rappresentano un pilastro fondamentale per la modernizzazione e l'efficientamento dei servizi digitali regionali. Senza questo cluster di gestione, non sarebbe possibile procedere all'implementazione di VCF, compromettendo gravemente la capacità di fornire un servizio adeguato, scalabile e sicuro a tutti gli enti che aderiscono al PSR (Polo Strategico Regionale). La mancata adozione in urgenza ritarderebbe l'attivazione dei servizi essenziali previsti dal piano strategico, con potenziali ripercussioni sulla continuità operativa e l'erogazione dei servizi agli enti pubblici e, indirettamente, ai cittadini. (interruzione di pubblico servizio in caso di fault dei sistemi). Si aggiunge a tutto ciò la necessità di rispondere ai requisiti imposti da ACN per l'adeguamento delle infrastrutture e dei servizi cloud della tipologia IaaS e PaaS che Regione del Veneto mette a disposizione delle altre Pubbliche Amministrazioni Locali attraverso il Polo Strategico Regionale.

Parallelamente e in modo sinergico all'acquisto dei server, l'intervento include l'acquisizione di licenze software aggiornate e il rinnovo del supporto della manutenzione (o supporto tecnico) per le apparecchiature Dell già esistenti e operative all'interno dei data center regionali. Questo acquisto combinato risponde all'esigenza critica di garantire la continuità operativa e il corretto funzionamento di tutta l'infrastruttura hardware Dell esistente, il cui supporto tecnico e la relativa manutenzione sono prossimi alla scadenza. Il mancato rinnovo del supporto metterebbe a rischio la stabilità e la sicurezza dell'infrastruttura attuale, rendendo urgente l'azione congiunta di acquisizione del nuovo hardware e contestuale rinnovo dei contratti di supporto per l'esistente.

**Lotto 3: Fornitura hardware “Rubrik”**

Sussiste la necessità di implementare in tempi rapidi un cluster Rubrik dedicato al PSR (Polo Strategico Regionale). Questo cluster è fondamentale per garantire un servizio di backup robusto e affidabile per l'intera infrastruttura del PSR, in particolare per tutte le Macchine Virtuali (VM) che risiedono nei diversi tenant (ambienti isolati) del PSR. L'obiettivo primario è mitigare il rischio di perdita di dati e assicurare un rapido ripristino in caso di incidente.

Attualmente, i servizi di backup si limitano principalmente all'utilizzo di semplici snapshot delle VM. Sebbene le snapshot siano utili per recuperi rapidi, esse presentano delle limitazioni significative in termini di

**REGIONE DEL VENETO**

giunta regionale

granularità e consistenza, soprattutto per i dati strutturati. Il cluster Rubrik dedicato, invece, rappresenta un salto qualitativo nell'erogazione dei servizi di protezione dei dati eseguendo backup consistenti a livello di Database. Questo si ottiene grazie all'impiego di agenti software specifici che, interagendo direttamente con i motori di Database (come ad esempio SQL Server, PostgreSQL, ecc.), garantiscono che il backup catturi lo stato dei dati in un momento in cui tutte le transazioni in sospeso sono completate o in uno stato noto e recuperabile. Ciò è essenziale per la validità dei dati al momento del ripristino, un requisito fondamentale per le applicazioni mission-critical.

In sintesi, l'adozione del cluster Rubrik dedicato non è solo un'espansione della capacità di backup, ma una trasformazione strategica che:

1. Aumentare la resilienza: Fornendo un meccanismo di backup dedicato e scalabile, separato dall'infrastruttura di Giunta Regionale;
2. Migliorare la consistenza: Abilitando backup consistenti tramite agenti, superando i limiti delle semplici snapshot a livello VM;
3. Ottimizzare il recupero (RTO/RPO): Consentendo di definire Recovery Point Objectives (RPO) più aggressivi (minore perdita di dati) e Recovery Time Objectives (RTO) più brevi;
4. Semplificare la gestione: Centralizzando la gestione di backup e recovery su una piattaforma unificata.
5. Permette di adeguarsi al Livello di Sicurezza 2 di ACN (Agenzia per la Cybersecurity Nazionale) mediante l'implementazione di misure di segregazione fisica e logica avanzate per la protezione dei dati dei servizi erogati.

**Lotto 4: Fortinet**

Sussiste la necessità di dare continuità al servizio per tecnologie e strumenti critici legati alla Cybersecurity, quali la VPN (FortiToken) e il WAF (Web Application Firewall). Il mantenimento delle licenze e degli aggiornamenti è essenziale per garantire che questi sistemi continuino a proteggere la nostra infrastruttura da attacchi esterni e per assicurare l'accesso sicuro ai servizi da parte del personale. Un'interruzione in questo ambito comporterebbe un grave rischio di esposizione e potenziali interruzioni di servizio, compromettendo la capacità operativa di Regione del Veneto.

**Lotto 5 (Radware)**

Sussiste l'urgenza e la necessità di garantire un miglioramento continuo del servizio di protezione dagli attacchi informatici. Questo è particolarmente critico in vista delle prossime elezioni regionali, un periodo in cui l'attenzione mediatica sui sistemi regionali è notevolmente innalzata. È imperativo rafforzare le nostre difese per prevenire interruzioni o compromissioni che potrebbero avere ripercussioni significative sulla fiducia pubblica. La protezione da attacchi DDoS e altre minacce avanzate è quindi non solo una questione di routine, ma un'esigenza strategica e temporale che richiede un'azione immediata.

Venezia, 07/11/2025



IL DIRETTORE  
dott. Idelfa Borgo

Area Risorse Finanziarie, Strumentali, ICT ed Enti Locali  
**Direzione ICT, Agenda Digitale e SOS affidamento servizi e forniture ict**  
Centro Vega -Palazzo Lybra -Via Pacinotti n.4 - 30175 Marghera- (Ve) Tel. 041/2792202-2204 - Fax 041/2792218  
ictagendadigitale@regione.veneto.it  
ictagendadigitale@pec.regione.veneto.it

