

1. Scop

Scopul elaborării prezentului Caiet de Sarcini constă în definirea cerințelor tehnice, funcționale, operaționale și de securitate pentru proiectarea, furnizarea, implementarea și punerea în funcțiune a infrastructurii unui centru de date (Data Center), destinat asigurării funcționării continue, sigure și scalabile a sistemelor informaționale critice ale entității.

Documentul are drept obiectiv:

- stabilirea parametrilor tehnici minimi și obligatorii pentru infrastructura IT (servere, stocare, rețea, virtualizare, backup);
- definirea cerințelor privind disponibilitatea, redundanța și continuitatea operațională;
- descrierea cerințelor de securitate fizică și cibernetică;
- stabilirea condițiilor de interoperabilitate cu infrastructura existentă;
- definirea cerințelor privind monitorizarea, administrarea și mentenanța sistemelor;
- asigurarea conformității cu standardele și bunele practici aplicabile în domeniul centrelor de date.

Prezentul Caiet de Sarcini constituie baza tehnică pentru inițierea procedurii de achiziție și evaluarea ofertelor, în vederea selectării unei soluții care să corespundă necesităților operaționale actuale și viitoare ale entității.

№	Marfa	Cantitatea buc.
1.	Infrastructura Servere pentru computing	6
2.	Sistem de stocare All Flash	2
3.	Sistem de stocare Backup	1
4.	Switch Ethernet pentru rețea de datacentru	4
5.	Switch Fibre Channel pentru rețea de datacentru	4
6.	Soft de virtualizare	1

2. Cerință generală de eligibilitate privind securitatea cibernetică și lanțul de aprovizionare aplicabilă tuturor echipamentelor, software-ului, firmware-ului și componentelor de management furnizate

Soluția propusă, inclusiv toate platformele hardware furnizate, sistemele de operare, firmware-ul, software-ul încorporat, software-ul de management, componentele de management cloud / pe bază de abonament, licențele și toate componentele conexe de suport, trebuie să fie furnizată de producători care nu sunt clasificați, identificați sau tratați în mod public drept furnizori cu risc ridicat pentru domeniul TIC critic, telecomunicații, rețele, centre de date sau infrastructură critică de către instituțiile Uniunii Europene, Grupul de cooperare NIS, ENISA, autoritățile competente ale statelor membre ale UE, ale statelor membre NATO sau ale altor jurisdicții care aplică cadre echivalente de evaluare a riscurilor de securitate cibernetică și securitate națională.

Nu vor fi acceptate echipamente, firmware, sisteme de operare, platforme de management, componente OEM / white-label / rebranduite sau soluții provenite de la producători care fac obiectul unor restricții publice, decizii de excludere, interdicții de achiziție, măsuri obligatorii de eliminare treptată sau măsuri aplicabile furnizorilor cu risc ridicat în infrastructura critică, din motive legate de securitate cibernetică, securitate națională, securitatea lanțului de aprovizionare, influență a unor state terțe sau control exercitat de un stat străin.

Ofertantul va prezenta o declarație prin care confirmă că echipamentele propuse și toate componentele esențiale hardware, software, firmware, software încorporat, management, suport și abonament nu sunt furnizate, dezvoltate, controlate sau menținute de un astfel de furnizor restricționat sau cu risc ridicat, nici direct, nici prin aranjamente OEM / white-label / rebranduite, prin entități afiliate sau prin orice alt aranjament indirect de furnizare.

La solicitare, ofertantul va prezenta documentație oficială a producătorului și/sau referințe publice de reglementare care confirmă conformitatea cu această cerință.

3. Caracteristici tehnice

INFRASTRUCTURA CENTRULUI DE DATE				
Cod CPV	Denumirea bunurilor/serviciilor	Un. de masura	Cant.	Specificarea tehnică deplină solicitată de către autoritatea contractantă
COMPARTIMENTUL SERVERE				
30232110-8	Infrastructura Servere pentru computing	buc	6	Computing Server
				Manufacturer eligibility and cybersecurity supply-chain risk: The proposed equipment shall comply with the general cybersecurity and supply-chain eligibility requirements applicable to all components of the proposed data-center infrastructure
				Manufacturer / Brand: rackmount server supplied by an internationally recognized enterprise server manufacturer.
				Form factor: rack-mount chassis, max. 2U.
				Processor: 2 installed current-generation enterprise-class processors, minimum 32 cores per processor, aggregate cache capacity of at least 280 MB; support for DDR5-6400 memory.
				Memory: min. 512 GB DDR5-6400 RDIMM installed. The platform shall support memory expansion through at least 32 DIMM slots; at least 16 DIMM slots shall remain free in the offered configuration.
				Boot disks: min. 2x 480 GB enterprise NVMe SSD installed and configured in RAID 1 for the hypervisor, using the manufacturers officially supported NVMe boot / RAID configuration.
				Ethernet adapter: min. 2x 10/25GbE SFP28 ports with support for RoCEv2, NVMe over TCP, VXLAN/VLAN offload or equivalent functions; minimum 2 compatible 10/25Gb SFP28 AOC cables, 3 m, shall be included.
				HBA: min. 2x 32Gb FC SFP+ ports with support for NVMe over FC, multipath, NPIV and certified drivers for the proposed hypervisor; min. 2 original or certified 32Gb FC short-wave transceivers shall be included.
				Platform security: hardware TPM 2.0; Secure Boot and firmware protection mechanisms according to the manufacturer's capabilities.
				Expansion: min.3x PCIe x16 Gen5 slots or equivalent and min. 2x OCP / LOM slots supporting different controllers / adapters.
				Cooling: redundant hot-swap fans - the maximum quantity supported by the proposed platform.
				Power supply: 2x redundant hot-swap power supplies, min. 1600W each or sized by the manufacturer for the proposed configuration, efficiency not lower than Platinum / 94%; power cords shall be included.
Management interfaces: dedicated Ethernet management port, local / serial console or equivalent, min. 2x USB 3.0 ports or equivalent.				
Administration/Management: remote KVM for each server, centralized management for all servers, firmware / update policies, security policies, automation / orchestration of operations; all required licenses shall be included for the required support period.				
Security / cryptographic compliance: the proposed equipment shall provide enterprise-grade cryptographic protection for platform security, secure management, TPM, protected communication channels, authentication, credential protection, firmware integrity control and drive encryption, where such functions are applicable in the proposed configuration. Cryptographic functions used for these purposes shall be based on cryptographic modules validated under FIPS 140-2 or FIPS				

				<p>140-3, or officially declared by the manufacturer as compliant with FIPS 140-2 / FIPS 140-3 requirements. This requirement applies to the relevant cryptographic and security functions of the equipment and shall not be interpreted as a requirement for FIPS validation of the entire server platform as a single device.</p> <p>Warranty and support: the proposed equipment shall be supplied with official manufacturer service support for at least 3 years, including access to software and firmware updates, 24/7 technical support, and on-site service with replacement of failed equipment or components on site, according to the manufacturer's official support terms.</p> <p>Support registration and confirmation: the equipment shall be registered on the official manufacturer support portal and attached to the final beneficiary / customer profile for access to updates, security notifications, technical recommendations, service entitlement management and future support renewals. The bidder shall provide an official document issued by the manufacturer or authorized manufacturer representative confirming the availability of the declared support level for the proposed equipment under this procurement. The document shall specify the support terms, support period, service type, support territory and the manufacturer's area of responsibility, and shall explicitly confirm that warranty and service support is provided directly by the manufacturer or through its official / authorized service partners, while the manufacturer remains responsible for fulfilling the relevant warranty and service obligations.</p>
COMPARTIMENTUL STOCARE ŞI BACKUP				
30232110-8	Sistem de stocare All Flash	set	1	<p>2x Enterprise All Flash storage system</p> <p>Manufacturer eligibility and cybersecurity supply-chain risk: The proposed equipment shall comply with the general cybersecurity and supply-chain eligibility requirements applicable to all components of the proposed data-center infrastructure</p> <p>Manufacturer / Brand: Internationally recognized enterprise storage manufacturer</p> <p>Purpose: Enterprise All Flash storage system for critical virtualized enterprise workloads, based on enterprise NVMe flash media / NVMe SSD / NVMe flash modules officially supported by the manufacturer</p> <p>Architecture: High-availability architecture with at least 2 controllers / controller nodes / storage nodes / HA-pair or equivalent manufacturer architecture, automatic failover, no single point of failure, redundant data path and management path, non-disruptive maintenance / upgrade.</p> <p>Form factor: Rackmount design. Base controller system / HA-system / controller-node configuration max. 4U, excluding external disk shelves / expansion shelves used for capacity expansion</p> <p>Media: Enterprise NVMe SSD TLC certified by the manufacturer for primary enterprise production workloads</p> <p>Initial capacity: Min. 12x 3.84 TB enterprise NVMe SSD SED / hot-swap per system, or equivalent raw capacity based on enterprise NVMe flash media / NVMe flash modules. Data-at-rest encryption must be supported at disk, controller, storage-system level or by an equivalent manufacturer mechanism</p> <p>Capacity scalability: Expandable to min. 2 PB raw capacity, according to the manufacturer's official architecture.</p> <p>Host ports / interfaces: Support for Ethernet 10/25GbE or higher with NVMe over TCP, and Fibre Channel 32Gb or higher with FC and NVMe over FC. All required host adapters, optical modules, transceivers and licenses for project connectivity shall be included. The supplied configuration shall provide redundant connectivity for all servers, SAN / Ethernet fabric, storage fabric and backup systems. After connecting all required components, at least 25% of activated front-end host ports shall remain free</p>

			<p>Host-connectivity scalability: The controller platform shall support scaling up to at least 32 front-end host ports per storage system, without controller platform replacement and without mandatory data migration. Supported host-port types shall include FC 32/64Gb and Ethernet 10/25GbE or higher, with NVMe over FC and NVMe over TCP support.</p> <p>Expansion resources: The controller platform shall provide at least 16 combined physical PCIe expansion slots / I/O adapter slots / I/O module positions / controller-node adapter positions, or an equivalent manufacturer-certified physical expansion mechanism, for host-connectivity, back-end connectivity, service / replication connections and/or controller-resource expansion. Front-end host ports, logical ports, licensed ports, protocol endpoints, transceivers, optical modules and already-installed fixed onboard ports shall not be counted as separate expansion resources unless they correspond to physical PCIe expansion slots, I/O adapter slots, I/O module positions or controller-node adapter positions documented by the manufacturer for the proposed controller platform</p> <p>Block protocols: NVMe over TCP, NVMe over FC, iSCSI and Fibre Channel shall be included and licensed for hypervisor connectivity, datastores, servers, SAN / Ethernet fabric, replication and metro / stretched storage scenarios</p> <p>NAS / file services: The primary storage shall support NAS / file services in addition to block access. NFSv4.1 or higher shall be included and licensed. NAS / file functionality may be native or provided through an integrated file services / NAS component from the same manufacturer, officially certified and supported with the proposed primary storage. If a separate file services / NAS component is used, it must be part of the same enterprise storage architecture, with unified manufacturer support, centralized management and monitoring, redundant data path / management path and no single point of failure. Generic NAS servers not officially supported as part of the proposed enterprise storage architecture shall not be accepted as equivalent.</p> <p>Storage features: Thin provisioning, inline or post-process deduplication and compression, volume / LUN resize, volume / LUN clone, volume / LUN QoS, snapshots, synchronous and asynchronous replication, hypervisor integration and backup software integration shall be included and licensed.</p> <p>Metro / stretched cluster: Support for metro cluster / stretched storage cluster / active-active / synchronous replication with automatic or transparent failover, or equivalent manufacturer functionality, at least for the block protocols used in the project</p> <p>Ransomware protection: Immutable snapshots / retention lock / tamper-proof snapshots, anomaly detection and alerting to monitoring system / SIEM, or equivalent manufacturer functionality, shall be included and licensed</p> <p>Non-disruptive scalability: The system shall support capacity, performance, front-end connectivity, back-end connectivity and/or controller-resource expansion by adding NVMe shelves, expansion shelves, controller nodes, storage nodes, HA-pairs, adapter modules or equivalent components, without planned downtime for connected hosts / datastores and without mandatory data migration to a new storage system</p> <p>Redundancy: Redundant controllers / controller nodes / storage nodes / HA-components, fans, power supplies, data path, management path and back-end connectivity. Back-end connections between controllers, shelves, nodes and/or expansion modules shall be redundant and sized by the manufacturer for the declared performance and scalability</p> <p>FIPS / cryptographic modules: Cryptographic functions used for secure management, encryption at-rest, protected replication, authentication, secure communication channels or other security functions shall use cryptographic modules validated under min. FIPS 140-2 or officially declared by the manufacturer as compliant with FIPS 140-2 minimum. This</p>
--	--	--	---

			<p>requirement applies only to relevant cryptographic modules and security functions and is not a requirement for FIPS validation of the entire storage system as a single device</p> <p>Management and monitoring: Included management and monitoring solution for day-one operation, showing at least latency, IOPS, throughput, disk / flash media status, cache / memory resources, host ports, back-end ports, volumes / LUNs / shares, events, alerts and proactive recommendations. Support for failure notifications, proactive health monitoring, update recommendations, capacity planning and integration with external monitoring systems and/or SIEM through API, SNMP, syslog or equivalent supported mechanisms</p> <p>Warranty and service: Minimum 3 years of official manufacturer support, including access to software and firmware updates, vendor support 24/7, on-site replacement / on-site support of failed equipment or components according to the manufacturer's official terms. The support SLA shall correspond to the proposed manufacturer support level and shall be confirmed by an official document from the manufacturer or authorized manufacturer representative. The equipment shall be registered on the official manufacturer support portal and assigned to the profile of the final beneficiary / customer in order to receive updates, security notifications, technical recommendations, service entitlement management and subsequent support renewal</p> <p>Service support confirmation: The bidder shall provide an official document from the manufacturer or authorized manufacturer representative confirming the availability of the declared service support level for the proposed equipment under this procurement. The document shall specify the support terms, validity period, type of service, support territory and manufacturer's area of responsibility, and shall explicitly confirm that warranty and service support is provided by the manufacturer directly or through its official / authorized service partners, while the manufacturer remains responsible for fulfilling the relevant warranty and service obligations.</p>
30232110-8	Sistem de stocare Backup	buc	<p>Backup Storage System</p> <p>Manufacturer eligibility and cybersecurity supply-chain risk: The proposed equipment shall comply with the general cybersecurity and supply-chain eligibility requirements applicable to all components of the proposed data-center infrastructure</p> <p>Manufacturer / Brand: Internationally recognized enterprise storage manufacturer</p> <p>Purpose: Enterprise block SAN storage system intended for use as storage capacity for backup repository servers within the backup infrastructure</p> <p>Architecture: Dual-active enterprise storage controller architecture with two hot-swappable controllers in the same storage system, automatic controller failover, redundant host paths and no single point of failure for block storage access. The system shall support uninterrupted LUN / volume access through the surviving controller in case of failure of one controller</p> <p>Form factor: Rackmount chassis, max. 2U for the base storage system.</p> <p>Drive bays: Minimum 12 hot-swap drive slots for enterprise HDD / SSD media. The system shall support expansion through expansion units to at least 36 drives or equivalent documented raw capacity.</p> <p>Drive media: The system shall use enterprise dual-port SAS / NL-SAS HDDs and/or SAS SSDs officially supported by the storage manufacturer. SATA drives, desktop-class drives, NAS-class drives or drives not certified by the storage system manufacturer shall not be accepted. All delivered drives shall be hot-swap and accessible through redundant controller paths according to the manufacturer architecture.</p>

			<p>Delivered capacity and SSD acceleration: Minimum raw capacity equivalent to 12x 14 TB enterprise HDD. The storage configuration shall additionally include at least 2 x enterprise SSD drives officially supported by the storage manufacturer for SSD cache / read cache / performance tier / acceleration / dedicated SSD tier or other manufacturer-supported performance acceleration use within the proposed enterprise storage array. All delivered HDD and SSD drives shall be hot-swap, officially supported / certified by the manufacturer for the proposed storage system and accessible through redundant controller paths according to the manufacturer architecture. SSD drives used only as generic NAS cache in an all-in-one NAS appliance shall not be considered equivalent.</p> <p>Host connectivity: Minimum 4x 16/32Gb Fibre Channel host ports with compatible short-wave FC transceivers included. Fibre Channel connectivity shall be officially supported by the manufacturer for the proposed storage system and implemented through storage controller host ports / controller I/O modules documented by the manufacturer for the proposed enterprise storage array. The Fibre Channel connectivity shall support redundant block SAN access, LUN / volume presentation, zoning and multipath operation. Optional Fibre Channel functionality implemented through general-purpose server / NAS add-on adapters shall not be used as a substitute for the required controller-based Fibre Channel SAN connectivity</p> <p>Block access and multipath: The system shall provide native block storage access through Fibre Channel, with support for LUN / volume presentation to backup repository servers and redundant multipath access. All required licenses and components for redundant FC block access shall be included</p> <p>Controller cache protection: The system shall support mirrored write cache between storage controllers with non-volatile / flash-backed / power-loss protected cache protection, or an equivalent manufacturer mechanism preventing data loss in case of controller or power failure.</p> <p>Backup integration: The solution shall be suitable for integration with the existing Veeam Backup & Replication platform as repository storage through Fibre Channel block connectivity to backup / repository servers. SMB / NFS / NAS access shall not be considered a substitute for the required Fibre Channel block connectivity.</p> <p>RAID / data protection: The system shall support enterprise RAID / parity-based data protection suitable for large-capacity drives of 14 TB or higher, with manufacturer-supported mechanisms for spare capacity, rebuild control and reduction of rebuild impact on system availability and performance.</p> <p>Data-at-rest encryption: The system shall support data-at-rest encryption / protection using AES-256 encryption, SED / FDE drives, storage-level encryption or equivalent manufacturer-supported mechanism. If encryption is implemented at the storage level, all required SED / FDE drives, licenses, keys / key-management components and configuration elements required for enabling encryption shall be included. All delivered encrypted drives shall be officially supported / certified by the storage manufacturer for the proposed system.</p> <p>Backup immutability: The solution shall allow implementation of immutable repository, retention lock, WORM or equivalent protection against unauthorized modification or deletion of backup data. Such protection may be implemented at storage system, backup software, operating system, file system, dedicated repository server or backup appliance level</p> <p>Management: Dedicated Ethernet management interface or equivalent out-of-band / in-band management mechanism according to the manufacturer architecture. Web-based management interface and/or CLI/API shall be supported. Support for SNMP, email alerts, syslog, vendor management</p>
--	--	--	---

				<p>tools or equivalent monitoring and notification mechanisms shall be provided</p> <p>Redundancy: Redundant hot-swap power supplies shall be included. Power cords shall be included. Controllers, data paths, fans and expansion paths shall be redundant according to the proposed manufacturer architecture</p> <p>Veeam Backup integration: The storage system shall be suitable for integration with the existing Veeam Backup & Replication platform as repository storage via Fibre Channel block connectivity to the backup / repository server, with LUN / volume presentation, redundant FC paths and multipath access. Integration may be implemented at repository server / OS / file system / backup software level. SMB / NFS / NAS access shall not be considered a substitute for the required FC block connectivity</p> <p>Warranty and support: The proposed equipment shall be supplied with official manufacturer service support for at least 3 years, including access to software and firmware updates, vendor technical support, and on-site service with replacement of failed equipment or components on site, according to the manufacturer's official support terms</p> <p>Support registration and confirmation: The equipment shall be registered on the official manufacturer support portal and attached to the final beneficiary / customer profile for access to updates, security notifications, technical recommendations, service entitlement management and future support renewals. The bidder shall provide an official document issued by the manufacturer or authorized manufacturer representative confirming the availability of the declared support level for the proposed equipment under this procurement. The document shall specify the support terms, support period, service type, support territory and the manufacturer's area of responsibility, and shall explicitly confirm that warranty and service support is provided directly by the manufacturer or through its official / authorized service partners, while the manufacturer remains responsible for fulfilling the relevant warranty and service obligations</p>
COMPARTIMENTUL REȚEA ȘI CONECTIVITATE				
30232110-8	Switch Ethernet pentru rețea de datacentru	buc	4	<p>Data-Centre Ethernet Switch</p> <p>Manufacturer eligibility and cybersecurity supply-chain risk: The proposed equipment shall comply with the general cybersecurity and supply-chain eligibility requirements applicable to all components of the proposed data-center infrastructure</p> <p>Manufacturer / Brand: The equipment shall be supplied by an internationally recognized manufacturer of enterprise and/or data-center networking equipment</p> <p>Chassis: 19" rackmount chassis, maximum 1U / 1.2U, with rackmount kit included</p> <p>Architecture: The switch shall provide redundant, non-blocking / line-rate architecture with low-latency forwarding performance and shall be suitable for deployment as a leaf / top-of-rack / aggregation switch in a data-center Ethernet fabric. The switch shall support advanced L2/L3 functionality required for redundant data-center networking, server connectivity, storage connectivity, virtualization platforms, backup infrastructure and VXLAN EVPN fabric deployment.</p> <p>Ports: Minimum 48x 1/10/25GbE SFP28 ports and minimum 6x 40/100GbE QSFP28 ports. Switches with a higher number of 40/100GbE QSFP28 uplink ports shall be accepted as equivalent or superior.</p> <p>Included optical modules and cables: The delivery shall include at least</p> <ul style="list-style-type: none"> ▪ 24x 10/25GbE SFP28 LR 10 km modules; ▪ 8x 10/25GbE SFP28 SR 100 m modules; ▪ 2x 100GbE QSFP28 LR 10 km modules; ▪ 2x 100GbE QSFP28 AOC / DAC 3 m modules/cables.

			<p>All optical modules, transceivers and cables shall be original, vendor-certified or officially supported by the switch manufacturer for the proposed switch model.</p> <p>Performance: min. switching capacity of 4.8 Tbps; min. forwarding performance of 1.8 Bpps / 1,800 Mpps; non-blocking / line-rate performance for the proposed port configuration; support for lossless Ethernet mechanisms required for virtualization, storage traffic and RDMA-related traffic.</p> <p>Packet buffer: Min. 32MB packet buffer or equivalent buffering architecture validated by the manufacturer as suitable for data-center, storage, virtualization and lossless Ethernet workloads</p> <p>Scalability: min. 500,000 IPv4 unicast routes, or an equivalent manufacturer-confirmed L3 scalability profile suitable for data-center leaf / aggregation deployment; min. 90,000 MAC address entries. <i>The above scalability parameters shall be confirmed by official manufacturer documentation.</i></p> <p>L2/L3 and Ethernet fabric features: All following features shall be supported and licensed, where licensing is required</p> <ul style="list-style-type: none"> ▪ VLAN tagging IEEE 802.1Q; ▪ LACP / port-channel / link aggregation; ▪ trunking; ▪ STP / RSTP / MSTP or equivalent loop-prevention mechanisms; ▪ jumbo frames; ▪ ACL; ▪ QoS; ▪ static routing; ▪ OSPF; ▪ BGP / MP-BGP; ▪ VXLAN with BGP EVPN control plane; ▪ VRF or equivalent traffic segmentation; ▪ multicast support; ▪ LLDP; ▪ UDLD or equivalent unidirectional link / link-failure detection mechanism; ▪ DCB / PFC / ECN / DCBX / RoCEv2-related or equivalent lossless Ethernet functionality. <p>Multi-chassis link aggregation: vPC, MC-LAG, VSX, MLAG or equivalent technology enabling LACP links to two independent switches without mandatory stacking and with independent control planes</p> <p>Licenses: All licenses required for the requested L2/L3, VXLAN EVPN, MLAG / VSX / vPC or equivalent, QoS, lossless Ethernet, security, automation, telemetry and monitoring functions shall be included in the offered price. The right to use the requested functions shall be perpetual or valid for the entire proposed support period (min. 5 Years), without requiring additional mandatory subscriptions for the basic operation of the proposed data-center fabric. Vendor support subscriptions are accepted if included in the proposed support package.</p> <p>Redundant fabric operation: The switch shall support multi-chassis link aggregation or equivalent high-availability technology, including MLAG / VSX / vPC or equivalent, allowing redundant connection of servers, storage systems and upstream/downstream network devices without a single point of failure</p> <p>Security and MACSec / link encryption: The switch shall support secure management via SSHv2, HTTPS/TLS, SNMPv3, role-based access control, RADIUS and/or TACACS+, event logging and integration with external monitoring / SIEM systems. The switch shall support IEEE 802.1AE MACSec / AES-256 or equivalent hardware-based link encryption on at least 2 x 40/100GbE QSFP28 uplink / backbone ports intended for inter-switch, backbone, inter-site</p>
--	--	--	--

			<p>or other connections exposed to a potentially untrusted environment.</p> <p>FIPS / cryptographic compliance: FIPS 140-2 / FIPS 140-3 requirements shall apply to the relevant cryptographic modules used for secure management, authentication, encrypted communication, MACSec / link encryption or other cryptographic functions, according to official manufacturer documentation</p> <p>Automation, monitoring and telemetry: The switch shall support out-of-band management, dedicated console port, minimum 1 x 100/1000Base-T management port, REST API or equivalent programmable interface, SNMP, sFlow / NetFlow / IPFIX or equivalent telemetry and monitoring mechanisms.</p> <p>Management: Dedicated console port and minimum 1 x 100/1000Base-T out-of-band management port</p> <p>Redundancy: Minimum 1+1 hot-swappable power supplies and hot-swappable fans with N+1 redundancy. <i>Airflow direction shall be suitable for the proposed rack layout</i></p> <p>Warranty and support: Minimum 3 years of official manufacturer support, including software / firmware updates, Next Business Day hardware replacement and vendor support. The equipment shall be registered on the official vendor support portal and attached to the final beneficiary / customer profile for access to support renewals, updates, notifications and recommendations. The bidder shall provide an official document from the manufacturer or authorized manufacturer representative confirming the availability and conditions of the proposed support level for the offered equipment under this procurement. The document shall specify the support term, service type, support territory and manufacturer responsibility, and shall explicitly confirm that warranty and service support is provided by the manufacturer directly or through its official / authorized service partners, while the manufacturer remains responsible for fulfilling the relevant warranty and service obligations</p>
30232110-8	Switch Fibre Channel pentru reţea de datacentru	buc	<p>Storage Area Network (SAN) Fibre Channel switch</p> <p>Manufacturer / Brand: Internationally recognized enterprise SAN / Fibre Channel switching manufacturer</p> <p>Manufacturer eligibility and cybersecurity supply-chain risk: The proposed equipment shall comply with the general cybersecurity and supply-chain eligibility requirements applicable to all components of the proposed data-center infrastructure</p> <p>Chassis: rackmount chassis 19" with included rackmount kit.</p> <p>Architecture: Enterprise SAN switch architecture with non-blocking / line-rate Fibre Channel switching, low latency, redundant fabric operation and suitability for mission-critical storage, virtualization and backup workloads</p> <p>Ports : Minimum 24 x 64Gb Fibre Channel ports. At least 8 ports shall be activated and licensed in the supplied configuration. The switch shall support further port activation up to the requested port count without replacing the chassis. Min. 8 x 32Gb or 64Gb Fibre Channel short-wave transceivers and minimum 1 x 64Gb Fibre Channel long-wave 10 km transceiver must be included. All supplied transceivers shall be original, vendor-certified or officially supported by the switch manufacturer for the proposed switch model.</p> <p>Fabric features: The following features shall be supported and licensed, where licensing is required: Fibre Channel zoning, ISL / E-port fabric connectivity, trunking or equivalent link aggregation, FEC or equivalent link reliability mechanism, QoS / traffic prioritization, fabric segmentation through VSAN / Virtual Fabrics / logical switch / fabric partitioning or equivalent manufacturer functionality.</p> <p>NVMe over FC: The switch shall support NVMe over Fibre Channel for connectivity between proposed servers, SAN fabrics and primary storage systems.</p>

				<p>NPIV / access gateway: The switch shall support NPIV and NPV / Access Gateway / F-port trunking or equivalent manufacturer functionality for scalable and redundant server-to-fabric connectivity.</p> <p>In-flight encryption: The switch shall support AES-256 or equivalent in-flight encryption for inter-switch / fabric links, where such encryption is used in the proposed architecture. If additional licenses are required for this functionality, they shall be included</p> <p>Licenses: All licenses required for the requested port activation, fabric services, zoning, ISL / trunking, QoS, NVMe over FC, NPIV / access gateway functionality, security, monitoring and management features shall be included in the offered price. Licenses shall be perpetual or valid for the entire proposed support period. If the manufacturer provides such licenses only as subscription-based licenses, the subscription period shall be at least 5 years.</p> <p>Management: Dedicated console port and minimum 1 x 100/1000Base-T out-of-band management port. The switch shall support secure management through HTTPS / TLS, SSH, SNMPv3 or equivalent secure management mechanisms.</p> <p>Monitoring and diagnostics: The switch shall support fabric monitoring, port statistics, event logs, alerts, diagnostics, SNMP / syslog or equivalent integration with external monitoring systems.</p> <p>Redundancy: Minimum 1+1 hot-swappable power supplies and redundant hot-swappable fans with N+1 or equivalent redundancy. Airflow direction shall be suitable for the proposed rack layout. Power cords shall be included.</p> <p>FIPS / cryptographic compliance: For cryptographic functions used for secure management, authentication, encrypted communication, in-flight encryption or other security functions, cryptographic modules validated under min. FIPS 140-2 or officially declared by the manufacturer as compliant with min. FIPS 140-2 requirements shall be used. This requirement applies only to relevant cryptographic modules and security functions and shall not be interpreted as a requirement for FIPS validation of the entire switch as a single device.</p> <p>Certifications and compliance: The equipment shall comply with applicable CE requirements and manufacturer quality / environmental management standards, where applicable</p> <p>Warranty and support: Minimum 5 years of official manufacturer support, including access to software / firmware updates, vendor support and Next Business Day hardware replacement or better according to the manufacturer's official support terms</p> <p>Support registration and confirmation: The equipment shall be registered on the official manufacturer support portal and attached to the final beneficiary / customer profile for access to support renewals, updates, security notifications and technical recommendations. The bidder shall provide an official document from the manufacturer or authorized manufacturer representative confirming the availability of the declared support level for the proposed equipment under this procurement. The document shall specify the support term, service type, support territory and manufacturer responsibility, and shall confirm that warranty and service support is provided directly by the manufacturer or through its official / authorized service partner</p>
COMPARTIMENTUL SOFT				
30232110-8	Soft de virtualizare	buc	1	<p>Virtualization software</p> <p>Type: Bare-metal virtualization platform with support for hardware-assisted virtualization on the CPUs of the proposed computing servers</p> <p>Hardware compatibility: The virtualization software shall be officially certified / supported by the virtualization software vendor for operation on the proposed server hardware.</p>

				<p>Guest operating systems: The platform shall support at least the following guest operating systems: Windows Server 2016, 2019, 2022, 2025; SUSE Linux; Ubuntu Linux; Red Hat Enterprise Linux; CentOS Linux; Microsoft Windows 11 Pro.</p> <p>Primary storage integration: The virtualization software shall support the proposed Primary Storage Metro / stretched cluster via at least NVMe over Fibre Channel protocol.</p> <p>External datastore support: The virtualization software shall support datastores on external storage through iSCSI, Fibre Channel and NFSv4 or higher.</p> <p>Management console availability: The virtualization management console shall support High Availability mode in active-passive or active-active configuration.</p> <p>Core virtualization features: The platform shall include and license the following functions: Virtual Machine HA, Virtual Machine Live Migration, Distributed Switch, Distributed Resource Scheduler or equivalent resource-balancing mechanism, VM snapshots and vTPM 2.0.</p> <p>Zero-downtime VM migration: The platform shall support migration of running virtual machines from one host to another with zero downtime.</p> <p>Zero-downtime storage migration: The platform shall support migration of running virtual machines from one datastore to another with zero downtime.</p> <p>Automation and scripting: The platform shall support execution of scripts, including shell, bash, PowerShell or equivalent, during VM provisioning, maintenance or automation workflows.</p> <p>Storage-based snapshots: The virtualization software shall support native or officially certified integration for creating storage-based snapshots of virtual machines on the proposed Primary Storage Metro / stretched cluster.</p> <p>Backup integration: The virtualization software shall be natively integrated or officially supported for integration with the existing Veeam Backup & Replication platform.</p> <p>Security and identity integration: The platform shall support Multi-Factor Authentication and integration with Microsoft Windows Active Directory.</p> <p>Licensing: The virtualization software shall be licensed for all CPU cores or sockets installed in the proposed computing servers, according to the vendor's licensing model. The license shall be perpetual with minimum 3 years of vendor support, or subscription-based with license and support included for at least 5 years.</p> <p>Vendor support: Vendor support shall be included with 24/7/365 availability for the required support period</p>
COMPARTIMENTUL LUCRĂRI ȘI SERVICII ASOCIATE				
30232110-8	Lucrări de instalare și configurare echipamente	set	1	<p>Physical installation of the equipment in racks, connection of power supply, labeling of equipment and cables, configuration of servers and the centralized server management and monitoring system, configuration of the primary storage in metro cluster mode, configuration of the virtualization system, configuration of network equipment and connection of such equipment to the airport network, configuration of a VXLAN fabric, VLANs, OSPF, BGP EVPN and network traffic filtering rules, configuration of two independent Fibre Channel fabrics, and migration of virtual and physical machines from the existing airport infrastructure.</p> <p>Configuration of the backup system and its connection to the hypervisor and storage, including testing of various data center fault-tolerance scenarios.</p>
30232110-8	Instruire personal IT	ore	20	Technical training for IT personnel on platform administration, monitoring and maintenance, with a certificate of participation.
30232110-8	Suport tehnic post-implimentare	luni	12	Remote / telephone support for questions, troubleshooting and consulting, with local interventions in emergency cases for 12 months after delivery, available 24/7 and included in the warranty.

1. Statut de partener oficial in Republica Moldova al fiecărui producător al componentelor soluției oferite.
2. Confirmarea autenticității produselor, a provenienței legale și a dreptului de livrare, suport și garanție pentru soluția oferită, prin documente emise de producător, distribuitor oficial, partener autorizat sau altă entitate abilitată în lanțul oficial de distribuție/suport.
3. Confirmarea capacității de prestare a serviciilor de garanție, suport tehnic și mentenanță pentru fiecare tip de echipament oferit, pe teritoriul Republicii Moldova, direct sau prin parteneri/centre de service autorizate, cu respectarea nivelurilor minime de serviciu solicitate.
4. Min 1 proiect realizat in ultimii 3 ani cu produse similare, de complexitate similara si suma nu mai puțin decât 60% ale ofertei