Ítem No.	1
Unidad de Medida	Unidad

SERVIDORES DE ÚLTIMA GENERACIÓN, JUNTO CON SUS COMPONENTES DE EXPANSIÓN, LICENCIAS DE GESTIÓN Y SOPORTE TÉCNICO ESPECIALIZADO

Item	Descripción del Requerimiento
Chasis	Montaje en rack de 1U
Soporte Ambiental	Enfriado por aire
CPU	Dos números de procesador Intel® Xeon® 6 6505P 2.2GHz 12-core 150W Processor
Memoria	Ranuras 32DIMM. 256GB con DIMMS de 32 GB escalables hasta 4,0 TB mediante DIMM registrado DDR5 (RDIMM) que funciona a 6400 MT/s
Protección de memoria	ECC avanzado, duplicación de memoria, tolerancia rápida a fallas, depuración de memoria
Bus Slots	El servidor debe admitir hasta tres ranuras PCI-Express 5.0 x16. Dos ranuras OCP x8/x16 o superiores adicionales
Almacenamiento optimizado para BOOT	Canitidad 2 x 960GB M.2 NVMe SED Hot Plug Boot Optimized Storage in RAID 1
Bahías de disco duro	Canitidad 10 x 960GB SATA 6G Read Intensive SFF BC Multi Vendor SSD
Controlador	El servidor debe admitir uno de los siguientes controladores, debe admitir el modo mixto que combina el funcionamiento del modo RAID y HBA simultáneamente::
Funciones de red	El servidor debe incluir las siguientes tarjetas de red: Cantidad 2 - Tarjetas Broadcom BCM57504 Ethernet 10/25Gb 4-port SFP28, incluyendo 4 unidades x ┌10GBase-T SFP+ Transceiver
Funciones de red	Cantidad 6 - Unidades x 10Gb SFP+ LR Transceiver
Funciones de red	Cantidad 1 - tarjetas Broadcom BCM57416 Ethernet 10Gb 2-port BASE-T
Funciones de red	Cantidad 1- Tarjeta Broadcom BCM5719 Ethernet 1Gb 4-port BASE-T OCP3
Interfaces	Puerto serie 1 (opcional) Puertos VGA 1 trasero, 1 delantero (opcional) Soporte USB 3.2 con hasta 5 en total: 1 frontal, 2 trasero, 2 internos. Puerto de administración dedicado de 1 GbE
Fuente de alimentación	Debe admitir fuentes de alimentación redundantes de conexión en caliente con una eficiencia mínima del 94%.
Fuente de alimentación	Debe admitir fuentes de alimentación redundantes de conexión en caliente con una eficiencia mínima del 96%. 800W Flex Slot Platinum Hot Plug Low Halogen Power Supply Kit
Fans	Ventiladores redundantes del sistema de conexión en caliente

Cumplimiento de los estándares de la industria	ACPI 6.5 Compliant PCIe 5.0 Compliant WOL Support Microsoft® Logo certifications PXE Support USB 3.2 Gen1 Compliant UEFI (Unified Extensible Firmware Interface Forum) Class 3 Support Embedded TPM Support Energy Star 4.0 SMBIOS 3.7 Redfish API IPMI 2.0 Advanced Encryption Standard (AES) SNMP v3 TLS 1.2 DMTF Redfish support for Secure Boot Key Management Active Directory v1.0 ASHRAE A3/A4
Seguridad del sistema	Seguridad de datos del servidor mejorada: cifrado y administración de claves, cifrado administrado por UEFI y unidades de autocifrado (SED) para una protección mejorada de los datos en reposo. Desinfecte los datos con borrado con un botón: debe cumplir con NIST SP 800-88. Debe ser compatible con FIPS 140-3, NIST SP 800-53, NIST SP 800-171 y NIST SP 800-88. Must proporciona una experiencia operativa intuitiva en la nube, lo que garantiza operaciones optimizadas y altamente seguras desde el borde hasta la nube. Opciones de seguridad física: interruptor de mantenimiento del sistema, seguridad USB, bloqueo de bisel e interruptor de detección de intrusiones en el chasis. Los servidores deben construirse utilizando una cadena de suministro confiable para someterse a inspecciones y puntos de control rigurosos para detectar y mitigar microcódigos maliciosos y piezas falsificadas a lo largo de la construcción y el ciclo de vida del servidor El servidor debe ofrecerse con el módulo de plataforma segura (TPM) 2.0. Compatibilidad con arranque seguro UEFI e inicio seguro Actualizaciones sin manipulaciones: componentes firmados y verificados digitalmente Raíz de confianza de silicio inmutable Capacidad para revertir el firmware Recuperación segura: recupere el firmware crítico a un buen estado conocido al detectar firmware comprometido
Operating Systems and Virtualization Software Support	Windows Server. Red Hat Enterprise Linux (RHEL) SUSE Linux Enterprise Server (SLES) VMware ESXi. VM Essentials Canonical Ubuntu Oracle Linux and Oracle KVM
Seguridad del firmware	1. Debe mantener un repositorio de recetas de firmware y controladores para ayudar a revertir o parchear el firmware comprometido. También debe almacenar la receta de recuperación de fábrica precargada para revertir al firmware seguro probado de

Gestión remota integrada	1. La administración remota del sistema debe admitir la consola remota gráfica basada en navegador junto con el botón de encendido virtual, el arranque remoto mediante una unidad USB / CD / DVD. Debe ser capaz de ofrecer la actualización de software y parches desde un cliente remoto utilizando Media/image/folder; Debe admitir la limitación de energía del servidor y los informes históricos y debe tener soporte para la autenticación multifactor 2. El servidor debe tener un puerto de administración remota dedicado de 1 Gbps 3. El servidor debe admitir la administración sin agente mediante el puerto de administración remota fuera de banda 4. El servidor debe admitir el monitoreo y el registro de cambios en el hardware del servidor y la configuración del sistema. Ayuda a diagnosticar problemas y brindar una resolución rápida cuando ocurren fallas en el sistema 5. Autenticación de dos factores 6. Cuentas de usuario locales o basadas en directorios con control de acceso basado en roles 7. Consola remota que comparte hasta 6 usuarios simultáneamente durante la operación previa al sistema operativo y al tiempo de ejecución del sistema operativo, reproducción de la consola: la reproducción de la consola captura y almacena para reproducir el video de la consola durante la última falla importante o secuencia de arranque de un servidor. Integración de Microsoft Terminal Services, cifrado SSL de 128 bits y compatibilidad con Secure Shell versión 2. Debería proporcionar soporte para AES en el navegador. Debe proporcionar funcionalidad de actualización remota de firmware. 8. Debe admitir la integración de API RESTful
Gestión de servidores	El software debe admitir la vista de panel para escanear rápidamente los recursos administrados para evaluar el estado general del centro de datos. Debe proporcionar un resumen visual del estado de los recursos que el usuario está autorizado a ver.
	El mínimo del panel debe mostrar un resumen de estado de lo siguiente: • Perfiles de servidor • Hardware de servidor • Alertas preventivas
	El software de gestión de sistemas debe proporcionar control de acceso basado en roles
	Aprovisionamiento sin intervención (ZTP) mediante SSDP con acceso remoto
	El software de gestión debe admitir la integración con el software de gestión de plataformas de virtualización más populares, como VM Essentials, VMware vCenter y vRealize Operations, y Microsoft System Center y Admin Center
	Debería ayudar a proporcionar una notificación proactiva de alertas de fallas de componentes reales o inminentes en componentes críticos como CPU, memoria y HDD.
	Debe tener un panel para las líneas base de firmware mientras se realizan las comprobaciones de firmware mínimas requeridas y se resaltan los dispositivos no conformes para las actualizaciones con la línea de base de firmware seleccionada
	El software de administración de servidores debe ser de la misma marca que el proveedor del servidor.

Monitoreo y administración habilitados para la nube	1. Ofrece agilidad operativa en la nube al unificar las operaciones informáticas como servicio en todo el ciclo de vida informático desde el perímetro hasta la nube. 2. Administra y controla los servidores independientemente de la ubicación física 3. Derechos basados en suscripción
	Administración del ciclo de vida del servidor 1. Actualizaciones de firmware sin problemas con actualizaciones inteligentes basadas solo en delta. 2. Gestión de firmware basada en grupos que se puede programar o bajo demanda 3. Actualizaciones de firmware en serie y en paralelo con la opción 'Detener en caso de falla' 4. Política basada en grupos para configuraciones, instalaciones del sistema operativo, configuración del BIOS. 5. Implementación de la imagen del sistema operativo 6. Soporte de API REST
	Compatibilidad 1. Creación automática de casos de soporte para eventos críticos de servicio. 2. Notificación de alertas críticas de hardware a través de notificaciones en la aplicación y por correo electrónico 3. Informes de cumplimiento de firmware bajo demanda 4. Consola remota usando un navegador web con soporte HTML5
	Gestión de identidades y accesos 1. Gestión unificada de identidad y acceso 2. Control de acceso basado en roles (RBAC) 3. Inicio de sesión único (SSO) 4. Políticas de restricción a nivel de recursos (RRP)
	Sostenibilidad - Informes de huella de carbono
	Información predictiva de IA para pronosticar los costos futuros de energía y las emisiones de carbono. Alertas basadas en umbrales.
	Información basada en IA con aprobaciones de políticas de flujo de trabajo
	El software debe ser compatible con la tenencia múltiple
	El software debe ofrecer visibilidad basada en mapas con una vista intuitiva del estado del servidor a través de un mapa global
	Monitoreo de servidores de múltiples proveedores
Memoria para QNAP	Cantidad 1- Memoria RMA de 16Gb - 3200 MHZ - PC4-25600
Tarjeta de red para Servidor DELL	Cantidad 1 - Tarjeta de red Intel XL710 10GBASE-T 4-port PCIe SFP+ - INTEL
Transceivers	Cantidad 4- Modulo 10GBASE-LR SFP+ Transceiver - EON
Memoria Equipo DELL	Cantidad 2 - Memoria 16G DIMM DDR4 Synchronous Registered 3200 MHz - DELL
Certificaciones de Partner	Se requiere la certificación de Partner del fabricante y distribuidor autorizado de la marca del equipo servidor.
Certificaciones de Ingeniería Especializada	Se requiere dos ingenieros certificados en: ASE para Computo o la certificación equivalente,