CRG03/22

ESPECIFICACIONES TÉCNICAS PARA EL SUMINISTRO E INSTALACIÓN DE EQUIPOS PARA AMPLIAR LA CAPACIDAD COMPUTACIONAL DEL CLÚSTER DE COMPUTACIÓN CIENTÍFICA, AMPLIAR LOS SISTEMAS DE ALMACENAMIENTO DE DATOS CIENTÍFICOS, PROPORCIONAR UNA PLATAFORMA DE SERVICIOS INFORMÁTICOS DEL CNAG – CRG Y ACTUALIZAR LA RED DEL CRG

1. Objetivo

El objeto de este Pliego de Prescripciones Técnicas es conseguir un marco homogéneo para poder valorar las ofertas presentadas para el suministro e instalación de equipos para ampliar a la infraestructura de cómputo, almacenamiento y redes en el CRG y en el CNAG-CRG.

Las especificaciones detalladas en las presentes condiciones generales y requisitos técnicos no son exhaustivas ni limitantes, por lo que cualquier otro elemento que la empresa licitante considere oportuno deberá incluirse y especificarse en la oferta presentada.

2. Introducción

CRG
El Centro de Regulación Genómica (CRG en adelante) es un centro de investigación compuesto por 4 programas con un total de 32 laboratorios. Además de esto, varias de las principales instalaciones del CRG ofrecen servicios científico-técnicos a todo el centro y a la comunidad científica mundial. Los equipos cliente que constan de aproximadamente 400 ordenadores de escritorio (150 Mac, 200 Windows, 50 Linux) y 100 estaciones de trabajo Linux se conectan utilizando múltiples conmutadores de 1Gbps en cada piso con el centro de datos del edificio mediante enlaces ascendentes de 10Gbps.

CNAG-CRG
El Centro Nacional de Análisis Genómico (CNAG-CRG en adelante) es un centro sin ánimo de lucro fundado en 2009 por el Ministerio de Economía y Competitividad y los Departamentos de Economía y Conocimiento y Salud de la Generalitat de Catalunya. Desde el 1 de julio de 2015, forma parte del Centro de Regulación Genómica (CRG). El CNAG-CRG está ubicado en el Parc Científic de Barcelona (PCB), y nace con la misión de desarrollar proyectos de secuenciación y análisis de ADN en colaboración con investigadores de Cataluña, España y la comunidad investigadora mundial, con el propósito de garantizar la competitividad de nuestro país en el área estratégica de la genómica. En marzo de 2010 se iniciaron las operaciones con 12 sistemas de secuenciación de última generación, lo que ha permitido al centro tener una capacidad de secuenciación de más de 800 Gbases al día, el equivalente a secuenciar completamente 6 genomas humanos cada 24 horas. Esta capacidad sitúa al CNAG - CRG como el segundo mayor centro europeo en cuanto a capacidad de secuenciación.

El sistema informático actual del CNAG - CRG está formado por 149 nodos informáticos con un total de 7840 núcleos. Hay 3 sistemas de almacenamiento: un sistema Lustre de 4,4 PB, un sistema Dell EMC Isilon de 6,4 PB que consta de 4 nodos H500 y 30 nodos A2000 , y una librería de cintas con una capacidad de 600 ranuras.

3. Equipos objeto de suministro

El objeto principal del contrato es el suministro e instalación de los equipos indicados en cada uno de los siguientes lotes:

LOTE 1: Suministro e instalación de una solución de virtualización para los nodos de servicio del clúster de computación científica del CNAG - CRG
Proporcionar una plataforma de virtualización para los servicios del clúster de computación del CNAG-CRG

LOTE 2: Suministro e instalación de switches de red para el CRG
Reemplazar los conmutadores de red al final de su vida útil en CRG por nuevos conmutadores con funciones de ciberseguridad mejoradas.

LOTE 3: Ampliación de capacidad y rendimiento de un sistema de almacenamiento para el clúster de computación científica del CNAG – CRG
Aumentar la capacidad y el rendimiento del clúster de almacenamiento Dell EMC Isilon existente en CNAG-CRG.

LOTE 4: Suministro e instalación de equipos para el clúster de computación científica CNAG-CRG
Proporcionar equipos que amplíen la capacidad de cálculo, redundancia y fiabilidad del clúster de computación científica del CNAG-CRG

LOTE 5: Suministro e instalación de cortafuegos para la red CNAG-CRG
Suministrar un firewall que permita una conexión a Internet independiente y segura para CNAG-CRG.

LOTE 6: Suministro e instalación de servidores para servicios informáticos para el CNAG-CRG
Suministrar servidores que permitan la prestación de servicios informáticos corporativos a CNAG-CRG.

LOTE 7: Suministro e instalación de nodos de cómputo para el proyecto vPDX.
Proporcionar capacidad computacional para el proyecto vPDX en CNAG-CRG

LOTE 8: Suministro e instalación de ampliación de almacenamiento para el proyecto vPDX.
Ampliar el clúster Dell-EMC Isilon en CNAG-CRG para proporcionar almacenamiento para el proyecto vPDX.

LOTE 9: Suministro e instalación de ampliación de almacenamiento para el proyecto 3Domics.

Ampliar el clúster Dell-EMC Isilon en CNAG-CRG para proporcionar almacenamiento para el proyecto 3Domics.

4. Alcance de los suministros licitados

Las ofertas que se presenten para cada uno de los Lotes, se ajustarán a las prescripciones contenidas en el Pliego de Cláusulas Particulares y en el presente Pliego de Prescripciones Técnicas.

Las ofertas incluirán todos los trabajos necesarios para el correcto suministro de los equipos, desde la fabricación, el transporte, la instalación en el CNAG - CRG para todos los componentes, los accesorios necesarios, la formación y el manual de funcionamiento y el de mantenimiento, con todas las soluciones técnicas, funcionales y de cualquier aspecto que resulten necesarias, hasta la realización de pruebas y ensayos que sean necesarios para la correcta verificación del resultado final de la instalación en el CNAG - CRG, el montaje del equipo y la gestión de los correspondientes residuos derivados de su instalación.

Todo el material suministrado debe de ser nuevo.

El licitador deberá detallar los trabajos en un Plan de proyecto que se consensuará con CNAG - CRG al inicio del proyecto.

Toda la documentación de la propuesta y del posterior proyecto deberá ser entregada en soporte digital en español o inglés.

En general, a parte de la tarea principal de suministro de equipos y servicios, la empresa proveedora deberá suministrar todos los medios personales, técnicos y de control necesarios para la correcta ejecución del proyecto de implantación.

1 KB = 1024 bytes

1 MB = 1024 KB

1 GB = 1024 MB

1 TB = 1024 GB

1 PB = 1024 TB

1 U = altura 44,45 mm (1,75")

5. Suministros que deben incluirse en el contrato

El contrato incluirá los siguientes suministros:

5.1. LOTE 1: Suministro e instalación de una solución de virtualización para los nodos de servicio del clúster de computación científica CNAG – CRG

Se requiere la instalación y configuración de una solución de virtualización basada en OpenStack y que permita la gestión de los nodos de servicio y nodos de inicio de sesión del clúster informático CNAG - CRG. Estos nodos proporcionan los servicios básicos para la administración del clúster como el sistema de colas, dns, dhcp, bases de datos, monitorización, etc. La solución constará de un mínimo de tres servidores que proporcionarán este servicio de virtualización de alta disponibilidad, así como un servidor utilizado para desplegar las máquinas virtuales. Si es necesario, la solución modular y escalable se puede ampliar posteriormente con equipos de similares características, permitiendo la gestión de un mayor número de máquinas virtuales según las necesidades futuras del CNAG.

Especificaciones técnicas

En las siguientes tablas se describen los requisitos de equipo y se asignan las letras R o D según si se trata de un requisito que debe cumplirse en la solución presentada (R) o un requisito deseable a tener y que estos serán valorados positivamente. soluciones que lo incorporan (D).

L1. Especificaciones técnicas de la solución de virtualización

Ref	Descripción
Hardware	
R	Un mínimo de 3 servidores (controladores) con las siguientes características mínimas cada uno: • 2 procesadores de código de instrucciones compatibles con x86_64 con un mínimo de 24 núcleos, una frecuencia base (excluyendo Max Boost) de 2,3 GHz (como, por ejemplo, AMD Rome 7352, o equivalente) • 256 GB de memoria principal (tecnología DDR4-3200 mínima) Cada uno de los servidores ofrecidos tendrá la siguiente configuración de disco: o 2 unidades SSD de 2,5" con una capacidad mínima de 960 GB, Enterprise Class M.2 SATA 6Gb/s y una resistencia mínima de 1 DWPD o 6 discos SSD de 2,5" con una capacidad mínima de 1,92 TB, SATA 6Gb/s de clase empresarial de 2,5" y una resistencia mínima de 1,5 DWPD o 6 discos con una capacidad mínima de 8TB, Enterprise Class 3.5" SATA 6Gb/s 7200rpm HDD
D	Se valorará un mayor número de servidores
D	Se valorará un procesador con un mayor número de núcleos

D	Se valorará un procesador con una frecuencia base más alta
D	Se considerará una mayor capacidad de memoria en servidores de igual o mayor velocidad
R	Un servidor (implementación de vm) con las siguientes características: • Un procesador de código de instrucciones compatible con x86_64 con un mínimo de 8 núcleos, una frecuencia base (excluyendo Max Boost) de 3,1 GHz (como, por ejemplo, AMD Rome 7232P, o equivalente) • 64 GB de memoria principal (tecnología DDR4-3200 mínima) • 2 unidades SSD de 2,5" con una capacidad mínima de 480 GB, Enterprise Class M.2 SATA 6Gb/s y una resistencia mínima de 1 DWPD
R	Todos los servidores deben tener las siguientes interfaces de red • Interfaz Dual Gigabit Ethernet para conexión a redes de gestión dentro y fuera de banda • Interfaz Dual 100 Gigabit Ethernet (QSFP56) para la red de datos.
R	Todos los servidores contarán con un sistema de gestión fuera de banda que permitirá el acceso a una consola remota, monitorización de alarmas y encendido y apagado.
R	Los servidores y cualquier elemento de la expansión deben tener una fuente de alimentación redundante.
R	Los servidores serán independientes, no compartirán un chasis común y no superarán las 2U
Software stack de virtualización	
R	Permitir la creación de máquinas virtuales, redes virtuales y ejecutando múltiples tenants
R	Proporcionará un portal de autoservicio que permitirá a los usuarios crear sus propias máquinas virtuales.
R	Proporcionará herramientas de interfaz de usuario, API y CLI
R	Podrá aprovisionar servidores bare metal (nodos de cómputo) así como máquinas virtuales (nodos de servicio y nodos de inicio de sesión)
R	Admitirá la ejecución de servidores bare metal y máquinas virtuales en la misma VLAN/VXLAN
R	Admitirá el aprovisionamiento de clústeres HPC que combinan servidores bare metal y virtuales
R	Admitirá entornos de clúster HPC seguros y aislados para permitir una colaboración segura
R	Admitirá el aprovisionamiento de entornos de Kubernetes para cargas de trabajo de investigación de IA, incluido el trabajo con aceleradores de GPU
R	Admitirá el aprovisionamiento de entornos Spark/Hail.
R	Se ha implementado previamente en otros entornos de investigación de secuenciación genómica similares.
R	La capa de redes definidas por software (SDN) deberá poder interoperar con Mellanox Fabrics
R	Admitirá instantáneas / copias de instancias (virtuales) con la capacidad de almacenar copias en NFS o S3, localmente o fuera del sitio
R	Admitirá la configuración automática de Mellanox Fabrics para entornos de

	servidor bare metal de varios inquilinos
R	Será compatible con la API de OpenStack
R	Los servidores utilizarán el sistema de archivos Ceph que proporcionará almacenamiento redundante de bloques y objetos que permitirá la migración en vivo de máquinas virtuales.
R	Se incluirán las licencias necesarias para los nodos del controlador
R	Se incluirá la licencia necesaria para el nodo de implementación de vm
R	Se incluirá un mínimo de 38 licencias bare-metal adicionales para los nodos de proceso de clúster, lo que permitirá aprovisionarlos
R	El soporte estándar para el software descrito en los puntos anteriores se incluirá durante 1 año.
R	Se incluirá la instalación y configuración de la solución de virtualización

5.2. LOTE 2: Suministro e instalación de conmutadores de red para el CRG

Se requiere la ampliación de la red del CRG para proporcionar la conectividad necesaria para todos los sitios de trabajo del CRG en el edificio PRBB.
El sistema de red actual del CRG está compuesto de 4 switches Fortinet FS-1048E y 2 switches Fortinet FS-448E, localizados en los 2 extremos del CPD en el PRBB, y están interconectados con una conexión de 100Gbps a través de una fibra de 20 metros. Este sistema de red actual proporciona una red integrada con un total de 192 puertos de 10Gbps y 48 puertos de 1Gbps. Esta red está directamente conectada a 2 firewall Fortigate FG-1500D para formar una red extendida dentro de un Security Fabric.
La solución de red descrita en este pliego técnico proporcionará una red integrada distribuida en las diferentes plantas del CRG en el edificio PRBB con la siguiente distribución:

- Planta -2: 48 puertos de 1Gbps
- Planta -1: 48 puertos de 1Gbps con una mínima de 5 puertos con PoE
- Planta 0N: 48 puertos de 1Gbps con una mínima de 5 puertos con PoE
- Planta 0S: 48 puertos de 1Gbps con una mínima de 5 puertos con PoE
- Planta 4N: 96 puertos de 1Gbps con una mínima de 10 puertos con PoE
- Planta 4S: 192 puertos de 1Gbps con una mínima de 20 puertos con PoE
- Planta 5N: 288 puertos de 1Gbps con una mínima de 30 puertos con PoE
- Planta 5S: 288 puertos de 1Gbps con una mínima de 30 puertos con PoE
- Planta 6N: 192 puertos de 1Gbps con una mínima de 20 puertos con PoE
- Planta 6S: 192 puertos de 1Gbps con una mínima de 20 puertos con PoE
- Equipos Spare: se provisionará un equipo con PoE y otro sin PoE del mismo modelo que los propuestos

Cada planta debería estar conectada con dos fibras de 10Gbps a 2 switches nuevos instalados en el CPD ofreciendo cada uno 24 puertos de 10Gbps.
Estos dos switches de agregación de los equipos de acceso de planta tendrán una interconexión redundada de 40Gbps entre ellos mediante dos cables DAC a 40Gbps de 3 metros.
Además, estos dos switches deberán conectarse a los switches FS-1048E en el CPD

mediante una interconexión redundada a 100Gbps.

Especificaciones Técnicas

A continuación, se describe en detalle las especificaciones técnicas de cada uno de los aspectos.
En las especificaciones técnicas, cada elemento de la lista se clasificará de la siguiente manera:
R: indicando que es un requerimiento obligatorio que la solución debe cubrir
D: indicando que es un requerimiento no obligatorio

Todos los equipos ofertados no pueden estar en la lista de "End-of-Sale" del fabricante.
Todo el material, conectores y adaptadores necesarios incluidos, debe ser nuevo y original del fabricante.
Las ópticas (SFPs) que se solicitan deben ser originales del fabricante.

Ref	Descripcion
Switches del CPD	
R	La nueva solución de red incluirá todos los elementos de red necesarios para extender la solución de red actual con una capacidad adicional de 48 puertos de 10Gbps
R	La oferta incluirá los dos switches adicionales con un mínimo de 24 puertos de 10Gbps y 4 puertos de 100Gbps
R	Los switches ofrecidos deben tener una altura de 1U
R	Los switches ofrecidos deben tener dos fuentes de alimentación redundante
R	Los switches ofrecidos deben ofrecer una capacidad de switching dúplex de 880Gbps
R	La nueva solución de red incluirá un mínimo de 40 transceptores SFP+ para las conexiones 10Gbps (Se deberá incluir un latiguillo de 2m por cada SFP+)
R	La nueva solución de red incluirá 2 cables DAC de 3m a 40G para la interconexión redundada entre los dos switches nuevos de agregación.
R	La nueva solución de red incluirá 4 transceptores QSFP28 para la interconexión con los dos switches actuales. (Se deberá incluir 2 latiguillos de 1m para realizar la conectividad)
R	La nueva solución de red debe ser integrada dentro de Security Fabric del CRG a través del protocolo FortiLink
R	La nueva solución de red debe poder ser gestionado directamente desde el firewall Fortinet FG1500D (Utilizando la propia webGUI del firewall), a fin de aplicar cambios de configuración sobre los puertos de los equipos (cambio de VLAN nativa, permitir VLAN y perfil de seguridad), actualizaciones y generación de topologías automáticas y gráficas de los equipos.
R	Requerimientos de funcionalidad: - Conmutadores Layer 2/3 - Características extensas de calidad de servicio (QoS) para aplicaciones esenciales que incluyen video, almacenamiento y telefonía IP - Seguridad completa para control de acceso a la red, cifrado y protección de recursos corporativos

	- Generación e implantación de políticas de seguridad sobre los elementos conectados a la red - SSHv2 - Soporte VLAN Privadas - Soporte 802.1x - Soporte de redundancia de enlaces (Duplicación de enlaces hacia los distintos elementos de red)
R	Requerimientos de funcionalidad de conmutación de Layer 2: - Soporte de VLANs simultáneas - Capacidad de filtrado de BPDUs de STP - Puerto espejo - Protección de bucles de Spanning-tree.
R	Requerimientos de funcionalidad de servicios de Layer 3: - Protocolo de Resolución de Direcciones - Protocolo de datagramas de usuario - Protocolo de configuración dinámica de host.
R	Los nuevos switches deben tener una funcionalidad de interfaz de línea de comandos CLI, así como de gestión basada en Web y GUI
R	Se deberá incluir el Soporte Extendido de fabricante por el periodo de (1) un año. Garantizando un SLA de 24x7 y reemplazo de pieza NBD
Switches de planta	
R	La nueva solución de red incluirá todos los elementos de red necesarios para ofrecer una solución de red de gestión con una capacidad total siguiente: - Planta -2: 48 puertos de 1Gbps - Planta -1: 48 puertos de 1Gbps con una mínima de 5 puertos con PoE - Planta 0N: 48 puertos de 1Gbps con una mínima de 5 puertos con PoE - Planta 0S: 48 puertos de 1Gbps con una mínima de 5 puertos con PoE - Planta 4N: 96 puertos de 1Gbps con una mínima de 10 puertos con PoE - Planta 4S: 192 puertos de 1Gbps con una mínima de 20 puertos con PoE - Planta 5N: 288 puertos de 1Gbps con una mínima de 30 puertos con PoE - Planta 5S: 288 puertos de 1Gbps con una mínima de 30 puertos con PoE - Planta 6N: 192 puertos de 1Gbps con una mínima de 20 puertos con PoE - Planta 6S: 192 puertos de 1Gbps con una mínima de 20 puertos con PoE - Equipos Spare: provisión de un equipo con PoE y otro sin PoE, del mismo modelo que los propuestos
R	La nueva solución de red incluirá 32 switches (10 equipos con PoE y 22 equipos sin PoE) con un mínimo de 48 puertos de 1Gbps RJ45 y 4 puertos de 10Gbps
R	Los switches ofrecidos deben tener una altura de 1U
R	Capacidad de fuente de alimentación redundante
R	Los switches ofrecidos deben ofrecer una capacidad de switching dúplex de 150Gbps
R	La nueva solución de red incluirá todos los conectores y cables necesarios para la conexión de los switches en stack por planta y con los dos switches del CPD a través

	de una conexión de 20Gbps
R	La nueva solución de red debe ser integrada dentro de Security Fabric del CRG a través del protocolo FortiLink
R	La nueva solución de red debe poder ser gestionada directamente desde el firewall Fortinet FG1500D (Utilizando la propia webGUI del firewall), a fin de aplicar cambios de configuración sobre los puertos de los equipos (cambio de VLAN nativa, permitir VLAN y perfil de seguridad), actualizaciones y generación de topologías automáticas y gráficas de los equipos
R	Requerimientos de funcionalidad: - Conmutadores Layer 2/3 - Características extensas de calidad de servicio (QoS) para aplicaciones esenciales que incluyen video, almacenamiento y telefonía IP - Seguridad completa para control de acceso a la red, cifrado y protección de recursos corporativos - Generación e implantación de políticas de seguridad sobre los elementos conectados a la red - SSHv2 - Soporte VLAN Privadas - Soporte 802.1x - Soporte de redundancia de enlaces (Duplicación de enlaces hacia los distintos elementos de red)
R	Requerimientos de funcionalidad de conmutación de Layer 2: - Soporte de VLANs simultáneas - Capacidad de filtrado de BPDUs de STP - Puerto espejo - Protección de bucles de Spanning-tree .
R	Requerimientos de funcionalidad de servicios de Layer 3: - Protocolo de Resolución de Direcciones - Protocolo de datagramas de usuario - Protocolo de configuración dinámica de host.
R	Los nuevos switches deben tener una capacidad de interfaz de línea de comandos CLI, así como de gestión basada en Web y GUI
R	Se deberá incluir el Soporte Extendido de fabricante por el periodo de (1) un año. Garantizando un SLA de 24x7 y reemplazo de pieza NBD.

5.3. LOTE 3 Ampliación de capacidad y rendimiento de un sistema de almacenamiento para el clúster de computación científica del CNAG – CRG

CNAG-CRG está en el proceso de ampliar en gran medida su capacidad de secuenciación con la compra de múltiples secuenciadores. Los sistemas de almacenamiento actuales se están acercando al límite de su capacidad y requieren una mejora del rendimiento actual para mantenerse al día con los requisitos de la instalación de secuenciación. Requerimos equipos que permitan expandir el Clúster Isilon existente que consta de 4 nodos H500 y 30

nodos A2000 comprado en 2021, aumentando su capacidad y mejorando su rendimiento. Requerimos aumentar el rendimiento general del sistema en al menos 45 GB / s al 100% de lecturas y la capacidad utilizable en 3652 TB

Especificaciones técnicas

Las especificaciones técnicas de cada aspecto se describen en detalle a continuación.

En las especificaciones técnicas, cada elemento de la lista se clasificará como sigue:

R: indicando que es un requisito obligatorio que la solución debe cubrir.

D: indicando que es un requisito no obligatorio.

Ref	Descripción
R	La expansión del sistema debe aumentar la capacidad neta total en un mínimo de 3652 TB, calculado como el aumento de la capacidad neta del sistema medido desde un cliente NFS utilizando el comando "df -h". Actualmente este valor es de 5.43PB por lo que la capacidad final después de la expansión debe ser de al menos 9PB. Toda la capacidad adicional debe estar disponible para extender cualquier volumen en el sistema actual y para estar disponible en el mismo espacio de nombres global.
D	Se valorará una mayor capacidad.
R	La expansión debe ser modular. Los módulos o nodos ofrecidos y en la cantidad ofrecida deben formar por sí mismos y sin ninguna modificación un sistema completamente autónomo. Cada módulo tiene que proporcionar conectividad de CPU, memoria, frontend y backend a la solución general, lo que permite el crecimiento lineal del sistema.
R	La expansión debe mantener la habilidad de los sistemas actuales para escalar a más de 200 módulos en un solo sistema distribuido donde todos los módulos comparten recursos, el trabajo se distribuye y no son necesarios módulos especiales o maestros.
R	La expansión debe mantener la propiedad del sistema actual de ser un único sistema coherente. La memoria caché de todos los módulos adicionales debe ser compartida y coherente con el sistema actual. El aumento mínimo de GB de RAM que la expansión debe añadir al sistema existente debe ser de 3552 GB, y debe mantener la capacidad del sistema para crecer en el futuro mediante la incorporación de nuevos módulos con memoria adicional de hasta decenas de Terabytes de memoria global.
R	Todos los módulos adicionales deben tener un sistema de memoria con SPS (StandBy Power Supply) para garantizar la consistencia de la memoria en caso de pérdida de energía de uno o más módulos.
R	Para garantizar la adaptabilidad a cualquier nuevo entorno, la expansión debe mantener la capacidad actual del sistema para mezclar diferentes tipos de módulos a medida que crece. Siempre respetando la arquitectura donde cada módulo añade rendimiento y/o capacidad. Esta flexibilidad permitirá que el sistema global escale

	linealmente hacia el eje de rendimiento o hacia el eje de capacidad según sea necesario mediante la adición de módulos apropiados al sistema.
R	La expansión debe mantener la propiedad del sistema actual de que si se mezclan diferentes tipos de módulos en el mismo sistema, se crearán diferentes niveles de servicio. A nivel de datos, y en base a políticas, debe existir la posibilidad de poder decidir en qué nivel de servicio queremos que los datos lleguen y residan, permitiendo que cambien automáticamente a otros niveles de servicio a medida que se cumplan ciertas condiciones (días de inactividad, etc...).
R	La expansión debe mantener la capacidad del sistema actual para proporcionar al menos dos niveles de servicio distintos, uno para la información más caliente y utilizada más recientemente y otro para datos archivados más fríos que deberían tener un costo por terabyte más barato que la capa caliente.
R	Los módulos que se agregan al sistema deben tener discos SSD destinados al almacenamiento de metadatos, almacenamiento de datos o caché para al menos mantener el nivel actual de rendimiento de metadatos por módulo del sistema actual.
R	El número mínimo de módulos que se propondrá será de 17 módulos para mejorar el rendimiento de E/S en términos de rendimiento e IOPS y para proporcionar un nuevo nivel de servicio para un rendimiento altamente exigente y 20 módulos para el nivel de servicio de información y archivado más fríos.
R	El sistema ampliado final debe ser capaz de equilibrar la capacidad de los diferentes módulos para poder ofrecer un rendimiento y ocupación comparables en todos y cada uno de ellos.
R	Cada nodo adicional debe proporcionar un mínimo de 1 puerto de red a 1 Gbps y un mínimo de dos puertos a 25 Gbps para el acceso desde equipos cliente cada uno (frontend). También se debe incluir el cableado necesario para conectar los módulos de extensión a la red CNAG-CRG a través de Ethernet de 25 Gb.
R	El rendimiento general del sistema global después de la expansión debería aumentar en al menos 45 GB/s en 100% de lectura y 29,6 GB/s en 100% de escritura.
R	Se incluirán los equipos de red y cableado necesarios que permitan la interconexión de los nuevos módulos con el sistema existente y mantendrán al menos el mismo nivel de conectividad por nodo del sistema actual.
R	La expansión debe mantener la capacidad de la solución actual para admitir la creación de pools de discos en los que almacenar archivos según directivas de antigüedad o tamaño, pero siempre dentro del mismo volumen.
R	La expansión debe mantener la capacidad del sistema actual para admitir el control de ocupación de espacio en disco en función de las directivas de usuario, grupo o directorio. También debe tener plantillas que sean automáticas y aplicables de forma predeterminada a las nuevas estructuras para directivas de usuario, grupo y directorio. Dichas políticas deben poder crearse y eliminarse en directorios con contenido existente, así como anidados en árboles de directorios complejos (políticas dentro de las políticas).
R	Los clientes deben poder utilizar cualquiera de los módulos del sistema expandido final y además tener acceso a todo el espacio tanto desde clientes Linux (soportará al menos Red Hat, Scientific Linux y CentOS), como Windows y Mac OS X, tanto en arquitectura x86 como en arquitectura x86_64.
R	El sistema ampliado debe mantener la autoridad para integrarse con Active Directory, LDAP e incluso ofrecer la posibilidad de definir ACL internamente.

R	El sistema ampliado debe mantener la utilidad de ofrecer la posibilidad de administración a través de la web, a través de CLI y a través de la API REST.
R	El sistema ampliado debe mantener el sistema de equilibrio de carga integrado para garantizar que las conexiones del cliente al sistema se distribuyan uniformemente entre los módulos de manera óptima y automática. Dicho equilibrio de carga debe poder particularizarse por entorno y considerar como variables el número de conexiones, el rendimiento o la CPU de cada nodo del sistema.
R	El sistema ampliado debe seguir soportando diferentes tipos de protección configurable y definible en caliente en cualquier momento y en cualquier nivel de segmentación (a nivel de recurso compartido, exportación, carpeta o incluso archivo), incluidos los tipos de protección que pueden soportar una falla de disco cuádruple para adaptar la confiabilidad a los datos durante su vida útil.
R	El sistema ampliado debe seguir teniendo funciones de autogestión para eliminar tareas, como la desfragmentación, de modo que el rendimiento no se degrade con el tiempo.
R	El sistema ampliado debe seguir ofreciendo sistemas proactivos de supervisión de bajo nivel que permitan poner en cuarentena un disco antes de que falle.
R	La solución ampliada debe seguir admitiendo el acceso a cualquier parte del sistema de archivos utilizando al menos los siguientes protocolos: NFSv3, NFSv4, SMB2, SMB3 (disponibilidad continua, multicanal, copia del lado del servidor, cifrado SMB3), HTTP, FTP, S3 y HDFS de forma nativa sin puertas de enlace.
R	Independientemente del protocolo utilizado para crear un archivo, el sistema expandido debe seguir permitiendo el acceso al mismo por cualquiera de los otros protocolos incluidos en la propuesta, en tiempo real, e incluso con los archivos en uso, pero siempre asegurando la coherencia en los datos.
R	El sistema expandido debe continuar la capacidad de realizar una actualización del sistema operativo de una manera no disruptiva, así como permitir que los administradores reviertan a la versión anterior si lo hacen. Esta reversión debe poder ser utilizada por los administradores del sistema sin la necesidad de involucrar un soporte especial del fabricante o proveedor de la plataforma.
R	El sistema ampliado debe seguir ofreciendo la posibilidad de filtrar los archivos que tienen que ser almacenados y no permitir que se almacenen ciertas políticas (Bloqueo de archivos por extensión)
R	La solución expandida debe continuar la propiedad de que el impacto en el rendimiento del fallo de un módulo no excederá en ningún caso el 10%, y este porcentaje debe disminuir a medida que el sistema crece.
R	El sistema expandido debe seguir soportando la caída de cualquier módulo y de desplazar a otro módulo todos los clientes que estaban conectados a él, de forma transparente y sin necesidad de interrumpir el servicio con esos clientes para NFS, SMB3 y HDFS.
R	El sistema expandido debe garantizar la coherencia de los datos cuando se accede a ellos o se guardan en el sistema de archivos.
R	El sistema expandido debe poder conectarse a conmutadores de diferentes fabricantes para acceder desde equipos cliente.
R	El sistema ampliado debe seguir ofreciendo la posibilidad de deduplicar información, independientemente del protocolo y/o ubicación de los datos dentro del sistema. Esta funcionalidad no se requiere entrada, pero el sistema debe estar listo

	para ser activado cuando se considere oportuno.
R	El sistema ampliado debe ser capaz de ofrecer una gestión basada en diferentes tenants.
R	La solución expandida debe ser capaz de integrarse con diferentes directorios activos a la vez.
R	La solución ampliada debe ser capaz de integrarse con diferentes proveedores de nube. Esta integración debería permitir la capacidad de archivar el contenido del sistema en la nube utilizando el protocolo S3.
R	El sistema ampliado debe incluir todo el software necesario para ofrecer toda la funcionalidad solicitada.

Instalación

Ref	Descripción
R	El licitador incluirá un rack de 42U y dimensiones H (202cm), W (72 cm), D (122 cm) para la instalación de la solución requerida, así como las PDU y el cableado necesario.
R	Se deben incorporar las PDU necesarias para conectar el sistema con líneas monofásicas de 32A.
R	Todos los componentes de la expansión (rack, servidor, switch, cable, fibra...) deben estar debidamente etiquetados, para ser identificados físicamente de forma única según la nomenclatura establecida entre CNAG-CRG y la empresa instaladora. Los cables y fibras deberán indicar el origen y el destino de la conexión.
R	Se debe incluir el montaje en rack de toda la expansión, además de la recolección de todos los materiales sobrantes de la instalación y el transporte.
R	Se deben incluir todas las guías, soportes y elementos necesarios para la correcta instalación de la expansión, así como todos los cables de alimentación correspondientes.

Documentación y formación

R	La documentación debe presentarse en formato digital en español o inglés en el que se describa: - Descripción general de los componentes de la solución - Esquema de conexiones e IP e instalación en el rack - Diagrama con la ocupación de los racks con los diversos equipos presentados en la solución y el número de U utilizadas por cada uno. - Ajustes de configuración utilizados - Explicación del proceso de instalación y las tareas realizadas
R	Se proporcionará formación que cubra suficientemente: - Conceptos, administración básica y procedimientos básicos de configuración - Optimización de la solución - Solución de problemas
R	Se debe presentar y evaluar un plan de proyecto. Este plan se acordará con el equipo técnico del CRG para minimizar los cortes y efectos en el servicio

5.4. LOTE 4: **Suministro e instalación de equipos para el clúster de computación científica CNAG-CRG**.

El clúster de computación CNAG-CRG consta de 149 nodos con un total de 7840 núcleos. Se requiere el suministro e instalación de un nuevo clúster informático para ampliar la capacidad informática actual del CNAG-CRG.

La extensión solicitada en esta especificación aumentará en un mínimo de 3456 el número de núcleos de propósito general para computación científica interconectados por una red de alto rendimiento y baja latencia basada en 100 GbE y proporcionará 2 switches para la red de gestión de la expansión.

Los aceleradores de procesadores basados en GPU o de la familia Xeon Phi no se considerarán para el cálculo de este número de núcleos ofrecidos.

Todos los nodos de la solución tendrán las mismas características

Especificaciones técnicas

En las siguientes tablas se describen los requisitos del equipo y se asignan las letras R o D según si se trata de un requisito que debe cumplirse en la solución presentada (R) o de un requisito deseable a tener y que se valorarán positivamente aquellas soluciones que lo incorporen (D).

Ref	Descripción
R	Un mínimo de 28 nodos de cómputo cada uno con las siguientes características: • 2 unidades centrales de procesamiento de código de instrucciones compatibles con x86_64, con 64 núcleos y frecuencia base (sin tener en cuenta Max Boost) de 2.2GHz(como, por ejemplo, AMD EPYC 7662, o equivalente) , • 1024 GB de memoria principal (tecnología DDR4-3200 mínima) • Dos SSD de 2,5" con una capacidad mínima de 480 GB y una resistencia mínima de 1,5 DWPD
R	Se considerarán unidades centrales de procesamiento con al menos el mismo nivel de rendimiento medido utilizando el punto de referencia passmark, siempre que tengan al menos 64 núcleos.
D	Se valorará un mayor número de nodos.
R	Todos los nodos de cómputo deben tener las siguientes interfaces de red: • Al menos dos interfaces Gigabit Ethernet con una conexión configurable para arrancar el nodo mediante PXE (red en banda) y la otra para la gestión fuera de banda (por ejemplo, ipmi, idrac, bmc, etc.) • Interfaz dual 100 Gigabit Ethernet (QSFP56) para la red de datos, que permitirá conexiones redundantes entre los nodos informáticos y el almacenamiento científico.
R	Los nodos de cómputo contarán con un sistema de gestión fuera de banda que permitirá el acceso a una consola remota, la monitorización de alarmas y el

	encendido y apagado.
R	Los nodos y cualquier elemento de la expansión deben tener una fuente de alimentación redundante.
R	Los nodos no pueden exceder 1U y pueden compartir un chasis común para mejorar esta densidad mínima.
R	En el caso de compartir el mismo chasis, cada nodo se puede quitar del chasis sin afectar al resto de nodos, que pueden seguir funcionando normalmente (intercambiables en caliente)
R	Todo el hardware del nodo informático será compatible con el sistema operativo CentOS 7 y 8.

Especificación técnica de los conmutadores de gestión

Ref	Descripción
Características generales de las dos redes	
R	Se proporcionarán dos conmutadores con las características siguientes que darán servicio a la gestión en banda y fuera de banda de la expansión informática.
R	Los switches propuestos deben tener calidad de centro de datos empresarial.
R	Se debe proporcionar el hardware necesario (conmutadores, cables, etc.) para establecer las redes de gestión en banda y fuera de banda con tecnología Gigabit Ethernet. El cableado de la red de administración en banda debe usar cables cat 7 blancos con conectores RJ45, el cableado para la red de administración fuera de banda debe ser con cables cat 7 rojos con conectores RJ45.
R	Todos los servidores de la solución de virtualización (Lote 1) y los nodos de cómputo (Lote 4) de esta especificación técnica deben estar conectados a las redes de gestión dentro y fuera de banda con dos cables diferentes.
R	Se debe incluir todo el cableado necesario para esta conexión: 48 cables de 1 GbE para la red de gestión en banda y 48 cables de 1GbE para la red de gestión fuera de banda de diferente color.
R	Los conmutadores deben tener el sistema operativo cumulus Linux preinstalado.
R	Se proporcionarán dos conmutadores para la solución propuesta con los siguientes requisitos: - Memoria mínima de 2 GB DRAM. - SSD de 8GB. - Capacidad de conmutación agregada - 176 Gbps - Enrutamiento de capa 3 sin bloqueo
R	Cada conmutador debe tener doble fuente de alimentación, intercambiable en caliente
R	Cada interruptor debe contener al menos: - 48 puertos RJ-45 10/100/1000BASE-T - 4 x puertos SFP+ 10G para enlace ascendente
R	Cada conmutador debe tener un tamaño máximo de 1U.
R	Cada conmutador debe ser instalado como un switch de parte superior del rack con puertos de red en la parte posterior (el extremo del pasillo caliente) con la dirección del flujo de aire de enfriamiento desde la parte delantera (pasillo frío) hacia la parte posterior.

5.5 LOTE 5 Suministro e instalación de un cortafuego para la red CNAG-CRG.

Se requiere la ampliación de la parte de seguridad de la red CNAG-CRG con la instalación de un clúster de firewall en el edificio PCB para poder tener una conexión a internet propia sin necesidad de redirigir todo el tráfico a través del clúster de firewall localizado en el edifico PRBB.
El sistema de seguridad actual de la red CRG está compuesto de 2 firewall Fortigate FG-1500D gestionado a través de un gestor de configuración FortiManager y un gestor de log FortiAnalyzer.

Especificaciones Técnicas

A continuación, se describe en detalle las especificaciones técnicas de cada uno de los aspectos.
En las especificaciones técnicas, cada elemento de la lista se clasificará de la siguiente manera:
R: indicando que es un requerimiento obligatorio que la solución debe cubrir
D: indicando que es un requerimiento no obligatorio

Todos los equipos ofertados no pueden estar en la lista de "End-of-Sale" del fabricante.
Todo el material, conectores y adaptadores necesarios incluidos, debe ser nuevo y original del fabricante.
Las ópticas (SFPs) que se solicitan deben ser originales del fabricante.
La propuesta debe incluir durante la totalidad de la duración del contrato todas las licencias y subscripciones necesarias para activar todas las funcionalidades asociadas a los requerimientos obligatorios incluidos en este pliego Técnico.

Ref	Descripción
Hardware - Cortafuegos	
R	2 cortafuegos modulares con fuente redundante (los cortafuegos deben ser en formato appliance de un único fabricante, excluyendo soluciones con máquinas virtuales o servidores)
R	Los 2 equipos físicos deben ser de características idénticas, redundadas y en alta disponibilidad. Han de poder trabajar en modo Activo-Pasivo como Activo-Activo.
R	Debe permitir funcionalidades de control de aplicaciones, IPS, Antimalware con Cloud Sandbox incluido, Webfilter, DNS filter, Antispam, protección antiDoS y Web Applicacion Firewall. Todas estas funcionalidades han de ser licenciadas para toda la duración del contrato.
R	Los equipos deben disponer de la funcionalidad de Firewalls virtuals para la creación de entornos totalmente diferenciales. Debe incluir un mínimo de 10 Firewalls virtuals.
R	La solución de seguridad debe permitir diferentes modos de funcionamiento: - Modo transparente - Modo routed - Modo sniffer
R	Se debe incluir a la propuesta, dentro de los mismos appliance, la funcionalidad de auditoria propia del sistema, que como resultado tiene un indicador o valor numérico de riesgo, como una puntuación negativa para cada parámetro auditado no complido. Estos parámetros que se tienen que comprobar deben ser como mínimo: política de seguridad sin uso en los últimos

	90 días, política de contraseñas débiles y comprobación del licenciamiento/soporte
R	La propia plataforma debe tener conectores automáticos con el objetivo de integrarse con identidades terceras y poder recibir información, direcciones IP, inventario de objetos y etiquetas. Esta funcionalidad debe ser soportada en los appliances de seguridad (sin necesidad de consola adicional). En concreto se requiere los siguientes: - Cloud pública: Google Cloud, Azure, AWS - Cloud privada: VMware NSX i ESXi, Openstack, Kubernetes - Fuentes de identidad: Active directory i Radius. - Fuentes de riesgos: Listado de ip, dominios, URLs y hash de malware customizados.
R	La misma solución de seguridad debe permitir la creación de automatismos para: - En caso de detección de un equipo comprometido, los cortafuegos envían: un email, una notificación tipo push a dispositivos Iphone, poder bloquear la dirección ip, invocar funciones AWS Lambda, Google functions, Azure Functions y Webhook. - En caso de cambio de configuración de los cortafuegos, un failover, reboot, actualización de firmas, de forma programada y cualquier evento, los cortafuegos envían: un email, una notificación tipo push a dispositivos Iphone y invocar funciones AWS Lambda, Google functions, Azure Functions, comanda por CLI y Webhook.
R	Los cortafuegos tendrán hardware específicos (de tipo ASIC) para asegurar el rendimiento requerido; en detalle, debe tener un hardware específico para analizar el tráfico de nivel 4 y otro totalmente diferente para el tráfico de nivel 7 y garantiza latencia baja
R	Los cortafuegos deben disponer de al menos 80 / 80 / 45 Gbps de rendimiento de firewall para paquetes de 1518, 512 i 64 bytes en IPv4; y de 80 / 80 / 45 Gbps de rendimiento de firewall per paquetes de 1518, 512 i 86 bytes en IPv6
R	Los cortafuegos deben gestionar un mínimo de 8 millones de sesiones concurrentes, como un mínimo de 500.000 sesiones nuevas por segundo.
R	Debe tener una capacidad de un mínimo de 100.000 políticas de Firewall
R	El rendimiento para el tráfico SSL VPN debe ser como mínimo de 8,4 Gbps y para el tráfico IPSEC VPN (512 bytes) de 48 Gbps
R	A nivel 7, el equipo debe disponer del rendimiento siguiente: - Rendimiento IPS: 12,5 Gbps para el tráfico Enterprise MIX. - Rendimiento NGFW (IPS y control de aplicaciones): 9,8 Gbps para el tráfico Enterprise MIX. - Rendimiento con Threat Protection (Firewall con IPS, control de aplicaciones y motor antimalware activados): 7,11 Gbps para el tráfico Enterprise MIX. - Rendimiento Inspección SSL con IPS: 10 Gbps. - Rendimiento para el control de aplicaciones: 26 Gbps para http 64K.
R	Los cortafuegos deben incluir las interfaces siguientes (como mínimo y per equipo): - 1 puerto de consola. - 2 puertos USB 3.0 para la conexión de modem 3G/4G y/o pendrive. - El puerto USB debe permitir la instalación del firmware y aplicación de configuración en el booting del equipo para realizar tareas automáticas de instalación - 2 puertos 40GE QSFP - 4 puertos 10GE 25 GE SFP28/SFP+ para el soporte de conectores ópticos 10G o 25G - 4 puertos 10GE SFP+ para el soporte de conectores ópticos 10G - 24 puertos 1GE (16 puertos 1GE RJ45 + 8 puertos 1GE SFP) - 2 puertos HA (alta disponibilidad dedicadas para establecer el clúster, con conectividad de 1G cada uno).

R	Los cortafuegos deben incluir los conectores SFP+ para todos los puertos compatible son 10GE
R	El cortafuego debe poder ser instalado en un rack de 19'' y no mas de 2 RU.
R	El cortafuego debe tener un consumo máximo inferior a 346 W.
R	El cortafuego debe tener como mínimo 2 discos duros de 480 GB SSD cada uno.
R	En el caso que el equipo Soporte la ampliación de memoria RAM y Disco Duro, el cortafuego debe estar equipado con la capacidad máxima de RAM y disco duro soportado por el fabricante.
R	El cortafuego debe tener dos fuentes de alimentación redundantes y con Hot Swap.
R	Los cortafuegos deben tener las funcionalidades de networking siguientes: - Soporte de protocolos RIP v1/v2, OSPF, ISIS, BGP, WCCP y Multicast para IPv4 e IPv6, Routing basado en política o PBR y funcionalidades avanzadas SD-WAN. - Soporte de VRFs (múltiples tablas de Routing) y multiVRF Routing (por BGP y OSPF). - Soporte Dual Stack IPv4 e IPv6 simultáneamente. - Network address translation NAT IPv4, NAT64 y NAT66. - DHCP server / DHCP Relay /DNS Server / DNS Proxy / NTP Server. - 802.1Q VLANs i Point-to-Point Protocol over Ethernet (PPPoE). - 802.3ad Capacidad de crear enlaces LACP para la agregación de puertos. - Capacidad de balanceo de servidores a nivel 4 para todos los servicios, así como posibilidad de hacer SSL off-loading por el tráfico HTTPS. - Es necesario que la solución de seguridad tenga capacidades integradas de SD-WAN, en concreto: o Balanceo inteligente de conexiones físicas y lógicas, indiferentemente del tipo de conexión WAN (MPLS, 3G/4G, FTTH, VPN, etc..). o El número mínimo de conexiones físicas y lógicas que se pueden añadir al SD-WAN debe ser de 256. o Verificación de la disponibilidad de Internet para cada una de las líneas, por protocolos http, ping, dns y TWANP. El número de Health-checks debe ser de como mínimo 100. o Verificación de calidad en tiempo real: jitter, packet loss y latencia por línea. o Configuración de políticas de SD-WAN inteligente basado en origen (usuarios AD y dirección IP), en el destino (dirección IP, aplicaciones y/o servicios de Internet/aplicaciones) y en la línea con mejor calidad de ese momento basado en valores de jitter, packet loss, latencia, tráfico de subida/bajada o ancho de banda, así como una combinación por pesos. o En el caso de necesidad de licenciamiento o suscripciones para activar estas funcionalidades, será necesario que éstas estén incluidas en la propuesta durante la duración completa del contrato. - Soporte de VXLAN y VXLAN VTEP por extensión de nivel 2 sobre redes de nivel 3. - El sistema propuesto debe tener una funcionalidad integrada de Traffic Shaping tanto de tráfico saliente como entrante siendo capaz de reservar ancho de banda y marcar el tráfico con DSCP. Este traffic shaping debe basarse en aplicaciones y URLs a nivel global de perfil o para ip.
R	Los cortafuegos deben tener las funcionalidades de alta disponibilidad siguientes:

	- La funcionalidad de alta disponibilidad debe estar disponible sin necesidad de licencia. - Apoyo HA tipo Activo – Pasivo, Activo - Activo y modo mixto. El modo mixto implica poder tener Firewalls virtuales activos y pasivos de forma mezclada, es decir, el máster de ciertos Firewalls virtuales sea la primera unidad de cortafuegos, mientras que la segunda unidad de cortafuegos sea master del resto de firewalls virtuales a la vez. - La transferencia de servicio de un equipo al otro debe poder hacerse sin cortes, ni pérdida de las conexiones tcp, ni parada de servicio. - Las configuraciones deben traspasarse de manera automática entre los dos equipos. - Capacidad de funcionamiento en modo activo/activo sincronizando sesiones entre los dos nodos, pero manteniendo direccionamiento IP diferenciado en las interfaces de cada nodo del clúster. - En el caso de necesidad de licenciamiento o suscripciones para activar la alta disponibilidad, será necesario que éstas estén incluidas en la propuesta durante la duración completa del contrato.
R	Los cortafuegos deben tener las funcionalidades de visibilidad siguientes: - Los equipos cortafuegos deben poder generar topologías gráficas físicas y lógicas, con la integración de otros cortafuegos del fabricante, para poder ser capaz de ver en un extremo a extremo que está pasando en toda la red. - Funcionalidad de consolidación de logs con diferentes niveles de agrupación, en concreto: por origen, destino, aplicación, amenaza, websites y políticas para su visualización. Esta visualización debe ser tipo "Drill-down", es decir, poder seleccionar unos de los objetos agrupados e ir filtrando el resultado en base a esta selección, hasta saber el detalle completo. Estos requerimientos deberán poder cumplirse desde la propia GUI de los appliances, en tiempo real, y sin necesidad de una consola central de gestión.
R	Los cortafuegos deben tener las funcionalidades de seguridad siguientes: - Capacidad de definir políticas de seguridad IPv4/v6 utilizando los siguientes parámetros de coincidencia: o Como origen (todas las opciones): ▪ Capacidad de definir una y/o más de una Interface de origen, incluyendo "año". Así como también "zonas". ▪ Capacidad de utilizar direcciones ip, rangos y/o redes, FQDN, países, servicios de internet y direcciones ip's reconocidas como origen de redes TOR, proxias anónimos (estas direcciones deben actualizarse automáticamente), así como los objetos exportados de dichos conectores al apartado de características generales del equipo. ▪ Capacidad de utilizar usuarios/grupos locales o remotos mediante conectores AD, NAC u otros repositorios de identidato. ▪ Capacidad para declarar horarios o "schedule" tanto por día/hora como fecha máxima de vencimiento. ▪ Capacidad de selección del servicio a utilizar. o Como destino: ▪ Capacidad de definir una y/o más de una Interface de destino, incluyendo "año". Así como también "zonas".

	▪ Capacidad de utilizar direcciones ip, rangos y/o redes, así como objetos FQDN, países y servicios de internet. - Capacidad de definir políticas de seguridad IPv4/v6 utilizando la siguiente parametrización: o Se debe poder seleccionar qué tráfico se analizará a nivel 4 y cuál a nivel 7, por política, sin excepción. o La configuración del NAT saliente debe poder configurarse dentro de cada una de las políticas de seguridad, de forma granular. o Las diferentes funcionalidades de seguridad avanzadas de nivel 7 se activarán de forma individual a nivel de política, nunca a nivel global. Además, estas se gestionarán con perfiles para ser granulares en los permisos. Estas funcionalidades son: antivirus, webfilter, DNS filter, Web Application Firewall, Control de aplicaciones, IPS, y DLP. o Decidir a nivel de política qué tráfico SSL será descifrado por su análisis y cuál sólo a nivel de certificado. o A nivel de logging, es necesario que la solución permita activar el logging de sólo nivel 7, o tanto de nivel 4 más nivel 7. También hay que hacer captura de packets en la propia política. - Capacidad de creación de reglas de DoS a nivel 3 y 4, pudiendo aplicarse por servicios publicados donde poder filtrar por direcciones ip o países por: ip_src_session, ip_dst_session, tcp_syn_flood, tcp_port_scan, tcp_src_session, tcp_dst_session, udp_flood, udp_scan, udp_src_session, udp_dst_session, icmp_flood, icmp_sweep, icmp_src_session, icmp_dst_session, sctp_flood, sctp_scan, sctp_src_session y sctp_dst_session. - Capacidad de definir políticas a nivel de Interface con el fin de denegar tráfico y no ser procesado por la política de seguridad global. Se deben poder utilizar direcciones IP's, países, así como rangos y redes ip como origen. - Para evitar el acceso de redes botnet, los cortafuegos deben tener una base de datos de reputación dinámica que bloquee los accesos a nivel de Interface. - Visualización del número de usos y cantidad de tráfico de cada regla de seguridad, de forma ágil tanto en la propia sección de políticas de seguridad, esto como también dentro de la configuración de cada política. También hay que ver la última vez que se ha utilizado.
	Los cortafuegos deben tener las funcionalidades de control de aplicacions siguientes: - Capacidad para identificar un mínimo de 1900 aplicaciones activas actuales (incluyendo aplicaciones web 2.0), como por ejemplo distinguir Facebook, de una sub-aplicación Facebook-chat o post. - La solución debe clasificar las aplicaciones en diferentes categorías y subcategorías, para poder aplicar reglas de acuerdo con estas categorías / subcategorías (control granular dentro de la aplicación). - Aplicar técnicas de identificación de aplicaciones en todos los puertos TCP / UDP y no sólo en los más comunes. - Capacidad para identificar las aplicaciones bajo túneles HTTPS. - Capacidad para identificar aplicaciones Industriales como Modbus. - Capacidad de creación de firmas de aplicaciones para un reconocimiento personalizado. Es obligatorio que en aquellas aplicaciones customizadas, también sean analizadas por motores de protección (IPS y antimalware).

	Los cortafuegos deben tener las funcionalidades de IPS siguientes: - Capacidad para proteger tanto a servidores como clientes con un mínimo de 10000 firmas de IPS, agrupadas por categoría, severidad, objetivo y protocolo. Ante la identificación de un ataque por IPS, es necesario que el cortafuego capture el tráfico en un archivo pcap con el fin de evidenciarlo y hacer un estudio posterior. - Capacidad para identificar patrones de ataques basados en comportamiento o rated-base, con el fin de bloquear intentos de ataques una vez superado un umbral de uso en un tiempo determinado. - Capacidad de creación de firmas de IPS para un reconocimiento personalizado.
	Los cortafuegos deben tener las funcionalidades de antimalware siguientes: - Capacidad de detección de malware (virus, grayware, worns, etc...) basado en firmas conocidas o métodos avanzados de detección. - Soporte de sandboxing en el cloud, con un tamaño mínimo de fichero de 100 MB indistintamente del tipo de fichero. - Capacidad para la eliminación del contenido dinámico (macros, javascript, URL) explotable dentro de documentos ofimáticos y pdf, que se distribuyen por protocolos SMTP, IMAP y http. - Capacidad de comprobación de si se trata de un fichero bueno o malo, en función del hashing y comparado con la BBDD del fabricante. Así como bloqueando mediante malware de repositorios externos de threat inteligence.
	Los cortafuegos deben tener las funcionalidades de Webfilter siguientes: - Capacidad de categorizar más de 250 millones de páginas web en más de 60 categorías web para aplicar: block, monitor y aplicación de cuotas de tiempo o tráfico por categoría. - Soporte de protocolos http v1.0, 1.1 y 1.2. - La base de datos de categorías web deberá consumirse como un servicio cloud en tiempo real y no podrá basarse únicamente en listados locales con el fin de tener la categorización de las url's lo más actualizado posible. - Soporte para restringir el acceso a Youtube y Google en modo "safe search". - Soporte de rating para imágenes por URL. - Apoyo para la creación de listas blancas/negras externas sin necesidad de licencia.
	Los cortafuegos deben tener las funcionalidades de DNS filter siguientes: - Capacidad de categorizar domins DNS en más de 60 categorías para poder realizar intercepción del tráfico DNS con las siguientes acciones: block, monitor y redirect (redirigir las consultas hacia un portal web cloud o personalizado de bloqueo). - La base de datos de categorías dns deberá consumirse como un servicio cloud en tiempo real y no podrá basarse únicamente en listados locales con el fin de tener la categorización de las url's lo más actualizado posible. - Soporte para restringir el acceso a Youtube y Google en modo "safe search". - Apoyo para la creación de listas blancas/negras externas sin necesidad de licencia.
	Otras funcionalidades de nivel 7 que la propuesta debe incluir y deben estar licenciadas son: - DLP - ICAP - Web application firewall
	Los cortafuegos deben tener las funcionalidades de VPN siguientes: - El dispositivo admite hasta un máximo de 10.000 usuarios simultáneos VPN SSL, ya sea con o sin agente, pero en cualquier caso sin licencia adicional.

	- El sistema propuesto deberá cumplir los estándares de la industria, sin el soporte externo adicional de hardware o módulos: IPSEC VPN (IPv4 e IPv6), PPTP VPN, L2TP VPN, SSL VPN y GRE sobre IPSEC. - El sistema propuesto deberá soportar 2 modos de funcionamiento SSL VPN: o Sin cliente - Acceso web: para clientes remotos que solo necesitan un navegador y no requiere la instalación de ningún agente, con el fin de acceder vía web a: HTTP / HTTPS Servidor intermediario, FTP, Telnet, SMB / CIFS, SSH, VNC y RDP. o Modo túnel: para equipos remotos que ejecutan una variedad de aplicaciones de cliente y servidor. - Soporte de agregación de túneles VPN y balanceo por packet pudiendo así añadir la anchura de banda de los accesos VPN IPsec entre sedes. - Capacidad de integración del propio fabricante de doble factor de autenticación vía token móvil, así como por SMS y correo electrónico, integrado en la misma plataforma de seguridad. Este token también debe poder usarse para el acceso a la GUI de los equipos cortafuegos.
	Los cortafuegos deben tener las funcionalidades de controladora de acceso seguro integrada siguientes: - El sistema debe ser capaz de actuar como controladora de puntos de acceso wireless así como de switches del propio fabricante. - La capacidad mínima de 4096 puntos de acceso wifi gestionados del mismo fabricante, y de switchs de 196 gestionados y del propio fabricante. - En el caso de necesidad de licenciamiento o suscripciones para activar la alta disponibilidad, será necesario que éstas estén incluidas en la propuesta durante la duración completa del contrato. - La gestión de los APs y Switches se hará desde la misma interfaz gráfica y CLI desde la que se gestiona el Firewall o desde la consola central de gestión.
	Los cortafuegos deben tener las funcionalidades de logging y reporting siguientes: Para el logging y reporting habrá que instalar una máquina virtual/appliance para que los cortafuegos envíen en tiempo real los logs generados, con el objetivo de que sea una: - Herramienta de monitoreo a tiempo real del tráfico filtrado por los diferentes módulos de los equipos. - Herramienta de monitoreo histórico externo a los dispositivos, almacenamiento de logs, reportes, del tráfico analizado por los equipos con capacidad de hacer informes de 6 meses aproximadamente (incluir licenciamiento y soporte necesario durante toda la duración del contrato). - Reportes y alarmas en función de direcciones, puertos, protocolos. - Reportes y alarmas en función de usuarios y/o grupos de usuarios (AD/LDAP). - Poder analizar, correlacionar y hacer informes de la información de seguridad de manera centralizada. - Panel de control con vista general de usuarios destacables, aplicaciones, destinos, sitios web, vulnerabilidades, etc. - Modelos de informes preconfigurados, editables, modificables y exportables. - Gestión de eventos con generación de alertas automáticas a administradores. - Visor de logs en tiempo real o histórico, que permita distinguirlos entre tráfico, eventos y seguridad. - Visión de logs por dispositivo, dominios de administración o agregados.

	- Capacidad de filtrado y granuralidad de análisis de logs. - Diseñador de alertas comprensible. - Posibilidad de generación de alertas por niveles de seguridad, eventos específicos, acciones o destinos y número de eventos en un determinado tiempo. - Capacidad de buscar alertas históricas. - Notificación de alertas por correo electrónico, SNMP o syslog. - Rotación de logs recopilados automática con envío de históricos a otros sistemas por email, FTP, HTTP, etc. - Visibilidad de los logs en formato TXT descargables. - Vista comparada de patrones de tráfico y amenazas. - Análisis exhaustivo de todas las actividades relacionadas con el tráfico y dispositivos. - Elaboración de informes sobre todas las actividades de tráfico y de dispositivos.
R	Los equipos deben actualizarse de forma dinámica y automática
Software y servicios	
R	Gestión por interfaces GUI (política, logs, usuarios...) y terminal (SSH)
R	Monitorización a través de SNMP, telnet y HTTP
R	Debe ser compatible con FortiManager para integrarse dentro de la solución actualmente implementada para la gestión de las configuraciones del cortafuego
R	Debe ser compatible con FortiAnalyzer para integrarse dentro de la solución actualmente implementada para la gestión de los logs del cortafuego
R	La solución debe incluir el soporte Hardware y las licencias necesarias para todas las funcionalidades descritas en el pliego técnico por un periodo de 3 años.
R	La solución debe incluir una suscripción de 3 años para le gestión y almacenamiento de los logs con un límite de 5GB / día con el soporte de FortiCare, IOC, SOC y FortiGuard.

5.6. LOTE 6 Suministro e instalación de servidores para servicios informáticos para el CNAG-CRG.

Se requiere la instalación en el CPD del CNAG-CRG en el edificio PCB de un sistema compuesto de 2 servidores y de un almacenamiento compartido para la instalación de todos los servicios necesarios para la gestión administrativa del CNAG-CRG (servidores de autenticación, servidores de DNS, servidores de DHCP, servidores de impresión…).

Especificaciones Técnicas

A continuación, se describe en detalle las especificaciones técnicas de cada uno de los aspectos.
En las especificaciones técnicas, cada elemento de la lista se clasificará de la siguiente manera:
R: indicando que es un requerimiento obligatorio que la solución debe cubrir
D: indicando que es un requerimiento no obligatorio

Todos los equipos ofertados no pueden estar en la lista de “End-of-Sale” del fabricante.
Todo el material, conectores y adaptadores necesarios incluidos, debe ser nuevo y original del fabricante.
Las ópticas (SFPs) que se solicitan deben ser originales del fabricante.

Ref	Descripción
Servidor	
R	Debe ofrecer 2 servidores que cumplan individualmente con las características mínima siguientes: • 2 procesadores x86_64 con un minimo de 16 cores y una frecuencia de 2.4GHz • 128 GB de memoria • 2 discos internos de una capacidad mínima de 240GB (Los discos internos deberán ser SSD y deberán ser intercambiables en caliente en caso de fallo hardware) • Interface HBA Fiber Channel de 16Gbps
R	Los 2 servidores deben tener las conexiones siguientes: • 1 conexión 100Mbps para la gestión • 2 conexiones de 10Gbps para los datos • 2 conexiones fiber channel de 16Gbps para el acceso al almacenamiento
R	Cada servidor debe tener un sistema de control remoto para la gestión de la configuración, de las alertas, para arrancar remotamente el servidor
R	Cada servidor debe tener una fuente de alimentación redundante.
R	Cada servidor debe tener una altura de 1U
Almacenamiento	
R	La solución debe ofrecer 1 cabina de almacenamiento que cumpla con las características mínimas siguientes: - Doble tarjeta fiber channel para la conexión con los 2 servidores - Capacidad mínima de 10TiB netos en RAID6 distribuido
R	El almacenamiento debe tener las conexiones siguientes: • 1 conexión 100Mbps para la gestion • 4 conexiones fiber channel de 16Gbps para la conexión con los servidores
R	El almacenamiento debe tener un sistema de control remoto para la gestión de la configuración, de las alertas, para arrancar remotamente el servidor
R	El almacenamiento debe tener una fuente de alimentación redundante.
R	El almacenamiento debe tener una altura máxima de 4U

5.7. LOTE 7: Suministro e instalación de nodos de cómputo para el proyecto vPDX

Se requiere el suministro e instalación de nodos para el clúster existente para proporcionar computación de alto rendimiento para el proyecto vPDX en CNAG-CRG.

La extensión solicitada en esta especificación aumentará en un mínimo de 256 el número de núcleos de propósito general para computación científica interconectados por una red de alto rendimiento y baja latencia basada en 100 GbE.

Los aceleradores de procesadores basados en GPU o de la familia Xeon Phi no se considerarán para el cálculo de este número de núcleos ofrecidos.

Todos los nodos de la solución tendrán las mismas características

Especificaciones técnicas

En las siguientes tablas se describen los requisitos del equipo y se asignan las letras R o D según si se trata de un requisito que debe cumplirse en la solución presentada (R) o de un requisito deseable a tener y que se valorarán positivamente aquellas soluciones que lo incorporen (D).

L2. Especificaciones técnicas de los nodos de clúster

Ref	Descripción
R	Dos nodos de cómputo cada uno con las siguientes características: • 2 unidades centrales de procesamiento de código de instrucciones compatibles con x86_64, con 64 núcleos y frecuencia base (sin tener en cuenta Max Boost) de 2.2GHz (como, por ejemplo, AMD EPYC 7662, o equivalente). • 1024 GB de memoria principal (tecnología DDR4-3200 mínima) • Dos SSD de 2,5" con una capacidad mínima de 480 GB y una resistencia mínima de 1,5 DWPD
R	Se considerarán unidades centrales de procesamiento de características técnicas equivalentes a AMD EPYC 7662con al menos el mismo nivel de rendimiento medido utilizando el punto de referencia passmark , siempre que tengan al menos 64 núcleos.
R	Todos los nodos de cómputo deben tener las siguientes interfaces de red: • Al menos dos interfaces Gigabit Ethernet con una conexión configurable para arrancar el nodo mediante PXE (red en banda) y la otra para la gestión fuera de banda (por ejemplo, ipmi, idrac, bmc, etc.) • Interfaz dual 100 Gigabit Ethernet (QSFP56) para la red de datos, que permitirá conexiones redundantes entre los nodos informáticos y el almacenamiento científico.
R	Los nodos de cómputo contarán con un sistema de gestión fuera de banda que permitirá el acceso a una consola remota, la monitorización de alarmas y el encendido y apagado.
R	Los nodos y cualquier elemento de la expansión deben tener una fuente de alimentación redundante.
R	Los nodos no pueden exceder 1U y pueden compartir un chasis común para mejorar esta densidad mínima.
R	En el caso de compartir el mismo chasis, cada nodo se puede quitar del chasis sin afectar al resto de nodos, que podrán seguir funcionando normalmente (intercambiables en caliente)
R	Todo el hardware del nodo informático será compatible con el sistema operativo CentOS 7 y 8.

5.8. LOTE 8: Suministro e instalación de ampliación de almacenamiento para el proyecto vPDX.

Se requiere el suministro e instalación de nodos para ampliar el sistema Dell-EMC Isilon existente que consta de 4 nodos H500 y 30 nodos A2000, a fin de proporcionar almacenamiento de alto rendimiento para el proyecto vPDX en CNAG-CRG. El sistema actual tiene un rack con un espacio disponible de 4U. Se prevé que este espacio se llene con 4 nodos de alto rendimiento que brinden almacenamiento SSD y se colocarán nodos de alto rendimiento adicionales que brinden almacenamiento SSD en el bastidor suministrado como parte del Lote 3 en esta licitación.

Especificaciones técnicas

Las especificaciones técnicas de cada aspecto se describen en detalle a continuación.

En las especificaciones técnicas, cada elemento de la lista se clasificará como sigue:

R: indicando que es un requisito obligatorio que la solución debe cubrir. D: indicando que es un requisito no obligatorio.

Ref	Descripción
R	La expansión del sistema debe aumentar la capacidad neta total en un mínimo de 15,3 TB, calculado como el aumento de la capacidad neta del sistema medido desde un cliente NFS utilizando el comando "df -h". Toda la capacidad adicional debe estar disponible para extender cualquier volumen en el sistema actual y para estar disponible en el mismo espacio de nombres global.
R	La expansión debe mantener la habilidad de los sistemas actuales para escalar a más de 200 módulos en un solo sistema distribuido donde todos los módulos comparten recursos, el trabajo se distribuye y no son necesarios módulos especiales o maestros.
R	La expansión debe mantener la propiedad del sistema actual de ser un único sistema coherente. La memoria caché de todos los módulos adicionales debe ser compartida y coherente con el sistema actual. El aumento mínimo de GB de RAM que la expansión debe añadir al sistema existente debe ser de 480 GB, y debe mantener la capacidad del sistema para crecer en el futuro mediante la incorporación de nuevos módulos con memoria adicional de hasta decenas de Terabytes de memoria global.
R	Todos los módulos adicionales deben tener un sistema de memoria con SPS (StandBy Power Supply) para garantizar la consistencia de la memoria en caso de pérdida de energía de uno o más módulos.
R	Para garantizar la adaptabilidad a cualquier nuevo entorno, la expansión debe mantener la capacidad actual del sistema para mezclar diferentes tipos de módulos a medida que crece. Siempre respetando la arquitectura donde cada módulo añade rendimiento y/o capacidad. Esta flexibilidad permitirá que el sistema global escale linealmente hacia el eje de rendimiento o hacia el eje de capacidad según sea necesario mediante la adición de módulos apropiados al sistema.
R	La expansión debe mantener la propiedad del sistema actual de que, si se mezclan diferentes tipos de módulos en el mismo sistema, se crearán diferentes niveles de servicio. A nivel de datos, y en base a políticas, debe existir la posibilidad de poder

	decidir en qué nivel de servicio queremos que los datos lleguen y residan, permitiendo que cambien automáticamente a otros niveles de servicio a medida que se cumplan ciertas condiciones (días de inactividad, etc...).
R	La expansión debe mantener la capacidad del sistema actual para proporcionar al menos dos niveles de servicio distintos, uno para la información más caliente y utilizada más recientemente y otro para datos archivados más fríos que deberían tener un costo por terabyte más barato que la capa caliente.
R	Los módulos que se agregan al sistema deben tener discos SSD destinados al almacenamiento de datos y metadatos para proporcionar el alto rendimiento requerido para esta carga de trabajo.
R	El número de módulos a proponer será de 5 módulos para este nivel de servicio de cargas de trabajo exigentes.
R	El sistema ampliado final debe ser capaz de equilibrar la capacidad de los diferentes módulos para poder ofrecer un rendimiento y ocupación comparables en todos y cada uno de ellos.
R	Cada nodo adicional debe proporcionar un mínimo de 1 puerto de red a 1 Gbps y un mínimo de dos puertos a 25 Gbps para el acceso desde equipos cliente cada uno (frontend). También se debe incluir el cableado necesario para conectar los módulos de extensión a la red CNAG-CRG a través de Ethernet de 25 Gb.
R	El rendimiento general del sistema global después de la expansión debería aumentar en al menos 14,8 GB/s en 100% de lectura y 8,7 GB/s en 100% de escritura.
R	Se incluirán los equipos de red y cableado necesarios que permitan la interconexión de los nuevos módulos con el sistema existente y mantendrán al menos el mismo nivel de conectividad por nodo del sistema actual.
R	La expansión debe mantener la capacidad de la solución actual para admitir la creación de pools de discos en los que almacenar archivos según directivas de antigüedad o tamaño, pero siempre dentro del mismo volumen.
R	La expansión debe mantener la capacidad del sistema actual para admitir el control de ocupación de espacio en disco en función de las directivas de usuario, grupo o directorio. También debe tener plantillas que sean automáticas y aplicables de forma predeterminada a las nuevas estructuras para directivas de usuario, grupo y directorio. Dichas políticas deben poder crearse y eliminarse en directorios con contenido existente, así como anidados en árboles de directorios complejos (políticas dentro de las políticas).
R	Los clientes deben poder utilizar cualquiera de los módulos del sistema expandido final y además tener acceso a todo el espacio tanto desde clientes Linux (soportará al menos Red Hat, Scientific Linux y CentOS), como Windows y Mac OS X, tanto en arquitectura x86 como en arquitectura x86_64.
R	El sistema ampliado debe mantener la autoridad para integrarse con Active Directory, LDAP e incluso ofrecer la posibilidad de definir ACL internamente.
R	El sistema ampliado debe mantener la utilidad de ofrecer la posibilidad de administración a través de la web, a través de CLI y a través de la API REST.
R	El sistema ampliado debe mantener el sistema de equilibrio de carga integrado para garantizar que las conexiones del cliente al sistema se distribuyan uniformemente entre los módulos de manera óptima y automática. Dicho equilibrio de carga debe poder particularizarse por entorno y considerar como variables el número de conexiones, el rendimiento o la CPU de cada nodo del sistema.

R	El sistema ampliado debe seguir soportando diferentes tipos de protección configurable y definible en caliente en cualquier momento y en cualquier nivel de segmentación (a nivel de recurso compartido, exportación, carpeta o incluso archivo), incluidos los tipos de protección que pueden soportar una falla de disco cuádruple para adaptar la confiabilidad a los datos durante su vida útil.
R	El sistema ampliado debe seguir teniendo funciones de autogestión para eliminar tareas, como la desfragmentación, de modo que el rendimiento no se degrade con el tiempo.
R	El sistema ampliado debe seguir ofreciendo sistemas proactivos de supervisión de bajo nivel que permitan poner en cuarentena un disco antes de que falle.
R	La solución ampliada debe seguir admitiendo el acceso a cualquier parte del sistema de archivos utilizando al menos los siguientes protocolos: NFSv3, NFSv4, SMB2, SMB3 (disponibilidad continua, multicanal, copia del lado del servidor, cifrado SMB3), HTTP, FTP, S3 y HDFS de forma nativa sin puertas de enlace.
R	Independientemente del protocolo utilizado para crear un archivo, el sistema expandido debe seguir permitiendo el acceso al mismo por cualquiera de los otros protocolos incluidos en la propuesta, en tiempo real, e incluso con los archivos en uso, pero siempre asegurando la coherencia en los datos.
R	El sistema expandido debe continuar la capacidad de realizar una actualización del sistema operativo de una manera no disruptiva, así como permitir que los administradores reviertan a la versión anterior si lo hacen. Esta reversión debe poder ser utilizada por los administradores del sistema sin la necesidad de involucrar un soporte especial del fabricante o proveedor de la plataforma.
R	El sistema ampliado debe seguir ofreciendo la posibilidad de filtrar los archivos que tienen que ser almacenados y no permitir que se almacenen ciertas políticas (Bloqueo de archivos por extensión)
R	La solución expandida debe continuar la propiedad de que el impacto en el rendimiento de una falla del módulo no excederá en ningún caso el 10%, y este porcentaje debe disminuir a medida que el sistema crece.
R	El sistema expandido debe seguir soportando la caída de cualquier módulo y de desplazar a otro módulo todos los clientes que estaban conectados a él, de forma transparente y sin necesidad de interrumpir el servicio con esos clientes para NFS, SMB3 y HDFS.
R	El sistema expandido debe garantizar la coherencia de los datos cuando se accede a ellos o se guardan en el sistema de archivos.
R	El sistema expandido debe poder conectarse a conmutadores de diferentes fabricantes para acceder desde equipos cliente.
R	El sistema ampliado debe seguir ofreciendo la posibilidad de deduplicar la información, independientemente del protocolo y/o ubicación de los datos dentro del sistema. Esta funcionalidad no se requiere de entrada, pero el sistema debe estar listo para ser activado cuando se considere apropiado.
R	El sistema ampliado debe ser capaz de ofrecer una gestión basada en diferentes tenants.
R	La solución expandida debe ser capaz de integrarse con diferentes directorios activos a la vez.
R	La solución ampliada debe ser capaz de integrarse con diferentes proveedores de nube. Esta integración debería permitir la capacidad de archivar el contenido del

	sistema en la nube utilizando el protocolo S3.
	El sistema ampliado debe incluir todo el software necesario para ofrecer toda la funcionalidad solicitada.

Instalación

Ref	Descripción
R	Se deben incorporar las PDU necesarias para conectar el sistema con líneas monofásicas de 32A.
R	Todos los componentes de la expansión (rack, servidor, switch, cable, fibra,...) deben estar debidamente etiquetados, para ser identificados físicamente de forma única según la nomenclatura establecida entre CNAG-CRG y la empresa instaladora. Los cables y fibras deberán indicar el origen y el destino de la conexión.
R	Se debe incluir el montaje en rack de toda la expansión , además de la recolección de todos los materiales sobrantes de la instalación y el transporte.
R	Se debe incluir todo el hardware necesario para montar la expansión , así como los cables de alimentación correspondientes.

Documentación y formación

R	La documentación debe presentarse en formato digital en español o inglés en el que se describa: - Descripción general de los componentes de la solución - Esquema de conexiones e IP e instalación en el rack - Diagrama con la ocupación de los racks con los diversos equipos presentados en la solución y el número de U utilizadas por cada uno. - Ajustes de configuración utilizados - Explicación del proceso de instalación y las tareas realizadas
R	Se proporcionará formación que cubra suficientemente: - Conceptos, administración básica y procedimientos básicos de configuración - Optimización de la solución - Solución de problemas
R	Se debe presentar y evaluar un plan de proyecto. Este plan se acordará con el equipo técnico del CRG para minimizar los cortes y efectos en el servicio

5.9. LOTE 9: Suministro e instalación de ampliación de almacenamiento para el proyecto 3Domics.

Se requiere el suministro e instalación de nodos de alta capacidad / archiving para expandir el sistema Del-EMC Isilon existente que consta de 4 nodos H500 y 30 nodos A2000, a fin de proporcionar almacenamiento masivo para el proyecto 3DOmics en CNAG-CRG. El sistema actual tiene un chasis capaz de admitir cuatro nodos A2000 que actualmente contiene solo 2 nodos. Se requieren dos nodos adicionales que tengan las mismas características y que sean compatibles con los nodos A2000 existentes para llenar el chasis.

Especificaciones técnicas

Las especificaciones técnicas de cada aspecto se describen en detalle a continuación.

En las especificaciones técnicas, cada elemento de la lista se clasificará como sigue:

R: indicando que es un requisito obligatorio que la solución debe cubrir. D: indicando que es un requisito no obligatorio.

Ref	Descripción
R	Los 2 nodos deben aumentar la capacidad neta total en un mínimo de 360 TB, calculado como el aumento de la capacidad neta del sistema medido desde un cliente NFS utilizando el comando "df -h". Toda la capacidad adicional debe estar disponible para extender cualquier volumen en el sistema actual y para estar disponible en el mismo espacio de nombres global.
R	La expansión debe mantener la habilidad de los sistemas actuales para escalar a más de 200 módulos en un solo sistema distribuido donde todos los módulos comparten recursos, el trabajo se distribuye y no son necesarios módulos especiales o maestros.
R	La expansión debe mantener la propiedad del sistema actual de ser un único sistema coherente. La memoria caché de todos los módulos adicionales debe ser compartida y coherente con el sistema actual. El aumento mínimo de GB de RAM que la expansión debe añadir al sistema existente debe ser de 128 GB, y debe mantener la capacidad del sistema para crecer en el futuro mediante la incorporación de nuevos módulos con memoria adicional de hasta decenas de Terabytes de memoria global.
R	Todos los módulos adicionales deben tener un sistema de memoria con SPS (StandBy Power Supply) para garantizar la consistencia de la memoria en caso de pérdida de energía de uno o más módulos.
R	Para garantizar la adaptabilidad a cualquier nuevo entorno, la expansión debe mantener la capacidad actual del sistema para mezclar diferentes tipos de módulos a medida que crece. Siempre respetando la arquitectura donde cada módulo añade rendimiento y/o capacidad. Esta flexibilidad permitirá que el sistema global escale linealmente hacia el eje de rendimiento o hacia el eje de capacidad según sea necesario mediante la adición de módulos apropiados al sistema.
R	Esta expansión debe mantener la propiedad del sistema actual de que mientras se mezclan diferentes tipos de módulos en el mismo sistema, se crearán diferentes niveles de servicio. A nivel de datos, y en base a políticas, debe existir la posibilidad de poder decidir en qué nivel de servicio queremos que los datos lleguen y residan, permitiendo que cambien automáticamente a otros niveles de servicio a medida que se cumplan ciertas condiciones (días de inactividad, etc...).
R	La expansión debe mantener la capacidad del sistema actual para proporcionar al menos dos niveles de servicio distintos, uno para la información más caliente y utilizada más recientemente y otro para datos archivados más fríos que deberían tener un costo por terabyte más barato que la capa caliente.
R	Los módulos que se agregan al sistema deben tener discos SSD destinados al almacenamiento y la caché de metadatos para al menos mantener el nivel actual de rendimiento de metadatos por módulo del sistema actual.

R	El sistema ampliado final debe ser capaz de equilibrar la capacidad de los diferentes módulos para poder ofrecer un rendimiento y ocupación comparables en todos y cada uno de ellos.
R	La expansión debe mantener la propiedad del sistema actual para poder replicar datos al sistema de almacenamiento de réplicas CRG manteniendo todos los parámetros de identificación de usuarios, permisos POSIX y ACL y tiempos de creación, modificación y acceso. Esta replicación debe realizarse a nivel de bloque entre cada iteración de réplica y debe utilizar la tecnología de instantáneas en origen y destino para garantizar la coherencia continua de los datos. No se requiere que esta funcionalidad esté disponible en el sistema suministrado, pero debe poder activar esta funcionalidad cuando se considere apropiado.
R	Cada nodo adicional debe proporcionar un mínimo de 1 puerto de red a 1 Gbps y un mínimo de dos puertos a 25 Gbps para el acceso desde equipos cliente cada uno (frontend). También se debe incluir el cableado necesario para conectar los módulos de extensión a la red CNAG-CRG a través de Ethernet de 25 Gb.
R	El rendimiento general del sistema global después de la expansión debería aumentar en al menos 1,3 GB/s en 100% de lectura y 1,1 GB/s en 100% de escritura.
R	Se incluirán los equipos de red y cableado necesarios que permitan la interconexión de los nuevos módulos con el sistema existente y mantendrán al menos el mismo nivel de conectividad por nodo del sistema actual.
R	La expansión debe mantener la capacidad de la solución actual para admitir la creación de pools de discos en los que almacenar archivos según directivas de antigüedad o tamaño, pero siempre dentro del mismo volumen.
R	La expansión debe mantener la capacidad del sistema actual para admitir el control de ocupación de espacio en disco en función de las directivas de usuario, grupo o directorio. También debe tener plantillas que sean automáticas y aplicables de forma predeterminada a las nuevas estructuras para directivas de usuario, grupo y directorio. Dichas políticas deben poder crearse y eliminarse en directorios con contenido existente, así como anidados en árboles de directorios complejos (políticas dentro de las políticas).
R	Los clientes deben poder utilizar cualquiera de los módulos del sistema expandido final y además tener acceso a todo el espacio tanto desde clientes Linux (soportará al menos Red Hat, Scientific Linux y CentOS), como Windows y Mac OS X, tanto en arquitectura x86 como en arquitectura x86_64.
R	El sistema ampliado debe mantener la autoridad para integrarse con Active Directory, LDAP e incluso ofrecer la posibilidad de definir ACL internamente.
R	El sistema ampliado debe mantener la utilidad de ofrecer la posibilidad de administración a través de la web, a través de CLI y a través de la API REST.
R	El sistema ampliado debe mantener el sistema de equilibrio de carga integrado para garantizar que las conexiones del cliente al sistema se distribuyan uniformemente entre los módulos de manera óptima y automática. Dicho equilibrio de carga debe poder particularizarse por entorno y considerar como variables el número de conexiones, el rendimiento o la CPU de cada nodo del sistema.
R	El sistema ampliado debe seguir soportando diferentes tipos de protección configurable y definible en caliente en cualquier momento y en cualquier nivel de segmentación (a nivel de recurso compartido, exportación, carpeta o incluso archivo), incluidos los tipos de protección que pueden soportar una falla de disco cuádruple

	para adaptar la confiabilidad a los datos durante su vida útil.
R	El sistema ampliado debe seguir teniendo funciones de autogestión para eliminar tareas, como la desfragmentación, de modo que el rendimiento no se degrade con el tiempo.
R	El sistema ampliado debe seguir ofreciendo sistemas proactivos de supervisión de bajo nivel que permitan poner en cuarentena un disco antes de que falle.
R	La solución ampliada debe seguir admitiendo el acceso a cualquier parte del sistema de archivos utilizando al menos los siguientes protocolos: NFSv3, NFSv4, SMB2, SMB3 (disponibilidad continua, multicanal, copia del lado del servidor, cifrado SMB3), HTTP, FTP, S3 y HDFS de forma nativa sin puertas de enlace.
R	Independientemente del protocolo utilizado para crear un archivo, el sistema expandido debe seguir permitiendo el acceso al mismo por cualquiera de los otros protocolos incluidos en la propuesta, en tiempo real, e incluso con los archivos en uso, pero siempre asegurando la coherencia en los datos.
R	El sistema expandido debe continuar la capacidad de realizar una actualización del sistema operativo de una manera no disruptiva, así como permitir que los administradores reviertan a la versión anterior si lo hacen. Esta reversión debe poder ser utilizada por los administradores del sistema sin la necesidad de involucrar un soporte especial del fabricante o proveedor de la plataforma.
R	El sistema ampliado debe seguir ofreciendo la posibilidad de filtrar los archivos que tienen que ser almacenados y no permitir que se almacenen ciertas políticas (Bloqueo de archivos por extensión)
R	La solución expandida debe continuar con la propiedad de que el impacto en el rendimiento del fallo de un módulo no excederá en ningún caso el 10%, y este porcentaje debe disminuir a medida que el sistema crece.
R	El sistema expandido debe seguir soportando la caída de cualquier módulo y de desplazar a otro módulo todos los clientes que estaban conectados a él, de forma transparente y sin necesidad de interrumpir el servicio con esos clientes para NFS, SMB3 y HDFS.
R	El sistema expandido debe garantizar la coherencia de los datos cuando se accede a ellos o se guardan en el sistema de archivos.
R	El sistema expandido debe poder conectarse a conmutadores de diferentes fabricantes para acceder desde equipos cliente.
R	El sistema ampliado debe seguir ofreciendo la posibilidad de deduplicar la información, independientemente del protocolo y/o ubicación de los datos dentro del sistema. Esta funcionalidad no se requiere de entrada, pero el sistema debe estar listo para ser activado cuando se considere apropiado.
R	El sistema ampliado debe ser capaz de ofrecer una gestión basada en diferentes tenants.
R	La solución expandida debe ser capaz de integrarse con diferentes directorios activos a la vez.
R	La solución ampliada debe ser capaz de integrarse con diferentes proveedores de nube. Esta integración debería permitir la capacidad de archivar el contenido del sistema en la nube utilizando el protocolo S3.
R	El sistema ampliado debe incluir todo el software necesario para ofrecer toda la funcionalidad solicitada.

Instalación

Ref	Descripción
R	Se deben incorporar las PDU necesarias para conectar el sistema con líneas monofásicas de 32A.
R	Todos los componentes de la expansión (rack, servidor, switch, cable, fibra...) deben estar debidamente etiquetados, para ser identificados físicamente de forma única según la nomenclatura establecida entre CNAG-CRG y la empresa instaladora. Los cables y fibras deberán indicar el origen y el destino de la conexión.
R	Se debe incluir el montaje en rack de toda la expansión , además de la recolección de todos los materiales sobrantes de la instalación y el transporte.
R	Se debe incluir todo el hardware necesario para montar la expansión , así como los cables de alimentación correspondientes.

Documentación y formación

R	La documentación debe presentarse en formato digital en español o inglés en el que se describa: - Descripción general de los componentes de la solución - Esquema de conexiones e IP e instalación en el rack - Diagrama con la ocupación de los racks con los diversos equipos presentados en la solución y el número de U utilizadas por cada uno. - Ajustes de configuración utilizados - Explicación del proceso de instalación y las tareas realizadas
R	Se proporcionará formación que cubra suficientemente: - Conceptos, administración básica y procedimientos básicos de configuración - Optimización de la solución - Solución de problemas
R	Se debe presentar y evaluar un plan de proyecto. Este plan se acordará con el equipo técnico del CRG para minimizar los cortes y efectos en el servicio

5.12. Especificaciones técnicas generales de los lotes 1, 3, 4, 7, 8 y 9.

Las siguientes especificaciones son comunes a los lotes 1, 3, 4, 7, 8, 9 de esta especificación técnica.

Infraestructura	
R	Todos los equipos (no aplicable para los lotes 3, 8 y 9) se instalarán en racks provistos por el CNAG-CRG de 19" y 42U, refrigerados por puertas frías activas y con 6 PDUs conectadas a la red a través de 6 C-TAC de 32A
R	En la documentación se debe presentar un diagrama con la ocupación de los racks con los diversos equipos presentados en la solución y el número de U utilizadas por cada uno.
R	Todo conexionado entre racks se deberá realizar a través de la parte superior del rack, no se permitirá la tirada de cables entre racks colindantes o por el falso suelo. El cableado dentro del rack deberá ser ordenado y nunca salir del espacio que determina la planta del rack.
R	Cada componente de la solución (rack, servidor, switch, cable, fibra,...) debe estar

	debidamente etiquetado, para ser identificado físicamente de forma única según la nomenclatura establecida entre el CNAG-CRG y la empresa instaladora. En los cables y fibras se deberá indicar el origen y destino de la conexión.
R	Se debe incluir el montaje de toda la solución en los racks, además de la recogida de todos los materiales sobrantes de la instalación y transporte.
R	Se deben incluir todas las guías, soportes y elementos necesarios para la correcta instalación del hardware, así como todos los cables de alimentación correspondientes.
Mantenimiento y soporte	
R	Garantía del fabricante y soporte estándar en todos los componentes de hardware (siguiente día hábil) y software.
R	Se facilitará lo siguiente: • Acceso a todo el software de actualización (incluidos los sistemas operativos y el firmware) de todos los componentes de la solución • Único punto de soporte para la notificación de problemas e incidencias de cualquier componente que conforma la solución
R	La documentación deberá presentarse en formato digital en inglés o español en el que se describa: • Descripción general de los componentes de la solución • Esquema de conexiones e IPs e instalación en el rack • Opciones de configuración utilizadas • Explicación del proceso de instalación y de las tareas realizadas
R	Se impartirá una formación que abarque suficientemente: • Conceptos, administración básica y procedimientos básicos de configuración • Optimización de soluciones • Solución de problemas
R	Se debe presentar y evaluar un plan de proyecto. Este plan se acordará con el equipo técnico del CNAG-CRG para minimizar los cortes y efectos en el servicio.

6. Garantía, mantenimiento y soporte

Esta parte describe los requisitos y extensiones relacionados con el mantenimiento y soporte de la solución a nivel global.

Ref	**Descripción**
R	Garantía estándar del fabricante y soporte en todos los componentes de los diferentes lotes (siguiente día hábil). Los días laborables estarán definidos por el calendario oficial definido por la Generalitat de Catalunya de festivos generales y locales en Cataluña y en la ciudad de Barcelona.
R	Se proporcionará un único punto de soporte (dentro del período de garantía y

	soporte) para solucionar problemas de cualquier componente de hardware que compone la solución.
R	Se requerirá soporte proactivo, notificando y recomendando actualizaciones de la versión de firmware de cualquier componente de la solución.

7. Suministro e instalación de equipos y plazos

Se considerarán las siguientes fases del proyecto con sus correspondientes hitos:

1. La fase de entrega, instalación y configuración del sistema objeto del suministro. Esta fase se iniciará a partir del día de la formalización del contrato y tendrá lugar en las instalaciones especificadas en el mismo, en la ciudad de Barcelona

.

2. Una vez recibido, instalado y configurado el sistema, se llevará a cabo la formación y se pondrá en producción real y se iniciará la fase de prueba de aceptación. Durante esta fase el CNAG-CRG verificará que el sistema cumple con los requisitos solicitados. Una vez finalizada con éxito esta fase, se emitirá la correspondiente acta de recepción y aceptación.

Para la ejecución de las fases indicadas de entrega, instalación y configuración del sistema y la prueba de aceptación, no podrá superarse el plazo máximo según la tabla en anexo desde la formalización del contrato.

lote	Nombre del lote	Plazos máximos en semanas- de recepción , instalación, configuración, validación, puesta en marcha y formación
1	Suministro e instalación de una solución de virtualización para los nodos de servicio del clúster de computación científica del CNAG - CRG	16
2	Suministro e instalación de switches de red para el CRG	26
3	Ampliación de capacidad y rendimiento de un sistema de almacenamiento para el clúster de computación científica del CNAG – CRG	15
4	Suministro e instalación de equipos para el clúster de computación científica CNAG-CRG	14
5	Suministro e instalación de cortafuegos para la red CNAG-CRG	12

6	Suministro e instalación de servidores para servicios informáticos para el CNAG-CRG	26
7	Suministro e instalación de nodos de cómputo para el proyecto vPDX.	14
8	Suministro e instalación de ampliación de almacenamiento para el proyecto vPDX.	15
9	Suministro e instalación de ampliación de almacenamiento para el proyecto 3Domics.	6

3. Posteriormente, se iniciará la fase de garantía, mantenimiento y soporte, una vez finalizada con éxito la fase de prueba de aceptación y emitido el informe de recepción y aceptación.

7.1 Plan del proyecto

El licitador deberá aportar el plan de proyecto correspondiente sobre su propuesta técnica. El plan del proyecto deberá contemplar y describir la metodología a utilizar durante al menos las fases indicadas en el apartado anterior y los recursos correspondientes para su cumplimiento.

El plan del proyecto también debe presentar toda la información que se necesitará del CNAG-CRG durante la fase de instalación.

7.2 Fase de entrega, instalación y configuración

Una vez recibido el material, se instalará y configurará, fases que incluirán al menos todos los trámites y todos los trabajos que el licitante considere necesarios para poder iniciar correctamente la fase de prueba de aceptación.

Una vez finalizada esta fase, el licitador presentará el expediente correspondiente, que contendrá al menos los documentos indicados en el apartado correspondiente del pliego de condiciones técnicas.

7.3 Fase de prueba de aceptación

Tras la entrega, instalación y configuración, se realizará la correspondiente puesta en marcha de los equipos.

Durante el período de prueba de aceptación, el CNAG-CRG verificará y el licitante deberá demostrar que las especificaciones de funcionalidad y rendimiento proporcionadas en el pliego de condiciones se cumplen utilizando el sistema instalado en producción.

En caso de anomalías, el CNAG-CRG notificará al licitante de acuerdo con el protocolo acordado en la fase de entrega, instalación y configuración y el licitante deberá corregir las deficiencias antes de que finalice el período de prueba de aceptación.

Una vez realizada la formación y el equipo en funcionamiento en los términos de funcionalidad y rendimiento indicados, y una vez recibida la documentación descrita en este folleto por parte del CNAG-CRG, tendrá lugar el acto formal y positivo de recepción y aceptación del material. que se formalizará mediante documento firmado por el adjudicatario y por el CNAG-CRG.

7.4 Garantía. Mantenimiento y soporte

La garantía, mantenimiento y soporte cumplirán con los requisitos mínimos (indicados en el apartado correspondiente de esta especificación) desde la firma del informe de instalación y cubrirán cualquier tipo de fallo de hardware en el entorno habitual del CNAG-CRG.

El costo del transporte de equipos o repuestos hacia y desde las instalaciones de CNAG-CRG para reparaciones o reemplazos estará incluido en la garantía.

Cualquier sustitución se realizará con un módulo que sea exactamente el mismo que el original en todas sus características. Excepcionalmente, y bajo el acuerdo explícito del CNAG-CRG, la sustitución podrá ser compatible con la original, pero de mayor capacidad.

En caso de fallos en más del 10% de los módulos durante el primer mes de operación, el proveedor deberá sustituir el 100% de los módulos ofrecidos por otros con igual rendimiento y cuyas especificaciones estén acordadas con el CNAG-CRG.

De lo contrario, se considerará que el proveedor ha incumplido una obligación contractual esencial.

En el caso de tres o más fallos de hardware en el mismo módulo durante cualquier período de seis meses dentro del período de garantía, no se aceptarán reparaciones adicionales a ese módulo y el proveedor debe proporcionar una unidad de reemplazo.

En caso de fallo del mismo componente de hardware en más del 20% de los módulos, el proveedor debe reemplazar el mismo componente en el 100% de los módulos.

8. Condiciones de aceptación

En este apartado se describen aquellas pruebas o condiciones que deben cumplirse para ser aceptadas según lo requerido en esta licitación.

Ref	Descripción
R	Una vez finalizada la instalación, se deberá verificar que se cumplen todos los requisitos establecidos en esta especificación para los diferentes lotes.

9. Financiación

9.1: Lotes 1, 3 y 4

El objeto de este contrato está cofinanciado al 50% por el Fondo Europeo de Desarrollo Regional (FEDER) de la Unión Europea, dentro del Proyecto de Ampliación de la capacidad de cálculo y almacenamiento masivo de datos genómicos con referencia, IU16-006344 en el marco del Programa Operativo FEDER de Cataluña 2014-2020 para la potenciación de las Grandes Infraestructuras Científicas y Tecnológicas con participación de la Generalitat de Catalunya, siendo el 50% restante cofinanciado con fondos internos del centro procedentes de la Generalitat de Catalunya

9.2: Lotes 2, 5 y 6

El presente contrato está financiado al 100% con los fondos internos del centro provenientes de la Generalitat de Catalunya

9.2: Lotes 7 y 8

El Proyecto del cual forman parte estos dos lotes para Suministro e instalación de nodos de cómputo y ampliación de almacenamiento han recibido financiación de la Fundación “la Caixa” con el código de proyecto HR20-00411

9.3. Lote 9

El sistema de almacenaje incluido en este lote forma parte de un proyecto que ha recibido financiación del programa de investigación e innovación Horizon 2020 de la Unión Europea en virtud del acuerdo de subvención n. 101000309

En Barcelona, el 9 de mayo de 2022

ÓRGANO DE CONTRATACIÓN CRG