ESPECIFICACIONES TECNICAS

OFERTAS

El oferente deberá presentar junto a la oferta:

Documentación que demuestre su condición de representante comercial en el país, de la/s marca/s de equipos ofertados, por medio de una nota extendida por el/los fabricante/s. No se aceptarán notas extendidas por mayoristas o empresas intermediarias.

Documentación que demuestre disponer de personal técnico certificado por el/los fabricante/s para las líneas de producto incluidas en su oferta, adjuntando los certificados correspondientes.

Nota emitida por el fabricante autorizando al oferente a presentar una oferta con equipamiento de su marca en el presente concurso, en la que se deberá detallar los productos que forman parte de la oferta.

Todos los requerimientos técnicos y funcionalidades esperadas de acuerdo a lo solicitado en el presente pliego, deben operar tanto en forma independiente unas de otras como en forma totalmente integrada y/o simultánea, sin limitación alguna.

1.1. Todos los elementos necesarios para dar cumplimiento a lo dispuesto por la cláusula anterior y nominada en el cuadro inferior deberán ser ofertados por el oferente como parte integral de su propuesta y entregados en su oportunidad, se hayan requerido expresamente o no en el presente Pliego de Especificaciones Técnicas Básicas.

Ren-glón	Ítem	Bien Ofertado / Servicio Conexo	Ref. Pliego	Canti-dad
1	1	Firewall de CORE	4.1	1
	2	Firewall para Estación Experimental	4.2	10
	3	Sistema de gestión centralizado	4.3	1
2	1	Switch de CORE	5.1	2
	2	Switch ToR	5.2	4
3	1	HPE M6710 1.2TB 6G SAS 10K 2.5in HDD. Part Number E7X49A.	7.1	28
	2	1.2 HPE 3Y Proactive Care 24x7 Service. Part Number H1K92A3#WUT.	7.1	28
4	1	SERVIDORES HP BL460 GEN10 PARA AM-PLIACION DE ENCLOSURE HP C7000 EXISTENTE EN EL INTA	8.1	2
5	1	16GB 2Rx4 PC3L-12800R-11 Kit PARA AM-PLIACION DE BL460c GEN8. (PN: 713985-B21)	9.1	40

Tabla General

PLAN DE ENTREGA Y CUMPLIMIENTO

Todos los plazos se contarán en días corridos a partir de la fecha de firma y recepción por parte de la empresa proveedora de la correspondiente Orden de Compra.

Todos los bienes serán entregados, en las dependencias que el INTA dispone en calle Chile 460 de la Ciudad autónoma de buenos aires, dentro de los sesenta (60) días corridos o bien en el Datacenter de *la empresa Telecom S.A. en la localidad de Gral. Pacheco provincia de Buenos Aires.*

De corresponder, al momento de entregarse los bienes deberá aportarse la documentación relativa a la importación de los mismos, incluyendo la licencia de exportación de software.

ESPECIFICACIONES TÉCNICAS GENERALES del EQUIPAMIENTO

Consideraciones Generales de todo el equipamiento a proveer

Todas las facilidades, features, características y especificaciones del hardware y software ofertado que sean necesarias para que dicho hardware y software se ajuste a los requerimientos de equipamiento y sistemas aquí enunciados, deberán estar disponibles (liberadas al mercado) al momento de la apertura de las ofertas. No se aceptarán facilidades que solo están disponibles en versiones beta de los paquetes de software o a modo de prototipo en el hardware.

Los elementos, unidades funcionales, dispositivos y accesorios estarán constituidos por unidades nuevas, sin uso previo y en perfecto estado de conservación y funcionamiento (se entiende por nuevo y sin uso, a que el INTA será el primer usuario de los equipos desde que estos salieron de fábrica).

El equipo ofrecido deberá cumplir con las especificaciones en materia de regulación de seguridad eléctrica, emisión de radiofrecuencia, emisión electromagnética y emisión de radiación, emitidas por los organismos competentes de los Estados Unidos, Canadá, la Comunidad Europea, Japón o equivalentes.

El equipamiento ofrecido deberá cumplir con todas las normas y recomendaciones que hayan emitido los organismos públicos y/o privados, nacionales e internacionales de competencia. Serán también exigibles las especificaciones que hubiere fijado la Comisión Nacional de Comunicaciones y que se encuentren en vigencia, cumpliendo además las normas del UIT-T (ex CCITT) de 1988 y conexas, además de los estándares IEEE, y las recomendaciones IETF Request for Comments (RFC), IMTC y ETSI correspondientes.

El equipo a proveer deberá estar vigentes y no poseer fecha de discontinuidad de fabricación a la fecha de presentación de la oferta.

El Oferente garantizará por escrito mediante declaración jurada incluida en la oferta, que estará en condiciones de seguir efectuando el mantenimiento, provisión de repuestos y soporte técnico tanto del hardware como del software de todos los bienes a proveer, durante un plazo de por lo menos tres (3) años a partir de la fecha de presentación de la oferta, independientemente de la continuidad de los bienes en el mercado por parte de la Empresa fabricante.

Todos los equipos a proveer deberán operar con corriente alterna de 220 V, 50 Hz, con conexión a tierra, sin posibilidad de conmutar manualmente a otro voltaje/frecuencia.

El equipo deberá poseer dos o más fuentes de alimentación que permitan al mismo seguir operando en caso de fallo en una de ellas.

Cada fuente de alimentación deberá ser provista con su respectivo cable de energía eléctrica, para tomacorriente de tres patas planas según norma IRAM 2073/82.

Todos los equipos ofrecidos deberán operar en rangos de temperatura ambiente desde 5 a 40 grados centígrados, sin necesidad de acondicionamiento especial.

El equipamiento deberá entregarse con todos los accesorios necesarios para su correcta instalación y funcionamiento, entiéndase por esto fuentes de alimentación, cables de conexión, y drivers de software.

Renglón 1

Consideraciones particulares del equipamiento Firewall de CORE

Se deberán proveer un (1) Firewall, que deberá operar en redundancia Activo-Activo con el actual equipo de CORE marca FortiNet modelo FortiGate 900D instalado en el NOC de la institución y poseer como mínimo las siguientes características técnicas:

Poseerá compatibilidad con todos y cada uno de los siguientes estándares: Gigabit Ethernet IEEE 802.3z y 10Gigabit Ethernet IEEE 802.3ae.

Cada Firewall deberá soportar la configuración de al menos dos (2) interface SFP+ 10Gigabit Ethernet *para conexión con redes WAN/LAN y veinte (20) interfaces Gigabit Ethernet para redes WAN/LAN de* las cuales la mitad deberán poseer bahías SPF para la instalación de módulos para fibra óptica multimodo y monomodo.

El sistema deberá permitir la definición de al menos doscientas cincuenta (250) interfaces virtuales (VLANs) en la que será posible definir al menos una interface IP por cada una.

El mecanismo de control de filtrado utilizado por el engine del firewall deberá estar basado en técnicas "statefull inspection" que crean conexiones virtuales, incluso para los protocolos connection-less como UDP y RPC.

El Firewall deberá poseer las configuraciones localmente, no dependiendo su funcionamiento de las herramientas de gestión centralizados.

Las reglas deben permanecer en medio físico, no volátil. Estas reglas deberán poder definirse, diferenciando protocolo, IP destino / IP origen, puerto destino / puerto origen y rango horario.

El dispositivo deberá soportar al menos la generación de 100.000 políticas de firewall.

El equipo deberá soportar la definición de al menos diez dominios virtuales.

El dispositivo deberá soportar SNAT, DNAT y PAT. Será posible la aplicación de SNAT y DNAT y PAT en forma simultánea sobre una misma conexión.

Deberá soportar NAT estático y dinámico y PAT sobre cualquier tipo de conexión, tanto para IPv4 como IPv6. Deberá soportar NAT46 y NAT64 sobre la totalidad de las políticas de firewall.

Deberá soportar la configuración de NAT estático sobre todas las interfaces físicas y lógicas utilizando direcciones IP virtuales que no sean las propias IP declaradas en las interfaces del firewall.

Cada Firewall deberá permitir el uso de objetos dinámicos aplicables a todo tipo de regla, definiendo las propiedades de los mismos sobre cada Firewall en particular. Los objetos deben poder referenciar servidores y redes como mínimo.

Cada Firewall deberá poseer capacidad de manejo de apertura de puertos dinámicos en base a protocolos de uso común (HTTP, SMTP, FTP, H323, SIP) y posibilidad de crear sesiones personalizadas que manejen dicho comportamiento.

Cada firewall no deberá tener un límite de concurrencia de usuarios impuesto por el hardware ni por el software o licencias.

Cada firewall deberá permitir al menos la recepción y tratamiento de 250.000 nuevas conexiones por segundo y deberá soportar al menos 10.000.000 de conexiones concurrentes.

El equipo deberá poseer la capacidad de entregar direcciones IP a los hosts conectados en sus interfaces LAN por medio del protocolo DHCP (DHCP server).

Cada Firewall deberá además soportar las siguientes funcionalidades:

- Autenticación de usuarios en forma local y remota por medio de los protocolos RADIUS y LDAP, debiendo ser compatible con Active Directory.
- Certificación ICSA en Firewall.

- Soporte de IPSec NAT Traversal.

Soporte de encaminamiento estático y dinámico soportando al menos los protocolos RIP y OSPF. El equipo deberá poder definir al menos 10.000 rutas estáticas para IPv4 y al menos 500 para IPv6.

El equipo deberá permitir la generación VPN de tipo Site to Site y Client to Site.

- El Firewall deberá soportar la generación de VPN utilizando protocolo IPSEC estándar o a través de SSL.

- Cada Firewall deberá permitir al menos dos mil (2000) VPN de cualquier tipo, activas simultáneamente, mediante IPSec o SSL, con mecanismo de intercambio de llaves para VPN de tipo Diffie Hellman Grupo 1,2 y 5 y mecanismos de autenticación de VPN mediante certificados digitales y clave pre-compartida.

- Deberá poseer certificación ICSA en IPSec.

El equipo, con su funcionalidad de Firewall activada, deberá soportar un tráfico consolidado entre todas sus interfaces (suma del tráfico no encriptado que cruza el Firewall) de por lo menos 30 Gbps para paquetes de cualquier tamaño y protocolo. Para la funcionalidad de VPN IPSec con encriptado 3DES de 168-bits, hash MD5 y SHA-1, deberá de soportar un throughput de al menos 25 Gbps. Para la funcionalidad de VPN SSL, deberá de soportar un throughput de al menos 4 Gbps.

La solución deberá soportar la funcionalidad de Proxy explicito para conexiones de los protocolos HTTP/HTTPS.

El Firewall deberá soportar la activación y desactivación de la funcionalidad de IPS y detección de anomalías para los protocolos soportados.

- Deberá soportar un throughput de IPS de al menos 4 Gbps ya sea para conexiones HTTP o cualquier otro protocolo.

- Deberá realizar el análisis de IPS basado en firmas las cuales se deberán poder agrupar para aplicar a las reglas.

- Deberá permitir armar firmas propias de IPS, a través de expresiones irregulares.

- Deberá realizar la actualización de firmas de IPS en forma automática y periódica, durante el periodo de garantía.

- Deberá poseer una base de conocimiento que detalle la definición de la regla.

- Deberá ante un ataque de IPS responder con una notificación o un bloqueo del tráfico.

- Deberá poseer la capacidad de excluir para una regla específica, una firma en particular; sin que ello implique deshabilitar por completo la utilización de esa firma en las demás reglas.

El Firewall deberá soportar la activación y desactivación de técnicas de detección y evasión de ataques de DOS (Denegación de servicio).

Cada Firewall deberá soportar la activación y desactivación de técnicas de protección de ataques de generación masiva de conexiones (SYN attack) permitiendo su configuración para una dirección IP en particular.

Deberá tener la posibilidad de aplicar la funcionalidad de antivirus por regla sobre conexiones HTTP, FTP, SMTP, POP3, IMAP y túneles VPN encriptados establecidas a través del equipo.

- Deberá permitir configurar excepciones para archivos de determinado tamaño o tipo.

- Deberá permitir la actualización automática de la base de filtrado antivirus durante el transcurso del período de garantía.

Deberá tener la funcionalidad de filtrado de contenidos Web.

- Deberá permitir o bloquear el acceso de los usuarios a diferentes sitios web considerados o no maliciosos.
- Deberá permitir la actualización automática de la base de filtrado de contenidos durante el transcurso del período de garantía.
- Deberá soportar al menos cincuenta (50) categorías en la base de filtrado.

Deberá tener la funcionalidad para detectar aplicaciones específicas agrupadas en al menos 16 categorías y aplicar políticas de seguridad a las mismas. Deberá poder definir al menos 250 sensores y soportar un throughput de 7 Gbps.

El equipo deberá proveerse con los servicios de actualización de firmas para los motores de filtrado descriptos en los puntos 3.2.22, 3.2.23, 3.2.24 y 3.2.25 por el término de 12 meses.

El equipo deberá poder resguardar su configuración de forma remota en un almacén central.

Debe permitir la administración del equipo por medio de los protocolos HTTP/HTTPS, Telnet/SSH y SNMP v1/v2.

Deberá permitir el registro local y remoto de eventos utilizando servidores syslog. La capacidad de almacenamiento local no podrá ser inferior a 240 GB.

Consideraciones particulares del equipamiento Firewall para Estación Experimental

Se deberán proveer diez (10) Firewalls, que deberán poseer como mínimo las siguientes características técnicas:

Poseerá compatibilidad con todos y cada uno de los siguientes estándares: Gigabit Ethernet IEEE 802.3z y 10Gigabit Ethernet IEEE 802.3ae.

Cada Firewall deberá soportar la configuración de al menos dos (2) interface SFP Gigabit Ethernet y diez (10) interfaces Gigabit Ethernet para redes WAN/LAN. Las interfaces SFP deberán soportar la instalación de módulos para fibra óptica multimodo y monomodo.

El sistema deberá permitir la definición de al menos doscientas cincuenta (250) interfaces virtuales (VLANs) en la que será posible definir al menos una interface IP por cada una.

El mecanismo de control de filtrado utilizado por el engine del firewall deberá estar basado en técnicas "statefull inspection" que crean conexiones virtuales, incluso para los protocolos connection-less como UDP y RPC.

El Firewall deberá poseer las configuraciones localmente, no dependiendo su funcionamiento de las herramientas de gestión centralizados.

Las reglas deben permanecer en medio físico, no volátil. Estas reglas deberán poder definirse, diferenciando protocolo, IP destino / IP origen, puerto destino / puerto origen y rango horario.

El dispositivo deberá soportar al menos la generación de 5.000 políticas de firewall.

El equipo deberá soportar la definición de al menos diez dominios virtuales.

El dispositivo deberá soportar SNAT, DNAT y PAT. Será posible la aplicación de SNAT y DNAT y PAT *en forma simultánea sobre una misma conexión.*

Deberá soportar NAT estático y dinámico y PAT sobre cualquier tipo de conexión, tanto para IPv4 como IPv6. Deberá soportar NAT46 y NAT64 sobre la totalidad de las políticas de firewall.

Deberá soportar la configuración de NAT estático sobre todas las interfaces físicas y lógicas utilizando direcciones IP virtuales que no sean las propias IP declaradas en las interfaces del firewall.

Cada Firewall deberá permitir el uso de objetos dinámicos aplicables a todo tipo de regla, definiendo las propiedades de los mismos sobre cada Firewall en particular. Los objetos deben poder referenciar servidores y redes como mínimo.

Cada Firewall deberá poseer capacidad de manejo de apertura de puertos dinámicos en base a protocolos de uso común (HTTP, SMTP, FTP, H323, SIP) y posibilidad de crear sesiones personalizadas que manejen dicho comportamiento.

Cada firewall no deberá tener un límite de concurrencia de usuarios impuesto por el hardware ni por el software o licencias.

Cada firewall deberá permitir al menos la recepción y tratamiento de 25.000 nuevas conexiones por segundo y deberá soportar al menos 1.000.000 de conexiones concurrentes.

El equipo deberá poseer la capacidad de entregar direcciones IP a los hosts conectados en sus interfaces LAN por medio del protocolo DHCP (DHCP server).

Cada Firewall deberá además soportar las siguientes funcionalidades:

- Autenticación de usuarios en forma local y remota por medio de los protocolos RADIUS y LDAP, debiendo ser compatible con Active Directory.
- Certificación ICSA en Firewall.
- Soporte de IPSec NAT Traversal.

Soporte de encaminamiento estático y dinámico soportando al menos los protocolos RIP y OSPF. El equipo deberá poder definir al menos 500 rutas estáticas para IPv4 e IPv6.

El equipo deberá permitir la generación VPN de tipo Site to Site y Client to Site.

- El Firewall deberá soportar la generación de VPN utilizando protocolo IPSEC estándar o a través de SSL.
- Cada Firewall deberá permitir al menos doscientos (200) VPN de cualquier tipo, activas simultáneamente, mediante IPSec o SSL, con mecanismo de intercambio de llaves para VPN de tipo Diffie Hellman Grupo 1,2 y 5 y mecanismos de autenticación de VPN mediante certificados digitales y clave pre-compartida.
- Deberá poseer certificación ICSA en IPSec.

El equipo, con su funcionalidad de Firewall activada, deberá soportar un tráfico consolidado entre todas sus interfaces (suma del tráfico no encriptado que cruza el Firewall) de por lo menos 4 Gbps para paquetes de cualquier tamaño y protocolo. Para la funcionalidad de VPN IPSec con encriptado 3DES de 168-bits, hash MD5 y SHA-1, deberá de soportar un throughput de al menos 2 Gbps. Para la funcionalidad de VPN SSL, deberá de soportar un throughput de al menos 200 Mbps.

La solución deberá soportar la funcionalidad de Proxy explicito para conexiones de los protocolos HTTP/HTTPS.

El Firewall deberá soportar la activación y desactivación de la funcionalidad de IPS y detección de anomalías para los protocolos soportados.

- Deberá soportar un throughput de IPS de al menos 400 Mbps ya sea para conexiones HTTP o cualquier otro protocolo.
- Deberá realizar el análisis de IPS basado en firmas las cuales se deberán poder agrupar para aplicar a las reglas.
- Deberá permitir armar firmas propias de IPS, a través de expresiones irregulares.
- Deberá realizar la actualización de firmas de IPS en forma automática y periódica, durante el periodo de garantía.
- Deberá poseer una base de conocimiento que detalle la definición de la regla.
- Deberá ante un ataque de IPS responder con una notificación o un bloqueo del tráfico.

- Deberá poseer la capacidad de excluir para una regla específica, una firma en particular; sin que ello implique deshabilitar por completo la utilización de esa firma en las demás reglas.

El Firewall deberá soportar la activación y desactivación de técnicas de detección y evasión de ataques de DOS (Denegación de servicio).

Cada Firewall deberá soportar la activación y desactivación de técnicas de protección de ataques de generación masiva de conexiones (SYN attack) permitiendo su configuración para una dirección IP en particular.

Deberá tener la posibilidad de aplicar la funcionalidad de antivirus por regla sobre conexiones HTTP, FTP, SMTP, POP3, IMAP y túneles VPN encriptados establecidas a través del equipo.

- Deberá permitir configurar excepciones para archivos de determinado tamaño o tipo.

Deberá tener la funcionalidad de filtrado de contenidos Web.

- Deberá permitir o bloquear el acceso de los usuarios a diferentes sitios web considerados o no maliciosos.
- Deberá soportar al menos cincuenta (50) categorías en la base de filtrado.

Deberá tener la funcionalidad para detectar aplicaciones específicas agrupadas en al menos 16 categorías y aplicar políticas de seguridad a las mismas. Deberá poder definir al menos 30 sensores y soportar un throughput de 500 Mbps.

El equipo deberá poder resguardar su configuración de forma remota en un almacén central.

Debe permitir la administración del equipo por medio de los protocolos HTTP/HTTPS, Telnet/SSH y SNMP v1/v2.

Deberá permitir el registro local y remoto de eventos utilizando servidores syslog.

Consideraciones particulares del sistema de gestión centralizado

Se deberán proveer un sistema de gestión centralizado en para los dispositivos destinados a estaciones experimentales incluidos en el presente renglón, que deberán poseer como mínimo las siguientes características técnicas:

Deberá estar basado en una aplicación capaz de correr en modo de virtual appliance permitiendo a futuro la ampliación de la misma a través de licencias de software.

Poseerá compatibilidad con todos y cada uno de los siguientes hypervisores: VMware ESX/ESXi 5.0/5.1/5.5/6.0, Microsoft Hyper-V 2008 R2/2012/2012 R2, Citrix XenServer 6.0+, Open Source Xen 4.1+, KVM y Amazon Web Services (AWS).

La capacidad inicial deberá permitir la gestión de al menos 10 dispositivos, con una capacidad final que deberá ser superior a 1000 dispositivos.

Deberá poder manejar una capacidad de almacenamiento de al menos 100 GB.

Deberá poder colectar al menos 1 GB de registros diarios de los diferentes equipos a los cuales está gestionando.

La herramienta, una vez implementada, deberá poder:

- Gestionar dispositivos individualmente o agrupados en grupos lógicos
- Realizar actualizaciones de fostware/firmware
- Descubrir nuevos dispositivos automáticamente.
- Crear, desplegar y monitorear redes privadas virtuales
- Delegar el control de funciones especificas a usuarios específicos
- Realizar auditorías de configuración y sus cambios en los dispositivos gestionados

Renglón 2

Consideraciones particulares del equipamiento Switch de CORE

Se deberán proveer dos (2) conmutadores, que deberán poder operar en modalidad de clúster virtual con los conmutadores instalados actualmente (marca Alcatel*Lucent modelo OmniSwitch 6900) en el centro de datos y en el NOC de la institución. El equipamiento deberá poseer como mínimo las siguientes características técnicas:

La configuración mínima de cada Conmutador de núcleo para MDF incluirá:

Conmutador de núcleo	Cantidad
Puertos 100/1000Base-T (RJ-45 UTP) para gestión fuera de banda	1
Puertos Ethernet 1/10GBase-T (RJ-45 UTP)	16
Bahías Ethernet 1/10GBase-X (SFP+)	10
Bahías Fibre channel 2/4/8 Gbps (SFP+)	2
Cables DAC SFP+ 10Gigabit Ethernet de 7 mts	2

La cantidad de fuentes de alimentación deberá ser la mínima necesaria para el correcto funcionamiento de los equipos. Los equipos deberán soportar una o más fuentes de redundancia (n+1), de forma tal que el fallo de cualquier fuente, no impacte en el funcionamiento de ningún elemento del sistema. Las fuentes podrán ser internas o externas. Las fuentes serán balanceadas, del tipo hot-swap y deben disponer de tomas de potencia individuales para cada una de ellas. La falla de una, no deberá ocasionar pérdida alguna de la información en tránsito por el dispositivo.

Se proveerá con un grupo de ventiladores internos, del tipo hot-swap, montados dentro del chasis, con la cantidad de unidades suficiente para extraer el calor generado por todas las placas internas de cada conmutador.

La performance de conmutación deberá ser de al menos 600 Gbps (Full rate) con la configuración inicial indicada en la Tabla anterior.

Los puertos 10 Gigabit Ethernet deberán tener conectores RJ-45 estándar para interfaces 1/10G Base-T o Bahías SFP+ estándar para interfaces 10 Gigabit Ethernet de fibra óptica multimodo/monomodo.

Poseerá compatibilidad con todos y cada uno de los siguientes estándares: Ethernet IEEE 802.3, Fast Ethernet IEEE 802.3u, Gigabit Ethernet IEEE 802.3z, 10 Gigiabit Ethernet IEEE 802.3ae, Spanning Tree IEEE 802.1d, Fast spanning tree 802.1w, Rapid spanning tree 802.1s.

Deberán poder efectuar el tagging de VLANs mediante el estándar IEEE 802.1Q. Los equipos deberán soportar etiquetados QinQ según el estándar IEEE 802.1ad.

El equipo deberá soportar FCoE según el estándar T11 FC-BB-5. Adicionalmente, deberá guardar compatibilidad con los estándares IEEE 802.1Qbg, IEEE 802.1Qbb e IEEE 802.1Qaz.

El equipo deberá soportar multi-chasis link aggregation.

El equipo deberá implementar IEEE 802.1aq (Shortest path bridging) o algún protocolo similar que permita controlar una topología full mesh utilizando todos los vínculos existentes simultáneamente. En caso de no utilizar SPB, el oferente deberá aclarar en su oferta que protocolo propone y una breve descripción de su funcionamiento

El equipo deberá poder definir al menos 250 interfaces IP simultáneas, soportando por hardware al menos 64 dominios de reenvío virtuales (VRF). El throughput efectivo no podrá ser inferior a 450 Mpps en capa 3.

El sistema de encaminamiento deberá ser compatible y operar bajo los siguientes protocolos de encaminamiento IP adicionales a los solicitados: OSPF v2/v3, IS-IS, BGPv4 y sus extensiones para IPv6. El equipo deberá encaminar e interactuar con IP multicast a través de los siguientes protocolos: DVMRP y PIM-SM.

Operará con capacidad de redundancia de encaminador mediante protocolo VRRPv2/v3.

Consideraciones particulares del equipamiento Switch ToR

Se deberán proveer cuatro (4) conmutadores destinado a ser utilizados dentro del NOC de la institución. El equipamiento deberá poseer como mínimo las siguientes características técnicas:

La configuración mínima de cada Conmutador de núcleo para MDF incluirá:

Conmutador de núcleo	Cantidad
Puertos 100/1000Base-T (RJ-45 UTP) para gestión fuera de banda	1
Puertos Gigabit Ethernet 1000Base-T (RJ-45 UTP)	20
Bahías Ethernet 1/10GBase-X (SFP+)	4
Cables DAC SFP+ 10Gigabit Ethernet de 7 mts	2

Los conmutadores deberán poder operar en modo virtual Chasis. La interconexión entre elementos del chasis virtual se llevará a cabo por puertos específicos para tal fin, adicionales a los especificados y la performance agregada no podrá ser inferior a 40 Gbps. Se deberá proveer para cada equipo un cable de interconexión con al menos 1 mt de longitud.

El virtual chasis deberá comportarse como una única entidad lógica desde el punto de vista administrativo, de gestión y monitoreo, es decir que todos los equipos que lo componen, serán accedidos mediante una sola dirección IP.

La cantidad de fuentes de alimentación deberá ser la mínima necesaria para el correcto funcionamiento de los equipos. Los equipos deberán soportar una o más fuentes de redundancia (n+1), de forma tal que el fallo de cualquier fuente, no impacte en el funcionamiento de ningún elemento del sistema. Las fuentes podrán ser internas o externas. Las fuentes serán balanceadas, del tipo hot-swap y deben disponer de tomas de potencia individuales para cada una de ellas. La falla de una, no deberá ocasionar pérdida alguna de la información en tránsito por el dispositivo.

Se proveerá con un grupo de ventiladores internos, del tipo hot-swap, montados dentro del chasis, con la cantidad de unidades suficiente para extraer el calor generado por todas las placas internas de cada conmutador.

La performance de conmutación deberá ser de al menos 200 Gbps (Full rate) con la configuración inicial indicada en la Tabla anterior.

Los puertos Gigabit Ethernet deberán tener conectores RJ-45 estándar para interfaces 100/1000Base-T. Las Bahías SFP+ estándar deberán soportar módulos de interfaces 10 Gigabit Ethernet de fibra óptica multimodo/monomodo.

Poseerá compatibilidad con todos y cada uno de los siguientes estándares: Ethernet IEEE 802.3, Fast Ethernet IEEE 802.3u, Gigabit Ethernet IEEE 802.3z, 10 Gigabit Ethernet IEEE 802.3ae, Spanning Tree IEEE 802.1d, Fast spanning tree 802.1w, Rapid spanning tree 802.1s.

Deberán poder efectuar el tagging de VLANs mediante el estándar IEEE 802.1Q. Los equipos deberán soportar etiquetados QinQ según el estándar IEEE 802.1ad.

El equipo deberá soportar multi-chasis link aggregation.

El equipo deberá implementar IEEE 802.1aq (Shortest path bridging) o algún protocolo similar que permita controlar una topología full mesh utilizando todos los vínculos existentes simultáneamente. En caso de no utilizar SPB, el oferente deberá aclarar en su oferta que protocolo propone y una breve descripción de su funcionamiento

El equipo deberá poder definir al menos 250 interfaces IP simultáneas, soportando por hardware al menos 64 dominios de reenvío virtuales (VRF). El throughput efectivo no podrá ser inferior a 150 Mpps en capa 3.

El sistema de encaminamiento deberá ser compatible y operar bajo los siguientes protocolos de encaminamiento IP adicionales a los solicitados: OSPF v2/v3, IS-IS, BGPv4 y sus extensiones para IPv6. El equipo deberá encaminar e interactuar con IP multicast a través de los siguientes protocolos: DVMRP y PIM-SM.

Operará con capacidad de redundancia de encaminador mediante protocolo VRRPv2/v3.

GARANTÍA DE BUEN FUNCIONAMIENTO PARA LOS RENGLONES 1 y 2.

Consideraciones generales

El plazo de la Garantía de Buen Funcionamiento para la totalidad de los bienes (hardware y software) será de 12 (doce) meses contados a partir de la emisión, por parte del Comprador, del Acta de Recepción Definitiva de los Bienes.

Deberá declararse bajo juramento que el oferente brindará por si o a través de sus subcontratistas, el servicio conexo de buen funcionamiento de acuerdo a lo solicitado para éste ítem, sin reservas significativas.

Todos los servicios a los que está obligado a realizar el Proveedor para cumplir con lo indicado en las Subcláusulas siguientes serán sin costo para el Comprador.

El servicio conexo de buen funcionamiento requerido alcanza a cualquier tipo de desperfecto, funcionamiento anormal, o fuera de servicio total o parcial, que ocurra sobre los bienes objeto de la presente (excluyéndose software), durante el plazo previsto para éste ítem y cualquiera fuese la causa que origine el desperfecto, funcionamiento anormal, o fuera de servicio, total o parcial. Entiéndase por desperfecto, funcionamiento anormal, o fuera de servicio, total o parcial, a cualquier tipo y clase de evento que no permita que los bienes requeridos, en forma conjunta o separada, puedan cumplir el desempeño deseado según las especificaciones técnicas realizadas.

El proveedor no podrá alegar inconvenientes con el fabricante para la obtención de los servicios mencionados, debiendo garantizar en toda circunstancia la posibilidad de escalamiento de los eventos.

El Adjudicatario brindará el buen funcionamiento preferentemente con personal especializado de la(s) empresa(s) fabricante(s) de los productos ofrecidos o de su representante oficial, o en su defecto con su propio personal o por un tercero, el que deberá estar debidamente certificado por él (los) fabricante(s) o su representante oficial. A sus efectos el Adjudicatario presentará la lista de técnicos habilitados para prestar el servicio al momento de la entrega de los bienes, pudiendo el INTA no aceptar el personal, total o parcialmente, propuesto. El Adjudicatario es responsable ante eventuales incumplimientos de los terceros que contrate.

Si el mantenimiento de los equipos no fuera efectuado directamente por el Adjudicatario, sino por un subcontratista, con la oferta se deberá adjuntar una declaración jurada de dicho contratista confirmando que acepta las condiciones de servicio estipuladas.

Todo el trabajo realizado por el Proveedor, sus empleados y subcontratistas conforme al contrato, será ejecutado con razonable habilidad y cuidado, y al menos con los niveles de habilidad y cuidados esperables de diseñadores y programadores competentes experimentados en los lenguajes de programación, herramientas y aplicaciones prácticas.

En caso que el Proveedor no pudiera concretar la reparación de los bienes dentro de los plazos estipulados deberá solucionar el inconveniente mediante el reemplazo de los bienes afectados por otros en condiciones de buen funcionamiento, sin que esto implique costo alguno para el Comprador.

El proveedor solo podrá efectuar dichos reemplazos con autorización explícita del INTA y no por su propia decisión.

Consideraciones particulares para el Servicio conexo de buen funcionamiento de hardware

Incluirá el servicio de reparación por personal calificado y reemplazo de las partes que se encuentren defectuosas por repuestos originales, nuevos y sin uso.

La reparación de los equipos deberá ser ejecutada a satisfacción del comprador, los equipos se entregarán al proveedor para su reparación en dependencias del INTA.

Consideraciones particulares para el Servicio conexo de buen funcionamiento de Software

La permanente actualización del software provisto, incluyendo el suministro de nuevas releases y versiones (cualquiera sea su nivel) y reparaciones (en general denominadas comercialmente como patches, temporary fixes, APARs, etc.), asimismo, también incluye, de ser necesario a criterio del Comprador, las tareas de instalación y configuración de los mismos (releases, versiones y reparaciones). Lo anterior alcanza e incluye a las actualizaciones tecnológicas producidas cuando el Proveedor libera al mercado del país de origen del software, una nueva versión del mismo producto, o un nuevo producto con características técnicas superiores – y que reemplazan al modelo ofrecido al comprador. Los nuevos releases, versiones, patches o fixes que sean liberados en el país de origen del software deberán ser puestos a disposición del comprador antes de treinta (30) días corridos de la fecha de liberación en el país de origen.

El análisis, determinación, corrección y documentación de problemas de software de base instalados. Para estos efectos el Comprador efectuará llamadas de servicio para soporte telefónico los días hábiles de 9:00 a 17:00 horas.

Si el problema de software produjera la detención del sistema el servicio de soporte deberá hacerse efectivo como si se tratara de una falla de hardware, según lo estipulado en cláusula servicio conexo de buen funcionamiento de hardware.

Renglón 3

Discos y soporte para ampliación de 33TB para sistema de almacenamiento HP 3PAR existente en el INTA.

ITEM	Descripción	Cantidad
1	HPE M6710 1.2TB 6G SAS 10K 2.5in HDD. **Part Number E7X49A.**	28
2	1.2 HPE 3Y Proactive Care 24x7 Service. **Part Number H1K92A3#WUT.**	28

Renglón 4

Servidores HP BL460 GEN10 para ampliación de Enclosure HP C7000 existente en el INTA. **Cantidad: 2 (dos)**

Procesadores: Dos (2) Intel Xeon-Gold 6130 (2.1GHz/16-core/120W)

Memoria RAM: 256GB (8x32GB) 2Rx4 PC4-2666V-R Smart Kit

Adaptadores de Red:

Un (1) HPE FlexFabric 10Gb 2P 536FLB FIO

Un (1) additional 10/100/1000 server adapter dedicated to iLO 5 management

Controladora de Discos: Smart Array P204i-b SR Gen10

Almacenamiento Interno: Dos (2) Discos HP de 300GB 6G SAS 15K rpm SFF (2.5-inch)

Licencias:

Un (1) HP iLO Advanced for BladeSystem 3 años 24x7 Technical Support and Updates E-LTU

SOPORTE

Soporte de garantía de hardware y Software (incluyendo partes, fletes y mano de obra) Pro Active Care por 3 años las 24 horas del día los 7 días de la semana con un tiempo de respuesta de 4hs.

Se deberá proveer con dos (2) licencias por servidor de VMware vSphere Enterprise Plus con Operation Management con subscripción de soporte por 3 años con asistencia 24x7.

Renglón 5

Memorias para ampliación de servidores HP BL460c Gen8 existentes en el INTA:

16GB 2Rx4 PC3L-12800R-11 Kit PARA AMPLIACION DE BL460c GEN8. (PN: 713985-B21)

Cantidad: 40 (Cuarenta)

Lic. Mariano Febo
Gerente de Contabilidad
y Gestión Administrativa (int.)