Dirección Nacional de Contrataciones Públicas
E.E.U.U. 961 c/ Tte. Fariña - Asunción, Paraguay
Tel. y Fax +595 21 4154000 - dncp@contrataciones.gov.py

Consultas Realizadas

Licitación 455042 - LPN N° 05/2024 "EXTENSIÓN DE GARANTÍA Y RENOVACIÓN DE SOPORTE DE EQUIPOS DEL DATACENTER" PLURIANUAL

Consulta 1 - Pliego de Bases y Condiciones/Porcentaje de multa

Consulta	Fecha de Consulta	12-10-2024

Se establece un porcentaje de multa por atraso de entrega de bienes de 0,50% por día de atraso.
Se solicita a la Convocante, establecer un % mas bajo de multa dentro de los estándares para evitar incumplimiento contractual en concordancia con la Ley 7021/2022 en su artículo c) Economía, Eficacia y Eficiencia: el Sistema Nacional de Suministro Público
buscará satisfacer las necesidades públicas con la oportunidad, la calidad y el costo
que aseguren al Estado paraguayo las mejores condiciones, la obtención de los
mejores resultados y el logro de las metas propuestas, a través de la utilización
adecuada de los recursos públicos.4- Principios Rectores inciso

Respuesta	Fecha de Respuesta	25-10-2024

El porcentaje de multa establecido por la Convocante tiene por finalidad la obtención de los mejores resultados y el logro de las metas propuestas, asegurando que en el caso de que el proveedor incumpla con el servicio contratado sea pasible de una multa equivalente al perjuicio causado a la institución, considerando la importancia de los datos albergados en los datacenter del MEC, los cuales son de uso institucional como de la ciudadanía.

Consulta 2 - Plazo de consultas

Consulta	Fecha de Consulta	12-10-2024

Solicitamos a la convocante extender la fecha actual de consultas, ya que consideramos que muy poco tiempo para analizar el llamado por el tamaño y la complicación de cumplimiento. La cual se podría interpretar como intención para para no permitir la participación de otros oferentes. en concordancia a lo dispuesto en la LEY N° 7021, en su Articulo 4- Principios rectores en su inciso d) Igualdad y Libre Competencia: todo potencial oferente que tenga la solvencia técnica, económica y legal necesaria para responder a los compromisos que supone la contratación con el Estado paraguayo y que cumpla con los requisitos establecidos en la presente Ley, en su reglamento, en las bases y condiciones y en las demás disposiciones administrativas, tendrá la posibilidad de participar sin restricciones y en igualdad de oportunidades en los procedimientos de contratación pública

Respuesta	Fecha de Respuesta	25-10-2024

Se informa que esta convocatoria se encuentra publicada desde fecha 04/10/24 por lo cual cumple con los plazos establecidos de publicación y consulta exigidos por las normativas vigentes.

Consulta 3 - Pliego de Bases y Condiciones/REQUISITOS DE PARTICIPACIÓN Y CRITERIOS DE EVALUACIÓN/Experiencia Requerida

Consulta	**Fecha de Consulta**	13-10-2024

Pliego de Bases y Condiciones/REQUISITOS DE PARTICIPACIÓN Y CRITERIOS DE EVALUACIÓN/Experiencia Requerida
Tratándose de una Extensión de Soporte de Datacenter, los requisitos establecidos están muy orientados a la provisión de Firewall, este siendo solo 1 ítem del proyecto, lo cual no necesariamente aplique a proveedores idóneos para los servicios que son solicitados. Adicionalmente, no se solicita experiencia en la provisión o instalación de equipos de las marcas existentes que garanticen la idoneidad del oferente para prestar los servicios solicitados.
Se solicita respetuosamente a la Convocante, que pueda reformular los requisitos de Experiencia Y Capacidad Técnica establecidos, de manera acorde y equitativa, según los servicios/bienes que son solicitados.

Respuesta	**Fecha de Respuesta**	25-10-2024

Esta claramente establecido la adecuación del Sistema de Seguridad de Red Perimetral además, la adquisición de este tipo de servicio y adecuación se encuentra orientada a la a dar mayor seguridad al sistema integral de todo el Datacenter, dentro de los cuales existen varios componentes que funcionan de manera sincronizada para obtener el resultado esperado
Los requisitos establecidos se encuentran redactados a fin de satisfacer de manera íntegra de todo el Datacenter

Consulta 4 - Pliego de Bases y Condiciones/REQUISITOS DE PARTICIPACIÓN Y CRITERIOS DE EVALUACIÓN/Capacidad Técnica, se solicita lo siguiente:

Consulta	**Fecha de Consulta**	13-10-2024

Autorización del fabricante o similar.
Para Grupo 1 ítem 1 al 11 Soporte Técnico Extendido para Datacenter Principal DCMT y para el Grupo 2 ítem 1 al 12 Soporte Técnico Extendido para Datacenter de Contingencia el oferente deberá presentar Carta de Autorización del Fabricante: La empresa oferente deberá contar con Autorización expedida por el fabricante para representantes, distribuidores y subdistribuidores de los productos ofrecidos; o el oferente deberá demostrar que cuenta con personal certificado en:
i. AOP -UPTIME INSTITUTE Accredited Operations Professional.
ii. ATS UPTIME INSTITUTE - Accredited Tier Specialist.

No se comprende la relación existente entre la Autorización del Fabricante/Distribuidor respecto a las certificaciones que son solicitadas, las que también podrían resultar limitativas para el llamado en cuestión.
Adicional a esto, no se solicitan criterios de calificación que consideren la experiencia y/o certificaciones técnicas del oferente en las marcas existentes que garanticen la idoneidad del oferente para prestar los servicios solicitados.
Solicitamos se pueda reformular los requisitos de capacidad técnica establecidos.

Respuesta	**Fecha de Respuesta**	25-10-2024

Esta claramente definido en los criterios de evaluación y las documentaciones técnicas solicitadas, además se ajusta lo peticionado en el PBC para dar mayor participación a potenciales oferentes y así no dirigir a un solo proveedor
La certificación solicitada es acorde a este tipo de llamado ya que es para administrar, mantener y tomar las decisiones adecuadas en cuanto a la seguridad de un datacenter por ende se requiere de técnicos especializados en área.

Consulta 5 - Pliego de Bases y Condiciones/REQUISITOS DE PARTICIPACIÓN Y CRITERIOS DE EVALUACIÓN/Capacidad Técnica

Consulta	Fecha de Consulta	13-10-2024

Pliego de Bases y Condiciones/REQUISITOS DE PARTICIPACIÓN Y CRITERIOS DE EVALUACIÓN/Capacidad Técnica, se solicita lo siguiente:
El oferente deberá contar con 2 personales con certificación ITILv4, dentro su staff permanente.

Solicitamos a la Convocante pueda aceptar ofertas que contemplen al menos 1 (un) personal ITILv4 dentro del staff permanente.

Respuesta	Fecha de Respuesta	25-10-2024

Se solicita esa cantidad por la criticidad del servicio de gestión, ya que es el Datacenter del MEC, y con esto se espera las mejores prácticas para la gestión de servicios de TI y mejorar los plazos de respuesta como lo dice la certificación. Además, ante la magnitud del servicio a contratar la cantidad de personal especializado solicitado es mínimamente a fin de garantizar el funcionamiento del datacenter

Consulta 6 - Pliego de Bases y Condiciones/SUMINISTROS REQUERIDOS – ESPECIFICACIONES TÉCNICAS/Grupo 1-ITEM 11. Adecuación del Sistema de Seguridad de Red Perimetral

Consulta	Fecha de Consulta	13-10-2024

Pliego de Bases y Condiciones/SUMINISTROS REQUERIDOS – ESPECIFICACIONES TÉCNICAS/Grupo 1-ITEM 11. Adecuación del Sistema de Seguridad de Red Perimetral, se solicita lo siguiente:
A fin de mejorar la seguridad perimetral de la red, se deberá de agregar 1 (un) equipo para alcanzar la redundancia en el Datacenter de Principal.
Sin embargo, en la tabla de especificaciones subsiguiente, se establece en Cantidad: 3 unidades.
Solicitamos a la Convocante, pueda aclarar la cobertura del servicio/bien requerido.

Respuesta	Fecha de Respuesta	25-10-2024

Al respecto será emitida una Adenda

Consulta 7 - Pliego de Bases y Condiciones/SUMINISTROS REQUERIDOS – ESPECIFICACIONES TÉCNICAS/ Grupo 1y 2 - ITEM 11. Adecuación del Sistema de Seguridad de Red Perimetral

Consulta	Fecha de Consulta	13-10-2024

Pliego de Bases y Condiciones/SUMINISTROS REQUERIDOS – ESPECIFICACIONES TÉCNICAS/ Grupo 1y 2 - ITEM 11. Adecuación del Sistema de Seguridad de Red Perimetral, se solicita lo siguiente:
Se solicita capacidad mínima de túneles IPSec Gateway-to-Gateway y Client-to-Gateway. Ciertos fabricantes de Firewall no especifican de manera aislada la cantidad de túneles IPSec soportados, por lo que solicitamos a la Convocante, establecer este requisito de manera unificada, especificando la cantidad mínima de túneles a ser soportados, adecuada según su infraestructura de TI.

Respuesta	Fecha de Respuesta	25-10-2024

Remitirse al Pliego. Esta claramente establecido la adecuación del Sistema de Seguridad de Red Perimetral en ambos datacenter deberán estar configurados en clúster por ende se requiere la extensión del existente y adecuación de lo que se requiera para que trabaje en la integración de ambos datacenter. Además, Los equipos ofertados deberán ser idéntico al equipo existente en la institución en sus componentes de Hardware y Software para la formación del clúster en alta disponibilidad. Por lo que cualquier equipo de distinta capacidad no podrá cumplir el esquema de redundancia que se está proyectando para los Data Center Principal y de Contingencia.

Consulta 8 - Pliego de Bases y Condiciones/SUMINISTROS REQUERIDOS – ESPECIFICACIONES TÉCNICAS/ Grupo 1y 2 - ITEM 11. Adecuación del Sistema de Seguridad de Red Perimetral

Consulta	Fecha de Consulta	13-10-2024

Pliego de Bases y Condiciones/SUMINISTROS REQUERIDOS – ESPECIFICACIONES TÉCNICAS/ Grupo 1y 2 - ITEM 11. Adecuación del Sistema de Seguridad de Red Perimetral, se solicita lo siguiente:
Se solicita 450.000 Nuevas Sesiones por Segundo.
Solicitamos a la Convocante pueda aceptar equipos que soporten al menos 400.000 Nuevas Sesiones por Segundo, siendo este número razonable, suficiente y con una diferencia no muy significativa a lo solicitado originalmente.

Respuesta	Fecha de Respuesta	25-10-2024

Remitirse al Pliego. Esta claramente establecido la adecuación del Sistema de Seguridad de Red Perimetral en ambos datacenter deberán estar configurados en clúster por ende se requiere la extensión del existente y adecuación de lo que se requiera para que trabaje en la integración de ambos datacenter. Además, Los equipos ofertados deberán ser idéntico al equipo existente en la institución en sus componentes de Hardware y Software para la formación del clúster en alta disponibilidad. Por lo que cualquier equipo de distinta capacidad no podrá cumplir el esquema de redundancia que se está proyectando para los Data Center Principal y de Contingencia.

Consulta 9 - Pliego de Bases y Condiciones/SUMINISTROS REQUERIDOS – ESPECIFICACIONES TÉCNICAS/ITEM 11. Adecuación del Sistema de Seguridad de Red Perimetral

Consulta	Fecha de Consulta	13-10-2024

Pliego de Bases y Condiciones/SUMINISTROS REQUERIDOS – ESPECIFICACIONES TÉCNICAS/ITEM 11. Adecuación del Sistema de Seguridad de Red Perimetral, se solicita lo siguiente:
A fin de mejorar la seguridad perimetral de la red, se deberá de agregar 1 (un) equipo para alcanzar la redundancia en el Datacenter de Principal.
Sin embargo, en Cantidad: 3 unidades. Se sugiere a la Convocante, solicitar equipos que posean mejor performance a los especificados para Seguridad Perimetral, y con esto, incluso poder disminuir la cantidad solicitada, contar con redundancia y lograr mayor eficiencia económica.

Respuesta	Fecha de Respuesta	25-10-2024

Remitirse al Pliego. Esta claramente establecido la adecuación del Sistema de Seguridad de Red Perimetral en ambos datacenter deberán estar configurados en clúster por ende se requiere la extensión del existente y adecuación de lo que se requiera para que trabaje en la integración de ambos datacenter. Además, Los equipos ofertados deberán ser idéntico al equipo existente en la institución en sus componentes de Hardware y Software para la formación del clúster en alta disponibilidad. Por lo que cualquier equipo de distinta capacidad no podrá cumplir el esquema de redundancia que se está proyectando para los Data Center Principal y de Contingencia.

Consulta 10 - Pliego de Bases y Condiciones/SUMINISTROS REQUERIDOS – ESPECIFICACIONES TÉCNICAS/ Grupo 1y 2 - ITEM 11. Adecuación del Sistema de Seguridad de Red Perimetral

Consulta	Fecha de Consulta	13-10-2024

Pliego de Bases y Condiciones/SUMINISTROS REQUERIDOS – ESPECIFICACIONES TÉCNICAS/ Grupo 1y 2 - ITEM 11. Adecuación del Sistema de Seguridad de Red Perimetral, se solicita lo siguiente:
Los equipos ofertados deberán contar con al menos 14 interfaces 1GE RJ45 – Exigido
Considerando que los equipos de Seguridad Perimetral solicitados contarán con la función de protección de Borde (su misión principal), y que a lo sumo se conectarán físicamente con equipos de Core dentro del Datacenter, por lo que no será necesario una cantidad considerable de puertos disponibles y que de seguro estas conexiones a nivel de core o distribución se realizarán con enlaces de mayor capacidad de tráfico, solicitamos a la Convocante, pueda aceptar equipos que ofrezcan al menos 6 (seis) puertos o interfaces de 1GE RJ45.

Respuesta	Fecha de Respuesta	25-10-2024

Remitirse al Pliego. Esta claramente establecido la adecuación del Sistema de Seguridad de Red Perimetral en ambos datacenter deberán estar configurados en clúster por ende se requiere la extensión del existente y adecuación de lo que se requiera para que trabaje en la integración de ambos datacenter. Además, Los equipos ofertados deberán ser idéntico al equipo existente en la institución en sus componentes de Hardware y Software para la formación del clúster en alta disponibilidad. Por lo que cualquier equipo de distinta capacidad no podrá cumplir el esquema de redundancia que se está proyectando para los Data Center Principal y de Contingencia.

Consulta 11 - Pliego de Bases y Condiciones/SUMINISTROS REQUERIDOS – ESPECIFICACIONES TÉCNICAS// Grupo 1y 2 - ITEM 11. Adecuación del Sistema de Seguridad de Red Perimetral

Consulta	Fecha de Consulta	13-10-2024

Pliego de Bases y Condiciones/SUMINISTROS REQUERIDOS – ESPECIFICACIONES TÉCNICAS// Grupo 1y 2 - ITEM 11. Adecuación del Sistema de Seguridad de Red Perimetral, se establece lo siguiente:
El Oferente deberá demostrar la capacidad de brindar soporte técnico local en la República del Paraguay, durante el periodo de garantía, de forma inmediata, para lo cual se deberá presentar Certificados de Capacitación Técnica (de al menos dos técnicos) de las versiones recientes de: Seguridad, Servidores, Switches, Routers, Software de Virtualización. Dichos técnicos mencionados en los Certificados de Capacitación deberán ser parte del plantel permanente del Oferente o podrá ser subcontratado.
El requisito no es muy específico respecto a la capacidad del oferente de instalar y configurar el Equipo ofertado. Solicitamos a la Convocante establecer un requisito más específico de manera a garantizar la calidad y lograr los resultados esperados.

Respuesta	Fecha de Respuesta	25-10-2024

Remitirse al Pliego. Esta claramente establecido "para lo cual se deberá presentar Certificados de Capacitación Técnica (de al menos dos técnicos) de las versiones recientes de: Seguridad, Servidores, Switches, Routers, Software de Virtualización. Dichos técnicos mencionados en los Certificados de Capacitación deberán ser parte del plantel permanente del Oferente o podrá ser subcontratado

Consulta 12 - Pliego de Bases y Condiciones/SUMINISTROS REQUERIDOS – ESPECIFICACIONES TÉCNICAS/ Grupo 1y 2 - ITEM 11. Adecuación del Sistema de Seguridad de Red Perimetral

Consulta	Fecha de Consulta	13-10-2024

Pliego de Bases y Condiciones/SUMINISTROS REQUERIDOS – ESPECIFICACIONES TÉCNICAS/ Grupo 1y 2 - ITEM 11. Adecuación del Sistema de Seguridad de Red Perimetral, se solicita lo siguiente:
El Oferente deberá contemplar curso oficial para 3 personas del Dpto. de Infraestructura Tecnológica dependiente de la Dirección de Tecnología de la Información y la Comunicación en configuración de del equipo, administración de políticas de seguridad, ruteo, ipp, clúster, nateo y políticas calidad de servicio, incluyendo los voucher para examen oficial, y todos los gastos incluidos para la capacitación fuera del país por el centro autorizado de entrenamiento (incluye pasajes aéreos, estadías, traslados, hospedajes y alimentación). La certificación debe ser oficial de la fabricante.
Considerando que tal servicio es solicitado para los equipos a ser ofertados para el Datacenter Principal y para el Datacenter de Contingencia, en caso, de ofertar equipos del mismo fabricante para ambos sitios, solicitamos a la Convocante aclarar si se deberán realizar de igual forma 2 eventos independientes, o se podría unificar a 1 solo evento de capacitación, que cumpla con los requisitos de entrenamiento establecidos en la presente especificación.

Respuesta	Fecha de Respuesta	25-10-2024

Esta claramente establecido en el Item correspondiente de lo que se requiere.

Consulta 13 - Pliego de Bases y Condiciones/SUMINISTROS REQUERIDOS – ESPECIFICACIONES TÉCNICAS/ Grupo 1y 2 - ITEM 11. Adecuación del Sistema de Seguridad de Red Perimetral

Consulta	Fecha de Consulta	13-10-2024

Pliego de Bases y Condiciones/SUMINISTROS REQUERIDOS – ESPECIFICACIONES TÉCNICAS/ Grupo 1y 2 - ITEM 11. Adecuación del Sistema de Seguridad de Red Perimetral, se establece lo siguiente:
Por razones de eficiencia de uso de energía, los equipos deberán contar con fuente de energía redundantes 100240VAC (5060Hz)
Se solicita a la Convocante esclarecer el requisito solicitado principalmente respecto a “100240VAC (5060Hz)” Considerar que el sistema eléctrico nacional es de 220V/50Hz.

Respuesta	Fecha de Respuesta	25-10-2024

Remitirse al Pliego. Esta claramente establecido la adecuación del Sistema de Seguridad de Red Perimetral en ambos datacenter deberán estar configurados en clúster por ende se requiere la extensión del existente y adecuación de lo que se requiera para que trabaje en la integración de ambos datacenter. Además, Los equipos ofertados deberán ser idéntico al equipo existente en la institución en sus componentes de Hardware y Software para la formación del clúster en alta disponibilidad. Por lo que cualquier equipo de distinta capacidad no podrá cumplir el esquema de redundancia que se está proyectando para los Data Center Principal y de Contingencia.

Consulta 14 - Pliego de Bases y Condiciones/SUMINISTROS REQUERIDOS – ESPECIFICACIONES TÉCNICAS/Grupo 2-ITEM 11. Adecuación del Sistema de Seguridad de Red Perimetral

Consulta	Fecha de Consulta	13-10-2024
Pliego de Bases y Condiciones/SUMINISTROS REQUERIDOS – ESPECIFICACIONES TÉCNICAS/Grupo 2-ITEM 11. Adecuación del Sistema de Seguridad de Red Perimetral, se solicita lo siguiente: A fin de mejorar la seguridad perimetral de la red, se deberán de agregar 2 (dos) equipos para reemplazar las 2 (dos) unidades existentes. Sin embargo, en la tabla de especificaciones subsiguiente, se establece en Cantidad: 3 unidades. Solicitamos a la Convocante, pueda aclarar la cobertura del servicio/bien requerido.		

Respuesta	Fecha de Respuesta	25-10-2024
Al respecto será emitida una Adenda		

Consulta 15 - Visita Tecnica

Consulta	Fecha de Consulta	14-10-2024
Solicitamos amablemente a la convocante establecer una fecha para visita técnica a los dos sitios objeto del llamado de manera a poder entender el alcance de la misma y preparar una oferte mas acorde.		

Respuesta	Fecha de Respuesta	25-10-2024
Remitirse al Pliego. Esta claramente establecido en el PBC lo que se requiere, se encuentra en detalle el alcance de los servicios a contratar, no es necesaria la visita a fin de entender el alcance de los mismos.		

Consulta 16 - Capacidad Técnica

Consulta	Fecha de Consulta	14-10-2024
Pliego de Bases y Condiciones/REQUISITOS DE PARTICIPACIÓN Y CRITERIOS DE EVALUACIÓN/Capacidad Técnica, se solicita lo siguiente: El oferente deberá contar con 2 personales con certificación ITILv4, dentro su staff permanente. Solicitamos a la Convocante omitir este requisito de manera a permitir mayor cantidad de oferentes o en su defecto permitir la contratación de personal con las mencionadas certificaciones.		

Respuesta	Fecha de Respuesta	25-10-2024
Se solicita esa cantidad por la criticidad del servicio y adaptar las mejores prácticas de gestión, ya que es el Datacenter del MEC, y con esto se espera las mejores prácticas para la gestión de servicios de TI y mejorar los plazos de respuesta como lo dice la certificación. Además, ante la magnitud del servicio a contratar la cantidad de personal especializado solicitado es mínimamente a fin de garantizar el funcionamiento del datacenter		

Consulta 17 - Capacidad Técnica

Consulta	Fecha de Consulta	14-10-2024
En el PBC se menciona que el oferente deberá contar con un personal con Certificación CDCP (Certified Data Center Professional) vigente. Esta última deberá ser emitida por una organización debidamente habilitada y reconocida a nivel mundial, de forma a constatar conocimientos sobre diseño y operación de Data Center, con criterios establecidos por estándares internacionales relacionados. Solicitamos favor aclarar si dicho personal debe ser miembro del staff permanente de la empresa o si puede ser contratado.		

Respuesta	Fecha de Respuesta	25-10-2024
Remitirse al Pliego. Lo solicitado está claramente establecido y la certificación solicitada es acorde a este tipo de llamado ya que es para administrar y mantener un datacenter por ende se requiere de técnicos especializados en área.		

Consulta 18 - Pliego de Bases y Condiciones/SUMINISTROS REQUERIDOS – ESPECIFICACIONES TÉCNICAS/ Grupo 1y 2 - ITEM 11. Adecuación del Sistema de Seguridad de Red Perimetral

Consulta	Fecha de Consulta	14-10-2024

Se solicita MTBF de 120.000 horas.
Se solicita aceptar equipos con MTBF de un minimo de 80.000horas, considerando seria equivalente cercano a 10 años, periodo en el el avance tecnologico tambien exigira renovaciones de performance y funcionalidades.

Respuesta	Fecha de Respuesta	25-10-2024

Remitirse al Pliego. Esta claramente establecido la adecuación del Sistema de Seguridad de Red Perimetral en ambos datacenter deberán estar configurados en clúster por ende se requiere la extensión del existente y adecuación de lo que se requiera para que trabaje en la integración de ambos datacenter. Además, Los equipos ofertados deberán ser idéntico al equipo existente en la institución en sus componentes de Hardware y Software para la formación del clúster en alta disponibilidad. Por lo que cualquier equipo de distinta capacidad no podrá cumplir el esquema de redundancia que se está proyectando para los Data Center Principal y de Contingencia.

Consulta 19 - Pliego de Bases y Condiciones/SUMINISTROS REQUERIDOS – ESPECIFICACIONES TÉCNICAS/ Grupo 1y 2 - ITEM 11. Adecuación del Sistema de Seguridad de Red Perimetral

Consulta	Fecha de Consulta	14-10-2024

Se solicita soporte de como minimo 750.000 sesiones SSL concurrentes.
Solicitamos a la Convocante aceptar equipos que soporten al menos 500.000 sesiones SSL concurrentes.

Respuesta	Fecha de Respuesta	25-10-2024

. Esta claramente establecido la adecuación del Sistema de Seguridad de Red Perimetral en ambos datacenter deberán estar configurados en clúster por ende se requiere la extensión del existente y adecuación de lo que se requiera para que trabaje en la integración de ambos datacenter. Además, Los equipos ofertados deberán ser idéntico al equipo existente en la institución en sus componentes de Hardware y Software para la formación del clúster en alta disponibilidad. Por lo que cualquier equipo de distinta capacidad no podrá cumplir el esquema de redundancia que se está proyectando para los Data Center Principal y de Contingencia.

Consulta 20 - Pliego de Bases y Condiciones/SUMINISTROS REQUERIDOS – ESPECIFICACIONES TÉCNICAS/ Grupo 1y 2 - ITEM 11. Adecuación del Sistema de Seguridad de Red Perimetral

Consulta	Fecha de Consulta	21-10-2024

Pliego de Bases y Condiciones/SUMINISTROS REQUERIDOS – ESPECIFICACIONES TÉCNICAS/ Grupo 1y 2 - ITEM 11. Adecuación del Sistema de Seguridad de Red Perimetral/ se solicita lo siguiente:
“La solución de VPN debe soportar la integración con los siguientes protocolos de autenticación:
- LDAP
- RADIUS
- ACE Management Servers (SecurID)
- Client Certificates, authenticated by trusted CAs”.
Solicitamos pueda establecerse como opcional el soporte de integración con protocolo de autenticación RSA ACE o SecurID o bien que se acepten en su lugar, otras opciones de autenticación como OAuth2 Server, PICC 4A Server, entre otras. De manera a contar con una mayor variedad de ofertas con productos igualmente eficientes adecuados al contexto de operación.

Respuesta	Fecha de Respuesta	25-10-2024

Respuesta: Favor remitirse al pliego, los protocolos
-LDAP
- RADIUS
- ACE Management Servers (SecurID)
- Client Certificates, authenticated by trusted CAs".
Son especificaciones mínimas y necesarias para nuestra Entidad, considerando las configuraciones ya en uso por los equipamientos actuales. Además, con esto se busca reforzarla y son certificados digitales que permiten a los usuarios y personas demostrar su identidad a un servidor

Consulta 21 - Pliego de Bases y Condiciones/SUMINISTROS REQUERIDOS – ESPECIFICACIONES TÉCNICAS/ Grupo 1y 2 - ITEM 11. Adecuación del Sistema de Seguridad de Red Perimetral/

Consulta	Fecha de Consulta	21-10-2024

Pliego de Bases y Condiciones/SUMINISTROS REQUERIDOS – ESPECIFICACIONES TÉCNICAS/ Grupo 1y 2 - ITEM 11. Adecuación del Sistema de Seguridad de Red Perimetral/ se solicita lo siguiente:
“La solución de VPN debe soportar la integración con los siguientes protocolos de autenticación:
- LDAP
- RADIUS
- ACE Management Servers (SecurID)
- Client Certificates, authenticated by trusted CAs”.
Solicitamos pueda establecerse como opcional el soporte de integración con protocolo de autenticación RSA ACE o SecurID, y sugerimos sea agregado en su lugar como requisito, protocolos como TACACS+, ampliamente difundido.

Respuesta	Fecha de Respuesta	25-10-2024

Favor remitirse al pliego, los protocolos
-LDAP
- RADIUS
- ACE Management Servers (SecurID)
- Client Certificates, authenticated by trusted CAs".
Son especificaciones mínimas y necesarias para nuestra Entidad, considerando las configuraciones ya en uso por los equipamientos actuales. El oferente podrá ofertar equipos con funcionalidades TACACS+ o superiores

Consulta 22 - SUMINISTROS REQUERIDOS – ESPECIFICACIONES TÉCNICAS/ Grupo 1y 2 - ITEM 11. Adecuación del Sistema de Seguridad de Red Perimetral

Consulta	Fecha de Consulta	21-10-2024

En el Pliego de Bases y Condiciones/SUMINISTROS REQUERIDOS – ESPECIFICACIONES TÉCNICAS/ Grupo 1y 2 - ITEM 11. Adecuación del Sistema de Seguridad de Red Perimetral/ se solicita lo siguiente:
“Autenticación vía certificado IKE PKI”
Se solicita a la Convocante pueda especificar qué tipo de autenticación debería soportar la solución solicitada.

Respuesta	Fecha de Respuesta	25-10-2024

Favor remitirse al Pliego. Las especificaciones son las mínimas y necesarias para nuestra Entidad, considerando las configuraciones ya en uso por los equipamientos actuales. El oferten deberá presentar equipos que soporten los protocolos IKE en sus versiones 1y 2 PKI con certificado X.509 o superiores

Consulta 23 - Grupo 1y 2 - ITEM 11. Adecuación del Sistema de Seguridad de Red Perimetral

Consulta	Fecha de Consulta	21-10-2024

En las Especificaciones Técnicas, se menciona lo siguiente:
“Deberá poseer la función resolución de direcciones vía DNS, para que conexiones como destino a dominios maliciosos sean resueltas por el Firewall como direcciones (IPv4 e IPv6), previamente definidos”
Solicitamos a la Convocante pueda aclarar este requerimiento.

Respuesta	Fecha de Respuesta	25-10-2024

Favor remitirse al pliego. Las especificaciones son mínimas y necesarias para nuestra Entidad, considerando las configuraciones ya en uso por los equipamientos actuales. La configuración de DNS para direcciones IPv4 e IPv6. Cuando un usuario solicita un sitio web, el Firewall busca en los servidores DNS configurados la dirección IP del sitio web para saber a qué servidor contactar para completar la transacción.
EL Firewall consulta a los servidores DNS siempre que necesita resolver un nombre de dominio en una dirección IP, como para NTP o servidores web definidos por sus nombres de dominio

Consulta 24 - Grupo 1y 2 - ITEM 11. Adecuación del Sistema de Seguridad de Red Perimetral

Consulta	Fecha de Consulta	21-10-2024

En las especificaciones técnicas - Grupo 1y 2 - ITEM 11. Adecuación del Sistema de Seguridad de Red Perimetral/ se menciona lo siguiente:
“Deberá soportar la creación de políticas QoS por: Dirección de origen, Dirección de Destino, por puertos, por aplicaciones, Ancho de banda garantizados, Ancho de Banda Máximo, por cola de prioridad”
Sugerimos a la Convocante, que de forma a agregar mayor Granularidad en la Gestión del Tráfico y mejorar la calidad de servicio a través de la Prioridad de Tráfico Crítico, considere dentro de los requisitos el soporte de creación de políticas de QoS aplicadas según VLAN, ToS, Traffic Class.

Respuesta	Fecha de Respuesta	25-10-2024

Favor remitirse al pliego, Los detalles técnicos son especificaciones mínimas requeridas y además el oferente podrá ofertar equipos capacidades superiores

Consulta 25 - Grupo 1y 2 - ITEM 11. Adecuación del Sistema de Seguridad de Red Perimetral

Consulta	Fecha de Consulta	21-10-2024

En las especificaciones técnicas se solicita: “Deberá permitir el bloqueo de virus y spyware en, por lo menos, los siguientes protocolos: HTTP, FTP, SMB, SMTP e POP3”

Sugerimos a la Convocante aceptar equipos que realicen bloqueo de virus y spyware sobre protocolo IMAP4, ampliamente utilizado.

Respuesta	Fecha de Respuesta	25-10-2024

Favor remitirse al pliego, Los detalles técnicos son especificaciones mínimas requeridas y además el oferente podrá ofertar equipos capacidades superiores

Consulta 26 - Grupo 1y 2 - ITEM 11. Adecuación del Sistema de Seguridad de Red Perimetral

Consulta	Fecha de Consulta	21-10-2024

En las ESPECIFICACIONES TÉCNICAS/ Grupo 1y 2 - ITEM 11. Adecuación del Sistema de Seguridad de Red Perimetral/ se menciona lo siguiente:

“Deberá contar con desencripción SSL y SSH”

Se solicita a la Convocante incluir como requisito la descencripción de tráfico TLS en lugar de SSH, considerando que el tráfico TLS es mucho más prevalente en la mayoría de las redes, especialmente con el crecimiento de aplicaciones web y la migración hacia HTTPS. Así también, las amenazas modernas a menudo se transmiten a través de conexiones TLS encriptadas, por lo tanto, es una funcionalidad más crítica.

Respuesta	Fecha de Respuesta	25-10-2024

Favor remitirse al pliego, Se encuentran especificado los mínimos y necesarias para nuestra Entidad, considerando las configuraciones ya en uso por los equipamientos actuales, se aceptan especificaciones superiores, sin comprometer las características mínimas expuestas

Consulta 27 - Grupo 1y 2 - ITEM 11. Adecuación del Sistema de Seguridad de Red Perimetral

Consulta	Fecha de Consulta	21-10-2024

Se menciona lo siguiente:
“Soporte multicast (PIM-SM);”
Se solicita a la Convocante aceptar de forma indistinta el soporte de Multicast PIM-SSM.

Respuesta	Fecha de Respuesta	25-10-2024

Favor remitirse al pliego, Se encuentran especificado los mínimos y necesarias para nuestra Entidad, considerando las configuraciones ya en uso por los equipamientos actuales, se aceptan especificaciones superiores, sin comprometer las características mínimas expuestas

Consulta 28 - Grupo 1y 2 - ITEM 11. Adecuación del Sistema de Seguridad de Red Perimetral/

Consulta	Fecha de Consulta	21-10-2024

En las Especificaciones técnicas se solicita: Los equipos ofertados deberán contar con la capacidad de enviar log para sistemas de monitoreo externos denominados comúnmente como SIEM (Security Information and Event Management), simultáneamente.

Se solicita a la Convocante aclarar mejor este requisito.

Respuesta	Fecha de Respuesta	25-10-2024

Favor remitirse al pliego, las especificaciones son mínimas y necesarias para nuestra Entidad, considerando las configuraciones ya están en uso por los equipamientos actuales. El requisito refiere a La capacidad de enviar log de eventos a otros sistemas de monitoreo externos

Consulta 29 - Grupo 1y 2 - ITEM 11. Adecuación del Sistema de Seguridad de Red Perimetral

Consulta	Fecha de Consulta	21-10-2024

Se sugiere a la Convocante considerar la inclusión como requisito la funcionalidad Botnet Prevention dentro de la plataforma a ser adquirida, lo que permitirá proteger de manera eficaz la red y sus dispositivos contra compromisos que podrían ser utilizados para actividades maliciosas.

Respuesta	Fecha de Respuesta	25-10-2024

Favor remitirse al pliego, las especificaciones son mínimas y necesarias para nuestra Entidad, considerando las configuraciones ya están en uso por los equipamientos actuales. El requisito refiere a La capacidad de enviar log de eventos a otros sistemas de monitoreo externos

Consulta 30 - Grupo 1y 2 - ITEM 11. Adecuación del Sistema de Seguridad de Red Perimetral/

Consulta	Fecha de Consulta	21-10-2024

Pliego de Bases y Condiciones/SUMINISTROS REQUERIDOS – ESPECIFICACIONES TÉCNICAS/ Grupo 1y 2 - ITEM 11. Adecuación del Sistema de Seguridad de Red Perimetral/ se menciona lo siguiente:

“Deberá contar funcionalidad NAT64,”

Sugerimos a la Convocante considerar el soporte de NAT 46, NAT 444 y Full Cone NAT de manera a otorgar mayor flexibilidad y capacidad de adaptación a diferentes necesidades de red (interoperabilidad, eficiencia en la gestión de direcciones y mejoras en el rendimiento).

Respuesta	Fecha de Respuesta	25-10-2024

Favor remitirse al pliego, se encuentran especificados lo mínimo y necesario para nuestra Entidad, considerando las configuraciones que ya están en uso por los equipamientos actuales. El oferente podrá ofertar equipos con NAT 46, NAT444 o superior

Consulta 31 - Grupo 1y 2 - ITEM 11. Adecuación del Sistema de Seguridad de Red Perimetral

Consulta	Fecha de Consulta	21-10-2024
SUMINISTROS REQUERIDOS – ESPECIFICACIONES TÉCNICAS- Grupo 1y 2 - ITEM 11. Adecuación del Sistema de Seguridad de Red Perimetral/ se menciona lo siguiente: “Debe desencriptar tráfico que use certificados ECC (como ECDSA)” Se sugiere a la Convocante considerar la desencripción de tráfico con certificados ECC, RSA, DSA, de manera a adquirir un equipo que responda con mayor flexibilidad a diversos entornos de operación.		

Respuesta	Fecha de Respuesta	25-10-2024
Favor remitirse al pliego, se encuentran especificados lo mínimo y necesario para nuestra Entidad, considerando las configuraciones que ya están en uso por los equipamientos actuales. El oferente podrá ofertar equipos con NAT 46, NAT444 o superior		

Consulta 32 - Grupo 1y 2 - ITEM 11. Adecuación del Sistema de Seguridad de Red Perimetral

Consulta	Fecha de Consulta	21-10-2024
Especificaciones Técnicas/Grupo 1y 2 - ITEM 11. Adecuación del Sistema de Seguridad de Red Perimetral/ se menciona lo siguiente: “Los equipos ofertados deberán soportar sub-interfaces ethernet lógicas.” Se solicita a la Convocante aclarar si deberá ser considerado el soporte de interfaces LACP o similar, interfaces redundantes, entre otras.		

Respuesta	Fecha de Respuesta	25-10-2024
Favor remitirse al pliego, se encuentran especificados lo mínimo y necesario para nuestra Entidad, considerando las configuraciones que ya están en uso por los equipamientos actuales. El oferente podrá ofertar equipos con NAT 46, NAT444 o superior		

Consulta 33 - Grupo 1y 2 - ITEM 11. Adecuación del Sistema de Seguridad de Red Perimetral

Consulta	Fecha de Consulta	21-10-2024
En las especificaciones técnicas se solicita que el cliente vpn ssl sea compatible con sistemas operativos Windows y Linux actuales. Se consulta a la Convocante si será necesaria la compatibilidad con sistemas operativos usuales en dispositivos móviles como IOS, Android.		

Respuesta	Fecha de Respuesta	25-10-2024
Favor remitirse al pliego, se encuentran especificados lo mínimo y necesario para nuestra Entidad, considerando las configuraciones que ya están en uso por los equipamientos actuales. El oferente podrá ofertar equipos con NAT 46, NAT444 o superior		

Consulta 34 - Pliego de Bases y Condiciones/REQUISITOS DE PARTICIPACIÓN Y CRITERIOS DE EVALUACIÓN/Capacidad Técnica,

Consulta	Fecha de Consulta	28-10-2024

Teniendo en cuenta lo solicitado
a) Autorización del fabricante o similar. Para Grupo 1 ítem 1 al 11 Soporte Técnico Extendido para Datacenter Principal DCMT y para el Grupo 2 ítem 1 al 12 Soporte Técnico Extendido para Datacenter de Contingencia el oferente deberá presentar Carta de Autorización del Fabricante: La empresa oferente deberá contar con Autorización expedida por el fabricante para representantes, distribuidores y subdistribuidores de los productos ofrecidos; o el oferente deberá demostrar que cuenta con personal certificado en: i. AOP -UPTIME INSTITUTE Accredited Operations Professional. ii. ATS UPTIME INSTITUTE - Accredited Tier Specialist
b) La respuesta a la consulta 4: “La certificación solicitada es acorde a este tipo de llamado ya que es para administrar, mantener y tomar las decisiones adecuadas en cuanto a la seguridad de un datacenter por ende se requiere de técnicos especializados en el área.

Consultamos si es aceptable un Profesional AOS (Accredited Operations Specialist) del Uptime.

Respuesta	Fecha de Respuesta	01-11-2024

Favor remitirse al Pliego. Consulta similar fue aclarada en la respuesta de la consulta 4. La certificación solicitada es acorde a este tipo de llamado.

Consulta 35 - Requisitos de Experiencia y Capacidad Técnica orientados al firewall en el soporte de Datacenter.

Consulta	Fecha de Consulta	29-10-2024

Solicitamos respetuosamente a la Convocante revisar y reformular los criterios de experiencia y capacidad técnica establecidos en el Pliego de Bases y Condiciones, específicamente en el requisito de experiencia orientada a la provisión de Firewalls. Si bien comprendemos la relevancia del firewall dentro del proyecto de extensión de soporte para el Datacenter, dicho criterio representa solo un ítem del alcance total. Este enfoque puede limitar la participación de proveedores capacitados para otros componentes técnicos solicitados, generando un sesgo no esencial hacia un área específica. Asimismo, sugerimos que se contemple la experiencia en la provisión y configuración de equipos de las marcas ya existentes en el Datacenter, ya que esto aseguraría la idoneidad y continuidad del servicio requerido.
El artículo 45 de la Ley N° 7021/2022 indica que los pliegos de bases y condiciones deben evitar imponer requisitos que limiten la competencia sin justificación técnica. Además, conforme a la Ley N° 7021/2022, debe prevalecer el principio de igualdad de condiciones para todos los oferentes, lo que asegura una evaluación justa y proporcional. Este ajuste permitiría que la selección se realice en base a criterios amplios de idoneidad técnica para la totalidad del proyecto, en línea con la normativa.

Respuesta	Fecha de Respuesta	01-11-2024

Favor remitirse al Pliego. Es sumamente importante contar con los requisitos mencionados en el PBC por la criticidad de los equipos dentro del Datacenter. La experiencia y la certificación solicitada es acorde a este tipo de llamado.

Consulta 36 - SUMINISTROS REQUERIDOS – ESPECIFICACIONES TÉCNICAS-Grupo 1y 2 - ITEM 11. Flexibilidad en la desencriptación de tráfico de red para múltiples certificados (ECC, RSA, DSA).

Consulta	**Fecha de Consulta**	29-10-2024

Sugerimos a la Convocante ampliar los requisitos de desencriptación de tráfico de red perimetral para que incluyan soporte a múltiples tipos de certificados, tales como ECC, RSA y DSA, además del ECDSA especificado en el pliego. La inclusión de estos certificados permitirá al equipo adquirido adaptarse de manera más flexible a diferentes entornos operativos y de seguridad, favoreciendo la interoperabilidad con una mayor variedad de configuraciones en infraestructura de red.
De acuerdo con el principio de valor por dinero establecido en la Resolución DNCP N° 922/2020, la convocatoria debe optimizar el uso de los recursos públicos mediante adquisiciones eficientes y flexibles. Incluir soporte para una gama de certificados permite una mejor adaptación a las tecnologías actuales y a futuros requerimientos de interoperabilidad, alineándose con el mandato de eficiencia en el uso de los recursos públicos.

Respuesta	**Fecha de Respuesta**	01-11-2024

Favor remitirse al Pliego: Para salvaguardar la inversión ya realizada por la institución, los equipos adquiridos deben formar un clúster altamente disponible con el equipo existente, por lo que se requiere que sean del mismo modelo con el mismo nivel de licencias y agregar diferentes algoritmos implicaría configuraciones innecesarias y sin la seguridad del correcto funcionamiento, Además de ello, una inadecuada compra de una marca o modelo que no sea compatible con la plataforma o equipos existentes ocasionaría problemas innecesarios para la criticidad del datacenter. Con todo lo mencionado se busca eficiencia en el uso de los recursos públicos ya existentes como menciona la disposición legal.

Consulta 37 - Especificaciones Técnicas/Grupo 1y 2 - ITEM 11. Adecuación del Sistema de Seguridad de Red Perimetral

Consulta	**Fecha de Consulta**	29-10-2024

El PBC en las Especificaciones Técnicas/Grupo 1y 2 - ITEM 11. Adecuación del Sistema de Seguridad de Red Perimetralmenciona lo siguiente: “Los equipos ofertados deberán soportar sub-interfaces ethernet lógicas.”
Solicitamos a la Convocante aclarar si, además del soporte para sub-interfaces Ethernet lógicas, los equipos deben incluir soporte para interfaces redundantes, tales como LACP o tecnologías similares. La especificación clara de estos requisitos es crucial para garantizar la configuración adecuada y la redundancia operativa del sistema de seguridad de red perimetral.
Conforme a la Ley N° 7021/2022 y sus reglamentaciones, los requisitos técnicos deben ser precisos y específicos para evitar interpretaciones ambiguas que puedan afectar la igualdad de participación. La claridad en estos aspectos permitirá a los oferentes cumplir con precisión los requisitos técnicos establecidos y contribuirá a una evaluación justa y transparente

Respuesta	**Fecha de Respuesta**	01-11-2024

Favor remitirse al Pliego: Para salvaguardar la inversión ya realizada por la institución, los equipos adquiridos deben formar un clúster altamente disponible con el equipo existente, por lo que se requiere que sean del mismo modelo con el mismo nivel de licencias y agregar diferentes algoritmos implicaría configuraciones innecesarias y sin la seguridad del correcto funcionamiento, Además de ello, una inadecuada compra de una marca o modelo que no sea compatible con la plataforma o equipos existentes ocasionaría problemas innecesarios para la criticidad del datacenter. Con todo lo mencionado se busca eficiencia en el uso de los recursos públicos ya existentes como menciona la disposición legal.

Consulta 38 - En las especificaciones técnicas se solicita que el cliente vpn ssl sea compatible con sistemas operativos Windows y Linux actuales.

Consulta	Fecha de Consulta	29-10-2024

Dado que el Pliego de Bases y Condiciones establece que el cliente VPN SSL debe ser compatible con sistemas operativos Windows y Linux, solicitamos a la Convocante considerar la inclusión de compatibilidad con sistemas operativos móviles, como iOS y Android. Esta compatibilidad es esencial en entornos donde se requiere acceso seguro desde dispositivos móviles, asegurando mayor flexibilidad y operatividad.
La Ley N° 7021/2022 y el Decreto N° 2264 promueven la elaboración de pliegos que no restrinjan innecesariamente la participación de los oferentes, adaptándose a las necesidades reales de la institución y evitando limitaciones técnicas no justificadas. La inclusión de sistemas operativos móviles amplía la aplicabilidad de la VPN, fomentando un mejor aprovechamiento de los recursos.

Respuesta	Fecha de Respuesta	01-11-2024

Favor remitirse al Pliego: Ya que solo se contempla VPNs de acceso SSL desde sistemas operativos Windows y Linux. Para salvaguardar la inversión ya realizada por la institución, los equipos adquiridos deben formar un clúster altamente disponible con el equipo existente, por lo que se requiere que sean del mismo modelo con el mismo nivel de licencias y agregar diferentes algoritmos implicaría configuraciones innecesarias y sin la seguridad del correcto funcionamiento, Además de ello, la una inadecuada compra de una marca o modelo que no sea compatible con la plataforma o equipos existentes ocasionaría problemas innecesarios para la criticidad del datacenter. Con todo lo mencionado se busca eficiencia en el uso de los recursos públicos ya existentes como menciona la disposición legal.

Consulta 39 - De los Requisitos de Participación y Criterios de Evaluación - Capacidad Técnica

Consulta	**Fecha de Consulta**	29-10-2024

En el Pliego de Bases y Condiciones, dentro de los Requisitos de Participación y Criterios de Evaluación - Capacidad Técnica, se solicita que el oferente presente una Carta de Autorización del Fabricante para el Soporte Técnico Extendido de los Datacenters, tanto Principal (Grupo 1, Ítems 1 al 11) como de Contingencia (Grupo 2, Ítems 1 al 12). Adicionalmente, se establece como alternativa a dicha autorización que el oferente cuente con personal certificado en:
• AOP (Accredited Operations Professional) por UPTIME INSTITUTE
• ATS (Accredited Tier Specialist) por UPTIME INSTITUTE.
Solicitamos respetuosamente a la Convocante revisar este requisito, ya que no se comprende con claridad la relación entre la Autorización del Fabricante o Distribuidor y las certificaciones técnicas solicitadas (AOP y ATS). La Autorización de Fabricante, en particular, puede ser innecesaria o limitativa, ya que muchos oferentes con competencia técnica en los servicios solicitados podrían no contar con dicha autorización, afectando injustificadamente su participación.
Adicionalmente, observamos que en este apartado no se han establecido criterios de calificación que consideren la experiencia específica del oferente en las marcas de los equipos a mantener, un aspecto que garantizaría de manera más efectiva la idoneidad para el servicio requerido.
Argumentación Técnica: La idoneidad técnica para el mantenimiento de un datacenter puede ser validada mediante certificaciones técnicas en operación y mantenimiento de infraestructura crítica (como las certificaciones AOP y ATS). No obstante, la exigencia de una Carta de Autorización del Fabricante o Distribuidor podría excluir a oferentes igualmente calificados que poseen experiencia y personal certificado en las competencias específicas requeridas, pero que no tienen acceso directo a la representación formal del fabricante. Este tipo de restricción puede reducir el número de competidores calificados, limitando innecesariamente la competencia y, por ende, afectando el principio de obtener el mejor valor por dinero.
Argumentación Legal: El artículo 45 de la Ley N° 7021/2022 de Suministro y Contrataciones Públicas, establece que los pliegos de bases y condiciones deben evitar requisitos que, sin justificación técnica suficiente, limiten la participación de oferentes. Asimismo, la Ley N° 7021/2022 promueve la igualdad de participación entre oferentes, asegurando que todos los competidores idóneos puedan acceder al proceso en condiciones justas. Al modificar este requisito, la Convocante alinearía el pliego con los principios legales de igualdad y competencia efectiva, permitiendo la participación de oferentes con experiencia certificada y capacidades comprobadas, aunque no posean representación directa del fabricante.

Respuesta	**Fecha de Respuesta**	01-11-2024

Favor remitirse al Pliego. Consulta similar fue aclarada en la respuesta de la consulta 4. La certificación solicitada es acorde a este tipo de llamado. Además, lo solicitado garantiza que el producto cumple con estándares de calidad y seguridad establecidos y de facilitar e identificar en caso de defectos o problemas, lo que es esencial para el manejo de garantías y reclamos.

Consulta 40 - De los Requisitos de Participación y Criterios de Evaluación - Capacidad Técnica,

Consulta	Fecha de Consulta	29-10-2024

En el Pliego de Bases y Condiciones, dentro de los Requisitos de Participación y Criterios de Evaluación - Capacidad Técnica, se solicita que el oferente cuente con al menos dos personas certificadas en ITILv4 dentro de su staff permanente. Solicitamos a la Convocante considerar la posibilidad de aceptar ofertas que cuenten con al menos un (1) personal certificado en ITILv4 en el staff permanente, o bien aceptar la inclusión de dicho personal certificado posterior a la adjudicación. Esta flexibilidad permitiría a los oferentes ajustar sus recursos especializados a los requisitos específicos del contrato una vez adjudicado, sin comprometer la calidad del servicio requerido.
Argumentación Técnica: La metodología ITILv4 representa un marco importante para la gestión de servicios de TI, y contar con personal certificado en ITILv4 es beneficioso para asegurar una administración de servicios alineada con las mejores prácticas. Sin embargo, la exigencia de contar con dos personas certificadas dentro del staff permanente puede ser excesivamente restrictiva, especialmente en contextos donde un solo especialista con certificación ITILv4 puede supervisar eficazmente el cumplimiento del marco metodológico y coordinar las prácticas de gestión de servicios. Esta flexibilización permitiría una adecuada adaptación de los recursos humanos de los oferentes a las necesidades del proyecto, sin comprometer el enfoque en la calidad de los servicios prestados.
Argumentación Legal: Conforme al artículo 45 de la Ley N° 7021/2022 de Suministro y Contrataciones Públicas, los pliegos de bases y condiciones deben evitar establecer requisitos restrictivos que no sean técnicamente indispensables, para garantizar una competencia justa y no limitar la participación innecesariamente. Además, el principio de igualdad en la contratación pública insta a que los requisitos de personal estén en consonancia con la naturaleza y escala del servicio requerido. Al permitir esta flexibilidad en el requisito de personal certificado en ITILv4, la Convocante estaría facilitando una mayor participación de oferentes calificados y respetando los principios de transparencia y equidad en el proceso.

Respuesta	Fecha de Respuesta	01-11-2024

Favor remitirse al Pliego. Consulta similar fue aclarada en la respuesta de la consulta 5. Se solicita esa cantidad por la criticidad del servicio de gestión, ya que es el Datacenter del MEC, y con esto se espera las mejores prácticas para la gestión de servicios de TI y mejorar los plazos de respuesta como lo dice la certificación. Como ya menciono es un Sitio Critico "DATACENTER" con lo solicitado se busca garantizar y optimizar los servicios de TI.

Consulta 41 - Pliego de Bases y Condiciones/SUMINISTROS REQUERIDOS – ESPECIFICACIONES TÉCNICAS/ITEM 11. Adecuación del Sistema de Seguridad de Red Perimetral

Consulta	Fecha de Consulta	29-10-2024

En el Pliego de Bases y Condiciones, en la sección de Suministros Requeridos – Especificaciones Técnicas – Ítem 11 (Adecuación del Sistema de Seguridad de Red Perimetral), se establece la necesidad de agregar un equipo adicional para alcanzar la redundancia en la seguridad perimetral del Datacenter Principal. Observamos, sin embargo, que el Pliego requiere una cantidad total de tres (3) unidades.

Con el objetivo de optimizar tanto la inversión como la eficiencia operativa, sugerimos que la Convocante considere especificar equipos de mayor rendimiento para la seguridad perimetral, lo cual permitiría alcanzar la redundancia y los niveles de seguridad requeridos con un menor número de unidades. Esto aportaría beneficios en términos de eficiencia económica y simplificación de la infraestructura, reduciendo así la complejidad operativa y los costos de mantenimiento.

Adicionalmente, se solicita a la Convocante revisar el requerimiento de que “los equipos ofertados deberán ser idénticos al equipo existente en la institución en sus componentes de hardware y software”, ya que este criterio representa un direccionamiento hacia una marca o modelo específico, limitando la igualdad de participación entre los oferentes y restringiendo la competencia sin una justificación técnica suficiente. Teniendo en cuenta principalmente que este no es llamado de excepción por dependencia tecnológica, por lo que no existe el argumento técnico suficiente para sustentar este requisito.

Argumentación Técnica: La redundancia en la seguridad perimetral de un Datacenter puede lograrse efectivamente mediante el uso de equipos de alta capacidad de procesamiento y rendimiento, especialmente si están diseñados para manejar picos de tráfico y proteger contra amenazas avanzadas. El requerimiento de tres unidades idénticas puede ser técnicamente innecesario si se especifican equipos de mayor performance, los cuales permitirían cubrir las necesidades de seguridad y redundancia con una infraestructura menos compleja y más fácil de gestionar. Esto no solo reduce costos de adquisición y mantenimiento, sino que también simplifica la gestión operativa del Datacenter, manteniendo al mismo tiempo altos estándares de seguridad.

Argumentación Legal: De acuerdo con el artículo 45 de la Ley N° 7021/2022 de Suministro y Contrataciones Públicas, los pliegos de bases y condiciones deben evitar requisitos que sin justificación técnica suficiente limiten la participación o direccionen el proceso hacia una marca o modelo específico, salvo que existan necesidades técnicas probadas. La exigencia de equipos “idénticos” puede interpretarse como una restricción de competencia que infringe el principio de igualdad de participación. Proponemos que se flexibilicen estos términos para permitir la inclusión de alternativas técnicamente equivalentes que cumplan con los requisitos de rendimiento y redundancia, asegurando así una mayor participación y competitividad en el proceso de selección.

Respuesta	Fecha de Respuesta	01-11-2024

VER ADENDA.

Consulta 42 - Requisito de Interfaces 1GE RJ45 en Equipos de Seguridad Perimetral.

Consulta	Fecha de Consulta	29-10-2024

En el Pliego de Bases y Condiciones, en la sección de Suministros Requeridos – Especificaciones Técnicas – Grupo 1 y 2 - Ítem 11 (Adecuación del Sistema de Seguridad de Red Perimetral), se establece que los equipos deben contar con al menos catorce (14) interfaces 1GE RJ45. Solicitamos a la Convocante reconsiderar este requisito, y aceptar equipos con al menos seis (6) puertos o interfaces de 1GE RJ45, dado que la misión principal de estos equipos es la protección de borde del Datacenter.
La configuración estándar en este tipo de sistemas de seguridad perimetral suele implicar la conexión con el Core del Datacenter, utilizando enlaces de mayor capacidad (como 10GE o superiores) para asegurar el rendimiento y capacidad de tráfico necesarios. La cantidad de catorce interfaces 1GE RJ45 puede ser excesiva y no esencial para la funcionalidad requerida, lo que podría restringir la participación de oferentes que dispongan de equipos equivalentes y compatibles con la arquitectura de red del Datacenter, pero con menor cantidad de interfaces de 1GE RJ45.
Además, solicitamos a la Convocante revisar la exigencia de que “los equipos ofertados deberán ser idénticos al equipo existente en sus componentes de hardware y software”, ya que este requisito podría limitar injustificadamente la competencia al direccionar la adquisición hacia una marca o modelo específico, afectando el principio de igualdad de condiciones entre oferentes.
Argumentación Técnica: Para la protección perimetral de un Datacenter, el uso de múltiples interfaces de alta capacidad (1GE o superiores) es comúnmente requerido solo en sistemas donde el tráfico distribuido o segmentado es vital. Sin embargo, en configuraciones estándares de borde, los enlaces de alta capacidad, como 10GE, suelen ser preferidos para la conectividad principal al Core del Datacenter, mientras que el uso de múltiples interfaces de 1GE puede no aportar valor adicional al rendimiento o seguridad de la red. Al permitir un menor número de interfaces 1GE RJ45, la Convocante facilitaría la participación de equipos de especificaciones equivalentes y de alto rendimiento que cumplan con los requerimientos sin comprometer la operatividad o seguridad del sistema.
Argumentación Legal: Según el artículo 45 de la Ley N° 7021/2022 de Suministro y Contrataciones Públicas, los pliegos de bases y condiciones deben evitar especificaciones excesivamente restrictivas, especialmente cuando no son técnicamente indispensables. La exigencia de equipos “idénticos” en hardware y software puede interpretarse como un posible direccionamiento que restringe la competencia sin justificación técnica suficiente. Flexibilizar estos términos permitiría una mayor variedad de equipos que cumplan con las exigencias de seguridad y rendimiento, fomentando la participación en condiciones de igualdad, como lo establece la normativa.

Respuesta	Fecha de Respuesta	01-11-2024

Favor remitirse al Pliego: Para salvaguardar la inversión ya realizada por la institución, los equipos adquiridos deben formar un clúster altamente disponible con el equipo existente, por lo que se requiere que sean del mismo modelo con el mismo nivel de licencias y agregar diferentes algoritmos implicaría configuraciones innecesarias y sin la seguridad del correcto funcionamiento, Además de ello, la inadecuada compra de una marca o modelo que no sea compatible con la plataforma o equipos existentes ocasionaría problemas innecesarios para la criticidad del datacenter y teniendo en cuenta que los requerimientos están basados en la infraestructura y topología actual y planificada a futuro de la convocante. En este sentido, contar con solo seis interfaces RJ45 1 Gbps no permitiría la implementación de la arquitectura planificada y aprobada, además de comprometer la escalabilidad y redundancia de la misma. Con todo lo mencionado se busca eficiencia en el uso de los recursos públicos ya existentes como menciona la disposición legal.

Consulta 43 - Soporte técnico local y especificidad en la capacidad de instalación y configuración de equipos de seguridad de red.

Consulta	Fecha de Consulta	29-10-2024

En el Pliego de Bases y Condiciones, específicamente en el apartado de Suministros Requeridos – Especificaciones Técnicas – Grupo 1 y 2 - Ítem 11 (Adecuación del Sistema de Seguridad de Red Perimetral), se establece que el oferente debe demostrar la capacidad de brindar soporte técnico local en Paraguay durante el periodo de garantía. Este requisito incluye la presentación de certificados de capacitación técnica de al menos dos técnicos en áreas específicas (seguridad, servidores, switches, routers, y software de virtualización). Dichos técnicos deben ser parte del plantel permanente del oferente o contar con la posibilidad de ser subcontratados.
No obstante, observamos que el requisito no define con claridad los aspectos técnicos específicos relacionados con la capacidad de instalación y configuración del equipo ofertado, lo cual es fundamental para asegurar la operatividad efectiva del sistema de seguridad de red perimetral en el entorno institucional. Solicitamos respetuosamente a la Convocante que especifique con mayor detalle los criterios de experiencia y competencia necesarios para la instalación y configuración del equipo, asegurando así que los técnicos certificados cuenten con la experiencia práctica y conocimientos especializados que garanticen el cumplimiento efectivo de los objetivos del proyecto.
Argumentación Técnica: La configuración e instalación adecuada de un sistema de seguridad de red perimetral exige habilidades avanzadas y específicas en administración de redes y seguridad informática, así como en la integración de dispositivos en infraestructuras críticas. Sin una claridad técnica en los requisitos de experiencia y competencia para la instalación y configuración, existe un riesgo de que el servicio contratado no cumpla con los estándares de operatividad y seguridad deseados. Detallar estos requisitos evitaría interpretaciones ambiguas, permitiendo que los oferentes demuestren una capacidad técnica probada, especialmente en la puesta en marcha y soporte de equipos complejos como firewalls, sistemas de enrutamiento y virtualización.
Argumentación Legal: Conforme al artículo 45 de la Ley N° 7021/2022 de Suministro y Contrataciones Públicas, los pliegos deben evitar requisitos vagos que puedan limitar o direccionar la participación sin justificación técnica, garantizando igualdad en el proceso de contratación. Además, el artículo 121 de la Ley N° 7021/2022 establece que las contrataciones deben permitir la participación en condiciones de igualdad para todos los oferentes. Por lo tanto, detallar los requisitos específicos sobre la capacidad técnica en instalación y configuración asegura no solo la competencia justa, sino que respalda la calidad del servicio y los resultados esperados, alineándose con los principios de igualdad y transparencia establecidos en la ley.

Respuesta	Fecha de Respuesta	01-11-2024

Favor remitirse al Pliego: Se solicita la certificación por la criticidad del servicio de gestión, ya que es el Datacenter del MEC y además está establecido en el PBC - Especificaciones Técnicas - Grupo 1 y 2 - Ítem 11 (Adecuación del Sistema de Seguridad de Red Perimetral).

Consulta 44 - Requisito de MTBF (Mean Time Between Failures) de 120,000 horas en Equipos de Seguridad Perimetral.

Consulta	**Fecha de Consulta**	29-10-2024

En el Pliego de Bases y Condiciones, específicamente en la sección de Suministros Requeridos – Especificaciones Técnicas – Grupo 1 y 2 - Ítem 11 (Adecuación del Sistema de Seguridad de Red Perimetral), se solicita un MTBF (Mean Time Between Failures) de 120,000 horas para los equipos. Solicitamos respetuosamente que la Convocante considere aceptar equipos con un MTBF mínimo de 80,000 horas, lo cual representaría aproximadamente diez años de vida útil operativa.
Este período coincide con los ciclos habituales de avance tecnológico en seguridad de redes, que demandan renovaciones en el rendimiento y en las funcionalidades para adaptarse a nuevas exigencias de seguridad. Una especificación de MTBF más flexible permitiría la participación de equipos de alta calidad y rendimiento, alineados con los ciclos de actualización tecnológica sin comprometer la funcionalidad o fiabilidad del sistema de seguridad.
Adicionalmente, solicitamos a la Convocante revisar la exigencia de que “los equipos ofertados deberán ser idénticos al equipo existente en la institución en sus componentes de hardware y software”. Este requerimiento podría interpretarse como una limitación a la competencia al orientar la compra hacia una marca o modelo específico, restringiendo la igualdad de participación entre los oferentes sin una justificación técnica suficiente.
Argumentación Técnica: Un MTBF de 80,000 horas (cerca de diez años) representa un estándar robusto y adecuado en términos de vida útil para los sistemas de seguridad de red, especialmente considerando el ritmo de avance tecnológico en este sector. Equipos con MTBF de este nivel ofrecen un rendimiento confiable y pueden ser actualizados con nuevas funcionalidades y mejoras de rendimiento, permitiendo que la infraestructura se mantenga alineada con los desarrollos y necesidades actuales de seguridad. La especificación de un MTBF de 120,000 horas podría resultar excesiva y excluir alternativas tecnológicas igualmente válidas, que podrían adaptarse mejor a un entorno de rápida evolución tecnológica.
Argumentación Legal: De acuerdo con el artículo 45 de la Ley N° 7021/2022, de Suministro y Contrataciones Públicas, los pliegos de bases y condiciones deben evitar requisitos técnicos excesivamente restrictivos, en especial aquellos que puedan limitar la competencia sin una justificación técnica clara. Además, exigir que los equipos “sean idénticos en hardware y software” podría interpretarse como un direccionamiento hacia una marca o modelo específicos, lo que contraviene el principio de igualdad de participación establecido en la ley. Permitir un MTBF de 80,000 horas y flexibilizar el requerimiento de "identicidad" en hardware y software facilitaría la participación de más proveedores, fomentando la competitividad en igualdad de condiciones.

Respuesta	**Fecha de Respuesta**	01-11-2024

Favor remitirse al Pliego: Para salvaguardar la inversión ya realizada por la institución, los equipos adquiridos deben formar un clúster altamente disponible con el equipo existente, por lo que se requiere que sean del mismo modelo con el mismo nivel de licencias y agregar diferentes algoritmos implicaría configuraciones innecesarias y sin la seguridad del correcto funcionamiento, Además de ello, la una inadecuada compra de una marca o modelo que no sea compatible con la plataforma o equipos existentes ocasionaría problemas innecesarios para la criticidad del datacenter. Con todo lo mencionado se busca eficiencia en el uso de los recursos públicos ya existentes como menciona la disposición legal.

Consulta 45 - Requisito de Protocolos de Autenticación en la Solución de VPN para la Seguridad de Red Perimetral.

Consulta	Fecha de Consulta	29-10-2024

En el Pliego de Bases y Condiciones, en la sección de Suministros Requeridos – Especificaciones Técnicas – Grupo 1 y 2 - Ítem 11 (Adecuación del Sistema de Seguridad de Red Perimetral), se especifica que la solución de VPN debe soportar integración con protocolos de autenticación tales como LDAP, RADIUS, ACE Management Servers (SecurID), y certificados de cliente autenticados por autoridades de certificación confiables (CAs). Solicitamos respetuosamente a la Convocante que considere establecer como opcional la integración con el protocolo RSA ACE o SecurID, y permita en su lugar opciones alternativas como OAuth2 Server, PICC 4A Server, entre otros.
Esto facilitaría una mayor participación de proveedores que ofrezcan soluciones de VPN igualmente eficientes y adaptadas al contexto operativo, sin estar limitados a un solo protocolo específico. De este modo, se ampliaría la gama de soluciones disponibles, garantizando la interoperabilidad y el cumplimiento de los requisitos de seguridad.
Argumentación Técnica: La interoperabilidad en sistemas de seguridad de red es un elemento clave para lograr una infraestructura de autenticación robusta y escalable. Protocolos como OAuth2, ampliamente utilizados en entornos modernos, pueden ofrecer el mismo nivel de seguridad y eficiencia que RSA ACE o SecurID, asegurando así la autenticación segura de los usuarios sin depender de un solo tipo de tecnología. La flexibilidad en la selección de protocolos de autenticación permite adaptar la solución a diferentes arquitecturas de red y maximizar la compatibilidad con el equipamiento actual y futuro, asegurando que la infraestructura de VPN pueda integrar una variedad de opciones de autenticación sin pérdida de calidad o seguridad.
Argumentación Legal: El artículo 45 de la Ley N° 7021/2022, de Suministro y Contrataciones Públicas, estipula que los pliegos de bases y condiciones deben evitar requisitos restrictivos que limiten la competencia sin justificación técnica. La exigencia de soporte exclusivo para protocolos como RSA ACE o SecurID puede ser interpretada como un direccionamiento hacia una tecnología o marca específica, lo cual restringe la participación de oferentes con soluciones tecnológicamente equivalentes. Flexibilizar este requerimiento permitiría la participación de una mayor diversidad de proveedores y opciones tecnológicas, promoviendo la igualdad de condiciones y fomentando una competencia efectiva, tal como establece la normativa.

Respuesta	Fecha de Respuesta	01-11-2024

Favor remitirse al Pliego: Considerando la importancia de la integración con protocolos de autenticación robustos en materia de seguridad, se requiere que la solución sea integrable con la mayor cantidad de tecnologías como se solicita en este requerimiento de integración con RSA ACE o SecurID y para salvaguardar la inversión ya realizada por la institución, los equipos adquiridos deben formar un clúster altamente disponible con el equipo existente, por lo que se requiere que sean del mismo modelo con el mismo nivel de licencias y agregar diferentes algoritmos implicaría configuraciones innecesarias y sin la seguridad del correcto funcionamiento, Además de ello, la una inadecuada compra de una marca o modelo que no sea compatible con la plataforma o equipos existentes ocasionaría problemas innecesarios para la criticidad del datacenter. Con todo lo mencionado se busca eficiencia en el uso de los recursos públicos ya existentes como menciona la disposición legal.

Consulta 46 - Requisito de Protocolos de Autenticación en la Solución de VPN para Seguridad de Red Perimetral.

Consulta	Fecha de Consulta	29-10-2024

En el Pliego de Bases y Condiciones, específicamente en Suministros Requeridos – Especificaciones Técnicas – Grupo 1 y 2 - Ítem 11 (Adecuación del Sistema de Seguridad de Red Perimetral), se establece que la solución de VPN debe integrar los siguientes protocolos de autenticación: LDAP, RADIUS, ACE Management Servers (SecurID), y certificados de cliente autenticados por autoridades de certificación confiables (CAs). Solicitamos a la Convocante considerar hacer opcional el soporte de integración con el protocolo RSA ACE o SecurID y, en su lugar, incluir como requisito el soporte para protocolos de autenticación ampliamente utilizados, tales como TACACS+.
La inclusión de TACACS+, un protocolo de autenticación ampliamente difundido y compatible con múltiples sistemas de seguridad, permitiría a los oferentes proporcionar una solución de VPN igualmente robusta, sin limitar la competencia a opciones específicas de autenticación. Esto ampliaría la posibilidad de participación y facilitaría la integración de soluciones eficientes y adecuadas a las necesidades de seguridad de la red institucional.
Argumentación Técnica: La interoperabilidad en los protocolos de autenticación de VPN es esencial para garantizar que los sistemas de seguridad de red se integren eficazmente con la infraestructura tecnológica existente. TACACS+ es un protocolo estándar ampliamente compatible, especialmente en entornos donde es necesaria la autenticación centralizada y la gestión de acceso de usuarios en la red. Su inclusión como requisito técnico garantiza una flexibilidad y adaptabilidad óptimas, ya que este protocolo es igualmente eficaz en la protección de la red perimetral y asegura el cumplimiento de los niveles de seguridad exigidos. El soporte para RSA ACE o SecurID puede limitar la competitividad, ya que son soluciones de autenticación propietarias, mientras que TACACS+ permite una mayor variedad de opciones en el mercado sin comprometer los estándares de seguridad.
Argumentación Legal: Conforme al artículo 45 de la Ley N° 7021/2022, de Suministro y Contrataciones Públicas, los pliegos deben evitar especificaciones restrictivas o direccionamientos que limiten la participación de los oferentes sin razones técnicas claras. La exigencia de protocolos de autenticación específicos, como RSA ACE o SecurID, podría interpretarse como un posible direccionamiento hacia tecnologías propietarias que restringen la igualdad de participación. Establecer el soporte para TACACS+ como requisito y dejar opcionales los protocolos RSA ACE o SecurID ampliaría la competencia y se alinearía con el principio de igualdad de condiciones en la contratación pública, facilitando una oferta de productos equivalentes técnicamente y promoviendo la transparencia en el proceso.

Respuesta	Fecha de Respuesta	01-11-2024

Favor remitirse al Pliego: Considerando la importancia de la integración con protocolos de autenticación robustos en materia de seguridad, se requiere que la solución sea integrable con la mayor cantidad de tecnologías como se solicita en este requerimiento de integración con RSA ACE o SecurID y para salvaguardar la inversión ya realizada por la institución, los equipos adquiridos deben formar un clúster altamente disponible con el equipo existente, por lo que se requiere que sean del mismo modelo con el mismo nivel de licencias y agregar diferentes algoritmos implicaría configuraciones innecesarias y sin la seguridad del correcto funcionamiento, Además de ello, la una inadecuada compra de una marca o modelo que no sea compatible con la plataforma o equipos existentes ocasionaría problemas innecesarios para la criticidad del datacenter. Con todo lo mencionado se busca eficiencia en el uso de los recursos públicos ya existentes como menciona la disposición legal.

Consulta 47 - Requisito de Autenticación vía Certificado IKE PKI en la Solución de Seguridad de Red Perimetral.

Consulta	Fecha de Consulta	29-10-2024

En el Pliego de Bases y Condiciones, en la sección de Suministros Requeridos – Especificaciones Técnicas – Grupo 1 y 2 - Ítem 11 (Adecuación del Sistema de Seguridad de Red Perimetral), se solicita que la solución soporte autenticación mediante certificado IKE PKI. Solicitamos respetuosamente a la Convocante que se especifique el tipo de autenticación específica que debe soportar la solución solicitada, aclarando si se requiere un tipo particular de implementación de IKE PKI o algún formato específico de certificado para asegurar la compatibilidad y la adecuación de las propuestas.

Esta solicitud de especificación adicional es importante para que los oferentes comprendan con precisión los requerimientos técnicos y puedan presentar propuestas alineadas con las expectativas y necesidades específicas de seguridad de la institución. Una mayor claridad en los detalles de autenticación evitará interpretaciones ambiguas que puedan afectar la igualdad de condiciones y asegurar una evaluación justa de las ofertas.

Argumentación Técnica: La autenticación mediante certificados IKE PKI (Internet Key Exchange Public Key Infrastructure) puede implementarse de varias formas y con distintos tipos de certificados, dependiendo de los protocolos de seguridad de red utilizados y los requisitos específicos de interoperabilidad y compatibilidad. Es fundamental para los oferentes conocer el tipo específico de autenticación y los formatos de certificados que se esperan (por ejemplo, certificados X.509, PKCS#12) para garantizar la funcionalidad de la solución en el contexto de seguridad de red perimetral de la institución. Sin esta precisión, existe el riesgo de que se presenten soluciones que no cumplan con las necesidades de autenticación, lo que podría afectar la seguridad y operatividad de la infraestructura de red.

Argumentación Legal: Conforme al artículo 45 de la Ley N° 7021/2022, de Suministro y Contrataciones Públicas, las especificaciones en los pliegos de bases y condiciones deben ser claras y detalladas para evitar interpretaciones ambiguas que puedan limitar la participación o afectar la equidad en la evaluación de ofertas. La falta de precisión en el tipo de autenticación mediante IKE PKI podría ser interpretada como una restricción innecesaria, que impide a los oferentes preparar propuestas adecuadas y compite con el principio de igualdad de participación. Al proporcionar una mayor claridad sobre los requisitos de autenticación, la Convocante fomenta una competencia justa y equitativa, respetando los principios de transparencia y competencia efectiva en el proceso de contratación pública.

Respuesta	Fecha de Respuesta	01-11-2024

Favor remitirse al Pliego: Considerando la importancia de la autenticación se requiere como mínimo el soporte de autenticación utilizando certificados X.509 es un método ampliamente usado para verificación de identidades de dispositivos en la red y a fin de dar confianza en materia de seguridad, se requiere que la solución sea integrable a los equipos adquiridos para formar un clúster altamente disponible, por lo que se requiere que sean del mismo modelo con el mismo nivel de licencias y agregar diferentes algoritmos implicaría configuraciones innecesarias y sin la seguridad del correcto funcionamiento, Además de ello, la una inadecuada compra de una marca o modelo que no sea compatible con la plataforma o equipos existentes ocasionaría problemas innecesarios para la criticidad del datacenter. Con todo lo mencionado se busca eficiencia en el uso de los recursos públicos ya existentes como menciona la disposición legal.

Consulta 48 - Requisito de Función de Resolución de Direcciones vía DNS en el Firewall para Detección de Dominios Maliciosos.

Consulta	Fecha de Consulta	29-10-2024

En las Especificaciones Técnicas del Pliego de Bases y Condiciones, se establece que el firewall deberá contar con una función de resolución de direcciones vía DNS, para que las conexiones hacia dominios maliciosos sean resueltas por el firewall como direcciones IPv4 e IPv6 previamente definidas. Solicitamos respetuosamente a la Convocante que aclare este requisito, en particular el alcance y los parámetros específicos de la función de resolución DNS solicitada.
Esta aclaración es fundamental para entender si el firewall debe integrar características adicionales de control de DNS, tales como listas de bloqueo específicas, actualización automática de listas de dominios maliciosos, o si debe resolver a direcciones particulares de manera personalizada. Esta precisión permitiría a los oferentes ajustar sus propuestas a los requisitos exactos de seguridad deseados, facilitando así una evaluación clara y equitativa de las ofertas.
Argumentación Técnica:
La funcionalidad de resolución DNS en un firewall puede implicar una variedad de configuraciones y niveles de protección. Dependiendo de los objetivos específicos de seguridad, el firewall puede requerir integración con bases de datos de amenazas en tiempo real o configurarse para interceptar solicitudes DNS y redirigirlas hacia direcciones IP predeterminadas. Sin una especificación clara sobre el alcance y los parámetros de la función de resolución DNS, los oferentes pueden interpretar el requerimiento de diferentes maneras, lo cual podría llevar a variaciones significativas en las propuestas, afectando la comparabilidad y la alineación con los objetivos de seguridad del sistema.
Argumentación Legal:
El artículo 45 de la Ley N° 7021/2022, de Suministro y Contrataciones Públicas, establece que los pliegos de bases y condiciones deben evitar ambigüedades y brindar una claridad técnica que permita a los oferentes comprender completamente los requisitos para preparar sus propuestas. La falta de precisión en este requerimiento puede interpretarse como una limitación que afecta la igualdad de participación, al no asegurar que todos los oferentes tengan la misma comprensión de los requisitos de seguridad. Proporcionar una aclaración detallada sobre esta funcionalidad fomentará una competencia justa y equitativa, alineada con los principios de transparencia y accesibilidad en el proceso de contratación pública.

Respuesta	Fecha de Respuesta	01-11-2024

Favor remitirse al Pliego: el firewall debe integrar características de control DNS, tales como: listas de bloqueo, bloqueos de dominios categorizados como maliciosos, y la resolución a direcciones IPs definidas por el administrador. Además, se requiere que la solución sea integrable a los equipos adquiridos para formar un clúster altamente disponible, por lo que se requiere que sean del mismo modelo con el mismo nivel de licencias y agregar diferentes algoritmos implicaría configuraciones innecesarias y sin la seguridad del correcto funcionamiento, Además de ello, la una inadecuada compra de una marca o modelo que no sea compatible con la plataforma o equipos existentes ocasionaría problemas innecesarios para la criticidad del datacenter. Con todo lo mencionado se busca eficiencia en el uso de los recursos públicos ya existentes como menciona la disposición legal.

Consulta 49 - Capacidad de los Equipos para Enviar Logs a Sistemas de Monitoreo Externos (SIEM).

Consulta	Fecha de Consulta	29-10-2024

En las Especificaciones Técnicas del Pliego de Bases y Condiciones se solicita que los equipos ofertados cuenten con la capacidad de enviar logs para sistemas de monitoreo externos, comúnmente denominados SIEM (Security Information and Event Management), de manera simultánea. Solicitamos respetuosamente a la Convocante que aclare este requisito, especificando los parámetros técnicos necesarios para asegurar la compatibilidad y funcionalidad en el envío de logs hacia plataformas SIEM.
Específicamente, solicitamos que se detalle si los equipos deben contar con capacidades específicas, tales como soporte para múltiples destinos de log, protocolos de transmisión de logs (por ejemplo, Syslog, HTTPS, etc.), formatos de log estándar (CEF, LEEF, JSON), y si se espera que el envío a los sistemas SIEM ocurra en tiempo real o bajo configuraciones específicas de intervalo de envío. Esta precisión permitiría a los oferentes ajustar sus propuestas a los requerimientos de monitoreo y seguridad necesarios, favoreciendo una evaluación técnica justa y precisa.
Argumentación Técnica: La integración de equipos de red con sistemas SIEM para la transmisión de logs puede implicar diversos niveles de configuración y compatibilidad, dependiendo de los protocolos, formatos y configuraciones de envío requeridos. Las especificaciones técnicas de estos elementos son esenciales para asegurar que los equipos ofrezcan un flujo de datos en tiempo real y compatible con la infraestructura de monitoreo externo. Sin claridad en estos detalles, los oferentes pueden interpretar el requisito de distintas maneras, generando inconsistencias en las propuestas que afecten tanto la capacidad de los equipos como la comparabilidad entre ofertas.
Argumentación Legal: El artículo 45 de la Ley N° 7021/2022, de Suministro y Contrataciones Públicas, establece que las especificaciones en los pliegos de bases y condiciones deben ser claras y detalladas para evitar ambigüedades que afecten la igualdad de condiciones entre los oferentes. La falta de precisión en este requisito puede interpretarse como una limitación, al no asegurar que todos los oferentes comprendan por igual los parámetros técnicos de envío de logs para sistemas SIEM. Proporcionar detalles específicos sobre este requisito técnico garantiza una competencia justa y equitativa, respetando los principios de transparencia y accesibilidad en el proceso de contratación pública.

Respuesta	Fecha de Respuesta	01-11-2024

Favor remitirse al Pliego: Para salvaguardar la inversión ya realizada por la institución, los equipos adquiridos deben formar un clúster altamente disponible con el equipo existente, por lo que se requiere que sean del mismo modelo con el mismo nivel de licencias y agregar diferentes algoritmos implicaría configuraciones innecesarias y sin la seguridad del correcto funcionamiento, Además de ello, la una inadecuada compra de una marca o modelo que no sea compatible con la plataforma o equipos existentes ocasionaría problemas innecesarios para la criticidad del datacenter. Con todo lo mencionado se busca eficiencia en el uso de los recursos públicos ya existentes como menciona la disposición legal.

Consulta 50 - IKE PKI

Consulta	Fecha de Consulta	29-10-2024

Pliego de Bases y Condiciones/SUMINISTROS REQUERIDOS – ESPECIFICACIONES TÉCNICAS/ Grupo 1y 2 - ITEM 11. Adecuación del Sistema de Seguridad de Red Perimetral/ se solicita lo siguiente:
“Autenticación vía certificado IKE PKI”
Se solicita a la Convocante pueda especificar qué tipo de autenticación debería soportar la solución requerida. Se vuelve a hacer este pedido esto considerando que en la consulta anterior, la respuesta fue esquiva, ignorando la ley de contrataciones de igualdad de participación entre todos los oferentes

Respuesta	Fecha de Respuesta	01-11-2024

Favor remitirse al Pliego: Considerando la importancia de la autenticación se requiere como mínimo el soporte de autenticación utilizando certificados X.509 es un método ampliamente usado para verificación de identidades de dispositivos en la red y a fin de dar confianza en materia de seguridad, se requiere que la solución sea integrable a los equipos adquiridos para formar un clúster altamente disponible, por lo que se requiere que sean del mismo modelo con el mismo nivel de licencias y agregar diferentes algoritmos implicaría configuraciones innecesarias y sin la seguridad del correcto funcionamiento, Además de ello, la una inadecuada compra de una marca o modelo que no sea compatible con la plataforma o equipos existentes ocasionaría problemas innecesarios para la criticidad del datacenter. Con todo lo mencionado se busca eficiencia en el uso de los recursos públicos ya existentes como menciona la disposición legal.

Consulta 51 - DNS

Consulta	Fecha de Consulta	29-10-2024
En las Especificaciones Técnicas, se menciona lo siguiente: “Deberá poseer la función resolución de direcciones vía DNS, para que conexiones como destino a dominios maliciosos sean resueltas por el Firewall como direcciones (IPv4 e IPv6), previamente definidos” Solicitamos a la Convocante pueda aclarar este requerimiento. Se vuelve a hacer este pedido esto considerando que en la consulta anterior, la respuesta fue esquiva, ignorando la ley de contrataciones de igualdad de participación entre todos los oferentes		

Respuesta	Fecha de Respuesta	01-11-2024
Favor remitirse al Pliego: el firewall debe integrar características de control DNS, tales como: listas de bloqueo, bloqueos de dominios categorizados como maliciosos, y la resolución a direcciones IPs definidas por el administrador. Además, se requiere que la solución sea integrable a los equipos adquiridos para formar un clúster altamente disponible, por lo que se requiere que sean del mismo modelo con el mismo nivel de licencias y agregar diferentes algoritmos implicaría configuraciones innecesarias y sin la seguridad del correcto funcionamiento, Además de ello, la una inadecuada compra de una marca o modelo que no sea compatible con la plataforma o equipos existentes ocasionaría problemas innecesarios para la criticidad del datacenter. Con todo lo mencionado se busca eficiencia en el uso de los recursos públicos ya existentes como menciona la disposición legal.		

Consulta 52 - SIEM

Consulta	Fecha de Consulta	29-10-2024
En las Especificaciones técnicas se solicita: Los equipos ofertados deberán contar con la capacidad de enviar log para sistemas de monitoreo externos denominados comúnmente como SIEM (Security Information and Event Management), simultáneamente. Se solicita a la Convocante aclarar mejor este requisito. Se vuelve a hacer este pedido esto considerando que en la consulta anterior, la respuesta fue esquiva, ignorando la ley de contrataciones de igualdad de participación entre todos los oferentes		

Respuesta	Fecha de Respuesta	01-11-2024
Favor remitirse al Pliego: Para salvaguardar la inversión ya realizada por la institución, los equipos adquiridos deben formar un clúster altamente disponible con el equipo existente, por lo que se requiere que sean del mismo modelo con el mismo nivel de licencias y agregar diferentes algoritmos implicaría configuraciones innecesarias y sin la seguridad del correcto funcionamiento, Además de ello, la una inadecuada compra de una marca o modelo que no sea compatible con la plataforma o equipos existentes ocasionaría problemas innecesarios para la criticidad del datacenter. Con todo lo mencionado se busca eficiencia en el uso de los recursos públicos ya existentes como menciona la disposición legal.		

Consulta 53 - desencripcion

Consulta	Fecha de Consulta	29-10-2024

SUMINISTROS REQUERIDOS – ESPECIFICACIONES TÉCNICAS- Grupo 1y 2 - ITEM 11. Adecuación del Sistema de Seguridad de Red Perimetral/ se menciona lo siguiente:
“Debe desencriptar tráfico que use certificados ECC (como ECDSA)”
Se sugiere a la Convocante considerar la desencripción de tráfico con certificados ECC, RSA, DSA, de manera a adquirir un equipo que responda con mayor flexibilidad a diversos entornos de operación.

Se Solicita a la convocante tomar las consultas con la seriedad requerida para un llamado tan importante, siendo que con la respuesta anterior no existe correlación entre la consulta y la respuesta emitida por ser un copy/paste de una respuesta anterior. Esto se podría considerar una actitud esquiva y un posible direccionamiento, lo que se contradice totalmente a la ley de contrataciones de igualdad de participación entre todos los oferentes.

Respuesta	Fecha de Respuesta	01-11-2024

Favor remitirse al Pliego: Considerando la importancia de la integración con protocolos de autenticación robustos en materia de seguridad, se requiere que la solución sea integrable con la mayor cantidad de tecnologías como se solicita en este requerimiento de integración con RSA ACE o SecurID y para salvaguardar la inversión ya realizada por la institución, los equipos adquiridos deben formar un clúster altamente disponible con el equipo existente, por lo que se requiere que sean del mismo modelo con el mismo nivel de licencias y agregar diferentes algoritmos implicaría configuraciones innecesarias y sin la seguridad del correcto funcionamiento, Además de ello, la una inadecuada compra de una marca o modelo que no sea compatible con la plataforma o equipos existentes ocasionaría problemas innecesarios para la criticidad del datacenter. Con todo lo mencionado se busca eficiencia en el uso de los recursos públicos ya existentes como menciona la disposición legal.

Consulta 54 - sub interfaces ethernet

Consulta	Fecha de Consulta	29-10-2024

Especificaciones Técnicas/Grupo 1y 2 - ITEM 11. Adecuación del Sistema de Seguridad de Red Perimetral/ se menciona lo siguiente:
“Los equipos ofertados deberán soportar sub-interfaces ethernet lógicas.”
Se solicita a la Convocante aclarar si deberá ser considerado el soporte de interfaces LACP o similar, interfaces redundantes, entre otras.

Se Solicita a la convocante tomar las consultas con la seriedad requerida para un llamado tan importante, siendo que con la respuesta anterior no existe correlación entre la consulta y la respuesta emitida por ser un copy/paste de una respuesta anterior. Esto se podría considerar una actitud esquiva y un posible direccionamiento, lo que se contradice totalmente a la ley de contrataciones de igualdad de participación entre todos los oferentes.

Respuesta	Fecha de Respuesta	01-11-2024

Favor remitirse al Pliego: Para salvaguardar la inversión ya realizada por la institución, los equipos adquiridos deben formar un clúster altamente disponible con el equipo existente, por lo que se requiere que sean del mismo modelo con el mismo nivel de licencias y agregar diferentes algoritmos implicaría configuraciones innecesarias y sin la seguridad del correcto funcionamiento, Además de ello, la una inadecuada compra de una marca o modelo que no sea compatible con la plataforma o equipos existentes ocasionaría problemas innecesarios para la criticidad del datacenter. Con todo lo mencionado se busca eficiencia en el uso de los recursos públicos ya existentes como menciona la disposición legal.

Consulta 55 - vpn ssl

Consulta	Fecha de Consulta	29-10-2024

n las especificaciones técnicas se solicita que el cliente vpn ssl sea compatible con sistemas operativos Windows y Linux actuales.
Se consulta a la Convocante si será necesaria la compatibilidad con sistemas operativos usuales en dispositivos móviles como IOS, Android.

Se Solicita a la convocante tomar las consultas con la seriedad requerida para un llamado tan importante, siendo que con la respuesta anterior no existe correlación entre la consulta y la respuesta emitida por ser un copy/paste de una respuesta anterior. Esto se podría considerar una actitud esquiva y un posible direccionamiento, lo que se contradice totalmente a la ley de contrataciones de igualdad de participación entre todos los oferentes.

Respuesta	Fecha de Respuesta	01-11-2024

Favor remitirse al Pliego: Ya que solo se contempla VPNs de acceso SSL desde sistemas operativos Windows y Linux. Para salvaguardar la inversión ya realizada por la institución, los equipos adquiridos deben formar un clúster altamente disponible con el equipo existente, por lo que se requiere que sean del mismo modelo con el mismo nivel de licencias y agregar diferentes algoritmos implicaría configuraciones innecesarias y sin la seguridad del correcto funcionamiento, Además de ello, la una inadecuada compra de una marca o modelo que no sea compatible con la plataforma o equipos existentes ocasionaría problemas innecesarios para la criticidad del datacenter. Con todo lo mencionado se busca eficiencia en el uso de los recursos públicos ya existentes como menciona la disposición legal.

Consulta 56 - tecnico datacenter

Consulta	Fecha de Consulta	29-10-2024

Pliego de Bases y Condiciones/REQUISITOS DE PARTICIPACIÓN Y CRITERIOS DE EVALUACIÓN/Capacidad Técnica, se solicita lo siguiente:
Autorización del fabricante o similar.
Para Grupo 1 ítem 1 al 11 Soporte Técnico Extendido para Datacenter Principal DCMT y para el Grupo 2 ítem 1 al 12 Soporte Técnico Extendido para Datacenter de Contingencia el oferente deberá presentar Carta de Autorización del Fabricante: La empresa oferente deberá contar con Autorización expedida por el fabricante para representantes, distribuidores y subdistribuidores de los productos ofrecidos; o el oferente deberá demostrar que cuenta con personal certificado en:
i. AOP -UPTIME INSTITUTE Accredited Operations Professional.
ii. ATS UPTIME INSTITUTE - Accredited Tier Specialist.

No se comprende la relación existente entre la Autorización del Fabricante/Distribuidor respecto a las certificaciones que son solicitadas, las que también podrían resultar limitativas para el llamado en cuestión. Adicional a esto, no se solicitan criterios de calificación que consideren la experiencia y/o certificaciones técnicas del oferente en las marcas existentes que garanticen la idoneidad del oferente para prestar los servicios solicitados.
Solicitamos se pueda reformular los requisitos de capacidad técnica establecidos.

Se Solicita a la convocante tomar las consultas con la seriedad requerida para un llamado tan importante, siendo que con la respuesta anterior se nota una actitud esquiva y un posible direccionamiento, lo que se contradice totalmente a la ley de contrataciones de igualdad de participación entre todos los oferentes.

Respuesta	Fecha de Respuesta	01-11-2024

Favor remitirse al Pliego. Consulta similar fue aclarada en la respuesta de la consulta 4. La certificación solicitada es acorde a este tipo de llamado. Además, lo solicitado garantiza que el producto cumple con estándares de calidad y seguridad establecidos y de facilitar e identificar en caso de defectos o problemas, lo que es esencial para el manejo de garantías y reclamos.

Consulta 57 - ITIL

Consulta	Fecha de Consulta	29-10-2024

Pliego de Bases y Condiciones/REQUISITOS DE PARTICIPACIÓN Y CRITERIOS DE EVALUACIÓN/Capacidad Técnica, se solicita lo siguiente:
El oferente deberá contar con 2 personales con certificación ITILv4, dentro su staff permanente.

Solicitamos a la Convocante pueda aceptar ofertas que contemplen al menos 1 (un) personal ITILv4 dentro del staff permanente, o en su lugar aceptar la inclusión de un personal con la certificación solicitada posterior a la contratación.

Respuesta	Fecha de Respuesta	01-11-2024

Favor remitirse al Pliego. Consulta similar fue aclarada en la respuesta de la consulta 5. Se solicita esa cantidad por la criticidad del servicio de gestión, ya que es el Datacenter del MEC, y con esto se espera las mejores prácticas para la gestión de servicios de TI y mejorar los plazos de respuesta como lo dice la certificación.

Consulta 58 - redundancia

Consulta	Fecha de Consulta	29-10-2024

Pliego de Bases y Condiciones/SUMINISTROS REQUERIDOS – ESPECIFICACIONES TÉCNICAS/ITEM 11. Adecuación del Sistema de Seguridad de Red Perimetral, se solicita lo siguiente:
A fin de mejorar la seguridad perimetral de la red, se deberá de agregar 1 (un) equipo para alcanzar la redundancia en el Datacenter de Principal.
Sin embargo, en Cantidad: 3 unidades. Se sugiere a la Convocante, solicitar equipos que posean mejor performance a los especificados para Seguridad Perimetral, y con esto, incluso poder disminuir la cantidad solicitada, contar con redundancia y lograr mayor eficiencia económica.

se consulta nuevamente a la convocante dado que en la respuesta anterior menciona que: "...Los equipos ofertados deberán ser idéntico al equipo existente en la institución en sus componentes de Hardware y Software" siendo un claro direccionamiento a una marca, modelo específicos, ignorando la ley de contrataciones de igualdad de participación entre todos los oferentes.

Respuesta	Fecha de Respuesta	01-11-2024

Favor remitirse al Pliego: Para salvaguardar la inversión ya realizada por la institución, los equipos adquiridos deben formar un clúster altamente disponible con el equipo existente, por lo que se requiere que sean del mismo modelo con el mismo nivel de licencias y agregar diferentes algoritmos implicaría configuraciones innecesarias y sin la seguridad del correcto funcionamiento, Además de ello, la inadecuada compra de una marca o modelo que no sea compatible con la plataforma o equipos existentes ocasionaría problemas innecesarios para la criticidad del datacenter y teniendo en cuenta que los requerimientos están basados en la infraestructura y topología actual y planificada a futuro de la convocante. En este sentido, contar con solo seis interfaces RJ45 1 Gbps no permitiría la implementación de la arquitectura planificada y aprobada, además de comprometer la escalabilidad y redundancia de la misma. Con todo lo mencionado se busca eficiencia en el uso de los recursos públicos ya existentes como menciona la disposición legal.

Consulta 59 - interfaces rj45

Consulta	Fecha de Consulta	29-10-2024

Pliego de Bases y Condiciones/SUMINISTROS REQUERIDOS – ESPECIFICACIONES TÉCNICAS/ Grupo 1y 2 - ITEM 11. Adecuación del Sistema de Seguridad de Red Perimetral, se solicita lo siguiente:
Los equipos ofertados deberán contar con al menos 14 interfaces 1GE RJ45 – Exigido
Considerando que los equipos de Seguridad Perimetral solicitados contarán con la función de protección de Borde (su misión principal), y que a lo sumo se conectarán físicamente con equipos de Core dentro del Datacenter, por lo que no será necesario una cantidad considerable de puertos disponibles y que de seguro estas conexiones a nivel de core o distribución se realizarán con enlaces de mayor capacidad de tráfico, solicitamos a la Convocante, pueda aceptar equipos que ofrezcan al menos 6 (seis) puertos o interfaces de 1GE RJ45

Se consulta nuevamente a la convocante dado que en la respuesta anterior menciona que: "...Los equipos ofertados deberán ser idéntico al equipo existente en la institución en sus componentes de Hardware y Software" siendo un claro direccionamiento a una marca, modelo específicos, ignorando la ley de contrataciones de igualdad de participación entre todos los oferentes.

Respuesta	Fecha de Respuesta	01-11-2024

Favor remitirse al Pliego: Para salvaguardar la inversión ya realizada por la institución, los equipos adquiridos deben formar un clúster altamente disponible con el equipo existente, por lo que se requiere que sean del mismo modelo con el mismo nivel de licencias y agregar diferentes algoritmos implicaría configuraciones innecesarias y sin la seguridad del correcto funcionamiento, Además de ello, la inadecuada compra de una marca o modelo que no sea compatible con la plataforma o equipos existentes ocasionaría problemas innecesarios para la criticidad del datacenter y teniendo en cuenta que los requerimientos están basados en la infraestructura y topología actual y planificada a futuro de la convocante. En este sentido, contar con solo seis interfaces RJ45 1 Gbps no permitiría la implementación de la arquitectura planificada y aprobada, además de comprometer la escalabilidad y redundancia de la misma. Con todo lo mencionado se busca eficiencia en el uso de los recursos públicos ya existentes como menciona la disposición legal.

Consulta 60 - certificados

Consulta	Fecha de Consulta	29-10-2024

Pliego de Bases y Condiciones/SUMINISTROS REQUERIDOS – ESPECIFICACIONES TÉCNICAS// Grupo 1y 2 - ITEM 11. Adecuación del Sistema de Seguridad de Red Perimetral, se establece lo siguiente:
El Oferente deberá demostrar la capacidad de brindar soporte técnico local en la República del Paraguay, durante el periodo de garantía, de forma inmediata, para lo cual se deberá presentar Certificados de Capacitación Técnica (de al menos dos técnicos) de las versiones recientes de: Seguridad, Servidores, Switches, Routers, Software de Virtualización. Dichos técnicos mencionados en los Certificados de Capacitación deberán ser parte del plantel permanente del Oferente o podrá ser subcontratado.
El requisito no es muy específico respecto a la capacidad del oferente de instalar y configurar el Equipo ofertado. Solicitamos a la Convocante establecer un requisito más específico de manera a garantizar la calidad y lograr los resultados esperados.

Se Solicita a la convocante tomar las consultas con la seriedad requerida para un llamado tan importante, siendo que la respuesta anterior muestra una actitud esquiva lo que se puede entender como un posible direccionamiento, lo que se contradice totalmente a la ley de contrataciones de igualdad de participación entre todos los oferentes.

Respuesta	Fecha de Respuesta	01-11-2024

Favor remitirse al Pliego: Se solicita la certificación por la criticidad del servicio de gestión, ya que es el Datacenter del MEC y además está establecido en el PBC - Especificaciones Técnicas - Grupo 1 y 2 - Ítem 11 (Adecuación del Sistema de Seguridad de Red Perimetral).

Consulta 61 - MTBF

Consulta	Fecha de Consulta	29-10-2024

Pliego de Bases y Condiciones/SUMINISTROS REQUERIDOS – ESPECIFICACIONES TÉCNICAS/ Grupo 1y 2 - ITEM 11. Adecuación del Sistema de Seguridad de Red Perimetral
Se solicita MTBF de 120.000 horas. Se solicita aceptar equipos con MTBF de un minimo de 80.000horas, considerando seria equivalente cercano a 10 años, periodo en el el avance tecnologico tambien exigira renovaciones de performance y funcionalidades. Se consulta nuevamente a la convocante dado que en la respuesta anterior menciona que: "...Los equipos ofertados deberán ser idéntico al equipo existente en la institución en sus componentes de Hardware y Software" siendo un claro direccionamiento a una marca, modelo específicos, ignorando la ley de contrataciones de igualdad de participación entre todos los oferentes.

Respuesta	Fecha de Respuesta	01-11-2024

Favor remitirse al Pliego: Para salvaguardar la inversión ya realizada por la institución, los equipos adquiridos deben formar un clúster altamente disponible con el equipo existente, por lo que se requiere que sean del mismo modelo con el mismo nivel de licencias y agregar diferentes algoritmos implicaría configuraciones innecesarias y sin la seguridad del correcto funcionamiento, Además de ello, la una inadecuada compra de una marca o modelo que no sea compatible con la plataforma o equipos existentes ocasionaría problemas innecesarios para la criticidad del datacenter. Con todo lo mencionado se busca eficiencia en el uso de los recursos públicos ya existentes como menciona la disposición legal.

Consulta 62 - protocolos

Consulta	Fecha de Consulta	29-10-2024

Pliego de Bases y Condiciones/SUMINISTROS REQUERIDOS – ESPECIFICACIONES TÉCNICAS/ Grupo 1y 2 - ITEM 11. Adecuación del Sistema de Seguridad de Red Perimetral/ se solicita lo siguiente:
“La solución de VPN debe soportar la integración con los siguientes protocolos de autenticación:
- LDAP
- RADIUS
- ACE Management Servers (SecurID)
- Client Certificates, authenticated by trusted CAs”.
Solicitamos pueda establecerse como opcional el soporte de integración con protocolo de autenticación RSA ACE o SecurID o bien que se acepten en su lugar, otras opciones de autenticación como OAuth2 Server, PICC 4A Server, entre otras. De manera a contar con una mayor variedad de ofertas con productos igualmente eficientes adecuados al contexto de operación.

Se Solicita esto considerando que lo solicitado corresponde al cumplimiento de un solo equipo, el Fortinet fg-1100e siendo un claro direccionamiento a una marca, modelo específicos, ignorando la ley de contrataciones de igualdad de participación entre todos los oferentes.

Respuesta	Fecha de Respuesta	01-11-2024

Favor remitirse al Pliego: Es para salvaguardar la inversión ya realizada por la institución, los equipos adquiridos deben formar un clúster altamente disponible con el equipo existente, por lo que se requiere que sean del mismo modelo con el mismo nivel de licencias y esto es técnicamente sabido que la agrupación de varios recursos "clúster" para ejecutar las tareas deben ser idénticos y asi llegar al objetivo principal que sería la integración tecnológica.

Consulta 63 - autenticación

Consulta	Fecha de Consulta	29-10-2024

Pliego de Bases y Condiciones/SUMINISTROS REQUERIDOS – ESPECIFICACIONES TÉCNICAS/ Grupo 1y 2 - ITEM 11. Adecuación del Sistema de Seguridad de Red Perimetral/ se solicita lo siguiente:
“La solución de VPN debe soportar la integración con los siguientes protocolos de autenticación:
- LDAP
- RADIUS
- ACE Management Servers (SecurID)
- Client Certificates, authenticated by trusted CAs”.
Solicitamos pueda establecerse como opcional el soporte de integración con protocolo de autenticación RSA ACE o SecurID, y sugerimos sea agregado en su lugar como requisito, protocolos como TACACS+, ampliamente difundido.

Se solicita esto considerando que lo solicitado corresponde al cumplimiento de un solo equipo, el Fortinet fg-1100e siendo un claro direccionamiento a una marca, modelo específicos, ignorando la ley de contrataciones de igualdad de participación entre todos los oferentes.

Respuesta	Fecha de Respuesta	01-11-2024

Favor remitirse al Pliego: Considerando la importancia de la integración con protocolos de autenticación robustos en materia de seguridad, se requiere que la solución sea integrable con la mayor cantidad de tecnologías como se solicita en este requerimiento de integración con RSA ACE o SecurID y para salvaguardar la inversión ya realizada por la institución, los equipos adquiridos deben formar un clúster altamente disponible con el equipo existente, por lo que se requiere que sean del mismo modelo con el mismo nivel de licencias y agregar diferentes algoritmos implicaría configuraciones innecesarias y sin la seguridad del correcto funcionamiento, Además de ello, la una inadecuada compra de una marca o modelo que no sea compatible con la plataforma o equipos existentes ocasionaría problemas innecesarios para la criticidad del datacenter. Con todo lo mencionado se busca eficiencia en el uso de los recursos públicos ya existentes como menciona la disposición legal.

Consulta 64 - EXPERIENCIA

Consulta	Fecha de Consulta	29-10-2024

Pliego de Bases y Condiciones/REQUISITOS DE PARTICIPACIÓN Y CRITERIOS DE EVALUACIÓN/Experiencia Requerida

Tratándose de una Extensión de Soporte de Datacenter, los requisitos establecidos están muy orientados a la provisión de Firewall, este siendo solo 1 ítem del proyecto, lo cual no necesariamente aplique a proveedores idóneos para los servicios que son solicitados. Adicionalmente, no se solicita experiencia en la provisión o instalación de equipos de las marcas existentes que garanticen la idoneidad del oferente para prestar los servicios solicitados.

Se solicita respetuosamente a la Convocante, que pueda reformular los requisitos de Experiencia Y Capacidad Técnica establecidos, de manera acorde y equitativa, según los servicios/bienes que son solicitados. Se vuelve a hacer este pedido esto considerando que en la consulta anterior, la respuesta fue esquiva, ignorando la ley de contrataciones de igualdad de participación entre todos los oferentes

Respuesta	Fecha de Respuesta	01-11-2024

Favor remitirse al Pliego: Es para salvaguardar la inversión ya realizada por la institución en cuanto a los equipos existentes y ponerlos en clúster y todo está integrado en el datacenter por ese motivo está incluido dentro del proyecto.