

HACIENDA
HIPOTECARIA

SOCIEDAD

SECRETARÍA DE HACIENDA CRÉDITO PÚBLICO

JDA

SF SOCIEDAD HIPOTECARIA FEDERAL

SOCIEDAD HIPOTECARIA FEDERAL, S.N.C.

RECIBIDO

★ 20 ENE 2021 ★

DIRECCIÓN DE ADMINISTRACIÓN

Ciudad de México, México, a 20 de enero de 2021.

SOCIEDAD HIPOTECARIA FEDERAL, S.N.C.

RECIBIDO

★ 20 ENE 2021 ★

DIRECCIÓN GENERAL ADJUNTA DE ADMINISTRACIÓN Y OPERACIONES DTI

14:31

SOLICITUD DE CONTRATACIÓN A TRAVÉS DE LICITACIÓN PÚBLICA
CONTRATACIÓN DEL SERVICIO ADMINISTRADO DE LA RED LAN PARA SHF.

MTRO. JUAN JAIME MOLINA VÉLEZ
DIRECTOR GENERAL ADJUNTO DE ADMINISTRACIÓN Y OPERACIONES.
PRESENTE.

SOCIEDAD HIPOTECARIA FEDERAL, S.N.C.

RECIBIDO

20 ENE. 2021

SUBDIRECCION DE RECURSOS MATERIALES Y SERVICIOS GENERALES

Sociedad Hipotecaria Federal cuenta con un contrato de arrendamiento que incluye equipo de RED LAN, switches de acceso, switches centrales, controladora principal para red inalámbrica, ya que el contrato de servicio, se tiene planeado iniciar la renovación de equipos a partir del 01 de abril de 2021, para lo cual la Dirección de Tecnologías de la Información, requiere de la realización de un procedimiento de licitación pública para la Contratación del Servicio Administrado de la RED LAN para SHF; por lo que le solicito su apoyo para llevar a cabo su formalización de acuerdo con lo siguiente: • Especificaciones técnicas de la RED LAN.

Descripción de los servicios:

HACIENDA

HIPOTECARIA

SOCIEDAD

FEDERAL

Se adjunta a la presente el "Anexo Técnico", el cual contiene los términos de referencia.

Para tales efectos, los plazos para la entrega de los bienes y/o prestación de los servicios, será de 45 meses a partir del 01 de abril del 2021. Procedimiento de contratación solicitado:

Licitación pública nacional.

La motivación para la contratación se basa en la necesidad de Sociedad Hipotecaria Federal (SHF), e la contratación del Servicio Administrado de Equipos para Infraestructura LAN (Red Área Local), con e



HACIENDA
SECRETARÍA DE HACIENDA Y CRÉDITO PÚBLICO



propósito de mantener la comunicación de tanto interna como externa con sus aplicaciones y servicios con el personal que labora en la institución así como lo son sus intermediarios financieros para efecto de mantener acceder de forma íntegra, confidencial y disponible de la información relacionada con sus procesos, con el propósito de asegurar la continuidad del negocio ante eventos de contingencia que pudieran afectar sus operaciones y provocar pérdidas significativas al negocio y su entorno financiero.

Para la Contratación del Servicio Administrado de la RED LAN para SHF, el plazo propuesto se considera de 45 meses, a fin de acceder a precios competitivos en el mercado.

Investigación de mercado.

El documento FO-CON-05 Cuadro Comparativo resultado de la investigación de mercado realizada, se encuentra incluido en el documento "Estudio de Mercado".

Cabe señalar que ninguno de los posibles proveedores está condicionando su propuesta y que con dichas características solicitadas no se limita la libre participación de otros posibles proveedores.

Monto estimado de la contratación:



HACIENDA

HIPOTECARIA

SOCIEDAD

FEDERAL

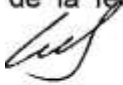
De conformidad con el resultado que arroja la investigación de mercado que al efecto se adjunta, el monto estimado de la contratación es de **\$36,800,530.20** (Treinta y seis millones ochocientos mil quinientos treinta pesos 20/100 M.N.) más el correspondiente Impuesto al Valor Agregado.

El flujo aproximado del ejercicio del presupuesto es el siguiente:

AÑO	IMPORTE X AÑO
2021	<u>7,360,106.04</u>
2022	<u>9,813,474.72</u>
2023	<u>9,813,474.72</u>
2024	<u>9,813,474.72</u>
TOTAL	<u>36,800,530.20</u>

Forma de pago propuesta:

El pago se realizará a mes vencido en moneda nacional, por un período de 45 meses con flujo de efectivo de 43 pagos con importes fijos, en un plazo no mayor de 20 días naturales contados a partir de la fecha en que se haya recibido la factura correspondiente, debidamente requisitada, como



2

Ejército Nacional 180, Col. Azules, C.P. 11590, Miguel Hidalgo, Ciudad de México.
Tel: 55 5263 4500 www.gob.mx/shf



de la fecha en que se haya recibido la factura correspondiente, debidamente requisitada, como

SECRETARÍA DE HACIENDA CRÉDITO PÚBLICO



resultado de la aceptación a entera satisfacción de SHF, de los entregables previamente definidos para estos efectos.

Cabe señalar que, con base en la investigación de mercado realizada por la Dirección a mi cargo, he determinado que el precio señalado para la presente contratación se encuentra dentro de los rangos

3

Col.

Miguel Hidalgo,

México.

HACIENDA

SOCIEDAD

HIPOTECARIA

FEDERAL

razonables de mercado y resulta conveniente para la Sociedad Hipotecaria Federal, S.N.C. en función de los beneficios que se obtendrán como resultado de llevar a cabo la contratación de mérito.

Partida 31904 (Servicios Integrales de
Infraestructura de Cómputo)

Ejercicio 2021

\$7,360,106.04

SOCIEDAD HIPOTECARIA FEDERAL,
SpN.,C.
SUBDIRECCIÓN DE PRESUPUESTO

1 5 ENE

SE CUENTA CON SUACIENCIA PRESUPUESTAL
EN (S) PARTIDA

Vo.Bo. Suficiencia Presupuestal.

El presupuesto a ejercer en los años subsecuentes, estará sujeto a la

aprobación del mismo por parte de la Cámara de Diputados



HACIENDA
SECRETARÍA DE HACIENDA Y CRÉDITO PÚBLICO



HACIENDA

HIPOTECARIA

SOCIEDAD

FEDERAL

Motivación y fundamentación legal.

De conformidad con el artículo 26 fracción I de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, someto a su consideración, a efecto de que se sigan los trámites y procedimientos a que haya lugar, la realización de un procedimiento de Licitación Pública, toda vez que esta contratación es necesaria para:

- A) Satisfacer la necesidad de Sociedad Hipotecaria Federal, S.N.C., de contar con el Contratación del Servicio Administrado de la RED LAN para SHF, como infraestructura para el manejo de información entre el usuario y el centro de datos, como herramienta esencial, para la integridad, confidencialidad y disponibilidad de la información relacionada con sus

procesos.

- B) Atender -la normatividad vigente y aplicable a Sociedad Hipotecaria Federal, S.N.C., en la materia.
- C) Disminución del riesgo tecnológico, al no realizar un proceso de migración y cambio de proveedor año con año.

Acreditamiento de los criterios del artículo 134 constitucional.

La presente solicitud de llevar a cabo una Licitación Pública Nacional para los servicios requeridos se encuentra fundamentada en el Artículo 134 Constitucional que establece los criterios de economía, eficacia, eficiencia, imparcialidad, honradez y transparencia, conforme a lo siguiente:

Economía.

SHF cuenta con los recursos presupuestales necesarios derivados de su operación, para hacer frente a los compromisos que deriven de la celebración de un contrato, consecuencia del procedimiento de Licitación Pública solicitado, conforme los importes determinados en la Investigación de Mercado (realizada por la Subdirección de Infraestructura Tecnológica, quedando debidamente documentado dentro del correspondiente Estudio de Mercado.

Eficacia y eficiencia.

Tal y como se desprende de la Investigación de Mercado, para efectuar la contratación de los servicios que refiere la presente solicitud, no resultan aplicables ni el procedimiento de Invitación a cuando menos Tres Personas ni Adjudicación Directa, debido a que en ambos casos se superan los montos de actuación correspondientes establecidos para la Institución y tampoco existe la posibilidad de que

HACIENDA

SOCIEDAD

HIPOTECARIA

FEDERAL

únicamente una empresa pueda cumplir con los requerimientos de SHF.



4

Ejército Nacional 180, Col. Azures, C.P. 11590, Miguel Hidalgo, Ciudad de México.
Tel: 55 5263 4500 www.gob.mx/shf



única nte una empresa pueda cumplir con los requerimientos de SHF.

HACIENDA

HIPOTECARIA

SOCIEDAD

FEDERAL



HACIENDA
SECRETARÍA DE HACIENDA Y CRÉDITO PÚBLICO



Consecuentemente, mediante la instrumentación de la presente contratación a través del procedimiento de Licitación Pública Nacional que se solicita, se satisface el criterio de eficacia, toda vez que representa el procedimiento que, atendiendo la normatividad aplicable, permitirá a SHF la obtención de los servicios requeridos bajo las condiciones más favorables para la Institución.

Por otra parte, el criterio de eficiencia queda de manifiesto, toda vez que con la contratación que se pretende llevar a cabo mediante el proceso licitatorio solicitado, se atenderá de forma automática la necesidad de mantener segura la operatividad de los procesos de las unidades administrativas y sustantivas de la SHF.

Imparcialidad y honradez.

Después de haber realizado el análisis de las distintas alternativas existentes en el mercado, se determinó que el procedimiento de contratación que se solicita es la mejor opción disponible para la SHF, por lo que se ha dado un cabal cumplimiento a los criterios de imparcialidad y honradez en la selección del procedimiento de contratación.

Por otra parte, dentro del Anexo "G" que formará parte de las bases de licitación, se incluyen, para el conocimiento de los interesados, los criterios de evaluación para efectuar la selección del proveedor, con base en el esquema de puntos y porcentajes, de conformidad con los lineamientos emitidos por la Secretaría de la Función Pública y el oficio TU-01/2012..

Transparencia.

El criterio de transparencia se acredita fehacientemente, en virtud de que, en la Investigación de Mercado, el flujo de información en todo momento fue accesible, claro, oportuno, completo y verificable para los participantes, información que se encuentra disponible en los archivos correspondientes.

Asimismo, se aporta mayor transparencia al determinarse con la Investigación de Mercado el procedimiento de contratación solicitado, en apego a la normatividad establecida en Ley, verificable en todo momento al verse publicado en el sistema COMPRANET, herramienta que la Secretaría de la Función Pública ha puesto a disposición de las instituciones que conforman el Gobierno Federal, como

HACIENDA

HIPOTECARIA

SOCIEDAD

FEDERAL

un mecanismo para brindar transparencia, igualdad y oportunidad de información a los interesados y a la ciudadanía.

Cabe mencionar que la Investigación de Mercado, mediante la cual se determinó la conveniencia de efectuar el procedimiento solicitado para efectuar la contratación de los servicios que SHF requiere, tuvo como sustento, entre otros, las consultas efectuadas al propio sistema COMPRANET.

5

Ejército Nacional 180, Col. Azures, C.P. 11590, Miguel Hidalgo, Ciudad de México.
Tel: 55 5263 4500 www.gob.mx/shf



SECRETORIA DE HACIENDA e RÉDITO PÚBLICO



En términos de los Lineamientos en materia de Adquisiciones, Arrendamientos y Servicios y de Obras públicas y servicios relacionados con las mismas, se precisa la siguiente información:

- I. La dirección de entrega será en el o los domicilios propuestos por el licitante que resulte adjudicado. Se establece además como domicilio de contacto en la Avenida Ejército Nacional 180, 7º Piso, Col. Anzures, Alcaldía Miguel Hidalgo, Ciudad de México, CP 11590, en la Subdirección de Infraestructura Tecnológica, en un horario de lunes a viernes de 9:00 a 19:00 horas.
- II. El Licitante Ganador brindará los servicios correspondientes al Contratación del Servicio Administrado de la RED LAN para SHF, por un periodo de 45 meses a partir de su contratación. Las reuniones de trabajo y las actividades de planeación de la solución podrán realizarse de forma inmediata, una vez realizado el acto de fallo.
- III. El servidor público facultado para recibir los servicios, quien será el responsable de su aceptación a satisfacción, su devolución o rechazo y de determinar los incumplimientos en el

8

Ejército Nacional 180, Col. Azures, C.P. 11590, Miguel Hidalgo, Ciudad de México.
Tel: 55 5263 4500 www.gob.mx/shf

HACIENDA

SOCIEDAD

HIPOTECARIA

FEDERAL

caso de los servicios, así como de hacer cumplir los plazos que se establezcan para tales efectos de acuerdo con estos lineamientos será el Subdirector de Infraestructura Tecnológica.

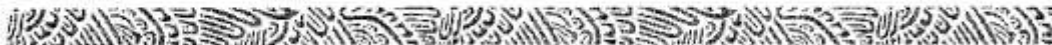
- IV. El tipo de pruebas o verificación física a que se someterán los servicios de acuerdo con lo establecido en el artículo 29 fracción X de la Ley de Adquisiciones, para ser recibidos a satisfacción, así como el responsable de llevarlas a cabo y el tiempo requerido para su realización, el cual no podrá exceder de diez días naturales contados a partir de la entrega de los bienes muebles o la prestación del servicio en el domicilio a que se refiere la fracción I de este lineamiento, se detallan en el anexo técnico.
- V. El procedimiento para la devolución o rechazo de los bienes muebles o para determinar los incumplimientos en la prestación de los servicios, lo cual solamente procederá por causas previstas en el contrato respectivo. En caso de incumplimiento, el servidor público facultado para recibir los servicios dará aviso al proveedor y a la Subdirección de Recursos Materiales y Servicios Generales, en el caso de que se deban aplicar penas.

Incumplimiento

El incumplimiento en la prestación de los servicios será comunicado al proveedor a más tardar el día hábil siguiente a aquél en que éste se determine, señalando las razones que lo motivaron, las cuales deberán estar vinculadas a las condiciones establecidas en el contrato, indicando el plazo para su reposición o corrección.

6

Ejército Nacional 180, Col. Azures, C.P. 11590, Miguel Hidalgo, Ciudad de México.
Tel: 55 5263 4500 www.gob.mx/shf



A
PÚBLICO

SIF

SECRETARIA DE HACIENDA Y CRÉDITO

9

Ejército Nacional Col. Azures. C.P. 11590, Miguel Hidalgo, Ciudad de México.
Tel: 55 5263 4500 www.gob.mx/shf

HACIENDA

HIPOTECARIA

SOCIEDAD

FEDERAL

FACTURAS

I. Área responsable, lugar y horario para su recepción;

Se entregará a la Subdirección de Recursos Materiales y Servicios Generales, ubicada en Ejército Nacional 180, Piso 8, Colonia Azures, Delegación Miguel Hidalgo, Ciudad de México, de lunes a viernes en días hábiles bancarios, en un horario de 9:00 a 18:00 horas.

II. Documentos que deberán acompañar a la misma.

La factura correspondiente deberá ir acompañada de los entregables respectivos.

III. El servidor público facultado para validar que las facturas o los documentos que presente el proveedor para su pago, cumplan los requisitos fiscales correspondientes y aquéllos de aceptación del bien mueble o servicio que amparen, quien será responsable de devolver al proveedor la factura o el documento de que se trate, dentro de los tres días hábiles siguientes al de su recepción, comunicándole los errores o deficiencias detectadas; será la Subdirectora de Recursos Materiales y Servicios Generales.

En el caso de que se comunique al proveedor la existencia de errores o deficiencias en la factura o el documento que hubiere presentado, será responsabilidad del proveedor subsanarlos y presentar nuevamente la factura o el documento que reúna los requisitos fiscales correspondientes en el menor tiempo posible.

En ningún caso procederá la devolución de facturas o de los documentos presentados por el proveedor, por errores que no afecten la validez fiscal del documento o por causas imputables a la dependencia o entidad.

Con base en lo anterior, le informo que dicha contratación es indispensable para la realización de las actividades de esta Dirección, por lo que le solicito nuevamente su apoyo para llevar a cabo el procedimiento de contratación respectivo.

Atentamente



ING. GREGORIO LINARES URENDA
DIRECTOR DE TECNOLOGÍAS DE LA INFORMACIÓN

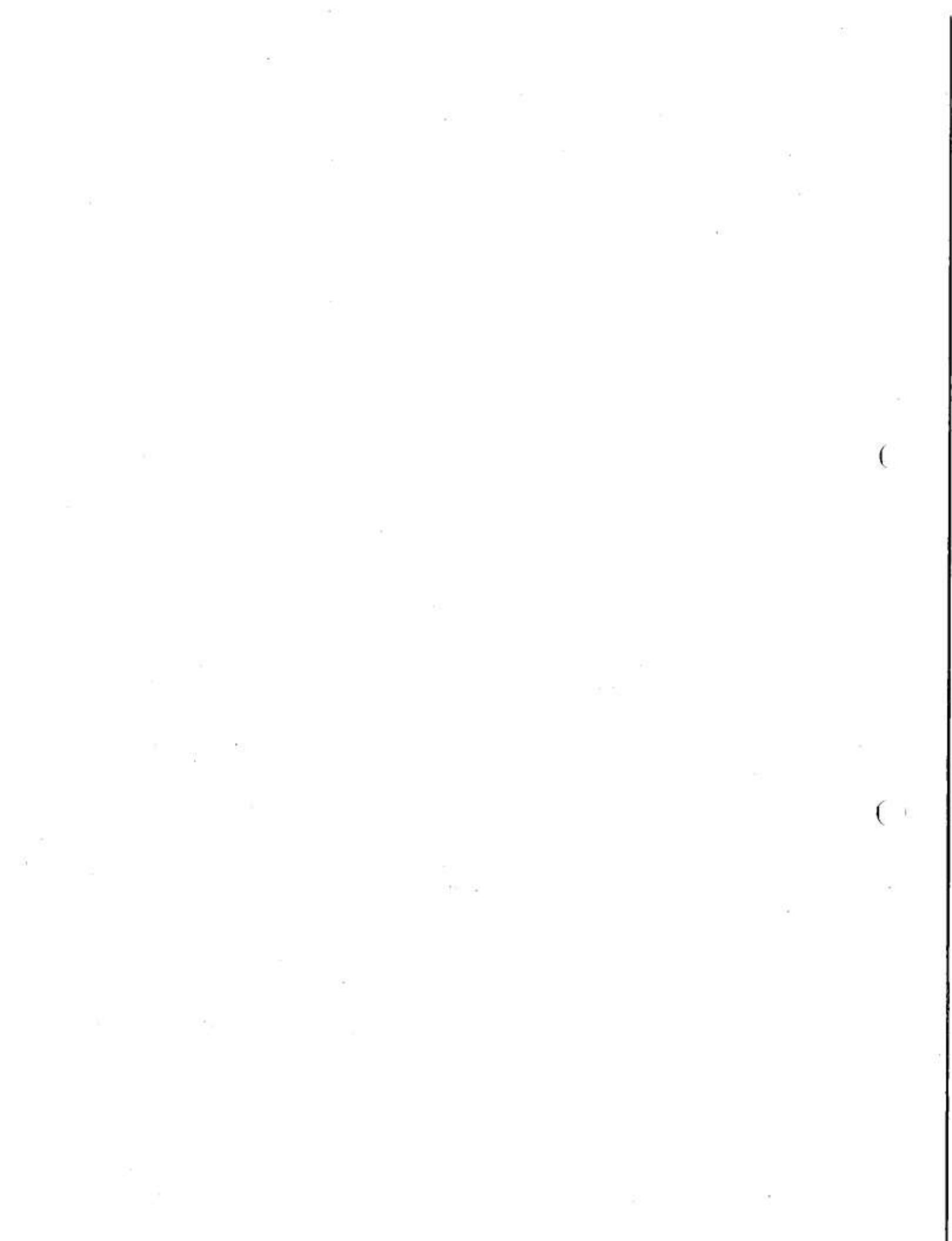


HACIENDA
HIPOTECARIA

SOCIEDAD
FEDERAL

C.c.p. Lic. María Elena Zaldívar Sánchez. - Director de Administración.

Lic. Bertha Alicia Robles Quintero. - Subdirectora de Recursos Materiales y Servicios Generales.





HACIENDA

SECRETARÍA DE HACIENDA PÚBLICA



SOCIEDAD
HIPOTECARIA
FEDERAL

Anexo A - Anexo Técnico.

SERVICIO ADMINISTRADO DE EQUIPOS PARA LA INFRAESTRUCTURA DE RED LAN.

1. INTRODUCCIÓN.

1.1 Sociedad Hipotecaria Federal

SHF es una Institución Financiera perteneciente a la Administración Pública Federal, como entidad paraestatal en su carácter de Banca de Desarrollo, su objetivo es impulsar el desarrollo de los mercados primario y secundario de crédito a la vivienda, mediante el otorgamiento de garantías destinadas a la construcción, adquisición y mejora de vivienda, preferentemente de interés social; al incremento de la capacidad productiva y del desarrollo tecnológico relacionados con la vivienda, así como a los financiamientos relacionados con el equipamiento de conjuntos habitacionales.

1 Antecedente

SHF cuenta con equipo de red LAN que incluye switches de acceso, switches centrales capa 3, puntos de acceso y controladora principal para red inalámbrica. SHF se encuentra en un proceso de licitación, ya que el contrato de arrendamiento con el actual proveedor está por finalizar. Se tiene planeado iniciar la renovación de equipos a partir de la firma del contrato.

1.4 Objetivo.

La presente licitación tiene por objeto la contratación plurianual del arrendamiento de equipos para la infraestructura LAN (Red de Área Local) para Sociedad Hipotecaria Federal, conforme las especificaciones técnicas y alcances de los servicios que se describen en el presente anexo.

1.5 Localidades.

Los servicios objeto de la presente contratación, serán proporcionados en el inmueble de SHF, ubicado en Ejercito Nacional #180, Colonia Anzures, Ciudad de México, C.P. 11590,

A - Anexo Técnico,

Delegación Miguel Hidalgo.

1 de 60



Delegación Miguel Hidalgo.

Y C n EDITO p ú BQCO



Anexo

2. ESPECIFICACIONES DE LOS SERVICIOS SOLICITADOS.

El periodo de contratación de los servicios será de 45 meses. Los equipos de comunicaciones necesarios son Switches Core, Switches de Acceso, Switches para Centro de Datos, Puntos de Acceso Inalámbricos, Controladora Inalámbrica, de acuerdo a lo descrito más adelante.

2.1 Suministro de Infraestructura.

- El Licitante acordará con SHF el plan de Suministro de la Infraestructura, estableciendo los tiempos y horarios de entrega. Este plan se detallará en la Fase de Planeación.
- El Licitante tendrá un plazo máximo de un mes a partir de la fecha de del fallo, como plazo para ejecutar el suministro al 100% de la infraestructura en las instalaciones de SHE
- El plan de Suministro de la Infraestructura deberá de sujetarse a las siguientes actividades:

A - Anexo Técnico,

- Entrega de la infraestructura en sitio: El Licitante entregará a SHF la infraestructura en las instalaciones de SHF, la cual deberá cumplir con la totalidad de las especificaciones solicitadas en el presente documento. El Licitante deberá de obtener la firma de conformidad del personal asignado por SHF, que valide el cumplimiento de las características solicitadas. Las características técnicas de la infraestructura están detalladas en el punto 3.
- Desempaque de Infraestructura: El Licitante deberá extraer de su empaque la infraestructura que entregará en las instalaciones de SHF para verificar y registrar números de serie de cada uno de los elementos.

Ante la falta de alguno de los elementos solicitados, se considera no aceptable o incompleta la instalación, por lo que no se realizarán los pagos correspondientes a la fase de operación hasta por un máximo de 60 días naturales, después de lo cual se procederá a la rescisión del contrato.

2.2 Transferencia de conocimientos.

Durante la fase de planeación, configuración e instalación, se deberá realizar transferencia de conocimientos al personal que SHF designe, respecto a cada una de las soluciones requeridas, sin costo adicional para SHF.

2 de 60



CREO ITO PÚBLICO



Anexo

2.3 Atención e Incidentes y Soporte Técnico.

3 de 60

A - Anexo Técnico,

Se requiere que el Licitante proporcione los medios de comunicación necesarios (teléfono local, celular, correo electrónico, mensajería instantánea), para establecer canales confiables de soporte técnico e interacción con el personal de SHF asignado para ello, para la resolución de incidencias de los servicios solicitados.

El Licitante deberá proporcionar el servicio de Mesa de Ayuda, el cual deberá tener un esquema 7*24*365. El servicio podrá ser prestado vía telefónica o en sitio, de acuerdo a la magnitud del evento.

El servicio de soporte técnico incluye el apoyo a los ingenieros de SHF para:

- Aclaración de dudas técnicas
- Atención de incidentes suscitados en la operación (mantenimiento correctivo)
- Configuración de los equipos o apoyo en la habilitación de nuevas funcionalidades

El Licitante deberá proporcionar un número telefónico y dirección de correo electrónico de la mesa de ayuda, con el objeto de brindar tanto soporte técnico como levantamiento de los reportes de servicio.

Por cada servicio efectuado, la empresa entregará a SHF un reporte en donde se anotará el número de control asignado y la información necesaria para llevar un adecuado manejo histórico de los servicios atendidos durante la vigencia del contrato; éste reporte será firmado de conformidad por el personal que SHF designe, una vez que el servicio sea completado.

El reporte de servicio deberá ser completado de la siguiente manera:

- Número e reporte
- Nombre de la Persona responsable por parte de SHF ■ Teléfono
- Marca del equipo atendido
- Número de serie del equipo atendido
- Clasificación del reporte: servicio, incidente
- Descripción de la falla reportada por SHF o del servicio requerido por SHF
- Nombre de la persona que levanta el reporte por parte de la empresa

A - Anexo Técnico,

- Diagnóstico de incidente (si aplica)
- Descripción y documentación de la solución
- Nombre de la Persona que atiende el reporte por parte de la empresa
- Fecha y hora de levantamiento del reporte
- Fecha y hora de cierre del reporte

3 de 60



Diagnóstico de incidente (si aplica)

CRÉDITO PÚBLICO



Anexo

2.4 Mantenimientos.

- Se realizarán las tareas de mantenimiento preventivo y correctivo a la infraestructura de hardware y a las herramientas propias para la administración del servicio que se encuentre bajo contrato, para asegurar y cumplir con los niveles de servicio solicitados.
- Para mantenimientos preventivos se programarán en conjunto con SHF con al menos 5 días hábiles de anticipación. El mantenimiento correctivo deberá ser contemplado como parte del servicio durante el tiempo que dure el contrato.

2.1.4 Mantenimiento Preventivo

- Se proporcionará un servicio de mantenimiento preventivo a todos los elementos que formen parte de la red LAN, incluyendo el peinado de cables en los IDF's y en los switch Core cada 12 meses y se deberá realizar durante la vigencia del contrato en forma programada. .
- Se proporcionará un servicio de mantenimiento preventivo cada 6 meses a todos los puntos de acceso inalámbrico, donde se verificará que no existan pérdidas de

A - Anexo Técnico,

potencia y con lo cual garantizará el nivel de servicio y la calidad de entrega del mismo a los usuarios.

- Las fechas y horarios de ejecución de los servicios de mantenimiento preventivo serán establecidas de común acuerdo entre SHF y el Licitante Ganador, pudiendo ser modificadas por causas de fuerza mayor o por la operación de SHF que imposibilite al Licitante Ganador que se lleve a cabo el servicio.
- Las actividades del servicio de mantenimiento preventivo que el Licitante Ganador proponga, deberán contemplar como mínimo:

i. Chequeo del buen funcionamiento de los equipos ii. Limpieza interna de back planes (aspirado y sopleteado de polvo, chasis). iii. Limpieza de slots y conectores de tarjetas.

iv. Limpieza de gabinete, tarjetas, fuentes de poder y revisión de cables.

v. Peinado de cableado en los IDF's y Switch Core.

- El Licitante Ganador deberá mantener actualizada la plataforma de software descrito a la última versión disponible por el fabricante de los equipos durante la vigencia del contrato.
- En caso de falla de un equipo de los servicios administrados, el Licitante Ganador deberá garantizar la continuidad del Servicio proporcionando, instalando y configurando



Anexo A - Anexo Técnico.



un equipo de la misma marca, con características similares o superiores, bajo la supervisión y autorización de SHF.

3. REQUERIMIENTOS.

A continuación, se describe el detalle de las necesidades que deben satisfacerlos servicios solicitados.

El proveedor deberá presentar una propuesta técnica, describiendo la forma en cómo se atienden los requerimientos solicitados, así como los demás términos y condiciones contenidos dentro de este documento. Para ello se deberá apoyar en manuales, hojas técnicas o publicaciones en internet por parte de los fabricantes. Para garantizar el correcto funcionamiento e integración de los componentes, así como la compatibilidad de los mismos, la solución de red alámbrica, red inalámbrica y de control de acceso a la red deberá ser del mismo fabricante.

3.1 Switch de Agregación.

3.1.1 Características Generales

- Switch apilable con desempeño mínimo de 2.1 Tbps y 1600 Mpps con arquitectura no bloqueable, aun cuando todas las interfaces estén transfiriendo paquetes a su máxima velocidad.
- El equipo deberá tener la capacidad de soportar al menos la siguiente densidad de puertos:
 - 0 48 puertos SFP+
 - 0 6 puertos QSFP28

0 1 puerto serial DB9. USB 0 mini-USB.

Anexo A - Anexo Técnico%

0 1 puerto 10/100/1000 BASE-T para Administración Fuera de Banda 0 1 puerto USB para transferencia de archivos .

- El equipo deberá soportar el siguiente tipo de interfaces:
 - Gigabit Ethernet•. SX, LX, 1000BASE-T en formato SFP
 - 10 Gigabit Ethernet: SR, LR, LRM, ER, y ZR en formato SFP+, así como solución de cables de cobre preensamblados en cobre o Twinax
 - 40 Gigabit Ethernet: SR4, LR4 y solución de cables de cobre preensamblados o Twinax
 - 100 Gigabit Ethernet: SR4, CWDM y solución de cables de cobre preensamblados o Twinax
 - Los puertos de 100 GbE o QSFP28 deberán tener la capacidad de dividirse ya sea en 4 puertos de 25 GbE o en 4 de 10 GbE, por medio de conectores especiales para este propósito y poder tener más densidad de puertos si es necesario

5 de 60



o Twinax
HACIENDA
 SECRETARÍA DE HACIENDA Y CRÉDITO PÚBLICO



**SOCIEDAD
 HIPOTECARIA
 FEDERAL**

especiales para este propósito y poder tener más densidad de puertos si es necesario

- El equipo debe soportar fuentes redundantes internas y hot-swap de AC y DC. ■ El equipo deberá soportar al menos un par de ventiladores que sean hot-swap
- Se requiere que la entrada del conector de la fuente de energía sean tipo C 14. ■ El equipo deberá estar diseñado para una altura no mayor a una unidad de rack (1 RU)
- Soportar al menos 90,000 direcciones MAC
- Soportar al menos 4094 VLANs
- Soporte de Jumbo Frames 9216 Bytes
- El equipo debe ser capaz de soportar apilamiento con un ancho de banda de al menos 600 Gbps por unidad o bien un agregado de al menos 5.4 Tbps ■ El equipo deberá tener capacidad de apilamiento de un mínimo de 9 equipos formando un

Soporte de

Anexo A - Anexo Técnicos

solo switch lógico, que soporte la inserción o retiro de cualquier switch del arreglo en caliente sin afectar la operación del resto de los miembros de

- El equipo deberá soportar apilamiento a larga distancia al menos hasta un máximo de 1 km, debido a la distribución de los IDFs que se prevé en un mediano plazo. • El equipo deberá soportar la funcionalidad MDI/MDIX
- Deberá tener la capacidad de soportar LAGs distribuidos a lo largo de un stack, es decir, que los puertos que lo formen puedan ser miembros de diferentes unidades, proporcionando redundancia y alta disponibilidad, de tal forma que si un miembro del stack es retirado el enlace se mantenga por el resto de los miembros que lo conforman
- El equipo deberá de soportar una funcionalidad que cuando esté trabajando en modo de stack, el firmware pueda ser actualizado sin la necesidad de perder los servicios en su totalidad sin causar fuertes afectaciones.

3.1.2 Funcionalidades de Capa 2, Switching

- El equipo deberá soportar al menos las siguientes funcionalidades y especificaciones:
 - Soporte de IEEE 802.1B STP
 - Soporte de IEEE 802.1w RSTP
 - Soporte de IEEE 802.1s MSTP
 - Soporte de PVST+, Per VLAN STP
 - Deberá soportar al menos 250 instancias de STP.
 - Soporte de IEEE 802.3ad LACP u 802.1 AX, con la capacidad de al menos 128 grupos de agregación y 8 puertos por cada grupo o LAG, no se aceptan protocolos propietarios.
 - Soporte de IEEE 802.1AB – LLDP Link Layer Discovery Protocol

6 de 60



RSTP

W



Soporte de

Anexo A - Anexo Técnico%

púaL'CO

- Soporte de LLDP-MED
- Soporte de protocolo de descubrimiento de dispositivos (Discovery Protocol) alternativo a LLDP
- Soporte de Remote Fault Notification
- Deberá soportar un protocolo o mecanismo cuya funcionalidad sea la de evitar loops basado en anillos o similar, alternativo a cualquiera de las modalidades de STP (RSTP o MSTP), esto con la finalidad de brindar un tiempo de convergencia menor a los antes descritos.
- Soportar una modalidad o mecanismo en la cual, dos switches puedan comportarse y verse como uno solo lógico, de tal forma que puedan tener conexiones a un mismo equipo o dispositivo de red en forma de un LAG distribuido, generando un esquema de redundancia.
- Soporte de PIM-SM v2 Snooping
- Soporte de GVRP (Generic VLAN Registration Protocol) o Multicast VLAN Registration (MVR)
- Soporte de IEEE 802.1Q VLAN Tagging
- Soporte de VLANs basadas por Puerto y Privadas ■ Soporte de Q-in-Q o vMANs.
- Capacidad de generar sesiones de espejeo de tráfico, desde un puerto o VLAN de origen hacia un puerto de destino, para propósitos de monitoreo e inspección de tráfico, con capacidad de filtrar el tráfico de monitoreo por ACLs o algún otro mecanismo. Dicha funcionalidad también deberá de estar disponible para hacer el monitoreo del tráfico de un equipo remoto o VLAN remota.
- Soporte de IGMP Snooping v1/v2 o Soporte de IGMP v2/v3 Fast Leave
- Soporte de MLD Snooping v1/v2
- Soporte de Root Guard o similar
- Soporte de BPDU Guard o Protection
- Soporte de UDLD
- Soporte de Cisco Discovery Protocol (CDP)
- Soporte del estándar IEEE 802.1B con la finalidad de soportar la extensión de equipos a lo largo de un campus y estos puedan gestionarse como una sola entidad.

Anexo A - Anexo Técnicos

3.1.3 Funcionalidades de Clasificación de Tráfico, Calidad de Servicio y Administración de Tráfico

- Contar con al menos 8 colas de prioridad (queues) y soportar los siguientes algoritmos de encolamiento: WRR (Weighted Round Robin), SP (Strick Priority), o una combinación de ambos.
- Soporte de IEEE 802.1p

7 de 60



Soporte de

Anexo A - Anexo Técnicos



- Soporte de DiffServ

- Soportar filtros o algún mecanismo de políticas para la clasificación de tráfico y

- marcado de los siguientes parámetros:

- 0 ToS/DSCP 0 802.1p o Mapeo de Direcciones MAC a colas de prioridad

- Soporte de rate-limit line-rate basado en hardware

- Soportar aplicación de filtros o políticas para definir rate limit tanto fijo como flexible (adaptado)

- Deberá soportar algún mecanismo que permita la contabilidad de bytes y paquetes que hagan correspondencia al tráfico clasificado por los filtros o políticas empleadas..

- Soporte de rate shaping

- Soporte de algún mecanismo que permita el control y limitación cuando se alcanzan

- altas tasas de tráfico de unicast, broadcast y multicast

- Soporte de algún mecanismo que pueda limitar el tráfico excesivo o innecesario al

- CPU del equipo como medida de protección, tales como ARP broadcast, TTL, MTU, entre otros.

- Soporte de la especificación RFC 2698 A Two Rate, Three Color



3.1.4 Funcionalidades de Capa 3

Ruteo estático IPv4 e IPv6

Soporte e inclusión de licencias para el soporte de IPv6, en caso de que el equipo a ofertar lo requiera.

Deberá soportar al menos 120,000 rutas en hardware

Soporte de ECMP

Soporte de VRRP para IPv4 e IPv6 con licenciamiento adicional

Soporte de OSPFv2/v3 con licenciamiento adicional

Soporte de

Anexo A - Anexo Técnico.

Soporte de RIPv1 y RIPv2

Soporte

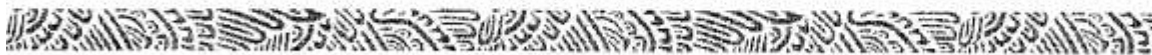
de

RIPng

- Soporte de BOOTP/DHCP relay y DHCP server
- Soporte de PIM-SM, PIM-SSM y PIM-DM con licenciamiento adicional
- Soporte de Policy Based Routing con licenciamiento adicional
- Soporte de BGP4 y BGP4+ con licenciamiento adicional
- Soporte de VRF en IPv4 e IPv6 con licenciamiento adicional
- Soporte de VRRP en IPv4 e IPv6
- Soportar al menos 100 instancias de VRF con licenciamiento adicional
- Soporte de GRE con licenciamiento adicional
- Soporte de las siguientes especificaciones para IPv6:
- Soporte de SNMPv3 sobre IPv6



8 de 60



server



- RFC 2460 — Internet Protocol, Version 6 (IPv6) Specification
- RFC 2464 — Transmission of IPv6 Packets over Ethernet Networks
- RFC 3513 — Internet Protocol Version 6 (IPv6) Addressing Architecture
- RFC 4862 — IPv6 Stateless Address Auto Configuration

3.1.5 Funciones de Seguridad

Soportar e incluir las siguientes funcionalidades:

El equipo deberá contar con algún mecanismo de protección contra ataques DOS

Soporte de ACLs en Ipv6

Soporte de ACLs estándar y extendidas

Soporte de

Anexo A - Anexo Técnicos

Deberá de soportar al menos 6,000 reglas de listas de control de acceso para garantizar la seguridad de la red.

Poseer un mecanismo que sea capaz de enviar mensajes o logs sobre el tráfico que es negado y permitido por una ACL

El equipo debe soportar múltiples métodos de autenticación: 802. IX, MAC y Web Autenticación de múltiples usuarios por 802. IX en el mismo puerto.

- Soporte de un mecanismo doble de autenticación sobre el mismo puerto basado en 802. IX y MAC, permitiendo que un dispositivo sea validado por el mecanismo de autenticación que soporte.
- Deberá soportar la asignación de un perfil de políticas o filtro de ACL cuando un usuario sea autenticado mediante 802. IX.
- Deberá soportar la asignación de un perfil de políticas o filtro de ACL cuando un usuario sea autenticado mediante su dirección MAC.
- Deberá soportar una funcionalidad la cual sea capaz de mitigar o bloquear mensajes de DHCP de equipos que intentan anunciarse como servidores inválidos o maliciosos.
- Soportar una funcionalidad que pueda limitar el número de direcciones MAC permitidas por puerto, o bien definir una determinada lista de direcciones MAC permitidas, y en caso de que se registre alguna violación o evento, se deberá desencadenar una acción tal como enviar un mensaje vía Syslog, trap SNMP e inclusive hasta llegar a deshabilitar el puerto en donde se presente el evento.
- Soporte de RADIUS, TACACS/TACACS+ con autenticación, autorización y contabilidad (AAA)
- Deberá soportar la funcionalidad de transparencia ante el paso de paquetes EAP.
- Soporte de SSL.
- Soporte de MAC Accounting

AAA para control y ejecución de comandos a nivel consola definir el formato de una dirección MAC que se envía a un

- Soporte de
- Capacidad para definir el formato de una dirección MAC que se envía a un servidor RADIUS.
- Soporte de RADIUS sobre TLS
- Soporte de AES con SSHv2 y SNMPv3



Anexo A - Anexo Técnico.



-
-
-
-
-
-

- Soportar los siguientes mecanismos o configuración de parámetros sobre sesiones de SSH:

- El valor de timeout
- Valor del puerto sobre el que se reciben conexiones
- Número de reintentos permitidos
- Tiempo máximo de uso de una sesión sin que la misma tenga actividad alguna u ociosa.
- Soportar los siguientes filtros de seguridad o criterios para las conexiones de usuarios que administren el equipo al menos para los accesos vía Telnet, Web y SNMP:
- Por dirección IP fuente
- Por VLAN
- Por listas de control de acceso .
- Soporte de MACsec con codificación en 128/256 bit
- Soporte de las siguientes especificaciones:

RFC 2866 - RADIOS Accounting

RFC 2865 -RADIUS Authentication

RFC 2868 - RADIUS Attributes for Tunnel Protocol Support

RFC 2869 - RADIUS Extensions

RFC 4432 - RSA Key Exchange for the Secure Shell (SSH) Transport Layer Protocol

RFC 2560 -X. 509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP

RFC 5280 — Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

Soporte de

Anexo A - Anexo Técnicos

RFC 6668 — SHA-2 Data Integrity Verification for the Secure Shell (SSH) Transport Layer Protocol

RFC 6614 - Transport Layer Security (TLS) Encryption for RADIOS

3.1.6 Funcionalidades de Administración

- ~~Soportar e incluir las siguientes~~ Soportar e incluir las siguientes funcionalidades:
- Administración vía línea de comandos
- Soporte de al menos 3 niveles de tipo de cuenta de usuario local administrador.
- Soporte de al menos 15 cuentas locales de usuario administrador.
- Las cuentas locales de administrador deberán tener las siguientes funcionalidades de seguridad o mecanismos soportados:
 - Una cuenta deberá bloquearse al menos después de 3 intentos fallidos, y podrá ser configurado para que este valor pueda ser diferente.
 - La contraseña de las cuentas deberá tener la capacidad de observar los siguientes lineamientos: Al menos 8 caracteres, empleo de combinaciones

10 de 60



funcionalidades:

Anexo A - Anexo Técnico.



-
-
- de caracteres alfanuméricos, así como especiales, uso de letras minúsculas y mayúsculas.
- o Poder validar que cuando se tenga que renovar la contraseña de una cuenta local de administración, el sistema sea capaz de evitar que emplee alguna reciente, dicho parámetro o histórico de contraseñas podrá ser configurado.
- Soporte de autoconfiguración o aprovisionamiento automático, es decir, deberá tener la funcionalidad de poder recibir mediante un proceso automático una IP de gestión y una configuración base de algún servidor TFTP y/o DHCP por ejemplo. Administración vía Telnet, SSH, SNMP.
- Soporte de sFlow o NetFlow, cualquiera de los dos anteriores deberá soportarse para IPv4 e IPv6 Soporte de TFTP
- Soporte de SCP o SFTP
- Soporte de Syslog para envío de al menos a 4 servidores
- El equipo deberá contar con un buffer local para almacenamiento de logs de al menos 2000 líneas.
- El equipo deberá tener la capacidad de enviar logs cuando un usuario administrador ingresa o deja la sesión de este registrando al menos la siguiente información:
 - o Nombre del usuario o Fecha y hora o
 - Si el usuario ingresó o dejó la sesión
- Soportar algún mecanismo que permita la creación y ejecución de tareas que incluyan un conjunto de comandos que puedan ser ejecutados de forma calendarizada, con la finalidad de ahorrar tiempo a los usuarios administradores en la ejecución de rutinas. Esta funcionalidad debe ser nativa al sistema operativo del equipo y no deberá ser provista por alguna herramienta externa.
- Deberá soportar la funcionalidad de reportar el estatus del cable conectado a los puertos del switch, reportando parámetros del cableado y longitud de este.
- Soporte de SNMPv1/v2/v3
- Soporte de RMON
- Soporte de gestión vía HTTP y HTTPS
- Soporte de las siguientes especificaciones:

Anexo A - Anexo Técnico.

- RFC 1901 — Introduction to Community-based SNMPv2
- ○ RFC 1905 - Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2)
- RFC 2576 Coexistence between SNMP Version 1, Version 2 and Version 3 of the Internet standard Network Management Framework
- ○ RFC 1155 Structure of Management Information (SMIv1)
- RFC 5905 – Network Time Protocol v4

11 de 60



A
CR EDITO PÚBLICO



3.1.7 Funcionalidades Especiales

- Funcionalidad para configurar un modelo de Redes Definidas por Software (SDN) mediante la especificación de estándar abierto OpenFlow 1.3, con el cual desde un Sistema Controlador se manipulen los flujos de datos para que de forma dinámica se configuren las tablas de flujos, esto con el fin de ser implementados en un futuro sin necesidad de cambiar el equipo.
- Soporte dual o híbrido de poder trabajar en un mismo puerto físico el control de datos vía flujos por SDN y al mismo tiempo reenvío de tráfico convencional en capa 2 y capa 3.
- El equipo deberá de soportar mecanismos para (a automatización de tareas o procesos para su integración con herramientas de uso libre tales como Puppet, Ansible o similares.

3.1.8 Especificaciones a cumplir y Condiciones de Operación

Rango de Temperatura de Operación: 0 °C a 45 °C

Humedad en condiciones operativas: 10 — 90 % Humedad relativa no condensada

Altura en condiciones operativas: 0 — 2800 m

Tener una disipación máxima de 1700 BTU/hr

Anexo A - Anexo Técnico.

Tener un MTBF (Mean Time Between Failure) de al menos 250,000 horas

UL 60950-1

FCC Class A (Part 15).

EN 60825-1 (Lasers Safety)

EN 55022 Class A.

EN 61000-3-2 (Harmonics)

EN 61000-3-3 (Flicker)

CISPR 22

IEC 60950-1 EN

61000-4-5 vcc1

Class A RoHS-

compliant

2011/65/EU

2012/19/EU

- 94/62/EC
- 2006/66/EC
- 1907/2006



12 de 60



94/62/EC

2006/66/EC

1907/2006



OE

CRÉDITO

Anexo A - Anexo Técnico.

3.2 Switch Multigigabit - Centro de Datos

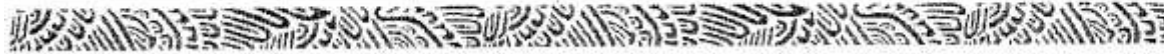
3.2.1 Características Generales

- Switch apilable con desempeño mínimo de 888 Gbps y 660 Mpps con arquitectura no bloqueable, aun cuando todas las interfaces estén transfiriendo paquetes a su máxima velocidad.
- El equipo deberá tener la capacidad de soportar al menos la siguiente densidad de puertos:
 - 0 24 puertos 10/100/1000 PoE+
 - 0 24 puertos 1/2.5/10 GbE PoE+/POH
 - 0 2 puertos QSFP+ 0 2 puertos SFP+ 0 1 puerto QSFP28
 - 0 1 puerto serial DB9. USB 0 mini-USB.
- 0 1 puerto 10/100/1000 BASE-T para Administración Fuera de Banda 0 1 puerto USB para transferencia de archivos
- El equipo deberá soportar el siguiente tipo de interfaces:
 - 0 Gigabit Ethernet: SX, LX, IOOBASE-T en formato SFP
 - 0 10 Gigabit Ethernet: SR, LR, LRM, ER, y ZR en formato SFP+, así como solución de cables de cobre preensamblados en cobre o Twinax.
 - 0 40 Gigabit Ethernet: SR4, LR4 y solución de cables de cobre preensamblados o Twinax
 - 0 100 Gigabit Ethernet: SR4, LR4 y solución de cables de cobre preensamblados o Twinax
- El equipo debe soportar fuentes redundantes y hot-swap de AC
- El equipo deberá soportar al menos un par de ventiladores que sean hot-swap Se requiere que la entrada del conector de la fuente de energía sean tipo C14.
- Soporte de los estándares IEEE 802.3af I at así como POH o IEEE 802.3bt El equipo deberá de poseer la capacidad de soportar al menos 1000 W para el aprovisionamiento total de POE.
El equipo deberá estar diseñado para una altura no mayor a una unidad de rack (1 RU)
Soportar al menos 70,000 direcciones MAC

Anexo A - Anexo Técnico.

- Soportar al menos 4094 VLANs
- Soporte de Jumbo Frames 9216 Bytes
- El equipo debe ser capaz de soportar apilamiento con un ancho de banda de al menos 160 Gbps por unidad o bien un agregado de al menos 1.4 Tbps Gbps
- El equipo deberá tener capacidad de apilamiento de un mínimo de 9 equipos formando un solo switch lógico, que soporte la inserción o retiro de cualquier switch del arreglo en caliente sin afectar la operación del resto de los miembros de la pila.

13 de 60



Soportar al menos 4094 VLANs

Anexo A - Anexo Técnico%

**HACIENDA**
SECRETARÍA DE HACIENDA Y CRÉDITO PÚBLICO

- El equipo deberá soportar apilamiento a larga distancia al menos hasta un máximo de 1 km, debido a la distribución de los IDFs que se prevé en un mediano plazo. ● El equipo deberá soportar la funcionalidad MDI/MDIX
- Deberá tener la capacidad de soportar LAGs distribuidos a lo largo de un stack, es decir, que los puertos que lo formen puedan ser miembros de diferentes unidades, proporcionando redundancia y alta disponibilidad, de tal forma que si un miembro del stack es retirado el enlace se mantenga por el resto de los miembros que lo conforman
- El equipo deberá de soportar una funcionalidad que cuando esté trabajando en modo de stack, el firmware pueda ser actualizado sin la -necesidad de perder los servicios en su totalidad sin causar fuertes afectaciones.

3.2.2 Funcionalidades de Capa 2, Switching

- El equipo deberá soportar al menos las siguientes funcionalidades y especificaciones:
- Soporte de IEEE 802. ID STP ● Soporte de IEEE 802. lw RSTP
- Soporte de IEEE 802. Is MSTP
- Soporte de PVST+, Per VLAN STP
- Deberá soportar al menos 254 instancias de STP.
- Soporte de IEEE 802.3ad LACP u 802.1 AX, con la capacidad de al menos 128 grupos de agregación y 8 puertos por cada grupo o LAG, no se aceptan protocolos propietarios.
- Soporte de IEEE 802. IAB - LLDP Link Layer Discovery Protocol
- Soporte de LLDP-MED
- Soporte de protocolo de descubrimiento de dispositivos (Discovery Protocol) alternativo a LLDP
- Soporte de Remote Fault Notification
- Deberá soportar un protocolo o mecanismo cuya funcionalidad sea la de evitar loops basado en anillos o similar, alternativo a cualquiera de las modalidades de STP (RSTP o MSTP), esto con la finalidad de brindar un tiempo de convergencia menor a los antes descritos. ● Soporte de PIM-SM v2 Snooping

Anexo A - Anexo Técnico.

- Soporte de GVRP (Generic VLAN Registration Protocol) o Multicast VLAN Registration (MVR)
- Soporte de IEEE 802.1Q VLAN Tagging
- Soporte de VLANs basadas por Puerto, MAC y Privadas
- Soporte de Q-in-Q o vMANs.
- Capacidad de generar sesiones de espejo de tráfico, desde un puerto o VLAN de origen hacia un puerto de destino, para propósitos de monitoreo e inspección de tráfico.

14 de 60



Soporte de GVRP (Generic
Registration (MVR)
Soporte de IEEE
Soporte de VLANs basadas por
Soporte de Q-in-Q o vMANs.
Capacidad de generar sesiones de
origen hacia un puerto de

A
PÚBLICO

SIF

DE CRÉDITO

tráfico, con capacidad de filtrar el tráfico de monitoreo por ACLs o algún otro mecanismo. Dicha funcionalidad también deberá de estar disponible para hacer el monitoreo del tráfico de un equipo remoto o VLAN remota. • Soporte de IGMP Snooping vllv2/v3

- Soporte de IGMP v2/v3 Fast Leave
- Soporte de MLD Snooping vl/v2
- Soporte de Root Guard o similar
- Soporte de BPDU Guard o Protection
- Soporte de UDLD
- Soporte de Cisco Discovery Protocol (CDP)
- Soporte del estándar IEEE 802.1BR con la finalidad de soportar la extensión de equipos a lo largo de un campus y estos puedan gestionarse como una sola entidad.

23 de 60

Anexo A - Anexo Técnico%

3-2.3 Funcionalidades de Clasificación de Tráfico, Calidad de Servicio y Administración de Tráfico

- Contar con al menos 8 colas de prioridad (queues) y soportar los siguientes algoritmos de encolamiento: WRR (Weighted Round Robin), SP (Strick Priority), o una combinación de ambos. • Soporte de IEEE 802.1p
- Soporte de DiffServ
- Soportar filtros o algún mecanismo de políticas para la clasificación de tráfico y marcado de los siguientes parámetros:

0 ToS/DSCP

- Mapeo de Direcciones MAC a colas de prioridad
- Soporte de rate-limit line-rate basado en hardware
- Soportar aplicación de filtros o políticas para definir rate limit tanto fijo como flexible (adaptado)
- Deberá soportar algún mecanismo que permita la contabilidad de bytes y paquetes que hagan correspondencia al tráfico clasificado por los filtros o políticas empleadas.
- Soporte de rate shaping
 - Soporte de algún mecanismo que permita el control y limitación cuando se alcanzan altas tasas de tráfico de unicast, broadcast y multicast.
 - Soporte de algún mecanismo que pueda limitar el tráfico excesivo o innecesario al CPU del equipo como medida de protección, tales como ARP broadcast, TL, MTU, entre otros.
- Soporte de la especificación RFC 2698 A Two Rate, Three Color

15 de 60



Soporte de

NDA
SECRETARÍA DE HACIENDA Y CRÉDITO PÚBLICO



Anexo A - Anexo Técnico.

3.2.4 Funcionalidades de Capa 3

- Ruteo estático IPv4 e IPv6
- Soporte e inclusión de licencias para el soporte de IPv6, en caso de que el equipo a ofertar lo requiera.
- Deberá soportar al menos 120,000 rutas en hardware
- Soporte de ECMP
- Soporte de VRRP para IPv4 e IPv6 con licencia adicional
- Soporte de OSPFv2/v3 con licencia adicional
- Soporte de RIPv1 y RIPv2
- Soporte de RIPv6
- Soporte de BOOTP/DHCP relay y DHCP server
- Soporte de PIM-SM, PIM-SSM y PIM-DM con licencia adicional
- Soporte de Policy Based Routing con licencia adicional
- Soporte de BGP4 y BGP4+ con licencia adicional
- Soporte de VRF en IPv4 e IPv6 con licencia adicional
- Soporte de VRRP en IPv4 e IPv6 con licencia adicional
- Soporte de GRE con licencia adicional
- Soporte de las siguientes especificaciones para IPv6 o Soporte de SNMPv3 sobre IPv6 o RFC 2460 — Internet Protocol, Version 6 (IPv6) Specification o RFC 2464 — Transmission of IPv6 Packets over Ethernet Networks o RFC 3513 — Internet Protocol Version 6 (IPv6) Addressing Architecture o RFC 4862 — IPv6 Stateless Address Auto Configuration

3.2.5 Funciones de Seguridad

- Soportar e incluir las siguientes funcionalidades:
- El equipo deberá contar con algún mecanismo de protección contra ataques DOS
- Soporte de ACLs en IPv6
- Soporte de ACLs estándar y extendidas
- Deberá de soportar al menos 6,000 reglas de listas de control de acceso para garantizar la seguridad de la red.

Anexo A - Anexo Técnico%

- Poseer un mecanismo que sea capaz de enviar mensajes o logs sobre el tráfico que
- El equipo debe soportar múltiples métodos de autenticación: 802.1X, MAC y Web
- Autenticación de múltiples usuarios por 802.1X en el mismo puerto.
- Soporte de un mecanismo doble de autenticación sobre el mismo puerto basado en 802.1X y MAC, permitiendo que un dispositivo sea validado por el mecanismo de autenticación que soporte.
- Deberá soportar la asignación de un perfil de políticas o filtro de ACL cuando un usuario sea autenticado mediante 802.1X.



16 de 60



es negado y permitido por una ACL El equipo debe soportar múltiples Autenticación de múltiples usuarios por Soporte de un mecanismo doble en 802. IX y MAC, de autenticación que soporte. Deberá soportar la asignación de usuario sea autenticado mediante

Anexo A - Anexo Técnico.

SECRETARÍA PÚBLICA



- Deberá soportar la asignación de un perfil de políticas o filtro de ACL cuando un usuario sea autenticado mediante su dirección MAC.
- Deberá soportar una funcionalidad la cual sea capaz de mitigar o bloquear mensajes de DHCP de equipos que intentan anunciarse como servidores inválidos o maliciosos.
- Soportar una funcionalidad que pueda limitar el número de direcciones MAC permitidas por puerto, o bien definir una determinada lista de direcciones MAC permitidas, y en caso de que se registre alguna violación o evento, se deberá desencadenar una acción tal como enviar un mensaje vía Syslog, trap SNMP e inclusive hasta llegar a deshabilitar el puerto en donde se presente el evento.
- Soporte de RADIUS, TACACS/TACACS+ con autenticación, autorización y contabilidad (AAA)
- Deberá soportar la funcionalidad de transparencia ante el paso de paquetes EAP..
- Soporte de SSL.
- Soporte de MAC Accounting
- Soporte de AAA para control y ejecución de comandos a nivel consola
- Capacidad para definir el formato de una dirección MAC que se envía a un servidor RADIUS.
- Soporte de RADIUS sobre TLS
- Soporte de AES con SSHV2 y SNMPv3
- Soportar los siguientes mecanismos o configuración de parámetros sobre sesiones de SSH:
 - o El valor de timeout o Valor del puerto sobre el que se reciben conexiones o Número de reintentos permitidos o Tiempo máximo de uso de una sesión sin que la misma tenga actividad alguna u ociosa.
- Soportar los siguientes filtros de seguridad o criterios para las conexiones de usuarios que administren el equipo al menos para los accesos vía Telnet, Web y SNMP:
 - o Por dirección IP fuente o Por VLAN

Anexo A - Anexo Técnico%

- o Por listas de control de acceso
- Soporte de la especificación IEEE 802.1AE (MACsec)
- Soporte de las siguientes especificaciones:
 - o RFC 2866 – RADIUS Accounting
 - o RFC 2865 – RADIUS Authentication
 - o RFC 2868 - RADIUS Attributes for Tunnel Protocol Support
 - o RFC 2869 - RADIUS Extensions
 - o RFC 4432 - RSA Key Exchange for the Secure Shell (SSH) Transport Layer Protocol

17 de 60



HACIENDA
SECRETARÍA DE HACIENDA Y CRÉDITO PÚBLICO



- o RFC 2560 - Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP
- o RFC 5280 — Internet (.509) Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
- o RFC 6668 — SHA-2 Data Integrity Verification for the Secure Shell (SSH) Transport Layer Protocol
- o FC 6614 — Transport Layer Security (TLS) Encryption for RADIUS

3.2.6 Funcionalidades de Administración

Soportar e incluir las siguientes funcionalidades:

Administración vía línea de comandos

Soporte de al menos 3 niveles de tipo de cuenta de usuario local administrador.

Soporte de al menos 5 cuentas locales de usuario administrador.

Las cuentas locales de administrador deberán tener las siguientes funcionalidades de seguridad o mecanismos soportados:

- o Una cuenta deberá bloquearse al menos después de 3 intentos fallidos, y podrá ser configurado para que este valor pueda ser diferente.
- o La contraseña de las cuentas deberá tener la capacidad de observar los siguientes lineamientos: Al menos 8 caracteres, empleo de combinaciones

Anexo A - Anexo Técnico-

de caracteres alfanuméricos, así como especiales, uso de letras minúsculas y mayúsculas.

- o Poder validar que cuando se tenga que renovar la contraseña de una cuenta local de administración, el sistema sea capaz de evitar que emplee alguna reciente, dicho parámetro o histórico de contraseñas podrá ser configurado.

Soporte de autoconfiguración o aprovisionamiento automático, es decir, deberá tener la funcionalidad de poder recibir mediante un proceso automático una IP de gestión y una configuración base de algún servidor TFTP y/o DHCP por ejemplo.

- Administración vía Telnet, SSH, SNMP.
- Soporte de sFlow o NetFlow, cualquiera de los dos anteriores deberá soportarse para IPv4 e IPv6
- Soporte de TFTP
- Soporte de SCP o SFTP
- Soporte de Syslog para envío de al menos a 4 servidores
- El equipo deberá contar con un buffer local para almacenamiento de logs de al menos 2000 líneas.
- El equipo deberá tener la capacidad de enviar logs cuando un usuario administrador ingresa o deja la sesión de este registrando al menos la siguiente información:

- o Nombre del usuario
- o Fecha y hora
- o Si el usuario ingresó o dejó la sesión

18 de 60



Administración vía Telnet, SSH, SNMP.
Soporte de sFlow o NetFlow, para IPv4
e IPv6

PÚBLICO



Soportar algún mecanismo que permita la creación y ejecución de tareas que incluyan un conjunto de comandos que puedan ser ejecutados de forma calendarizada, con la finalidad de ahorrar tiempo a los usuarios administradores

Anexo A - Anexo Técnico%

en la ejecución de rutinas. Esta funcionalidad debe ser nativa al sistema operativo del equipo y no deberá ser provista por alguna herramienta externa.

- Deberá soportar la funcionalidad de reportar el estatus del cable conectado a los puertos del witch, reportando parámetros del cableado y longitud de este, Soporte de SNMPv1/v2/v3
- Soporte de RMON
- Soporte de gestión vía HTTP y HTTPS
- Soporte de la especificación IEEE 802.3ah
- Soporte de la funcionalidad EEE (Energy Efficient Ethernet) o similar.
- Soporte de las siguientes especificaciones:
 - 0 RFC 1901 — Introduction to Community-based SNMPv2 o RFC 1905 - Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2) o RFC 2576 Coexistence between SNMP Version 1, Version 2 and Version 3 of the Internet standard Network Management Framework o RFC 1155 Structure of Management Information (SMIv1) 0 RFC 5905 - Network Time Protocol v4

3.2.7 Funcionalidades Especiales

Funcionalidad para configurar un modelo de Redes Definidas por Software (SDN) mediante la especificación de estándar abierto OpenFlow 1.3, con el cual desde un Sistema Controlador se manipulen los flujos de datos para que de forma dinámica se configuren las tablas de flujos, esto con el fin de ser implementados en un futuro sin necesidad de cambiar el equipo.

- Soporte dual o híbrido de poder trabajar en un mismo puerto físico el control de datos vía flujos por SDN y al mismo tiempo reenvío de tráfico convencional en capa 2 y capa 3.
- El equipo deberá de soportar mecanismos para la automatización de tareas o procesos para su integración con herramientas de uso libre tales como Puppet, Ansible o similares.
-

3.2.8 Especificaciones a cumplir y Condiciones de Operación

- Rango de Temperatura de Operación: 0°C a 45°C
- Humedad en condiciones operativas: 10 – 90 % Humedad relativa no condensante
- El equipo no deberá de generar una disipación de calor mayor a 800 BTU/hr
- Altura en condiciones operativas: 0 – 2800 m



Anexo A - Anexo Técnico-



- Tener un MTBF (Mean Time Between Failure) de al menos 200,000 horas
- UL 60950-1
- FCC Class A (Part 15) EN
- 60825-1 (Lasers Safety)
- EN 55022 Class A
- EN 61000-3-2 (Harmonics)
- EN 61000-3-3 (Flicker)
- CISPR 22
- IEC 60950-1 EN
- 61000-4-5 vccI
- Class A RoHS-compliant
- 2011/65/EU
- 2012/19/EU
- 94/627EC
- 2006/66/EC
- 1907/2006

3.3 Switch Acceso 48 Puertos PoE

3.3.1 Características Generales

- Switch apilable con desempeño mínimo de 336 Gbps y 250 Mpps con arquitectura no bloqueable, aun cuando todas las interfaces estén transfiriendo paquetes a su máxima velocidad.
El equipo deberá tener la capacidad de soportar al menos la siguiente densidad de puertos:
 - 48 puertos 10/100/1000 BASE-T PoE+
 - 4 puertos SFP/SFP+

Anexo A - Anexo Técnico.

- 0 2 puertos QSFP+
- 0 1 puerto serial DB9. USB o mini-USB.
- 0 1 puerto 10/100/1000 BASE-T para Administración Fuera de Banda. 0 1 puerto USB para transferencia de archivos
- El equipo deberá soportar el siguiente tipo de interfaces:
 - 0 Gigabit Ethernet: SX, LX, BX, IOOBASE-T en formato SFP
 - 0 10 Gigabit Ethernet: SR, LR, LRM, ER, y ZR en formato SFP+, así *isí* como como solución de cables de cobre preensamblados en cobre o Twinax
 - *de cables de cobre* preensamblados o Twinax
- El equipo debe soportar fuentes redundantes y hot-swap de AC y DC.
- El equipo deberá soportar al menos un par de ventiladores que sean hot-swap

20 de 60



- 0 40 Gigabit Ethernet: SR4, LR4 y solución preensamblados o Twinax

El equipo debe soportar fuentes

El equipo deberá soportar

p üBLtcol



Se requiere que la entrada del conector de la fuente de energía sean tipo C14. Soporte de los estándares IEEE 802.3af 1 at Soporte de PoE* 0 IEEE 802.3bt El equipo deberá de poseer la capacidad de soportar al menos 1000 W para el aprovisionamiento total de POE.

El equipo deberá estar diseñado para una altura no mayor a una unidad de rack (1 RU)

Soportar al menos 30,000 direcciones MAC

Soportar al menos 4094 VLANs

Soporte de Jumbo Frames 9216 Bytes

Anexo A - Anexo Técnico-

El equipo debe ser capaz de soportar apilamiento con un ancho de banda de al menos 80 Gbps por unidad o bien un agregado de al menos 720 Gbps El equipo deberá tener capacidad de apilamiento de un mínimo de 9 equipos formando un solo switch lógico, que soporte la inserción o retiro de cualquier switch del arreglo en caliente sin afectar la operación del resto de los miembros de la pila. El equipo deberá soportar apilamiento a larga distancia al menos hasta un máximo de 1 km, debido a la distribución de los IDFs que se prevé en un mediano plazo.

El equipo deberá soportar la funcionalidad MDI/MDIX

Deberá tener la capacidad de soportar LAGs distribuidos a lo largo de un stack, es decir, que los puertos que lo formen puedan ser miembros de diferentes unidades, proporcionando redundancia y alta disponibilidad, de tal forma que si un miembro del stack es retirado el enlace se mantenga por el resto de los miembros que lo conforman

El equipo deberá de soportar una funcionalidad que cuando esté trabajando en modo de stack, el firmware pueda ser actualizado sin la necesidad de perder los servicios en su totalidad sin causar fuertes afectaciones.

3.3.2 Funcionalidades de Capa 2, Switching

- El equipo deberá soportar al menos las siguientes funcionalidades y especificaciones:
- Soporte de IEEE 802.1D STP
- Soporte de IEEE 802.1w RSTP
- Soporte de IEEE 802.1s MSTP
- Soporte de PVST+, Per VLAN STP
- Deberá soportar al menos 250 instancias de STP.
- Soporte de IEEE 802.3ad LACP u 802.1 AX, con la capacidad de al menos 128 grupos de agregación y 8 puertos por cada grupo o LAG, no se aceptan protocolos propietarios.
- Soporte de IEEE 802.1AB – LLDP Link Layer Discovery Protocol
- Soporte de LLDP-MED



Anexo A - Anexo Técnico.

- Soporte de protocolo de descubrimiento de dispositivos (Discovery Protocol) alternativo a LLDP
- Soporte de Remote Fault Notification
Deberá soportar un protocolo o mecanismo cuya funcionalidad sea la de evitar loops basado en anillos o similar, alternativo a cualquiera de las modalidades de STP (RSTP o MSTP), esto con la finalidad de brindar un tiempo de convergencia menor a los antes descritos. Soporte de PIM-SM v2 Snooping
- Soporte de GVRP (Generic VLAN Registration Protocol) o Multicast VLAN Registration (MVR)
- Soporte de IEEE 802. IQ VLAN Tagging
- Soporte de VLANs basadas por Puerto y Privadas Soporte de Q-in-Q o vMANs.
Capacidad de generar sesiones de espejeo de tráfico, desde un puerto o VLAN de origen hacia un puerto de destino, para propósitos de monitoreo e inspección de tráfico, con capacidad de filtrar el tráfico de monitoreo por ACLs o algún otro mecanismo. Dicha funcionalidad también deberá de estar disponible para hacer el monitoreo del tráfico de un equipo remoto o VLAN remota. Soporte de IGMP Snooping vllv21v3
- Soporte de IGMP v21v3 Fast Leave
- Soporte de MLD Snooping vllv2
- Soporte de Root Guard o similar
- Soporte de BPDU Guard o Protection
- Soporte de UDLD.
- Soporte de Cisco Discovery Protocol (CDP)
Soporte del estándar IEEE 802. IBR con la finalidad de soportar la extensión de equipos a lo largo de un campus y estos puedan gestionarse como una sola entidad.

3.3.3 Funcionalidades de Clasificación de Tráfico, Calidad de Servicio y Administración de Tráfico

- Contar con al menos 8 colas de prioridad (queues) y soportar los siguientes algoritmos de encolamiento: WRR (Weighted Round Robin), SP (Strick Priority), o una combinación de ambos. Soporte de IEEE 802. Ip Soporte de DiffServ
Soportar filtros o algún mecanismo de políticas para la clasificación de tráfico y marcado de los siguientes parámetros:

Anexo A - Anexo Técnico-

- ToS/DSCP
- 802.1p
- Mapeo de Direcciones MAC a colas de prioridad



22 de 60



A
PÚBLICO

SIF

y

Soporte de rate-limit line-rate basado en hardware

Soportar aplicación de filtros o políticas para definir rate limit tanto fijo como flexible (adaptado)

Deberá soportar algún mecanismo que permita la contabilidad de bytes y paquetes que hagan correspondencia al tráfico clasificado por los filtros o políticas empleadas.

Soporte de rate shaping

Soporte de algún mecanismo que permita el control y limitación cuando se alcanzan altas tasas de tráfico de unicast, broadcast y multicast

Soporte de algún mecanismo que pueda limitar el tráfico excesivo o innecesario al CPU del equipo como medida de protección, tales como ARP broadcast, TTL, MTU, entre otros.

Soporte de la especificación RFC 2698 A Two Rate, Three Color Soporte de PFC (Priority-based Flow Control)

Anexo A - Anexo Técnico.

3.3.4 Funcionalidades de Capa 3

- Ruteo estático IPv4 e IPv6
- Soporte e inclusión de licencias para el soporte de IPv6, en caso de que el equipo a ofertar lo requiera.
- Deberá soportar al menos 15,000 rutas en hardware
- Soporte de ECMP
- Soporte de VRRP para IPv4 e IPv6
- Soporte de OSPFv2/v3
- Soporte de RIPv1 y RIPV2
- Soporte de RIPng
- Soporte de BOOTP/DHCP relay y DHCP server
- Soporte de PIM-SM, PIM-SSM y PIM-DM
- Soporte de Policy Based Routing
- Soporte de BGP4 y BGP4 +
- Soporte de VRF en IPv4 e IPv6
- Soporte de VRRP en IPv4 e IPv6
- Soporte de las siguientes especificaciones para IPv6:
 - Soporte de SNMPv3 sobre IPv6
 - 0 RFC 2460 - Internet Protocol, Version 6 (IPv6) Specification o RFC 2464 —
 - Transmission of IPv6 Packets over Ethernet Networks o RFC 3513 —
 - Internet Protocol Version 6 (IPv6) Addressing Architecture o RFC 4862 —
 - IPv6 Stateless Address Auto Configuration

3.3.5 Funciones de Seguridad

- El equipo deberá contar con algún mecanismo de protección contra ataques DoS
- Soporte de ACLs en IPv6





Anexo A - Anexo Técnico.



SECRETARÍA DE

- Soporte de ACLs estándar y extendidas
- Deberá de soportar al menos 6,000 reglas de listas de control de acceso para garantizar la seguridad de la red.
- Poseer un mecanismo que sea capaz de enviar mensajes o logs sobre el tráfico que es negado y permitido por una ACL
- El equipo debe soportar múltiples métodos de autenticación: 802. IX, MAC y Web
- Autenticación de múltiples usuarios por 802. IX en el mismo puerto.
- Soporte de un mecanismo doble de autenticación sobre el mismo puerto basado en 802. IX y MAC, permitiendo que un dispositivo sea validado por el mecanismo de autenticación que soporte.
- Deberá soportar la asignación de un perfil de políticas o filtro de ACL cuando un usuario sea autenticado mediante 802. IX.
- Deberá soportar la asignación de un perfil de políticas o filtro de ACL cuando un usuario sea autenticado mediante su dirección MAC.
- Deberá soportar una funcionalidad la cual sea capaz de mitigar o bloquear mensajes de DHCP de equipos que intentan anunciarse como servidores inválidos o maliciosos.
- Soportar una funcionalidad que pueda limitar el número de direcciones MAC permitidas por puerto, o bien definir una determinada lista de direcciones MAC permitidas, y en caso de que se registre alguna violación o evento, se deberá desencadenar una acción tal como enviar un mensaje vía Syslog, trap SNMP e inclusive hasta llegar a deshabilitar el puerto en donde se presente el evento.
- Soporte de RADIUS, TACACS/TACACS+ con autenticación, autorización y contabilidad (AAA)
- Deberá soportar la funcionalidad de transparencia ante el paso de paquetes EAP.
- Soporte de SSL.
- Soporte de MAC Accounting

Anexo A - Anexo Técnico.

- Soporte de AAA para control y ejecución de comandos a nivel consola • Capacidad para definir el formato de una dirección MAC que se envía a un servidor RADIUS.
- Soporte de RADIUS sobre TLS
- Soporte de AES con SSHv2 y SNMPv3
- Soportar los siguientes mecanismos o configuración de parámetros sobre sesiones de SSH:
 - El valor de timeout o Valor del puerto sobre el que se reciben conexiones o Número de reintentos permitidos o Tiempo máximo de uso de una sesión sin que la misma tenga actividad alguna u ociosa.
- Soportar los siguientes filtros de seguridad o criterios para las conexiones de usuarios que administren el equipo al menos para los accesos vía Telnet, Web SNMP:



24 de 60

DE

Pú8Ltc0



- Por dirección IP fuente 0 Por VLAN o Por listas de control de acceso
- Soporte de la especificación IEEE 802. IAE (MACsec)
- Soporte de las siguientes especificaciones:
 - 0 RFC 2866 - RADIUS Accounting
 - 0 RFC 2865 - RADIUS Authentication
 - 0 RFC 2868 - RADIUS Atributes for Tunnél Protocol Support
 - 0 RFC 2869 - RADIUS Extensions
 - 0 RFC 4432 - RSA Key Exchange for the Secure Shell (SSH) Transport Layer Protocol
 - 0 RFC 2560 - X.509 Internet Public Key Infrastructure Online Certificate Status Protocol — OCSP



Anexo A - Anexo Técnico.

- RFC 5280 — Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
- RFC 6668 - SHA-2 Data Integrity Verification for the Secure Shell (SSH) Transport Layer Protocol
- RFC 6614 - Transport Layer Security (TLS) Encryption for RADIOS □ RFC 5996 - Internet Key Exchange Protocol Version 2 (IKEv2)
- RFC 4303 IP Encapsulating Security Payload (ESP)
- RFC 5903 Elliptic Curve Groups Modulo a Prime (ECP Groups) for IKE and IKEv2
- RFC 4754 IKEv2 Authentication Using the Elliptic Curve Digital Signature Algorithm (ECDSA)

3.3.6 Funcionalidades de Administración

- Soportar e incluir las siguientes funcionalidades:
- Administración vía línea de comandos
- Soporte de al menos 3 niveles de tipo de cuenta de usuario local administrador.
- Soporte de al menos 15 cuentas locales de usuario administrador.
- Las cuentas locales de administrador deberán tener las siguientes funcionalidades de seguridad o mecanismos soportados:
 - Una cuenta deberá bloquearse al menos después de 3 intentos fallidos, y podrá ser configurado para que este valor pueda ser diferente.
 - La contraseña de las cuentas deberá tener la capacidad de observar los siguientes lineamientos: Al menos 8 caracteres, empleo de combinaciones de caracteres alfanuméricos, así como especiales, uso de letras minúsculas y mayúsculas.

Anexo A - Anexo Técnico.

- o Poder validar que cuando se tenga que renovar la contraseña de una cuenta local de administración, el sistema sea capaz de evitar que emplee alguna reciente, dicho parámetro o histórico de contraseñas podrá ser configurado.

25 de 60



validar que cuando se tenga que
local de administración,
reciente, dicho parámetro o

público



- Soporte de autoconfiguración o aprovisionamiento automático, es decir, deberá tener la funcionalidad de poder recibir mediante un proceso automático una IP de gestión y una configuración base de algún servidor TFTP y/o DHCP por ejemplo. ● Administración vía Telnet, SSH, SNMP.
- Soporte de sFlow o NetFlow, cualquiera de los dos anteriores deberá soportarse para IPv4 e IPv6 ● Soporte de TFTP
- Soporte de SCP o SFTP
- Soporte de Syslog para envío de al menos a 4 servidores
- El equipo deberá contar con un buffer local para almacenamiento de logs de al menos 2000 líneas.
- El equipo deberá tener la capacidad de enviar logs cuando un usuario administrador ingresa o deja la sesión de este registrando al menos la siguiente información:
- Nombre del usuario o Fecha y hora o Si el usuario ingresó o dejó la sesión
- Soportar algún mecanismo que permita la creación y ejecución de tareas que incluyan un conjunto de comandos que puedan ser ejecutados de forma calendarizada, con la finalidad de ahorrar tiempo a los usuarios administradores en la ejecución de rutinas. Esta funcionalidad debe ser nativa al sistema operativo del equipo y no deberá ser provista por alguna herramienta externa.

Anexo A - Anexo Técnico.

- Deberá soportar la funcionalidad de reportar el estatus del cable conectado a los puertos del switch, reportando parámetros del cableado y longitud de este. • Soporte de SNMPv1/v2/v3
- Soporte de RMON
- Soporte de gestión vía HTTP y HTTPS
- Soporte de la especificación IEEE 802.3ah
- Soporte de la funcionalidad EEE (Energy Efficient Ethernet) o similar. • Soporte de las siguientes especificaciones:
- RFC 1901 — Introduction to Community-based SNMPv2 o RFC 1905 - Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2) o RFC 2576 Coexistence between SNMP Version 1, Version 2 and Version 3 of the Internet standard Network Management Framework
 - o RFC 1155 Structure of Management Information (SMIv1)
 - o RFC 5905 – Network Time Protocol v4

3.3.7 Funcionalidades Especiales

- Funcionalidad para configurar un modelo de Redes Definidas por Software (SDN) mediante la especificación de estándar abierto OpenFlow 1.3, con el cual desde el Sistema Controlador se manipulen los flujos de datos para que de forma dinámica

26 de 60



Management Framework o RFC 1155 Structure of Management o RFC 5905 - Network Time

Anexo A - Anexo Técnico.



se configuren las tablas de flujos, esto con el fin de ser implementados en un futuro sin necesidad de cambiar el equipo.

- Soporte dual o híbrido de poder trabajar en un mismo puerto físico el control de datos vía flujos por SDN y al mismo tiempo reenvío de tráfico convencional en capa 2 y capa 3.
- El equipo deberá de soportar mecanismos para la automatización de tareas o procesos para su integración con herramientas de uso libre tales como Puppet, Ansible o similares.

3.3.8 Especificaciones a cumplir y Condiciones de Operación

- Rango de Temperatura de Operación: 0 °C a 48 °C
 - Humedad en condiciones operativas: 10 90 % Humedad relativa no condensada
 - El equipo no deberá de generar una disipación de calor mayor a 400 BTU/hr
 - Altura en condiciones operativas: 0 — 2800 m
 - Tener un MTBF (Mean Time Between Failure) de al menos 400,000 horas
 - UL 60950-1
 - FCC Class A (Part 15)
 - EN 60825-1 (Lasers Safety)
-
- EN 55022 Class A

W

g



Anexo A - Anexo Técnico.

- EN 61000-3-2 (Harmonics)
- EN 61000-3-3 (Flicker)
- CISPR 22
- IEC 60950-1
- EN 61000-4-5 ■ vcl
- Class A
- RoHS-compliant
- 2011/65/EU
- 2012/19/EU
- 94/62/EC ■ 2006/66/EC
- 1907/2006



3.4 Controladora WiFi.

3.4.1 Características Generales

Controladora inalámbrica tipo appliance físico o virtual con alto nivel de desempeño para redes empresariales con capacidad de gestionar al menos hasta 800 Puntos de Acceso.

En el caso de proponer una solución basada en appliance físico, deberá de cumplir al menos con las siguientes características: 2 puertos 1000 BASE-T
1 puerto USB

1 puerto de consola RJ45, DB9 0 USB Alimentarse mediante conexión del tipo CA.
No deberá de ser mayor a 1 RU

Anexo A - Anexo Técnico.

Poseer LEDs indicadores, los cuales al menos puedan mostrar los estados de operación de este mediante diferentes colores o algún otro distintivo a nivel físico Capacidad de operar en el siguiente rango de temperaturas: 0^o C — 38^o C

- Capacidad de operar en el siguiente rango de humedad no condensada: 10 — 80% Deberá poseer un MTBF (Mean Time Between Failure) de al menos de 40,000 horas

-

3.4.2 Funcionalidades, Desempeño y Soporte de Especificaciones Inalámbricas

-

-

-

-

-

-

-

-

-

Deberá de tener la capacidad de soportar al menos hasta 800 Puntos de Acceso, o bien hasta 2400 en modalidad de redundancia y/o cluster

Deberá de soportar la menos hasta 20,000 dispositivos conectados en forma concurrente y al menos hasta 50,000 en modalidad de redundancia y/o cluster.

Soportar un esquema de alta disponibilidad activo-activo o cluster de al menos hasta 3 elementos, bajo un esquema N+1

La solución ofertada también deberá contar con la función de poder gestionar y monitorear los switches de la misma marca del fabricante, ya que ello permite la unificación de la administración de las plataformas.

-

-

-

-

Anexo A - Anexo Técnico.

- Soportar al menos las siguientes tareas de configuración base para los switches/routers;
- Actualización de firmware manual y programada sobre tanto en forma individual como en grupo.
- Inventario mostrando al menos datos como modelo, versión y versión de firmware
- Configuración de al menos los siguientes parámetros a nivel de puerto:
- Descripción o nombre
- VLAN
- PoE
- Velocidad



28 de 60



switches/routers;

Actualización de firmware manual y programada



OE t

- Configuración de parámetros de enrutamiento
- Creación de pilas o stacks
- Herramientas de diagnóstico tales como PING y TRACEROUTE
- Respaldo y repositorio de múltiples configuraciones para su uso potencial posterior.
- Restauración de alguna configuración específica
- Monitoreo de memoria, CPU y fuentes de poder
- Monitoreo de alarmas y eventos
- Monitoreo de puertos

Anexo A - Anexo Técnico.

- Monitoreo de tráfico
- Soporte de al menos 2000 VLANs y 1000 SSIDs
- Deberá de colaborar en conjunto con el Punto de Acceso para tener la capacidad de adaptarse al medio y detectar interferencias, con la finalidad de hacer un uso óptimo del RF y así proveer el mejor desempeño para el soporte de tráfico de datos, audio y video.
- Deberá de poseer un mecanismo que tenga la capacidad de seleccionar el mejor canal de Wi-Fi de acuerdo a la capacidad y condiciones en tiempo real del mismo con la finalidad de proporcionar un mejor desempeño en la entrega de servicios a los dispositivos conectados.
- La solución deberá de proveer mecanismos que en conjunto con los Puntos de Acceso ayudan a optimizar los siguientes escenarios:
 - Capacidad para garantizar la calidad de servicio de las conexiones existentes, en caso de una posible sobre carga o demanda, deteniendo y/o dosificando nuevas solicitudes en caso de que estas puedan degradar el desempeño de las primeras.
 - Balanceo en tiempo real de cargas sobre ambas bandas de WiFi conforme se detecten cambios en el medio.
 - Adaptación de las zonas de cobertura de los Puntos de Acceso, con la finalidad de ajustarse automáticamente a las condiciones del medio para poder cubrir zonas oscuras de RF o en caso contrario reducción de la zona a cubrir para evitar interferencias
- Soporte de la especificación IEEE 802.11d
- Soporte de la especificación IEEE 802.11k
- Soporte de la especificación IEEE 802.11r
- Soporte de la especificación IEEE 802.11w
- Soporte de algún mecanismo que permita optimizar el tráfico de gestión Wi-Fi, sobre todo en ambientes donde la carga de este, suele ser considerable y podría disminuir o afectar de forma negativa el tiempo de aire disponible en los Puntos de

Acceso

- Soporte de la especificación IEEE 802.11e/WMM
- Deberá de poseer un mecanismo en la cual se tenga la opción de poder desconectar a los dispositivos que operen en el estándar 802.11b y forzar al resto de los dispositivos a usar tasas más elevadas, esto con la finalidad de hacer más



Anexo A - Anexo Técnicoz

eficiente el uso del tiempo de conexión y ancho de banda de los dispositivos que operan bajo 802.11 alg/n/ac

- Poseer una funcionalidad en la cual se permita establecer una tasa mínima de conexión entre el dispositivo y el Punto de Acceso.

- Poseer un mecanismo en el cual se permita programar la activación de un SSID basado en día y hora

- Soporte de QoS y asignación de prioridades en capa 2 y 3.

- Soporte de limitación de tasas o mejor conocido como rate limit por SSID. Deberá tener la capacidad de hacer un bypass sobre la tecnología o funcionalidad de los portales temporales que emplean dispositivos como Apple conocida como CNA (Captive Network Assistant) al emplear la autenticación mediante un portal cautivo.

Poseer una funcionalidad en la cual los Puntos de Acceso puedan tener la capacidad de aceptar o negar conexiones basados en parámetros de desempeño en cuanto a un número máximo de dispositivos soportados previamente definido y la carga de los radios.

- Soportar el balanceo de dispositivos entre Puntos de Acceso vecinos, con el objetivo de evitar la saturación en los mismos.

- Soportar la funcionalidad de sobrevivencia en el Punto de Acceso a pesar de que la controladora presente algún evento de indisponibilidad o bien se tengan problemas de conectividad sobre el túnel de gestión hacia la controladora. La solución deberá contar con la funcionalidad de selección automática de canal para garantizar un mejor desempeño a los dispositivos conectados basado en mediciones de tráfico en tiempo de real, así como un mecanismo de barrido de canales para el ajuste de potencias óptimo y para la detección de Puntos de Acceso maliciosos.

3.4.3 Funciones de Seguridad y de Gestión en los Puntos de Acceso

- Deberá de soportar un esquema que permita la creación de grupos de trabajo o entidades lógicas para los Puntos de Acceso, con la finalidad de clasificarlos de acuerdo al tipo de servicio que brinden para un manejo más sencillo en los despliegues y configuraciones de los mismos.

Soportar la funcionalidad en la cual se puedan desplegar servicios en donde los dispositivos que pertenecen a un mismo SSID puedan ser clasificados en diferentes VLANs para una mejor gestión y planeación de los servicios. Se deberán de soportar al menos 50 pools de VLAN con al menos 12 VLANs cada uno.

Soportar LLDP sobre la configuración de los Puntos de Acceso.

Anexo A - Anexo Técnico%

- Deberá ser capaz de realizar al menos las siguientes configuraciones sobre los puertos de los Puntos de Acceso:

- o Habilitar/deshabilitar el(los) puerto(s).
- o Etiquetado y manejo de VLANs (puertos de acceso y tipo trunk)

Deberá de soportar los siguientes mecanismos de seguridad:

- WEP
- WPA-PSK
- WPA-TKIP
- WPA2-AES
- IEEE 802.11i
- EAP-SIM
- EAP-AKA

Deberá de soportar los siguientes esquemas de autenticación:

- IEEE 802.1X
 - Dirección MAC con soporte para el manejo del formato de la misma.
 - Active Directory/LDAP
 - RADIUS
 - HotSpot 2.0
 - Web
 - Guest
 - HotSpot/WISPr con la funcionalidad de Walled Garden y soporte de redireccionamiento con HTTPS
- Soporte de LDAP sobre SSL
- Soporte de TLS
- Soporte de AAA Authentication y AAA Accounting
- Soportar la viabilidad de emplear los servicios AAA en dos modalidades:
 - o Empleando a la controladora como cliente o NAS (Proxy)
 - o Empleando a los Puntos de Acceso como cliente o NAS (No Proxy)
- Deberá soportar o prevenir la comunicación de dispositivos que convivan en la misma subred y/o VLAN
- Soportar un mecanismo para definir filtros en los cuales los dispositivos inalámbricos sean capaces de conectarse con dispositivos de la red alámbrica, a pesar de que entre los mismos dispositivos inalámbricos se encuentre restringida la comunicación en la misma subred. y lo VLAN
- Poseer una funcionalidad que permita limitar el número de dispositivos inalámbricos por cada radio en los Puntos de Acceso.
- Soportar autenticación local de acuerdo a una base de datos de usuarios interna con capacidad de hasta 20,000 cuentas



Anexo A - Anexo Técnico.

- Soporte de mecanismo de calidad de servicio basados en el estándar IEEE 802.11 emMM
 - Soporte de al menos 4 colas de prioridad
- Soporte de algún mecanismo que permita dar prioridad de algún servicio o SSID en contraste con otros.
 - Soporte de los siguientes mecanismos de autodescubrimiento a un equipo controlador:
 - DNS Discovery
 - DHCP Options

31 de 60



Soporte de los

0 CLI 0 Web

- Soporte de funcionalidades de detección y prevención de intrusos tales como la identificación de Puntos de Acceso maliciosos, eventos tipo Spoofing, y redes tipo Ad-Hoc.
- Para la funcionalidad de detectar Puntos de Acceso maliciosos o conocidos como rogues, se deberá de proporcionar al menos la siguiente información de los mismos:
 - Dirección MAC
 - Canal 0 SSID o
 - Radio 0 RSSI o
 - Codificación

Soporte el manejo de DHCP Option 82

Deberá de soportar un mecanismo que permita el bloqueo específico y manual de dispositivos inalámbricos. Deberá de soportar un mecanismo que permita la desconexión específica de dispositivos inalámbricos.

- Soportar la funcionalidad de configurar y desplegar roles asociados a usuarios de forma específica basada en atributos en interacción con entidades AAA como
- RADIUS o algún mecanismo similar que permita su aplicación de forma particular

sobre usuarios autenticados.

Deberá tener un mecanismo que permita la creación de cuentas o pases para usuarios invitados con las siguientes capacidades: o Generación de forma automática.

- Gestión del número máximo de dispositivos por usuario.
- Gestionar periodo de efectividad del pase.
- Exportar las cuentas a archivos tipo CSV o TXT o Generación de cuentas desde un archivo existente CSV o TXT o Impresión de las cuentas o pases.

Anexo A - Anexo Técnico%

- o Envío de cuentas o pases vía correo y SMS.

Soportar la funcionalidad de manejar una base de datos local para autenticación de dispositivos.

Soportar la creación de políticas o filtros con base en los siguientes parámetros: o Dirección MAC o Dirección IP o Puerto TCP/UDP o Tipo de protocolo o Por aplicativos (Capa 7)

- o Por sistema operativo del dispositivo inalámbrico

- La solución ofertada deberá de poseer la funcionalidad para poder filtrar navegación cumpliendo al menos con las siguientes consideraciones:



32 de 60



o Por sistema operativo del

Anexo A - Anexo Técnico,



- - Filtrado por categoría de contenido predeterminada y/o por categorías a seleccionar por el usuario administrador
 - Por URL o nombre de dominio, con la capacidad de catalogar ya sea como sitios permitidos (listas blancas) o restringidos (listas negras o bloqueadas) ○ Soportar al menos una base de 70 categorías.
 - Visualización de estadísticas del filtrado, mediante alguna tabla o dashboard

El soporte de políticas por aplicativo deberá de tener los siguientes tipos de control: ○ Negar o Permitir o Aplicar una limitación de tasa de transferencia o rate limit o Aplicación de calidad de servicio

- Deberá de tener la capacidad de actualizar periódicamente la base de datos de aplicativos a reconocer.
- Deberá de poseer un mecanismo para manejar tráfico del protocolo Bonjour en sus siguientes modalidades:
 - Funcionar como Gateway del mismo protocolo para el reenvío de tráfico de una VLAN a otra.
 - Funcionar como control del mismo tráfico para la limitación en su propagación.

Se deberá de soportar los siguientes protocolos de túnel entre la controladora y los

- Puntos de Acceso:

○ SoftGRE

Soporte de algún mecanismo que garantice que los dispositivos inalámbricos obtengan una dirección IP de un servicio de DHCP en un periodo configurable y evitar la conexión de dispositivos que se configuren con una IP de forma estática. Proveer mecanismos de DHCP y NAT directamente desde los Puntos de Acceso, esto con la finalidad de minimizar en costos en localidades remotas o de baja densidad de servicios.

Soportar el reconocimiento de aplicaciones en uso de los dispositivos inalámbricos que se encuentran conectados a los Puntos de Acceso administrados, proporcionando al menos la siguiente información: ○ Cantidad y/o

A - Anexo Técnico.

volumen del tráfico o Gráficas o tablas que muestren los aplicativos más empleados.

- o Lista de dispositivos Top N en donde se pueda verificar la dirección IP, dirección MAC y el tipo de sistema operativo.

3.4.4 Funciones de Administración y Monitoreo

- Deberá tener la capacidad de ser gestionado mediante:
 - o SNMP v1/v2/v3 e inclusive debe ser soportado que puedan estar activos simultáneamente dos versiones del mismo protocolo, como por ejemplo

33 de 60



Y CRÉDITO PÚBLICO



Anexo

- SNMPv2 y v3, así también se deber soportar codificación tipo DES y AES bajo SNMPv3 o SSH
 - O HTTPS
 - Deberá de tener la funcionalidad de proveer reportes proporcionando al menos las siguientes estadísticas:
 - o Cantidad de dispositivos inalámbricos o Asociaciones nuevas y fallidas de dispositivos o Conexiones históricas de dispositivos o Uso de recursos de la controladora o Tráfico de envío y recepción por SSID, radio o Puntos de Acceso. o Puntos de Acceso Maliciosos o Rogue
- Soporte de envío y recepción de reportes por medio de una cuenta de correo electrónico mediante el uso del protocolo SMTP.
- Soporte de respaldos, estadísticas y reportes mediante el uso del protocolo FTP o TFTP.
- Soporte de envío y distribución de pases de acceso para invitados mediante los servicios de SMS de los diferentes operadores móviles.

Anexo A - Anexo Técnico,

Deberá de tener la funcionalidad de gestionar el registro automático de los Puntos de Acceso mediante reglas para su debido manejo al menos bajo los siguientes criterios:

- o Por subred o Por rangos de direcciones IP o Por georeferencias o coordenadas GPS o por algún uso de identificador y/o etiqueta.

Deberá de poseer un mecanismo o funcionalidad que permita de manera automática clasificar o etiquetar a los Puntos de Acceso más críticos, basado en un umbral predeterminado con base en la cantidad del tráfico de datos. Deberá de proporcionar al menos los siguientes parámetros del sistema controlador o cluster: 0 Uso del CPU o Uso de la memoria o Uso de disco o Alarmas y eventos, los cuales deberán de tener una opción de filtrado para su uso y visualización.

- Deberá de poseer un panel de gestión intuitivo, de fácil uso y con la opción a ser personalizado de acuerdo a las gráficas y estadísticas que deseen monitorearse. El panel de gestión deberá de tener al menos los siguientes elementos y funcionalidades de monitoreo:
 - o Información y estadísticas relevantes sobre los Puntos de Acceso y de la misma controladora y/o cluster.
 - o Iconos o distintivos similares que muestren el estado operativo de los Puntos de Acceso y de la Controladora, incluyendo la opción de



personalizarlos mediante el manejo de umbrales de acuerdo a diferentes parámetros tales como latencia y dispositivos conectados.

- o Integración o visualización de mapas tales como Google Maps o similar.
- o Análisis de tráfico relevante a los Puntos de Acceso, servicios WLAN y dispositivos conectados, así como la personalización de las vistas de dicho tráfico para mostrarlo de acuerdo a diferentes parámetros o criterios; dicho tráfico deberá tener la opción de mostrarse tanto en tiempo real como históricamente.

Deberá de incluir una funcionalidad que permita la importación de planos o .layouts referidos mediante coordenadas de GPS, con los cuales se permita tener la ubicación de los Puntos de Acceso y poder monitorear el tráfico de los mismos tale como cantidad de clientes conectados, cantidad de tráfico, canales en uso y latencia.

A - Anexo Técnico.

Soportar la funcionalidad de proporcionar mapas de calor de los Puntos de Acceso sobre algún plano de piso o layout tanto para la banda de 2.4 GHz como la de 5 GHz.

Permitir la generación de solicitudes de certificados e importación de estos o ya existentes, emitidos por una entidad o proveedor público, para ser incorporado dentro del sistema para la gestión del mismo y para servicios tales como HotSpot o similares.

Deberá de soportar una funcionalidad que permita generar plantillas a partir de configuraciones existentes para el despliegue de nuevos servicios a partir de plantillas previamente elaboradas de una forma más dinámica y sencilla. La solución deberá de soportar un mecanismo en el cual se permitan las actualizaciones de sistema operativo o firmware sobre los Puntos de Acceso basadas en grupos o secciones, es decir, que no necesariamente una actualización de firmware deba de afectar necesariamente a todos los Puntos de Acceso registrados.

La solución deberá ofrecer el listado de al menos los siguientes atributos de los Puntos de Acceso registrados:

- Dirección IP (tanto interna como externa si fuese el caso de pasar por un NAT y/o PAT)
 - Dirección MAC
 - Modelo
 - Versión de firmware
 - Estado operativo y/o administrativo
 - Fecha de registro
- Deberá soportar la extracción o descarga de los logs individuales por Punto de Acceso para efecto de análisis y revisión de eventos.
- Deberá de soportar las siguientes funciones y despliegue de la siguiente información sobre los Puntos de Acceso:
 - Configuración base
 - Tráfico





Anexo A - Anexo Técnico, Anexo

- o Alarmas y eventos o Clientes conectados o Opción de reinicio o Herramientas de troubleshooting o similar
- Soportar la funcionalidad de configuración de servicios WLAN basado en grupos o entidades, de tal forma que por ejemplo un servicio de invitados sea provisionado en ciertas zonas y en otras no. .
- Despliegue de eventos y alarmas proporcionando al menos la siguiente información:
Fecha y hora o Tipo
 - o código o
 - Detalles o
 - Severidad
- Deberá de tener la capacidad de exportar las alarmas en archivos tipo TXT o CSV, Deberá de detener la capacidad de enviar avisos mediante correos o generar traps
- SNMP cuando se genere algún tipo de evento.
Deberá de soportar mecanismos de sincronización mediante el protocolo NTP o SNT p.
Deberá de soportar el envío de logs a un servidor tipo Syslog con al menos las siguientes opciones de configuración:
 - o Manejo de al menos dos servidores (primario y secundario). o Gestión de "facilities" o Filtrado de eventos mediante el manejo de prioridades (debug, informational, warning, minor, major, etc)
- Deberá de soportar el despliegue de al menos la siguiente información sobre los dispositivos inalámbricos asociados: o Dirección IP O Dirección MAC
 - o SSID O servicio WLAN
 - o Dirección MAC del Punto de Acceso al que se está conectado o Nombre del Punto de Acceso
 - o Sistema Operativo
 - o Trafico RX/TX
 - o Mecanismo de autenticación y codificación

A - Anexo Técnico.

0 RSSI

- SNR
- Canal
- Tipo de Radio (802.11 a/b/g/n/ac)
- VLAN
- Hora y fecha en que inició la sesión

- Deberá de poseer alguna herramienta o mecanismo de soporte y análisis de los eventos de conexión de los dispositivos a la red inalámbrica en tiempo real.



36 de 60



0 SNR

Anexo A - Anexo Técnico.



-
-
-
-
-

- Deberá de poseer la funcionalidad de hacer análisis de espectro de RF en tiempo real sobre los Puntos de Acceso tanto en la banda de 2.4 GHz como la de 5 GHz. . La solución deberá de poseer algún mecanismo que permita generar capturas de paquetes en los Puntos de Acceso tanto para los radios de ambas bandas como para el puerto Ethernet de estos.

Permitir la creación de roles de usuarios con diferentes privilegios para la administración de la controladora.

Soporte de autenticación de usuarios administrativos mediante RADIUS y

TACACS+

- Soporte de filtros y/o listas de control de acceso para el acceso vía CLI a la controladora

- Soportar la funcionalidad de proveer diferentes versiones o parches de firmware en los APS sin la necesidad de actualizar el sistema operativo de la controladora en su totalidad

Deberá de proveer una función de mostrar el registro de actividades hechas por los usuarios administradores de la plataforma proporcionando al menos la siguiente información y con la disponibilidad a ser exportada a un archivo en formato de texto o CSV: o Usuario administrador o Fecha y hora del cambio o Dirección IP o Acción ejecutada

- Capacidad para cargar y ejecutar scripts de forma grupal y/o masiva sobre diversos Puntos de Acceso.

- Deberá de soportar la integración con plataformas de gestión, configuración o monitoreo terceros mediante el uso de APIs.



3.5 Access Point Primario

3.5.1 Características Generales

Anexo A - Anexo Técnico

Punto de Acceso para interiores con soporte de 802.11ax 4x4:4 en el radio de 2.4 GHz y en el de 5 GHz, MU-MIMO y OFDMA con capacidades de alto desempeño para ambientes de muy alta demanda.

- El equipo deberá de soportar al menos 01 puerto Gigabit Ethernet con el soporte de al menos 2.5 Gbps y un puerto 1 GbE
- 01 puerto USB para para la integración de otras tecnologías inalámbricas o de convergencia.
- El equipo deberá de alimentarse mediante los siguientes mecanismos:
 - o Soporte de IEEE 802.3af/at

J



37 de 60



HACIENDA
SECRETARÍA DE HACIENDA Y CRÉDITO PÚBLICO



-
-
-
-
- o Alimentación por adaptador de corriente de CD. Soporte de SoftGRE, L2TP O GRE
- Deberá soportar los siguientes mecanismos de gestión:
 - o Centralizado mediante una consola de administración o controladora. o Nube del fabricante.
 - o Modalidad autónoma y/o independiente con la capacidad de administrar a otros Puntos de Acceso sin la necesidad de un esquema de controladora.
-
-
-

3.5.2 Funcionalidades, Desempeño y Soporte de Especificaciones Inalámbricas

El equipo deberá de contar con las certificaciones de Wi-Fi:

- o Wi-Fi Alliance alb/g/n/ac/ax o Passpoint

Deberá trabajar en la banda de 2.4 GHz y 5 GHz.

El- equipo deberá de poseer un arreglo de antenas, que tengan la capacidad de adaptarse al medio y detectar interferencias, con la finalidad de hacer un uso

Anexo A - Anexo Técnico.

óptimo del RF y así proveer el mejor desempeño para el soporte de tráfico de datos, audio y video.

Deberá de poseer un mecanismo que tenga la capacidad de seleccionar el mejor canal de Wi-Fi de acuerdo con la capacidad y condiciones de este, con la finalidad de proporcionar un mejor desempeño en la entrega de servicios a los dispositivos conectados.

Soporte de balanceo por banda y por clientes

Soporte de IPv4 e Ipv6

Soporte de IEEE 802. IQ

Soporte de LLDP

Soporte de los siguientes estándares: o

IEEE 802.11a/b/g/n/

- o Deberá soportar al menos las siguientes tasas físicas:

2400 Mbps en el radio de 5 GHz

1100 Mbps en el radio de 2.4 GHz

Soporte de canalización en 20 MHz, 40 MHz, 80 y 160 MHz Deberá proveer una ganancia de al menos:

- x 25 dBm en el radio de 2.4 GHz
- o 26 dBm en el radio de 5 GHz

- El equipo deberá de poseer una ganancia de al menos 2 dBi en las antenas y poseer una sensibilidad de al menos -92 dBm
- El equipo deberá de soportar en su totalidad al menos hasta 800 dispositivos inalámbricos simultáneos
- Soporte de al menos hasta 20 SSIDs en total.
- Soporte de reconocimiento de aplicativos, limitación de ancho de banda, así como listas de control de acceso



Anexo A - Anexo Técnico%

- Soporte integrado de radio BLE o ZigBee con la finalidad de ser integrado en soluciones IOT o similares
- Debe incluir de manera nativa o a través de un software o aplicación externa del mismo fabricante de la solución inalámbrica propuesta, una herramienta que permita la administración centralizada de dispositivos IOT o similares basados BLE o Zigbee y que maneje APIS abiertas que permitan la integración con otros sistemas de IOT de terceros.
- Soporte de formación de redes Mesh

3.5.3 Funciones de Seguridad y de Gestión

- El equipo deberá de soportar los siguientes mecanismos de seguridad:
 - WPA-PSK
 - WPA-TKIP
 - WPA2-AES
 - WPA3
 - IEEE 802.11i
- El equipo deberá de soportar las siguientes especificaciones y funciones Wi-Fi:
 - WISPr
 - HotSpot 2.0
 - Portal Cautivo
 - Soporte de IEEE 802.1X como suplicante
- El equipo deberá de soportar las siguientes especificaciones:
 - IEEE 802.11r IEEE
 - 802.11k
 - IEEE 802.11v
 - WMM
 - LDPC
 - Beamforming
- Soporte de funcionalidades de detección de intrusos en conjunto con el esquema de gestión con la controladora.
 - Deberá de tener la capacidad de realizar análisis de espectro
 - Soporte de mecanismos de QoS

Anexo A - Anexo Técnico.

3.5.4 Especificaciones Ambientales, Protección y de Consumo

- Deberá de cumplir con las siguientes certificaciones:
- EN 60950-1 Safety
- EN50121-1 Railway EMC
- IEC 61373 Railway Shock & Vibration
- EN 60601-1-2 Medical

39 de 60



HACIENDA
SECRETARÍA DE HACIENDA Y CRÉDITO PÚBLICO



EN 62311 Human Safety/RF Exposure

WEEE/ROHS compliance

UL 2043

Deberá tener la capacidad de operar en el siguiente rango de temperaturas:

0° C - 45° C

Deberá tener la capacidad de operar bajo las siguientes condiciones de humedad:

10% - 95% sin condensación

Deberá de poseer un mecanismo de seguridad física del tipo Kensington Lock o hidden latching o similar.

Deberá de ser aprovisionado con todos los elementos de montaje necesarios para su adecuada instalación

3.6 Access Point Secundario

3.6.1 Características Generales

Punto de Acceso para interiores con soporte de 802.11ac 2x2:2 MU-MIMO doble banda 2.415 GHz para ambientes pequeños y medianos empresariales.

Anexo A - Anexo Técnico%

- El equipo de Punto de Acceso de red inalámbrica a considerar, deberá ser una solución basada en el estándar IEEE 802.11ac Wave 2, que permita habilitar el acceso de red para los usuarios en general, como dispositivos móviles (tablets y smartphones).
- El equipo deberá de soportar al menos 4 puertos Ethernet, sobre los cuales se puedan conectar otros dispositivos tales como teléfonos IP, servicios IPTV o similares. Así también al menos uno de estos puertos deberá de tener la capacidad de aprovisionar POE.
- El equipo deberá de alimentarse mediante el soporte de IEEE 802.3af Soporte de L2TP y GRE
- Deberá soportar los siguientes mecanismos de gestión:

-

-

-

-

-

-

-

Anexo A - Anexo Técnico.

o Centralizado mediante una consola de administración o controladora o Nube del fabricante o Modalidad autónoma y/o independiente con la capacidad de administrar a otros Puntos de Acceso sin la necesidad de un esquema de controladora. El equipo deberá de poseer LEDs indicadores, los cuales al menos puedan

mostrar los siguientes estados de este mediante diferentes colores o algún otro distintivo a nivel físico:

- o Operación del equipo (boot, modo normal, etc.).
- o Verificación si el equipo trabaja en modo autónomo o centralizado
- o Operación de la banda de 2.4 GHz
- o Operación de la banda de 5 GHz



mostrar los siguientes estados de este mediante diferentes colores o algún otro distintivo a nivel físico:

- o Operación del equipo (boot, modo normal, etc.).
- o Verificación si el equipo trabaja en modo autónomo o centralizado
- o Operación de la banda de 2.4 GHz

Anexo A Anexo Técnico.



-
-
-

3.6.2 Funcionalidades, Desempeño y Soporte de Especificaciones Inalámbricas

- El equipo deberá de contar al menos con las siguientes certificaciones
 - Wii: o Wi-Fi Alliance o Passpoint
 - Deberá trabajar en la banda de 2.4 GHz y 5 GHz.
- El equipo deberá de poseer un arreglo múltiple de antenas, que tengan la capacidad de adaptarse al medio y detectar interferencias, con la finalidad de hacer un uso óptimo del RF y así proveer el mejor desempeño para el soporte de tráfico de datos, audio y video.
 - Deberá de poseer un mecanismo que tenga la capacidad de seleccionar el mejor canal de Wi-Fi de acuerdo a la capacidad y condiciones de este con la finalidad de proporcionar un mejor desempeño en la entrega de servicios a los dispositivos conectados.
- Soporte para poder formar redes tipo malla o mesh
- Soporte de IPv4 e IPv6
- Soporte de IEEE 802.1Q
- El equipo deberá de tener embebido en conjunto con la herramienta de gestión o similar, una función que permita hacer un análisis de espectro básico Soporte de los siguientes estándares:
 - IEEE 802.11a/b/g/n/ac
- Deberá soportar al menos las siguientes tasas físicas:
 - 867 Mbps en el radio de 5 GHz
 - 300 Mbps en el radio de 2.4 GHz
- Soporte de canalización en 20 MHz, 40 MHz y 80 MHz
- Deberá proveer una ganancia de al menos:
 - 18 dBm en el radio de 2.4 GHz
 - 20 dBm en el radio de 5 GHz

Anexo A - Anexo Técnico.

La solución deberá contar con la funcionalidad de selección de la banda de operación por cada SSID:

- o Capacidad de irradiar en 5 GHz únicamente. o Capacidad de irradiar en 2.4 GHz únicamente.
- o Ambas bandas, pero con la capacidad de detectar dispositivos que soporten ambas bandas, direccionándolos a la de 5 GHz por estar menos congestionada.

El equipo deberá de poseer una sensibilidad de al menos -98 dBm

El equipo deberá de soportar en su totalidad al menos hasta 80 dispositivos inalámbricos simultáneos

- Soporte de al menos hasta 16 SSIDs en total.
- Soporte y asignación de prioridades.
- Deberá soportar la integración para soluciones IoT

41 de 60



LICO

3.6.3 Funciones de Seguridad y de Gestión.

El equipo deberá de soportar los siguientes mecanismos de seguridad:

- 0 WPA-PSK
- 0 WPA-TKIP
- 0 WPA2-AES
- 0 IEEE 802.11i

El equipo deberá de soportar las siguientes especificaciones y funciones Wi-Fi:

- 0 WISPr o
- HotSpot 2.0 o
- Portal Cautivo

65 de 60

Anexo A - Anexo Técnico.

Soporte de IEEE 802. IX como suplicante

El equipo deberá de soportar las siguientes especificaciones:

- ○ IEEE 802.11r
- IEEE 802.11k
- WMM ○ LDPC
- Beamforming

Soporte de los siguientes mecanismos de autodescubrimiento a un equipo controlador:

- ○ DNS Discovery ○
- DHCP Options

- Soporte de funcionalidades de detección de intrusos en conjunto con el esquema de gestión con la controladora.

Para efectos de sincronía deberá de soportar el protocolo NTP.

Deberá tener la capacidad de ser gestionado mediante:

- ○ SNMP ○
- Telnet ○
- SSH
- HTTP/HTTPS

Soporte de FTP/TFTP

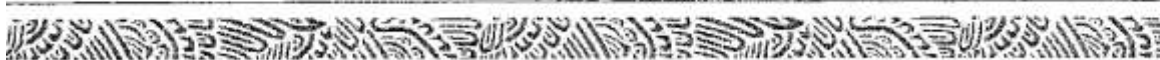
Deberá de tener la capacidad de proveer servicios tales como:

- ○ DHCP
- Especificaciones Ambientales, Protección y de Consumo
- Deberá de cumplir con las siguientes certificaciones:
- ○ EN 60950-1 Safety
- EN 50121-1 Railway EMC
- IEC 61373 Railway Shock & Vibration
- WEEE/RoHS compliance



- Deberá tener la capacidad de operar en el siguiente rango de temperaturas:

42 de 60



Y PÚBLICO



Anexo A - Anexo Técnico.

- ○
 - ○ c - 38 ° C
 - Deberá tener la capacidad de operar bajo las siguientes condiciones de humedad:
 - 10% - 95% sin condensación
- Deberá de ser aprovisionado con todos los elementos de montaje necesarios para su adecuada instalación,

3.7 Plataforma de localización de activos

3.7.1 Características Generales

- Sistema de localización de dispositivos para la red WLAN para el análisis y comportamiento de la ubicación y comportamiento de estos
- La solución deberá tener la capacidad de ser desplegada como un software o máquina virtual local que resida en las instalaciones de la institución
- La solución deberá de tener una sensibilidad de al menos 5 metros como margen de error en la localización de un dispositivo
- Deberá ser capaz de detectar tanto dispositivos que se encuentren conectados a la red de la institución como aquellos que no lo estén
- La solución deberá de proporcionar o tener la capacidad de ser calibrada o recalibrada en caso de un nuevo despliegue o que haya cambios en la ubicación de los APS o bien si estos son reemplazados o reajustados, de tal forma que la información que entregue sea la óptima.
- Deberá de proporcionar información de la ubicación de los dispositivos detectados en tiempo real y de forma histórica.
- Deberá de tener la capacidad de mostrar la densidad de dispositivos detectados mediante mapas de calor en tiempo real, dichos mapas deberán actualizarse de forma automática al menos cada 2 minutos.
- Para los mapas de densidad de dispositivos, la herramienta deberá de poseer una función que permita ajustar los colores o los contrastes empleados.
- Deberá de proporcionar la opción del uso de alguna herramienta para dispositivos móviles para realizar funciones de ajustes, triangulación o calibración.
- Poseer una función con la cual se pueda hacer la búsqueda de un dispositivo de forma específica.
- La herramienta deberá soportar el manejo de APIS y JSON sobre HTTPS de tal forma que se encuentre abierta para interoperar con soluciones de terceros para poder entregar un análisis completo del comportamiento de los dispositivos mediante reportes, dashboards o entregables propios de dichas soluciones. La

Anexo A - Anexo Técnico.

solución deberá de ser capaz de entregar información, la cual pueda ser usada por terceros para poder implementar campañas de mercadotecnia y/o monetización por el uso de la red, de acuerdo con el los dispositivos.

Anexo A - Anexo Técnico.

■



oe

Púa LICO

■

■

- Las APIS de la herramienta deberán permitir al menos la extracción de la siguiente información:

- o Lugar o Recinto de la Red WLAN en análisis o Mapas de ubicación o Dispositivos o Cuentas de usuarios administradores

■

- Deberá tener la capacidad de editar planos de los sitios o recintos de interés en donde se requiera el uso de la herramienta, para los cuales deberá soportar al menos los siguientes formatos de archivos: PNG y JPEG.

■

- Soportar múltiples sitios en una misma instancia o consola de administración Deberá tener la capacidad de proporcionar históricos de los dispositivos al menos con la siguiente recurrencia: o Por hora o Por día o Por semana o Por mes

■

- Capacidad para retener datos por al menos 45 días.

La solución deberá poder proporcionar al menos las siguientes estadísticas:

■

- Dispositivos únicos o de primera vez o Días transcurridos

■

- desde la última visita o Tiempo promedio de permanencia de los dispositivos o Dispositivos nuevos vs Recurrentes o Recurrencia de dispositivos

La solución deberá de poder ofrecer mecanismos de cifrado para poder proteger los datos punto a punto

Las estadísticas deberán poder ser exportadas en archivos TXT o CSV

■

- La consola de administración deberá de soportar al menos 3 tipos de cuentas de usuarios administradores con diferentes privilegios.

■

3.8 Sistema de Control de usuarios basado en certificados

3.8.1 Características Generales

Solución para realizar el registro y control de dispositivos corporativos y personales a la red LAN, mediante la identificación y asignación de políticas. La solución deberá ser provista ya sea mediante la instalación y configuración de un

Anexo A - Anexo Técnico%

appliance que puede ser físico o virtual, este deberá residir en las instalaciones de la institución.

- Deberá ser capaz de controlar y facilitar el acceso a dispositivos propios de la institución, así como también a los dispositivos personales que los usuarios posean y deseen emplear en las redes que así lo permita la institución.
- Deberá soportar el control y registro de al menos 1000 usuarios, o bien al menos 1000 dispositivos móviles.

h'@xico

Año de
Independen



- La solución deberá de tener la capacidad de ser dimensionada con base en el número de usuarios de dispositivos.
- La solución deberá tener la versatilidad de ser empleada para ser compatible e interoperar tanto en ambientes LAN como WLAN de múltiples fabricantes bajo mecanismos estándares de seguridad.

3.9 Funciones de Seguridad y de Enrolamiento

- La solución deberá de brindar enrolamiento de dispositivos empleando mecanismos estándares basados al menos en WPA2-Enterprise y tener la facultad de emitir certificados digitales propios de la herramienta por dispositivo. La solución deberá de brindar la facilidad de crear un entorno de autoservicio a los usuarios, de tal forma que, al hacer el enrolamiento de sus dispositivos, no dependan de la asistencia directa en sitio del staff de TI para proveer acceso al servicio, o ya sea mediante el uso de mecanismos de patrocinio tales como la emisión de tokens vía correo y SMS. La herramienta deberá de proporcionar mecanismos que guíen de forma sencilla a los usuarios mediante un asistente para hacer el enrolamiento de sus dispositivos y proveer la información necesaria tales como la instalación de agentes o algún aplicativo en particular Soporte de AAA

Anexo A - Anexo Técnico,

Deberá de tener la capacidad de brindar visibilidad y control sobre los dispositivos que se conecten a la red.

Deberá de proporcionar la granularidad de proveer políticas de seguridad que puedan limitar anchos de banda y accesos de acuerdo con los siguientes criterios: o Por usuario o Por dispositivo o Por VLAN

Proveer funcionalidades de análisis de posturas para el análisis de los dispositivos de tal forma que, si estas no se cumplen en los mismos, puedan ser corregidas o también negar el servicio, al menos deberá de soportar la validación y remediación de:

- Parámetros de configuración del registro
- Firewall
- Aplicativos tipo antivirus
- Verificación de activación de bloqueo de pantalla o PIN
- Poseer la funcionalidad de servidor RADIUS integrado y de conectarse a otros servicios RADIUS externos
- Tener la capacidad de integrarse con autoridades externas emisoras de certificados
- Soporte de OCSP
- Capacidad para interconectarse con alguna infraestructura externa de certificados

45 de 60



HACIENDA
SECRETARÍA DE HACIENDA Y CRÉDITO PÚBLICO



Manejo y administración de certificados locales con la capacidad de revocación automática

Deberá soportar empleo de ACLs y VLANs dinámicas

Soporte de integración con Directorio Activo

Soporte de LDAP y LDAPS

Soporte de RADIUS COA

Manejo de base datos de usuarios locales

Soporte de los siguientes mecanismos de autenticación:

Anexo A - Anexo Técnico%

- 0 Web
- 0 MAC 0
- SAML o
- OAuth
- o HotSpot 2.0
- 0 PEAP
- 0 EAP-TLS
- 0 EAP-SIM

Soporte e integración de autenticación con al menos las siguientes redes sociales:
o Facebook o LinkedIn o Google

Soporte de personalización de portales de acuerdo con lo que la institución requiera y ajustarlo a la imagen de esta.

Integración con Chromebook para la emisión de certificados en dichos dispositivos permitiendo el enrolamiento en una forma más transparente usando mecanismos de autenticación de doble factor vía Web.

Monitoreo y gestión de certificados, con la capacidad de revocar los mismos de forma individual o por grupos.

- Poseer una herramienta gráfica que permita visualizar el flujo de enrolamiento de los dispositivos.
-

3.10 Funciones de Administración, Visibilidad e Integración

- La solución deberá de tener una arquitectura del tipo multitenant, de tal forma que puedan ser administradas redes independientes empleando una sola instancia

- Soportar al menos los siguientes sistemas operativos de dispositivos:

- o Windows
- o Chrome
- o Android
- o iOS
- o Ubuntu
- o Mac OS
- o Blackberry



Anexo A - Anexo Técnico,

OE HACIÜ40A

PÚBLICO



- Capacidad para monitorear y relacionar por dispositivo y por usuario, así como su certificado en uso
- Deberá de tener capacidad para integrarse con soluciones de terceros tales como: firewalls, MDMs, filtrados de contenido o cualquier otra que soporte el manejo de
- Soporte de integración con Eduroam.
- Soporte e integración con soluciones de asistentes virtuales tales como Alexa o similares, con la cual permitan interactuar para la emisión de pases temporales a la red en los dispositivos que lo tengan en uso.
- Deberá de proveer al menos tres tipos de usuarios administradores con diferentes privilegios
- Tener la capacidad de manejar scripts para la ejecución de tareas de la herramienta
- Manejo y soporte de reportes en formato .CSV o similar
- Soporte para programar la generación de reportes al menos por día y por semana, con la capacidad de ser enviados a múltiples destinatarios vía correo. .
- Deberá de tener disponible la ayuda en línea o documentación de la herramienta embebida en la misma para su uso de forma más ágil y organizada. ■ Soporte de al menos las siguientes herramientas de diagnóstico:

0 DNS Lookup o Verificación de servidor de certificados

Anexo A - Anexo Técnico,

47 de 60



OE HACIENDA

púa LICO

3.11 Plataforma de detección de movimiento lateral.

Requerimientos Generales

- La solución debe incluir el licenciamiento para publicar emulaciones o trampas en 16 VLANs
- La solución debe estar basada en la red y sin utilización de agentes
- La solución puede correr sobre hardware o como plataforma virtual en VMWare ESX, Microsoft Hyper-V o Linux KVM.
- La solución debe soportar además plataformas de Nube Pública en forma de máquina virtual nativa de Microsoft Azure y Amazon EC2 Cloud, sin necesidad de utilizar conectores sobre sistemas operativos genéricos o propietarios. .
- La solución debe de emplear trampas o honeypots que deberán ser desplegados estratégicos al interior de la red para la identificación de amenazas.
- La solución debe tener la capacidad de monitorear comunicaciones en VLANs y el tráfico de salida a Internet.
- La solución en sus diversos componentes debe estar basada en un sistema operativo endurecido y cerrado.
- La solución deberá soportar como mínimo el despliegue de 512 emulaciones o trampas en un appliance físico o virtual para cada sitio requerido, permitiendo a la convocante decidir el número a utilizar por VLAN.
- Los servidores Windows son una de las plataformas más utilizadas en las organizaciones. Esto hace que para que la solución requerida por la convocante sea

Anexo A - Anexo Técnico,

más creíble, debe de soportar el despliegue de al menos 250 trampas basadas en Servidores Windows 2008R2, 2012 R2 o 2016 por cada sitio.

- Las PCs de escritorio y laptops con Windows y MAC son las más utilizadas en las organizaciones. Esto hace que para que la solución requerida por la convocante sea más creíble, debe de soportar el despliegue de al menos 250 trampas basadas en Windows 10 o Mac OS.
- Para lograr una cobertura completa del engaño, la solución debe incluir licenciamiento para implementar señuelos de al menos <CANTIDAD> endpoints por localidad, permitiendo a la convocante implementar esta funcionalidad en donde sea necesario.
- La solución no debe requerir licencias de sistemas operativos para las emulaciones, trampas o honeypots.
- La solución debe apoyar la mezcla de trampas o emulaciones falsas con los activos del entorno productivo de la entidad bajo el concepto del uso del engaño. ■ Con el objetivo de incrementar la cobertura de la plataforma del engaño, la solución debe soportar la capacidad de construir trampas personalizadas (Construye tu Propia Trampa, Build Your Own Trap) de cualquier dispositivo conectado a la red de la organización.

La solución debe integrar, sin necesidad de licenciamiento adicional, un servicio de Detección de Inteligencia de Ataques. Este servicio debe proporcionar notificaciones por parte del fabricante respecto a malware, otras campañas que



DE HACIENDA ?

A
PÚBLICO

SIF

afectan industrias o vulnerabilidades específicas. Esto con el objetivo de informar en tiempo para parchar vulnerabilidades y fortalecer controles de seguridad. ■ La solución debe poder adaptarse a cambios en el entorno productivo mediante la ejecución de escaneos para identificar nuevos activos o plataformas operativas en la red de la entidad.

- La solución deberá soportar el acceso basado en roles para segregar funciones y capacidades de la plataforma por usuario.
- La arquitectura de la solución debe contar con una gestión centralizada de todos los sitios o localidades basada en web.

Anexo A - Anexo Técnico,

- La solución debe tener la capacidad de integrarse con un sistema SIEM correlacionador de eventos, mediante Syslog u ODBC.
- La solución debe permitir generar reportes al menos de Top de direcciones IP destino, Top de IP fuentes maliciosas, Ataques de Alto Riesgo Diarios y Semanales.

Inteligencia y Detección de Amenazas

- La solución debe de incluir la capacidad, licencias y componentes de hardware requeridos para monitorear el tráfico generado del interior de la red hacia Internet, para poder identificar comportamiento basado en botnets, comando y control (C2) y responder rápidamente ante la identificación de equipos comprometidos.
- La solución no debe estar basada en firmas para detectar el malware o la actividad maliciosa.
- La solución debe soportar al menos los siguientes mecanismos para la detección de malware o ataques:
- Cajas de arena (sandboxing) o Análisis estático o Integración con VirusTotal.
- La solución debe de soportar al menos la integración con las siguientes plataformas de Sandbox de los siguientes fabricantes: McAfee, Cisco, Palo Alto Networks, ThreatTrack, Cuckoo.
- La solución debe apoyar la exportación manual de Indicadores de Compromiso (IOCs) mediante el formato STIX o a través de integraciones automáticas con dispositivos de terceros.
- La solución debe de ser capaz de capturar el código malicioso y payloads asociados para su análisis, a pesar de no ser una amenaza conocida previamente. ■ La solución debe generar notificaciones después de la detección de posibles amenazas internas o de malware.
- La solución debe de minimizar los falsos positivos en la generación de alertas. ■ La solución puede utilizar un análisis dinámico descentralizado basado en la nube para realizar un análisis forense y controlado del malware capturado desde los sensores o trampas.

La solución debe de ser capaz de identificar no solo ataques o comportamiento basados en malware, sino cualquier comportamiento malicioso de interacción humana o automatizado que haga contacto con los sensores desplegados.

Anexo A Anexo Técnico.

**HACIENDA**
SECRETARÍA DE HACIENDA Y CRÉDITO PÚBLICO

- La solución debe de permitir la integración nativa a la plataforma de administración de la tecnología del engaño sin necesidad de licenciamiento o productos adicionales de la misma marca.
- La solución debe permitir la integración con Cisco ISE, ForeScout, Checkpoint o Fortinet que apoyen la respuesta ante un evento de manera automática o bajo demanda.
- La solución debe permitir incluir datos falsos independientes en cada trampa para hacer más creíble el engaño hacia el atacante.
- La solución debe incluir la siguiente información relacionada con el ataque: o IP del atacante y el objetivo o Análisis preliminar o Captura de la sesión en la red (PCAP) o Servicios utilizados durante los ataques o interacción con la trampa ■ La solución debe permitir la extracción del malware original para realizar un análisis forense externo o una retención' legal de ser necesario.
- La plataforma de permitir identificar y filtrar los eventos generados desde las trampas o sensores por la naturaleza de su actividad: o Conexión o Reconocimiento o Interacción o Infección
- La solución debe tener la capacidad de proporcionar información ficticia configurable e independiente por trampa, como puertos, mensajes de bienvenida (banners), credenciales de acceso sobre cada servicio (ftp, smb, etc) para hacer más factible engañar al atacante.
- La solución debe poder emular de forma nativa, al menos los siguientes ambientes Windows: Directorio Activo, DNS, SMB, FTP, SQL. Además de Linux, Mac, Cisco, Juniper, Impresoras. SAP. Sistemas industriales SCADA (Rockwell, Siemens), IOT (Luz WiFi Phillips), dispositivos ATM y plataformas SWIFT.
- Las emulaciones deben poder mostrar diferentes "Huellas Digitales" de sistemas operativos Windows de la misma familia (Windows XP, Windows 7, Windows 8, Windows 2003, Windows Server 2012 R2, Windows Server 2008 R2, Windows Server 2016) además de otros sistemas operativos como Linux (CentOS, Redhat) Switchs Cisco, Cámaras Axis, entre otros.
- La solución deberá permitir visualizar estadísticas de los eventos o amenazas basado en la naturaleza de esta dentro de la entidad.

Anexo A - Anexo Técnico.

3.12 Cableado de servicios adicionales.

Se requiere de los siguientes servicios para el edificio principal de SHE

- Instalación de uplinks de fibra óptica de 10Gb, para conexión vertical entre MDF's y los Switches Core que se encontraran en el Centro de Datos de piso 7
- Se tendrá que realizar el tendido de fibra óptica utilizando las verticales del edificio

50 de 60



SECRETARÍA DE HACIENDA Y CRÉDITO PÚBLICO



Anexo

- La trayectoria será desde el Switch Core del Centro de Datos, pasando por escalerilla y utilizando la vertical del edificio
- Serán dos jumpers de fibra a 10Gb por piso, uno conectado a cada Switch de Acceso del Stack para funciones de redundancia. ● El proveedor será el encargado de considerar todo el material necesario para llevar a cabo esto, incluyendo los Gbics de cada punta.

3.13 Router Cisco c881.

- Se requiere el equipo ruteador marca Cisco modelo c881, para conexión a Banco de México, los lineamientos de Banxico requieren que sea este equipo en específico para generar una VPN de Backup en caso de falla de los enlaces dedicados principal y secundario.

4. PLAN DE TRABAJO.

A - Anexo Técnico

El licitante ganador deberá entregar por escrito, durante los 5 días hábiles posteriores a la firma del contrato, un plan en el que deberá indicar las actividades a desarrollar para la entrega de los Servicios de Telefonía, duración expresada en días y los recursos humanos a utilizar, considerando como fecha límite para el inicio de operación de los servicios, en condiciones óptimas y a entera satisfacción de la SHF.

Este plan deberá ser validado y autorizado por SHF, previo a su ejecución, debiendo contener los horarios que sean acordados.

El Plan de Trabajo del Licitante deberá contener cuando menos las siguientes actividades, cumpliendo con los tiempos establecidos para cada Fase:

Actividad
Instalación y configuración por parte del Proveedor de los elementos de la solución
Entrega del Proveedor y recepción por parte de SHF de la solución instalada, configurada y puesta a punto
Soporte por parte del Proveedor a la operación de la solución y atención a las fallas reportadas por el personal designado por SHF para dicho efecto
Entrega por parte del Proveedor de los reportes mensuales de disponibilidad de los servicios

Handwritten mark resembling a stylized 'D' or 'U'.

Handwritten mark resembling a stylized 'L' or '7'.



OZ

Púa Lico



Devolución de los equipos que sean propiedad del proveedor
--

Anexo A - Anexo Técnico.

5. FASES DEL CONTRATO.

5.1. Planeación, Instalación y configuración.

El contrato tendrá una duración de 45 meses, sin embargo, solo se pagarán los 43 meses relativos a la fase de operación, siendo el primer y último mes correspondientes a la planeación y cierre descritas en el punto 4. PLAN DE TRABAJO, las cuales no tendrán costo.

El contrato arrancará en forma inmediata una vez adjudicado el contrato al Licitante. Una vez asignado el contrato, será responsabilidad del Licitante ganador ejecutar las tareas técnicas y administrativas necesarias para programar el arranque del proyecto en coordinación con SHF.

La fase de planeación tendrá lugar desde la asignación del contrato, a partir de la fecha de fallo, a través de reuniones durante las cuales se deberán ajustar los programas de trabajo y se afinarán los detalles de integración técnica correspondientes. Es responsabilidad del Licitante ganador coordinar y ejecutar todas las tareas necesarias para cumplir en tiempo y forma con los planes de trabajo. En esta fase se entregarán al Proveedor los formatos y los contenidos de manera detallada de los reportes que deberán ser entregados a SHF de manera periódica. El Licitante ganador puede hacer modificaciones a dichos documentos, previa autorización de SHF, con el objetivo de enriquecer la información que se entregará. Para esta fase, el Licitante ganador deberá designar como responsable a un administrador de proyectos para el desarrollo de las actividades de esta etapa, así como para la elaboración de la documentación correspondiente.

La entrega total de los equipos telefónicos, configuración y pruebas de la solución del Centro de Llamadas, así como la preparación del conmutador para el soporte integral de cada una de las soluciones, deberán estar concluidas en esta fase.

Durante esta fase no se realizará pago alguno por las actividades realizadas.

5.2. Operación.

A - Anexo Técnico

fase dará inicio a más tardar el 31 de marzo de 2021 después de la fase planeación migración, tendrá una duración de 43 meses, en la cual el Licitante ganador deberá proporcionar los servicios de soporte, garantías y mantenimiento para la infraestructura entregada a SHF cumpliendo con los SLA's establecidos en el presente anexo. Cualquier desviación o incumplimiento de los SLA's por parte del Licitante ganador, lo hará acreedor a la pena o sanción establecida en el punto **13 Nivel de Servicio**.

52 de 60



Esta
y

Anexo A - Anexo Técnico



HACIENDA
SECRETARÍA DE HACIENDA Y CRÉDITO PÚBLICO



5.3. Cierre.

A la finalización de la etapa de Operación, iniciará un proceso de migración para transferir los servicios objeto de esta contratación, a un nuevo Licitante ganador que SHF designe o una nueva infraestructura con el Proveedor Saliente. La fase de cierre tendrá una duración de 1 mes y se ejecutará de acuerdo al plan de trabajo que elabore SHF. El Proveedor Saliente y SHF o un nuevo Proveedor que SHF designe, deberán trabajar de manera conjunta para ajustar el plan de migración, con el objetivo de garantizar que durante la transición de los servicios no exista degradación de los mismos.

En caso de que el Proveedor Saliente resulte seleccionado nuevamente para la continuidad de los servicios, para el caso en que SHF licitara nuevamente los servicios bajo condiciones y alcances similares, el plan de trabajo de la etapa de cierre, deberá ajustarse al plan de transición del siguiente contrato.

Para toda la infraestructura proporcionada por el Proveedor, el retiro será realizado en coordinación con la entrega del nuevo contrato o solución que dará continuidad a la operación de SHF.

Durante esta fase no se realizará pago alguno por las actividades realizadas.

6. LUGAR Y CONDICIONES DE ENTREGA DE LOS SERVICIOS

Las reuniones de trabajo y las actividades de aprovisionamiento de la solución •podrán realizarse de forma inmediata, una vez realizado la firma del contrato.

La dirección de entrega de los servicios será la siguiente:

Sitio	
Edificio Principal de SHF	Dirección Ejército Nacional 180, Piso 7 Colonia Anzures Alcaldía. Miguel Hidalgo C.P. 11590

Anexo A - Anexo Técnico%

	Ciudad de México.
--	-------------------

7. ROLES DEFINIDOS

Los roles responsabilidades que se han definido para llevar a cabo la administración de los servicios descritos, son los siguientes:

7.1. **PROVEEDOR DE SERVICIOS DE INFRAESTRUCTURA TECNOLÓGICA DE SHF, COMO responsable de:**

- Generar un canal de comunicación eficiente con el Proveedor.

53 de 60



DE

- Participar en reuniones de trabajo y seguimiento periódicos, relativos a los servicios contratados.
- Aprobar o en su caso rechazar los entregables y documentación generados, producto de los servicios proporcionados por el Proveedor.
- Revisar y solicitar los ajustes necesarios de los entregables y documentación generados por el Proveedor, hasta lograr la entera satisfacción de SHF.
- En su caso, rechazar la solicitud de pago presentada, señalando las causas de esto último.
- En caso de aprobar los entregables, firmar conjuntamente con el Proveedor la carta de Aceptación Técnica, de manera previa a la presentación de factura por parte del Proveedor, en los casos donde se requiera su firma.
- Remitir a la Subdirección de Gobierno de TI de SHF la Carta de Aceptación Técnica, para estar en posibilidad de liberar el pago correspondiente.

Anexo A - Anexo Técnico.

- En su caso, notificar a la Subdirección de Gobierno de TI de SHF, sobre las penalizaciones aplicables por el incumplimiento de los nivel de servicio, dentro de los tiempos y las vigencias establecidos.

7.2. El Titular de la Subdirección de Gobierno de TI de SHF como Enlace Administrativo de SHF, responsable de:

- Integrar el expediente de pago, incluyendo la evidencia de los servicios y/o entregables que resulten aprobados por la Subdirección de Infraestructura Tecnológica.
- Solicitar la autorización de pago a la Dirección General Adjunta de Administración, Operaciones y Tecnologías, así como a la Dirección de Tecnologías de la información.
- Tramitar el pago ante la Subdirección de Recursos Materiales y, en su caso, notificar sobre la aplicación de penas convencionales correspondientes.

7.3. Líder del Proyecto del Proveedor:

- Coordinar la realización de los servicios contratados, cumpliendo con los nivel de servicio especificados.
- ~~Generar un canal de comunicación eficiente entre SHF y el Proveedor.~~
- Proporcionar a solicitud de SHF en todo momento, cualquier estatus referente a la realización de los servicios contratados.
- Apoyar a la definición y mejora de los procesos y documentos requeridos para la interacción operativa entre SHF y el proveedor.
- Participar junto con el personal de SHF en reuniones de trabajo y seguimiento periódicos, relativos a los servicios proporcionados por el Proveedor.
- Asegurar el cumplimiento de los tiempos comprometidos con SHF.

54 de 60



Generar



HACIENDA
SECRETARÍA DE HACIENDA Y CRÉDITO PÚBLICO



Anexo A - Anexo Técnico%

- Cumplir con los entregables en tiempo, contenido y estándares de calidad establecidos por SHF para los servicios proporcionados por el Proveedor.
- En su caso, efectuar los ajustes solicitados por SHF, en relación a los entregables y documentación generados como resultado de los servicios proporcionados por el Proveedor.
- Una vez aceptados los entregables y documentos referidos, firmar conjuntamente con el Subdirector de Infraestructura Tecnológica, la Carta de Aceptación Técnica, previo a la presentación de la factura a SHF.
- Facilitar y dar el apoyo que el personal de SHF requiera para realizar las reuniones de trabajo y/o definición y seguimiento, en las oficinas de SHF o del mismo Proveedor.
- Coordinar la correcta gestión de los recursos operativos del Proveedor para la atención de los requerimientos de SHE

8. SOPORTE TÉCNICO Y MESA DE AYUDA.

El PROVEEDOR deberá proporcionar el servicio de mesa de ayuda, el cual deberá tener un esquema de 7*24*365. El servicio podrá ser prestado vía telefónica o en sitio, de acuerdo a la magnitud del evento y/o consideración de Sociedad Hipotecaria Federal. El servicio de soporte técnico incluye el apoyo a los ingenieros de Sociedad Hipotecaria Federal para:

- . Aclaración de dudas técnicas
- . Atención de incidentes suscitados en la operación (mantenimiento correctivo) - Configuración de los equipos o apoyo en la habilitación de nuevas funcionalidades

El Proveedor deberá proporcionar un número telefónico y dirección de correo electrónico de la mesa de ayuda, con el objeto de brindar tanto soporte técnico como levantamiento de los reportes de servicio.

Por cada servicio efectuado, la empresa entregará a SHF un reporte en donde se anotará el número de control asignado y la información necesaria para llevar un adecuado manejo histórico de los servicios atendidos durante la vigencia del contrato; éste reporte será firmado de conformidad por el usuario, una vez que el servicio sea completado.

El reporte de servicio deberá ser completado de la siguiente manera:

- . Número de reporte
- . Nombre de la Persona responsable por parte de SHF. Teléfono

Anexo A - Anexo Técnico.

- Marca del equipo atendido.
- Modelo del equipo atendido.
- Número de serie del equipo atendido.
- Clasificación del reporte: servicio, incidente
- Descripción de la falla reportada por SHF o del servicio requerido por SHF

55 de 60



DE

PÚBLICO

- Nombre de la Persona que levanta el reporte por parte de la empresa. @
- Diagnóstico de incidente (si aplica)
- Descripción y documentación de la solución
- Nombre de la Persona que atiende el reporte por parte de la empresa.
- Fecha y hora de levantamiento del reporte. Fecha y hora de cierre del reporte

9. ENTREGABLES.

El proyecto tendrá los siguientes entregables:

- El Proveedor deberá entregar reportes mensuales a mes vencido, los primeros 5 días de cada mes de los mantenimientos preventivos, incidentes y solicitudes de soporte técnico, los cuales deben de incluir al menos la siguiente información: No. de folio o ticket, fecha inicial de la solicitud o incidente, descripción, solución y fecha de cierre.

- b) Fecha y hora de inicio del incidente.
- c) Fecha y hora de resolución del incidente.
- d) Servicio Telefónico afectado.
- e) Tiempo de afectación a cada Servicio Telefónico

56 de 60



Anexo A - Anexo Técnico%

En caso de no existir solicitudes de soporte técnico, incidentes o mantenimientos preventivos durante el período, deberá entregar el reporte declarando que no existieron..

El reporte de llamadas deberá contener lo siguiente:

1. El Reporte mensual debe enviarse vía correo electrónico al responsable designado por SHF para este efecto, un archivo en formato de Hoja de Cálculo de Excel con lo siguiente:
 - a) Por cada tipo de llamada saliente (local, larga distancia nacional, larga distancia internacional, celular local, celular nacional, celular internacional):
 - Detalle de la llamada:
 - Identificación del número

 - Hora de inicio
 - Hora de término
 - Duración
 - Importe de la llamada, en moneda nacional
 - Número total de llamadas por tipo de llamada
 - Importe total de las llamadas por tipo de llamada
2. Reporte mensual de incidentes. Informe de todos los incidentes en el mes, con el detalle de cada uno:
 - a) Descripción del incidente.



HACIENDA
SECRETARÍA DE HACIENDA Y CRÉDITO PÚBLICO



10. GARANTÍAS.

De conformidad con el Artículo 48 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, el Proveedor garantizará los servicios, mediante fianza expedida por institución financiera autorizada, por el 10% del importe máximo del contrato antes del Impuesto al Valor Agregado.

Anexo A - Anexo Técnico.

11. ÁREAS DE TRABAJO Y CONEXIÓN DIRECTA A LA RED DE SHF.

Para la realización de los servicios descritos en el presente documento en tiempo y forma, el Proveedor deberá contar con la infraestructura y equipo necesario.

12. REQUISITOS PARA PRESENTAR LA SOLICITUD DE PAGO Y CONDICIONES DE PAGO.

Los servicios contratados, serán pagados contra entrega y aprobación de los servicios y documentación solicitada para cada entregable, y una vez que éstos estén a entera satisfacción de SHF, observando lo que a continuación se indica.

El pago se realizará en moneda nacional, a mes vencido, en un plazo no mayor de 20 días naturales contados a partir de la fecha en que se haya recibido la factura correspondiente, debidamente requisitada, como resultado de la aceptación a entera satisfacción de SHF, de los entregables previamente definidos para estos efectos.

El pago de los servicios se realizará conforme a las políticas y procedimientos establecidos por la Subdirección de Recursos Materiales de SHF para el pago a Proveedores, observando invariablemente el siguiente procedimiento:

Deberá efectuarse la entrega/recepción de los bienes y/o servicios en SHF y se revisará el cumplimiento de los mismos, de acuerdo a lo establecido en el contrato y sus anexos.

1. El Proveedor hará entrega de la CARTA DE ACEPTACIÓN TÉCNICA de los entregables debidamente firmada por él y por los participantes establecidos por SHF.



Anexo A - Anexo Técnico.

DE

PUBLICO

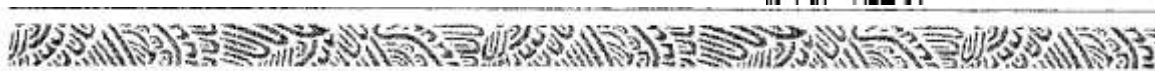


2. Aceptados los servicios y/o entregables y formalizada la CARTA DE ACEPTACIÓN TÉCNICA, el proveedor estará en condiciones de presentar su factura a revisión para pago.
 - El proveedor hará entrega de la factura correspondiente a la Subdirección de Recursos Materiales, quién a su vez solicitará la autorización de pago por los canales definidos. Ambos procesos de acuerdo a las políticas, procedimientos y tiempos establecidos para tales efectos en SHF y en el clausulado del contrato.

El no sujetarse al procedimiento establecido, significará que SHF no llevó a cabo la revisión a su entera satisfacción y por tanto, los bienes o servicios se tendrán por no aceptados, en cuyo caso, SHF se reserva el derecho de devolver la factura al Proveedor, cuando ésta haya sido entregada sin mediar el procedimiento establecido o bien presente algún error.

13. NIVEL DEL SERVICIO Y PENALIZACIONES.

Descripción de la métrica	Porcentaje Mínimo	Métrica	Ventana de medición	Penalización
		SOCIEDAD HIPOTECARIA FEDERAL		
Tiempo solución a fallas de hardware	>= 99.95 %	2 horas a partir de la generación del ticket en mesa de ayuda	mensual	5 al milla cada hora de atraso monto de facturación
Tiempo solución a fallas de software	99.95/0	3 horas a partir de la generación del ticket en mesa de ayuda	mensual	5 al milla cada hora de atraso monto de facturación
Finalización de la fase de migración y planeación	Con base en el plan de trabajo establecido.	31. de marzo de 2021	Única	5 al milla cada día de atraso monto de facturación del p mes servicio.
Fallas después de realizado el mantenimiento preventivo	99.95%	2 horas a partir de la generación del ticket en mesa de ayuda	mensual	5 al milla cada hora de atraso monto total facturación



HACIENDA

SOCIEDADHIPOTECARIA
FEDERAL

A - Anexo Técnicoa
Anexo

14. PROPOSICIÖN ECONOMICA

Anexo - Anexo Técnico.

A CANTIDAD	B TIPO DE ELEMENTO	C NÚMERO DE MESES	D IMPORTE UNITARIO		E IMPORTE TOTAL	
			(M.N. IVA)	sin IVA)	(M.N. IVA)	sin IVA)
20	Switch de 48 puertos PoE	45				
2	Switch para Centro de Datos	45				
2	Switch Core	45				
1	Herramienta de administración, análisis y monitoreo de la red	45				
1	Plataforma de Control de Identidad y Acceso a la red.	45				
1	Plataforma de Gestión de Permisos de Navegación en Internet	45				
1	Router Cisco C881	45				
2	Controladora WiFi	45				
40	Access Point Primario	45				
27	Access Point Secundario	45				
1	Plataforma de localización de activos	45				
1	Sistema de Control de usuarios basados en certificados	45				
1	Funciones de Seguridad y de Enrolamiento	45				
26	Jumpers de fibra a 10Gb para interconexión entre Switches Core y Switches de Acceso en MDF's	45				
			TOTAL			

WJ

1



A - Anexo Técnico
A

La descripción de las columnas es:

DESCRIPCIÓN

COLUMNA	
	Cantidad de elementos requeridos
	Descripción del elemento requerido
	Número de años en que se cubrirá el importe cotizado
	Importe por elemento (unidad)
	Columna A multiplicada por el número de elementos
TOTAL r COTIZACIÓN	Suma de los importes de la columna E (Importe total), monto que será tomado en consideración para efectos de cotización



HACIENDA

HIPOTECARIA

SOCIEDAD

FEDERAL

SECRETARÍA DE HACIENDA Y CRÉDITO PÚBLICO



Solicitud de Información sobre Soluciones Tecnológicas.

RA — Requerimiento de Información.

CONTRATACIÓN DEL SERVICIO ADMINISTRADO DE LA RED LAN PARA SHF.

Área solicitante: Subdirección de Infraestructura Tecnológica (SIT).
Tel: 5263-4500 ext. 4940.

Fecha: Enero del 2021.

Estimado: PROVEEDOR.

Sociedad Hipotecaria Federal, como entidad del Gobierno Federal, sus actividades de suministro, arrendamientos y servicios, están reguladas entre otras disposiciones por la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, y su Reglamento.

En este sentido y en términos de lo previsto en el artículo 2, fracción X de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, su representada ha sido identificada por Sociedad Hipotecaria Federal, como un posible prestador de servicio y/o proveedor.

Razón de lo anterior y con el objeto de identificar: a).- la existencia de bienes, arrendamientos o servicios en las condiciones solicitadas por Sociedad Hipotecaria Federal, b).- proveedores a nivel nacional o internacional, y c).- el precio estimado; nos permitimos solicitar su valioso apoyo a efecto de proporcionarnos una cotización de los bienes y/o servicios y/o arrendamientos descritos más adelante en el siguiente documento.

HACIENDA

SOCIEDAD

HIPOTECARIA

FEDERAL

Su cotización se requiere enviarla a nombre del Lic. Eduardo Morales Barrios, con número de teléfono 5263-4500 ext. 4940, debiendo remitirla en primera instancia vía correo electrónico a la dirección emorales@shf.gob.mx, con copia a meulogio@shf.gob.mx; xterna200@shf.gob.mx y posteriormente

Ejército Nacional 180, 7º Piso, Col. Anzures, Del. Miguel Hidalgo, México, D.F., CP 11590.

Ejército Nacional 180, Col. Azures, C.P. 11590, Miguel Hidalgo, Ciudad de México.
Tel: 55 5263 4500 www.gob.mx/shf



(vía mensajería) en original debidamente firmada por persona facultada, a la siguiente dirección: Ejército Nacional 180, 7º Piso, Col. Anzures, Del. Miguel Hidalgo, México, D.F., CP 11590.



HACIENDA
SECRETARÍA DE HACIENDA Y CRÉDITO PÚBLICO



A continuación, se extiende la presente Solicitud de Información (Request For Information o RFI), con la finalidad de que pueda analizar los requerimientos y demás términos contenidos en este documento y presentar una cotización referente a la Contratación del Servicio Administrado de la Red Lan para SHF, de conformidad con lo siguiente:

1. INTRODUCCIÓN.

SHF es una Institución Financiera perteneciente a la Administración Pública Federal, como entidad paraestatal en su carácter de Banca de Desarrollo, cuyo objetivo es impulsar el desarrollo de los mercados primario y secundario de crédito a la vivienda, mediante el otorgamiento de garantías destinadas a la construcción, adquisición y mejora de vivienda, preferentemente de interés social; al incremento de la capacidad productiva y del desarrollo tecnológico relacionados con la vivienda; así como a los financiamientos relacionados con el equipamiento de conjuntos habitacionales.

HACIENDA

SOCIEDAD

HIPOTECARIA

2. REQUERIMIENTOS DE SHF.

Por la importancia que tienen las comunicaciones de voz y datos para la operación de todas las áreas de la institución, resulta imperante para SHF, contar con los servicios administrados para la Red Lan, e i no contar con los servicios activos afectaría el cumplimiento de la normatividad para las entidades financiera y en la operación con dependencias externas y entre las áreas internas.

Los requerimientos técnicos se encuentran establecidos en el anexo A (Proposición técnica) adjunto a este RFI, con la finalidad de obtener una propuesta técnica y económica por cada uno de los proveedores participantes, donde dicha propuesta deberá cubrir en su totalidad los servicios establecidos por SHF en un marco que garantice la calidad de los mismos.

Para la presentación de la propuesta económica, los proveedores interesados deberán ajustarse al formato señalado en el numeral 4 de este documento de RFI y proporcionar los datos solicitados dentro del numeral 3 siguiente y lo especificado en el Anexo 1 del presente documento.

3. DATOS DEL LICITANTE.

EL LICITANTE deberá proporcionar los siguientes datos:



SECRETARÍA DE HACIENDA Y CRÉDITO PÚBLICO



FEDERAL

COMPañÍA Y DATOS DE REFERENCIA	CONTACTO	CORREO ELECTRÓNICO	DIRECCIÓN	TELÉFONO	TELÉFONO
Nombre de la compañía: Tipo de sociedad: Página Web:	Nombre de la persona responsable de la información contenida en este RH	dirección de email	Dirección de Localización de la compañía (las que apliquen): Oficinas corporativas Oficinas locales (MEX) Oficinas locales (USA) Oficinas locales (Europa) Otras oficinas		Numero teléfono: Numero de Fax:



HACIENDA

HIPOTECARIA

SOCIEDAD

FEDERAL

4. ESTIMADOS ECONÓMICOS PARA LA PROPUESTA.

EL PROVEEDOR DE SERVICIOS deberá entregar una propuesta económica que considere todos los elementos solicitados en este RFI.

La cotización deberá integrarse siguiendo invariablemente el formato descrito a continuación y en moneda nacional (MXN):

CANTIDAD DE ELEMENTOS	TIP O ELEMENTO	C	D	E	IMPORTE TOTAL	IMPORTE TOTAL
		NÚMERO DE MESES	IMPORTE UNITARIO (M.N. sin IVA)	IMPORTE TOTAL (M.N. sin IVA)		
		MESES			{M.N. sin IVA}	(M.N. sin IVA)
2	Switch Agregación 48 Puertos		48			
2	Switch Multigigabit 48 Puertos		48			
30	Switch POE 48 Puertos		48			
2	Controladora WiFi		48			
40	Access Point Primario		48			
27	Access Point Secundario		48			
1	Plataforma de localización de activos		48			
	Sistema de Control de usuarios basado en certificados		48			
	Funciones de Seguridad y de Enrolamiento		48			
26	Jumpers de fibra a IOGb para interconexión entre		48			

HACIENDA

SOCIEDAD

HIPOTECARIA

	Switches Core y Switches de Acceso en MDFs			
--	--	--	--	--

3

Ejército Nacional 180, Col. Azules, C.P. 11590, Miguel Hidalgo, Ciudad de México.
Tel: 55 5263 4500 www.gob.mx/shf



5

Ejército Nacional 100, Col. Azules, C.P. 11590, Miguel Hidalgo, Ciudad de México.
Tel: 55 5263 4500 www.gob.mx/shf

HACIENDA

HIPOTECARIA

SOCIEDAD

FEDERAL



HACIENDA
SECRETARÍA DE HACIENDA Y CRÉDITO PÚBLICO



TOTAL	
-------	--

La descripción de las columnas es:

COLUMNA

DESCRIPCIÓN

Cantidad de elementos requeridos del rubro.

Descripción del elemento requerido del rubro.

Número de meses a partir del rubro. Importe por elemento (unidad del rubro).

$E=A*C*D$ (el importe total del rubro es igual a la multiplicación de número de elementos o los meses del servicio el importe unitario).

TOTAL, Suma de los importes de la columna E (Importe total de los rubros), monto que será tomado COTIZACIÓN en consideración para efectos de cotización Nota importante:

Es requisito fundamental ajustarse al formato anterior, para efectos de su consideración en el presente estudio de mercado.

El monto de la propuesta deberá hacerse en Moneda Nacional (Pesos)

5. DOCUMENTACIÓN A ENTREGAR COMO PARTE DE LA PROPUESTA TÉCNICA

- Propuesta técnica cumpliendo o excediendo el 100% de las características mínimas establecidas en el anexo A (Proposición técnica). En caso de no cumplir al menos con el 100% de las características mínimas establecidas, la propuesta será desechada.
- Plan en el que deberá indicar las actividades a desarrollar para la entrega y configuración de los elementos solicitados; duración expresada en días y los recursos humanos a utilizar, que contemple todas las actividades del punto 8 Plan de Trabajo descritas en el anexo A (Proposición técnica).



6. CRITERIOS DE EVALUACIÓN

SHF verificará que las proposiciones que presenten los Proveedores, así como la documentación requerida, cumplan con los requisitos establecidos. La evaluación de la proposición técnica se realizará conforme al esquema del precio más bajo ofertado en la proposición económica.

SECRETARÍA DE

Financiero PÚBLICO



Una vez recibidas las proposiciones, se procederá a su apertura y se desecharán las que hubieren omitido alguno de los requisitos exigidos en estas Bases.

6.1. Proposición económica

EL PROVEEDOR deberá entregar una proposición económica que considere los servicios solicitados en este documento. A esta proposición económica se le denominará Monto Total de la proposición y deberá estar compuesto por la sumatoria Total de la columna Valor Total de los elementos correspondiente a lo establecido en la sección 4. Estimados económicos para la propuesta.

6.2. Criterios de Asignación

Sólo se podrá adjudicar el contrato a EL PROVEEDOR cuya proposición cumplió con los requisitos legales, haya presentado la documentación solicitada en el punto 5 y su proposición económica sea la más baja.

En caso de empate entre dos o más proposiciones, se procederá conforme a lo dispuesto por los artículos 36 Bis segundo y tercer párrafos de la Ley y conforme lo estipulado en la convocatoria de licitación.

Atentamente

5



HACIENDA

HIPOTECARIA

SOCIEDAD

FEDERAL

Eduardo Morales Barrios

Subdirector de Infraestructura Tecnológica



HACIENDA
SECRETARÍA DE HACIENDA Y CRÉDITO PÚBLICO



Solicitud de Información sobre Soluciones Tecnológicas.

RFI — Requerimiento de Información.

CONTRATACIÓN DEL SERVICIO ADMINISTRADO DE LA RED LAN PARA SHF

ANEXO 1 .

PARA FORMULAR SU COTIZACIÓN, LOS PROVEEDORES DEBERAN
CONSIDERAR LOS SIGUIENTES ASPECTOS:

Indicaciones generales.

Establecer claramente en su cotización el lugar y fecha.

. El archivo adjunto de especificaciones técnicas se hace consistir en Fojas.

Considerar en su cotización que el pago es a los 20 días naturales posteriores a la entrega de los servicios, previa aceptación por parte de SHF, así como lo siguiente:

1.- Las especificaciones de los bienes cotizados (que se anexan al presente).

HACIENDA

SOCIEDAD

HIPOTECARIA

FEDERAL

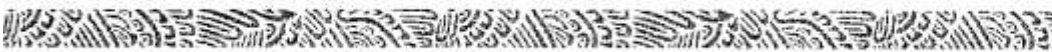
2.- EL LICITANTE deberá indicar dentro de su cotización lo siguiente:

- El Origen de los Bienes (nacional o importado) y, en su caso, el % (. correspondiente al grado de contenido nacional.
- En caso de que el proceso de fabricación de los bienes requeridos sea superior a 90 días, señale el tiempo que le corresponda a su producto:

FO-CON-04

6

Ejército Nacional 180, Col. Azules, C.P. 11590, Miguel Hidalgo, Ciudad de México.
Tel: 55 5263 4500 www.gob.mx/shf



Y

9

Ejército Nacional 100, Col. Azules, C.P. 11590, Miguel Hidalgo, Ciudad de México.
Tel: 55 5263 4500 www.gob.mx/shf



- Vigencia de su Propuesta o cotización hasta 3 meses a partir de la fecha de cotización.

3.- Los métodos de prueba empleados para la determinación de sus especificaciones, en caso de que estos sean diferentes a los señalados en la especificación de Sociedad Hipotecaria Federal, en caso de aplicar.

- Normas.
- Registros Sanitarios o Permisos Especiales.

4.- Condiciones de entrega [REQUERIDO POR SHFI:

- De acuerdo a los tiempos y condiciones establecidas en este RFI. ■
Entregas parciales con una vigencia máxima al (Fecha) —N/A—.
- Lugar de entrega será: oficinas de SHF.
- Anticipo: N/A.
- Para el caso de dudas, comentarios o aclaraciones remitirlas a los correos:

emorales@shf.gob.mx
meulogio@shf.gob.mx

5.- Garantías.

Tipos de garantía requeridas por SHF:

- Porcentaje de garantía de cumplimiento: 10⁰/0 del importe cotizado antes de IVA.
- De responsabilidad civil señalando su vigencia: _____.

Otras indicaciones.



HACIENDA
SECRETARÍA DE HACIENDA Y CRÉDITO PÚBLICO



EL LICITANTE deberá indicar el tiempo de experiencia comprobable en años prestando o suministrando los servicios o bienes de la misma naturaleza objeto del presente documento.

EL LICITANTE deberá señalar si para prestar o suministrar los servicios o bienes señalados utiliza distribuidores o canales autorizados, o bien lo realiza de manera directa.

EL LICITANTE deberá tomar en cuenta que la Fecha Lfmjite para presentar la Cotización es el 95

deEnetôde 2027)

Nota. - Para efectos de control interno, en el caso de no recibir respuesta o manifestar un inconveniente o imposibilidad, se procederá a hacer la anotación respectiva en nuestros registros, circunstancias que deberán ser consideradas al momento de definir el tipo de procedimiento de contratación.

Favor de enviar acuse de recibo de esta solicitud al correo electrónico a: emorales@shf.gob.mx y meuloqio@shf.gob.mx

NOTA: Vencido el plazo de recepción de cotizaciones, Sociedad Hipotecaria Federal al amparo de lo previsto en el artículo 26 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, definirá el procedimiento a seguir para la contratación, el cual puede ser: LICITACIÓN PÚBLICA; INVITACIÓN NACIONAL".

Este documento no genera obligación alguna para la dependencia o entidad.

	Funciones de *guridad y de Enrolamiento			
26	Jumpers da fibra a IOGb para entru Swi2ches Core y SwWws de Acwsa en MDFs	48		

Los precios expresados se encuentran en moneda nacional MXN,

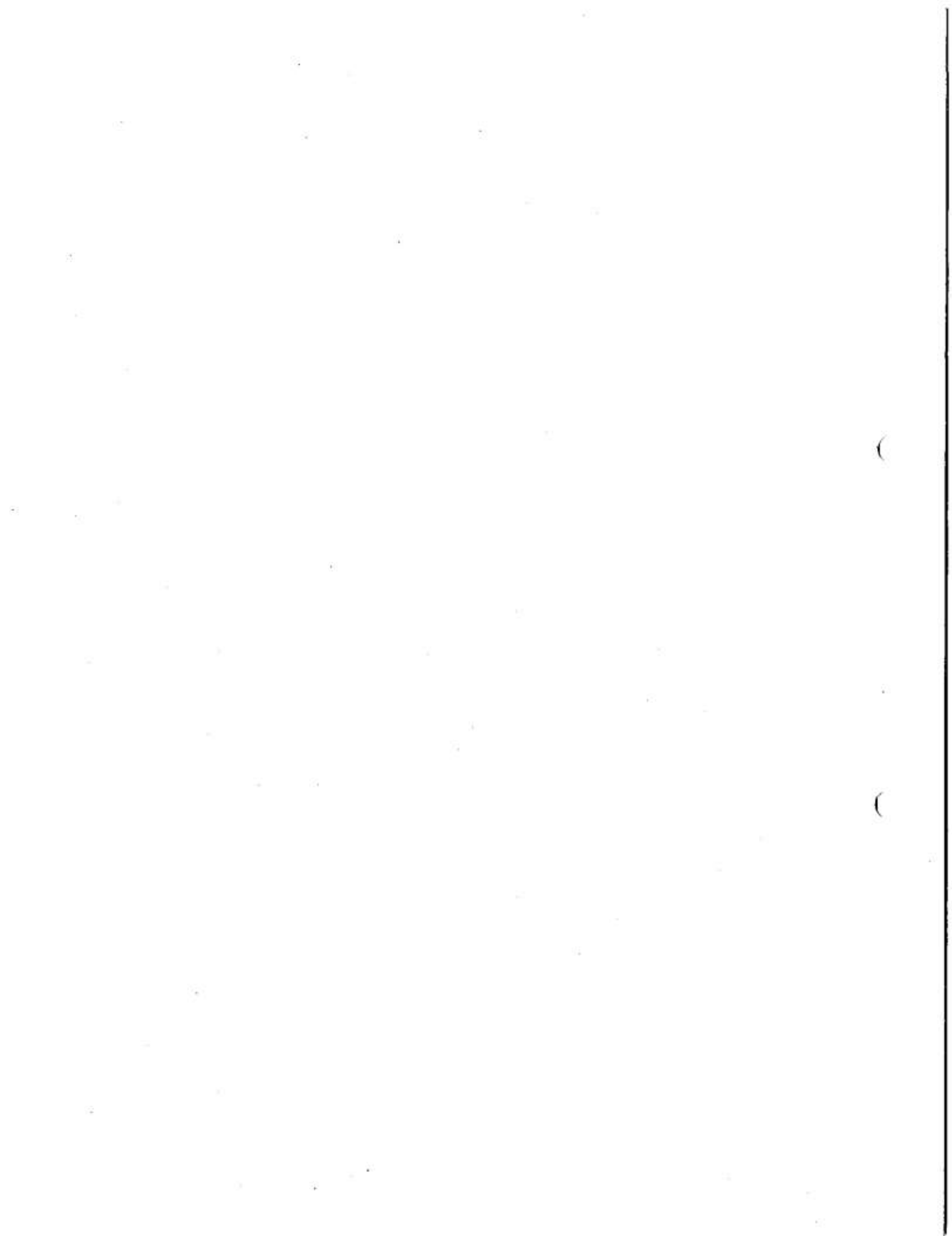
Propuesta valida por 60 días.

Esperamos que la información antes detallada cumpla con sus expectativas.

De antemano gracias,

Erika Patiño Schulenburg
Business Development Manager

Peten Sur Col., Narvarte. Delegacióri Benito Juárez, CDM,X, CP 03020



PROPUESTA ECONOMICA

SERVICIO ADMINISTRADO DE EQUIPOS PARA LA INFRAESTRUCTURA DE RED LAN.

Sociedad Hipotecaria Federal
Subdirección de Infraestructura Tecnológica
At'n. Lic. Eduardo Morales Barrios

Estimado Lic. Morales,
Adjunto Propuesta Económica, para la CONTRATACIÓN DEL SERVICIO ADMINISTRADO DE EQUIPOS PARA LA INFRAESTRUCTURA DE RED LAN.

CANTIDAD	DESCRIPCIÓN	CANTIDAD	PRECIO UNITARIO	TOTAL
2	Switch Agregación 48 Puertos	48	\$2,122,752.62	\$4,245,505.25
2	Switch Multigigabit 48 Puertos	48	\$955,860.94	\$1,911,721.89
30	Switch PoE 48 Puertos	48	\$576,417.89	\$17,292,536.74
2	Controladora WiFi	48	\$540,022.08	\$1,080,044.17
40	Access Point Primario	48	\$60,947.70	\$2,437,908.10
27	Access Point Secundario	48	\$27,465.97	\$741,581.11
1	Plataforma de localización de activos	48	\$437,986.51	\$437,986.51
1	Sistema de Control de usuarios basado en certificados	48	\$2,088,903.12	\$2,088,903.12
1	Funciones de Seguridad y de Enrolamiento	48	\$2,088,903.12	\$2,088,903.12
26	Jumpers de fibra a 10Gb para interconexión entre Switches Core y Switches de Acceso en MDF's	48	\$7,720.00	\$370,560.00
			TOTAL	\$32,695,650.00

Agradezco la atención, quedo pendiente de comentarios.

15 de enero del 2021

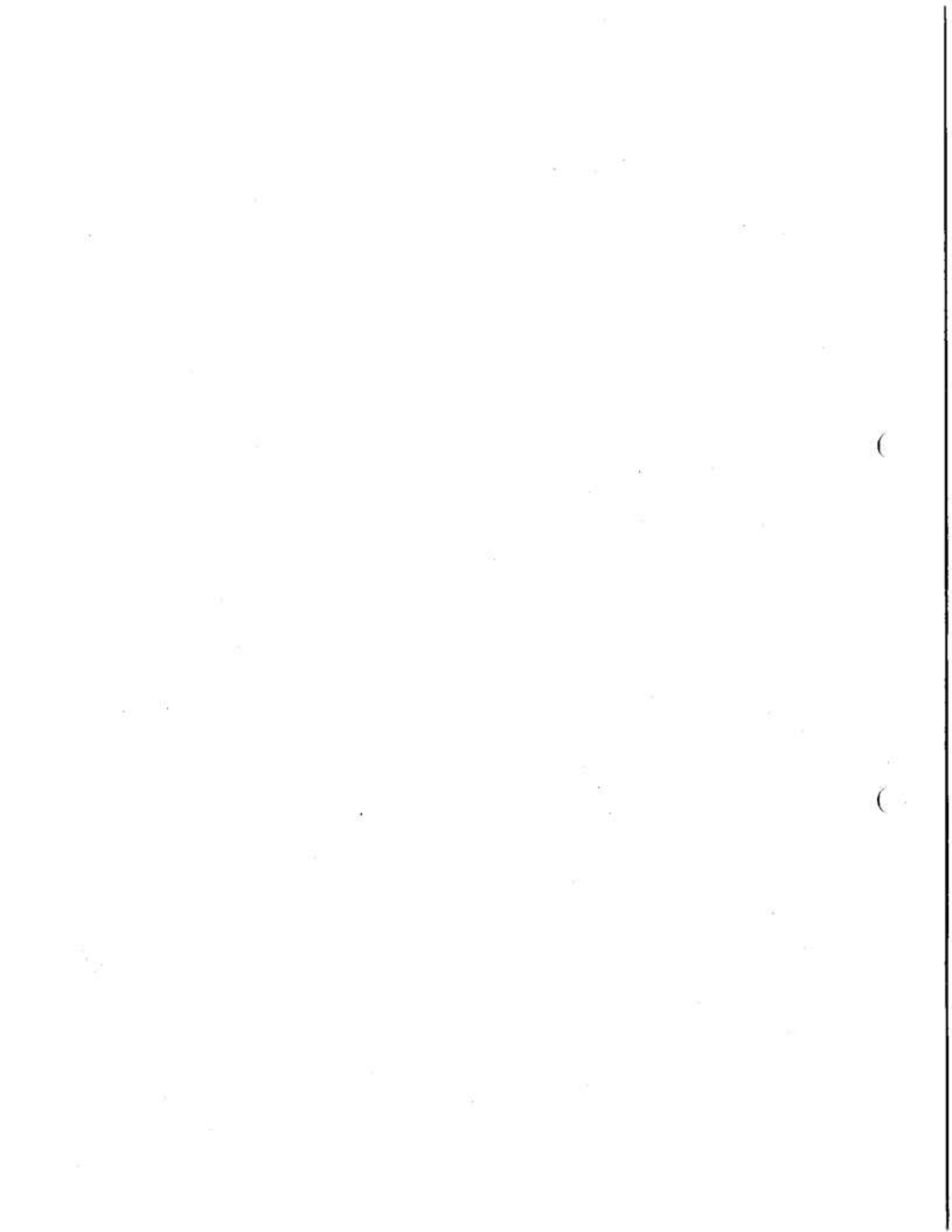
ATENTAMENTE
LUIS FERNANDO
REPRESENTANTE



GUTIERREZ MANZANO
LEGAL



TECNOLOGÍA Y MERCADOS EMERGENTES, S.A. DE C.V.



FORMATO DE COTIZACIÓN

CONTRATACIÓN DEL SERVICIO ADMINISTRADO DE
EQUIPOS PARA LA INFRAESTRUCTURA DE RED LAN

Ciudad de México, 15 de enero de 2021

LIC. EDUARDO MORALES BARRIOS
SUBDIRECTOR DE INFRAESTRUCTURA TECNOLÓGICA
SOCIEDAD HIPOTECARIA FEDERAL

Por este conducto pongo a su consideración nuestra propuesta para la
Contratación del Servicio Administrado de Equipos para la
Infraestructura de Red LAN.

COMPAÑÍA Y DATOS - DE REFERENCIA	APSFİNÍŞÖRACIÖN-DESOCIJCIONEŞİ?SÍAŞDECİVe
-PÁGINA wa	
-CONTACTO	ÓSCÄküViLCÀNÚEVASERkÂT:O
CORREECTR NICO	
DIRECCIÖN	

- CANTIDAD- ELÉMÉNİOS			tJÑITÁKİO	
				.esitíeiV:Â
2	Switch Agregación 48 Puertos	48		
2	Switch Multigigabit 48 Puertos	48		\$2,031 , 185.69
30	Switch POE 48 Puertos	48	\$612,43834	
2	Controladora WiFi	48	\$573,768.15	

Oficina

(81) 8123 2899



arsintegradores.com

40	Access Point Primario	48	\$64,756.33	\$2,590,253.36
27	Access Point Secundario	48	\$29,182.32	\$787,922.63
	Plataforma de localización de activos	48	\$465,356.36	\$465,356.36
	Sistema de Control de USUariOS basado en certificados	48	\$2,21	\$2,219,439.00
	Funciones de Seguridad y de Enrolamiento	48	\$2,219,439.00	\$2,219,439.00
26	Jumpers de fibra a IOGb para interconexión entre Switches Core y Switches de Acceso en MDF's	48	\$9,650.00	\$463,200.00
			TOTAL	\$34,808,290.00

Condiciones de entrega:

De acuerdo a los tiempos y condiciones establecidas en este RFI.

Vigencia de su Propuesta o cotización: 45 días

Entregas parciales con Una vigencia máxima a l (Fecha): No Aplica

Lugar de entrega será: Oficinas de SHF

Anticipo: No Aplica

Ángel óscar Villanueva Serrato

Representante Legal

ARS Integración de Soluciones S.A. de C.V.

Oficina

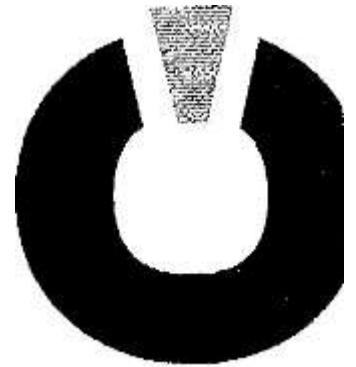
(81) 8123 2899

Tepatitlán 201 Col. Mitras Sur, Mty. Nb, 64020

silcom@

DesarrollosTI

Constitución 814
Santa Catarina, 66350, NL.



Santa Catarina, NL, 15 de enero del 2021

LIC. EDUARDO MORALES BARRIOS
SUBDIRECTOR INF-RAE-STRUCTURA TECNOLÓGICA
SOCIEDAD HIPOTECARIA FEDERAL

P R E S E N T E

Estimado Lic. Morales:

Anexo la cotización de nuestra empresa.

EMPRESA	
Compañía y datos de referencia	SILCOM INFORMÁTICA Y COMUNICACIONES, S.A. DE C.V. TIPO DE SOCIEDAD: SOCIEDAD ANÓNIMA PAGINA WEB: www.silcom.com.mx
Contacto	Juan Antonio Serrato Vázquez
Correo electrónico	licitaciones@silcom.com.mx
Dirección	Constitución 814, Centro de Santa Catarina, Santa Catarina, NL 66350
Teléfono	+52 (81) 8151-7901

COTIZACIÓN				
CANTIDAD	TIPO DE ELEMENTO	MESES	PRECIO UNITARIO (SIN IVA)	IMPORTE TOTAL (SIN IVA)
2	Switch Agregación 48 Puertos	48	\$2,183,220.34	\$4,366,440.67
2	Switch Multigigabit 48 Puertos	48	\$983,089.14	\$1,966,178.28
30	Switch PoE 48 Puertos	48	\$592,837.45	\$17,785,123.65
2	Controladora WIFI	48	\$555,404.89	\$1,110,809.79
40	Access Point Primario	48	\$62,683.83	\$2,507,353.18
27	Access Point Secundario	48	\$28,248.35	\$762,705.44
1	Plataforma de localización de activos	48	\$450,462.79	\$450,462.79
1	Sistema de Control de usuarios basado en certificados	48	\$2,148,406.61	\$2,148,406.61

led
2

o.(81) 8151 7901
silcom.com.mx



Constitución 814
Santa Catarina, 66350, NL



1	Funciones de Seguridad y de Enrolamiento	48	\$2,148,406.61	\$2,148,406.61
26	Jumpers de fibra a 10Gb para interconexión entre Switches Core y Switches de Acceso en MDFs	48	\$8,106.00	\$389,088.00
			SUBTOTAL	\$33,634,975.00
			IVA	\$5,381,596.00
			TOTAL	\$39,016,571.00

(

CONDICIONES	
Condiciones de venta:	De acuerdo a los tiempos y condiciones establecidas en este RFI.
Lugar de entrega:	Oficinas SHF
Vigencia de la cotización:	31 de marzo de 2020
Anticipo:	No aplica

Atentamente,



JUAN ANTONIO SERRATO VAZQUEZ.
REPRESENTANTE LEGAL
SILCOM INFORMÁTICA Y COMUNICACIONES, SA DE CV
licitaciones@silcom.com.mx



o. 8151 7901
silcom.com.mx



RESULTADO DE LA INVESTIGACIÓN DE MERCADO

CONTRATACIÓN DE SERVICIOS ADMINISTRADOS DE RED LAN PARA SHRF

CUADRO COMPARATIVO DE PRECIOS

15 DE MAYO 2021

Requisición: SIN NUMERO

de los servicios: NACIONAL

DESCRIPCIÓN	CANTIDAD	Máximo		Mínimo		Máximo	Mínimo	Máximo	Mínimo	VALOR TOTAL (MEDIANA)	10%
		Máximo	Mínimo	Máximo	Mínimo						
Switch Agregación 48 Puertos	2	\$4,510,807.55	\$4,742,475.55	\$4,956,440.57	\$4,745,905.25	\$4,438,624.11	\$4,892,486.52			\$4,438,624.11	\$4,892,486.52
Switch Multigigabit 48 puertos	2	\$2,051,165.69	\$2,135,504.20	\$1,695,178.28	\$1,511,721.69	\$1,996,681.99	\$2,198,850.16			\$1,996,681.99	\$2,198,850.16
Switch PoE 48 puertos	30	\$18,373,150.11	\$19,316,768.30	\$17,785,123.85	\$17,292,536.74	\$18,079,136.88	\$19,887,090.57			\$18,079,136.88	\$19,887,090.57
Controladora WiFi	2	\$1,147,536.30	\$1,205,471.97	\$1,110,809.79	\$1,080,044.17	\$1,125,173.05	\$1,242,090.35			\$1,125,173.05	\$1,242,090.35
Acceso Point Primario	40	\$2,590,253.36	\$2,723,284.71	\$2,507,353.19	\$2,437,908.10	\$2,548,803.27	\$2,803,683.50			\$2,548,803.27	\$2,803,683.50
Acceso Point Secundario	27	\$787,922.83	\$828,369.11	\$762,705.44	\$741,581.11	\$775,314.04	\$852,845.44			\$775,314.04	\$852,845.44
Plataforma de localización de activos	1	\$463,356.36	\$489,256.33	\$450,462.79	\$437,986.51	\$457,909.59	\$503,700.53			\$457,909.59	\$503,700.53
Sistema de Control de usuarios basada en certificados	1	\$2,219,439.00	\$2,333,425.81	\$2,148,406.61	\$2,086,803.12	\$2,183,922.81	\$2,402,315.09			\$2,183,922.81	\$2,402,315.09
Funciones de Seguridad y de Enroscamiento	1	\$2,219,439.00	\$2,333,425.81	\$2,148,406.61	\$2,086,803.12	\$2,183,922.81	\$2,402,315.09			\$2,183,922.81	\$2,402,315.09
Jumpers de fibra a 10Gb para interconexiones entre Switches y Switches de Acceso a MDF's	26	\$463,200.00	\$416,880.00	\$389,086.00	\$370,560.00	\$402,984.00	\$443,282.40			\$402,984.00	\$443,282.40
TOTAL	132	\$54,888,290.00	\$36,525,679.99	\$33,634,975.02	\$32,695,650.01	\$34,186,472.51	\$37,618,319.76			\$34,186,472.51	\$37,618,319.76

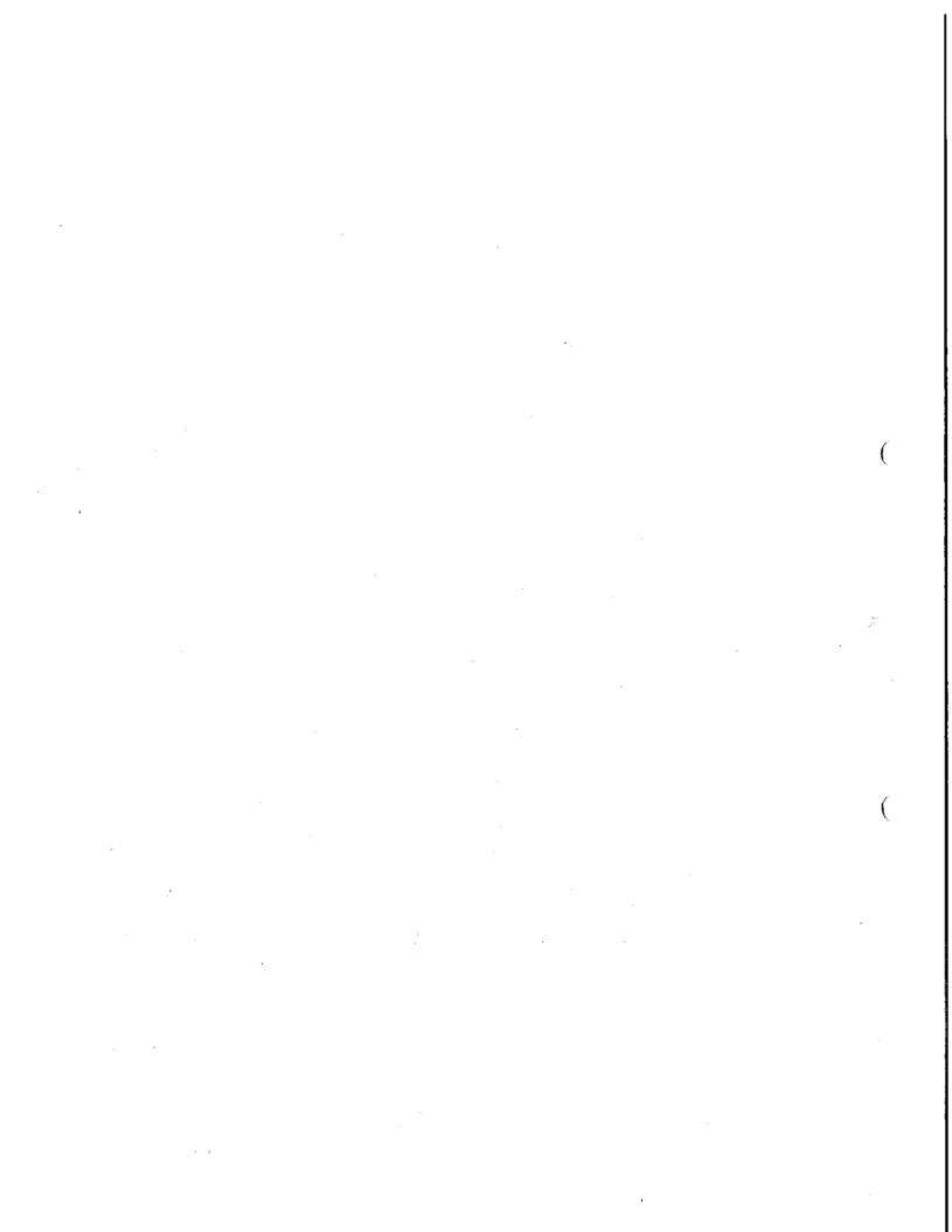
INFORMACIÓN OBTENIDA DE PROVEEDORES DEL RAMO CORRESPONDIENTE (INCISO II DEL ART. 28 DEL RIAASSP)

Mediana

ELABORÓ

Lic. Eduardo Morales Barrios

FO-COM-05





Sociedad Hipotecaria Federal

SOCIEDAD HIPOTECARIA FEDERAL

INVESTIGACIÓN DE MERCADO

CONTRATACIÓN DEL SERVICIO ADMINISTRADO DE LA RED LAN PARA SHF.

Nombre del proveedor (2)	Número de identificación del bien, arrendamiento o servicio (3)	Proporciona las condiciones solicitadas de calidad y oportunidad (4)	Cantidad que puede surtir (5)	Origen del bien (6)	Requisito 1 (7)	Precio (8)
ARS INTEGRACIÓN DE SOLUCIONES, S. A. DE C. V.	1	Se indica en el Anexo A	Todas	Nacional	Se indica en el Anexo A	\$34,808,290.00
IMPORTE COTIZADO						
Redes y Colaboración Digital, S. A. de C. V.	1	Se indica en el Anexo A	Todas	Nacional	Se indica en el Anexo A	\$36,525,880.00
IMPORTE COTIZADO						
SILCOM INFORMÁTICA Y COMUNICACIONES, S. A. DE C. V.	1	Se indica en el Anexo A	Todas	Nacional	Se indica en el Anexo A	\$33,634,975.00
IMPORTE COTIZADO						
TECNOLOGÍA Y MERCADOS EMERGENTES, S. A. DE C. V.	1	Se indica en el Anexo A	Todas	Nacional	Se indica en el Anexo A	\$32,695,650.00
IMPORTE COTIZADO						



SOCIEDAD HIPOTECARIA FEDERAL

Sociedad Hipotecaria Federal

INVESTIGACIÓN DE MERCADO

CONTRATACIÓN DEL SERVICIO ADMINISTRADO DE LA RED LAN PARA SHF.

Fecha (9)	15 DE ENERO DEL 2021
No. de requisición (10)	
Procedimiento (11)	COMPARACIÓN DE PRECIOS

No. de Partida (12)	CUCOP (13)	DESCRIPCIÓN (14)
31904	319040004	SERVICIOS INTEGRALES DE INFRAESTRUCTURA DE CÓMPUTO

FUENTES CONSULTADAS (15)

- COMPRANET
- COMPRANET-IM
- INTERNET
- PROVEEDORES SERVICIO

Elaboró (16)

Lic. Eduardo Morales Barrios